Bereitstellen von VMware Identity Manager in der DMZ

VMware Identity Manager 2.9.1
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

Bereitstellen von VMware Identity Manager in der DMZ

Bereitstellen von VMware Identity Manager in der DMZ bietet Erläuterungen zum Bereitstellen von VMware Identity Manager in der DMZ statt im internen Netzwerk. Informationen zum Bereitstellen von VMware Identity Manager im internen Netzwerk finden Sie unter *Installieren und Konfigurieren von VMware Identity Manager*.

Angesprochene Zielgruppe

Die Informationen sind für erfahrene Windows- und Linux-Systemadministratoren bestimmt, die mit den VMware-Technologien, speziell mit vCenter™, ESX™ und vSphere® sowie mit Netzwerkkonzepten, Active Directory und Datenbanken vertraut sind. Das zugrunde liegende Betriebssystem für die virtuellen Appliances VMware Identity Manager und VMware Identity Manager Connector ist SUSE Linux 11.

Die Kenntnis anderer Technologien wie der Adaptiven RSA-Authentifizierung, RSA SecurID und RADIUS ist ebenfalls hilfreich, wenn Sie diese Funktionen implementieren möchten.

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.

1 Bereitstellungsmodelle

Es sind zwei grundsätzliche Arten von Modellen für die Bereitstellung von VMware Identity Manager in der DMZ verfügbar: Das eine Modell wird in eine VMware AirWatch®-Bereitstellung integriert und für das andere Modell ist AirWatch nicht erforderlich, da es VMware Identity Manager Connector verwendet.

Sie haben auch die Möglichkeit, Bereitstellungsmodelle zu kombinieren, wenn Sie eine Funktionalität benötigen, die nur in einem der Modelle unterstützt wird.

- Bereitstellungsmodell mit AirWatch Cloud Connector

  Wenn Sie über eine vorhandene AirWatch-Bereitstellung verfügen, können Sie VMware Identity Manager in diese schnell integrieren. In diesem Modell werden Benutzer und Gruppe von Ihrem Unternehmensverzeichnis synchronisiert. Die Benutzerauthentifizierung wird von AirWatch gesteuert. Sie stellen VMware Identity Manager in der DMZ bereit.

  Beachten Sie, dass die Integration von VMware Identity Manager in Ressourcen wie Horizon 7 und in von Citrix veröffentlichten Ressourcen in diesem Modell nicht unterstützt wird. Es wird nur die Integration in Web-Anwendungen und in native mobile Anwendungen unterstützt.

  Siehe „Lokales Bereitstellungsmodell unter Verwendung von AirWatch Cloud Connector“, auf Seite 8.

- Bereitstellungsmodell unter Verwendung von VMware Identity Manager Connector (im ausgehenden Verbindungsmodus)

  In Szenarien, für die keine AirWatch-Bereitstellung erforderlich ist, können Sie die virtuelle VMware Identity Manager Server-Appliance in der DMZ und eine virtuelle VMware Identity Manager Connector-Appliance im Unternehmensnetzwerk installieren. Der Konnektor verbindet den Server mit lokalen Diensten wie z. B. Active Directory. Der Konnektor wird im ausgehenden Verbindungsmodus installiert und benötigt keinen geöffneten eingehenden Firewall-Port 443. In diesem Modell werden Benutzer und Gruppe von Ihrem Unternehmensverzeichnis synchronisiert und die Benutzerauthentifizierung wird von VMware Identity Manager Connector gesteuert.

  Siehe „Lokales Bereitstellungsmodell unter Verwendung von VMware Identity Manager Connector im ausgehenden Verbindungsmodus“, auf Seite 10.

  - Hinzufügen der Unterstützung der Kerberos-Authentifizierung zu Ihrer VMware Identity Manager Connector-Bereitstellung

    Sie können die Kerberos-Authentifizierung für interne Benutzer (dafür ist die eingehende Verbindungsmodus erforderlich) Ihrer Bereitstellung auf der Basis der ausgehenden Verbindungskonnektoren hinzufügen.

    Siehe „Hinzufügen der Unterstützung für die Kerberos-Authentifizierung zu Ihrer Bereitstellung“, auf Seite 12.

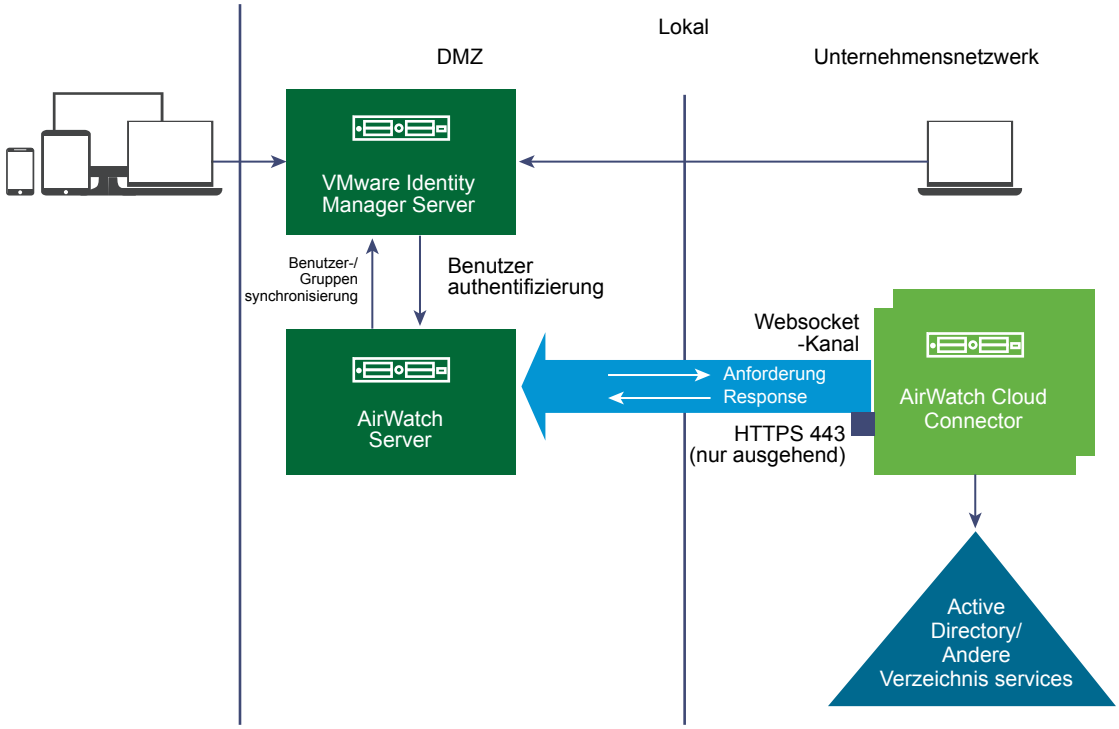
Dieses Kapitel behandelt die folgenden Themen:

Lokales Bereitstellungsmodell unter Verwendung von AirWatch Cloud Connector

Wenn Sie über eine vorhandene AirWatch-Bereitstellung verfügen, können Sie VMware Identity Manager in diese Ihren integrieren. Sie stellen die virtuelle VMware Identity Manager-Appliance in der DMZ bereit. In diesem Modell werden Benutzer und Gruppe von Ihrem Unternehmensverzeichnis synchronisiert. Die Benutzerauthentifizierung wird von AirWatch gesteuert.

Beachten Sie, dass die Integration von VMware Identity Manager mit Ressourcen wie Horizon 7 oder mit von Citrix veröffentlichten Ressourcen in diesem Modell nicht unterstützt wird. Es wird nur die Integration in Web-Anwendungen und in native mobile Anwendungen unterstützt.

Abbildung 1-1. Bereitstellung mit AirWatch Cloud Connector



Voraussetzungen

Sie müssen über folgende Komponenten verfügen:

- Eine AirWatch Server-Bereitstellung
- Eine AirWatch Cloud Connector-Instanz, die lokal bereitgestellt und in Ihr Unternehmensverzeichnis integriert ist

Port-Anforderungen

Die folgenden Ports sind für den VMware Identity Manager-Server erforderlich:

- Eingehender 443-Port (HTTPS)

- Eingehender 88-Port (TCP/UDP) – nur iOS
- Eingehender 5262-Port (TCP/UDP) – nur Android

Informationen zu den Anforderungen der AirWatch-Bereitstellung finden Sie in der AirWatch-Dokumentation.

Unterstützte Authentifizierungsmethoden

Dieses Bereitstellungsmodell unterstützt die im Folgenden aufgeführten Authentifizierungsmethoden. Diese Methoden sind über den integrierten Identitätsanbieter von VMware Identity Manager verfügbar.

- Kennwort (AirWatch Connector)
- Mobile SSO-Anmeldung (für iOS)
- Mobile SSO-Anmeldung (für Android)
- Geräte-Compliance (mit AirWatch)
- Zertifikat (Bereitstellung in der Cloud)
- VMware Verify

Unterstützte Verzeichnisintegrationen

Sie integrieren Ihr Unternehmensverzeichnis in AirWatch. In der AirWatch-Dokumentation finden Sie Informationen zu den unterstützten Verzeichnistypen.

Unterstützte Ressourcen

Sie können in diesem Bereitstellungsmodell folgende Ressourcentypen in VMware Identity Manager integrieren:

- Web-Anwendungen
- Native mobile Anwendungen

Sie können in diesem Bereitstellungsmodell folgende Ressourcentypen NICHT in VMware Identity Manager integrieren:

- Horizon 7, Horizon 6 oder View-Desktop- und Anwendungspools
- Von Citrix veröffentlichte Ressourcen
- Anwendungen im ThinApp-Paket
- Horizon Air – Cloud-gehostete Anwendungen und Desktops

Zusätzliche Info

- Kapitel 2, „Bereitstellen von VMware Identity Manager in der DMZ“, auf Seite 15
- Integrieren von AirWatch mit VMware Identity Manager im *Administratorhandbuch für VMware Identity Manager*.
- AirWatch-Dokumentation

Lokales Bereitstellungsmodell unter Verwendung von VMware Identity Manager Connector im ausgehenden Verbindungsmodus

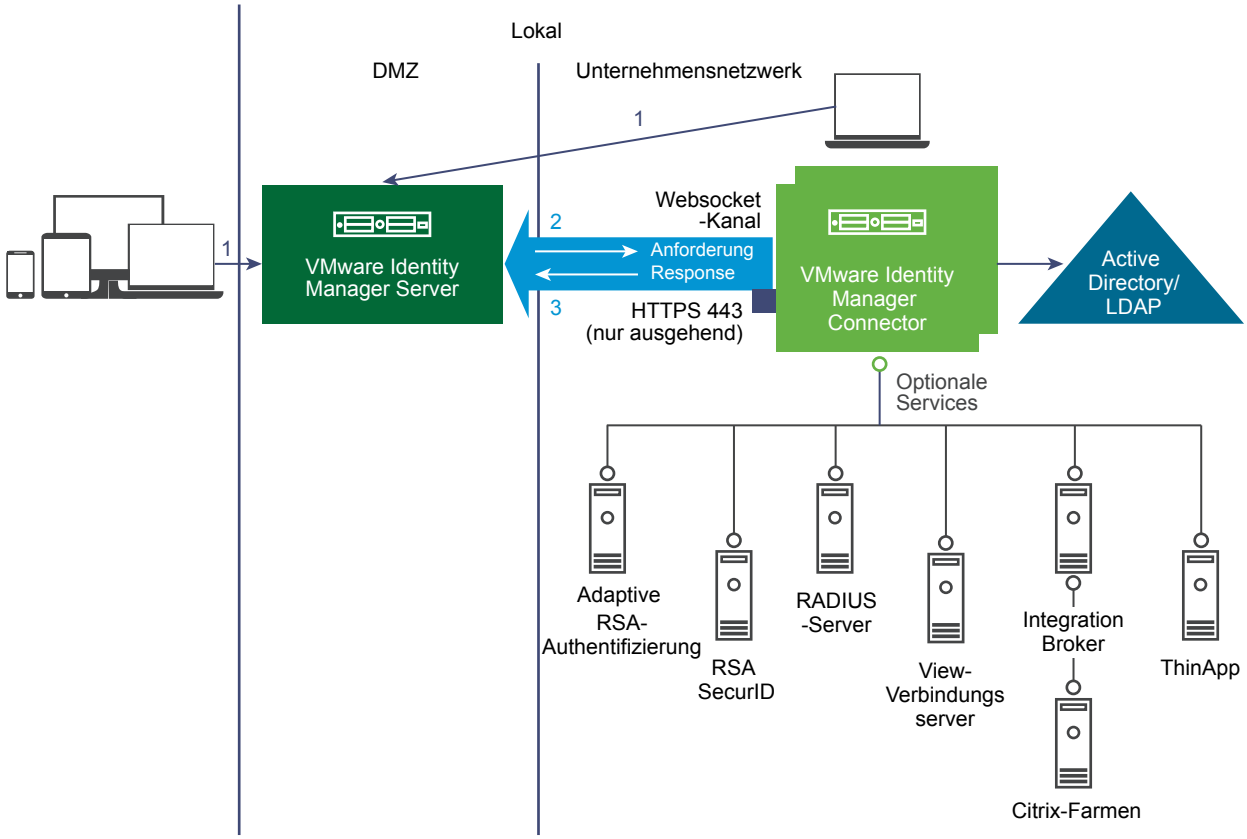
In diesem Modell installieren Sie die virtuelle VMware Identity Manager-Appliance in der DMZ. Sie installieren auch eine eigenständige virtuelle VMware Identity Manager Connector-Appliance im ausgehenden Verbindungsmodus im Unternehmensnetzwerk. Dieses Modell enthält keine AirWatch-Komponenten.

Benutzer und Gruppe werden von Ihrem Unternehmensverzeichnis synchronisiert, und die Benutzerauthentifizierung wird von einem eigenständigen VMware Identity Manager Connector gesteuert. Der Konnektor bietet auch die Möglichkeit, Ressourcen wie Horizon 7-Desktops und -Anwendungen mit dem VMware Identity Manager-Dienst zu synchronisieren.

Hinweis Für einige Authentifizierungsmethoden ist kein Konnektor erforderlich, da diese direkt vom Dienst verwaltet werden.

Wichtig Verwenden Sie den eigenständigen Konnektor zur Synchronisierung von Benutzern und Gruppen und für die Benutzerauthentifizierung anstelle des in die VMware Identity Manager-Appliance integrierten Konnektors.

Abbildung 1-2. Verwenden von VMware Identity Manager Connector im ausgehenden Modus



Port-Anforderungen

Die folgenden Ports sind für den VMware Identity Manager-Server erforderlich:

- Eingehender 443-Port (HTTPS)
- Eingehender 88-Port (TCP/UDP) – nur iOS

- Eingehender 5262-Port (TCP/UDP) – nur Android

VMware Identity Manager Connector wird im ausgehenden Verbindungsmodus installiert und benötigt keinen geöffneten eingehenden Port 443. Der Konnektor kommuniziert mit dem VMware Identity Manager-Dienst über einen Websocket-basierten Kommunikationskanal.

Unter Kapitel 2, „Bereitstellen von VMware Identity Manager in der DMZ“, auf Seite 15 und Kapitel 3, „Bereitstellen von VMware Identity Manager Connector im Unternehmensnetzwerk“, auf Seite 17 finden Sie eine vollständige Liste der Ports.

Unterstützte Authentifizierungsmethoden

Dieses Bereitstellungsmodell unterstützt alle Authentifizierungsmethoden. Für einige Authentifizierungsmethoden ist kein Konnektor erforderlich. Diese werden direkt durch den Service über den integrierten Identitätsanbieter verwaltet.

- Kennwort – verwendet den Konnektor
- Adaptive RSA-Authentifizierung – verwendet den Konnektor
- RSA SecurID – verwendet den Konnektor
- RADIUS – verwendet den Konnektor
- Zertifikat (Cloudbereitstellung) – über den integrierten Identitätsanbieter
- VMware Verify – über den integrierten Identitätsanbieter
- Mobile SSO-Anmeldung (iOS) – über den integrierten Identitätsanbieter
- Mobile SSO-Anmeldung (Android) – über den integrierten Identitätsanbieter
- Eingehendes SAML – über einen externen Identitätsanbieter

Hinweis Weitere Informationen zur Verwendung von Kerberos finden Sie unter „Hinzufügen der Unterstützung für die Kerberos-Authentifizierung zu Ihrer Bereitstellung“, auf Seite 12.

Hinweis Dieses Bereitstellungsmodell unterstützt nicht die Zertifkatauthentifizierung über den Konnektor. Die Authentifizierungsmethode „Zertifikat (Cloudbereitstellung)“ ist verfügbar.

Unterstützte Verzeichnisintegrationen

Sie können in diesem Bereitstellungsmodell folgende Typen von Unternehmensverzeichnissen in den VMware Identity Manager-Dienst integrieren:

- Active Directory über LDAP
- Active Directory, integrierte Windows-Authentifizierung.
- LDAP-Verzeichnis

  Wenn Sie ein LDAP-Verzeichnis integrieren möchten, sind unter „Integrieren in LDAP-Verzeichnisse“ in *Installieren und Konfigurieren von VMware Identity Manager* die entsprechenden Beschränkungen aufgeführt.

Alternativ können Sie mit den folgenden Methoden Benutzer im VMware Identity Manager-Dienst erstellen:

- Erstellen Sie lokale Benutzer direkt im VMware Identity Manager-Dienst.
- Erstellen Sie mit der Just-in-Time-Bereitstellung Benutzer im VMware Identity Manager-Dienst automatisch bei der Anmeldung und verwenden Sie dafür von einem externen Identitätsanbieter gesendete SAML-Assertionen.

Unterstützte Ressourcen

Sie können in diesem Bereitstellungsmodell folgende Ressourcentypen in den VMware Identity Manager-Dienst integrieren:

- Web-Anwendungen
- Horizon 7, Horizon 6 oder View-Desktop- und Anwendungspools
- Von Citrix veröffentlichte Ressourcen
- Anwendungen im ThinApp-Paket
- Horizon Air – Cloud-gehostete Anwendungen und Desktops (Tech Preview)

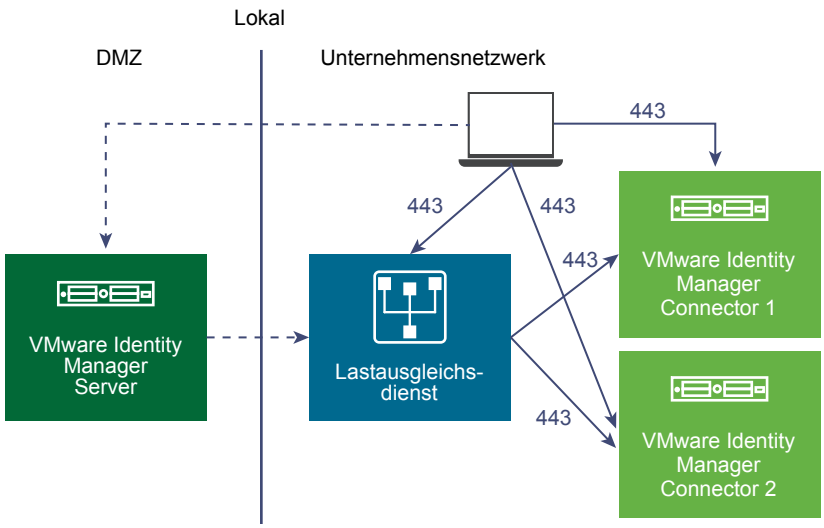
Zusätzliche Info

- Kapitel 2, „Bereitstellen von VMware Identity Manager in der DMZ“, auf Seite 15 und Kapitel 3, „Bereitstellen von VMware Identity Manager Connector im Unternehmensnetzwerk“, auf Seite 17
- Verzeichnisse
  - „Integrieren in Ihr Unternehmensverzeichnis“ in *Installieren und Konfigurieren von VMware Identity Manager*
  - „Verwenden von lokalen Verzeichnissen“ in *Installieren und Konfigurieren von VMware Identity Manager*
  - „Just-in-Time-Benutzerbereitstellung“ im *Administratorhandbuch für VMware Identity Manager*.
- „Konfigurieren der Benutzerauthentifizierung in VMware Identity Manager“ im *Administratorhandbuch für VMware Identity Manager*.
- *Einrichten von Ressourcen in VMware Identity Manager*

Hinzufügen der Unterstützung für die Kerberos-Authentifizierung zu Ihrer Bereitstellung

Sie können die Kerberos-Authentifizierung für interne Benutzer hinzufügen. Dafür ist die eingehende Verbindung für Ihre Bereitstellung auf der Basis der ausgehenden VMware Identity Manager-Verbindungskonnektoren erforderlich. Die gleichen Konnektoren können so konfiguriert werden, dass die Kerberos-Authentifizierung für Benutzer verwendet wird, die vom internen Netzwerk aus zugreifen, und eine andere Authentifizierungsmethode für Benutzer, die von außerhalb zugreifen. Dies kann durch die Definition von Authentifizierungsrichtlinien auf der Basis von Netzwerkbereichen erreicht werden.

Abbildung 1-3. Hinzufügen der Kerberos-Authentifizierung



Beachten Sie, dass die Konfiguration der Hochverfügbarkeit sich für die Kerberos-Authentifizierung unterscheidet.

Weitere Informationen finden Sie unter „Hinzufügen der Unterstützung für die Kerberos-Authentifizierung zu Ihrer VMware Identity Manager Connector-Bereitstellung“, auf Seite 29.

Bereitstellen von VMware Identity Manager in der DMZ

2

Sie können die virtuelle VMware Identity Manager-Appliance in der DMZ bereitstellen, wenn Sie diese nicht im Unternehmensnetzwerk bereitstellen möchten. Wenn Sie die VMware Identity Manager-Appliance in der DMZ bereitstellen, stellen Sie auch einen eigenständigen VMware Identity Manager Connector im ausgehenden Verbindungsmodus im Unternehmensnetzwerk bereit.

System- und Netzwerkkonfigurationen - Anforderungen

Die System- und Netzwerkkonfigurationsanforderungen für die Bereitstellung von VMware Identity Manager in der DMZ sind identisch mit den Anforderungen für die Bereitstellung von VMware Identity Manager im Unternehmensnetzwerk wie sie unter System- und -Netzwerkkonfigurationen – Anforderungen und Vorbereiten auf die Bereitstellung von VMware Identity Manager in *Installieren und Konfigurieren von VMware Identity Manager* beschrieben sind. Ausgenommen sind die hier aufgeführten Unterschiede.

- Sie müssen keinen eingehenden Firewallport für eine Appliance im Unternehmensnetzwerk öffnen.

  Die virtuelle VMware Identity Manager-Appliance wird in der DMZ bereitgestellt. VMware Identity Manager Connector wird im Unternehmensnetzwerk im ausgehenden Verbindungsmodus bereitgestellt und kommuniziert mit dem Dienst über einen Websocket-basierten Kommunikationskanal.

- Sie müssen für den externen Zugriff auf VMware Identity Manager keinen Reverse-Proxy-Server und keinen Lastausgleichsdienst bereitstellen.

- Ein Lastausgleichsdienst wird nur benötigt, wenn Sie eine Hochverfügbarkeit und eine Redundanz für die virtuelle VMware Identity Manager-Appliance konfigurieren.

- Die folgenden Ports werden verwendet. Ihre Bereitstellung benötigt möglicherweise nur einen Teil davon.

Port	Quelle	Ziel	Beschreibung
443	Lastausgleichsdienst	Virtuelle VMware Identity Manager-Appliance	HTTPS
443	Virtuelle VMware Identity Manager-Appliance	Virtuelle VMware Identity Manager-Appliance	HTTPS
443	Browser	Virtuelle VMware Identity Manager-Appliance	HTTPS
88	Browser	Virtuelle VMware Identity Manager-Appliance	TCP/UDP Nur iOS
5262	Browser	Virtuelle VMware Identity Manager-Appliance	TCP/UDP Nur Android
443	Virtuelle VMware Identity Manager-Appliance	vapp-updates.vmware.com	Zugriff auf den VMware-Upgrade-Server

Port	Quelle	Ziel	Beschreibung
8443	Browser	Virtuelle VMware Identity Manager-Appliance	Administratorport HTTPS
25	Virtuelle VMware Identity Manager-Appliance	SMTP-Server	TCP-Port zum Weiterleiten ausgehender E-Mails
53	Virtuelle VMware Identity Manager-Appliance	DNS-Server	TCP/UDP Jede virtuelle Appliance muss über Zugriff auf den DNS-Server über Port 53 verfügen und eingehenden SSH-Datenverkehr über Port 22 zulassen.
TCP: 9300-9400 UDP: 54328	Virtuelle VMware Identity Manager-Appliance	Virtuelle VMware Identity Manager-Appliance	Überwachungsanforderungen
5432	Virtuelle VMware Identity Manager-Appliance	Datenbank	Der PostgreSQL-Standardport ist 5432. Der Oracle-Standardport ist 1521.
443	Virtuelle VMware Identity Manager-Appliance	AirWatch REST-API	HTTPS Für die Compliance-Überprüfung von Geräten und die Authentifizierungsmethode „ACC-Kennwort“, wenn diese verwendet wird.

Bereitstellen der VMware Identity Manager-Appliance

Informationen zum Bereitstellen und Konfigurieren der virtuellen VMware Identity Manager-Appliance finden Sie unter Bereitstellen von VMware Identity Manager und Verwalten der Systemkonfigurationseinstellungen der Appliance in *Installieren und Konfigurieren von VMware Identity Manager*.

Konfigurieren für Failover und Redundanz

Informationen zum Konfigurieren von Failover und Redundanz für die virtuelle VMware Identity Manager-Appliance finden Sie in den folgenden Abschnitten in *Installieren und Konfigurieren von VMware Identity Manager*:

- Konfigurieren von Failover und Redundanz in einem einzelnen Rechenzentrum
- Bereitstellen von VMware Identity Manager in einem sekundären Rechenzentrum für Failover und Redundanz

Hinweis Der Abschnitt „Aktivieren des externen Zugriffs auf VMware Identity Manager mithilfe eines Lastausgleichsdienstes“ ist nicht anwendbar auf Szenarien, in denen VMware Identity Manager in der DMZ bereitgestellt wird.

Bereitstellen von VMware Identity Manager Connector im Unternehmensnetzwerk

3

Wenn Sie die virtuelle VMware Identity Manager-Appliance in der DMZ bereitstellen, müssen Sie auch eine eigenständige VMware Identity Manager Connector-Appliance in Ihrem Unternehmensnetzwerk im ausgehenden Verbindungsmodus bereitstellen.

Der Konnektor verbindet den VMware Identity Manager-Dienst mit anderen Komponenten im Unternehmensnetzwerk wie z. B. Active Directory und Horizon 7.

Der Konnektor kommuniziert mit dem Dienst im ausgehenden Verbindungsmodus über einen Kommunikationskanal.

Hinweis Wenn Sie über eine AirWatch-Bereitstellung verfügen und AirWatch Cloud Connector verwenden, ist VMware Identity Manager Connector nicht erforderlich, es sei denn, Sie verfügen über Anwendungsfälle, die von VMware Identity Manager Connector unterstützt werden. Siehe „Lokales Bereitstellungsmodell unter Verwendung von AirWatch Cloud Connector“, auf Seite 8.

System- und Netzwerkkonfigurationen - Anforderungen

Siehe „System- und Netzwerkkonfigurationen - Anforderungen“, auf Seite 18.

Bereitstellen und Konfigurieren von VMware Identity Manager Connector

Informationen zum Bereitstellen und Konfigurieren von VMware Identity Manager Connector im ausgehenden Verbindungsmodus finden Sie in den im Folgenden aufgeführten Themen.

- „Bereitstellen von VMware Identity Manager Connector“, auf Seite 18
- „Konfigurieren der Hochverfügbarkeit für den VMware Identity Manager Connector“, auf Seite 26
- „Hinzufügen der Unterstützung für die Kerberos-Authentifizierung zu Ihrer VMware Identity Manager Connector-Bereitstellung“, auf Seite 29

Failover und Redundanz

Informationen zum Konfigurieren des Konnektors für Failover und Redundanz finden Sie in den im Folgenden aufgeführten Themen.

- „Konfigurieren der Hochverfügbarkeit für den VMware Identity Manager Connector“, auf Seite 26
- „Hinzufügen der Unterstützung für die Kerberos-Authentifizierung zu Ihrer VMware Identity Manager Connector-Bereitstellung“, auf Seite 29

Dieses Kapitel behandelt die folgenden Themen:

Bereitstellen von VMware Identity Manager Connector

Um den VMware Identity Manager-Konnektor bereitzustellen, installieren Sie die virtuelle Konnektor-Appliance in vCenter Server, schalten die Appliance ein und aktivieren diese mit einem Aktivierungscode, den Sie in der VMware Identity Manager-Verwaltungskonsole generieren. Außerdem konfigurieren Sie Einstellungen für die Appliance wie beispielsweise Kennwörter.

Nach der Installation und Konfiguration von Connector wechseln Sie zur Verwaltungskonsole von VMware Identity Manager, um die Verbindung mit Ihrem Unternehmensverzeichnis einzurichten, die Authentifizierungsadapter im Konnektor und den ausgehenden Modus für den Konnektor zu aktivieren.

System- und Netzwerkkonfigurationen - Anforderungen

Berücksichtigen Sie Ihre gesamte Bereitstellung, einschließlich der Ressourcen, die Sie integrieren möchten, wenn Sie Entscheidungen über Hardware, Ressourcen und Netzwerkanforderungen treffen.

Unterstützte vSphere- und ESX-Versionen

Sie installieren die virtuelle Appliance in vCenter Server. Es werden die folgenden Versionen von vSphere und ESX Server unterstützt:

- 5.0 U2 und höher
- 5.1 und höher
- 5.5 und höher
- 6.0 und höher

Der VMware vSphere® Client™ oder der VMware vSphere® Web Client wird für die Bereitstellung der OVA-Datei und für den Remotezugriff auf die bereitgestellte virtuelle Appliance benötigt. Der vSphere Client ist auf der Produktdownload-Seite von vSphere auf my.vmware.com verfügbar.

VMware Identity Manager Connector – Anforderungen für die virtuelle Appliance

Stellen Sie sicher, dass die Anforderungen für die Anzahl der Server und für die jedem Server zugeteilten Ressourcen erfüllt werden.

Anzahl der Benutzer	Bis zu 1.000	1.000-10.000	10.000-25.000	25.000-50.000	50.000-100,1000
Anzahl der Konnektorserver	1 Server	2 Server mit Lastausgleich	2 Server mit Lastausgleich	2 Server mit Lastausgleich	2 Server mit Lastausgleich
CPU (pro Server)	2 CPUs	4 CPUs	4 CPUs	4 CPUs	4 CPUs
RAM (pro Server)	6 GB	6 GB	8 GB	16 GB	16 GB
Festplattenspeicher (pro Server)	60 GB	60 GB	60 GB	60 GB	60 GB

Netzwerkkonfiguration - Anforderungen

Komponente	Mindestanforderung
DNS-Datensatz und statische IP-Adresse	Die Anforderungen für den Konnektor entsprechen den Anforderungen für die virtuelle VMware Identity Manager-Appliance. Weitere Informationen finden Sie unter Erstellen von DNS-Datensätzen und IP-Adressen im Handbuch *Installieren und Konfigurieren von VMware Identity Manager*.
Firewall-Port	Stellen Sie sicher, dass der ausgehende Firewall-Port 443 der Konnektorinstanz für Ihre VMware Identity Manager-URL geöffnet ist.

Port-Anforderungen

Die in der Connector-Serverkonfiguration verwendeten Ports werden im Folgenden beschrieben. Auf Ihre Bereitstellung trifft möglicherweise nur ein Teil davon zu.

Port	Quelle	Ziel	Beschreibung
443	Virtuelle Konnektor-Appliance	VMware Identity Manager-Dienst	HTTPS
443	Virtuelle Konnektor-Appliance	vapp-updates.vmware.com	Zugriff auf den Upgrade-Server
8443	Browser	Virtuelle Konnektor-Appliance	Administratorport HTTPS
389, 636, 3268, 3269	Virtuelle Konnektor-Appliance	Active Directory	Es werden Standardwerte angezeigt. Diese Ports sind konfigurierbar.
445	Connector-va	VMware ThinApp-Repository	Zugriff auf ThinApp-Repository
5500	Virtuelle Konnektor-Appliance	RSA SecurID-System	Es wird der Standardwert angezeigt. Dieser Port ist konfigurierbar.
53	Virtuelle Konnektor-Appliance	DNS-Server	TCP/UDP Jede virtuelle Appliance muss über Zugriff auf den DNS-Server über Port 53 verfügen und eingehenden SSH-Datenverkehr über Port 22 zulassen.
88, 464, 135	Virtuelle Konnektor-Appliance	Domänencontroller	TCP/UDP
389, 443	Virtuelle Konnektor-Appliance	View-Verbindungsserver	Zugreifen auf View-Verbindungsserver-Instanzen für die Horizon-/View-Integration

Verzeichnisanforderungen

Sie integrieren Ihr Unternehmensverzeichnis mit VMware Identity Manager und synchronisieren Benutzer und Gruppen aus Ihrem Unternehmensverzeichnis mit dem Dienst. Sie können die folgenden Verzeichnistypen integrieren:

- Eine Active Directory-Umgebung, die aus einer einzelnen Active Directory-Domäne, mehreren Domänen in einer einzelnen Active Directory-Struktur oder mehreren Domänen in mehreren Active Directory-Strukturen besteht.

  VMware Identity Manager unterstützt Active Directory auf Windows 2008, 2008 R2, 2012 und 2012 R2, mit einer Domain-Funktionsebene und einer Forest-Funktionsebene ab Windows 2003.

- Ein LDAP-Verzeichnis

Die virtuelle Connector-Appliance muss auf Ihr Verzeichnis zugreifen können.

Hinweis Sie können auch lokale Verzeichnisse im VMware Identity Manager-Dienst erstellen.

Checklisten zur Bereitstellung

Die Anforderungen für den Konnektor sind ähnlich wie die Anforderungen für die virtuelle VMware Identity Manager-Appliance. Weitere Informationen finden Sie unter Checklisten zur Bereitstellung im Handbuch *Installieren und Konfigurieren von VMware Identity Manager*.

Generieren eines Aktivierungscodes für Connector

Bevor Sie den VMware Identity Manager-Konnektor installieren, melden Sie sich bei der VMware Identity Manager-Verwaltungskonsole an und generieren Sie einen Aktivierungscode für den Konnektor. Dieser Aktivierungscode wird zur Einrichtung der Kommunikation zwischen dem Dienst und dem Konnektor verwendet.

Vorgehensweise

1 Melden Sie sich bei der Verwaltungskonsole an.

2 Klicken Sie auf die Registerkarte **Identitäts- und Zugriffsmanagement**.

3 Klicken Sie auf **Einrichten**.

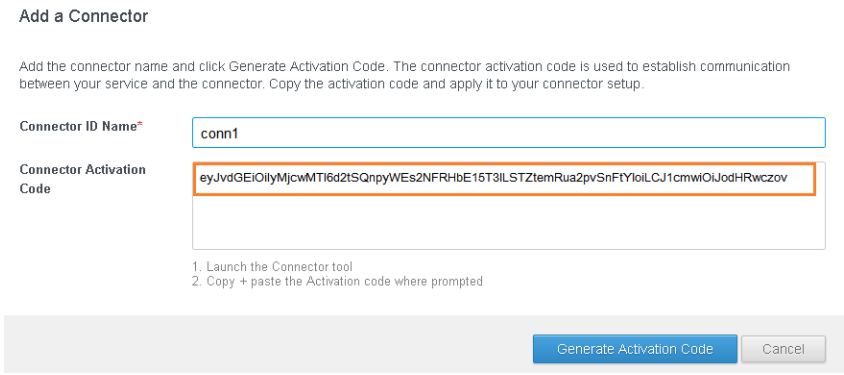
4 Auf der Connectors-Seite klicken Sie auf **Verzeichnis hinzufügen**.

5 Geben Sie einen Namen für Connector ein.

6 Klicken Sie auf **Aktivierungscode generieren**.

  Der Aktivierungscode wird auf der Seite dargestellt.

7 Kopieren und speichern Sie den Aktivierungscode.



Sie benötigen den Aktivierungscode später bei der Bereitstellung des Konnektors.

Sie können jetzt die virtuelle Konnektor-Appliance installieren.

Installieren und Konfigurieren der virtuellen Konnektor-Appliance

Um den Konnektor bereitzustellen, installieren Sie die virtuelle Konnektor-Appliance mithilfe des vSphere Client oder des vSphere Web Client in vCenter Server, schalten die Appliance ein und aktivieren diese mithilfe des Aktivierungscodes, den Sie in der VMware Identity Manager-Verwaltungskonsole generiert haben.

Voraussetzungen

- Laden Sie die OVA-Datei des Konnektors von der VMware Identity Manager-Produktseite auf my.vmware.com herunter.
- Stellen Sie sicher, dass vSphere Client oder vSphere Web Client verfügbar ist.
- Verwenden Sie für den vSphere Web Client Firefox oder Chrome. Verwenden Sie zum Bereitstellen der OVA-Datei nicht den Internet Explorer.
- Ermitteln Sie die DNS-Datensätze und den Hostnamen für Ihre Appliance.

Vorgehensweise

1 Wählen Sie im vSphere Client oder im vSphere Web Client **Datei > OVF-Vorlage bereitstellen** aus.

2 Führen Sie die Anweisungen des Assistenten durch, um die Vorlage bereitzustellen.

Seite	Beschreibung
Quelle	Navigieren Sie zum Speicherort des OVA-Pakets oder geben Sie eine URL ein.
Details der OVA-Vorlage	Überprüfen Sie, ob Sie die richtige Version ausgewählt haben.
Lizenz	Lesen Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Akzeptieren**.
Name und Speicherort	Geben Sie den Namen der virtuellen Appliance ein. Der Name muss im Bestandsordner eindeutig sein und er darf bis zu 80 Zeichen lang sein. Bei Namen wird die Groß-/Kleinschreibung beachtet. Wählen Sie einen Speicherort für die virtuelle Appliance:
Host/Cluster	Wählen Sie den Host oder Cluster zum Ausführen der bereitgestellten Vorlage aus.
Ressourcenpool	Wählen Sie den Ressourcenpool aus.
Speicher	Wählen Sie den Speicherort aus, an dem die Dateien der virtuellen Maschine gespeichert werden sollen.

Seite	Beschreibung
Festplattenformat	Wählen Sie das Festplattenformat für die Dateien aus. Wählen Sie für Produktionsumgebungen das Format **Thick Provision** aus. Verwenden Sie für Evaluierungen und Tests das Format **Thin Provision** aus.
Netzwerkzuordnung	Ordnen Sie die Netzwerke in Ihrer Umgebung den Netzwerken der OVF-Vorlage zu.
Eigenschaften	a Wählen Sie im Feld **Einstellung der Zeitzone** die richtige Zeitzone aus. b Das Kontrollkästchen für das Programm zur Verbesserung der Kundenerfahrung ist standardmäßig aktiviert. VMware erfasst anonyme Daten zu Ihrer Bereitstellung, um besser auf Benutzeranforderungen reagieren zu können. Wenn die Daten nicht erfasst werden sollen, deaktivieren Sie das Kontrollkästchen. c Geben Sie im Textfeld „Hostname“ den zu verwendenden Hostnamen ein. Wenn dieses Feld leer ist, wird zum Suchen des Hostnamens Reverse-DNS verwendet. d Um die statische IP-Adresse für Connector zu konfigurieren, geben Sie die Adresse für jedes der folgenden Felder ein: „Standard-Gateway“, „DNS“, „IP-Adresse“ und „Netzmaske“. **Wichtig** Wenn eines dieser vier Felder oder das Feld „Hostname“ leer ist, wird DHCP verwendet. Um DHCP zu verwenden, lassen Sie die Adressfelder leer.
Bereit zum Abschließen	Überprüfen Sie Ihre Auswahl und klicken Sie auf **Beenden**.

Je nach der Geschwindigkeit Ihres Netzwerks kann die Bereitstellung mehrere Minuten dauern. Im Dialogfeld mit der Fortschrittsanzeige können Sie den Stand der Bereitstellung verfolgen.

3 Ist die Bereitstellung abgeschlossen, wählen Sie die Connector-Appliance aus, klicken Sie mit der rechten Maustaste und wählen Sie aus dem eingeblendeten Kontextmenü **Energie > Einschalten**.

Die Connector-Appliance wird initialisiert. Sie können die Registerkarte **Konsole** öffnen, um die Details anzuzeigen. Wenn die Initialisierung der virtuellen Appliance abgeschlossen ist, werden auf dem Bildschirm „Konsole“ die Connector-Version und die URLs zur Anmeldung beimConnector-Setup-Assistenten angezeigt.

4 Um den Setup-Assistenten auszuführen, geben Sie in Ihren Browser die Connector-URL ein, die in der Registerkarte „Konsole“ angezeigt wird.

5 Klicken Sie auf der Seite „Willkommen“ auf **Fortfahren**.

6 Erstellen Sie sichere Kennwörter für die folgenden Administratorkonten für die virtuelle Connector-Appliance.

Sichere Kennwörter bestehen aus mindestens acht Zeichen, enthalten Zeichen in Groß- und Kleinbuchstaben sowie mindestens eine Ziffer oder ein Sonderzeichen.

Option	Beschreibung
Appliance-Administrator	Erstellen Sie das Administratorkennwort für die Appliance. Der Benutzername lautet **admin** und kann nicht geändert werden. Sie verwenden dieses Konto und dieses Kennwort für die Anmeldung bei den Connector-Diensten, um Zertifikate, Appliance-Kennwörter und die Syslog-Konfiguration zu verwalten. **Wichtig** Das Kennwort des Benutzers **admin** muss aus mindestens sechs Zeichen bestehen.
Root-Konto	Für die Installation der Connector-Appliance wird ein Standard-VMware-Root-Kennwort verwendet. Erstellen Sie ein neues Root-Kennwort.
sshuser-Konto	Erstellen Sie das Kennwort für den Remotezugriff auf die Connector-Appliance.

7 Klicken Sie auf **Fortfahren**.

8 Auf der Seite „Connector aktivieren“ fügen Sie den Aktivierungscode ein und klicken Sie auf **Fortfahren**.

Der Aktivierungscode wird überprüft, und die Kommunikation zwischen dem VMware Identity Manager-Dienst und Ihrer Connector-Instanz wird eingerichtet.

Die Connector-Einrichtung ist abgeschlossen.

Weiter

Klicken Sie auf den Link auf der Seite „Setup ist abgeschlossen“, um die Verwaltungskonsole aufzurufen. Richten Sie dann die Verzeichnisverbindung ein.

Einrichten eines Verzeichnisses

Richten Sie nach dem Bereitstellen der virtuellen Konnektor-Appliance ein Verzeichnis in der VMware Identity Manager-Verwaltungskonsole ein. Sie können Benutzer und Gruppen aus Ihrem Unternehmensverzeichnis mit dem VMware Identity Manager-Dienst synchronisieren.

VMware Identity Manager unterstützt die Integration der nachfolgend aufgeführten Verzeichnistypen.

- Active Directory über LDAP
- Active Directory, integrierte Windows-Authentifizierung.
- LDAP-Verzeichnis

Weitere Informationen finden Sie unter Integrieren in Ihr Unternehmensverzeichnis.

Hinweis Sie können auch lokale Verzeichnisse im VMware Identity Manager-Dienst erstellen. Informationen hierzu finden Sie unter Verwenden von lokalen Verzeichnissen.

Vorgehensweise

1 Klicken Sie auf den Link auf der Seite „Setup ist abgeschlossen“, die nach der Aktivierung des Konnektors angezeigt wird.

Die Registerkarte **Identitäts- und Zugriffsmanagement > Verzeichnisse** wird angezeigt.

2 Klicken Sie auf **Verzeichnis hinzufügen**, und wählen Sie den Typ des Verzeichnisses aus, das Sie hinzufügen möchten.

3 Folgen Sie den Anweisungen des Assistenten zur Eingabe der Konfigurationsinformationen für das Verzeichnis, wählen Sie die Gruppen und Benutzer aus, die synchronisiert werden sollen, und synchronisieren Sie die Benutzer mit dem VMware Identity Manager-Dienst.

Informationen zum Einrichten eines Verzeichnisses finden Sie unter Integrieren in Ihr Unternehmensverzeichnis.

Weiter

Klicken Sie auf die Registerkarte **Benutzer & Gruppen** und überprüfen Sie, ob Benutzer synchronisiert wurden.

Aktivieren von Authentifizierungsadaptern im Konnektor

Für den Konnektor im ausgehenden Modus sind verschiedene Authentifizierungsadapter verfügbar, u. a. PasswordIdpAdapter, RSAAIdpAdapter, SecurIDAdapter und RadiusAuthAdapter. Konfigurieren und aktivieren Sie die Adapter, die Sie verwenden möchten.

Vorgehensweise

1 Klicken Sie in der VMware Identity Manager-Verwaltungskonsole auf die Registerkarte **Identitäts- und Zugriffsmanagement**.

2 Klicken Sie auf **Einrichten** und wählen Sie anschließend die Registerkarte **Konnektoren** aus.

Der von Ihnen bereitgestellte Konnektor wird angezeigt.

3 Klicken Sie auf den Link in der Spalte **Worker**.

4 Klicken Sie auf die Registerkarte **Authentifizierungsadapter**.

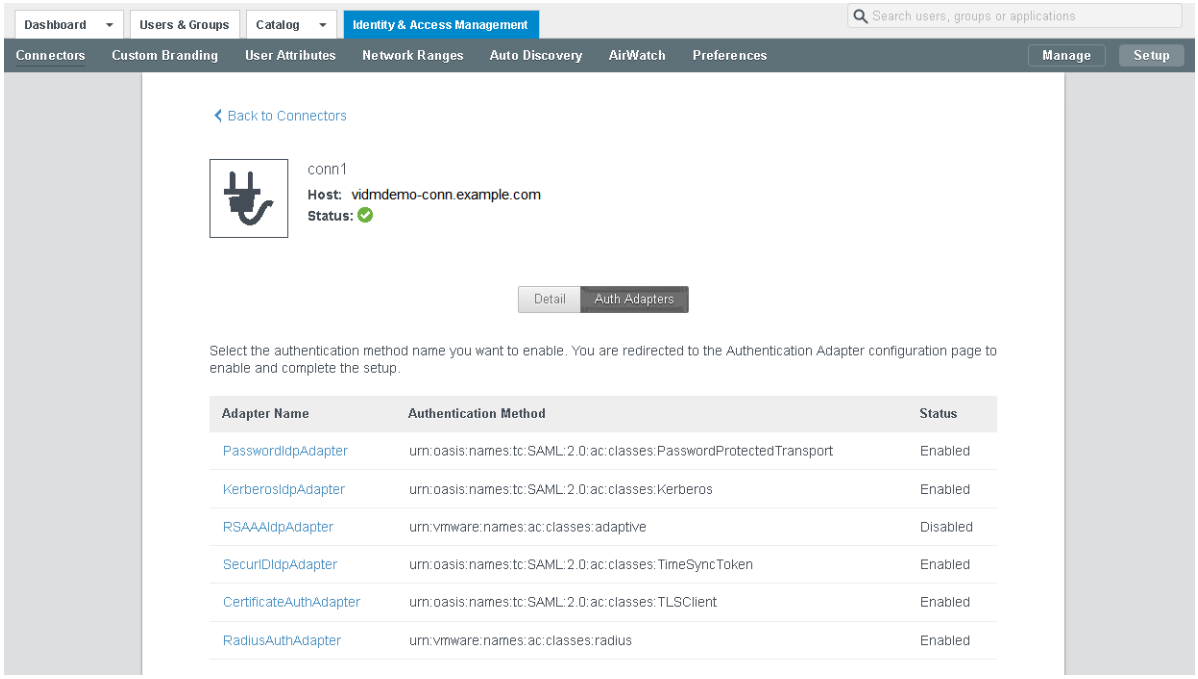
Es werden alle verfügbaren Authentifizierungsadapter für den Konnektor aufgeführt.

Wenn Sie bereits ein Verzeichnis eingerichtet haben, ist PasswordIdpAdapter bereits mit den Konfigurationsinformationen konfiguriert und aktiviert, die Sie beim Erstellen des Verzeichnisses festgelegt haben.

5 Konfigurieren und aktivieren Sie die Authentifizierungsadapter, die Sie verwenden möchten, durch Klicken auf den Link für jeden Adapter und durch Eingabe der Konfigurationsinformationen. Sie müssen mindestens einen Authentifizierungsadapter aktivieren.

Informationen zur Konfiguration bestimmter Authentifizierungsadapter finden Sie im *Administratorhandbuch für VMware Identity Manager*.

Beispiel:



Aktivieren des ausgehenden Modus für den Konnektor

Um den Modus der ausgehenden Verbindung für den Konnektor zu aktivieren, verknüpfen Sie den Konnektor mit dem integrierten Identitätsanbieter.

Der integrierte Identitätsanbieter ist standardmäßig im VMware Identity Manager-Dienst verfügbar und bietet zusätzliche integrierte Authentifizierungsmethoden wie z. B. VMware Verify. Informationen zum integrierten Identitätsanbieter erhalten Sie im *Administratorhandbuch für VMware Identity Manager*.

Hinweis Der Konnektor kann gleichzeitig im ausgehenden und im regulären Modus verwendet werden. Auch wenn Sie den ausgehenden Modus aktivieren, können Sie immer noch eine Kerberos-Authentifizierung für interne Benutzer mithilfe von Authentifizierungsmethoden und Richtlinien konfigurieren.

Vorgehensweise

1 Klicken Sie in der Verwaltungskonsole auf der Registerkarte **Identitäts- und Zugriffsmanagement** auf **Verwalten**.

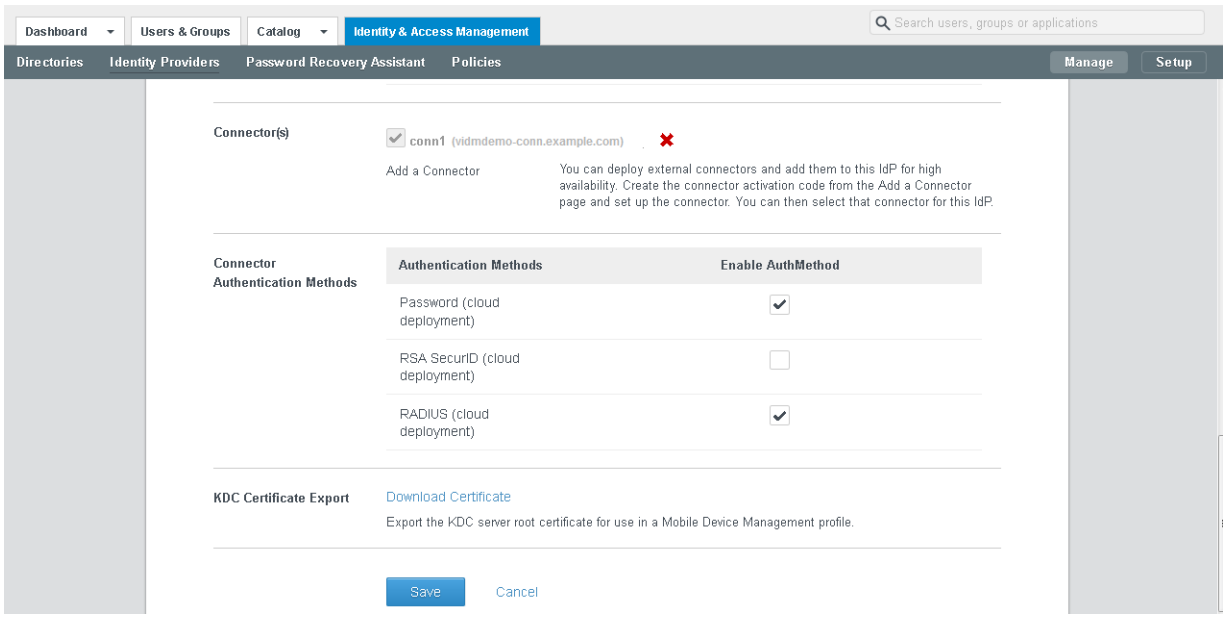
2 Klicken Sie auf die Registerkarte **Identitätsanbieter**.

3 Klicken Sie auf den Link **Integriert**.

4 Geben Sie die folgenden Informationen ein.

Option	Beschreibung
Benutzer	Wählen Sie das Verzeichnis oder die Domänen aus, die der integrierte Identitätsanbieter verwendet.
Netzwerk	Wählen Sie die Netzwerkbereiche aus, die der integrierte Identitätsanbieter verwendet.
Konnektor(en)	Wählen Sie den eingerichteten Konnektor aus. **Hinweis** Wenn Sie später zusätzliche Konnektoren für eine Hochverfügbarkeit hinzufügen, wählen Sie hier alle Konnektoren für die Verknüpfung mit dem integrierten Identitätsanbieter aus. VMware Identity Manager verteilt den Datenverkehr automatisch auf alle mit dem integrierten Identitätsanbieter verknüpften Konnektoren. Ein Lastausgleichsdienst ist nicht erforderlich.
Connector-Authentifizierungsmethoden	Die von Ihnen für den Konnektor aktivierten Bereitstellungsmethoden werden angezeigt. Wählen Sie die Authentifizierungsmethoden aus, die Sie verwenden möchten. PasswordIdpAdapter wurde beim Erstellen eines Verzeichnisses automatisch konfiguriert bzw. aktiviert und wird auf dieser Seite als **Kennwort (Cloudbereitstellung)** angezeigt. Dies weist darauf hin, dass der Adapter mit dem Konnektor im ausgehenden Modus verwendet wird.

Beispiel:



5 Klicken Sie auf **Speichern**, um die Konfiguration des integrierten Identitätsanbieters zu speichern.

6 Bearbeiten Sie Richtlinien für die Verwendung der von Ihnen aktivierten Authentifizierungsmethoden.

a Klicken Sie in der Registerkarte **Identitäts- und Zugriffsmanagement** auf **Verwalten**.

b Klicken Sie auf die Registerkarte **Richtlinien** und auf die Richtlinie, die Sie bearbeiten möchten.

c Klicken Sie unter **Richtlinienregeln** auf den Link in der Spalte **Authentifizierungsmethode** für die Regel, die Sie ändern möchten.

d Wählen Sie auf der Seite „Richtlinienregel bearbeiten“ die Authentifizierungsmethode aus, die Sie für diese Regel verwenden möchten.

e Klicken Sie auf **OK**.

f Klicken Sie auf **Speichern**.

Weitere Informationen zur Konfiguration von Richtlinien finden Sie im *Administratorhandbuch für VMware Identity Manager*.

Der ausgehende Modus ist jetzt für den Konnektor aktiviert. Wenn ein Benutzer sich mithilfe einer der für den Konnektor auf der Seite des integrierten Identitätsanbieters aktivierten Authentifizierungsmethoden anmeldet, ist eine HTTP-Umleitung zum Konnektor nicht erforderlich.

Konfigurieren der Hochverfügbarkeit für den VMware Identity Manager Connector

Durch Hinzufügen mehrerer virtueller Konnektor-Appliances zu einem Cluster können Sie den VMware Identity Manager Connector für Hochverfügbarkeit und Failover einrichten. Wenn auf eine virtuelle Appliance nicht mehr zugegriffen werden kann, sind andere Konnektoren aber weiterhin verfügbar.

Zum Erstellen des Clusters installieren Sie neue virtuelle Konnektor-Appliances und konfigurieren diese auf die gleiche Weise, wie Sie den ersten Konnektor eingerichtet haben.

Sie müssen dann alle Konnektorinstanzen mit dem integrierten Identitätsanbieter verknüpfen. Der VMware Identity Manager-Dienst verteilt den Datenverkehr automatisch auf alle mit dem integrierten Identitätsanbieter verknüpften Konnektoren. Ein Lastausgleichsdienst ist nicht erforderlich. Wenn ein Konnektor aufgrund eines Netzwerkproblems nicht mehr verfügbar ist, leitet der Dienst den Datenverkehr nicht mehr zu diesem Konnektor weiter. Wird die Konnektivität wiederhergestellt, sendet der Dienst wieder Datenverkehr zum Konnektor.

Nach der Einrichtung des Konnektor-Clusters sind die von Ihnen im Konnektor aktivierten Authentifizierungsmethoden hochverfügbar. Wenn eine Konnektorinstanz nicht verfügbar ist, kann die Authentifizierung weiterhin durchgeführt werden. Für die Verzeichnissynchronisierung müssen Sie allerdings beim Ausfall einer Konnektorinstanz eine andere Konnektorinstanz manuell als Synchronisierungskonnektor auswählen. Die Verzeichnissynchronisierung kann nur auf jeweils einem Connector aktiviert werden.

Hinweis Dieser Abschnitt bezieht sich nicht auf die Hochverfügbarkeit der Kerberos-Authentifizierung. Siehe „Hinzufügen der Unterstützung für die Kerberos-Authentifizierung zu Ihrer VMware Identity Manager Connector-Bereitstellung“, auf Seite 29.

Installieren zusätzlicher Konnektorinstanzen

Nachdem Sie die erste Konnektorinstanz installiert und konfiguriert haben, können Sie zusätzliche Konnektoren für Hochverfügbarkeit hinzufügen. Installieren Sie neue virtuelle Konnektor-Appliances und konfigurieren Sie diese exakt auf die gleiche Weise wie die erste Konnektorinstanz.

Voraussetzungen

Sie haben die erste Konnektorinstanz, wie in „Bereitstellen von VMware Identity Manager Connector“, auf Seite 18 erläutert, installiert und konfiguriert.

Vorgehensweise

1 Installieren und konfigurieren Sie eine neue Konnektorinstanz, wie im Folgenden dargestellt.

- „Generieren eines Aktivierungscodes für Connector“, auf Seite 20

- „Installieren und Konfigurieren der virtuellen Konnektor-Appliance“, auf Seite 21

2 Verknüpfen Sie den neuen Konnektor mit dem `WorkspaceIDP` der ersten Konnektorinstanz.

   a Wählen Sie in der Verwaltungskonsole die Registerkarte **Identitäts- und Zugriffsmanagement** und dann die Registerkarte **Identitätsanbieter** aus.

   b Suchen Sie auf der Seite „Identitätsanbieter“ nach dem `WorkspaceIDP` der ersten Konnektorinstanz und klicken Sie auf den Link.

   c Wählen Sie im Feld **Konnektoren** den neuen Konnektor aus.

   d Geben Sie das Bind-DN-Kennwort ein und klicken Sie auf **Konnektor hinzufügen**.

   e Klicken Sie auf **Speichern**.

3 Wenn Sie einer Active Directory-Domäne in der ersten Konnektorinstanz beigetreten sind, müssen Sie der Domäne der neuen Konnektorinstanz ebenfalls beitreten.

   a Klicken Sie in der Registerkarte **Identitäts- und Zugriffsmanagement** auf **Einrichten**.

   Die neue Konnektorinstanz wird auf der Konnektorenseite dargestellt.

   b Klicken Sie auf **Domäne beitreten** neben dem neuen Konnektor und geben Sie die Domäneninformationen an.

Hinweis Für Verzeichnisse vom Typ „Integrierte Windows-Authentifizierung“ (IWA) sind folgende Schritte erforderlich:

   a Führen Sie einen Beitritt der neuen Konnektorinstanz zu der Domäne durch, der das IWA-Verzeichnis in der Originalkonnektorinstanz beigetreten ist.

      1 Wählen Sie die Registerkarte **Identitäts- und Zugriffsmanagement** aus und klicken Sie auf **Einrichten**.

      Die neue Konnektorinstanz wird auf der Konnektorenseite dargestellt.

      2 Klicken Sie auf **Domäne beitreten** und geben Sie die Domäneninformationen an.

   b Speichern Sie die IWA-Verzeichniskonfiguration.

      1 Wählen Sie die Registerkarte **Identitäts- und Zugriffsmanagement** aus.

      2 Auf der Seite „Verzeichnisse“ klicken Sie auf den Link des IWA-Verzeichnisses.

      3 Klicken Sie auf **Speichern**, um die Verzeichniskonfiguration zu speichern.

---

4 Konfigurieren und aktivieren Sie Authentifizierungsadapter im neuen Konnektor.

Wichtig Die Authentifizierungsadapter der Konnektoren in Ihrem Cluster müssen alle identisch konfiguriert sein. Für alle Konnektoren müssen die gleichen Authentifizierungsmethoden aktiviert sein.

---

   a Klicken Sie in der Registerkarte **Identitäts- und Zugriffsmanagement** auf **Einrichten** und dann auf die Registerkarte **Konnektoren**.

   b Klicken Sie auf den Link in der Spalte **Worker** des neuen Konnektors.

c Klicken Sie auf die Registerkarte **Authentifizierungsadapter**.

Es werden alle verfügbaren Authentifizierungsadapter für den Konnektor aufgeführt.

PasswordIdpAdapter ist bereits konfiguriert und aktiviert, da Sie den neuen Konnektor mit dem Verzeichnis verknüpft haben, das dem ersten Konnektor zugeordnet ist.

d Konfigurieren und aktivieren Sie die anderen Authentifizierungsadapter in der gleichen Weise wie für den ersten Konnektor. Stellen Sie sicher, dass die Konfigurationsinformationen identisch sind.

Informationen zur Konfiguration von Authentifizierungsadaptern finden Sie im *Administratorhandbuch für VMware Identity Manager*.

Weiter

„Hinzufügen eines neuen Konnektors zu einem integrierten Identitätsanbieter“, auf Seite 28

Hinzufügen eines neuen Konnektors zu einem integrierten Identitätsanbieter

Nach der Bereitstellung und Konfiguration der neuen Konnektorinstanz fügen Sie diese dem integrierten Identitätsanbieter hinzu. Aktivieren Sie dann die gleichen Authentifizierungsmethoden wie für den ersten Konnektor. VMware Identity Manager verteilt den Datenverkehr automatisch auf alle mit dem integrierten Identitätsanbieter verknüpften Konnektoren.

Vorgehensweise

1 Klicken Sie in der Verwaltungskonsole auf der Registerkarte **Identitäts- und Zugriffsmanagement** auf **Verwalten**.

2 Klicken Sie auf die Registerkarte **Identitätsanbieter**.

3 Klicken Sie auf den Link **Integriert**.

4 Wählen Sie im Feld **Konnektoren** den neuen Konnektor aus der Dropdown-Liste aus und klicken Sie auf **Konnektor hinzufügen**.

5 Im Abschnitt **Methode für Connector-Authentifizierung** aktivieren Sie die gleichen Authentifizierungsmethoden, die Sie für den ersten Konnektor ausgewählt haben.

Die Authentifizierungsmethode „Kennwort (Cloudbereitstellung)“ wird automatisch konfiguriert und aktiviert. Sie müssen die anderen Authentifizierungsmethoden selbst aktivieren.

Wichtig Die Authentifizierungsadapter der Konnektoren in Ihrem Cluster müssen alle identisch konfiguriert sein. Für alle Konnektoren müssen die gleichen Authentifizierungsmethoden aktiviert sein.

Informationen zur Konfiguration bestimmter Authentifizierungsadapter finden Sie im *Administratorhandbuch für VMware Identity Manager*.

6 Klicken Sie auf **Speichern**, um die Konfiguration des integrierten Identitätsanbieters zu speichern.

Aktivieren der Verzeichnissynchronisierung in einem weiteren Konnektor bei einem Ausfall

Beim Ausfall einer Konnektorinstanz wird die Authentifizierung automatisch von einer anderen Konnektorinstanz verarbeitet. Für die Verzeichnissynchronisierung müssen Sie jedoch die Verzeichniseinstellungen im VMware Identity Manager-Dienst verändern, damit eine andere Konnektorinstanz statt der ursprünglichen Konnektorinstanz verwendet wird. Die Verzeichnissynchronisierung kann nur auf jeweils einem Connector aktiviert werden.

Vorgehensweise

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

2 Klicken Sie auf die Registerkarte **Identitäts- und Zugriffsmanagement** und dann auf **Verzeichnisse**.

3 Klicken Sie auf das Verzeichnis, das der ursprünglichen Konnektorinstanz zugeordnet war.

Tipp Sie können diese Informationen auf der Seite **Einrichten > Konnektoren** anzeigen.

4 Wählen Sie im Abschnitt **Verzeichnissynchronisierung und -authentifizierung** der Verzeichnisseite in der Dropdown-Liste **Synchronisierungs-Konnektor** eine andere Konnektorinstanz aus.

5 In das Textfeld **Bind-DN-Kennwort** geben Sie Ihr Kennwort für das Active Directory-Bind-Konto ein.

6 Klicken Sie auf **Speichern**.

Hinzufügen der Unterstützung für die Kerberos-Authentifizierung zu Ihrer VMware Identity Manager Connector -Bereitstellung

Sie können die Kerberos-Authentifizierung für interne Benutzer hinzufügen. Dafür ist die eingehende Verbindung für Ihre Bereitstellung auf der Basis der ausgehenden Verbindungskonnektoren erforderlich. Die gleichen Konnektoren können so konfiguriert werden, dass die Kerberos-Authentifizierung für Benutzer verwendet wird, die vom internen Netzwerk aus zugreifen, und eine andere Authentifizierungsmethode für Benutzer, die von außerhalb zugreifen. Dies kann durch die Definition von Authentifizierungsrichtlinien auf der Basis von Netzwerkbereichen erreicht werden.

Hinweis Damit die Hochverfügbarkeit für die Kerberos-Authentifizierung eingerichtet werden kann, ist ein Lastausgleichsdienst erforderlich.

Konfigurieren und Aktivieren des Kerberos-Authentifizierungsadapters

Konfigurieren und aktivieren Sie KerberosIdpAdapter in VMware Identity Manager Connector. Wenn Sie einen Cluster für Hochverfügbarkeit bereitgestellt haben, konfigurieren und aktivieren Sie den Adapter in allen Konnektoren Ihres Clusters.

Wichtig Die Authentifizierungsadapter der Konnektoren in Ihrem Cluster müssen alle identisch konfiguriert sein. Für alle Konnektoren muss die gleiche Authentifizierungsmethode konfiguriert werden.

Weitere Informationen zur Konfiguration der Kerberos-Authentifizierung finden Sie im *Administratorhandbuch für VMware Identity Manager*.

Voraussetzungen

Der Konnektor muss der Active Directory-Domäne beitreten.

Vorgehensweise

1 Klicken Sie in der VMware Identity Manager-Verwaltungskonsole auf die Registerkarte **Identitäts- und Zugriffsmanagement**.

2 Klicken Sie auf **Einrichten** und wählen Sie anschließend die Registerkarte **Konnektoren** aus.

Es werden alle von Ihnen bereitgestellten Konnektoren aufgeführt.

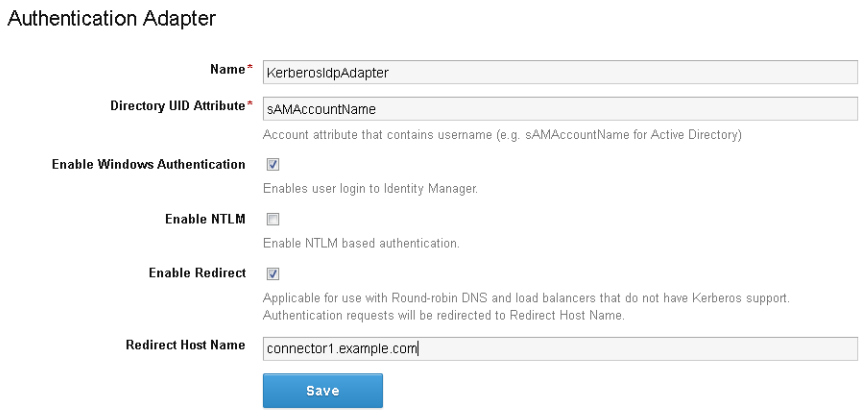
3 Klicken Sie auf den Link in der Spalte **Worker** eines der Konnektoren.

4 Klicken Sie auf die Registerkarte **Authentifizierungsadapter**.

5 Klicken Sie auf den KerberosIdpAdapter-Link und konfigurieren bzw. aktivieren Sie den Adapter.

Option	Beschreibung
Name	Der Standardname des Adapters lautet KerberosIdpAdapter. Sie können diesen Namen ändern.
Verzeichnis-UID-Attribut	Das Kontoattribut, das den Benutzernamen enthält.
Windows-Authentifizierung aktivieren	Wählen Sie diese Option aus.
NTLM aktivieren	Sie müssen diese Option nicht auswählen, es sei denn Ihre Active Directory-Infrastruktur beruht auf der NTLM-Authentifizierung.
Umleitung aktivieren	Wenn Sie über mehrere Konnektoren in einem Cluster verfügen und eine Kerberos-Hochverfügbarkeit mithilfe eines Lastausgleichsdienstes einrichten möchten, wählen Sie diese Option aus und geben Sie einen Wert für **Hostnamen umleiten** ein. Wenn Ihre Bereitstellung nur über einen Konnektor verfügt, müssen Sie die Optionen **Umleitung aktivieren** und **Hostnamen umleiten** nicht verwenden.
Hostnamen umleiten	Wenn Sie die Option **Umleitung aktivieren** auswählen, müssen Sie einen Wert eingeben. Geben Sie den Hostnamen des Konnektors ein. Wenn der Hostname des Konnektors beispielsweise „konnektor1.beispiel.de“ lautet, geben Sie **`konnektor1.beispiel.de`** in das -Textfeld ein.

Beispiel:



Weitere Informationen zur Konfiguration von KerberosIdPAdapter finden Sie im *Administratorhandbuch für VMware Identity Manager*.

6 Wenn Sie einen Cluster bereitgestellt haben, konfigurieren und aktivieren Sie KerberosIdPAdapter in allen Konnektoren Ihres Clusters.

Stellen Sie sicher, dass der Adapter in allen Konnektoren identisch konfiguriert wird.

Weiter

Richten Sie bei Bedarf eine Hochverfügbarkeit für die Kerberos-Authentifizierung ein. Die Kerberos-Authentifizierung ist ohne Lastausgleichsdienst nicht hochverfügbar.

Konfigurieren der Hochverfügbarkeit für die Kerberos-Authentifizierung

Um die Hochverfügbarkeit für die Kerberos-Authentifizierung zu konfigurieren, müssen Sie in Ihrem internen Netzwerk einen Lastausgleichsdienst innerhalb der Firewall installieren und diesem die Konnektor-Appliances hinzufügen.

Sie müssen auch bestimmte Einstellungen des Lastausgleichsdienstes konfigurieren, eine SSL-Vertrauensstellung zwischen dem Lastausgleichsdienst und dem Konnektor einrichten sowie die Konnektorauthentifizierungs-URL für die Verwendung des Hostnamens des Lastausgleichsdienstes ändern.

Konfigurieren der Lastausgleichsdienst-Einstellungen.

Sie müssen für den Lastausgleichsdienst bestimmte Einstellungen wie z. B. die Aktivierung der „X-Forwarded-For“-Kopfzeilen, die korrekte Festlegung der Lastausgleichsdienst-Zeitüberschreitung und die Aktivierung von Sticky-Sitzungen konfigurieren.

Konfigurieren Sie diese Einstellungen.

- „X-Forwarded-For“-Kopfzeilen

  Sie müssen "X-Forwarded-For"-Kopfzeilen auf dem Lastausgleichsdienst aktivieren. Dadurch wird zudem die Authentifizierungsmethode bestimmt. Weitere Informationen finden Sie in der vom Anbieter des Lastausgleichsdienstes bereitgestellten Dokumentation.

- Zeitüberschreitung für den Lastausgleichsdienst

  Damit der Connector ordnungsgemäß funktioniert, müssen Sie möglicherweise den Zeitüberschreitungswert für die Lastausgleichsdienst-Anforderung erhöhen. Der Wert wird in Minuten angegeben. Wenn der eingestellte Wert für die Zeitüberschreitung zu niedrig ist, wird möglicherweise folgender Fehler angezeigt:

  ```
  Fehler 502: Der Dienst ist derzeit nicht verfügbar
  ```

- Aktivieren von Sticky-Sitzungen

  Sie müssen die Einstellung Sticky-Sitzung im Lastausgleichsdienst aktivieren, wenn Ihre Bereitstellung über mehrere Connector-Appliances verfügt. Dann verknüpft der Lastausgleichsdienst eine Benutzersitzung mit einer bestimmten Connector-Instanz.

Anwenden des Root-Zertifikats von VMware Identity Manager Connector auf den Lastausgleich

Wenn die virtuelle VMware Identity Manager Connector-Appliance mit einem Lastausgleich konfiguriert ist, müssen Sie ein SSL-Vertrauensverhältnis zwischen dem Lastausgleich und dem Connector einrichten. Das Connector-Root-Zertifikat muss in den Lastausgleichsdienst kopiert werden.

Das Connector-Zertifikat kann von den Admin-Seiten für die Connector-Appliance unter https://*myconnector.mycompany*:8443/cfg/ssl heruntergeladen werden.

Wenn der Connector-Domänenname auf den Lastausgleichsdienst verweist, kann das SSL-Zertifikat nur auf den Lastausgleichsdienst angewendet werden.

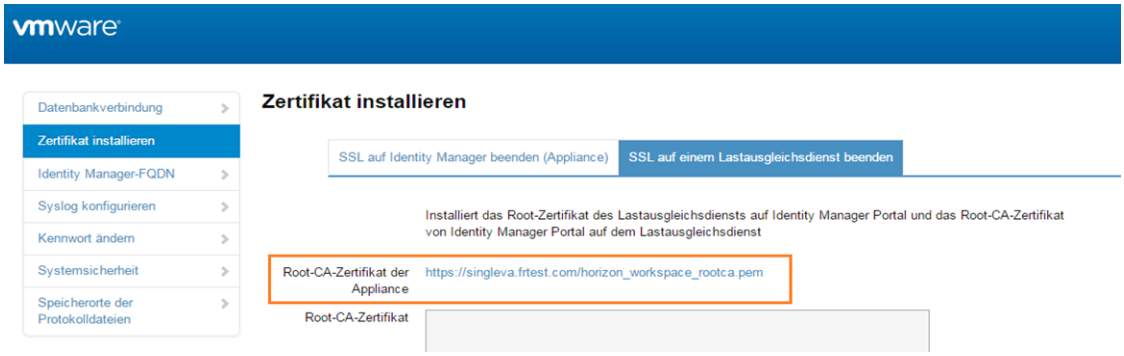
Da der Lastausgleich mit der virtuellen Connector-Appliance kommuniziert, müssen Sie das Connector-Root-CA-Zertifikat als vertrauenswürdiges Root-Zertifikat auf den Lastausgleich kopieren.

Vorgehensweise

1 Melden Sie sich bei den Connector Admin-Seiten für die Appliance, https://*myconnector.mycompany*:8443/cfg/ssl, als Administrator an.

2 Wählen Sie **Zertifikat installieren** aus.

3 Wählen Sie die Registerkarte **SSL auf einem Lastausgleichsdienst beenden** aus und klicken Sie im Feld **Root-CA-Zertifikat der Appliance** auf den Link `https://hostname/horizon_workspace_root-ca.pem`.



4 Kopieren Sie alle Angaben zwischen den Zeilen -----BEGIN CERTIFICATE----- und -----END CERTIFICATE---- inklusive dieser Zeilen und fügen Sie das Stammzertifikat bei jedem Lastenausgleichsdienst an der geeigneten Position ein. Sehen Sie sich hierzu die Dokumentation zum Lastausgleich an.

Weiter

Kopieren Sie das Root-Zertifikat des Lastausgleichsdienstes und fügen Sie es in die VMware Identity ManagerConnector-Appliance ein.

Anwenden des Root-Zertifikats des Lastausgleichs auf den VMware Identity Manager Connector

Wenn die virtuelle VMware Identity Manager Connector-Appliance mit einem Lastausgleich konfiguriert ist, müssen Sie ein Vertrauensverhältnis zwischen dem Lastausgleich und dem Connector einrichten. Sie müssen sowohl das Root-Zertifikat des Connectors in den Lastausgleich kopieren als auch das Root-Zertifikat des Lastausgleichs in den Connector kopieren.

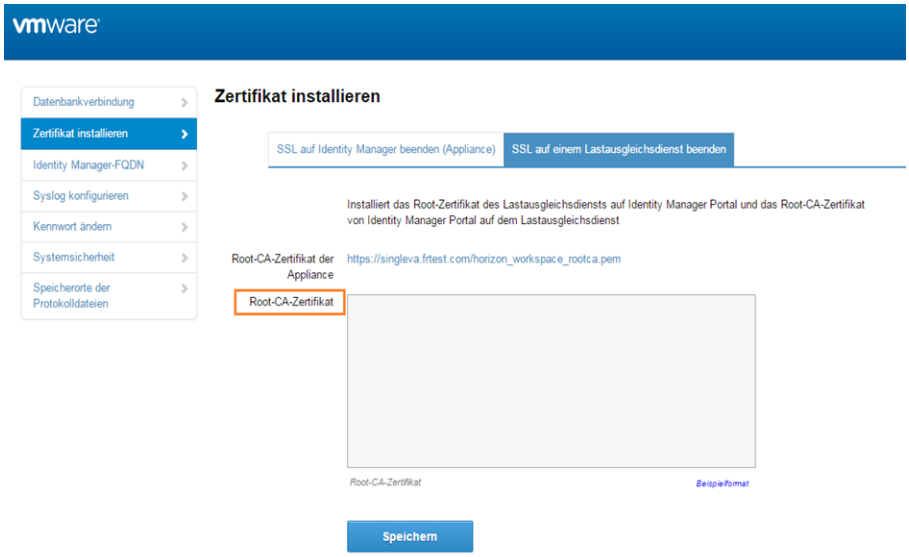
Vorgehensweise

1 Beziehen Sie das Root-Zertifikat des Lastausgleichsdienstes.

2 Navigieren Sie zur Admin-Seite für die Connector-Appliance unter https://*myconnector.mycompany*:8443/cfg/ssl und melden Sie sich als Administrator an.

3 Wählen Sie auf der Seite **Zertifikat installieren** die Registerkarte **SSL auf einem Lastausgleichsdienst beenden**.

4 Fügen Sie den Text aus dem Root-Zertifikat des Lastausgleichsdienstes in das Feld **Root-CA-Zertifikat** ein.



5 Klicken Sie auf **Speichern**.

Ändern des Konnektor-IdP-Hostnamens in den Lastausgleichsdienst-Hostnamen

Nachdem Sie dem Lastausgleichsdienst die virtuellen Konnektor-Appliances hinzugefügt haben, müssen Sie den IdP-Hostnamen für den Workspace-IdP jedes Konnektors in den Hostnamen des Lastausgleichsdienstes ändern.

Voraussetzungen

Die virtuelle Connector-Appliance muss hinter einem Lastausgleichsdienst konfiguriert werden. Stellen Sie sicher, dass als Port für den Lastausgleichsdienst 443 verwendet wird. Verwenden Sie für diesen Zweck nicht 8443, da diese Portnummer für Verwaltungszwecke genutzt wird und für jede virtuelle Appliance eindeutig ist.

Vorgehensweise

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

2 Klicken Sie auf die Registerkarte **Identitäts- und Zugriffsmanagement**.

3 Klicken Sie auf die Registerkarte **Identitätsanbieter**.

4 Klicken Sie auf der Seite „Identitätsanbieter“ auf den Link des Workspace-IdP für Ihre Connector-Instanz.

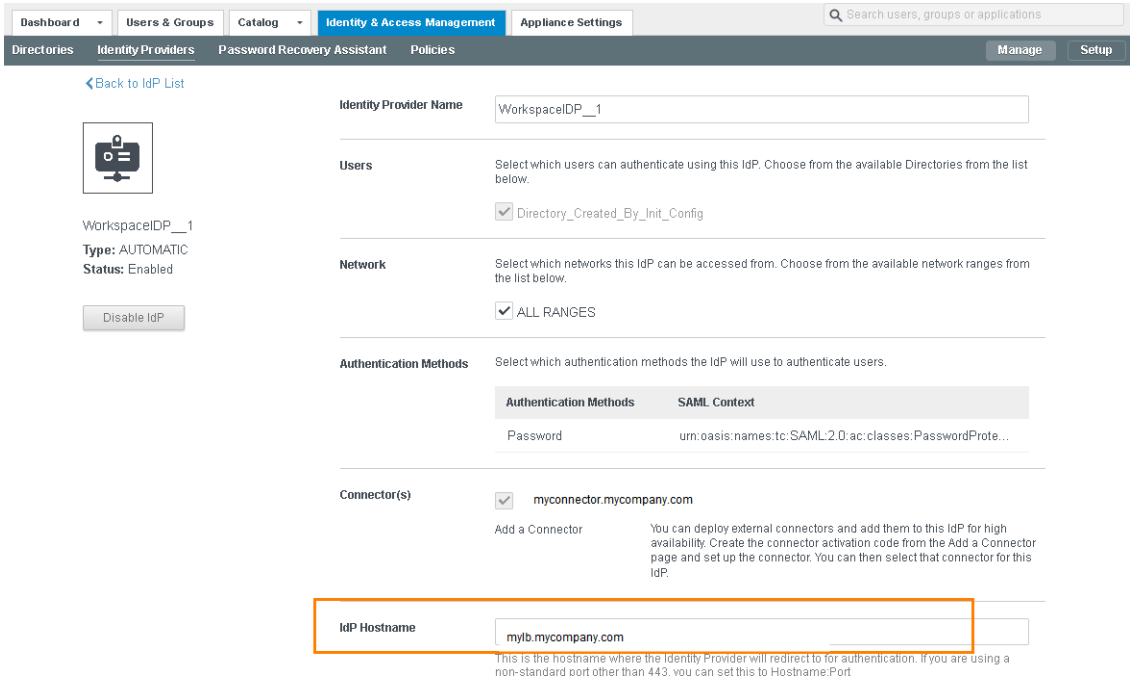
5 Ändern Sie im Textfeld **IdP-Hostname** den Hostnamen vom Connector-Hostnamen in den Lastausgleichsdienst-Hostnamen.

   Wenn Ihr Connector-Hostname beispielsweise `myconnector` lautet und der Hostname Ihres Lastausgleichsdienstes `mylb`, ändern Sie die URL

   `myconnector.mycompany.com:`*`port`*

auf:

`mylb.mycompany.com:`*`port`*



Index