VMware Identity Manager implementeren in de DMZ

VMware Identity Manager 2.9.1
VMware Identity Manager 2.8

vmware®

U vindt de recentste technische documentatie op de website van VMware:

https://docs.vmware.com/nl/

Op de VMware-website vindt u tevens de nieuwste productupdates.

Als u opmerkingen over deze documentatie heeft, kunt u uw feedback sturen naar:

docfeedback@vmware.com

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

Inhoud

VMware Identity Manager implementeren in de DMZ

VMware Identity Manager implementeren in de DMZ bevat informatie over hoe u VMware Identity Manager implementeert in de DMZ in plaats van in het interne netwerk. Voor informatie over het implementeren van VMware Identity Manager in het interne netwerk raadpleegt u *VMware Identity Manager installeren en configureren*.

Doelgroep

De informatie is geschreven voor ervaren Windows- en Linux-systeembeheerders die bekend zijn met technologie van VMware, in het bijzonder met vCenter™, ESX™, en vSphere®, en netwerkconcepten, Active Directory en databases. SUSE Linux 11 is het onderliggende besturingssysteem voor de virtual VMware Identity Manager-appliances en virtual appliances van de VMware Identity Manager-connector.

Kennis van andere technologieën zoals RSA Adaptive Authentication, RSA SecurID en RADIUS is ook handig wanneer u dergelijke functies wilt implementeren.

Woordenlijst technische publicatie VMware

De technische publicatie van VMware bevat een woordenlijst met termen waarmee u wellicht niet bekend bent. Ga naar http://www.vmware.com/support/pubs voor definities van termen zoals deze worden gebruikt in de technische documentatie van VMware.

1 Implementatiemodellen

Er zijn twee hoofdtypen implementatiemodellen beschikbaar voor implementatie van VMware Identity Manager in de DMZ, een model dat integreert met een VMware AirWatch®-implementatie en een model dat AirWatch niet nodig heeft en de VMware Identity Manager-connector gebruikt.

U kunt ook implementatiemodellen combineren wanneer u functionaliteit nodig heeft die niet in een van de modellen wordt ondersteund.

- Implementatiemodel met behulp van AirWatch Cloud Connector

  Als u over een bestaande AirWatch-implementatie beschikt, kunt u VMware Identity Manager hiermee snel integreren. AirWatch verzorgt in dit model de gebruikersverificatie en de synchronisatie van gebruikers en groepen vanuit uw bedrijfsdirectory. U implementeert VMware Identity Manager in de DMZ.

  Houd er rekening mee dat VMware Identity Manager met bronnen zoals Horizon 7 en gepubliceerde Citrix-bronnen niet in dit model worden ondersteund. Alleen integratie met webapplicaties en ingebouwde mobiele applicaties wordt ondersteund.

  Zie "Implementatiemodel op locatie met de AirWatch Cloud Connector," op pagina 8.

- Implementatiemodel met VMware Identity Manager-connector in de verbindingsmodus alleen uitgaand

  In scenario's waarvoor geen AirWatch-implementatie is vereist, kunt u de virtual appliance van de VMware Identity Manager-server installeren in de DMZ en een virtual appliance van de VMware Identity Manager-connector in het bedrijfsnetwerk. De connector verbindt de server met services op locatie, zoals Active Directory. De connector wordt geïnstalleerd in de verbindingsmodus alleen uitgaand en daarom hoeft de ingaande firewallpoort 443 niet te worden geopend. In dit model worden de synchronisatie van gebruikers en groepen vanuit uw bedrijfsdirectory en de gebruikersverificatie uitgevoerd door de VMware Identity Manager-connector.

  Zie "Implementatiemodel op locatie met VMware Identity Manager-connector in de verbindingsmodus alleen uitgaand," op pagina 10.

  - Ondersteuning voor Kerberos-verificatie toevoegen aan uw VMware Identity Manager-connectorimplementatie

    U kunt Kerberos-verificatie voor interne gebruikers (waarvoor een inkomende verbindingsmodus is vereist) toevoegen aan uw implementatie die is gebaseerd op connectoren met de verbindingsmodus alleen uitgaand.

    Zie "Ondersteuning voor Kerberos-verificatie toevoegen aan uw implementatie," op pagina 12.

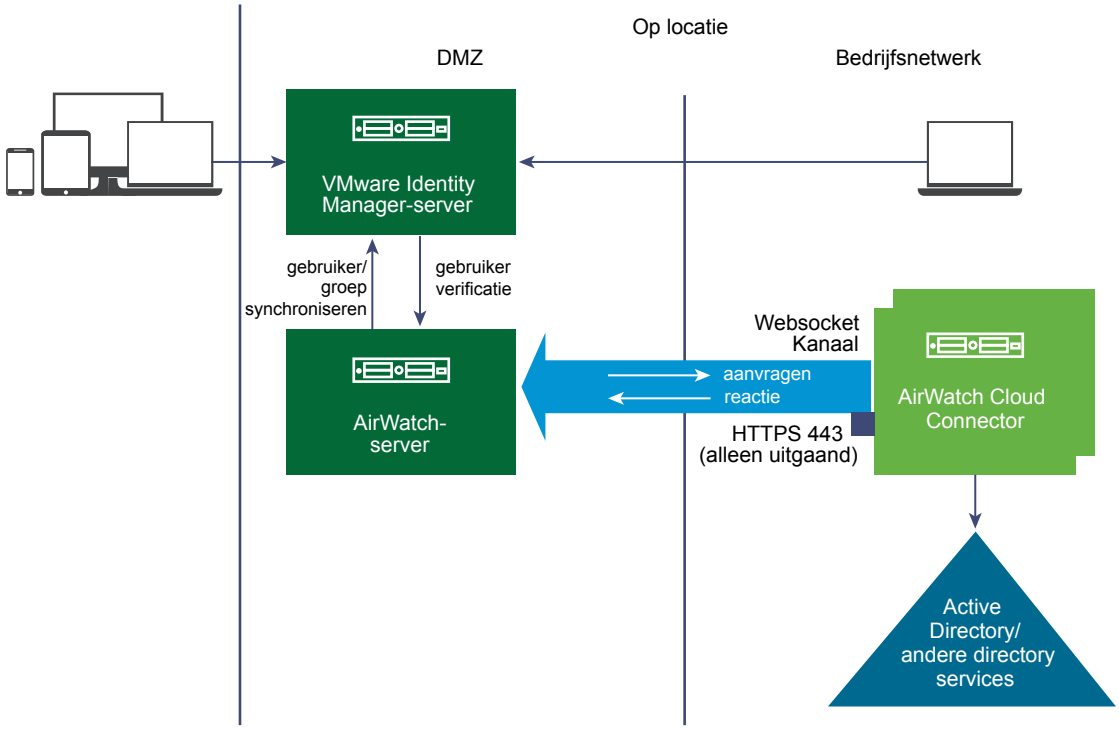
Dit hoofdstuk omvat de volgende onderwerpen:

Implementatiemodel op locatie met de AirWatch Cloud Connector

Als u over een bestaande AirWatch-implementatie beschikt, kunt u VMware Identity Manager hiermee integreren. U implementeert de virtual VMware Identity Manager-appliance in de DMZ. AirWatch verzorgt in dit model de gebruikersverificatie en de synchronisatie van gebruikers en groepen vanuit uw bedrijfsdirectory.

Houd er rekening mee dat VMware Identity Manager met bronnen zoals Horizon 7 of gepubliceerde Citrix-bronnen niet in dit model wordt ondersteund. Alleen integratie met webapplicaties en ingebouwde mobiele applicaties wordt ondersteund.

Figuur 1-1. Implementatie met de AirWatch Cloud Connector



Vereisten

U moet over de volgende onderdelen beschikken:

- Implementatie van een AirWatch-server
- Een AirWatch Cloud Connector-instantie die ter plekke geïmplementeerd en geïntegreerd is met uw bedrijfsdirectory

Vereisten voor de poorten

De volgende poorten zijn vereist voor de VMware Identity Manager-server:

- Inkomend 443 (HTTPS)
- Inkomend 88 (TCP/UDP) - alleen iOS

- Inkomend 5262 (TCP/UDP) - alleen Android

Voor implementatievereisten voor AirWatch kunt u de documentatie van AirWatch raadplegen.

Ondersteunde verificatiemethoden

Dit implementatiemodel ondersteunt de volgende verificatiemethoden. Deze methoden zijn beschikbaar via de VMware Identity Manager ingebouwde identiteitsprovider.

- Wachtwoord (AirWatch Connector)
- Mobiele SSO (voor iOS)
- Mobiele SSO (voor Android)
- Compliance van apparaat (met AirWatch)
- Certificaat (cloudimplementatie)
- VMware Verify

Ondersteunde directory-integraties

U kunt uw bedrijfsdirectory integreren met AirWatch. Zie de AirWatch-documentatie voor de typen ondersteunde directory's.

Ondersteunde bronnen

U kunt de volgende typen bronnen integreren met VMware Identity Manager in dit implementatiemodel:

- Webapplicaties
- Ingebouwde mobiele applicaties

U kunt de volgende bronnen niet integreren met VMware Identity Manager in dit implementatiemodel:

- Horizon 7, Horizon 6, of View-desktop en -applicatiegroepen
- Gepubliceerde Citrix-bronnen
- Verpakte ThinApp-applicaties
- Horizon Air - In de cloud gehoste apps en desktop

Aanvullende informatie

- Hoofdstuk 2, “VMware Identity Manager implementeren in de DMZ,” op pagina 15
- AirWatch integreren met VMware Identity Manager in de *Beheergids voor VMware Identity Manager*.
- AirWatch-documentatie

Implementatiemodel op locatie met VMware Identity Manager-connector in de verbindingsmodus alleen uitgaand

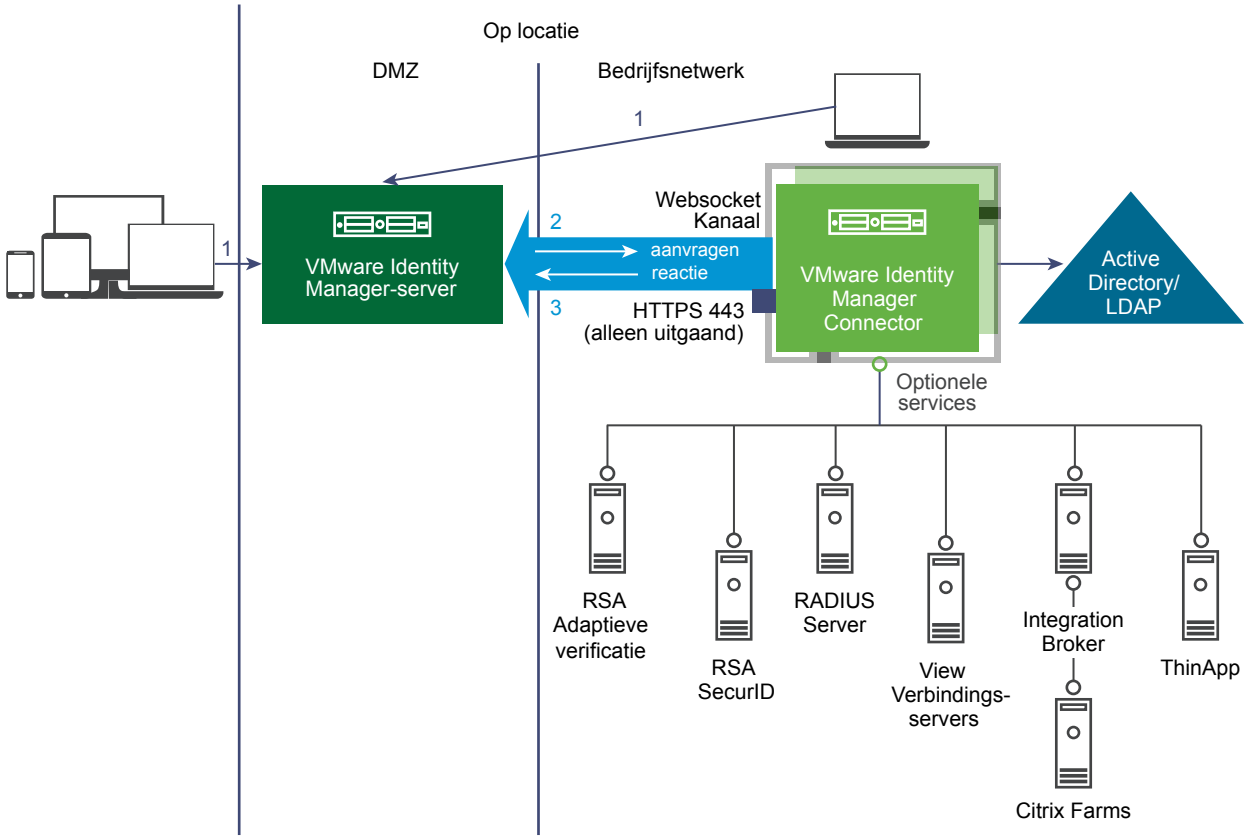
In dit model installeert u de virtual VMware Identity Manager-appliance in de DMZ. U installeert ook een zelfstandige virtual appliance van de VMware Identity Manager-connector in de verbindingsmodus alleen uitgaand in het bedrijfsnetwerk. Bij dit model zijn er geen AirWatch-onderdelen.

De synchronisatie van gebruikers en groepen vanuit uw bedrijfsdirectory en de gebruikersverificatie worden uitgevoerd door de zelfstandige VMware Identity Manager-connector. De connector kan ook bronnen, zoals Horizon 7-desktops en -applicaties, synchroniseren met de VMware Identity Manager-service.

Opmerking Voor sommige verificatiemethoden is echter geen connector nodig. Deze worden direct door de service beheerd.

Belangrijk Gebruik de zelfstandige connector in plaats van de connector die is geïntegreerd met de VMware Identity Manager-appliance, om gebruikers en groepen te synchroniseren en gebruikers te verifiëren.

Figuur 1-2. VMware Identity Manager-connector gebruiken in de uitgaande modus



Vereisten voor de poorten

De volgende poorten zijn vereist voor de VMware Identity Manager-server:

- Inkomend 443 (HTTPS)
- Inkomend 88 (TCP/UDP) - alleen iOS

- Inkomend 5262 (TCP/UDP) - alleen Android

De VMware Identity Manager-connector wordt geïnstalleerd met de verbindingsmodus alleen uitgaand en daarom hoeft de ingaande poort 443 niet te worden geopend. De connector communiceert met de VMware Identity Manager-service via een op een websocket gebaseerd communicatiekanaal.

Zie Hoofdstuk 2, "VMware Identity Manager implementeren in de DMZ," op pagina 15 en Hoofdstuk 3, "VMware Identity Manager-connector implementeren in het bedrijfsnetwerk," op pagina 17 voor een volledige lijst met gebruikte poorten.

Ondersteunde verificatiemethoden

Dit implementatiemodel ondersteunt alle verificatiemethoden. Voor sommige van deze verificatiemethoden is geen connector vereist en deze worden direct door de service beheerd via een ingebouwde identiteitsprovider.

- Wachtwoord - gebruikt de connector
- RSA Adaptieve verificatie - gebruikt de connector
- RSA SecurID - gebruikt de connector
- RADIUS - gebruikt de connector
- Certificaat (cloudimplementatie) - via de ingebouwde identiteitsprovider
- VMware Verify - via de ingebouwde identiteitsprovider
- Mobiele SSO (iOS) - via de ingebouwde identiteitsprovider
- Mobiele SSO (Android) - via de ingebouwde identiteitsprovider
- Ingaande SAML via een onafhankelijke identiteitsprovider

Opmerking Zie "Ondersteuning voor Kerberos-verificatie toevoegen aan uw implementatie," op pagina 12 voor informatie over het gebruik van Kerberos.

Opmerking Dit implementatiemodel ondersteunt geen certificaatverificatie via de connector. De certificaat (cloudimplementatie)-verificatiemethode is beschikbaar.

Ondersteunde directory-integraties

U kunt de volgende typen bedrijfsdirectory's integreren met de VMware Identity Manager-service in dit implementatiemodel:

- Active Directory via LDAP
- Active Directory, Geïntegreerde Windows-verificatie
- LDAP-directory

  Als u van plan bent om een LDAP-directory te integreren, raadpleegt u de bewerkingen in 'Integreren met LDAP-directory's' in *VMware Identity Manager installeren en configureren*.

U kunt ook de volgende methoden gebruiken om gebruikers te maken in de VMware Identity Manager-service:

- Maak lokale gebruikers direct in de VMware Identity Manager-service.
- Gebruik Just-in-Time-inrichting om gebruikers bij aanmelding in de VMware Identity Manager-service dynamisch te maken, met behulp van SAML-asserties die door een identiteitsprovider van derden worden verzonden.

Ondersteunde bronnen

U kunt de volgende typen bronnen integreren met de VMware Identity Manager-service in dit implementatiemodel:

- Webapplicaties
- Horizon 7, Horizon 6, of View-desktop en -applicatiegroepen
- Gepubliceerde Citrix-bronnen
- Verpakte ThinApp-applicaties
- Horizon Air - Cloud gehoste apps en bureaublad (Tech-voorbeeld)

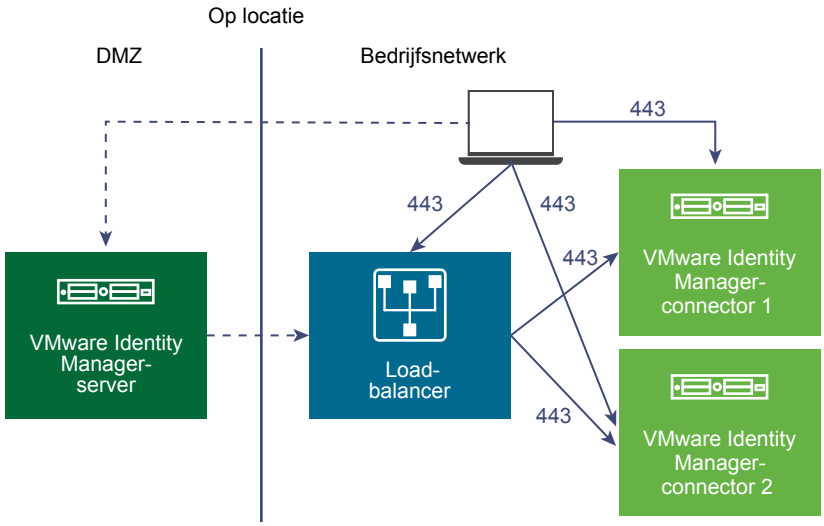
Aanvullende informatie

- Hoofdstuk 2, “VMware Identity Manager implementeren in de DMZ,” op pagina 15 en Hoofdstuk 3, “VMware Identity Manager-connector implementeren in het bedrijfsnetwerk,” op pagina 17
- Directory's
  - 'Integreren met uw bedrijfsdirectory' in *VMware Identity Manager installeren en configureren*
  - 'Lokale directory's gebruiken' in *VMware Identity Manager installeren en configureren*
  - 'Just-in-Time-gebruikersinrichting' in *VMware Identity Manager-beheer*.
- 'Gebruikersverificatie configureren in VMware Identity Manager' in *VMware Identity Manager-beheer*
- *Bronnen instellen in VMware Identity Manager*

Ondersteuning voor Kerberos-verificatie toevoegen aan uw implementatie

U kunt Kerberos-verificatie voor interne gebruikers, waarvoor een inkomende verbindingsmodus is vereist, toevoegen aan uw implementatie die is gebaseerd op VMware Identity Manager-connectoren met de verbindingsmodus alleen uitgaand. Dezelfde connectoren kunnen worden geconfigureerd om gebruik te maken van Kerberos-verificatie voor gebruikers die vanuit het interne netwerk komen en van een andere verificatiemethode voor gebruikers die van buiten komen. Dit kan worden bereikt door verificatiebeleidsregels te definiëren op basis van netwerkbereiken.

Figuur 1-3. Kerberos-verificatie toevoegen



Houd er rekening mee dat de manier waarop hoge beschikbaarheid van Kerberos-verificatie wordt geconfigureerd, anders is.

Zie "Ondersteuning van Kerberos-verificatie aan uw VMware Identity Manager Connector-implementatie toevoegen," op pagina 29 voor meer informatie.

VMware Identity Manager implementeren in de DMZ

2

U kunt de virtual VMware Identity Manager-appliance in de DMZ implementeren als u deze niet wilt implementeren in het bedrijfsnetwerk. Wanneer u de VMware Identity Manager-appliance implementeert in de DMZ, implementeert u ook een zelfstandige VMware Identity Manager-connector met de verbindingsmodus alleen uitgaand in het bedrijfsnetwerk.

Vereisten voor systeem- en netwerkconfiguratie

De vereisten voor de systeem- en netwerkconfiguratie voor de implementatie van VMware Identity Manager in de DMZ zijn vergelijkbaar met de vereisten voor de implementatie van VMware Identity Manager in het bedrijfsnetwerk, zoals beschreven in Vereisten voor systeem- en netwerkconfiguratie en Implementatie van VMware Identity Manager voorbereiden in *VMware Identity Manager installeren en configureren*, met uitzondering van de verschillen die hier worden beschreven.

- U hoeft geen inkomende firewallpoort voor appliances te openen in het bedrijfsnetwerk.

  De virtual VMware Identity Manager-appliance wordt geïmplementeerd in de DMZ. De VMware Identity Manager-connector wordt geïmplementeerd in het bedrijfsnetwerk met de verbindingsmodus alleen uitgaand en communiceert met de service via een op een websocket gebaseerd communicatiekanaal.

- U hoeft geen omgekeerde proxy of load-balancer te implementeren om externe toegang tot VMware Identity Manager mogelijk te maken.

- Er is alleen een load-balancer nodig als u hoge beschikbaarheid en redundantie configureert voor de virtual VMware Identity Manager-appliance.

- De volgende poorten worden gebruikt. Mogelijk heeft uw implementatie hiervan slechts een subreeks nodig.

Poort	Source	Target	Beschrijving
443	Load-balancer	Virtual VMware Identity Manager-appliance	HTTPS
443	Virtual VMware Identity Manager-appliance	Virtual VMware Identity Manager-appliance	HTTPS
443	Browsers	Virtual VMware Identity Manager-appliance	HTTPS
88	Browsers	Virtual VMware Identity Manager-appliance	TCP/UDP Alleen iOS
5262	Browsers	Virtual VMware Identity Manager-appliance	TCP/UDP Alleen Android

Poort	Source	Target	Beschrijving
443	Virtual VMware Identity Manager-appliance	vapp-updates.vmware.com	Toegang tot de VMware-upgradeserver
8443	Browsers	Virtual VMware Identity Manager-appliance	Poort voor beheerders HTTPS
25	Virtual VMware Identity Manager-appliance	SMTP-server	TCP-poort om uitgaande e-mails door te geven
53	Virtual VMware Identity Manager-appliance	DNS-server	TCP/UDP Elke virtual appliance moet toegang hebben tot de DNS-server op poort 53 en inkomend SSH-verkeer moet zijn ingeschakeld op poort 22.
TCP: 9300-9400 UDP: 54328	Virtual VMware Identity Manager-appliance	Virtual VMware Identity Manager-appliance	Auditbehoeften
5432	Virtual VMware Identity Manager-appliance	Database	De standaardpoort voor PostgreSQL is 5432. De standaardpoort voor Oracle is 1521.
443	Virtual VMware Identity Manager-appliance	AirWatch REST API	HTTPS Voor compliancecontrole van het apparaat en de verificatiemethode ACC-wachtwoord, als deze wordt gebruikt.

De VMware Identity Manager-appliance implementeren

Voor informatie over het implementeren en configureren van de virtual VMware Identity Manager-appliance raadpleegt u VMware Identity Manager implementeren en Systeemconfiguratie-instellingen voor appliance beheren in *VMware Identity Manager installeren en configureren*.

Failover en redundantie configureren

Voor informatie over het configureren van failover en redundantie voor de virtual VMware Identity Manager-appliance raadpleegt u de volgende gedeelten in *VMware Identity Manager installeren en configureren*:

- Failover en redundantie in een enkel datacenter configureren
- VMware Identity Manager in een tweede datacenter implementeren voor failover en redundantie

Opmerking Het gedeelte 'Een load-balancer of omgekeerde proxy gebruiken om externe toegang tot VMware Identity Manager toe te staan' geldt niet voor scenario's waarbij VMware Identity Manager wordt geïmplementeerd in de DMZ.

VMware Identity Manager -connector implementeren in het bedrijfsnetwerk 3

Wanneer u de virtual VMware Identity Manager-appliance implementeert in de DMZ, moet u ook een zelfstandige appliance van de VMware Identity Manager-connector implementeren in uw bedrijfsnetwerk met de verbindingsmodus alleen uitgaand.

De connector verbindt de VMware Identity Manager-service met andere onderdelen in het bedrijfsnetwerk, zoals Active Directory en Horizon 7.

De connector communiceert met de service in de verbindingsmodus alleen uitgaand via een communicatiekanaal.

Opmerking Als u een AirWatch-implementatie hebt en de AirWatch Cloud Connector gebruikt, is de VMware Identity Manager-connector niet vereist tenzij u behoefte hebt aan de gebruikstoepassingen die worden ondersteund door de VMware Identity Manager-connector. Zie "Implementatiemodel op locatie met de AirWatch Cloud Connector," op pagina 8.

Vereisten voor systeem- en netwerkconfiguratie

Zie "Vereisten voor systeem- en netwerkconfiguratie," op pagina 18.

VMware Identity Manager-connector implementeren en configureren

Voor informatie over het implementeren en configureren van de VMware Identity Manager-connector in de verbindingsmodus alleen uitgaand, raadpleegt u de volgende onderwerpen.

- "De VMware Identity Manager-connector implementeren," op pagina 18
- "Hoge beschikbaarheid voor de VMware Identity Manager-connector configureren," op pagina 26
- "Ondersteuning van Kerberos-verificatie aan uw VMware Identity Manager Connector-implementatie toevoegen," op pagina 29

Failover en redundantie

Voor informatie over het configureren van de connector voor failover en redudantie raadpleegt u de volgende onderwerpen.

- "Hoge beschikbaarheid voor de VMware Identity Manager-connector configureren," op pagina 26
- "Ondersteuning van Kerberos-verificatie aan uw VMware Identity Manager Connector-implementatie toevoegen," op pagina 29

Dit hoofdstuk omvat de volgende onderwerpen:

De VMware Identity Manager-connector implementeren

Om de VMware Identity Manager-connector te implementeren, installeert u de virtual appliance van de connector in vCenter Server, schakelt u deze in en activeert u deze met een activeringscode die u genereert in de VMware Identity Manager-beheerconsole. U kunt ook instellingen van de appliance configureren, zoals wachtwoorden instellen.

Nadat u de Connector heeft geïnstalleerd en geconfigureerd, gaat u naar de VMware Identity Manager-beheerconsole om de verbinding met uw bedrijfsdirectory

Vereisten voor systeem- en netwerkconfiguratie

Denk na over uw gehele implementatie, onder andere over welke bronnen u wilt integreren, en wanneer u beslissingen neemt over hardware, bronnen en netwerkvereisten.

Ondersteund versies van vSphere en ESX

U installeert de virtual appliance in vCenter Server. De volgende vSphere- en ESX-serverversies worden ondersteund:

- 5.0 U2 en hoger
- 5.1 en hoger
- 5.5 en hoger
- 6.0 en hoger

VMware vSphere® Client™ of VMware vSphere® Web Client is vereist om het OVA-bestand te implementeren en op afstand toegang te krijgen tot de geïmplementeerde virtual appliance. De vSphere Client is beschikbaar op de downloadpagina van vSphere op my.vmware.com.

Vereisten voor de virtual appliance van de VMware Identity Manager -connector

Zorg ervoor dat u voldoet aan de vereisten voor het aantal servers en de bronnen die zijn toegewezen aan elke server.

Aantal gebruikers	Tot 1.000	1000-10.000	10.000-25.000	25.000-50.000	50.000-100.1000
Aantal connectorservers	1 server	2 servers met load balancing	2 servers met load balancing	2 servers met load balancing	2 servers met load balancing
CPU (per server)	2 CPU's	4 CPU's	4 CPU's	4 CPU's	4 CPU's
RAM (per server)	6 GB	6 GB	8 GB	16 GB	16 GB
Schijfruimte (per server)	60 GB	60 GB	60 GB	60 GB	60 GB

Vereisten voor netwerkconfiguratie

Onderdeel	Minimumvereiste
DNS-record en statisch IP-adres	De vereisten voor de connector zijn dezelfde als de vereisten voor de virtual appliance van de VMware Identity Manager. Zie DNS-records en IP-adressen maken in *VMware Identity Manager installeren en configureren*.
Firewallpoort	Zorg dat de uitgaande firewallpoort 443 van de connectorinstantie naar de URL van de VMware Identity Manager is geopend.

Vereisten voor de poorten

De poorten die worden gebruikt in de Connector-serverconfiguratie worden hieronder beschreven. Uw implementatie kan hiervan slechts een subreeks bevatten.

Poort	Source	Target	Beschrijving
443	Connector van virtual appliance	VMware Identity Manager-service	HTTPS
443	Connector van virtual appliance	vapp-updates.vmware.com	Toegang tot de upgradeserver
8443	Browsers	Connector van virtual appliance	Poort voor beheerders HTTPS
389, 636, 3268, 3269	Connector van virtual appliance	Active Directory	De standaardwaarden worden weergegeven. Deze poorten kunnen worden geconfigureerd.
445	Connector-va	VMware ThinApp-opslagplaats	Toegang tot de ThinApp-opslagplaats
5500	Connector van virtual appliance	RSA SecurID-systeem	De standaardwaarde wordt weergegeven. Deze poort kan worden geconfigureerd.
53	Connector van virtual appliance	DNS-server	TCP/UDP Elke virtual appliance moet toegang hebben tot de DNS-server op poort 53 en inkomend SSH-verkeer moet zijn ingeschakeld op poort 22
88, 464, 135	Connector van virtual appliance	Domeincontroller	TCP/UDP
389, 443	Connector van virtual appliance	View-verbindingsserver	Toegang tot View-verbindingsserverinstanties voor integraties van Horizon/View

Vereisten voor directory

U kunt uw bedrijfsdirectory integreren met VMware Identity Manager om gebruikers en groepen van uw bedrijfsdirectory te synchroniseren met de service. U kunt de volgende typen directory's integreren.

- Een Active Directory-omgeving die bestaat uit één domein van Active Directory, meerdere domeinen in één forest van Active Directory of meerdere domeinen over meerdere forests van Active Directory.

  VMware Identity Manager ondersteunt Active Directory in Windows 2008, 2008 R2, 2012 en 2012 R2, met het functionaliteitsniveau domein en het functionaliteitsniveau forest voor Windows 2003 en hoger.

- Een LDAP-directory

Uw directory moet toegankelijk zijn voor de Connector-virtual appliance.

Opmerking U kunt ook lokale directory's maken in de VMware Identity Manager-service.

Implementatiecontrolelijsten

De vereisten voor de connector zijn vergelijkbaar met de vereisten voor de virtual appliance van de VMware Identity Manager. Zie Implementatiecontrolelijsten in *VMware Identity Manager installeren en configureren*.

Activeringscode voor connector genereren

Voordat u de VMware Identity Manager-connector installeert, meldt u zich aan op de VMware Identity Manager-beheerconsole als lokale beheerder en genereert u een activeringscode voor de connector. De activeringscode wordt gebruikt om de communicatie tussen de service en de connector tot stand te brengen.

Procedure

1 Meld u aan op de beheerconsole.

2 Klik op het tabblad **Identiteits- en toegangsbeheer**.

3 Klik op **Installatie**.

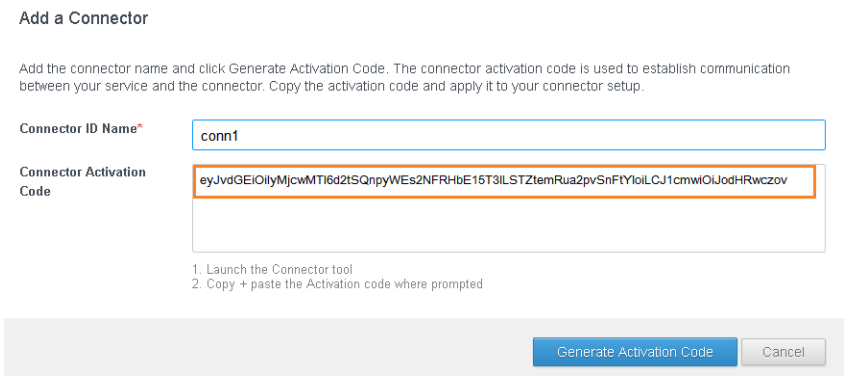
4 Op de pagina Connectors klikt u op **Connector toevoegen**.

5 Voer een naam in voor de Connector.

6 Klik op **Activeringscode genereren.**

De activeringscode wordt op de pagina weergegeven.

7 Kopieer de activeringscode en sla deze op.



U heeft de activeringscode later nodig wanneer u de connector implementeert.

U kunt de virtual appliance van de connector nu installeren.

De virtual appliance van de connector installeren en configureren

Om de connector te implementeren, installeert u de virtual appliance van de connector in vCenter Server met behulp van de vSphere Client of de vSphere Web Client, schakelt u deze in en activeert u deze met de activeringscode die u in de VMware Identity Manager-beheerconsole hebt gegenereerd.

Vereisten

- Download het OVA-bestand van de connector via de VMware Identity Manager-productpagina op my.vmware.com.

- Controleer of u over vSphere Client of vSphere Web Client beschikt.
- Als u met de vSphere Web Client werkt, gebruik u Firefox of Chrome als browser. Implementeer het OVA-bestand niet met behulp van Internet Explorer.
- Zoek de DNS-records en de hostnaam die u voor uw appliance wilt gebruiken.

Procedure

1 Selecteer **Bestand > OVF-sjabloon implementeren** in de vSphere Client of de vSphere Web Client

2 Volg de wizard om het sjabloon te implementeren.

Pagina	Beschrijving
Bron	Blader naar de locatie van het OVA-pakket of voer de bijbehorende URL in.
Details OVA-sjabloon	Controleer of u de juiste versie hebt geselecteerd.
Licentie	Lees de licentieovereenkomst voor eindgebruikers en klik op **Accepteren**.
Naam en Locatie	Geef een naam op voor de virtual appliance. Dit moet een unieke naam in de inventarismap zijn van maximaal 80 tekens. Namen zijn hoofdlettergevoelig. Selecteer een locatie voor de virtual appliance.
Host / Cluster	Selecteer de host of cluster waar de geïmplementeerde sjabloon wordt uitgevoerd.
Brongroep	Selecteer de brongroep.
Opslag	Selecteer de locatie waar de bestanden van de virtual machine worden opgeslagen.
Schijfindeling	Selecteer de schijfindeling voor de bestanden. Selecteer voor productieomgevingen een **Thick Provision**-indeling. Gebruik de indeling **Thin Provision** voor evaluaties en tests.
Netwerktoewijzing	Wijs de netwerken in uw omgeving toe aan de netwerken van de OVF-sjabloon.
Eigenschappen	a Selecteer de juiste tijdzone in het veld **Instelling tijdzone**. b Het selectievakje Programma ter verbetering van de klantervaring is standaard ingeschakeld. Om beter tegemoet te komen aan de behoeften van gebruikers, verzamelt VMware anonieme gegevens over uw implementatie. Schakel het selectievakje uit als u niet wilt dat deze gegevens worden verzameld. c Voer in het tekstvak Hostnaam de naam van de host in. Als dit vak leeg is, wordt de hostnaam opgezocht via een omgekeerde DNS-zoekactie. d Als u het statische IP-adres voor Connector wilt configureren, geeft u de adressen op voor: Default Gateway, DNS, IP-adres en Netmask. **Belangrijk** Als u een van deze vier adresvelden niet invult en geen hostnaam opgeeft, wordt DHCP gebruikt. U stelt DHCP in door de adresvelden leeg te laten.
Gereed om te voltooien	Bekijk uw selecties en klik op **Voltooien**.

De implementatie kan, afhankelijk van de netwerksnelheid, enige minuten duren. U kunt de voortgang volgen in het dialoogvenster Voortgang.

3 Als de implementatie is voltooid, selecteert u de Connector-apparaat, klikt u met de rechtermuisknop en selecteert u **Aan/uit > Inschakelen**.

De Connector-apparaat wordt geïnitialiseerd. Op het tabblad **Console** kunt u de details bekijken. Wanneer de virtual appliance is geïnitialiseerd, ziet u in het consolescherm de Connector-versie en de URL's waarmee u zich bij de installatiewizard van de Connector kunt aanmelden.

4 Om de installatiewizard uit te voeren, richt u uw browser op de Connector-URL die op het tabblad Console wordt weergegeven.

5 Klik op **Doorgaan** op de welkomstpagina.

6 Maak sterke wachtwoorden voor de volgende beheerderaccounts voor de virtual Connector-appliance.

Sterke wachtwoorden moeten minstens acht tekens lang zijn en bestaan uit een combinatie van hoofdletters en kleine letters en minstens één cijfer of speciaal teken.

Optie	Beschrijving
Apparaatbeheerder	Maak het wachtwoord voor de apparaatbeheerder. De gebruikersnaam is **admin**. U kunt deze naam niet wijzigen. Meld u met dit account en wachtwoord aan bij de Connectorservices om certificaten, appliancewachtwoorden en systeemlogboekconfiguratie te beheren. **Belangrijk** Het wachtwoord voor de **beheerdersgebruiker** moet minstens zes tekens lang zijn.
Rootaccount	De Connector-toepassing is geïnstalleerd op basis van een standaardhoofdwachtwoord van VMware. Maak een nieuw rootwachtwoord.
sshuser-account	Maak het wachtwoord voor de externe toegang tot de connectortoepassing.

7 Klik op **Doorgaan**.

8 Plak de activeringscode op de pagina Connector activeren en klik op **Doorgaan**.

De activeringscode wordt gecontroleerd en de communicatie tussen de VMware Identity Manager-service en uw Connector -instantie wordt tot stand gebracht.

De installatie van Connector is voltooid.

Wat nu te doen

Klik op de link op de pagina 'Installatie is voltooid' om naar de beheerconsole te gaan. Stel dan de directoryverbinding in.

Een directory instellen

Nadat u de virtual appliance van de connector hebt geïmplementeerd, stelt u een directory in de VMware Identity Manager-beheerconsole in. U kunt gebruikers en groepen in uw bedrijfsdirectory synchroniseren naar de VMware Identity Manager-service.

VMware Identity Manager biedt ondersteuning voor de integratie van de volgende directorytypen.

- Active Directory via LDAP
- Active Directory, Geïntegreerde Windows-verificatie
- LDAP-directory

Zie Integreren met uw bedrijfsdirectory voor meer informatie.

Opmerking U kunt ook lokale directory's maken in de VMware Identity Manager-service. Zie Lokale directory's gebruiken.

Procedure

1 Klik op de koppeling op de pagina Instellen is voltooid. Deze pagina wordt weergegeven zodra u de connector hebt geactiveerd.

Het tabblad **Identiteits- en toegangsbeheer > Directory's** wordt weergegeven.

2 Klik op **Directory toevoegen** en selecteer het directorytype dat u wilt toevoegen.

3 Volg de wizard om de configuratiegegevens van de directory in te voeren, selecteer de groepen en gebruikers die u wilt synchroniseren en synchroniseer gebruikers met de VMware Identity Manager-service.

Zie Integreren met uw bedrijfsdirectory voor informatie over hoe u een directory instelt.

Wat nu te doen

Klik op het tabblad **Gebruikers en groepen** en controleer of gebruikers zijn gesynchroniseerd.

Verificatieadapters op de connector inschakelen

Voor de connector in de modus uitgaand zijn verschillende verificatieadapters beschikbaar, zoals PasswordIdpAdapter, RSAAIdpAdapter, SecurIDAdapter en RadiusAuthAdapter. Configureer de adapters die u wilt gebruiken en schakel deze in.

Procedure

1 Klik op het tabblad **Identiteits- en toegangsbeheer** in de VMware Identity Manager-beheerconsole.

2 Klik op **Installatie** en klik dan op het tabblad **Connectors**.

De connector die u hebt geïmplementeerd, wordt vermeld.

3 Klik op de koppeling in de kolom **Werker**.

4 Klik op het tabblad **Verificatieadapters**.

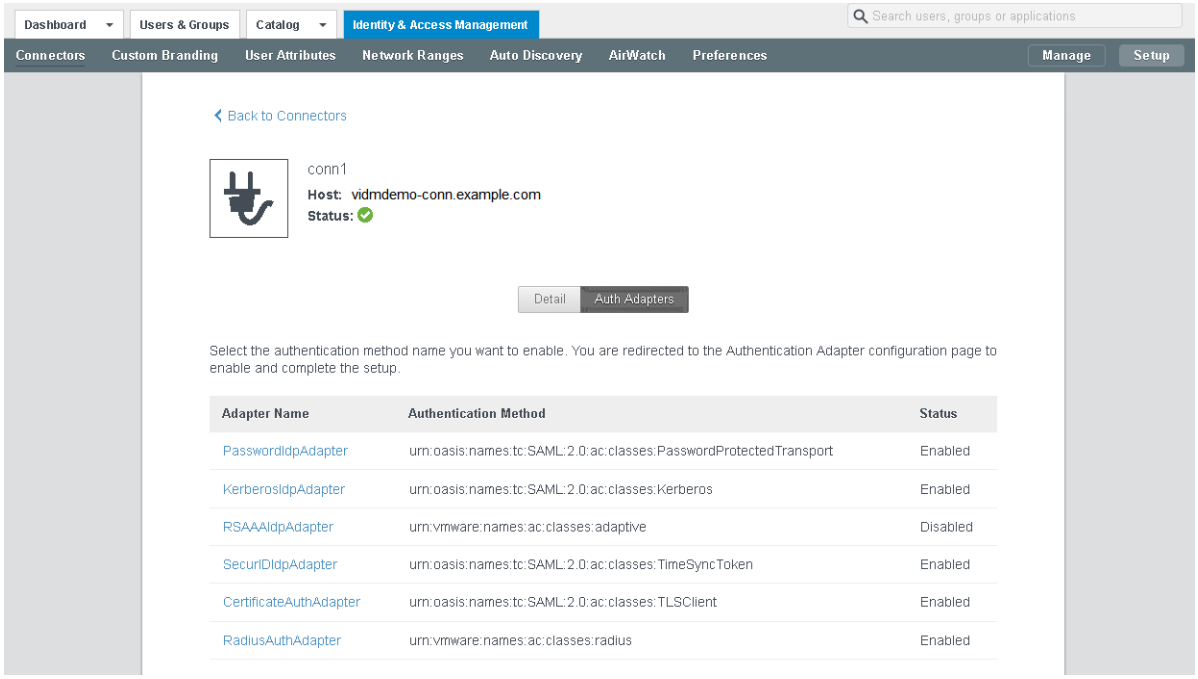
Alle beschikbare verificatieadapters voor de connector worden vermeld.

Wanneer u al een directory heeft ingesteld, is de PasswordIdpAdapter al geconfigureerd en ingeschakeld met de configuratie-informatie die u heeft gespecificeerd toen u de directory maakte.

5 Configureer de verificatieadapters die u wilt gebruiken en schakel deze in door op de koppeling voor elke verificatieadapter te klikken en de configuratie-informatie in te voeren. U moet minimaal één verificatieadapter inschakelen.

Raadpleeg de *Handleiding VMware Identity Manager-beheer* voor informatie over het configureren van specifieke verificatieadapters.

Bijvoorbeeld:



Uitgaande modus voor de connector inschakelen

Om de verbindingsmodus alleen uitgaand voor de connector in te schakelen, koppelt u de connector aan de ingebouwde identiteitsprovider.

De ingebouwde identiteitsprovider is standaard beschikbaar in de VMware Identity Manager-service en biedt aanvullende ingebouwde verificatiemethoden, zoals VMware Verify. Zie de *Handleiding VMware Identity Manager-beheer* voor informatie over de ingebouwde identiteitsprovider.

Opmerking De connector kan tegelijk worden gebruikt in de uitgaande en de reguliere modus. Zelfs als u de uitgaande modus inschakelt, kunt u nog steeds Kerberos-verificatie voor interne gebruikers configureren met verificatiemethoden en beleid.

Procedure

1 Klik in de beheerconsole op het tabblad **Identiteits- en toegangsbeheer** op **Beheren**.

2 Klik op het tabblad **Identiteitsproviders**.

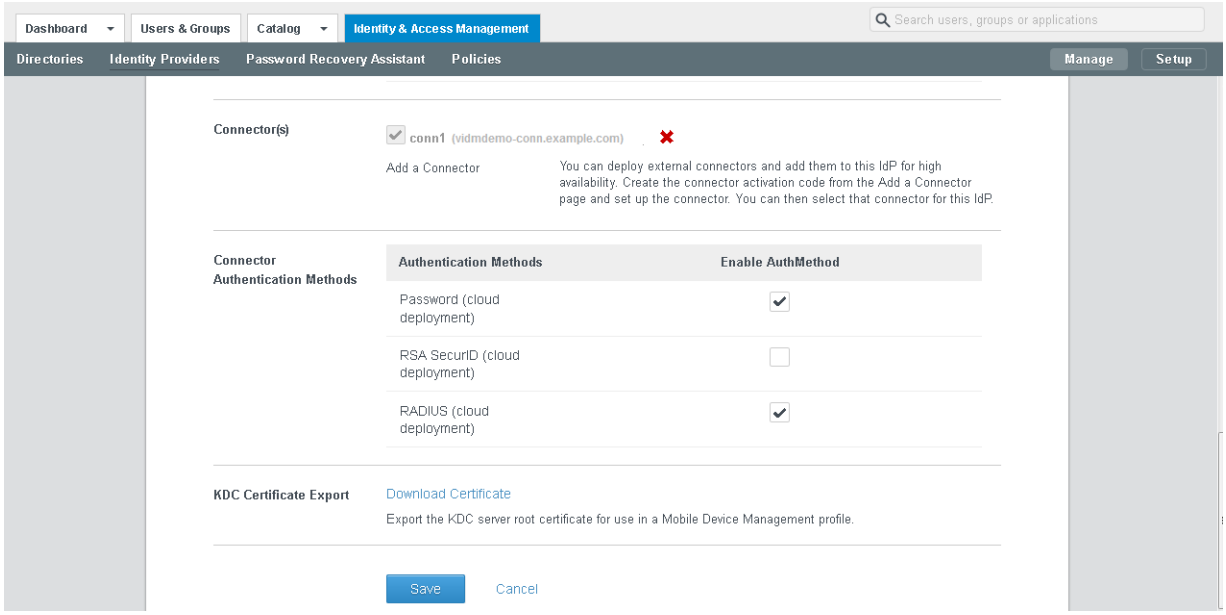
3 Klik op de koppeling **Ingebouwd**.

4 Geef de volgende informatie op.

Optie	Beschrijving
Gebruikers	Selecteer de directory of de domeinen die de ingebouwde identiteitsprovider gaan gebruiken.
Netwerk	Selecteer de netwerkbereiken die de ingebouwde identiteitsprovider gaan gebruiken.

Optie	Beschrijving
Connector(en)	Selecteer de connector die u heeft ingesteld. **Opmerking** Op een later moment, wanneer u extra connectors voor hoge beschikbaarheid toevoegt, selecteert u deze en voegt u deze hier allemaal toe om ze te koppelen aan de ingebouwde identiteitsprovider. VMware Identity Manager verdeelt het verkeer automatisch tussen alle connectors die aan de ingebouwde identiteitsprovider gekoppeld zijn. Een load balancer is niet vereist.
Verificatiemethoden voor connector	De implementatiemethoden die u voor de connector heeft ingeschakeld, worden weergegeven. Selecteer de verificatiemethoden die u wilt gebruiken. De PasswordIdpAdapter, die automatisch geconfigureerd en ingeschakeld is toen u een directory aanmaakte, wordt op deze pagina weergegeven als **Wachtwoord (cloud geïmplementeerd)**, en dit geeft aan dat deze wordt gebruikt met de connector in de uitgaande modus.

Bijvoorbeeld:



5 Klik op **Opslaan** om de configuratie van de ingebouwde identiteitsprovider op te slaan.

6 Bewerk beleidsregels om de verificatiemethoden die u heeft ingeschakeld te gebruiken.

   a Klik in het tabblad **Identiteits- en toegangsbeheer** op **Beheren**.

   b Klik op het tabblad **Beleid** en klik op het beleid dat u wilt bewerken.

   c Onder **Beleidsregels** klikt u voor de regel die u wilt bewerken op de koppeling in de kolom **Verificatiemethode**.

   d Op de pagina Beleidsregel bewerken selecteert u de verificatiemethode die u voor deze regel wilt gebruiken.

   e Klik op **OK**.

   f Klik op **Opslaan**.

   Raadpleeg de *Handleiding VMware Identity Manager-beheer* voor meer informatie over het configureren van beleid.

De uitgaande modus van de connector is nu ingeschakeld. Wanneer een gebruiker zich aanmeldt via een van de verificatiemethoden die u heeft ingeschakeld voor de connector op de pagina van de ingebouwde identiteitsprovider, is een HTTP-omleiding naar de connector niet vereist.

Hoge beschikbaarheid voor de VMware Identity Manager -connector configureren

U kunt de VMware Identity Manager-connector instellen voor hoge beschikbaarheid en failover door meerdere connector-virtual appliances in een cluster toe te voegen. Als een van de virtual appliances om wat voor reden dan ook niet beschikbaar is, zijn andere connectors wel beschikbaar.

Als u een cluster wilt maken, installeert u nieuwe virtual appliances van de connector en configureert u ze op exact dezelfde wijze als de eerste connector.

U koppelt dan alle connectorinstanties aan de ingebouwde identiteitsprovider. De VMware Identity Manager-service verdeelt het verkeer automatisch tussen alle connectoren die aan de ingebouwde identiteitsprovider gekoppeld zijn. Een load balancer is niet vereist. Als een van de connectoren door een netwerkprobleem niet beschikbaar is, leidt de service er geen verkeer naar toe. Wanneer de verbinding is hersteld, leidt de service weer verkeer naar de connector.

Wanneer u de connectorcluster heeft ingesteld, zijn de verificatiemethoden die u op de connector heeft ingesteld, hoog zichtbaar. Als een van de connectorinstanties niet beschikbaar is, is verificatie nog steeds beschikbaar. Voor het synchroniseren van de directory moet u echter, in geval van een fout van de connectorinstantie, handmatig een andere connectorinstantie selecteren als de synchronisatieconnector. Directorysynchronisatie kan slechts voor één connector tegelijk worden ingeschakeld.

Opmerking Dit gedeelte geldt niet voor hoge beschikbaarheid van Kerberos-verificatie. Zie "Ondersteuning van Kerberos-verificatie aan uw VMware Identity Manager Connector-implementatie toevoegen," op pagina 29.

Extra connectorinstanties installeren

Nadat u de eerste connectorinstantie hebt geïnstalleerd en geconfigureerd, kunt u extra connectors toevoegen voor hoge beschikbaarheid. Installeer nieuwe virtual appliances van de connector en configureer ze net als de eerste connectorinstantie.

Vereisten

U hebt de eerste connectorinstantie geïnstalleerd en geconfigureerd zoals beschreven in "De VMware Identity Manager-connector implementeren," op pagina 18.

Procedure

1 Volg deze instructies om een nieuwe connectorinstantie te installeren en te configureren.

- "Activeringscode voor connector genereren," op pagina 20
- "De virtual appliance van de connector installeren en configureren," op pagina 20

2 Koppel de nieuwe connector aan de `WorkSpaceIDP` van de eerste connectorinstantie.

a In de beheerconsole selecteert u het tabblad **Identiteits- en toegangsbeheer** en selecteert u vervolgens het tabblad **Identiteitsprovider**.

b Zoek op de pagina Identiteitsprovider de `WorkspaceIDP` van de eerste connectorinstantie en klik op de koppeling.

c Selecteer de nieuwe connector in het veld **Connector(s)**.

d Voer het Bind DN-wachtwoord in en klik op **Connector toevoegen**.

e Klik op **Opslaan**.

3 Wanneer u in de eerste connectorinstantie was toegevoegd aan een Active Directory-domein, moet u zich ook toevoegen aan het domein in de nieuwe connectorinstantie.

a Klik in het tabblad **Identiteits- en toegangsbeheer** op **Installatie**.

De nieuwe connectorinstantie wordt vermeld op de pagina Connectoren .

b Klik op **Aan domein toevoegen** naast de nieuwe connector en geef de informatie over het domein op.

Opmerking Voer de volgende acties uit voor directory's van het type Integrated Windows Authentication (IWA).

a Voeg de nieuwe connectorinstantie toe aan het domein waaraan de IWA-directory in de oorspronkelijke connectorinstantie was toegevoegd.

1 Selecteer het tabblad **Identiteits- en toegangsbeheer** en klik vervolgens op **Installatie**.

De nieuwe connectorinstantie wordt vermeld op de pagina Connectoren .

2 Klik op **Aan domein toevoegen** en geef de informatie over het domein op.

b Sla de configuratie van de IWA-directory op.

1 Selecteer het tabblad **Identiteits- en toegangsbeheer**.

2 Klik op de Directorypagina op de link IWA-directory.

3 Klik op **Opslaan** om de configuratie van de directory op te slaan.

---

4 Configureer de verificatieadapters op de nieuwe connector en schakel deze in.

Belangrijk Verificatieadapters op alle connectoren in uw cluster moeten identiek zijn geconfigureerd. Op alle connectoren moeten dezelfde verificatiemethoden ingeschakeld zijn.

---

a Klik in het tabblad **Identiteits- en toegangsbeheer** op **Installatie** en klik dan op het tabblad **Connectoren** .

b Klik op de koppeling in de kolom **Werker** van de nieuwe connector.

c Klik op het tabblad **Verificatieadapters**.

Alle beschikbare verificatieadapters voor de connector worden vermeld.

De PasswordIdpAdapter is al geconfigureerd en ingeschakeld omdat u de nieuwe connector heeft gekoppeld aan de directory die is gekoppeld is aan de eerste connector.

d Configureer de andere verificatieadapters op dezelfde manier als de eerste connector en schakel deze op dezelfde manier in. Zorg ervoor dat de configuratie-informatie identiek is.

Raadpleeg de *Handleiding VMware Identity Manager-beheer* voor informatie over het configureren van verificatieadapters.

Wat nu te doen

"Nieuwe connector aan ingebouwde identiteitsprovider toevoegen," op pagina 28

Nieuwe connector aan ingebouwde identiteitsprovider toevoegen

Wanneer u de nieuwe connectorinstantie heeft geïmplementeerd en geconfigureerd, voegt u deze toe aan de ingebouwde identiteitsprovider en schakelt u dezelfde verificatiemethoden in die op de eerste connector zijn ingeschakeld. VMware Identity Manager verdeelt het verkeer automatisch tussen alle connectors die aan de ingebouwde identiteitsprovider gekoppeld zijn.

Procedure

1 Klik in de beheerconsole op het tabblad **Identiteits- en toegangsbeheer** op **Beheren**.

2 Klik op het tabblad **Identiteitsproviders**.

3 Klik op de koppeling **Ingebouwd**.

4 Selecteer in het veld **Connector(s)** de nieuwe connector in het vervolgkeuzemenu en klik op **Connector toevoegen**.

5 Schakel in het gedeelte **Verificatiemethoden voor connector** dezelfde verificatiemethoden in die u voor de eerste connector geselecteerd heeft.

De verificatiemethode Wachtwoord (cloudimplementatie) wordt automatisch geconfigureerd en ingeschakeld. U moet de andere verificatiemethoden inschakelen.

Belangrijk Verificatieadapters op alle connectoren in uw cluster moeten identiek zijn geconfigureerd. Op alle connectoren moeten dezelfde verificatiemethoden ingeschakeld zijn.

Raadpleeg de *Handleiding VMware Identity Manager-beheer* voor informatie over het configureren van specifieke verificatieadapters.

6 Klik op **Opslaan** om de configuratie van de ingebouwde identiteitsprovider op te slaan.

Synchronisatie van directory's inschakelen op een andere connector in geval van een fout

In het geval dat er fouten optreden met een connectorinstantie, wordt de verificatie automatisch afgehandeld door een andere connectorinstantie. Voor het synchroniseren van directory's moet u de directory-instellingen in de VMware Identity Manager-service wijzigen om een andere connectorinstantie te kunnen gebruiken, in plaats van de oorspronkelijke connectorinstantie. De synchronisatie van directory's kan slechts voor één connector per keer worden ingeschakeld.

Procedure

1 Meld u aan op de beheerconsole van VMware Identity Manager.

2 Klik op het tabblad **Identiteits- en toegangsbeheer** en klik vervolgens op **Directory's**.

3 Klik op de directory die is gekoppeld aan de oorspronkelijke connectorinstantie.

Tip U kunt deze informatie bekijken op de pagina **Installatie > Connectoren**.

4 In het gedeelte **Directorysynchronisatie en -verificatie** van de pagina met directory's selecteert u in het vervolgkeuzemenu **Synchronisatieconnector** een andere connectorinstantie.

5 In het veld **Wachtwoord Bind-DN** geeft u het wachtwoord van uw Active Directory-bindingsaccount op.

6 Klik op **Opslaan**.

Ondersteuning van Kerberos-verificatie aan uw VMware Identity Manager Connector -implementatie toevoegen

U kunt Kerberos-verificatie voor interne gebruikers, waarvoor een inkomende verbindingsmodus vereist is, toevoegen aan uw implementatie die is gebaseerd op connectoren met alleen een uitgaande verbindingsmodus. Dezelfde connectoren kunnen worden geconfigureerd om gebruik te maken van Kerberos-verificatie voor gebruikers die vanuit het interne netwerk komen en van een andere verificatiemethode voor gebruikers die van buiten komen. Dit kan worden bereikt door verificatiebeleidsregels te definiëren op basis van netwerkbereiken.

Opmerking Om hoge beschikbaarheid voor Kerberos-verificatie in te stellen, is een load balancer vereist.

Kerberos-verificatieadapter configureren en inschakelen

Configureer de KerberosIdpAdapter en schakel deze in op de VMware Identity Manager-connector. Wanneer u een cluster voor hoge beschikbaarheid hebt geïmplementeerd, configureert u de adapter en schakelt u deze in op alle connectors in uw cluster.

Belangrijk Verificatieadapters op alle connectors in uw cluster moeten identiek zijn geconfigureerd. Op alle connectors moeten dezelfde verificatiemethoden worden geconfigureerd.

Raadpleeg de *Handleiding VMware Identity Manager-beheer* voor informatie over het configureren van Kerberos-verificatie.

Vereisten

De connector moet worden gekoppeld aan het domein Active Directory.

Procedure

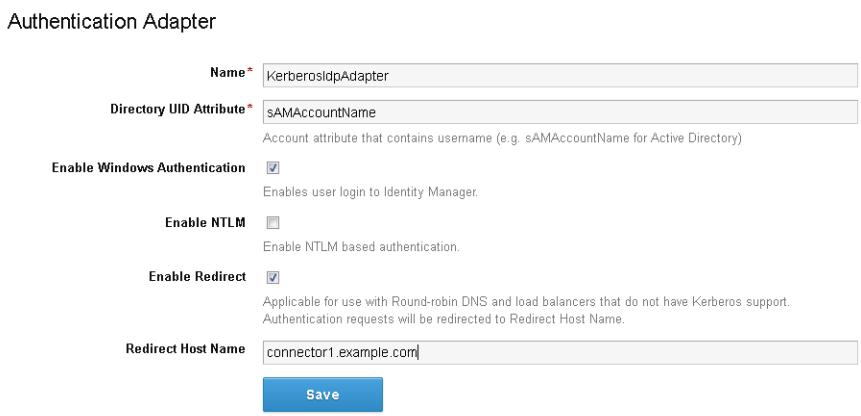
1. Klik in de VMware Identity Manager-beheerconsole op het tabblad **Identiteits- en toegangsbeheer**.
2. Klik op **Installatie** en klik dan op het tabblad **Connectors**.

   Alle connectors die u hebt geïmplementeerd worden weergegeven.
3. Klik op de koppeling in de kolom **Werker** van een van de connectors.
4. Klik op het tabblad **Verificatieadapters**.
5. Klik op de koppeling KerberosIdpAdapter en configureer de adapter en schakel deze in.

Optie	Beschrijving
Naam	De standaardnaam van de adapter is KerberosIdpAdapter. U kunt deze naam wijzigen.
Directory-UID-kenmerk	Het accountkenmerk dat de gebruikersnaam bevat.
Windows-verificatie inschakelen	Selecteer deze optie.
NTLM inschakelen	U hoeft deze optie alleen te selecteren wanneer uw Active Directory-infrastructuur van NTLM-verificatie afhankelijk is.

Optie	Beschrijving
Omleiden inschakelen	Selecteer deze optie en geef een waarde op voor **Hostnaam omleiden** wanneer u meerdere connectors in een cluster hebt en van plan bent om Kerberos-hoge beschikbaarheid in te stellen met behulp van een load balancer. Wanneer uw implementatie slechts één connector heeft, hoeft u de opties **Omleiden inschakelen** en **Hostnaam omleiden** niet te gebruiken.
Hostnaam doorverwijzen	Wanneer de optie **Omleiden inschakelen** is geselecteerd, is een waarde vereist. Voer de eigen hostnaam van de connector in. Wanneer de hostnaam van de connector bijvoorbeeld connector1.voorbeeld.com is, voert u **`connector1.voorbeeld.com`** in het -tekstvak in.

Bijvoorbeeld:



Raadpleeg de *Handleiding VMware Identity Manager-beheer* voor informatie over het configureren van de KerberosIdPAdapter.

6 Wanneer u een cluster hebt geïmplementeerd, configureert u de KerberosIdPAdapter op alle connectors in uw cluster.

Configureer de adapter op alle connectors op dezelfde manier.

Wat nu te doen

Stel indien nodig hoge beschikbaarheid in voor Kerberos-verificatie. Kerberos-verificatie is niet maximaal beschikbaar zonder een load balancer.

Hoge beschikbaarheid voor Kerberos-verificatie configureren

Om hoge beschikbaarheid voor Kerberos-verificatie te configureren, installeert u een load balancer in uw interne netwerk binnen de firewall en voegt u connectorappliances hieraan toe.

U moet ook bepaalde instellingen op de load balancer configureren, SSL-vertrouwen tot stand brengen tussen de load balancer en de connector, en de URL voor connectorverificatie wijzigen zodat de hostnaam van de load balancer wordt gebruikt.

Load balancer-instellingen configureren

U moet bepaalde instellingen op de load balancer configureren, zoals X-Forwarded-For-koppen inschakelen, de time-out van de load balancer juist instellen en sticky-sessies inschakelen.

Configureer deze instellingen.

- X-Forwarded-For-koppen

U moet X-Forwarded-For-koppen inschakelen op uw load-balancer. Hiermee wordt de verificatiemethode bepaald. Raadpleeg de documentatie die is meegeleverd door de leverancier van uw load-balancer voor meer informatie.

- Time-out van load-balancer

  Voor een juiste werking van de Connector moet u de standaardtime-out voor load-balancer-verzoeken verhogen. De waarde is ingesteld in minuten. Als de time-out te kort is ingesteld, wordt wellicht de volgende fout weergegeven.

  ```
  502–fout: De service is momenteel niet beschikbaar
  ```

- Sticky-sessies inschakelen

  U moet de instelling voor sticky-sessies inschakelen op de load-balancer als uw implementatie meerdere connectorapplicaties heeft. De load-balancer bindt vervolgens de sessie van een gebruiker aan een specifieke connectorinstantie.

Rootcertificaat van de VMware Identity Manager-connector toepassen op de load-balancer

Wanneer de virtual appliance van de VMware Identity Manager-Connector is geconfigureerd met een load-balancer, moet u SSL-vertrouwen tot stand brengen tussen de load-balancer en de Connector. Het rootcertificaat van de Connector moet worden gekopieerd naar de load-balancer.

Het certificaat van Connector kunt u downloaden van de beheerderspagina's van het connectorapparaat op https://*myconnector.mycompany*:8443/cfg/ssl.

Wanneer de domeinnaam van Connector naar de load-balancer wijst, kan het SSL-certificaat uitsluitend worden toegepast op de load-balancer.

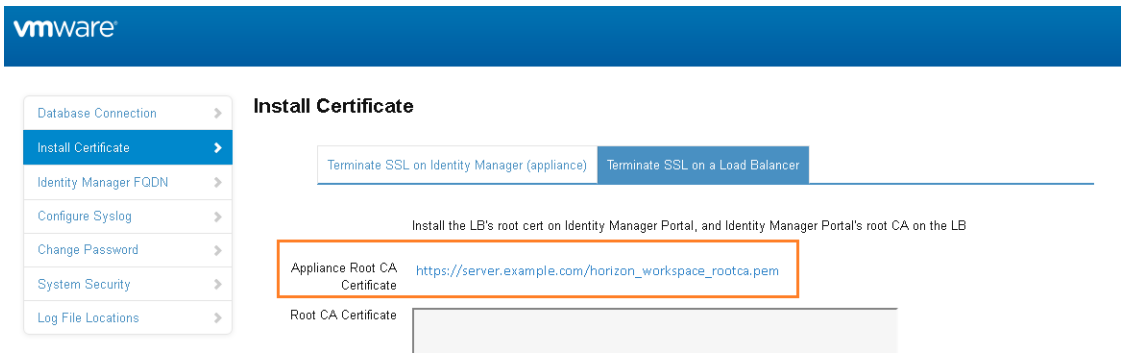
Aangezien de load-balancer communiceert met de virtual appliance van de Connector, moet u het root-CA-certificaat van de Connector naar de load-balancer kopiëren als vertrouwd rootcertificaat.

Procedure

1 Meld u aan op de beheerderspagina's van het Connector-apparaat, https://*myconnector.mycompany*:8443/cfg/ssl, als de beheerdersgebruiker.

2 Selecteer **Certificaat installeren**.

3 Selecteer het tabblad **SSL beëindigen op een load-balancer** en klik in het veld **Basis CA-certificaat van apparaat** op de link `https://hostnaam/horizon_workspace_rootca.pem`.



4 Kopieer alles tussen en inclusief de regels -----BEGIN CERTIFICATE----- en -----END CERTIFICATE----- en plak het basiscertificaat op de juiste locatie op elk van uw load-balancers. Raadpleeg de documentatie over de load-balancer.

Wat nu te doen

Kopieer en plak het basiscertificaat van de load-balancer naar de VMware Identity ManagerConnector-appliance.

Rootcertificaat voor load-balancer toepassen op de VMware Identity Manager-connector

Wanneer de virtual appliance van VMware Identity Manager-Connector is geconfigureerd met een load-balancer, moet u vertrouwen tot stand brengen tussen de load-balancer en de Connector. Naast het kopiëren van het rootcertificaat van de Connector naar de load-balancer, moet u het rootcertificaat van de load-balancer kopiëren naar de Connector.

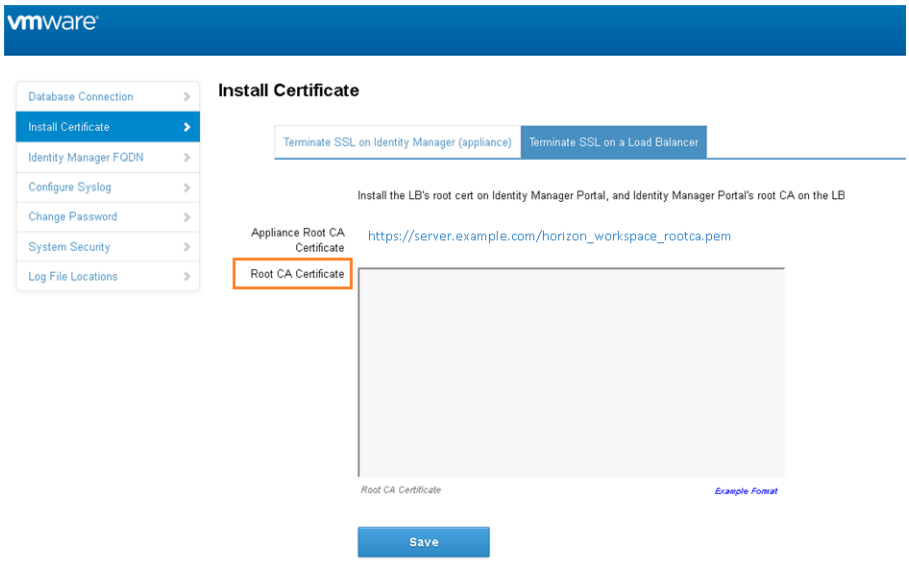
Procedure

1 Basiscertificaat van load-balancer verkrijgen

2 Ga naar de beheerpagina van het Connector-apparaat op https://*myconnector*.*Mycompany*:8443/cfg/ssl en meld u aan als de beheerdersgebruiker.

3 Op de pagina **Certificaat installeren** selecteert u het tabblad **SSL beëindigen op een load-balancer**.

4 Plak de tekst van het certificaat van de load-balancer in het veld **Basis CA-certificaat**.



5 Klik op **Opslaan**.

IdP-hostnaam van de connector wijzigen in de hostnaam van de load balancer

Wanneer u de connector van de virtual appliances aan de load balancer heeft toegevoegd, moet u de IdP-hostnaam op de Workspace IdP van elke connector wijzigen in de hostnaam van de load balancer.

Vereisten

De virtual appliance van Connector moet achter een load-balancer worden geconfigureerd. Zorg ervoor dat de poort van de load-balancer 443 is. Gebruik 8443 niet, omdat dit poortnummer de beheerderspoort is en uniek is voor elke virtual appliance.

Procedure

1 Meld u aan op de beheerconsole van VMware Identity Manager.

2 Klik op het tabblad **Identiteits- en toegangsbeheer**.

3 Klik op het tabblad **Identiteitsproviders**.

4 Klik in de pagina Identiteitsprovider op de koppeling Workspace IdP voor uw Connector-instantie.

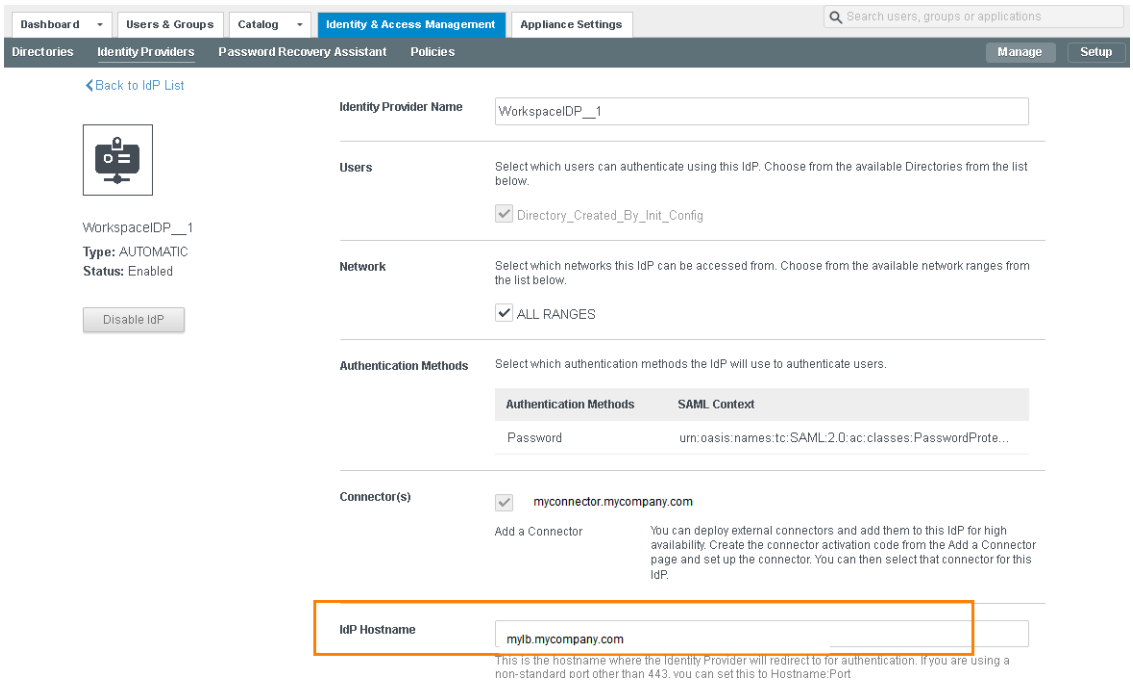
5 Wijzig in het tekstvak **IdP-hostnaam** de hostnaam van de Connector-hostnaam in de hostnaam van de load balancer.

Wanneer bijvoorbeeld uw Connector-hostnaam `myconnector` is en de hostnaam van uw load balancer `mylb` is, wijzigt u de URL-

`myconnector.mycompany.com:`*`poort`*

als volgt:

`mylb.mycompany.com:`*`poort`*



Index