VMware Identity Manager installeren en configureren

VMware Identity Manager 2.9.1

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

Over installeren en configureren van VMware Identity Manager

VMware Identity Manager installeren en configureren geeft informatie over het installatie- en configuratieproces voor het VMware Identity Manager-apparaat. Wanneer de installatie is voltooid, kunt u de beheerconsole gebruiken om gebruikers recht te geven op beheerde toegang tot multi-apparaten voor de applicaties van uw organisatie, waaronder applicaties van Windows, Software as a Service (SaaS) en de desktops View of Horizon.uikIn de handleiding wordt ook uitgelegd hoe u uw implementatie voor hoge beschikbaarheid kunt configureren.

Doelgroep

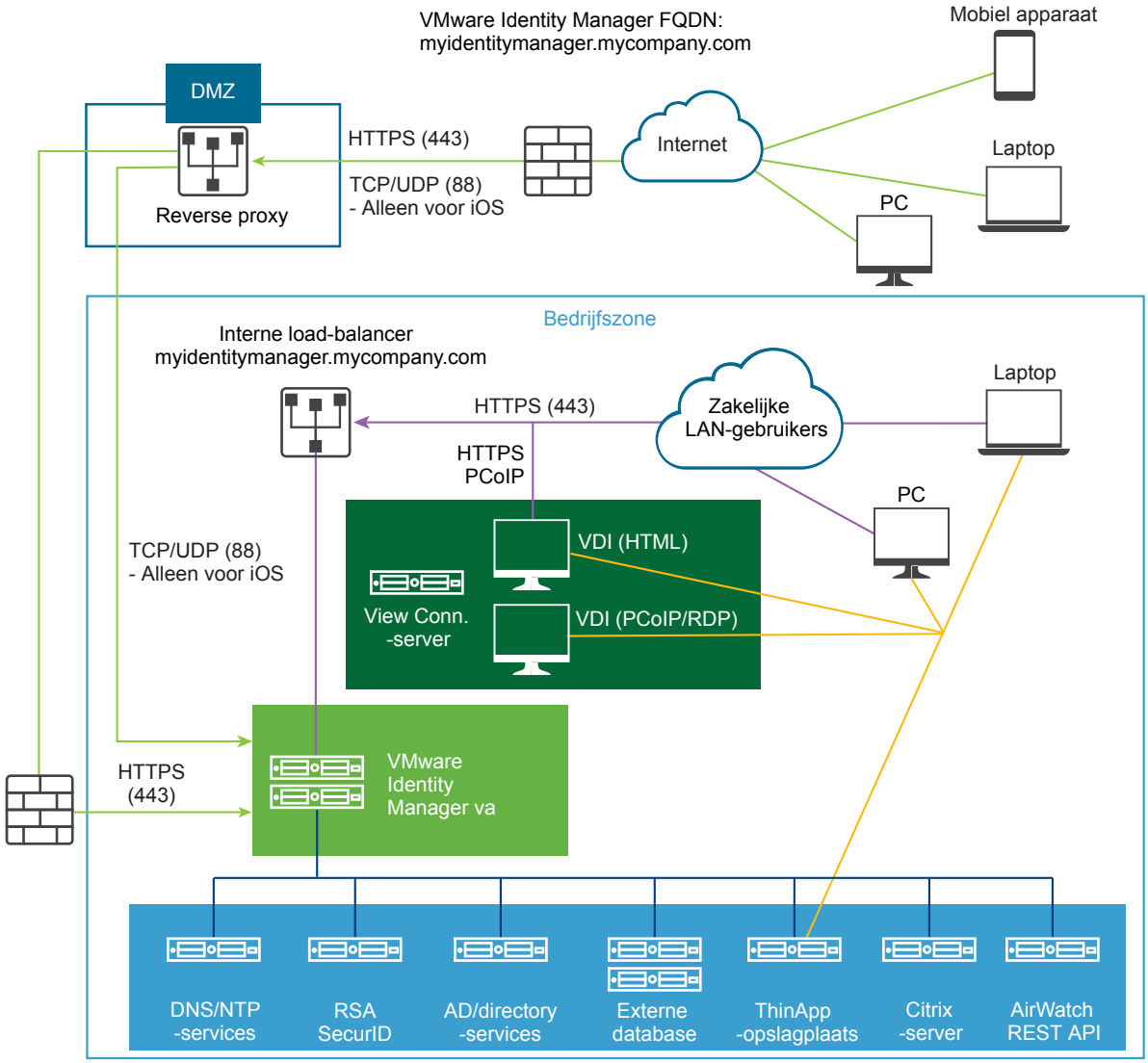
Deze informatie is bedoeld voor beheerders van VMware Identity Manager. De informatie is geschreven voor ervaren beheerders van het Windows- en Linuxsysteem die vertrouwd zijn met VMware-technologie, met name vCenter™, ESX™, vSphere® en View™, netwerkconcepten, Active Directory-servers, databases, backup- en herstelprocedures, Simple Mail Transfer Protocol (SMTP) en NTP-servers. SUSE Linux 11 is het onderliggende besturingssysteem voor de virtual appliance. Kennis van andere technologieën, zoals VMware ThinApp® en RSA SecurID is handig als u deze functies wilt implementeren.

Installatie van VMware Identity Manager voorbereiden

1

Voor de taken om VMware Identity Manager te implementeren en in te stellen, moet u de voorwaarden voltooien, het OVA-bestand van VMware Identity Manager implementeren en de installatie via de VMware Identity Manager-installatiewizard voltooien.

Figuur 1-1. VMware Identity Manager -architectuurdiagram voor gewone implementaties



Opmerking Als u van plan bent om verificatie op basis van certificaten of smartcards in te schakelen, gebruikt u de instelling SSL-doorvoer van de load-balancer in plaats van de instelling SSL beëindigen. Deze configuratie zorgt ervoor dat de SSL-handshake plaatsvindt tussen de connector, een onderdeel van VMware Identity Manager en de client.

Opmerking Afhankelijk van de locatie van de AirWatch-implementatie kunnen de AirWatch REST API's zich in de cloud of op locatie bevinden.

Dit hoofdstuk omvat de volgende onderwerpen:

Vereisten voor systeem- en netwerkconfiguratie

Denk na over uw gehele implementatie, onder andere over hoe u bronnen integreert, en wanneer u beslissingen neemt over hardware, bronnen en netwerkvereisten.

Ondersteund versies van vSphere en ESX

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

Opmerking U moet tijdsynchronisatie inschakelen op ESX-hostniveau met behulp van een NTP-server. Anders treedt er een tijdafwijking op tussen de virtual appliances.

Als u meerdere virtual appliances op verschillende hosts implementeert, kunt u de optie Synchroniseren met host uitschakelen voor tijdsynchronisatie en configureert u de NTP-server in elke virtual appliance rechtstreeks om ervoor te zorgen dat er geen afwijkingen optreden tussen de virtual appliances.

Hardwarevereisten

Zorg ervoor dat u voldoet aan de vereisten voor het aantal virtual VMware Identity Manager-appliances en de bronnen die zijn toegewezen aan elke appliance.

Aantal gebruikers	Tot 1.000	1000-10.000	10.000-25.000	25.000-50.000	50.000-100.000
Aantal VMware Identity Manager-servers	1 server	3 servers met load balancing	3 servers met load balancing	3 servers met load balancing	3 servers met load balancing
CPU (per server)	2 CPU's	2 CPU's	4 CPU's	8 CPU's	8 CPU's
RAM (per server)	6 GB	6 GB	8 GB	16 GB	32 GB
Schijfruimte (per server)	60 GB	100 GB	100 GB	100 GB	100 GB

Als u extra, externe virtual appliances van de connector installeert, moet u ervoor zorgen dat u voldoet aan de volgende vereisten.

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

Databasevereisten

Stel VMware Identity Manager in met een externe database om servergegevens op te slaan en te ordenen. Er is een interne PostgreSQL-database ingesloten in de virtual appliance, maar deze wordt niet aanbevolen voor gebruik in productie-implementaties.

Raadpleeg voor meer informatie over specifieke databaseversies en servicepackconfiguraties die worden ondersteund, de VMware-productinteroperabiliteitsmatrix op https://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

De volgende vereisten gelden voor een externe SQL Server-database.

Aantal gebruikers	Tot 1.000	1000-10.000	10.000-25.000	25.000-50.000	50.000-100.000
CPU	2 CPU's	2 CPU's	4 CPU's	8 CPU's	8 CPU's
RAM	4 GB	4 GB	8 GB	16 GB	32 GB
Schijfruimte	50 GB	50 GB	50 GB	100 GB	100 GB

Vereisten voor netwerkconfiguratie

Onderdeel	Minimumvereiste
DNS-record en IP-adres	IP-adres en DNS-record
Firewallpoort	Zorg ervoor dat de ingaande firewallpoort 443 naar de VMware Identity Manager-instantie of de load-balancer is geopend voor gebruikers.
Reverse proxy	Implementeer een reverse proxy zoals F5 Access Policy Manager in DMZ om gebruikers toe te staan op afstand toegang te krijgen tot de VMware Identity Manager-gebruikersportal.

Vereisten voor de poorten

De poorten die worden gebruikt in de serverconfiguratie, worden hieronder beschreven. Uw implementatie kan slechts een subset van deze poorten bevatten. Bijvoorbeeld:

- Als u gebruikers en groepen wilt synchroniseren vanuit Active Directory, moet VMware Identity Manager zijn verbonden met Active Directory.
- Als u wilt synchroniseren met ThinApp, moet de VMware Identity Manager aan het Active Directory-domein worden toegevoegd en zijn verbonden met de ThinApp-opslagplaats-share.

Poort	Portal	Source	Target	Beschrijving
443	HTTPS	Load-balancer	Virtual VMware Identity Manager-appliance	
443	HTTPS	Virtual VMware Identity Manager-appliance	Virtual VMware Identity Manager-appliance	
443	HTTPS	Browsers	Virtual VMware Identity Manager-appliance	
443	HTTPS	Virtual VMware Identity Manager-appliance	vapp-updates.vmware.com	Toegang tot de upgradeserver
8443	HTTPS	Browsers	Virtual VMware Identity Manager-appliance	Poort voor beheerders

Poort	Portal	Source	Target	Beschrijving
25	SMTP	Virtual VMware Identity Manager-appliance	SMTP	Poort om uitgaande e-mails door te geven
389 636 3268 3269	LDAP LDAPS MSFT-GC MSFT-GC-SSL	Virtual VMware Identity Manager-appliance	Active Directory	De standaardwaarden worden weergegeven. Deze poorten kunnen worden geconfigureerd.
445	TCP	Virtual VMware Identity Manager-appliance	VMware ThinApp-opslagplaats	Toegang tot de ThinApp-opslagplaats
5500	UDP	Virtual VMware Identity Manager-appliance	RSA SecurID-systeem	De standaardwaarde wordt weergegeven. Deze poort kan worden geconfigureerd.
53	TCP/UDP	Virtual VMware Identity Manager-appliance	DNS-server	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	TCP/UDP	Virtual VMware Identity Manager-appliance	Domeincontroller	
9300–9400 54328	TCP UDP	Virtual VMware Identity Manager-appliance	Virtual VMware Identity Manager-appliance	Auditbehoeften
1433, 5432, 1521	TCP	Virtual VMware Identity Manager-appliance	Database	De standaardpoort voor Microsoft SQL is 1433. De standaardpoort voor Oracle is 1521.
443		Virtual VMware Identity Manager-appliance	View-server	Toegang tot de View-server
80, 443	TCP	Virtual VMware Identity Manager-appliance	Citrix Integration Broker-server	Verbinding met de Citrix Integration Broker. De poortoptie is afhankelijk van de installatie van een certificaat op de Integration Broker-server
443	HTTPS	Virtual VMware Identity Manager-appliance	AirWatch REST API	Voor compliancecontrole van het apparaat en de verificatiemethode van het AirWatch Cloud Connector-wachtwoord, als dat wordt gebruikt.

Poort	Portal	Source	Target	Beschrijving
88	UDP	Unified Access Gateway	Virtual VMware Identity Manager-appliance	UDP-poort die moet worden geopend voor mobiele SSO
5262	TCP	mobiel Android-apparaat	AirWatch HTTPS-proxyservice	AirWatch Tunnel-client leidt verkeer naar de HTTPS-proxy voor Android-apparaten.
88	UDP	mobiel iOS-apparaat	Virtual VMware Identity Manager-appliance	Poort die wordt gebruikt voor Kerberos-verkeer van iOS-apparaten naar de in de cloud gehoste KDC-service.
443	HTTPS/TCP			

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.

Ondersteunde webbrowsers om toegang te krijgen tot de beheerconsole

De VMware Identity Manager-beheerconsole is een webapplicatie die u gebruikt om uw tenant te beheren. U kunt de Beheerconsole openen via de volgende browsers.

- Internet Explorer 11 voor Windows-systemen
- Google Chrome 42.0 of later voor Windows- en Mac-systemen
- Mozilla Firefox 40 of later voor Windows- en Mac-systemen
- Safari 6.2.8 en later voor Mac-systemen

Opmerking In Internet Explorer 11 moet JavaScript zijn ingeschakeld en moeten cookies worden toegestaan om te kunnen verifiëren via VMware Identity Manager.

Ondersteunde browsers voor toegang tot Workspace ONE-portal

Eindgebruikers hebben toegang tot de Workspace ONE-portal via de volgende browsers.

- Mozilla Firefox (meest recente versie)
- Google Chrome (meest recente versie)
- Safari (meest recente versie)
- Internet Explorer 11
- Microsoft Edge-browser
- Systeemeigen browser en Google Chrome op Android-apparaten
- Safari op iOS-apparaten

Opmerking In Internet Explorer 11 moet JavaScript zijn ingeschakeld en moeten cookies worden toegestaan om te kunnen verifiëren via VMware Identity Manager.

Voorbereiding op de implementatie van VMware Identity Manager

Voordat u VMware Identity Manager implementeert, moet u uw omgeving voorbereiden. Deze voorbereiding omvat het downloaden van het VMware Identity Manager OVA-bestand, het maken van DNS-records, en het verkrijgen van IP-adressen.

Vereisten

Voordat u met de installatie van VMware Identity Manager begint, voltooit u eerst de vereiste taken.

- U hebt één of meer ESX-servers nodig om het virtuele VMware Identity Manager-apparaat te implementeren.

  Opmerking Raadpleeg voor meer informatie over ondersteunde vSphere- en ESX-serverversies de VMware-productinteroperabiliteitsmatrices op http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

- Voor VMware vSphere Client of vSphere Web Client moet het OVA-bestand worden geïmplementeerd en moet er op afstand verbinding worden gemaakt met de geïmplementeerde virtual appliance om netwerken te configureren.
- Download het VMware Identity Manager OVA-bestand van de VMware-website.

Maak DNS-records en IP-adressen

Een DNS-vermelding en een statisch IP-adres moeten beschikbaar zijn voor de VMware Identity Manager van de virtual appliance. Aangezien elk bedrijf zijn IP-adressen en DNS-records op een andere wijze beheert, vraagt u, voordat u met de installatie begint, om de DNS-record en de IP-adressen die u wilt gebruiken.

Reverse lookup configureren is optioneel. Wanneer u reverse lookup implementeert, moet u een PTR-record definiëren op de DNS-server, zodat de virtual appliance de juiste netwerkconfiguratie gebruikt.

U kunt de volgende lijst voorbeelden van DNS-records gebruiken wanneer u uw netwerkbeheerder spreekt. Vervang de voorbeeldinformatie door informatie uit uw omgeving. Dit voorbeeld toont forward DNS-records en IP-adressen.

Tabel 1-1. Voorbeelden van forward DNS-records en IP-adressen

Domeinnaam	Brontype	IP-adres
myidentitymanager.company.com	De	10.28.128.3

Dit voorbeeld toont reverse DNS-records en IP-adressen.

Tabel 1-2. Voorbeelden van reverse DNS-records en IP-adressen

IP-adres	Brontype	Hostnaam
10.28.128.3	PTR	myidentitymanager.company.com

Nadat u de configuratie van DNS hebt voltooid, controleert u of de reverse DNS-lookup goed is geconfigureerd. De opdracht `host IPaddress` van de virtual appliance moet bijvoorbeeld leiden tot het opzoeken van de DNS-naam.

Een op Unix/Linux gebaseerde DNS-server gebruiken

Als u een op Unix of Linux gebaseerde DNS-server gebruikt en van plan bent om de van de VMware Identity Manager toe te voegen aan het domein van Active Directory, zorgt u ervoor dat de juiste servicebronrecords (SRV) voor elke domeincontroller van Active Directory worden gemaakt.

Opmerking Als u een load balancer heeft met een Virtual IP-adres (VIP) vóór de DNS-servers, houd er dan rekening mee dat VMware Identity Manager het gebruik van een VIP niet ondersteunt. U kunt meerdere DNS-servers specificeren die door een komma worden gescheiden.

Databaseopties met VMware Identity Manager

Stel VMware Identity Manager in met een externe database om servergegevens op te slaan en te ordenen. Er is een interne PostgreSQL-database geïntegreerd in de toepassing, maar deze wordt niet aanbevolen voor gebruik in productie-implementaties.

Als u een externe database wilt gebruiken, moet uw databasebeheerder een lege externe database en een schema voorbereiden voordat er verbinding wordt gemaakt met de externe database in de installatiewizard. Licentiegebruikers kunnen een Microsoft SQL-databaseserver of Oracle-databaseserver gebruiken om een externe databaseomgeving met hoge beschikbaarheid in te stellen. Zie "Aan de database koppelen," op pagina 34.

Uw bedrijfsdirectory aansluiten

VMware Identity Manager gebruikt de infrastructuur van uw bedrijfsdirectory voor gebruikersverificatie en -beheer. U kunt VMware Identity Manager integreren met 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. U kunt VMware Identity Manager ook integreren met een LDAP-directory. De virtual appliance van VMware Identity Manager moet verbinding maken met de directory om gebruikers en groepen te synchroniseren.

Uw directory moet in hetzelfde LAN-netwerk toegankelijk zijn als de virtual appliance van VMware Identity Manager.

Raadpleeg Hoofdstuk 4, "Integreren met uw Enterprise-directory," op pagina 45 voor meer informatie.

Implementatiecontrolelijsten

U kunt de implementatiecontrolelijst gebruiken om de benodigde informatie te verzamelen om de virtual appliance van VMware Identity Manager te installeren.

Informatie voor Fully Qualified Domain Name (FQDN)

Tabel 1-3. Informatiecontrolelijst van Fully Qualified Domain Name (FQDN)

Informatie om te verzamelen	Vermeld de informatie
FQDN van VMware Identity Manager	

Netwerkinformatie voor de virtual appliance van VMware Identity Manager

Tabel 1-4. Controlelijst van netwerkinformatie

Informatie om te verzamelen	Vermeld de informatie
IP-adres	U moet een statisch IP-adres gebruiken en dit moet een PTR hebben, evenals een A-record die is gedefinieerd in de DNS.
DNS-naam voor deze virtual appliance	

Tabel 1-4. Controlelijst van netwerkinformatie (Vervolgd)

Informatie om te verzamelen	Vermeld de informatie
Standaard gateway-adres	
Netmask of prefix	

Directory-informatie

VMware Identity Manager ondersteunt de integratie met omgevingen van Active Directory of LDAP-directory.

Tabel 1-5. Controlelijst van domeincontroller van Active Directory

Informatie om te verzamelen	Vermeld de informatie
Servernaam van Active Directory	
Domeinnaam van Active Directory	
Basis-DN	
Voor Active Directory over LDAP: de Bind-DN-gebruikersnaam en het wachtwoord	
Voor Active Directory met geïntegreerde Windows-verificatie: de gebruikersnaam en het wachtwoord van het account dat rechten heeft om computers aan het domein toe te voegen.	

Tabel 1-6. Informatiecontrolelijst van LDAP-directoryserver

Informatie om te verzamelen	Vermeld de informatie
Naam of IP-adres van LDAP-directoryserver	
Poortnummer van LDAP-directoryserver	
Basis-DN	
Bind-DN-gebruikersnaam en wachtwoord	
LDAP-zoekfilters voor groepsobjecten, objecten van bindingsgebruikers en gebruikersobjecten	
LDAP-kenmerknamen voor lidmaatschap, object-UUID en kenmerkende naam (DN)	

SSL-certificaten

U kunt een SSL-certificaat toevoegen nadat u de virtual appliance van VMware Identity Manager hebt geïmplementeerd.

Tabel 1-7. Informatiecontrolelijst SSL-certificaat

Informatie om te verzamelen	Vermeld de informatie
SSL-certificaat	
Privésleutel	

Licentiecode

Tabel 1-8. Informatiecontrolelijst van licentiecode van VMware Identity Manager

Informatie om te verzamelen	Vermeld de informatie
Licentiecode	

Opmerking De informatie van de licentiecode wordt ingevoerd in de beheerconsole op de pagina **Appliance-instellingen > Licentie** nadat de installatie is voltooid.

Externe database

Tabel 1-9. Informatiecontrolelijst van externe database

Informatie om te verzamelen	Vermeld de informatie
Hostnaam van database	
Poort	
Gebruikersnaam	
Wachtwoord	

Programma voor de verbetering van de gebruikerservaring

Wanneer u de virtual appliance VMware Identity Manager installeert, kunt u ervoor kiezen om mee te doen aan het programma voor de verbetering van gebruikerservaring van VMware.

Wanneer u meedoet aan het programma, verzamelt VMware anonieme gegevens over uw implementatie om beter te kunnen reageren op de vereisten van gebruikers. Er worden geen gegevens verzameld aan de hand waarvan uw organisatie kan worden herleid.

Voordat de gegevens worden verzameld, maakt VMware alle velden die informatie bevatten die specifiek is voor uw organisatie, anoniem.

Opmerking Wanneer uw netwerk is geconfigureerd om via HTTP-proxy toegang te krijgen tot het internet, moet u de proxy-instellingen in de virtual appliance VMware Identity Manager wijzigen om deze informatie te kunnen verzenden. Zie "Proxyserverinstellingen instellen voor VMware Identity Manager," op pagina 30.

VMware Identity Manager implementeren 2

Om VMware Identity Manager te implementeren, implementeert u het OVF-sjabloon met behulp van de vSphere Client of de vSphere Web Client, schakelt u de virtual appliance van VMware Identity Manager in en configureert u de instellingen.

Nadat de virtual appliance van VMware Identity Manager is geïmplementeerd, gebruikt u de wizard Setup om de omgeving van VMware Identity Manager te installeren.

Gebruik de informatie in de implementatiecontrolelijst om de installatie te voltooien. Zie "Implementatiecontrolelijsten," op pagina 16.

Dit hoofdstuk omvat de volgende onderwerpen:

Het OVA-bestand van VMware Identity Manager installeren

U implementeert het OVA-bestand van VMware Identity Manager met behulp van de vSphere Client of de vSphere Web Client. U kunt het OVA-bestand downloaden en implementeren vanaf een lokale locatie die toegankelijk is voor de vSphere Client, of het bestand implementeren via een web-URL.

Opmerking Als u de vSphere Web Client gebruikt, moet u de Firefox- of de Chrome-browser gebruiken om het OVA-bestand te implementeren. Gebruik geen Internet Explorer.

Vereisten

Controleer Hoofdstuk 1, "Installatie van VMware Identity Manager voorbereiden," op pagina 9.

Procedure

1 Download het VMware Identity Manager OVA-bestand via My VMware.

2 Meld u aan bij de vSphere Client of de vSphere Web Client.

3 Selecteer **Bestand > OVF-sjabloon implementeren**.

4 In de wizard OVF-sjabloon implementeren geeft u de volgende informatie op.

Pagina	Beschrijving
Bron	Blader naar de locatie van het OVA-pakket of voer de bijbehorende URL in.
OVF-sjabloondetails	Controleer de productgegevens, waaronder de vereisten voor de versie en de grootte.
Licentieovereenkomst voor eindgebruikers	Lees de licentieovereenkomst voor eindgebruikers en klik op **Accepteren**.
Naam en Locatie	Geef een naam op voor het virtual VMware Identity Manager-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 het cluster waarin u de virtual appliance wilt uitvoeren.
Brongroep	Selecteer de brongroep.
Opslag	Selecteer de locatie voor de bestanden van de virtual appliance. U kunt ook een VM-opslagprofiel selecteren.
Schijfindeling	Selecteer de schijfindeling voor de bestanden. Voor productieomgevingen selecteert u een van de Thick Provision-indelingen. Gebruik de Thin Provision-indeling voor evaluaties en tests. In de Thick Provision-indeling wordt alle benodigde ruimte voor de virtuele schijf toegewezen tijdens de implementatie. In de Thin Provision-indeling gebruikt de schijf alleen de hoeveelheid opslagruimte die nodig is voor de eerste bewerkingen.
Netwerktoewijzing	Wijs de netwerken die worden gebruikt in VMware Identity Manager toe aan netwerken in uw inventaris.
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 te kunnen reageren op de vereisten 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 (FQDN)** de naam van de host in. Als dit vak leeg is, wordt de hostnaam opgezocht via een omgekeerde DNS-zoekactie. d Configureer de netwerkeigenschappen. ■ Als u een statisch IP-adres wilt configureren voor VMware Identity Manager, geeft u het adres op in de velden **Standaardgateway**, **DNS**, **IP-adres**, en **Netmask**. **Opmerking** Als u een load balancer heeft met een Virtual IP-adres (VIP) vóór de DNS-servers, houd er dan rekening mee dat VMware Identity Manager het gebruik van een VIP niet ondersteunt. U kunt meerdere DNS-servers specificeren die door een komma worden gescheiden. **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. **Opmerking** De velden **Domeinnaam** en **Zoekpad van domein** worden niet gebruikt. U kunt deze velden leeg laten. (Optioneel) Nadat VMware Identity Manager is geïnstalleerd, kunt u IP-groepen configureren. Zie "(Optioneel) IP-adresgroepen toevoegen," op pagina 21.
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 dat wordt weergegeven.

5 Wanneer de implementatie is voltooid, klikt u op **Sluiten** in het voortgangsdialoogvenster.

6 Selecteer het virtual VMware Identity Manager-appliance dat u hebt geïmplementeerd, klik er met de rechtermuisknop op en selecteer **Energie > Inschakelen**.

Het virtual VMware Identity Manager-appliance wordt geïnitialiseerd. Op het tabblad **Console** kunt u de details bekijken. Wanneer de virtual appliance is geïnitialiseerd, ziet u in het consolescherm de VMware Identity Manager-versie, het IP-adres en de URL's waarmee u zich bij de VMware Identity Manager-webinterface kunt aanmelden om de installatie te voltooien.

Wat nu te doen

- (Optioneel) Voeg IP-groepen toe.
- Configureer de instellingen voor VMware Identity Manager, waaronder de verbinding met uw Active Directory of LDAP-directory en selecteer gebruikers en groepen om te synchroniseren met VMware Identity Manager.

(Optioneel) IP-adresgroepen toevoegen

Netwerkconfiguratie met IP-adresgroepen is optioneel in VMware Identity Manager. U kunt handmatig IP-adresgroepen toevoegen aan de virtual appliance van VMware Identity Manager nadat deze is geïnstalleerd.

IP-adresgroepen werken als DHCP-servers om IP-adressen van de groep toe te wijzen aan de virtual appliance van VMware Identity Manager. Om de IP-adresgroepen te gebruiken, bewerkt u de netwerkeigenschappen van de virtual appliance om de eigenschappen aan te passen naar dynamische eigenschappen en om de netmask, gateway en DNS-instellingen te configureren.

Vereisten

De virtual appliance moet zijn uitgeschakeld.

Procedure

1 In de vSphere Client of de vSphere Web Client klikt u met de rechter muisknop op de virtual appliance van VMware Identity Manager en selecteert u **Instellingen bewerken**.

2 Selecteer het tabblad **Opties**.

3 Onder **vApp-opties** klikt u op **Geavanceerd**.

4 In de sectie Eigenschappen aan de rechterkant klikt u op de knop **Eigenschappen**.

5 In het dialoogvenster Geavanceerde configuratie van eigenschappen configureert u de volgende sleutels:

- vami.DNS.WorkspacePortal
- vami.netmask0.WorkspacePortal
- vami.gateway.WorkspacePortal

a Selecteer een van de sleutels en klik op **Bewerken**.

b In het dialoogvenster Instellingen van eigenschap bewerken, naast het veld **Type**, klikt u op **Bewerken**.

c In het dialoogvenster Eigenschaptype bewerken selecteert u **Dynamische eigenschap** en selecteert u de geschikte waarde uit het vervolgkeuzemenu voor **Netmask**, **Gateway-adres** en **DNS-servers**.

d Klik op **OK** en klik opnieuw op **OK**.

e Herhaal deze stappen om elke sleutel te configureren.

6 Start de virtual appliance.

De eigenschappen zijn geconfigureerd om IP-adresgroepen te gebruiken.

Wat nu te doen

Configureer VMware Identity Manager-instellingen.

Instellingen van VMware Identity Manager configureren

Nadat de OVA van VMware Identity Manager is geïmplementeerd, gebruikt u de wizard Setup om wachtwoorden in te stellen en een database te selecteren. Vervolgens stelt u de verbinding in naar uw Active Directory of LDAP-directory.

Vereisten

- De virtual appliance van VMware Identity Manager is ingeschakeld.
- Als u een externe database gebruikt, is de externe database geconfigureerd en is de verbindingsinformatie van de externe database beschikbaar. Zie "Aan de database koppelen," op pagina 34 voor informatie.
- Bekijk Hoofdstuk 4, "Integreren met uw Enterprise-directory," op pagina 45, "Met Active Directory integreren," op pagina 47 en "Een LDAP-directory met de service integreren," op pagina 62 voor vereisten en beperkingen.
- U hebt de informatie van uw Active Directory of LDAP-directory.
- Wanneer multi-forest Active Directory is geconfigureerd en de lokale domeingroep bevat leden van domeinen in verschillende forests, moet de Bind DN-gebruiker die op de Directorypagina van VMware Identity Manager wordt gebruikt, worden toegevoegd aan de beheerdersgroep van het domein waarin de lokale domeingroep verblijft. Als u dit niet doet, ontbreken deze leden in de lokale domeingroep.
- U hebt een lijst van de gebruikerskenmerken die u als filters wilt gebruiken en een lijst van de groepen die u wilt toevoegen aan VMware Identity Manager.

Procedure

1. Ga naar de URL van VMware Identity Manager die wordt weergegeven op het blauwe scherm op het tabblad **Console**. Bijvoorbeeld `https://hostname.example.com`.
2. Accepteer het certificaat, indien hierom wordt gevraagd.
3. Klik op de pagina Aan de slag op **Doorgaan**.
4. Op de pagina Wachtwoorden instellen, stelt u wachtwoorden in voor de volgende beheerdersaccounts, die worden gebruikt om het apparaat te beheren. Klik vervolgens op **Doorgaan**.

Account	
Apparaatbeheerder	Stel het wachtwoord in voor de **beheerdersgebruiker**. Deze gebruikersnaam kan niet worden gewijzigd. Het account van de **beheerdersgebruiker** wordt gebruikt om de apparaatinstellingen te beheren. **Belangrijk** Het wachtwoord voor de **beheerdersgebruiker** moet minstens zes tekens lang zijn.
Apparaathoofdgebruiker	Stel het wachtwoord van de **`hoofdgebruiker`** in. De **hoofdgebruiker** heeft volledige rechten op het apparaat.
Gebruiker op afstand	Stel het wachtwoord van de **sshuser** in, dat wordt gebruikt om u op afstand aan te melden op het apparaat met een SSH-verbinding.

5 Op de pagina Database selecteren selecteert u de database die moet worden gebruikt.

Raadpleeg "Aan de database koppelen," op pagina 34 voor meer informatie.

- Als u een externe database gebruikt, selecteert u **Externe database** en voert u de verbindingsinformatie in van de externe database, de gebruikersnaam en het wachtwoord. Om te controleren of VMware Identity Manager verbinding kan maken met de database, klikt u op **Verbinding testen**.

  Nadat u de verbinding hebt gecontroleerd, klikt u op **Doorgaan**.

- Als u de interne database gebruikt, klikt u op **Doorgaan**.

  Opmerking Het gebruik van de interne database wordt afgeraden bij productie-implementaties.

De verbinding met de database wordt geconfigureerd en de database wordt opgestart. Wanneer het proces is voltooid, verschijnt de pagina **Instellen is voltooid**.

6 Klik op de link **Meld u aan op de beheerdersconsole** op de pagina **Het instellen is voltooid** om u aan te melden op de beheerconsole om de verbinding met de Active Directory of de LDAP-directory in te stellen.

7 Meld u aan op de beheerconsole als de **beheerdersgebruiker** met het wachtwoord dat u instelt.

U bent aangemeld als een lokale beheerder. De Directorypagina verschijnt. Voordat u een directory toevoegt, zorgt u ervoor dat u Hoofdstuk 4, "Integreren met uw Enterprise-directory," op pagina 45, "Met Active Directory integreren," op pagina 47 en "Een LDAP-directory met de service integreren," op pagina 62 bekijkt voor vereisten en beperkingen.

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

9 Klik op **Instellen > Gebruikerskenmerken** om de gebruikerskenmerken te selecteren die naar de directory worden gesynchroniseerd.

Standaardkenmerken worden vermeld en u kunt de kenmerken selecteren die zijn vereist. Als een kenmerk als vereist wordt gemarkeerd, worden alleen gebruikers met dat kenmerk naar de service gesynchroniseerd. U kunt ook andere kenmerken toevoegen.

Belangrijk Nadat een directory is gemaakt, kunt u een kenmerk niet wijzigen naar een vereist kenmerk. U moet nu die selectie doen.

Wees u er ook van bewust dat de instellingen op de pagina Gebruikerskenmerken van toepassing zijn op alle directory's in de service. Wanneer u een kenmerk markeert als vereist, moet u het gevolg ervan op de andere directory's overwegen. Als een kenmerk als vereist is gemarkeerd, worden gebruikers zonder dat kenmerk niet op de service gesynchroniseerd.

Belangrijk Als u XenApp-bronnen wilt synchroniseren met VMware Identity Manager, moet u **distinguishedName** instellen als een vereist kenmerk.

10 Klik op **Opslaan**.

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

12 Klik op de Directorypagina op **Directory toevoegen** en selecteer **Active Directory via LDAP/IWA toevoegen** of **LDAP-directory toevoegen** op basis van het type directory dat u integreert.

U kunt ook een lokale directory in de service maken. Zie Hoofdstuk 5, "Lokale directory's gebruiken," op pagina 69 voor meer informatie over het gebruik van lokale directory's.

13 Voor Active Directory volgt u deze stappen.

a Voer een naam in voor de directory die u in VMware Identity Manager maakt en selecteer het type directory, ofwel **Active Directory via LDAP** of **Active Directory (geïntegreerde Windows-verificatie (IWA))**.

b Verstrek de verbindingsinformatie.

Optie	Beschrijving
Active Directory via LDAP	1 In het veld **Synchronisatieconnector** selecteert u de Connector die u wilt gebruiken om gebruikers en groepen van Active Directory te synchroniseren naar de directory van VMware Identity Manager. Een connectorcomponent is altijd standaard beschikbaar met de VMware Identity Manager-service. Deze connector verschijnt in het vervolgkeuzemenu. Als u meerdere VMware Identity Manager-apparaten installeert voor hoge beschikbaarheid, verschijnt de connectorcomponent van elk van die apparaten in de lijst. 2 In het veld **Verificatie** selecteert u **Ja** als u deze Active Directory wilt gebruiken om gebruikers te verifiëren. Als u een externe identiteitsprovider wilt gebruiken om gebruikers te verifiëren, klikt u op **Nee**. Nadat u de verbinding van de Active Directory hebt geconfigureerd om gebruikers en groepen te synchroniseren, gaat u naar de pagina **Identiteits- en toegangsbeheer > Beheren > Identiteitsproviders** om de externe identiteitsprovider voor verificatie toe te voegen. 3 In het veld **Zoekkenmerk directory** selecteert u het accountkenmerk dat de gebruikersnaam bevat. 4 Als de Active Directory de opzoekfunctie DNS Service Location gebruikt, selecteert u het volgende. ■ In de sectie **Server Location** schakelt u het selectievakje **Deze directory ondersteunt DNS Service Location** in. Een bestand `domain_krb.properties` dat automatisch is ingevuld met een lijst domeincontrollers, wordt gemaakt wanneer de directory is gemaakt. Zie “Domeincontrollers selecteren (bestand domain_krb.properties),” op pagina 49. ■ Als Active Directory de versleuteling STARTTLS vereist, schakelt u het selectievakje **Deze directory vereist dat alle verbindingen SSL gebruiken** in de sectie **Certificaten** in en kopieert en plakt u het basis CA-certificaat van de Active Directory in het veld **SSL-certificaat**. Zorg ervoor dat het certificaat in PEM-formaat is en neem de regels "BEGIN CERTIFICATE" en "END CERTIFICATE" op. **Opmerking** Als de Active Directory STARTTLS vereist en u verstrekt het certificaat niet, kunt u de directory niet maken. 5 Als de Active Directory geen opzoekfunctie van DNS Service Location gebruikt, selecteert u het volgende. ■ In de sectie **Server Location** controleert u of het selectievakje **Deze directory ondersteunt DNS Service Location** niet is ingeschakeld en voert u de serverhostnaam en het poortnummer van de Active Directory in. Zie de sectie Multi-domein, Single Forest Active Directory-omgeving in “Active Directory-omgevingen,” op pagina 47 om de directory als een globale catalogus te configureren. ■ Als de Active Directory toegang over SSL vereist, schakelt u het selectievakje **Deze directory vereist dat alle verbindingen SSL gebruiken** in de sectie **Certificaten** in en kopieert en plakt u het basis CA-certificaat van de Active Directory in het veld **SSL-certificaat**. Zorg ervoor dat het certificaat in PEM-formaat is en neem de regels "BEGIN CERTIFICATE" en "END CERTIFICATE" op.

Optie	Beschrijving
	Opmerking Als de Active Directory SSL vereist en u verstrekt het certificaat niet, kunt u de directory niet maken. 6 In de sectie **Wijziging van wachtwoord toestaan** selecteert u **Wijziging van wachtwoord inschakelen** als u wilt dat gebruikers hun wachtwoorden kunnen resetten vanaf de aanmeldingspagina van VMware Identity Manager als het wachtwoord verloopt of als de beheerder van Active Directory het wachtwoord van de gebruiker reset. 7 In het veld **Base DN** voert u de DN in vanwaar de accountzoekopdrachten moeten starten. Bijvoorbeeld OU=myUnit,DC=myCorp,DC=com. 8 In het veld **Bind DN** voert u het account in dat naar gebruikers kan zoeken. Bijvoorbeeld CN=binduser,OU=myUnit,DC=myCorp,DC=com. **Opmerking** Het gebruik van een gebruikersaccount van Bind DN met een wachtwoord dat niet verloopt, wordt aanbevolen. 9 Nadat u het bindingswachtwoord hebt ingevoerd, klikt u op **Verbinding testen** om te controleren of de directory verbinding kan maken met uw Active Directory.
Active Directory (geïntegreerde Windows-verificatie)	1 In het veld **Synchronisatieconnector** selecteert u de Connector die u wilt gebruiken om gebruikers en groepen van Active Directory te synchroniseren naar de directory van VMware Identity Manager. Een connectorcomponent is altijd standaard beschikbaar met de VMware Identity Manager-service. Deze connector verschijnt in het vervolgkeuzemenu. Als u meerdere VMware Identity Manager-apparaten installeert voor hoge beschikbaarheid, verschijnt de connectorcomponent van elk van die apparaten in de lijst. 2 Als u deze Active Directory wilt gebruiken om gebruikers te verifiëren, klikt u in het veld **Verificatie** op **Ja**. Als u een externe identiteitsprovider wilt gebruiken om gebruikers te verifiëren, klikt u op **Nee**. Nadat u de verbinding van de Active Directory hebt geconfigureerd om gebruikers en groepen te synchroniseren, gaat u naar de pagina **Identiteits- en toegangsbeheer > Beheren > Identiteitsproviders** om de externe identiteitsprovider voor verificatie toe te voegen. 3 In het veld **Zoekkenmerk directory** selecteert u het accountkenmerk dat de gebruikersnaam bevat. 4 Als de Active Directory de versleuteling STARTTLS vereist, schakelt u het selectievakje **Deze directory vereist dat alle verbindingen STARTTLS gebruiken** in de sectie **Certificaten** in en kopieert en plakt u het basis CA-certificaat van de Active Directory in het veld **SSL-certificaat**. Zorg ervoor dat het certificaat in PEM-formaat is en neem de regels "BEGIN CERTIFICATE" en "END CERTIFICATE" op. Als de directory meerdere domeinen heeft, voegt u één voor één het basis CA-certificaat voor alle domeinen toe. **Opmerking** Als de Active Directory STARTTLS vereist en u verstrekt het certificaat niet, kunt u de directory niet maken. 5 Voer de naam in van het Active Directory-domein dat wordt toegevoegd. Voer een gebruikersnaam en wachtwoord in dat de rechten heeft om het domein toe te voegen. Raadpleeg "Vereiste rechten voor het toevoegen aan een domein," op pagina 55 voor meer informatie. 6 In de sectie **Wijziging van wachtwoord toestaan** selecteert u **Wijziging van wachtwoord inschakelen** als u wilt dat gebruikers hun wachtwoorden kunnen resetten vanaf de aanmeldingspagina van VMware Identity Manager als het wachtwoord verloopt of als de beheerder van Active Directory het wachtwoord van de gebruiker reset.

Optie	Beschrijving
	7 In het veld **Gebruikers-UPN Bind** voert u de User Principal Name (UPN) van de gebruiker in die met het domein kan worden geverifieerd. Bijvoorbeeld username@example.com. **Opmerking** Het gebruik van een gebruikersaccount van Bind DN met een wachtwoord dat niet verloopt, wordt aanbevolen. 8 Voer het wachtwoord van de Bind DN-gebruiker in.

c Klik op **Opslaan en Volgende**.

De pagina met de lijst domeinen verschijnt.

14 Voor LDAP-directory's volgt u deze stappen.

a Verstrek de verbindingsinformatie.

Optie	Beschrijving
Directorynaam	Een naam voor de directory die u in VMware Identity Manager maakt.
Directory synchroniseren en verificatie	1 In het veld **Synchronisatieconnector** selecteert u de connector die u wilt gebruiken om gebruikers en groepen te synchroniseren van uw LDAP-directory naar de directory van VMware Identity Manager. Een connectorcomponent is altijd standaard beschikbaar met de VMware Identity Manager-service. Deze connector verschijnt in het vervolgkeuzemenu. Als u meerdere VMware Identity Manager-apparaten installeert voor hoge beschikbaarheid, verschijnt de connectorcomponent van elk van die apparaten in de lijst. U hebt geen afzonderlijke connector nodig voor een LDAP-directory. Een connector kan meerdere directory's ondersteunen, ongeacht of het directory's zijn van Active Directory of LDAP. 2 In het veld **Verificatie** selecteert u **Ja** als u deze LDAP-directory wilt gebruiken om gebruikers te verifiëren. Als u een externe identiteitsprovider wilt gebruiken om gebruikers te verifiëren, selecteert u **Nee**. Nadat u de directoryverbinding hebt toegevoegd om gebruikers en groepen te synchroniseren, gaat u naar de pagina **Identiteits- en toegangsbeheer > Beheren > Identiteitsproviders** om de identiteitsprovider voor verificatie toe te voegen. 3 In het veld **Zoekkenmerk directory** specificeert u het LDAP-directorykenmerk dat voor de gebruikersnaam wordt gebruikt. Als het kenmerk niet wordt vermeld, selecteert u **Aangepast** en typt u de kenmerknaam. Bijvoorbeeld **`cn`**.
Serverlocatie	Voer de serverhost en het poortnummer van de LDAP-directory in. Voor de serverhost kunt u de FQDN of het IP-adres specificeren. Bijvoorbeeld **`myLDAPserver.example.com`** of **`100.00.00.0`**. Als u een cluster servers achter een load-balancer hebt, voert u in plaats daarvan de informatie van de load-balancer in.
LDAP-configuratie	Specificeer de zoekfilters en kenmerken van LDAP die VMware Identity Manager kan gebruiken om uw LDAP-directory op te vragen. Standaardwaarden worden verstrekt op basis van het kern-LDAP-schema. **LDAP-vragen** ■ **Groepen ophalen**: het zoekfilter om groepsobjecten te verkrijgen. Bijvoorbeeld: **`(objectClass=group)`** ■ **Bindingsgebruiker ophalen**: het zoekfilter om een bindingsgebruikerobject te verkrijgen, ofwel de gebruiker die zich aan de directory kan binden. Bijvoorbeeld: **`(objectClass=person)`** ■ **Gebruiker ophalen**: het zoekfilter om gebruikers te verkrijgen om te synchroniseren. Bijvoorbeeld: **`(&(objectClass=user)(objectCategory=person))`** **Kenmerken** ■ **Lidmaatschap**: het kenmerk dat wordt gebruikt in uw LDAP-directory om leden van een groep te definiëren. Bijvoorbeeld: **`lid`** ■ **Object-UUID**: het kenmerk dat wordt gebruikt in uw LDAP-directory om de UUID van een gebruiker of groep te definiëren. Bijvoorbeeld: **`entryUUID`**

Optie	Beschrijving
	■ **Distinguished Name**: het kenmerk dat wordt gebruikt in uw LDAP-directory voor de kenmerkende naam van een gebruiker of groep. Bijvoorbeeld: **`entryDN`**
Certificaten	Als uw LDAP-directory toegang over SSL vereist, selecteert u **Deze directory vereist dat alle verbindingen SSL gebruiken** en kopieert en plakt u het basis CA-SSL-certificaat van de LDAP-directoryserver. Zorg ervoor dat het certificaat in PEM-formaat is en neem de regels "BEGIN CERTIFICATE" en "END CERTIFICATE" op.
Gegevens van bindingsgebruiker	**Basis DN**: voer de DN in vanwaar zoekopdrachten worden gestart. Bijvoorbeeld cn=users,dc=example,dc=com **Bind DN**: voer de gebruikersnaam in die wordt gebruikt om aan de LDAP-directory te binden. **Opmerking** Het gebruik van een gebruikersaccount van Bind DN met een wachtwoord dat niet verloopt, wordt aanbevolen. **Wachtwoord Bind-DN**: voer het wachtwoord in voor de Bind DN-gebruiker.

b Klik op **Verbinding testen** om de verbinding met de LDAP-directoryserver te testen.

Als de verbinding niet is gelukt, controleert u de informatie die u hebt ingevoerd en brengt u passende wijzigingen aan.

c Klik op **Opslaan en Volgende**.

De pagina die het domein vermeldt, verschijnt.

15 Voor een LDAP-directory wordt het domein vermeld. Dit kan niet worden aangepast.

Voor een Active Directory via LDAP worden de domeinen vermeld en kunnen deze niet worden aangepast.

Voor Active Directory (met geïntegreerde Windows-verificatie) selecteert u de domeinen die moeten worden gekoppeld aan deze Active Directory-verbinding.

Opmerking Als u een vertrouwend domein toevoegt nadat de directory is gemaakt, stelt de service niet automatisch het nieuwe vertrouwende domein vast. Als u het vaststellen van het domein voor de service wilt inschakelen, moet Connector het domein verlaten en hieraan opnieuw deelnemen. Wanneer Connector opnieuw deelneemt aan het domein, wordt het vertrouwende domein in de lijst weergegeven.

Klik op **Volgende**.

16 Controleer of de kenmerknamen van VMware Identity Manager zijn toegewezen aan de juiste kenmerken van Active Directory of LDAP en breng zo nodig wijzigingen aan.

Belangrijk Als u een LDAP-directory integreert, moet u een toewijzing voor het **domeinkenmerk** specificeren.

17 Klik op **Volgende**.

18 Selecteer de groepen die u vanaf uw Active Directory of LDAP-directory wilt synchroniseren naar de VMware Identity Manager-directory.

Optie	Beschrijving
Geef de DN's van de groep op	Als u groepen wilt selecteren, kunt u een of meer groeps-DN's opgeven en de onderliggende groepen selecteren. a Klik op **+** en geef de groeps-DN op. Bijvoorbeeld CN=gebruikers,DC=voorbeeld,DC=bedrijf,DC=com. **Belangrijk** Geef de groeps-DN's op onder de basis-DN die u hebt ingevoerd. Als een groeps-DN buiten de basis-DN ligt, worden gebruikers van die DN gesynchroniseerd, maar kunnen zij zich niet aanmelden. b Klik op **Groepen zoeken**. De kolom **Te synchroniseren groepen** bevat het aantal groepen dat is gevonden in de DN. c Als u alle groepen in de DN wilt selecteren, klikt u op **Alles selecteren**. Of klik op **Selecteren** en selecteer de specifieke groepen die u wilt synchroniseren. **Opmerking** Wanneer uw LDAP-directory meerdere groepen met dezelfde naam bevat, moet u voor deze groepen unieke namen opgeven in de VMware Identity Manager-service. U kunt de naam wijzigen wanneer u de groep selecteert. **Opmerking** Wanneer u een groep synchroniseert, worden gebruikers die geen Domeingebruikers als hun primaire groep in Active Directory hebben, niet gesynchroniseerd.
Geneste groepsleden synchroniseren	De optie **Geneste groepsleden synchroniseren** is standaard ingeschakeld. Wanneer deze optie is ingeschakeld, worden alle gebruikers gesynchroniseerd die direct tot de groep behoren die u selecteert en alle gebruikers die tot de geneste groepen eronder behoren. Let op dat de geneste groepen niet worden gesynchroniseerd; alleen de gebruikers die tot de geneste groepen behoren, worden gesynchroniseerd. In de VMware Identity Manager-directory zijn deze gebruikers leden van de bovenliggende groep die u hebt geselecteerd om te synchroniseren. Als de optie **Geneste groepsleden synchroniseren** is uitgeschakeld, wanneer u een groep opgeeft om te synchroniseren, worden alle gebruikers gesynchroniseerd die tot die groep behoren. Gebruikers die tot geneste groepen eronder behoren, worden niet gesynchroniseerd. Het uitschakelen van deze functie is handig voor grote Active Directory-configuraties waarbij het doorkruisen van een groepsstructuur veel tijd en middelen kost. Als u deze optie uitschakelt, zorgt u ervoor dat u alle groepen selecteert waarvan u de gebruikers wilt synchroniseren.

19 Klik op **Volgende**.

20 Geef zo nodig extra gebruikers op om te synchroniseren.

a Klik op **+** en voer de gebruikers-DN's in. Bijvoorbeeld: CN=gebruikers,CN=Gebruikers,OU=mijnAfdeling,DC=mijnOnderneming,DC=com.

Belangrijk Geef de gebruikers-DN's op onder de basis-DN die u hebt ingevoerd. Als een gebruikers-DN buiten de basis-DN ligt, worden gebruikers van die DN gesynchroniseerd, maar kunnen zij zich niet aanmelden.

b (Optioneel) Als u gebruikers wilt uitsluiten, maakt u een filter om sommige gebruikerstypen uit te sluiten.

U selecteert het gebruikerskenmerk waarop moet worden gefilterd, de queryregel en de waarde.

21 Klik op **Volgende**.

22 Neem de pagina door om te zien hoeveel gebruikers en groepen naar de directory worden gesynchroniseerd en om het synchronisatieschema te bekijken.

   Klik op de koppelingen **Bewerken** om wijzigingen aan te brengen aan gebruikers en groepen of aan de synchronisatiefrequentie.

23 Klik op **Directory synchroniseren** om de synchronisatie van de directory te starten.

Opmerking Als zich een netwerkfout voordoet en de hostnaam kan niet uniek worden opgelost met behulp van reverse DNS, dan stopt het configuratieproces. U moet de netwerkproblemen verhelpen en de virtual appliance opnieuw opstarten. Vervolgens kunt u doorgaan met het implementatieproces. De nieuwe netwerkinstellingen zijn niet beschikbaar totdat u de virtual appliance opnieuw hebt opgestart.

Wat nu te doen

Voor informatie over het instellen van een load-balancer of een configuratie met hoge beschikbaarheid, raadpleegt u Hoofdstuk 6, “Geavanceerde configuratie voor het VMware Identity Manager-apparaat,” op pagina 77.

U kunt de catalogus met bronnen aanpassen voor de applicaties van uw organisatie en gebruikerstoegang inschakelen tot deze bronnen. U kunt ook andere bronnen instellen, waaronder View, ThinApp en op Citrix gebaseerde applicaties. Zie *Bronnen instellen in VMware Identity Manager*

Proxyserverinstellingen instellen voor VMware Identity Manager

De VMware Identity Manager virtual appliance heeft toegang tot de applicatiescatalogus in de cloud en andere webservices op internet. Als uw netwerkconfiguratie internettoegang biedt via een HTTP-proxy, moet u uw proxy-instellingen aanpassen in de VMware Identity Manager-apparaat.

Schakel uw proxy in om alleen internetverkeer te verwerken. Als u er zeker van wilt zijn dat de proxy goed is ingesteld, moet u de parameter voor intern verkeer binnen het domein instellen op `no-proxy`.

Opmerking Proxyservers waarvoor verificatie is vereist, worden niet ondersteund.

Procedure

1 Meld u via de vSphere Client aan als hoofdgebruiker bij de VMware Identity Manager virtual appliance.

2 Voer `YaST` in op de opdrachtregel om het hulpprogramma `YaST` uit te voeren.

3 Selecteer **Netwerkservices** in het linkerdeelvenster en selecteer **Proxy**.

4 Voer in de velden **URL HTTP-proxy** en **URL HTTPS-proxy** de URL's van de proxyserver in.

5 Selecteer **Voltooien** en sluit het hulpprogramma `YaST` af.

6 Herstart de Tomcat-server op de VMware Identity Manager virtual appliance om de nieuwe proxy-instellingen te gebruiken.

```
service horizon-workspace restart
```

De catalogus met cloudapplicaties en andere webservices is nu beschikbaar in VMware Identity Manager.

De licentiecode invoeren

Nadat u het VMware Identity Manager-apparaat hebt geïmplementeerd, voert u uw licentiecode in.

Procedure

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

2 Selecteer het tabblad **Appliance-instellingen** en klik vervolgens op **Licentie**.

3 Op de pagina Licentie-instellingen voert u de licentiecode in en klikt u op **Opslaan**.

Configuratie-instellingen voor systeemapplicaties beheren 3

Nadat de eerste configuratie van de applicatie is voltooid, kunt u naar de pagina's voor apparaatbeheer gaan om certificaten te installeren, wachtwoorden te beheren en systeeminformatie van de virtual appliance te bewaken.

U kunt tevens de database, FQDN en het systeemlogboek bijwerken, en logboekbestanden downloaden.

Naam van pagina	Beschrijving van instelling
Databaseverbinding	De instelling voor de databaseverbinding, intern of extern, is ingeschakeld. U kunt het type database wijzigen. Wanneer u Externe database selecteert, kunt u de URL van de externe database, de gebruikersnaam en het wachtwoord invoeren. Als u een externe database wilt instellen, raadpleegt u "Aan de database koppelen," op pagina 34.
Certificaat installeren	Op deze pagina installeert u een aangepast of zelf-ondertekend certificaat voor VMware Identity Manager en als VMware Identity Manager is geconfigureerd met een load-balancer, kunt u het basiscertificaat van de load-balancer installeren. De locatie van het CA-basiscertificaat van de VMware Identity Manager wordt ook op deze pagina weergegeven, op het tabblad **SSL beëindigen op een load-balancer**. Zie "SSL-certificaten gebruiken," op pagina 38.
Identity Manager FQDN	De VMware Identity Manager FQDN wordt weergegeven op deze pagina. U kunt deze wijzigen. VMware Identity Manager FQDN is de URL waarmee gebruikers toegang kunnen krijgen tot de service.
Syslog configureren	Op deze pagina kunt u een externe syslog-server inschakelen. Logboeken van VMware Identity Manager worden naar deze externe server verzonden. Zie "De Syslog-server inschakelen," op pagina 41.
Wachtwoord wijzigen	Op deze pagina kunt u het beheerderswachtwoord van de VMware Identity Manager wijzigen.
Systeembeveiliging	Op deze pagina kunt u het hoofdwachtwoord voor het VMware Identity Manager-apparaat en het ssh-wachtwoord dat u gebruikt om u op afstand aan te melden, wijzigen.
Locaties van logboekbestanden	Er wordt een lijst met logboekbestanden en de locaties van hun directory's op deze pagina weergegeven. U kunt de logboekbestanden bundelen in een zip-bestand om te downloaden. Zie "Logboekbestandsgegevens," op pagina 42.

U kunt ook de connector-URL wijzigen. Zie "De connector-URL aanpassen," op pagina 41.

Dit hoofdstuk omvat de volgende onderwerpen:

Configuratie-instellingen voor het apparaat wijzigen

Nadat u VMware Identity Manager hebt geconfigureerd, kunt u naar de pagina's met Appliance-instellingen gaan om de huidige configuratie bij te werken en systeeminformatie van de virtual appliance te bewaken.

Procedure

1 Meld u aan op de beheerconsole.

2 Selecteer het tabblad **Apparaatinstellingen** en klik op **Configuratie beheren**.

3 Meld u aan met het wachtwoord voor de servicebeheerder.

4 Selecteer in het linkerdeelvenster de pagina die u wilt bekijken of bewerken.

Wat nu te doen

Controleer of de instellingen of updates die u doorvoert, van kracht zijn.

Aan de database koppelen

Een interne PostgreSQL-database is in de VMware Identity Manager-appliance ingebouwd, maar het is niet raadzaam om deze te gebruiken bij productie-implementaties. Om een externe database met VMware Identity Manager te gebruiken, moet uw databasebeheerder een lege database en een schema voorbereiden voordat de database kan worden gekoppeld aan de database in VMware Identity Manager.

U kunt een koppeling tot stand brengen met de externe databaseverbinding wanneer u de VMware Identity Manager-installatiewizard uitvoert. U kunt ook naar de pagina Apparaatinstellingen > VA-configuratie > Installatie databaseverbinding gaan om de verbinding met de externe database te configureren.

Licentiegebruikers kunnen een externe Oracle-database of Microsoft SQL Server gebruiken om een databaseomgeving met hoge beschikbaarheid in te stellen.

Een Microsoft SQL-database configureren

Om een Microsoft SQL-database voor de VMware Identity Manager te gebruiken, moet u een nieuwe database in de Microsoft SQL-server maken.

Maak een database met de naam **saas** op de Microsoft SQL-server en maak een gebruikers-login genaamd **horizon**.

Opmerking De standaard sortering is hoofdlettergevoelig.

Vereisten

- Ondersteunde versie van de Microsoft SQL-server is geïnstalleerd als een externe databaseserver.
- Implementatie van load-balancer is geconfigureerd.
- Beheerdersrechten om databasecomponenten te openen en te maken met behulp van Microsoft SQL Server Management Studio of van een andere Microsoft SQL Server CLI client.

Procedure

1 Meld u aan op de sessie van Microsoft SQL Server Management Studio als de systeembeheerder van een gebruikersaccount met rechten van een systeembeheerder.

Het editorvenster verschijnt.

2 Klik in de werkbalk op **Nieuwe zoekopdracht**.

3 Knip en plak de volgende opdrachten in het editorvenster.

Microsoft SQL-opdrachten

```
CREATE DATABASE saas
COLLATE Latin1_General_CS_AS;
ALTER DATABASE saas SET READ_COMMITTED_SNAPSHOT ON;
GO
BEGIN
CREATE LOGIN horizon WITH PASSWORD = N'H0rizon!';
END
GO
USE saas;
IF EXISTS (SELECT * FROM sys.database_principals WHERE name = N'horizon')
DROP USER [horizon]
GO
CREATE USER horizon FOR LOGIN horizon
WITH DEFAULT_SCHEMA = saas;
GO
CREATE SCHEMA saas AUTHORIZATION horizon
GRANT ALL ON DATABASE::saas TO horizon;
GO
```

4 Klik op de werkbalk op **Uitvoeren**.

De databaseserver van Microsoft SQL is nu klaar om te worden aangesloten op de database van de VMware Identity Manager.

Wat nu te doen

Configureer de externe database op de server van de VMware Identity Manager. Ga op de beheerconsole van de VMware Identity Manager naar de pagina Appliance-instellingen > VA-configuratie > Installatiepagina van databaseverbinding. Voer de JDBC URL in als **`jdbc:sqlserver://<hostnaam-of-DB_VM_IP_ADDR>;DatabaseName=saas`**. Voer de gebruikersnaam en het wachtwoord in die voor de database zijn aangemaakt. Zie "VMware Identity Manager configureren om een externe database te gebruiken," op pagina 37.

Een Oracle-database configureren

Tijdens de installatie van de Oracle-database moet u bepaalde Oracle-configuraties specificeren voor de optimale prestaties met VMware Identity Manager.

Vereisten

De Oracle-database die u maakt, wordt `saas` genoemd. VMware Identity Manager vereist door Oracle geciteerde identificaties voor de gebruikersnaam en het schema. Daarom moet u dubbele aanhalingstekens gebruiken wanneer u de gebruikersnaam en het schema van `saas` van Oracle maakt.

Procedure

1 Specificeer de volgende instellingen wanneer u een Oracle-database maakt.

   a Selecteer de configuratieoptie **General Purpose/Transaction Processing Database**.

   b Klik op **Unicode gebruiken > UTF8**.

   c Gebruik de nationale tekenset.

2 Maak verbinding met de Oracle-database nadat de installatie is voltooid.

3 Meld u aan op de Oracle-database als de systeemgebruiker.

4 Verhoog de procesverbindingen. Elke extra virtuele machine van de service vereist minimaal 300 procesverbindingen om met VMware Identity Manager te werken. Als bijvoorbeeld uw omgeving twee virtuele machines van de service heeft, voert u de opdracht `alter` uit als sys of systeemgebruiker.

   a Verhoog de procesverbindingen met behulp van de opdracht `alter`.

   ```
   alter system set processes=600 scope=spfile
   ```

   b Start de database opnieuw op.

5 Maak een database-trigger die alle gebruikers kunnen gebruiken.

Voorbeeld van SQL om een database-trigger te maken

```
CREATE OR REPLACE
TRIGGER CASE_INSENSITIVE_ONLOGON
AFTER LOGON ON DATABASE
DECLARE
username VARCHAR2(30);
BEGIN
username:=SYS_CONTEXT('USERENV','SESSION_USER');
IF username = 'saas' THEN
execute immediate 'alter session set NLS_SORT=BINARY_CI';
execute immediate 'alter session set NLS_COMP=LINGUISTIC';
END IF;
EXCEPTION
WHEN OTHERS THEN
NULL;
END;
```

6 Voer de Oracle-opdrachten uit om een nieuw gebruikersschema te maken.

Voorbeeld van SQL om een nieuwe gebruiker te maken

```
CREATE USER "saas"
IDENTIFIED BY <password>
DEFAULT TABLESPACE USERS
TEMPORARY TABLESPACE TEMP
PROFILE DEFAULT
ACCOUNT UNLOCK;
GRANT RESOURCE TO "saas" ;
GRANT CONNECT TO "saas" ;
ALTER USER "saas" DEFAULT ROLE ALL;
GRANT UNLIMITED TABLESPACE TO "saas";
```

De interne database beheren

Standaard is de interne PostgreSQL-database geconfigureerd en klaar voor gebruik. Het gebruik van de interne database wordt afgeraden bij productie-implementaties.

Wanneer de VMware Identity Manager is geïnstalleerd en geactiveerd, wordt tijdens het initialisatieproces een willekeurig wachtwoord voor de gebruiker van de interne database gegenereerd. Dit wachtwoord is uniek voor elke implementatie en staat in het bestand `/usr/local/horizon/conf/db.pwd`.

Zie KB 2094258 om uw interne database voor een hoge zichtbaarheid te configureren.

VMware Identity Manager configureren om een externe database te gebruiken

Nadat u de database hebt ingesteld in de wizard Setup van VMware Identity Manager, kunt u VMware Identity Manager configureren om een andere database te gebruiken.

U moet VMware Identity Manager richten op een begonnen, ingevulde database. U kunt bijvoorbeeld een database gebruiken die is geconfigureerd als gevolg van een succesvolle uitvoering van de VMware Identity Manager-wizard Setup, een database van een back-up of een database van een herstelde momentopname.

Vereisten

- Installeer en configureer de ondersteunde Microsoft SQL- of Oracle-editie als externe databaseserver. Voor informatie over specifieke versies die worden ondersteund door VMware Identity Manager, raadpleegt u de VMware-productinteroperabiliteitsmatrices op http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Procedure

1 In de beheerconsole klikt u op **Appliance-instellingen** en selecteert u **VA-configuratie**.

2 Klik op **Configuratie beheren**.

3 Meld u aan met het beheerderswachtwoord van VMware Identity Manager.

4 Op de Setuppagina van de databaseverbinding selecteert u **Externe database** als het databasetype.

5 Voer informatie in over de databaseverbinding.

   a Typ de JDBC-URL van de databaseserver.

Microsoft SQL	`jdbc:sqlserver://hostnaam_of_IP_adres;DatabaseName=horizon`
Oracle	`jdbc:oracle:thin:@//hostnaam_of_IP_adres:poort/sid`

   b Typ de naam van de gebruiker met lees- en schrijfrechten op de database.

Microsoft SQL	`horizon`
Oracle	`"saas"`

   c Typ het wachtwoord voor de gebruiker die u hebt gemaakt toen u de database hebt geconfigureerd.

6 Klik op **Verbinding testen** om de informatie te controleren en op te slaan.

SSL-certificaten gebruiken

Wanneer het VMware Identity Manager-apparaat is geïnstalleerd, wordt automatisch een standaard SSL-servercertificaat gegenereerd. U kunt dit zelf-ondertekende certificaat gebruiken voor algemene tests van uw implementatie. VMware raadt u ten zeerste aan zakelijke SSL-certificaten te genereren en te installeren in uw productie-omgeving.

Een certificaat van autoriteit (CA) is een vertrouwde entiteit die de identiteit van het certificaat en de maker garandeert. Wanneer een certificaat is ondertekend door een vertrouwde CA, ontvangen gebruikers geen berichten meer waarin ze worden gevraagd het certificaat te controleren.

Als u VMware Identity Manager implementeert met het zelf ondertekende SSL-certificaat, moet het CA-basiscertificaat beschikbaar zijn als vertrouwde CA voor alle clients die toegang hebben tot VMware Identity Manager. De clients kunnen machines van eindgebruikers, load-balancers, proxy's, enzovoort zijn. U kunt de basis-CA downloaden van *https://myconnector.domain.com/horizon_workspace_rootca.pem*.

U kunt een ondertekend CA-certificaat installeren vanaf de pagina **Appliance-instellingen > Configuratie beheren > Certificaat installeren**. U kunt ook het CA-basiscertificaat van de load-balancer aan deze pagina toevoegen.

Openbare certificaatautoriteit toepassen

Wanneer de VMware Identity Manager-service is geïnstalleerd, wordt een standaard SSL-servercertificaat gegenereerd. U kunt dit standaardcertificaat gebruiken voor testdoeleinden. U dient vervolgens voor uw omgeving commerciële SSL-certificaten te genereren en installeren.

Opmerking Als de VMware Identity Manager naar een load-balancer verwijst, wordt het SSL-certificaat toegepast op de load-balancer.

Vereisten

Genereer een aanvraag voor certificaatondertekening om een geldig, ondertekend certificaat van een certificeringsinstantie te verkrijgen. Als uw organisatie SSL-certificaten heeft die zijn ondertekend door een certificeringsinstantie, kunt u deze certificaten gebruiken. Het certificaat moet de indeling PEM hebben.

Procedure

1 Klik in de beheerconsole op **Toepassingsinstellingen**.

De configuratie van de virtuele toepassing wordt standaard geselecteerd.

2 Klik op **Configuratie beheren**.

3 In het dialoogvenster dat verschijnt, voert u het beheerdersgebruikerswachtwoord voor de server van VMware Identity Manager in.

4 Selecteer **Certificaat installeren**.

5 Selecteer **Aangepast Certificaat** op het tabblad SSL beëindigen op Identity Manager-toepassing.

6 Plak in het tekstvak **SSL-certificaatketen** het host-, tussen- en basiscertificaat, in die volgorde.

Het SSL-certificaat werkt alleen als u de hele certificaatketen in de juiste volgorde invoert. Kopieer voor elk certificaat de volledige inhoud vanaf de regel -----BEGIN CERTIFICATE----- tot en met -----END CERTIFICATE----

Zorg ervoor dat de FQDN van de host in het certificaat is opgenomen.

7 Plak de privésleutel in het tekstvak Privésleutel. Kopieer alle inhoud vanaf ----BEGIN RSA PRIVATE KEY tot en met ---END RSA PRIVATE KEY.

8 Klik op **Opslaan.**

Voorbeeld: Voorbeelden van certificaten

Voorbeeld van certificaatketen
-----BEGIN CERTIFICATE-----
jlQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+ ... ... W53+O05j5xsxzDJfWr1lqBlFF/OkIYCPcyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
WdR9Vpg3WQT5+C3HU17bUOwvhp/rjlQvt90+ ... ... O05j5xsxzDJfWr1lqBlFF/OkIYCPW53+cyK1

Voorbeeld van certificaatketen
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
dR9Vpg3WQTjlQvt9W5+C3HU17bUOwvhp/r0+ ... ... 5j5xsxzDJfWr1lqW53+O0BlFF/OkIYCPcyK1
-----END CERTIFICATE-----

Voorbeeld van privésleutel
-----BEGIN RSA PRIVATE KEY-----
jlQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+ ... ... 1lqBlFFW53+O05j5xsxzDJfWr/OkIYCPcyK1
-----END RSA PRIVATE KEY-----

SSL-certificaten toevoegen

Wanneer u het certificaat toepast, zorg dan dat u de gehele certificaatketen invoert. Het certificaat dat wordt geïnstalleerd, moet de indeling PEM hebben.

Het SSL-certificaat werkt alleen als u de hele certificaatketen invoert. Kopieer voor elk certificaat de volledige inhoud vanaf de regel -----BEGIN CERTIFICATE----- tot en met -----END CERTIFICATE----

Belangrijk U moet de certificaatketen toevoegen in de volgorde SSL-certificaat, CA-tussencertificaten, CA-basiscertificaat.

Voorbeeld van certificaatketen
-----BEGIN CERTIFICATE-----
SSL-certificaat - SSL-certificaat van apparaat
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA-tussen-/uitgiftecertificaat
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA-basiscertificaat
-----END CERTIFICATE-----

De URL van de VMware Identity Manager-service wijzigen

U kunt de URL van de VMware Identity Manager-service wijzigen. Dit is de URL die gebruikers gebruiken om toegang te krijgen tot de service. U kunt bijvoorbeeld de URL wijzigen in een URL voor een load-balancer.

Procedure

1 Meld u aan bij de VMware Identity Manager-beheerconsole.

2 Klik op het tabblad **Appliance-instellingen** en selecteer vervolgens **VA-configuratie**.

3 Klik op **Configuratie beheren** en meld u aan met het wachtwoord van de **`beheerdersgebruiker`**.

4 Klik op **Identity Manager FQDN** en geef de nieuwe URL op in het veld **Identity Manager FQDN**.

   Gebruik de indeling **`https://FQDN:poort`**. Een poort specificeren is optioneel. De standaardpoort is 443.

   Bijvoorbeeld: **`https://myservice.example.com`**.

5 Klik op **Opslaan**.

Wat nu te doen

Schakel de gebruikersinterface van de nieuwe portal in.

1 Ga naar https://*VMwareIdentityManagerURL*/admin om de beheerconsole te openen.

2 Klik in de beheerconsole op de pijl op het tabblad **Catalogus** en selecteer **Instellingen**.

3 Selecteer **Nieuwe eindgebruikersinterface van portal** in het linkerdeelvenster en klik op **Nieuwe gebruikersinterface van portal inschakelen**.

De connector-URL aanpassen

U kunt de connector-URL aanpassen door de hostnaam van de identiteitsprovider bij te werken in de beheerconsole. Als u de connector als identiteitsprovider gebruikt, is de connector-URL de URL van de aanmeldingspagina en is deze zichtbaar voor eindgebruikers.

Procedure

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

2 Klik op het tabblad **Identiteits- en toegangsbeheer** en klik vervolgens op het tabblad **Identiteitsproviders**.

3 Op de pagina Identiteitsproviders selecteert u de identiteitsprovider die u wilt bijwerken.

4 In het veld **IdP-hostnaam** voert u de nieuwe hostnaam in.

   Gebruik de notatie **`hostnaam:poort`**. Een poort specificeren is optioneel. De standaardpoort is 443.

   Bijvoorbeeld **`vidm.example.com`**.

5 Klik op **Opslaan**.

De Syslog-server inschakelen

Gebeurtenissen van de service op applicatiesniveau kunnen worden geëxporteerd naar een externe Syslog-server. Gebeurtenissen van besturingssystemen worden niet geëxporteerd.

Aangezien de meeste bedrijven niet over onbeperkte schijfruimte beschikken, slaat de virtual appliance niet de volledige logboekgeschiedenis op. Als u meer geschiedenis wilt opslaan of als u een centrale locatie voor uw logboekgeschiedenis wilt maken, kunt u een externe Syslog-server instellen.

Als u tijdens de eerste configuratie geen Syslog-server opgeeft, kunt u deze later configureren via de pagina **Apparaatinstellingen > VA-configuratie > Configuratie beheren > Configuratie systeemlogboek**.

Vereisten

Stel een externe Syslog-server in. U kunt een van de beschikbare standaardsyslogservers gebruiken. Verschillende Syslog-servers beschikken over geavanceerde zoekmogelijkheden.

Procedure

1 Meld u aan op de beheerconsole.

2 Klik op de tab **Apparaatinstellingen**, selecteer **VA-configuratie** in het linkerdeelvenster en klik op **Configuratie beheren**.

3 Selecteer **Systeemlogboek configureren** in het linkerdeelvenster.

4 Klik op **Inschakelen**.

5 Geef het IP-adres of de FQDN van de systeemlogboekserver op waarop u de logboeken wilt opslaan.

6 Klik op **Opslaan.**

Er wordt een kopie van uw logboeken naar de Syslog-server verzonden.

Logboekbestandsgegevens

De VMware Identity Manager -logboekbestanden kunnen u helpen bij het oplossen van bugs en problemen. De onderstaande logboekbestanden zijn een algemeen startpunt. U kunt aanvullende logboeken vinden in de directory `/opt/vmware/horizon/workspace/logs`.

Tabel 3-1. Logboekbestanden

Onderdeel	Locatie van logboekbestand	Beschrijving
Identity Manager Service-logboeken	`/opt/vmware/horizon/workspace/logs/horizon.log`	Informatie over activiteiten binnen de VMware Identity Manager-applicatie, zoals rechten, gebruikers en groepen.
Configuratielogboekbestanden	`/opt/vmware/horizon/workspace/logs/configurator.log`	Aanvragen die de configurator van de REST-client en de webinterface ontvangt.
Connectorlogboekbestanden	`/opt/vmware/horizon/workspace/logs/connector.log`	Een record van elke ontvangen aanvraag van de webinterface. Elke logboekvermelding bevat tevens de verzoek-URL, het tijdstempel en de uitzonderingen. Er worden geen synchronisatie-acties geregistreerd.
Updatelogboeken	`/opt/vmware/var/log/update.log` `/opt/vmware/var/log/vami`	Een record van uitgaande berichten met betrekking tot updateverzoeken tijdens een upgrade van VMware Identity Manager. De bestanden in de directory `/opt/vmware/var/log/vami` zijn handig voor het oplossen van problemen. U kunt deze bestanden na een upgrade op alle virtual machines vinden.
Apache Tomcat-logboeken	`/opt/vmware/horizon/workspace/logs/catalina.log`	Apache Tomcat-registraties van berichten die niet in andere logboekbestanden zijn geregistreerd.

Logboekgegevens verzamelen

Tijdens testen of problemen oplossen kunnen de logboeken feedback geven over de activiteiten en prestaties van de virtual appliance en ook informatie geven over problemen die zich voordoen.

U verzamelt de logboeken van elk apparaat dat zich in uw omgeving bevindt.

Procedure

1 Meld u aan op de beheerconsole.

2 Selecteer het tabblad **Apparaatinstellingen** en klik op **Configuratie beheren**.

3 Klik op **Bestandslocaties vastleggen** en klik op **Logboekbundel voorbereiden**.

De informatie wordt verzameld op een tar.gz-bestand dat u kunt downloaden.

4 Download de voorbereide bundel.

Wat nu te doen

Doe dit voor elk apparaat om alle logboeken te verzamelen.

De wachtwoorden van uw apparaat beheren

Wanneer u de virtual appliance hebt geconfigureerd, hebt u wachtwoorden gemaakt voor de beheerdersgebruiker, de hoofdgebruiker, en de ssh-gebruiker. U kunt deze wachtwoorden wijzigen via de pagina's met Appliance-instellingen.

Zorg dat u sterke wachtwoorden maakt. 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.

Procedure

1 Klik in de beheerconsole op het tabblad **Appliance-instellingen**.

2 Klik op **VA-configuratie > Configuratie beheren**.

3 Als u het beheerderswachtwoord wilt wijzigen, selecteert u **Wachtwoord wijzigen**. Als u de hoofd- of ssh-gebruikerswachtwoorden wijzigt, selecteert u **Systeembeveiliging**.

Belangrijk Het wachtwoord voor de beheerdersgebruiker moet minstens zes tekens lang zijn.

4 Geef het nieuwe wachtwoord op.

5 Klik op **Opslaan**.

SMTP-instellingen configureren

Configureer SMTP-serverinstellingen om e-mailmeldingen te ontvangen van de service VMware Identity Manager.

E-mailmeldingen worden verzonden naar nieuwe gebruikers die zijn gemaakt als lokale gebruikers en wanneer een wachtwoord opnieuw wordt ingesteld in de VMware Identity Manager-service.

Procedure

1 Meld u aan op de beheerconsole.

2 Selecteer het tabblad **Appliance-instellingen** en klik op **SMTP**.

3 Voer de hostnaam van de SMTP-server in.

Bijvoorbeeld: `smtp.example.com`.

4 Voer het poortnummer van de SMTP-server in.

Bijvoorbeeld: `25`.

5 (Optioneel) Voer een gebruikersnaam en wachtwoord in als de SMTP-server verificatie vereist.

6 Klik op **Opslaan**.

Integreren met uw Enterprise-directory

4

U kunt VMware Identity Manager integreren met uw Enterprise directory om gebruikers en groepen van uw Enterprise directory te synchroniseren met de VMware Identity Manager-service.

De volgende typen directory's worden ondersteund.

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

Voer de volgende taken uit om te integreren met uw Enterprise directory.

- Specificeer de kenmerken voor de gebruikers in de VMware Identity Manager-service.
- Maak een map aan in de VMware Identity Manager-service en gebruik daarvoor hetzelfde type map dat uw Enterprise directory heeft en specificeer de informatie over de verbinding.
- Wijs de VMware Identity Manager-kenmerken toe aan de kenmerken die worden gebruikt in uw Active Directory of in de LDAP-directory.
- Specificeer de gebruikers en groepen die u wilt synchroniseren.
- Synchroniseer gebruikers en groepen.

Wanneer u uw Enterprise directory hebt geïntegreerd en de eerste synchronisatie hebt uitgevoerd, kunt u de configuratie bijwerken, een synchronisatieschema instellen om regelmatig te synchroniseren, of op een willekeurig moment een synchronisatie starten.

Dit hoofdstuk omvat de volgende onderwerpen:

Belangrijke concepten met betrekking tot de integratie van directory's

Bepaalde concepten maken integraal deel uit van begrijpen hoe de VMware Identity Manager-service kan worden geïntegreerd in de omgeving van uw Active Directory of LDAP-directory.

Connector

De Connector, een onderdeel van de service, voert de volgende functies uit.

- De gebruikers- en groepsgegevens van uw Active Directory of LDAP-directory worden met de service gesynchroniseerd.
- Als deze wordt gebruikt als een identiteitsprovider, verifieert deze gebruikers naar de service.

  De Connector is de standaardidentiteitsprovider. U kunt ook identiteitsproviders van derden gebruiken die het SAML 2.0-protocol ondersteunen. Gebruik een externe identiteitsprovider voor een verificatietype dat niet door de Connector wordt ondersteund of als de externe identiteitsprovider de voorkeur heeft op basis van het beveiligingsbeleid van uw bedrijf.

  Opmerking Als u identiteitsproviders van derden gebruikt, kunt u de Connector configureren om gegevens van gebruikers en groepen te synchroniseren of u kunt Just-in-Time-gebruikers-provisioning configureren. Raadpleeg het gedeelte Just-in-Time-gebruikers-provisioning in *VMware Identity Manager-beheer* voor meer informatie.

Directory

De VMware Identity Manager-service heeft een eigen concept van een directory, die overeenkomt met de Active Directory of LDAP-directory in uw omgeving. Deze directory maakt gebruik van kenmerken om gebruikers en groepen te definiëren. U maakt één of meer directory's in de service en vervolgens synchroniseert u deze directory's met uw Active Directory of LDAP-directory. U kunt de volgende directorytypen maken in de service.

- Active Directory
  - Active Directory via LDAP. Maak dit directorytype als u verbinding wilt maken met één Active Directory-domeinomgeving. Voor het directorytype Active Directory via LDAP verbindt de Connector met Active Directory met behulp van eenvoudige bindingsverificatie.
  - Active Directory, Geïntegreerde Windows-verificatie. Maak dit directorytype als u verbinding wilt maken met een Active Directory-omgeving met meerdere domeinen of meerdere forests. De Connector verbindt met Active Directory met behulp van Geïntegreerde Windows-verificatie.

  Het type en het aantal directory's dat u maakt, is afhankelijk van uw Active Directory-omgeving, zoals één domein of meerdere domeinen, en van het vertrouwenstype dat tussen de domeinen wordt gebruikt. In de meeste omgevingen maakt u één directory.
- LDAP-directory

De service heeft geen rechtstreekse toegang tot uw Active Directory of LDAP-directory. Alleen de Connector heeft rechtstreekse toegang. Daarom koppelt u elke directory die in de service is gemaakt, aan een Connector-instantie.

Werker

Als u een directory koppelt aan een Connector-instantie, maakt de Connector een partitie voor de gekoppelde directory, een werker genaamd. Aan een Connector-instantie kunnen meerdere werkers gekoppeld zijn. Elke werker fungeert als identiteitsprovider. U definieert en configureert verificatiemethoden per werker.

De Connector synchroniseert gegevens van gebruikers en groepen tussen uw Active Directory of LDAP-directory en de service via een of meer werkers.

Belangrijk U kunt niet twee werkers van de Active Directory van het type Geïntegreerde Windows-verificatie op dezelfde Connector-instantie hebben.

Beveiligingsoverwegingen

Voor bedrijfsdirectory's die zijn geïntegreerd met de VMware Identity Manager-service moeten beveiligingsinstellingen, zoals regels voor de complexiteit van gebruikerswachtwoorden en beleid voor accountvergrendeling, rechtstreeks worden geconfigureerd in bedrijfsdirectory. VMware Identity Manager overschrijft deze instellingen niet.

Met Active Directory integreren

U kunt VMware Identity Manager integreren met uw Active Directory-implementatie om gebruikers en groepen van Active Directory te synchroniseren met VMware Identity Manager.

Zie ook "Belangrijke concepten met betrekking tot de integratie van directory's," op pagina 46.

Active Directory-omgevingen

U kunt de service integreren met een Active Directory-omgeving die bestaat uit één Active Directory-domein, meerdere domeinen in één Active Directory-forest of meerdere domeinen in meerdere Active Directory-forests.

Omgeving met één Active Directory-domein

In een implementatie met één Active Directory-domein kunt u gebruikers en groepen van één Active Directory-domein synchroniseren.

Selecteer de optie Active Directory via LDAP wanneer u een directory aan de service toevoegt voor deze omgeving.

Voor meer informatie raadpleegt u:

- "Domeincontrollers selecteren (bestand domain_krb.properties)," op pagina 49
- "Gebruikerskenmerken beheren die vanuit Active Directory worden gesynchroniseerd," op pagina 53
- "Vereiste rechten voor het toevoegen aan een domein," op pagina 55
- "Verbinding van Active Directory met de service configureren," op pagina 55

Active Directory-omgeving met één forest en meerdere domeinen

In een Active Directory-implementatie met één forest en meerdere domeinen kunt u gebruikers en groepen van meerdere Active Directory-domeinen binnen één forest synchroniseren.

U kunt de service voor deze Active Directory-omgeving configureren als één Active Directory-directorytype met geïntegreerde Windows-verificatie of, als alternatieve optie, als het directorytype Active Directory via LDAP met de optie voor de globale catalogus geconfigureerd.

- De aanbevolen optie is om het enkele Active Directory-type met geïntegreerde Windows-verificatie te maken.

  Wanneer u een directory voor deze omgeving toevoegt, selecteert u de optie Active Directory (geïntegreerde Windows-verificatie).

  Voor meer informatie raadpleegt u:

  - "Domeincontrollers selecteren (bestand domain_krb.properties)," op pagina 49

- "Gebruikerskenmerken beheren die vanuit Active Directory worden gesynchroniseerd," op pagina 53
- "Vereiste rechten voor het toevoegen aan een domein," op pagina 55
- "Verbinding van Active Directory met de service configureren," op pagina 55

- Als Geïntegreerde Windows-verificatie niet werkt in uw Active Directory-omgeving, maakt u een directory van het type Active Directory via LDAP en selecteert u de optie globale catalogus.

  Hier volgen een aantal beperkingen in verband met het selecteren van de optie globale catalogus:

  - De Active Directory-objectkenmerken die worden gekopieerd naar de globale catalogus worden in het Active Directory-schema vermeld als gedeeltelijke kenmerkreeks (PAS). Alleen deze kenmerken zijn beschikbaar voor het toewijzen van kenmerken door de service. Indien nodig kunt u het schema bewerken of kenmerken die in de globale catalogus zijn opgeslagen, toevoegen of verwijderen.
  - In de globale catalogus wordt uitsluitend het groepslidmaatschap (het lidmaatschapskenmerk) van universele groepen opgeslagen. Er worden alleen universele groepen gesynchroniseerd met de service. Indien nodig wijzigt u het bereik van een groep van een lokaal of globaal domein naar een universeel domein.
  - Het account van de bindings-DN dat u opgeeft wanneer u een directory in de service configureert, moet over toestemmingen beschikken om het kenmerk Token-Groups-Global-And-Universal (TGGAU) te kunnen lezen.

  Active Directory gebruikt poorten 389 en 636 voor standaard LDAP-query's. Voor globale catalogusquery's worden poorten 3268 en 3269 gebruikt.

  Wanneer u een directory toevoegt voor de globale catalogusomgeving, geeft u het volgende op tijdens de configuratie.

  - Selecteer de optie Active Directory via LDAP.
  - Schakel het selectievakje voor de optie **Deze directory ondersteunt de locatie van de DNS-service**.
  - Selecteer de optie **Deze directory heeft een Global Catalog**. Wanneer u deze optie selecteert, wordt het serverpoortnummer automatisch gewijzigd in 3268. Omdat de basis-DN niet noodzakelijk is tijdens het configureren van de optie globale catalogus, wordt het tekstvak Basis-DN niet weergegeven.
  - Voeg de serverhostnaam van de Active Directory toe.
  - Als voor uw Active Directory toegang via SSL is vereist, selecteert u de optie **Voor deze map is vereist dat alle verbindingen SSL gebruiken** en plakt u het certificaat in het daarvoor bestemde tekstvak. Wanneer u deze optie selecteert, wordt het serverpoortnummer automatisch gewijzigd in 3269.

Active Directory-omgeving met meerdere forests met vertrouwensrelaties

In een Active Directory-implementatie met meerdere forests met vertrouwensrelaties kunt u gebruikers en groepen uit meerdere Active Directory-domeinen met meerdere forests synchroniseren als er een vertrouwensrelatie in twee richtingen bestaat tussen de domeinen.

Wanneer u een directory voor deze omgeving toevoegt, selecteert u de optie Active Directory (geïntegreerde Windows-verificatie).

Voor meer informatie raadpleegt u:

- "Domeincontrollers selecteren (bestand domain_krb.properties)," op pagina 49
- "Gebruikerskenmerken beheren die vanuit Active Directory worden gesynchroniseerd," op pagina 53
- "Vereiste rechten voor het toevoegen aan een domein," op pagina 55

- "Verbinding van Active Directory met de service configureren," op pagina 55

Active Directory-omgeving met meerdere forests zonder vertrouwensrelaties

In een Active Directory-implementatie met meerdere forests zonder vertrouwensrelaties kunt u gebruikers en groepen uit meerdere Active Directory-domeinen met meerdere forests synchroniseren zonder dat er een vertrouwensrelatie in twee richtingen bestaat tussen de domeinen. In deze omgeving kunt u meerdere directory's maken in de service: één directory voor elk forest.

Het type directory's dat u in de service maakt, is afhankelijk van het forest. Voor forests met meerdere domeinen selecteert u de optie Active Directory (geïntegreerde Windows-verificatie). Voor een forest met één domein kiest u de optie Active Directory via LDAP.

Voor meer informatie raadpleegt u:

- "Domeincontrollers selecteren (bestand domain_krb.properties)," op pagina 49
- "Gebruikerskenmerken beheren die vanuit Active Directory worden gesynchroniseerd," op pagina 53
- "Vereiste rechten voor het toevoegen aan een domein," op pagina 55
- "Verbinding van Active Directory met de service configureren," op pagina 55

Domeincontrollers selecteren (bestand domain_krb.properties)

Het bestand `domain_krb.properties` geeft aan welke domeincontrollers worden gebruikt voor directory's waarbij de DNS-zoekactie voor de servicelocatie (SRV-records) is ingeschakeld. Het bestand bevat een lijst met domeincontrollers voor elk domein. Het wordt in eerste instantie gemaakt door de connector, maar u moet het vervolgens zelf bijhouden. Het bestand overschrijft de DNS-zoekacties voor de servicelocatie.

DNS-zoekacties voor servicelocaties zijn ingeschakeld voor de volgende directorytypen:

- Active Directory via LDAP waarvoor de optie **Deze directory ondersteunt DNS-servicelocatie** is ingeschakeld
- Active Directory (Geïntegreerde Windows-verificatie), waarbij de servicelocatie altijd via DNS wordt opgezocht

Bij de aanmaak van een directory waarvoor de servicelocatie via DNS wordt opgezocht, wordt automatisch het bestand `domain_krb.properties` gemaakt in de directory `/usr/local/horizon/conf` van de virtual machine en automatisch ingevuld met de domeincontrollers voor elk domein. Om het bestand in te vullen zoekt de connector naar domeincontrollers die zich op dezelfde site als de connector bevinden en selecteert hier twee bereikbare controllers die de snelste respons hebben.

Wanneer u aanvullende directory's maakt waarvoor de servicelocatie via DNS wordt opgezocht, of nieuwe domeinen toevoegt aan een directory met geïntegreerde Windows-verificatie, worden de nieuwe domeinen met bijbehorende domeincontrollers opgenomen in het bestand.

U kunt de standaardselectie te allen tijde overschrijven door het bestand `domain_krb.properties` te bewerken. Als best practice wordt aanbevolen om het bestand `domain_krb.properties` voor een nieuwe directory direct te controleren om te kijken of de vermelde domeincontrollers optimaal zijn voor uw configuratie. Bij een mondiale Active Directory-implementatie waarbij meerdere domeincontrollers over verschillende geografische locaties zijn verspreid, krijgt u de snelste communicatie met Active Directory wanneer u een domeincontroller kiest die zich vlak bij de connector bevindt.

Ook voor andere wijzigingen moet u het bestand handmatig bijwerken. De volgende regels zijn van applicatie.

- Het bestand `domain_krb.properties` wordt gemaakt op de virtual machine van de connector. In een normale implementatie zonder aanvullende connectoren wordt het bestand gemaakt op de virtual machine van de VMware Identity Manager-service. Als u een aanvullende connector voor de directory gebruikt, wordt het bestand gemaakt op de virtual machine van de connector. Een virtual machine kan slechts één `domain_krb.properties`-bestand bevatten.

- Wanneer u een nieuwe directory maakt waarbij de servicelocatie via DNS wordt opgezocht, wordt het bestand automatisch gemaakt en gevuld met de domeincontrollers voor elk domein.
- De domeincontrollers voor elk domein worden in volgorde van prioriteit weergegeven. De eerste domeincontroller in de lijst zal door de connector worden gebruikt om verbinding met Active Directory te maken. Als deze niet bereikbaar is, wordt de tweede controller in de lijst geprobeerd enzovoort.
- Het bestand wordt alleen bijgewerkt wanneer u een nieuwe directory maakt waarvoor de servicelocatie via DNS wordt opgezocht of wanneer u een domein toevoegt aan een directory met geïntegreerde Windows-verificatie. Het nieuwe domein wordt met bijbehorende domeincontrollers aan het bestand toegevoegd.

  Houd er rekening mee dat een bestaande domeinvermelding in het bestand niet wordt bijgewerkt. Stel dat u een directory hebt gemaakt en deze vervolgens verwijdert, dan wordt het bestand niet bijgewerkt en blijft de originele vermelding van het domein in het bestand gehandhaafd.
- Ook in andere gevallen wordt het bestand niet automatisch bijgewerkt. Als u een directory bijvoorbeeld verwijdert, wordt de domeinvermelding niet uit het bestand verwijderd.
- Als een vermelde domeincontroller in het bestand onbereikbaar wordt, moet u het bestand handmatig bewerken en de vermelding verwijderen.
- Als u een domeinvermelding handmatig toevoegt of bewerkt, worden uw wijzigingen niet overschreven.

Voor informatie over het bewerken van het bestand `domain_krb.properties`, zie "Het bestand domain_krb.properties bewerken," op pagina 51.

Belangrijk Het bestand `/etc/krb5.conf` moet altijd overeenkomen met het bestand `domain_krb.properties`. Telkens als u het bestand `domain_krb.properties` bijwerkt, moet u ook het bestand `krb5.conf` bijwerken. Zie "Het bestand domain_krb.properties bewerken," op pagina 51 en het Knowledge Base-artikel 2091744 voor meer informatie.

Selectie van domeincontrollers waarmee het bestand domain_krb.properties automatisch wordt gevuld

Om het bestand `domain_krb.properties` automatisch in te vullen, wordt op basis van IP-adres en netmasker gekeken op welk subnet de connector zich bevindt, waarna de Active Directory-configuratie wordt gebruikt om de site op dat subnet te identificeren. Vervolgens wordt de lijst met domeincontrollers voor die site opgehaald en gefilterd om het juiste domein te bepalen, waarna de twee domeincontrollers met de snelste respons worden geselecteerd.

Om de dichtstbijzijnde domeincontrollers te kunnen bepalen, stelt VMware Identity Manager de volgende vereisten:

- Het subnet van de connector moet aanwezig zijn in de Active Directory-configuratie of er moet een subnet zijn opgegeven in het bestand `runtime-config.properties`. Zie "De standaardsubnetselectie overschrijven," op pagina 51.

  Het subnet wordt gebruikt om de site te bepalen.
- De Active Directory-configuratie moet site-aware zijn.

Als het subnet niet kan worden bepaald of als uw Active Directory-configuratie niet site-aware is, worden geen DNS-zoekacties voor servicelocaties gebruikt om domeincontrollers te zoeken, en wordt het bestand gevuld met een paar domeincontrollers die bereikbaar zijn. Omdat deze domeincontrollers zich mogelijk niet op dezelfde geografische locatie bevinden als de connector, kunnen er vertragingen of time-outs optreden in de communicatie met Active Directory. Geef in dat geval handmatig de juiste domeincontrollers voor elk domein op in het bestand `domain_krb.properties`. Zie "Het bestand domain_krb.properties bewerken," op pagina 51.

Voorbeeldbestand domain_krb.properties

```
example.com=host1.example.com:389,host2.example.com:389
```

De standaardsubnetselectie overschrijven

Bij de automatische invulling van het bestand `domain_krb.properties` zoekt de connector naar domeincontrollers op dezelfde site, zodat de vertraging tussen de connector en Active Directory minimaal blijft.

Daarbij wordt op basis van IP-adres en subnetmasker gekeken op welk subnet de connector zich bevindt, waarna de Active Directory-configuratie wordt gebruikt om de site op dat subnet te identificeren. Als het subnet van de virtual machine zich niet in een Active Directory-omgeving bevindt of als u de automatische subnetselectie wilt overschrijven, kunt u zelf een subnet opgeven in het bestand `runtime-config.properties`.

Procedure

1 Meld u als hoofdgebruiker aan bij de virtual machine van de VMware Identity Manager.

Opmerking Als u een aanvullende connector voor de directory gebruikt, meldt u zich aan bij de virtual machine van de connector.

---

2 Bewerk het bestand `/usr/local/horizon/conf/runtime-config.properties` om het volgende kenmerk toe te voegen.

```
siteaware.subnet.override=subnet
```

waarbij *subnet* het subnet is van de site waarvan u de domeincontrollers wilt gebruiken. Bijvoorbeeld:

```
siteaware.subnet.override=10.100.0.0/20
```

3 Sla het bestand op en sluit het.

4 Start de service opnieuw op.

```
service horizon-workspace restart
```

Het bestand domain_krb.properties bewerken

Het bestand `/usr/local/horizon/conf/domain_krb.properties` geeft aan welke domeincontrollers worden gebruikt voor directory's waarbij de locatie van services via DNS kan worden opgezocht. U kunt het bestand desgewenst bewerken om de lijst met domeincontrollers voor een domein te wijzigen of om domeinvermeldingen toe te voegen of te verwijderen. Uw wijzigingen worden niet overschreven.

Het bestand wordt in eerste instantie door de connector gemaakt en automatisch ingevuld. In bepaalde scenario's moet u het bestand handmatig bijwerken, zoals:

- Als de standaard gekozen domeincontrollers niet optimaal zijn voor uw configuratie, kunt u het bestand bewerken om aan te geven welke domeincontrollers u wilt gebruiken.
- Als u een directory verwijdert, dient u tevens de bijbehorende domeinvermelding uit het bestand te verwijderen.
- Wanneer een of meer domeincontrollers in het bestand niet te bereiken zijn, verwijdert u deze uit het bestand.

Zie ook "Domeincontrollers selecteren (bestand domain_krb.properties)," op pagina 49.

Procedure

1 Meld u als hoofdgebruiker aan bij de virtual machine van de VMware Identity Manager.

Opmerking Als u een aanvullende connector voor de directory gebruikt, meldt u zich aan bij de virtual machine van de connector.

2 Stel de directory's in op `/usr/local/horizon/conf`.

3 Bewerk het bestand `domain_krb.properties` om de lijst met hostwaarden voor het domein uit te breiden of te bewerken.

Gebruik de volgende notatie:

domein=host:poort,host2:poort,host3:poort

Bijvoorbeeld: .

```
example.com=examplehost1.example.com:389,examplehost2.example.com:389
```

Geef de domeincontrollers op volgorde van prioriteit weer. De eerste domeincontroller in de lijst zal door de connector worden gebruikt om verbinding met Active Directory te maken. Als deze niet bereikbaar is, wordt de tweede controller in de lijst geprobeerd enzovoort.

Belangrijk De domeinnamen mogen geen hoofdletters bevatten.

4 Wijzig de eigenaar van het bestand `domain_krb.properties` in `horizon` en groepeer het als `www` met behulp van de volgende opdracht.

```
chown horizon:www /usr/local/horizon/conf/domain_krb.properties
```

5 Start de service opnieuw op.

```
service horizon-workspace restart
```

Wat nu te doen

Nadat u het bestand `domain_krb.properties` hebt bewerkt, bewerkt u het bestand `/etc/krb5.conf`. Het bestand `krb5.conf` moet altijd overeenkomen met het bestand `domain_krb.properties`.

1 Bewerk het bestand `/etc/krb5.conf` en werk het gedeelte `realms` bij om dezelfde domein-naar-host-waarden op te geven die worden gebruikt in het bestand `/usr/local/horizon/conf/domain_krb.properties`. U hoeft het poortnummer niet op te geven. Als het bestand `domain_krb.properties` bijvoorbeeld de domeinvermelding `example.com=examplehost.example.com:389` heeft, werkt u het bestand `krb5.conf` als volgt bij.

```
[realms]
GAUTO-QA.COM = {
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO2QA\.GAUTO-QA\.COM\\.*)s/^GAUTO2QA\.GAUTO-
QA\.COM/GAUTO2QA/
auth_to_local = RULE:[1:$0\$1](^GLOBEQE\.NET\\.*)s/^GLOBEQE\.NET/GLOBEQE/
auth_to_local = DEFAULT
kdc = examplehost.example.com
}
```

Opmerking Het is mogelijk om meerdere kdc-vermeldingen te hebben. Dit is echter geen vereiste omdat er in de meeste gevallen slechts één kdc-waarde is. Als u ervoor kiest om extra kdc-waarden te definiëren, heeft elke regel een kdc-vermelding die een domeincontroller definieert.

2 Start de werkruimteservice opnieuw.

```
service horizon-workspace restart
```

Raadpleeg Knowledge Base-artikel 2091744.

Problemen oplossen voor domain_krb.properties

Gebruik de volgende informatie voor het oplossen van problemen met het bestand `domain_krb.properties`.

De fout "Fout bij omzetten van domein"

De Fout bij omzetten van domein treedt op wanneer het bestand `domain_krb.properties` al een vermelding van een domein bevat en u voor hetzelfde domein een nieuwe directory van een ander type probeert te maken. U moet de domeinvermelding in het bestand `domain_krb.properties` dan eerst handmatig verwijderen voordat u de nieuwe directory maakt.

Domeincontrollers zijn niet bereikbaar

De toegevoegde domeinvermeldingen aan het bestand `domain_krb.properties` worden niet automatisch bijgewerkt. Als een van de vermelde domeincontrollers in het bestand onbereikbaar wordt, moet u het bestand handmatig bewerken en de vermelding verwijderen.

Gebruikerskenmerken beheren die vanuit Active Directory worden gesynchroniseerd

Tijdens de installatie van de VMware Identity Manager-servicedirectory selecteert u Active Directory-gebruikerskenmerken en -filters om op te geven welke gebruikers in de VMware Identity Manager-directory worden gesynchroniseerd. U kunt de gebruikerskenmerken die worden gesynchroniseerd wijzigen via de beheerconsole, tabblad Identiteits- en toegangsbeheer, Installatie > Gebruikerskenmerken.

Wijzigingen die worden gemaakt en opgeslagen op de pagina Gebruikerskenmerken, worden toegevoegd aan de pagina Toegewezen kenmerken in de VMware Identity Manager-directory. De kenmerkwijzigingen worden bijgewerkt naar de directory bij de volgende synchronisatie naar Active Directory.

De pagina Gebruikerskenmerken geeft de standaarddirectorykenmerken weer die kunnen worden toegewezen aan Active Directory-kenmerken. U selecteert de kenmerken die vereist zijn en u kunt andere Active Directory-kenmerken toevoegen die u met de directory wilt synchroniseren. Houd er bij het toevoegen van kenmerken rekening mee dat de kenmerknaam die u invoert hoofdlettergevoelig is. Zo zijn adres, Adres en ADRES verschillende kenmerken.

Tabel 4-1. Active Directory-standaardkenmerken om te synchroniseren met de directory

Kenmerknaam van de VMware Identity Manager-directory	Standaardtoewijzing aan Active Directory-kenmerk
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
domain	canonicalName. Voegt de Fully Qualified Domain Name van het object toe.
disabled (externe gebruiker uitgeschakeld)	userAccountControl. Gemarkeerd met UF_Account_Disable Wanneer een account is uitgeschakeld, kunnen gebruikers zich niet aanmelden om toegang te krijgen tot hun applicaties en bronnen. De bronnen waarvoor gebruikers rechten hadden, worden niet uit het account verwijderd, zodat wanneer de markering van het account wordt verwijderd, gebruikers zich kunnen aanmelden en toegang krijgen tot hun bronnen waarvoor rechten zijn verleend
phone	telephoneNumber

Tabel 4-1. Active Directory-standaardkenmerken om te synchroniseren met de directory (Vervolgd)

Kenmerknaam van de VMware Identity Manager-directory	Standaardtoewijzing aan Active Directory-kenmerk
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName.

Kenmerken selecteren om te synchroniseren met de directory

Wanneer u de VMware Identity Manager-directory instelt om te synchroniseren met Active Directory, geeft u de gebruikerskenmerken op die met de directory moeten worden gesynchroniseerd. Voordat u de directory instelt, kunt u op de pagina Gebruikerskenmerken opgeven welke standaardkenmerken vereist zijn en kunt u aanvullende kenmerken toevoegen die u aan Active Directory-kenmerken wilt toewijzen.

Wanneer u de pagina Gebruikerskenmerken configureert voordat de directory is gemaakt, kunt u standaardkenmerken wijzigen van vereist naar niet-vereist, eventueel kenmerken markeren en aangepaste kenmerken toevoegen.

Nadat de directory is gemaakt, kunt u een vereist kenmerk wijzigen zodat dit niet-vereist wordt en u kunt aangepaste kenmerken verwijderen. U kunt een kenmerk niet wijzigen zodat het een vereist kenmerk wordt.

Wanneer u andere kenmerken toevoegt om met de directory te synchroniseren, kunt u, nadat de directory is gemaakt, naar de pagina Toegewezen kenmerken van de directory gaan om deze kenmerken toe te wijzen aan de Active Directory-kenmerken.

Belangrijk Als u XenApp-bronnen wilt synchroniseren met VMware Identity Manager, moet u **distinguishedName** instellen als een vereist kenmerk. U moet dit opgeven voordat de VMware Identity Manager-directory wordt gemaakt.

Procedure

1 Klik in de beheerconsole op het tabblad Identiteits- en toegangsbeheer op **Installatie > Gebruikerskenmerken**.

2 Controleer in de sectie Standaardkenmerken de lijst met vereiste kenmerken en breng de nodige wijzigingen aan om aan te geven welke kenmerken vereist moeten zijn.

3 Voeg in de sectie Kenmerken de naam van het VMware Identity Manager-directorykenmerk toe aan de lijst.

4 Klik op **Opslaan**.

   De standaardkenmerkstatus wordt bijgewerkt en de kenmerken die u hebt toegevoegd, worden aan de lijst Toegewezen kenmerken van de directory toegevoegd.

5 Nadat de directory is gemaakt, gaat u naar de pagina **Beheren > Directory's** en selecteert u de directory.

6 Klik op **Synchronisatie-instellingen > Toegewezen kenmerken**.

7 Selecteer in het vervolgkeuzemenu voor de kenmerken die u hebt toegevoegd, het Active Directory-kenmerk waarnaar u wilt toewijzen.

8 Klik op **Opslaan.**

De volgende keer dat de directory met Active Directory wordt gesynchroniseerd, wordt de directory bijgewerkt.

Vereiste rechten voor het toevoegen aan een domein

Mogelijk moet u de VMware Identity Manager-connector in sommige gevallen aan een domein toevoegen. Bij Active Directory via LDAP-directory's maakt u eerst de directory en voegt u vervolgens de controller toe aan het domein. Bij directory's van het type Active Directory (Geïntegreerde Windows-verificatie) wordt de connector automatisch aan het domein toegevoegd wanneer u de directory maakt. In beide gevallen moet u verificatiegegevens opgeven.

Voor het toevoegen aan een domein hebt u Active Directory-verificatiegegevens nodig met de bevoegdheid "computer lid maken van AD-domein". Deze bevoegdheid wordt in Active Directory ingesteld met de volgende rechten:

- Computerobjecten maken
- Computerobjecten verwijderen

Wanneer u aan een domein deelneemt, wordt een computerobject gemaakt in de standaardlocatie in Active Directory, tenzij u een aangepaste OU opgeeft.

Volg deze stappen om aan een domein deel te nemen als u geen rechten hebt om aan een domein deel te nemen.

1 Vraag uw Active Directory-beheerder om het computerobject in Active Directory te maken op een locatie die voldoet aan het beleid van uw organisatie. Geef de hostnaam van de connector op. Zorg dat u de volledig gekwalificeerde domeinnaam invoert, bijvoorbeeld `server.example.com`.

Tip U ziet de hostnaam in de kolom **Hostnaam** op de pagina Connectoren van de beheerconsole. Klik op **Identiteits- en toegangsbeheer > Setup > Connectoren** om de pagina Connectoren weer te geven.

2 Als het computerobject is gemaakt, gebruikt u een willekeurige domeingebruikersaccount in de VMware Identity Manager-beheerconsole om de computer aan het domein toe te voegen.

De opdracht **Aan domein toevoegen** is beschikbaar op de pagina **Connectoren**, die u weergeeft door te klikken op **Identiteits- en toegangsbeheer > Setup > Connectoren**.

Optie	Beschrijving
Domein	Selecteer of typ het Active Directory-domein waaraan u wilt deelnemen. Zorg ervoor dat u de volledig gekwalificeerde domeinnaam invoert. Bijvoorbeeld: **server.example.com**.
Domeingebruiker	De gebruikersnaam van een Active Directory-gebruiker die de rechten heeft om systemen aan het Active Directory-domein te koppelen.
Domeinwachtwoord	Het wachtwoord van de gebruiker.
Organisatie-eenheid (OU)	(Optioneel) De organisatie-eenheid van het computerobject. Met behulp van deze optie wordt een computerobject gemaakt in de opgegeven OU in plaats van de standaard OU van de computer. Bijvoorbeeld: **ou=testou,dc=test,dc=example,dc=com**.

Verbinding van Active Directory met de service configureren

In de beheerconsole specificeert u de vereiste informatie om aan uw Active Directory te verbinden en selecteert u gebruikers en groepen om te synchroniseren met de directory van VMware Identity Manager.

De verbindingsopties van de Active Directory zijn Active Directory via LDAP of geïntegreerde Windows-verificatie van Active Directory. De verbinding Active Directory via LDAP ondersteunt de opzoekfunctie DNS Service Location. Met de geïntegreerde Windows-verificatie van Active Directory configureert u het domein om toe te voegen.

Vereisten

- Selecteer welke kenmerken verplicht zijn en voeg zo nodig extra kenmerken toe op de pagina Gebruikerskenmerken. Zie "Kenmerken selecteren om te synchroniseren met de directory," op pagina 54.

  Belangrijk Als u de XenApp-bronnen wilt synchroniseren met VMware Identity Manager moet u van **distinguishedName** een vereist kenmerk maken. U moet deze selectie uitvoeren voordat u een directory maakt, omdat kenmerken niet kunnen worden gewijzigd in vereiste kenmerken nadat een directory is gemaakt.

- Lijst met de Active Directory-groepen en -gebruikers die u wilt synchroniseren vanuit Active Directory.
- Voor Active Directory via LDAP bevat de vereiste informatie de Base DN, Bind DN en het Bind DN-wachtwoord.

  Opmerking Het gebruik van een gebruikersaccount van Bind DN met een wachtwoord dat niet verloopt, wordt aanbevolen.

- Voor geïntegreerde Windows-verificatie in Active Directory is de vereiste informatie onder andere het UPN-adres en -wachtwoord van de gebruiker van de binding voor het domein.

  Opmerking Het gebruik van een gebruikersaccount van Bind DN met een wachtwoord dat niet verloopt, wordt aanbevolen.

- Als de Active Directory toegang via SSL of STARTTLS vereist, is het basis CA-certificaat van de domeincontroller van Active Directory vereist.
- Voor geïntegreerde Windows-verificatie in Active Directory, met een configuratie van meerdere forests voor Active Directory en een lokale domeingroep met meerdere leden van domeinen in verschillende forests, moet u ervoor zorgen dat de gebruiker van de binding wordt toegevoegd aan de groep Administrators van het domein waarin zich de lokale domeingroep bevindt. Als u dit niet doet, ontbreken deze leden in de lokale domeingroep.

Procedure

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

2 Op de Directorypagina klikt u op **Directory toevoegen**.

3 Voer een naam in voor deze directory van VMware Identity Manager.

4 Selecteer het type Active Directory in uw omgeving en configureer de verbindingsinformatie.

Optie	Beschrijving
Active Directory via LDAP	a In het veld **Connector synchroniseren** selecteert u de te gebruiken Connector om met Active Directory te synchroniseren. b Als deze Active Directory wordt gebruikt om gebruikers te verifiëren, klikt u in het veld **Verificatie** op **Ja**. Als een externe identiteitsprovider wordt gebruikt om gebruikers te verifiëren, klikt u op **Nee**. Nadat u de verbinding van Active Directory hebt geconfigureerd om gebruikers en groepen te synchroniseren, gaat u naar de pagina Identiteits- en toegangsbeheer > Beheren > Identiteitsprovider. c In het veld **Zoekkenmerk directory** selecteert u het accountkenmerk dat de gebruikersnaam bevat. d Als de Active Directory de opzoekfunctie DNS Service Location gebruikt, selecteert u het volgende. ■ In de sectie **Server Location** schakelt u het selectievakje **Deze directory ondersteunt DNS Service Location** in. Een bestand `domain_krb.properties` dat automatisch is ingevuld met een lijst domeincontrollers, wordt gemaakt wanneer de directory is gemaakt. Zie "Domeincontrollers selecteren (bestand domain_krb.properties)," op pagina 49. ■ Als Active Directory de versleuteling STARTTLS vereist, schakelt u het selectievakje **Deze directory vereist dat alle verbindingen SSL gebruiken** in de sectie **Certificaten** in en kopieert en plakt u het basis CA-certificaat van de Active Directory in het veld **SSL-certificaat**. Zorg ervoor dat het certificaat in PEM-formaat is en neem de regels "BEGIN CERTIFICATE" en "END CERTIFICATE" op. **Opmerking** Als de Active Directory STARTTLS vereist en u verstrekt het certificaat niet, kunt u de directory niet maken. e Als de Active Directory geen opzoekfunctie van DNS Service Location gebruikt, selecteert u het volgende. ■ In de sectie **Server Location** controleert u of het selectievakje **Deze directory ondersteunt DNS Service Location** niet is ingeschakeld en voert u de serverhostnaam en het poortnummer van de Active Directory in. Zie de sectie Multi-domein, Single Forest Active Directory-omgeving in "Active Directory-omgevingen," op pagina 47 om de directory als een globale catalogus te configureren. ■ Als de Active Directory toegang over SSL vereist, schakelt u het selectievakje **Deze directory vereist dat alle verbindingen SSL gebruiken** in de sectie **Certificaten** in en kopieert en plakt u het basis CA-certificaat van de Active Directory in het veld **SSL-certificaat**.

Optie	Beschrijving
	Zorg ervoor dat het certificaat in PEM-formaat is en neem de regels "BEGIN CERTIFICATE" en "END CERTIFICATE" op. **Opmerking** Als de Active Directory SSL vereist en u verstrekt het certificaat niet, kunt u de directory niet maken. f In het veld **Base DN** voert u de DN in vanwaar de accountzoekopdrachten moeten starten. Bijvoorbeeld OU=myUnit,DC=myCorp,DC=com. g In het veld **Bind DN** voert u het account in dat naar gebruikers kan zoeken. Bijvoorbeeld CN=binduser,OU=myUnit,DC=myCorp,DC=com. **Opmerking** Het gebruik van een gebruikersaccount van Bind DN met een wachtwoord dat niet verloopt, wordt aanbevolen. h Nadat u het bindingswachtwoord hebt ingevoerd, klikt u op **Verbinding testen** om te controleren of de directory verbinding kan maken met uw Active Directory.
Active Directory (geïntegreerde Windows-verificatie)	a In het veld **Connector synchroniseren** selecteert u de te gebruiken Connector om met Active Directory te synchroniseren. b Als deze Active Directory wordt gebruikt om gebruikers te verifiëren, klikt u in het veld **Verificatie** op **Ja**. Als een externe identiteitsprovider wordt gebruikt om gebruikers te verifiëren, klikt u op **Nee**. Nadat u de verbinding van Active Directory hebt geconfigureerd om gebruikers en groepen te synchroniseren, gaat u naar de pagina Identiteits- en toegangsbeheer > Beheren > Identiteitsprovider. c In het veld **Zoekkenmerk directory** selecteert u het accountkenmerk dat de gebruikersnaam bevat. d Als de Active Directory de versleuteling STARTTLS vereist, schakelt u het selectievakje **Deze directory vereist dat alle verbindingen STARTTLS gebruiken** in de sectie **Certificaten** in en kopieert en plakt u het basis CA-certificaat van de Active Directory in het veld **SSL-certificaat**. Zorg ervoor dat het certificaat in PEM-formaat is en neem de regels "BEGIN CERTIFICATE" en "END CERTIFICATE" op. Als de directory meerdere domeinen heeft, voegt u één voor één het basis CA-certificaat voor alle domeinen toe. **Opmerking** Als de Active Directory STARTTLS vereist en u verstrekt het certificaat niet, kunt u de directory niet maken. e Voer de naam in van het Active Directory-domein dat wordt toegevoegd. Voer een gebruikersnaam en wachtwoord in dat de rechten heeft om het domein toe te voegen. Raadpleeg "Vereiste rechten voor het toevoegen aan een domein," op pagina 55 voor meer informatie. f In het veld bindingsgebruiker-UPN voert u de User Principal Name (UPN) van de gebruiker in die met het domein kan worden geverifieerd. Bijvoorbeeld username@example.com. **Opmerking** Het gebruik van een gebruikersaccount van Bind DN met een wachtwoord dat niet verloopt, wordt aanbevolen. g Voer het wachtwoord van de bindingsgebruiker in.

5 Klik op **Opslaan en Volgende**.

De pagina met de lijst domeinen verschijnt.

6 Voor Active Directory over LDAP worden de domeinen vermeld met een vinkje.

Voor Active Directory (met geïntegreerde Windows-verificatie) selecteert u de domeinen die moeten worden gekoppeld aan deze Active Directory-verbinding.

Opmerking Als u een vertrouwend domein toevoegt nadat de directory is gemaakt, stelt de service niet automatisch het nieuwe vertrouwende domein vast. Als u het vaststellen van het domein voor de service wilt inschakelen, moet Connector het domein verlaten en hieraan opnieuw deelnemen. Wanneer Connector opnieuw deelneemt aan het domein, wordt het vertrouwende domein in de lijst weergegeven.

Klik op **Volgende**.

7 Controleer of de kenmerknamen van de VMware Identity Manager-directory zijn toegewezen aan de juiste Active Directory-kenmerken en breng zo nodig wijzigingen aan. Klik vervolgens op **Volgende**.

8 Selecteer de groepen die u vanuit Active Directory wilt synchroniseren met de VMware Identity Manager-directory.

Optie	Beschrijving
Geef de DN's van de groep op	Als u groepen wilt selecteren, kunt u een of meer groeps-DN's opgeven en de onderliggende groepen selecteren. a Klik op **+** en geef de groeps-DN op. Bijvoorbeeld CN=gebruikers,DC=voorbeeld,DC=bedrijf,DC=com. **Belangrijk** Geef de groeps-DN's op onder de basis-DN die u hebt ingevoerd. Als een groeps-DN buiten de basis-DN ligt, worden gebruikers van die DN gesynchroniseerd, maar kunnen zij zich niet aanmelden. b Klik op **Groepen zoeken**. De kolom **Te synchroniseren groepen** bevat het aantal groepen dat is gevonden in de DN. c Als u alle groepen in de DN wilt selecteren, klikt u op **Alles selecteren**. Of klik op **Selecteren** en selecteer de specifieke groepen die u wilt synchroniseren. **Opmerking** Wanneer u een groep synchroniseert, worden gebruikers die geen Domeingebruikers als hun primaire groep in Active Directory hebben, niet gesynchroniseerd.
Geneste groepsleden synchroniseren	De optie **Geneste groepsleden synchroniseren** is standaard ingeschakeld. Wanneer deze optie is ingeschakeld, worden alle gebruikers gesynchroniseerd die direct tot de groep behoren die u selecteert en alle gebruikers die tot de geneste groepen eronder behoren. Let op dat de geneste groepen niet worden gesynchroniseerd; alleen de gebruikers die tot de geneste groepen behoren, worden gesynchroniseerd. In de VMware Identity Manager-directory zijn deze gebruikers leden van de bovenliggende groep die u hebt geselecteerd om te synchroniseren. Als de optie **Geneste groepsleden synchroniseren** is uitgeschakeld, wanneer u een groep opgeeft om te synchroniseren, worden alle gebruikers gesynchroniseerd die tot die groep behoren. Gebruikers die tot geneste groepen eronder behoren, worden niet gesynchroniseerd. Het uitschakelen van deze functie is handig voor grote Active Directory-configuraties waarbij het doorkruisen van een groepsstructuur veel tijd en middelen kost. Als u deze optie uitschakelt, zorgt u ervoor dat u alle groepen selecteert waarvan u de gebruikers wilt synchroniseren.

9 Klik op **Volgende**.

10 Geef zo nodig extra gebruikers op om te synchroniseren.

a Klik op + en voer de gebruikers-DN's in. Bijvoorbeeld: CN=gebruikers,CN=Gebruikers,OU=mijnAfdeling,DC=mijnOnderneming,DC=com.

Belangrijk Geef de gebruikers-DN's op onder de basis-DN die u hebt ingevoerd. Als een gebruikers-DN buiten de basis-DN ligt, worden gebruikers van die DN gesynchroniseerd, maar kunnen zij zich niet aanmelden.

b (Optioneel) Als u gebruikers wilt uitsluiten, maakt u een filter om sommige gebruikerstypen uit te sluiten.

U selecteert het gebruikerskenmerk waarop moet worden gefilterd, de queryregel en de waarde.

11 Klik op **Volgende**.

12 Neem de pagina door om te zien hoeveel gebruikers en groepen naar de directory worden gesynchroniseerd en om het synchronisatieschema te bekijken.

Klik op de koppelingen **Bewerken** om wijzigingen aan te brengen aan gebruikers en groepen of aan de synchronisatiefrequentie.

13 Klik op **Directory synchroniseren** om synchroniseren naar de directory te starten.

De verbinding met Active Directory is gemaakt en gebruikers en groepen worden gesynchroniseerd van de Active Directory naar de directory van VMware Identity Manager. De Bind DN-gebruiker heeft standaard een beheerdersrol in VMware Identity Manager.

Wat nu te doen

- Als u een directory hebt gemaakt die DNS Service Location ondersteunt, wordt er een bestand `domain_krb.properties` gemaakt en automatisch ingevuld met een lijst domeincontrollers. Bekijk het bestand om de lijst domeincontrollers te controleren of te bewerken. Zie “Domeincontrollers selecteren (bestand domain_krb.properties),” op pagina 49.
- Stel verificatiemethoden in. Nadat gebruikers en groepen met de directory zijn gesynchroniseerd, kunt u aanvullende verificatiemethoden voor de connector instellen als de connector ook voor verificatie wordt gebruikt. Als de identiteitsprovider voor verificatie een derde is, configureert u de betreffende identiteitsprovider voor de connector.
- Controleer het standaardtoegangsbeleid. Het standaardtoegangsbeleid is geconfigureerd om alle toepassingen in alle netwerkbereiken toegang te verlenen tot de webbrowser, met een sessietime-out van acht uur. De andere mogelijkheid is het verlenen van toegang tot een clientapp met een sessietime-out van 2160 uur (90 dagen). U kunt het standaardtoegangsbeleid wijzigen en bij het toevoegen van Webapplicaties aan de catalogus, kunt u nieuw toegangsbeleid maken.
- Pas aangepaste merkvermelding toe op de beheerconsole, de portalpagina's van gebruikers en het aanmeldscherm.

Gebruikers de mogelijkheid geven om Active Directory-wachtwoorden te wijzigen

U kunt gebruikers de mogelijkheid geven om hun Active Directory-wachtwoorden op elk gewenst moment te wijzigen via de Workspace ONE-portal of -app. Gebruikers kunnen ook hun Active Directory-wachtwoorden opnieuw instellen vanaf de VMware Identity Manager-aanmeldingspagina als het wachtwoord is verlopen of als de Active Directory-beheerder het wachtwoord opnieuw heeft ingesteld, waardoor de gebruiker het wachtwoord bij de volgende aanmelding moet wijzigen.

U kunt deze optie per directory inschakelen door de optie **Wijziging van wachtwoord toestaan** te selecteren op de pagina Directory-instellingen.

Wanneer gebruikers zich hebben aangemeld bij de portal Workspace ONE kunnen zij hun wachtwoord wijzigen door op hun naam in de rechterbovenhoek te klikken, dan **Account** in het vervolgkeuzemenu te selecteren en vervolgens op de koppeling **Wachtwoord wijzigen** te klikken. In de app Workspace ONE kunnen gebruikers hun wachtwoord wijzigen door op het menupictogram met drie streepjes te klikken en **Wachtwoord** te selecteren.

Verlopen wachtwoorden of wachtwoorden die door de beheerder in Active Directory opnieuw zijn ingesteld, kunnen vanaf de aanmeldingspagina worden gewijzigd. Wanneer een gebruiker zich probeert aan te melden met een verlopen wachtwoord, wordt de gebruiker gevraagd het wachtwoord opnieuw in te stellen. De gebruiker moet het oude wachtwoord en het nieuwe wachtwoord invoeren.

De vereisten voor het nieuwe wachtwoord worden bepaald aan de hand van het beleid inzake Active Directory-wachtwoorden. Het toegestane aantal pogingen hangt ook af van het beleid inzake Active Directory-wachtwoorden.

De volgende beperkingen zijn van toepassing.

- De optie **Wijziging van wachtwoord toestaan** is alleen beschikbaar bij connectorversie 2016.11.1 en hoger als u extra, zelfstandige virtual appliances van een connector gebruikt.
- Wanneer een directory aan VMware Identity Manager wordt toegevoegd als globale catalogus, is de optie **Wijziging van wachtwoord toestaan** niet beschikbaar. Directory's kunnen worden toegevoegd als Active Directory via LDAP of Geïntegreerde Windows-verificatie, met de poort 389 of 636.
- Het wachtwoord van een gebruiker van een bindings-DN kan niet opnieuw worden ingesteld via VMware Identity Manager, zelfs niet als het is verlopen of als de Active Directory-beheerder het opnieuw heeft ingesteld.

  Opmerking Het gebruik van een gebruikersaccount van Bind DN met een wachtwoord dat niet verloopt, wordt aanbevolen.

- Wachtwoorden van gebruikers met aanmeldingsnamen die uit multibyte-tekens (geen ASCII-tekens) bestaan, kunnen niet opnieuw worden ingesteld vanuit VMware Identity Manager.

Vereisten

- Poort 464 moet open zijn van de VMware Identity Manager naar de domeincontrollers.

Procedure

1. Klik in de beheerconsole op het tabblad **Identiteits- en toegangsbeheer**.
2. Op het tabblad **Directory's** klikt u op de directory.
3. In het gedeelte **Wijziging van wachtwoord toestaan** schakelt u het selectievakje **Wijziging van wachtwoord inschakelen** in.
4. Geef het wachtwoord van de bindings-DN op in het gedeelte **Details van bindingsgebruiker** en klik op **Opslaan**.

Met LDAP-directory's integreren

U kunt uw bedrijfs-LDAP-directory integreren met VMware Identity Manager om gebruikers en groepen van de LDAP-directory te synchroniseren met de VMware Identity Manager-service.

Zie ook "Belangrijke concepten met betrekking tot de integratie van directory's," op pagina 46.

Beperkingen van LDAP-directory-integratie

Voor de integratiefunctie van de LDAP-directory gelden momenteel de volgende beperkingen.

- U kunt slechts één domein van een LDAP-directory-omgeving integreren

  Om meerdere domeinen van een LDAP-directory te integreren, moet u extra VMware Identity Manager-mappen aanmaken, één voor elk domein.

- De volgende verificatiemethoden worden niet ondersteund voor VMware Identity Manager-mappen van het type LDAP-directory.
  - Kerberos-verificatie
  - Adaptieve RSA-verificatie
  - ADFS als een externe identiteitsprovider
  - SecurID
  - Radiusverificatie met Vasco en SMS-wachtwoordcodeserver
- U kunt niet worden toegevoegd aan een LDAP-domein.
- Integratie met View of gepubliceerde Citrix-bronnen wordt niet ondersteund voor VMware Identity Manager-mappen van het type LDAP-directory.
- Gebruikersnamen mogen geen spaties bevatten. Wanneer een gebruikersnaam een spatie bevat, wordt de gebruiker gesynchroniseerd, maar zijn de rechten niet beschikbaar voor de gebruiker.
- Wanneer u van plan bent om zowel Active Directory als LDAP-directory's toe te voegen, let er dan op dat u geen kenmerken op de pagina Gebruikerskenmerken markeert als zijnde vereist, behalve userName dat wel kan worden gemarkeerd als zijnde vereist. De instellingen op de pagina Gebruikerskenmerken gelden voor alle directory's in de service. Wanneer een kenmerk als zijnde vereist is gemarkeerd, worden gebruikers zonder dat kenmerk niet gesynchroniseerd met de VMware Identity Manager-service.
- Wanneer uw LDAP-directory meerdere groepen met dezelfde naam bevat, moet u voor deze groepen unieke namen specificeren in de VMware Identity Manager-service. U kunt de namen specificeren wanneer u de groepen selecteert die moeten worden gesynchroniseerd.
- De optie die gebruikers toestaat om verlopen wachtwoorden opnieuw in te stellen, is niet beschikbaar.
- Het bestand `domain_krb.properties` wordt niet ondersteund.

Een LDAP-directory met de service integreren

U kunt uw bedrijfs-LDAP-directory integreren met VMware Identity Manager om gebruikers en groepen van de LDAP-directory te synchroniseren met de VMware Identity Manager-service.

Om uw LDAP-directory te integreren, maakt u een overeenkomstige VMware Identity Manager-directory aan en synchroniseert u gebruikers en groepen van uw LDAP-directory met de VMware Identity Manager-directory. U kunt een planning voor regelmatig synchroniseren instellen voor volgende updates.

U kunt ook de LDAP-kenmerken selecteren die u voor gebruikers wilt synchroniseren en deze toewijzen aan VMware Identity Manager-kenmerken.

De configuratie van uw LDAP-directory kan worden gebaseerd op standaardschema's of u kunt aangepaste schema's gebruiken. Wellicht hebt u ook gedefinieerde aangepaste kenmerken. Om VMware Identity Manager uw LDAP-directory te laten vragen om gebruikers- of groepsobjecten te verkrijgen, moet u de LDAP-zoekfilters en namen van kenmerken opgeven die van applicatie zijn op uw LDAP-directory.

In het bijzonder dient u de volgende informatie op te geven.

- LDAP-zoekfilters voor het verkrijgen van groepen, gebruikers en de Bind-gebruiker
- LDAP-kenmerknamen voor groepslidmaatschap, UUID en distinguished name

Voor de integratiefunctie van de LDAP-directory gelden bepaalde beperkingen. Zie "Beperkingen van LDAP-directory-integratie," op pagina 62.

Vereisten

- Let op: de mogelijkheid om LDAP-directory's te integreren is alleen beschikbaar bij connectorversie 2016.6.1 en hoger als u extra, externe virtual appliances met een connector gebruikt.
- Controleer de kenmerken op de pagina **Identiteits- en toegangsbeheer > Installatie > Gebruikerskenmerken** en voeg extra kenmerken toe die u wilt synchroniseren. U wijst deze VMware Identity Manager-kenmerken later toe aan uw LDAP-directorykenmerken wanneer u de directory maakt. Deze kenmerken worden gesynchroniseerd voor de gebruikers in de directory.

  Opmerking Wanneer u gebruikerskenmerken wijzigt, houd er dan rekening mee dat deze wijzigingen ook gevolgen kunnen hebben voor andere directory's in de service. Wanneer u van plan bent om zowel Active Directory als LDAP-directory's toe te voegen, let er dan op dat u geen kenmerken markeert als zijnde vereist, behalve het kenmerk **userName** dat wel kan worden gemarkeerd als zijnde vereist. De instellingen op de pagina Gebruikerskenmerken gelden voor alle directory's in de service. Wanneer een kenmerk als zijnde vereist is gemarkeerd, worden gebruikers zonder dat kenmerk niet gesynchroniseerd met de VMware Identity Manager-service.
- Een Bind-DN-gebruikersaccount. Het gebruik van een gebruikersaccount van Bind DN met een wachtwoord dat niet verloopt, wordt aanbevolen.
- In uw LDAP-directory moet de UUID van gebruikers en groepen een standaard tekstindeling hebben.
- In uw LDAP-directory moet een domeinkenmerk aanwezig zijn voor alle gebruikers en groepen.

  U kunt dit kenmerk toewijzen aan het kenmerk van het VMware Identity Manager **domein** wanneer u de VMware Identity Manager-directory aanmaakt.
- Gebruikersnamen mogen geen spaties bevatten. Wanneer een gebruikersnaam een spatie bevat, wordt de gebruiker gesynchroniseerd, maar zijn de rechten niet beschikbaar voor de gebruiker.
- Wanneer u certificaatverificatie gebruikt, moeten gebruikers waarden hebben voor userPrincipalName en e-mailadreskenmerken.

Procedure

1. Klik in de beheerconsole op het tabblad **Identiteits- en toegangsbeheer**.
2. Klik op de pagina Mappen op **Map toevoegen** en selecteer **LDAP-directory toevoegen**.

3 Voer de vereiste informatie in op de pagina LDAP-directory toevoegen.

Optie	Beschrijving
Directorynaam	Een naam voor de VMware Identity Manager-map.
Directory synchroniseren en verificatie	a In het veld **Synchronisatieconnector** selecteert u de connector die u wilt gebruiken om gebruikers en groepen te synchroniseren van uw LDAP-directory naar de directory van VMware Identity Manager. Een connectorcomponent is altijd standaard beschikbaar met de VMware Identity Manager-service. Deze connector verschijnt in het vervolgkeuzemenu. Als u meerdere VMware Identity Manager-apparaten installeert voor hoge beschikbaarheid, verschijnt de connectorcomponent van elk van die apparaten in de lijst. U hebt geen afzonderlijke connector nodig voor een LDAP-directory. Een connector kan meerdere directory's ondersteunen, ongeacht of het directory's zijn van Active Directory of LDAP. Zie 'Extra connectorappliances installeren' in de *installatiehandleiding voor VMware Identity Manager* voor de scenario's waarin u extra connectors nodig hebt. b In het veld **Verificatie** selecteert u **Ja** wanneer u deze LDAP-directory wilt gebruiken voor het verifiëren van gebruikers. Als u een externe identiteitsprovider wilt gebruiken om gebruikers te verifiëren, selecteert u **Nee**. Nadat u de directoryverbinding hebt toegevoegd om gebruikers en groepen te synchroniseren, gaat u naar de pagina **Identiteits- en toegangsbeheer > Beheren > Identiteitsproviders** om de identiteitsprovider voor verificatie toe te voegen. c In het veld **Zoekkenmerk directory** specificeert u het LDAP-directorykenmerk dat voor de gebruikersnaam wordt gebruikt. Als het kenmerk niet wordt vermeld, selecteert u **Aangepast** en typt u de kenmerknaam. Bijvoorbeeld **`cn`**.
Serverlocatie	Voer de serverhost en het poortnummer van de LDAP-directory in. Voor de serverhost kunt u de FQDN of het IP-adres specificeren. Bijvoorbeeld **`myLDAPserver.example.com`** of **`100.00.00.0`**. Als u een cluster servers achter een load-balancer hebt, voert u in plaats daarvan de informatie van de load-balancer in.

Optie	Beschrijving
LDAP-configuratie	Specificeer de zoekfilters en kenmerken van LDAP die VMware Identity Manager kan gebruiken om uw LDAP-directory op te vragen. Standaardwaarden worden verstrekt op basis van het kern-LDAP-schema. **LDAP-vragen** ■ **Groepen ophalen**: het zoekfilter om groepsobjecten te verkrijgen. Bijvoorbeeld: **`(objectClass=group)`** ■ **Bindingsgebruiker ophalen**: het zoekfilter om een bindingsgebruikerobject te verkrijgen, ofwel de gebruiker die zich aan de directory kan binden. Bijvoorbeeld: **`(objectClass=person)`** ■ **Gebruiker ophalen**: het zoekfilter om gebruikers te verkrijgen om te synchroniseren. Bijvoorbeeld:**`(&(objectClass=user)(objectCategory=person))`** **Kenmerken** ■ **Lidmaatschap**: het kenmerk dat wordt gebruikt in uw LDAP-directory om leden van een groep te definiëren. Bijvoorbeeld: **`lid`** ■ **Object-UUID**: het kenmerk dat wordt gebruikt in uw LDAP-directory om de UUID van een gebruiker of groep te definiëren. Bijvoorbeeld: **`entryUUID`** ■ **Distinguished Name**: het kenmerk dat wordt gebruikt in uw LDAP-directory voor de kenmerkende naam van een gebruiker of groep. Bijvoorbeeld: **`entryDN`**
Certificaten	Als uw LDAP-directory toegang over SSL vereist, selecteert u **Deze directory vereist dat alle verbindingen SSL gebruiken** en kopieert en plakt u het basis CA-SSL-certificaat van de LDAP-directoryserver. Zorg ervoor dat het certificaat in PEM-formaat is en neem de regels "BEGIN CERTIFICATE" en "END CERTIFICATE" op.
Gegevens van bindingsgebruiker	**Basis DN**: voer de DN in vanwaar zoekopdrachten worden gestart. Bijvoorbeeld cn=users,dc=example,dc=com **Bind DN**: voer de gebruikersnaam in die wordt gebruikt om aan de LDAP-directory te binden. **Opmerking** Het gebruik van een gebruikersaccount van Bind DN met een wachtwoord dat niet verloopt, wordt aanbevolen. **Wachtwoord Bind-DN**: voer het wachtwoord in voor de Bind DN-gebruiker.

4 Klik op **Verbinding testen** om de verbinding met de LDAP-directoryserver te testen.

Als de verbinding niet is gelukt, controleert u de informatie die u hebt ingevoerd en brengt u passende wijzigingen aan.

5 Klik op **Opslaan en Volgende**.

6 Verifieer op de pagina Domeinen of het juiste domein wordt weergegeven en klik dan op **Volgende**.

7 Verifieer op de pagina Kenmerken toewijzen of de VMware Identity Manager-kenmerken zijn toegewezen aan de juiste LDAP-kenmerken.

Belangrijk U moet een toewijzing specificeren voor het **domein**-kenmerk.

U kunt kenmerken toevoegen aan de lijst via de pagina Gebruikerskenmerken.

8 Klik op **Volgende**.

9 Op de groepspagina klikt u op **+** om de groepen te selecteren die u van de LDAP-directory wilt synchroniseren met de VMware Identity Manager-directory.

Als u meerdere groepen hebt met dezelfde naam in uw LDAP-directory, moet u unieke namen ervoor specificeren op de groepspagina.

De optie **Geneste groepsgebruikers synchroniseren** is standaard ingeschakeld. Wanneer deze optie is ingeschakeld, worden alle gebruikers gesynchroniseerd die direct tot de groep behoren die u selecteert en alle gebruikers die tot de geneste groepen eronder behoren. Let op dat de geneste groepen niet worden gesynchroniseerd; alleen de gebruikers die tot de geneste groepen behoren, worden gesynchroniseerd. In de directory van VMware Identity Manager verschijnen deze gebruikers als leden van de bovenste groep die u hebt geselecteerd om te synchroniseren. Hierdoor wordt de hiërarchie onder een geselecteerde groep platter en worden gebruikers op alle niveaus weergegeven in VMware Identity Manager als leden van de geselecteerde groep.

Als deze optie is uitgeschakeld, wanneer u een groep specificeert om te synchroniseren, worden alle gebruikers gesynchroniseerd die direct tot die groep behoren. Gebruikers die tot geneste groepen eronder behoren, worden niet gesynchroniseerd. Het uitschakelen van deze optie is handig voor grote directoryconfiguraties waar het doorkruisen van een groepsstructuur veel middelen en tijd kost. Als u deze optie uitschakelt, zorgt u ervoor dat u alle groepen selecteert waarvan u de gebruikers wilt synchroniseren.

10 Klik op **Volgende**.

11 Klik op **+** om extra gebruikers toe te voegen. Voer bijvoorbeeld `CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com` in

Om gebruikers uit te sluiten, maakt u een filter om sommige typen gebruikers uit te sluiten. U selecteert het gebruikerskenmerk waarop moet worden gefilterd, de queryregel en de waarde.

Klik op **Volgende**.

12 Geef de pagina weer om te controleren hoe veel gebruikers en groepen worden gesynchroniseerd met de directory en om het standaard synchronisatieschema te bekijken.

Klik op de koppelingen **Bewerken** om wijzigingen aan te brengen aan gebruikers en groepen of aan de synchronisatiefrequentie.

13 Klik op **Directory synchroniseren** om de synchronisatie van de directory te starten.

De verbinding met de LDAP-directory wordt tot stand gebracht en gebruikers en groepen worden gesynchroniseerd van de LDAP-directory met de VMware Identity Manager-directory. De Bind DN-gebruiker heeft standaard een beheerdersrol in VMware Identity Manager.

Een directory toevoegen na configureren van failover en redundantie

Als u een nieuwe directory toevoegt aan de VMware Identity Manager-service nadat u al een cluster hebt geïmplementeerd voor hoge beschikbaarheid, en u wilt de nieuwe directory onderdeel maken van de configuratie voor hoge beschikbaarheid, moet u de directory toevoegen aan alle apparaten in uw cluster.

Dit doet u door het connectoronderdeel van elk van de service-instanties aan de nieuwe directory toe te voegen.

Procedure

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

2 Selecteer het tabblad **Identiteits- en toegangsbeheer** en selecteer vervolgens het tabblad **Identiteitsproviders**.

3 Op de pagina Identiteitsproviders zoekt u de identiteitsprovider voor de nieuwe directory en klikt u op de naam van de identiteitsprovider.

4 In het veld **IdP-hostnaam** voert u de FQDN van de load-balancer in, als deze niet al is ingesteld op de juiste FQDN van de load-balancer.

5 In het veld **Connector(en)** selecteert u de toe te voegen connector.

6 Voer het wachtwoord in en klik op **Opslaan**.

7 Op de pagina Identiteitsproviders klikt u opnieuw op de naam van de identiteitsprovider en controleert u of het veld **IdP-hostnaam** de juiste hostnaam weergeeft. Het veld **IdP-hostnaam** moet de FQDN van de load-balancer weergeven. Als de naam onjuist is, voert u de FQDN van de load-balancer in en klikt u op **Opslaan**.

8 Herhaal de voorgaande stappen om alle connectoren toe te voegen die in het veld **Connector(en)** staan vermeld.

Opmerking Nadat u elke connector hebt toegevoegd, controleert u de IdP-hostnaam en past u deze, indien nodig, aan zoals beschreven in stap 7.

De directory is nu gekoppeld aan alle connectoren in uw implementatie.

Lokale directory's gebruiken 5

Een lokale directory is een van de typen directory's die u in de VMware Identity Manager-service kunt maken. Met een lokale directory kunt u lokale gebruikers in de service inrichten en toegang geven tot specifieke applicaties zonder dat u deze aan uw bedrijfsdirectory hoeft toe te voegen. Een lokale directory is niet verbonden met een bedrijfsdirectory en gebruikers en groepen worden niet via een bedrijfsdirectory gesynchroniseerd. In plaats daarvan maakt u lokale gebruikers rechtstreeks in de lokale directory aan.

In de service is een standaard lokale directory met de naam Systeemdirectory beschikbaar. U kunt ook meerdere nieuwe lokale directory's maken.

Systeemdirectory

De Systeemdirectory is een lokale directory die automatisch in de service wordt gemaakt wanneer deze wordt ingesteld. Deze directory heeft het domein Systeemdomein. U kunt de naam of het domein van de Systeemdirectory niet wijzigen, en geen nieuwe domeinen eraan toevoegen. Bovendien kunt u de Systeemdirectory of het Systeemdomein niet verwijderen.

De lokale beheerder die wordt gemaakt wanneer u voor de eerste keer de applicatie VMware Identity Manager instelt, wordt gemaakt in het Systeemdomein van de Systeemdirectory.

U kunt andere gebruikers aan de Systeemdirectory toevoegen. Standaard wordt de Systeemdirectory gebruikt om een paar lokale beheerders in te stellen om de service te beheren. Om eindgebruikers en extra beheerders in te richten en deze rechten te geven tot applicaties, raden wij u aan om een nieuwe lokale directory te maken.

Lokale directory's

U kunt meerdere lokale directory's maken. Elke lokale directory kan een of meerdere domeinen bevatten. Wanneer u een lokale gebruiker maakt, specificeert u de directory en het domein voor de gebruiker.

U kunt ook kenmerken selecteren voor alle gebruikers in de lokale directory. Gebruikerskenmerken zoals Gebruikersnaam, Achternaam en Voornaam worden op het algemene niveau in de VMware Identity Manager-service gespecificeerd. Er is een standaardlijst met kenmerken beschikbaar en u kunt aangepaste kenmerken toevoegen. Algemene gebruikerskenmerken gelden voor alle directory's in de service, inclusief lokale directory's. Op het niveau van de lokale directory kunt u selecteren welke kenmerken vereist zijn voor de directory. Op deze manier kunt u een aangepaste set met kenmerken hebben voor verschillende lokale directory's. Houd er rekening mee dat voor lokale directory's Gebruikersnaam, Achternaam, Voornaam en het e-mailadres altijd vereist zijn.

Opmerking De mogelijkheid om gebruikerskenmerken op directoryniveau aan te passen, is alleen beschikbaar voor lokale directory's, niet voor Active Directory- of LDAP-directory's.

Lokale directory's maken is handig in de volgende scenario's.

- U kunt een lokale directory maken voor een specifiek type gebruiker dat geen deel uitmaakt van uw bedrijfsdirectory. Bijvoorbeeld: u kunt een lokale directory maken voor partners die doorgaans geen deel uitmaken van uw bedrijfsdirectory en hen toegang geven tot alleen de specifieke applicaties die ze nodig hebben.
- U kunt meerdere lokale directory's maken als u verschillende gebruikerskenmerken of verificatiemethoden wilt voor verschillende sets gebruikers. U kunt bijvoorbeeld een lokale directory voor distributeurs maken die gebruikerskenmerken bevat zoals regio en marktaandeel, en een andere directory voor leveranciers met kenmerken zoals productcategorie en type leverancier.

Identiteitsprovider voor Systeemdirectory en Lokale directory's

Standaard wordt de Systeemdirectory die hoort bij een identiteitsprovider, Systeemidentiteitsprovider genoemd. De methode met een wachtwoord (cloud-directory) wordt standaard ingeschakeld bij deze identiteitsprovider en geldt voor het beleid default_access_policy_set voor het netwerkbereik ALL RANGES en het apparaattype Webbrowser. U kunt extra verificatiemethoden configureren en het verificatiebeleid instellen.

Wanneer u een nieuwe lokale directory maakt, hoort deze niet bij een identiteitsprovider. Nadat u de directory hebt gemaakt, maakt u een nieuwe identiteitsprovider van het type Embedded en koppelt u de directory aan deze provider. Schakel de verificatiemethode Wachtwoord (clouddirectory) in voor de identiteitsprovider. Meerdere lokale directory's kunnen aan dezelfde identiteitsprovider worden gekoppeld.

De VMware Identity Manager-connector is niet vereist voor de Systeemdirectory of voor lokale directory's die u maakt.

Raadpleeg "Gebruikersverificatie in VMware Identity Manager configureren" in *VMware Identity Manager-beheer* voor meer informatie.

Wachtwoord beheren voor gebruikers van lokale directory's

Standaard kunnen alle gebruikers van lokale directory's hun wachtwoord wijzigen in de portal of app Workspace ONE. U kunt een wachtwoordbeleid voor lokale gebruikers instellen. Indien nodig, kunt u ook wachtwoorden van lokale gebruikers resetten.

Wanneer gebruikers zich hebben aangemeld bij de portal Workspace ONE kunnen zij hun wachtwoord wijzigen door op hun naam in de rechterbovenhoek te klikken, dan **Account** in het vervolgkeuzemenu te selecteren en vervolgens op de koppeling **Wachtwoord wijzigen** te klikken. In de app Workspace ONE kunnen gebruikers hun wachtwoord wijzigen door op het menupictogram met drie streepjes te klikken en **Wachtwoord** te selecteren.

Raadpleeg "Gebruikers en Groepen beheren" in *VMware Identity Manager-beheer* voor informatie over het beleid voor het instellen van wachtwoorden en het resetten van wachtwoorden van lokale gebruikers.

Dit hoofdstuk omvat de volgende onderwerpen:

- "Een lokale directory maken," op pagina 70
- "Instellingen voor lokale directory wijzigen," op pagina 75
- "Een lokale directory verwijderen," op pagina 76

Een lokale directory maken

Als u een lokale directory wilt maken, geeft u de gebruikerskenmerken op voor de directory, maakt u de directory en identificeert u deze met een identiteitsprovider.

1 Gebruikerskenmerken instellen op globaal niveau op pagina 71

Voordat u een lokale directory maakt, bekijkt u de globale gebruikerskenmerken op de pagina Gebruikerskenmerken en voegt u zo nodig aangepaste kenmerken toe.

2 Lokale directory maken op pagina 72

Nadat u de algemene gebruikerskenmerken heeft gecontroleerd en ingesteld, maakt u de lokale directory.

3 De lokale directory koppelen aan een identiteitsprovider op pagina 74

Koppel de lokale directory aan een identiteitsprovider zodat gebruikers in de directory kunnen worden geverifieerd. Maak een nieuwe identiteitsprovider van het type Embedded en schakel de verificatiemethode Wachtwoord (lokale directory) hiervoor in.

Gebruikerskenmerken instellen op globaal niveau

Voordat u een lokale directory maakt, bekijkt u de globale gebruikerskenmerken op de pagina Gebruikerskenmerken en voegt u zo nodig aangepaste kenmerken toe.

Gebruikerskenmerken, zoals voornaam, achternaam, e-mailadres en domein, maken deel uit van het profiel van een gebruiker. In de VMware Identity Manager-service worden gebruikerskenmerken gedefinieerd op het globale niveau en toegepast op alle directory's in de service, waaronder lokale directory's. Op het lokale directoryniveau kunt u overschrijven dat een kenmerk vereist of optioneel is voor gebruikers in die lokale directory, maar u kunt geen aangepaste kenmerken toevoegen. Als een kenmerk is vereist, moet u er een waarde voor opgeven wanneer u een gebruiker maakt.

De volgende woorden kunnen niet worden gebruikt wanneer u aangepaste kenmerken maakt.

Tabel 5-1. Woorden die niet kunnen worden gebruikt als Namen voor aangepaste kenmerken

actief	adressen	kostencentrum
afdeling	weergavenaam	divisie
e-mails	medewerkersnummer	rechten
externe id	groepen	id
ims	plek	manager
meta	naam	bijnaam
organisatie	wachtwoord	telefoonnummer
foto's	voorkeurstaal	profiel-URL
rollen	tijdzone	titel
userName	type gebruiker	x509-certificaat

Opmerking De mogelijkheid om gebruikerskenmerken over te schrijven op directoryniveau is alleen van toepassing op lokale directory's, niet op Active Directory of LDAP-directory's.

Procedure

1 Klik in de beheerconsole op de tab **Identiteits- en toegangsbeheer**.

2 Klik op **Instellen** en klik vervolgens op de tab **Gebruikerskenmerken**.

3 Bekijk de lijst met gebruikerskenmerken en voeg zo nodig extra kenmerken toe.

Opmerking Hoewel u op deze pagina kunt selecteren welke kenmerken zijn vereist, wordt u aanbevolen de selectie voor lokale directory's te maken op het niveau van de lokale directory. Als een kenmerk op deze pagina is gemarkeerd als vereist, is het van toepassing op alle directory's in de service, inclusief Active Directory- of LDAP-directory's.

4 Klik op **Opslaan**.

Wat nu te doen

Maak de lokale directory.

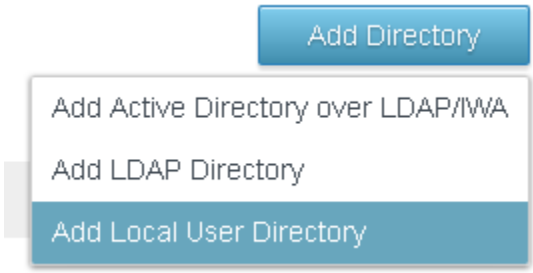
Lokale directory maken

Nadat u de algemene gebruikerskenmerken heeft gecontroleerd en ingesteld, maakt u de lokale directory.

Procedure

1 Klik in de beheerconsole op het tabblad **Identiteits- en toegangsbeheer** en klik dan op het tabblad **Directory's**.

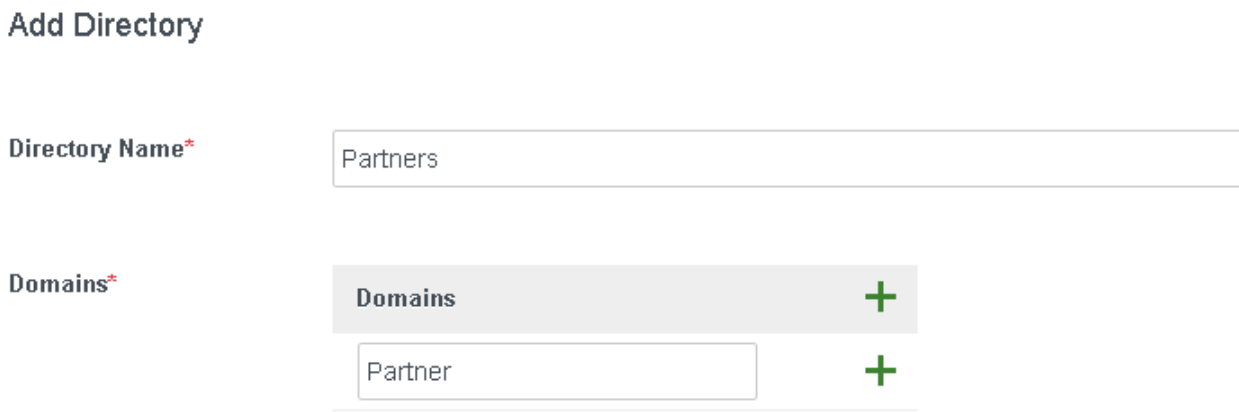
2 Klik op **Directory toevoegen** en selecteer **Lokale gebruikersdirectory toevoegen** via het vervolgkeuzemenu.



3 Op de pagina Directory toevoegen, voert u een directorynaam in en specificeert u minimaal één domeinnaam.

De domeinnaam moet uniek zijn voor alle directory's in de service.

Bijvoorbeeld:



4 Klik op **Opslaan**.

5 Klik op de pagina Directory's op de nieuwe directory.

6 Klik op het tabblad **Gebruikerskenmerken**.

Alle kenmerken van de pagina Identiteits- en toegangsbeheer > Installatie > Gebruikerskenmerken worden voor de lokale directory vermeld. Kenmerken die op deze pagina als vereist zijn aangeduid, worden ook als vereist weergegeven op de pagina van de lokale directory.

7 Kenmerken voor de lokale directory aanpassen.

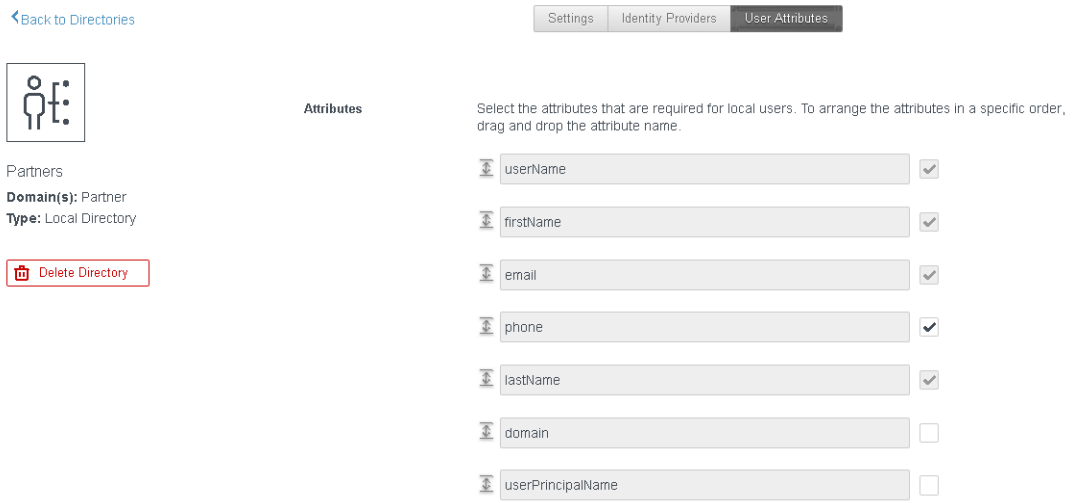
U kunt specificeren welke kenmerken vereist en welke kenmerken optioneel zijn. U kunt ook de volgorde wijzigen waarin de kenmerken worden weergegeven.

Belangrijk De kenmerken Gebruikersnaam, Voornaam, Achternaam en E-mailadres zijn altijd vereist voor lokale directory's.

- Om een kenmerk vereist te maken, selecteert u het selectievakje naast de naam van het kenmerk.
- Om een kenmerk optioneel te maken, deselecteert u het selectievakje naast de naam van het kenmerk.
- Om de volgorde van de kenmerken te wijzigen, klikt u op een kenmerk en sleept u het naar de nieuwe locatie.

Wanneer een kenmerk vereist is, moet u een waarde voor het kenmerk specificeren wanneer u een gebruiker maakt.

Bijvoorbeeld:



8 Klik op **Opslaan**.

Wat nu te doen

Koppel de lokale directory aan de identiteitsprovider die u wilt gebruiken om de gebruikers in de directory te verifiëren.

De lokale directory koppelen aan een identiteitsprovider

Koppel de lokale directory aan een identiteitsprovider zodat gebruikers in de directory kunnen worden geverifieerd. Maak een nieuwe identiteitsprovider van het type Embedded en schakel de verificatiemethode Wachtwoord (lokale directory) hiervoor in.

Opmerking Gebruik niet de ingebouwde identiteitsprovider. Het inschakelen van de verificatiemethode Wachtwoord (lokale directory) voor de ingebouwde identiteitsprovider wordt niet aanbevolen.

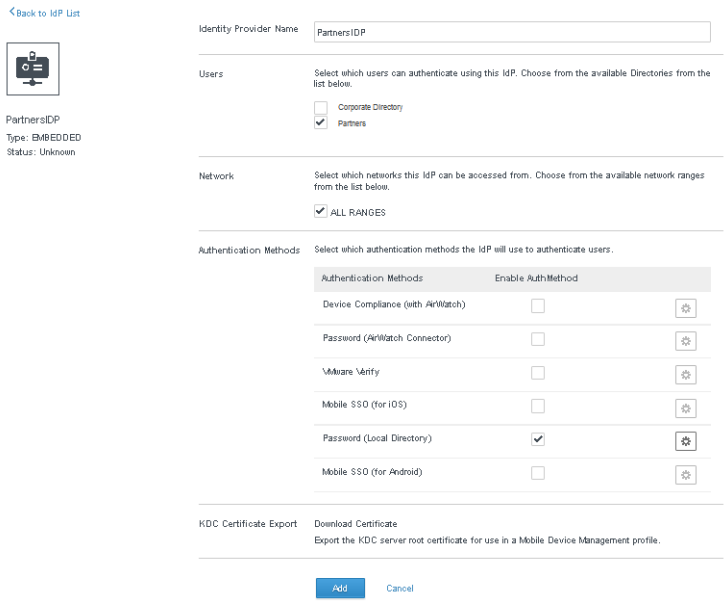
Procedure

1 Klik op het tabblad **Identiteits- en toegangsbeheer** op de tab **Identiteitsproviders**.

2 Klik op **Identiteitsprovider toevoegen** en selecteer **Ingebouwde IdP maken**.

3 Geef de volgende informatie op.

Optie	Beschrijving
Naam van identiteitsprovider	Geef een naam op voor de identiteitsprovider.
Gebruikers	Selecteer de lokale directory die u hebt gemaakt.
Netwerk	Selecteer de netwerken voor toegang tot deze identiteitsprovider.
Verificatiemethoden	Selecteer Wachtwoord (lokale directory).
KDC-certificaat exporteren	U hoeft het certificaat niet te downloaden tenzij u mobiele SSO configureert voor iOS-apparaten die worden beheerd met AirWatch.



4 Klik op **Toevoegen**.

De identiteitsprovider wordt gemaakt en gekoppeld aan de lokale directory. Later kunt u andere verificatiemethoden configureren voor deze identiteitsprovider. Zie "Gebruikersverificatie configureren in VMware Identity Manager" in *Beheer VMware Identity Manager* voor meer informatie over verificatie.

U kunt dezelfde identiteitsprovider gebruiken voor meerdere lokale directory's.

Wat nu te doen

Maak lokale gebruikers en groepen. U maakt lokale gebruikers en groepen op het tabblad **Gebruikers en groepen** van de beheerconsole. Zie 'Gebruikers en groepen beheren' in *Beheer VMware Identity Manager Administration* voor meer informatie.

Instellingen voor lokale directory wijzigen

Nadat u een lokale directory hebt gemaakt, kunt u de bijbehorende instellingen op elk gewenst moment wijzigen.

U kunt de volgende instellingen wijzigen.

- Wijzig de directorynaam.
- Voeg of verwijder domeinen of wijzig hun naam.
  - De domeinnamen moeten uniek zijn voor alle directory's in de service.
  - Wanneer u een domeinnaam wijzigt, worden de gebruikers die waren gekoppeld aan het oude domein, gekoppeld aan het nieuwe domein.
  - De directory moet ten minste één domein hebben.
  - U kunt geen domein toevoegen aan de systeemdirectory of het systeemdomein verwijderen.
- Voeg nieuwe gebruikerskenmerken toe of maak een bestaand kenmerk vereist of optioneel.
  - Als de lokale directory nog geen gebruikers heeft, kunt u nieuwe kenmerken toevoegen als optioneel of vereist en bestaande kenmerken wijzigen in vereist of optioneel.
  - Als u al gebruikers hebt gemaakt in de lokale directory, kunt u nieuwe kenmerken alleen toevoegen als optionele kenmerken en bestaande kenmerken wijzigen van vereist in optioneel. U kunt een optioneel kenmerk niet vereist maken nadat gebruikers zijn gemaakt.

- De kenmerken Gebruikersnaam, Voornaam, Achternaam en E-mailadres zijn altijd vereist voor lokale directory's.
- Omdat gebruikerskenmerken worden gedefinieerd op algemeen niveau in de VMware Identity Manager-service, worden alle nieuwe kenmerken die u toevoegt, weergegeven in alle directory's in de service.

- Wijzig de volgorde waarin kenmerken worden weergegeven.

Procedure

1 Klik op de tab **Identiteits- en toegangsbeheer**.

2 Klik op de pagina Directory's op de directory die u wilt bewerken.

3 Bewerk de instellingen voor de lokale directory.

Optie	Actie
De directorynaam wijzigen	a Bewerk de directorynaam op het tabblad **Instellingen**. b Klik op **Opslaan**.
Een domein toevoegen, verwijderen of hernoemen	a Bewerk de lijst **Domeinen** op het tabblad **Instellingen**. b Klik op het groene pluspictogram om een domein toe te voegen. c Klik op het rode verwijderpictogram om een domein te verwijderen. d Bewerk de domeinnaam in het tekstvak om de naam van een domein te wijzigen.
Gebruikerskenmerken toevoegen aan de directory	a Klik op de tab **Identiteits- en toegangsbeheer** en klik vervolgens op **Installatie**. b Klik op de tab **Gebruikerskenmerken**. c Voeg kenmerken toe aan de lijst **Andere kenmerken toevoegen om te gebruiken** en klik op **Opslaan**.
Een kenmerk vereist of optioneel maken voor de directory	a Klik op de tab **Identiteits- en toegangsbeheer** en klik vervolgens op de tab **Directory's**. b Klik op de naam van de lokale directory en klik op de tab **Gebruikerskenmerken**. c Schakel het selectievakje in naast een kenmerk om het vereist te maken of schakel het selectievakje uit om het kenmerk optioneel te maken. d Klik op **Opslaan**.
De volgorde van de kenmerken wijzigen	a Klik op de tab **Identiteits- en toegangsbeheer** en klik vervolgens op de tab **Directory's**. b Klik op de naam van de lokale directory en klik op de tab **Gebruikerskenmerken**. c Klik en sleep de kenmerken naar de nieuwe positie. d Klik op **Opslaan**.

Een lokale directory verwijderen

U kunt een lokale directory verwijderen die u hebt gemaakt in de VMware Identity Manager-service. U kunt de systeemdirectory verwijderen, die standaard wordt gemaakt wanneer u de service voor het eerst instelt.

Voorzichtig Wanneer u een directory verwijdert, worden ook alle gebruikers in de directory verwijderd uit de service.

Procedure

1 Klik op de tab **Identiteits- en toegangsbeheer** en klik vervolgens op de tab **Directory's**.

2 Klik op de directory die u wilt verwijderen.

3 Klik op **Directory verwijderen** op de directorypagina.

Geavanceerde configuratie voor het VMware Identity Manager -apparaat

6

Nadat u de basisinstallatie van de virtual appliance van VMware Identity Manager hebt voltooid, moet u mogelijk andere configuratietaken uitvoeren, zoals externe toegang tot de VMware Identity Manager mogelijk maken en redundantie configureren.

Het architectuurschema van VMware Identity Manager toont hoe u de VMware Identity Manager-omgeving kunt implementeren. Zie Hoofdstuk 1, "Installatie van VMware Identity Manager voorbereiden," op pagina 9 voor een typische implementatie.

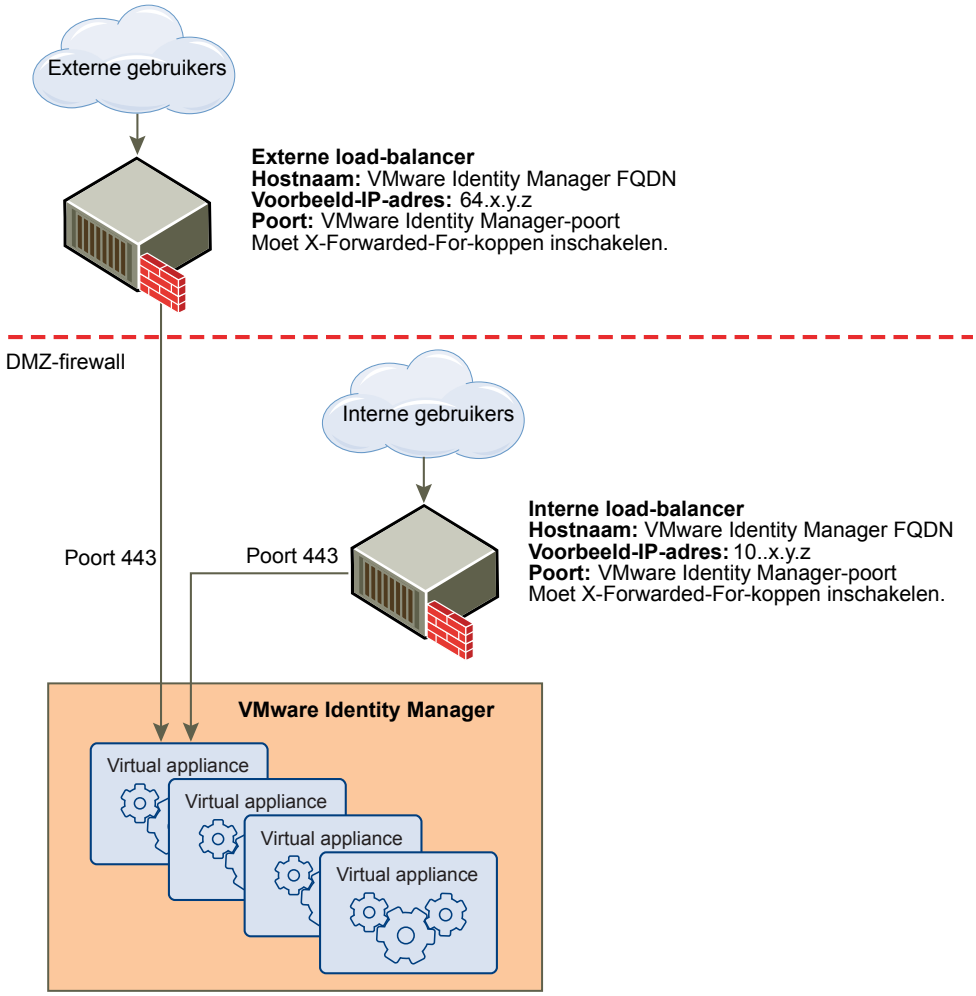
Dit hoofdstuk omvat de volgende onderwerpen:

Een load-balancer of reverse proxy gebruiken om externe toegang tot VMware Identity Manager in te schakelen

Tijdens de implementatie wordt de virtual VMware Identity Manager -appliance ingesteld in het interne netwerk. Als u wilt dat gebruikers van buiten het netwerk verbinding kunnen maken met de service, moet u een load-balancer of een reverse proxy in de DMZ installeren, zoals Apache, nginx, F5, enz.

Als u geen load-balancer of reverse proxy gebruikt, kunt u het aantal VMware Identity Manager-toepassingen later niet uitbreiden. Wellicht moet u meer applicaties toevoegen om redundantie en load balancing te kunnen bieden. In het volgende diagram wordt de basisimplementatiearchitectuur getoond die u kunt gebruiken om externe toegang in te schakelen.

Figuur 6-1. Externe load-balancerproxy met virtual machine



De VMware Identity Manager -FQDN opgeven tijdens de implementatie

Tijdens de implementatie van de VMware Identity Manager -virtual machine voert u de VMware Identity Manager FQDN en het poortnummer in. Deze waarden moeten naar de hostnaam verwijzen waarvan u wilt dat deze toegankelijk is voor eindgebruikers.

De VMware Identity Manager -virtual machine wordt altijd uitgevoerd op poort 443. U kunt een ander poortnummer voor de load-balancer gebruiken. Als u een ander poortnummer gebruikt, moet u dit opgeven tijdens de implementatie.

Instellingen voor de load-balancer die moeten worden geconfigureerd.

Instellingen voor de load-balancer die moeten worden geconfigureerd zijn onder andere het inschakelen van de X-Forwarded-For-koppen, het op de juiste manier instellen van de time-out van de load-balancer en het inschakelen van sticky-sessies. Bovendien moet SSL-vertrouwen worden geconfigureerd tussen de VMware Identity Manager-virtual appliance en de load-balancer.

- 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 VMware Identity Manager moet u de standaardtime-out voor load-balancer-verzoeken verhogen. De waarde is ingesteld in minuten. Als de time-outinstelling te laag is, wordt wellicht de volgende foutmelding 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 VMware Identity Manager-applicaties heeft. De load-balancer bindt vervolgens de sessie van een gebruiker aan een specifieke instantie.

Het basiscertificaat van VMware Identity Manager toepassen op de load-balancer

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

Het certificaat van VMware Identity Manager kunt u downloaden van de beheerconsole vanaf de pagina **Appliance-instellingen > VA-configuratie > Configuratie beheren**.

Als de FQDN van VMware Identity Manager naar een load-balancer wijst, kan het SSL-certificaat uitsluitend worden toegepast op de load-balancer.

Aangezien de load-balancer met de virtual appliance van VMware Identity Manager communiceert, moet u het basis CA-certificaat van VMware Identity Manager kopiëren naar de load-balancer als een vertrouwd basiscertificaat.

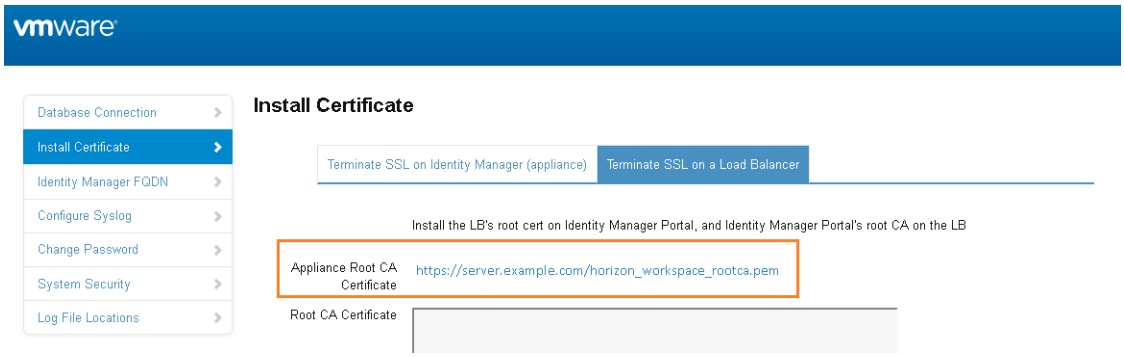
Procedure

1 In de beheerconsole selecteert u het tabblad **Appliance-instellingen** en selecteert u **VA-configuratie**.

2 Klik op **Configuratie beheren**.

3 Selecteer **Certificaat installeren**.

4 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`.



5 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 documenten die worden verstrekt door de verkoper van uw load-balancer.

Wat nu te doen

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

Basiscertificaat van load-balancer toepassen op VMware Identity Manager

Wanneer de virtual appliance van VMware Identity Manager met de load-balancer is geconfigureerd, moet u vertrouwen wekken tussen de load-balancer en VMware Identity Manager. Naast het kopiëren van het basiscertificaat van VMware Identity Manager naar de load-balancer, moet u het basiscertificaat van de load-balancer kopiëren naar VMware Identity Manager.

Procedure

1 Basiscertificaat van load-balancer verkrijgen

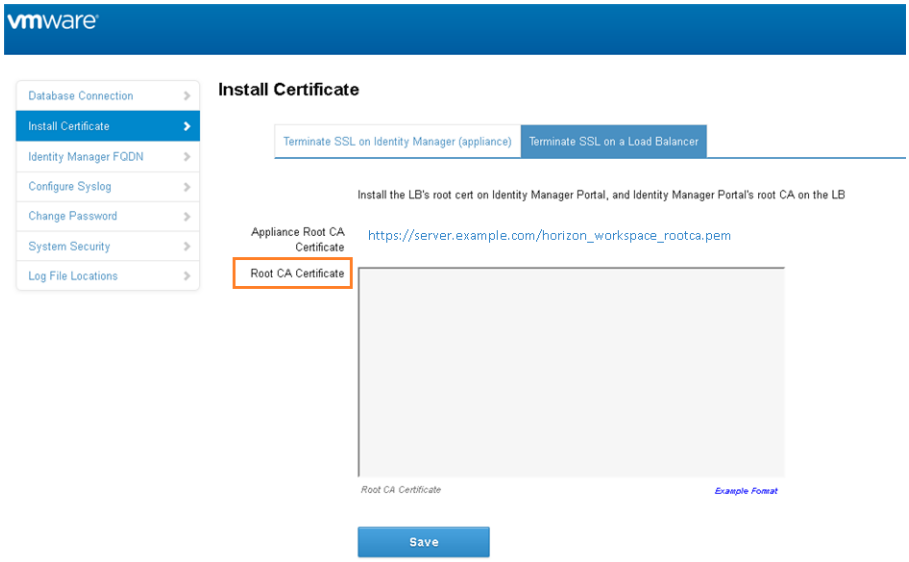
2 In de beheerconsole VMware Identity Manager selecteert u het tabblad **Appliance-instellingen** en selecteert u **VA-configuratie**.

3 Klik op **Configuratie beheren**.

4 Meld u aan met het wachtwoord van de beheerdersgebruiker.

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

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



7 Klik op **Opslaan**.

Proxyserverinstellingen instellen voor VMware Identity Manager

De VMware Identity Manager virtual appliance heeft toegang tot de applicatiescatalogus in de cloud en andere webservices op internet. Als uw netwerkconfiguratie internettoegang biedt via een HTTP-proxy, moet u uw proxy-instellingen aanpassen in de VMware Identity Manager-apparaat.

Schakel uw proxy in om alleen internetverkeer te verwerken. Als u er zeker van wilt zijn dat de proxy goed is ingesteld, moet u de parameter voor intern verkeer binnen het domein instellen op `no-proxy`.

Opmerking Proxyservers waarvoor verificatie is vereist, worden niet ondersteund.

Procedure

1 Meld u via de vSphere Client aan als hoofdgebruiker bij de VMware Identity Manager virtual appliance.

2 Voer `YaST` in op de opdrachtregel om het hulpprogramma `YaST` uit te voeren.

3 Selecteer **Netwerkservices** in het linkerdeelvenster en selecteer **Proxy**.

4 Voer in de velden **URL HTTP-proxy** en **URL HTTPS-proxy** de URL's van de proxyserver in.

5 Selecteer **Voltooien** en sluit het hulpprogramma `YaST` af.

6 Herstart de Tomcat-server op de VMware Identity Manager virtual appliance om de nieuwe proxy-instellingen te gebruiken.

```
service horizon-workspace restart
```

De catalogus met cloudapplicaties en andere webservices is nu beschikbaar in VMware Identity Manager.

Failover en redundantie in een enkel datacenter configureren

U kunt meerdere virtual VMware Identity Manager-appliances in een cluster toevoegen voor failover en redundantie. Als een van de virtual appliances om een bepaalde reden wordt afgesloten, is VMware Identity Manager nog steeds beschikbaar.

Eerst installeert en configureert u een virtual VMware Identity Manager-appliance en dan kloont u deze. Het klonen van de virtual appliance creëert een duplicaat van het apparaat met dezelfde configuratie als van het originele apparaat. U kunt de gekloonde virtual appliance aanpassen om de naam, de netwerkinstellingen en andere eigenschappen, indien nodig, te wijzigen.

Voordat u de virtual appliance van VMware Identity Manager kloont, moet u deze achter een load-balancer configureren en de Fully Qualified Domain Name (FQDN) wijzigen om overeen te komen met de FQDN van de load-balancer. Voltooi ook de configuratie van de directory in de VMware Identity Manager-service voordat u apparaat kloont.

Na het klonen wijst u een nieuw IP-adres toe aan de gekloonde virtual appliance voordat u deze inschakelt. Het IP-adres van de gekloonde virtual appliance moet dezelfde richtlijnen volgen als het IP-adres van de originele virtual appliance. Het IP-adres moet leiden tot een geldige hostnaam met behulp van forward- en reverse DNS.

Alle nodes in het VMware Identity Manager-cluster zijn identiek en bijna staatloze kopieën van elkaar. Synchroniseren naar Active Directory en naar bronnen die worden geconfigureerd, zoals View of ThinApp, is uitgeschakeld op de gekloonde virtual appliances.

1 Aanbevolen aantal nodes in VMware Identity Manager-cluster op pagina 82

   U wordt aangeraden een VMware Identity Manager-cluster met drie nodes in te stellen.

2 Wijzig FQDN van VMware Identity Manager in FQDN van load-balancer op pagina 82

   Voordat u de virtual appliance van VMware Identity Manager kloont, moet u de Fully Qualified Domain Name (FQDN) wijzigen, zodat deze overeenkomt met de FQDN van de load-balancer.

3 De virtual appliance klonen op pagina 83

4 Een nieuw IP-adres toewijzen aan gekloonde virtual appliance op pagina 84

   U moet een nieuw IP-adres toewijzen aan elke gekloonde virtual appliance voordat u deze inschakelt. Het IP-adres moet kunnen worden opgelost in DNS. Als het adres zich niet in de reverse DNS bevindt, moet u ook de hostnaam toewijzen.

5 Synchronisatie van directory's inschakelen op een andere -instantie in geval van een fout op pagina 86

6 Een knooppunt verwijderen uit een cluster op pagina 87

   Als een knooppunt in een VMware Identity Manager-cluster niet correct werkt en u het niet kunt herstellen, kunt u het verwijderen uit de cluster met de opdracht Knooppunt verwijderen. De opdracht verwijdert de knooppuntvermeldingen uit de VMware Identity Manager-database.

Aanbevolen aantal nodes in VMware Identity Manager -cluster

U wordt aangeraden een VMware Identity Manager-cluster met drie nodes in te stellen.

Het VMware Identity Manager-apparaat bevat Elasticsearch, een zoek- en analysemachine. Elasticsearch heeft een bekende beperking bij clusters met twee nodes. Voor een beschrijving van de "split brain"-beperking van Elasticsearch, raadpleegt u de Elasticsearch-documentatie. Houd er rekening mee dat u geen Elasticsearch-instellingen hoeft te configureren.

Een VMware Identity Manager-cluster met twee nodes biedt mogelijkheden voor failover met een paar beperkingen in vergelijking met Elasticsearch. Als een van de nodes uitvalt, zijn de volgende beperkingen van toepassing tot de node weer wordt ingeschakeld:

- Op het dashboard worden geen gegevens weergegeven.
- De meeste rapporten zijn niet beschikbaar.
- Synchronisatielogboekgegevens van directory's worden niet weergegeven.
- Het zoekveld in de rechterbovenhoek van de beheerconsole geeft geen resultaten weer.
- Automatisch aanvullen is niet beschikbaar voor tekstvelden.

Er gaan geen gegevens verloren gedurende de tijd dat de node is afgesloten. Gegevens van audit-gebeurtenissen en synchronisatielogboeken worden opgeslagen en worden weergegeven wanneer de node is hersteld.

Wijzig FQDN van VMware Identity Manager in FQDN van load-balancer

Voordat u de virtual appliance van VMware Identity Manager kloont, moet u de Fully Qualified Domain Name (FQDN) wijzigen, zodat deze overeenkomt met de FQDN van de load-balancer.

Vereisten

- Het VMware Identity Manager-apparaat wordt toegevoegd aan een load-balancer.
- U hebt het basis CA-certificaat van de load-balancer toegepast op VMware Identity Manager.

Procedure

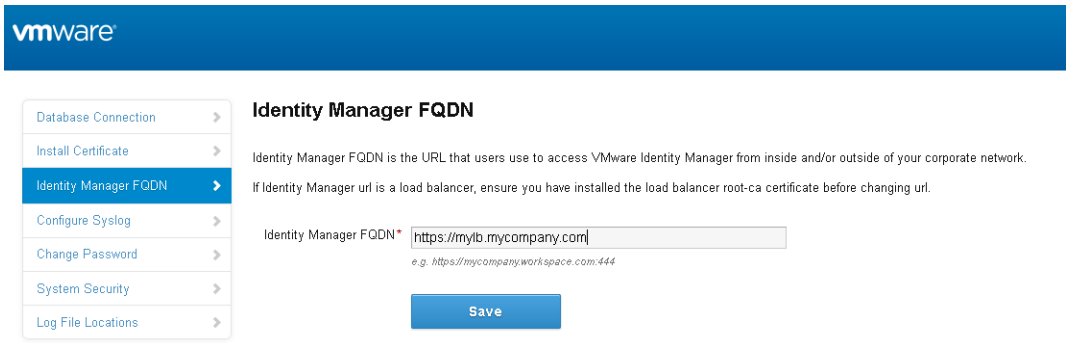
1. Meld u aan op de beheerconsole van VMware Identity Manager.
2. Selecteer het tabblad **Appliance-instellingen**.
3. Op de pagina Configuratie van virtual appliance klikt u op **Configuratie beheren**.
4. Voer uw beheerderswachtwoord in om u aan te melden.
5. Klik op **Identity Manager configuratie**.
6. In het veld **Identity Manager FQDN** wijzigt u het hostnaamdeel van de URL van de hostnaam van VMware Identity Manager in de hostnaam van de load-balancer.

   Als uw hostnaam van VMware Identity Manager bijvoorbeeld `myservice` is en de hostnaam van uw load-balancer is `mylb`, wijzigt u de URL

   ```
   https://myservice.mycompany.com
   ```

   als volgt:

   ```
   https://mylb.mycompany.com
   ```



7 Klik op **Opslaan**.

- De FQDN van de service is gewijzigd in de FQDN van de load-balancer.
- De URL van de identiteitsprovider is gewijzigd in de URL van de load-balancer.

Wat nu te doen

Kloon de virtual appliance.

De virtual appliance klonen

Kloon de virtual appliance van VMware Identity Manager om meerdere virtual appliances van hetzelfde type te maken om verkeer te verdelen en mogelijke uitvaltijd te voorkomen.

Het gebruik van meerdere virtual appliances van VMware Identity Manager verbetert de beschikbaarheid, verzoeken van de load-balancer aan de service, en vermindert de reactietijden naar de eindgebruiker.

Vereisten

- De virtual appliance van VMware Identity Manager moet achter een load-balancer worden geconfigureerd. Zorg ervoor dat de poort van de load-balancer 443 is. Gebruik niet 8443, omdat dit poortnummer de beheerderspoort is en uniek is voor elke virtual appliance.
- Een externe database wordt geconfigureerd zoals beschreven in "Aan de database koppelen," op pagina 34.
- Zorg ervoor dat u de directory-configuratie in VMware Identity Manager voltooit.
- Meld u aan op de console van de virtual appliance als hoofdgebruiker en verwijder het bestand `/etc/udev/rules.d/70-persistent-net.rules`, als dat bestaat. Als u dit bestand niet verwijdert vóór het klonen, wordt de netwerkvoorziening niet correct geconfigureerd op de gekloonde virtual appliance.

Procedure

1 Meld u aan op de vSphere Client of vSphere Web Client en navigeer naar de virtual appliance van VMware Identity Manager.

2 Klik met de rechter muisknop op de virtual appliance en selecteer **Klonen**.

3 Voer de naam in voor de gekloonde virtual appliance en klik op **Volgende**.

De naam moet uniek zijn binnen de VM-map.

4 Selecteer de host of cluster waarop de gekloonde virtual appliance wordt uitgevoerd en klik op **Volgende**.

5 Selecteer de brongroep waarin de gekloonde virtual appliance wordt uitgevoerd en klik op **Volgende**.

6 Voor het virtuele schijfformaat selecteert u **Zelfde formaat als bron**.

7 Selecteer de data-opslaglocatie waar u de bestanden van de virtual appliance wilt opslaan en klik op **Volgende**.

8 Selecteer **Niet aanpassen** als de optie gastbesturingssysteem.

9 Herzie de opties en klik op **Voltooien**.

De gekloonde virtual appliance is geïmplementeerd. U kunt de virtual appliance niet gebruiken of bewerken totdat het klonen is voltooid.

Wat nu te doen

Wijs een IP-adres toe aan de gekloonde virtual appliance voordat u deze inschakelt en toevoegt aan de load-balancer.

Een nieuw IP-adres toewijzen aan gekloonde virtual appliance

U moet een nieuw IP-adres toewijzen aan elke gekloonde virtual appliance voordat u deze inschakelt. Het IP-adres moet kunnen worden opgelost in DNS. Als het adres zich niet in de reverse DNS bevindt, moet u ook de hostnaam toewijzen.

Procedure

1 In de vSphere Client of de vSphere Web Client selecteert u de gekloonde virtual appliance.

2 Op het tabblad **Samenvatting** klikt u onder**Opdrachten** op **Instellingen bewerken**.

3 Selecteer **Opties** en selecteer in de lijst **vApp-opties Eigenschappen**.

4 Wijzig het IP-adres in het veld **IP-adres**.

5 Als het IP-adres zich niet in de reverse DNS bevindt, voegt u de hostnaam toe in het tekstveld **Hostnaam**.

6 Klik op **OK**.

7 Schakel de gekloonde applicatie in en wacht tot het blauwe aanmeldscherm verschijnt op het tabblad **Console**.

Belangrijk Voordat u de gekloonde applicatie inschakelt, zorgt u ervoor dat het originele apparaat volledig is ingeschakeld.

Wat nu te doen

- Wacht een paar minuten tot de Elasticsearch-cluster is gemaakt, voordat u de gekloonde virtual appliance toevoegt aan de load-balancer.

  Elasticsearch, een zoek- en analyse-engine, is geïntegreerd in de virtual appliance.

  a Meld u aan op de gekloonde virtual appliance.

  b Controleer de Elasticsearch-cluster:

  ```
  curl –XGET 'http://localhost:9200/_cluster/health?pretty=true'
  ```

  Verifieer of het resultaat overeenkomt met het aantal nodes.

- Voeg de gekloonde virtual appliance toe aan de load-balancer en configureer de load-balancer om verkeer te verspreiden. Raadpleeg de documentatie van uw leverancier van de load-balancer voor informatie.

- Als u een domein hebt toegevoegd aan de originele service-instantie, moet u het domein toevoegen aan de gekloonde service-instanties.

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

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

Het connectoronderdeel van elk van de gekloonde service-instanties wordt vermeld op de Connectorpagina.

c Voor elke vermelde connector, klikt u op **Aan domein toevoegen** en specificeert u de domeingegevens.

Voor meer informatie over Active Directory, raadpleegt u "Met Active Directory integreren," op pagina 47.

- Voor directory's van het type geïntegreerde Windows-verificatie (IWA) moet u het volgende doen:

  a Voor de gekloonde service-instanties voegt u het domein toe waaraan de IWA-directory in de originele service-instantie is toegevoegd.

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

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

  Het connectoronderdeel van elk van de gekloonde service-instanties wordt vermeld op de Connectorpagina.

  3 Voor elke vermelde connector, klikt u op **Aan domein toevoegen** en specificeert u de domeingegevens.

  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.

- Als u het bestand `/etc/krb5.conf` handmatig hebt bijgewerkt in de originele service-instantie, bijvoorbeeld om storingen of vertraging bij weergavesynchronisatie te verhelpen, moet u het bestand in de gekloonde instantie bijwerken nadat de gekloonde instantie is toegevoegd aan het domein. Voer de volgende taken uit in alle gekloonde service-instanties.

  a Bewerk het bestand `/etc/krb5.conf` en werk het gedeelte `realms` bij om dezelfde domein-naar-host-waarden op te geven die worden gebruikt in het bestand `/usr/local/horizon/conf/domain_krb.properties`. U hoeft het poortnummer niet op te geven. Als het bestand `domain_krb.properties` bijvoorbeeld de domeinvermelding `example.com=examplehost.example.com:389` heeft, werkt u het bestand `krb5.conf` als volgt bij.

```
[realms]
GAUTO-QA.COM = {
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO2QA\.GAUTO-QA\.COM\\.*)s/^GAUTO2QA\.GAUTO-
QA\.COM/GAUTO2QA/
auth_to_local = RULE:[1:$0\$1](^GLOBEQE\.NET\\.*)s/^GLOBEQE\.NET/GLOBEQE/
auth_to_local = DEFAULT
kdc = examplehost.example.com
}
```

Opmerking Het is mogelijk om meerdere kdc-vermeldingen te hebben. Dit is echter geen vereiste omdat er in de meeste gevallen slechts één kdc-waarde is. Als u ervoor kiest om extra kdc-waarden te definiëren, heeft elke regel een kdc-vermelding die een domeincontroller definieert.

  b Start de werkruimteservice opnieuw.

```
service horizon-workspace restart
```

Opmerking Raadpleeg ook Knowledge Base-artikel 2091744.

- Schakel de verificatiemethoden in die zijn geconfigureerd voor Connector op elk van de gekloonde instanties. Raadpleeg de *VMware Identity Manager Administration Guide* voor informatie.

De virtual appliance van de VMware Identity Manager-service is nu in hoge mate beschikbaar. Verkeer wordt verspreid naar de virtual appliances in uw cluster op basis van de configuratie van de load-balancer. Verificatie naar de service is in hoge mate beschikbaar. Voor de directorysynchronisatiefunctie van de service moet u echter, in geval van een service-instantiefout, handmatig directorysynchronisatie inschakelen op een gekloonde service-instantie. Directorysynchronisatie wordt door het connectoronderdeel van de service afgehandeld en kan slechts op één connector tegelijk worden ingeschakeld. Zie "Synchronisatie van directory's inschakelen op een andere -instantie in geval van een fout," op pagina 86.

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

In het geval dat er fouten optreden met een service-instantie, wordt de verificatie automatisch afgehandeld door een gekloonde instantie, zoals geconfigureerd in de load-balancer. Voor het synchroniseren van directory's moet u de directory-instellingen in de VMware Identity Manager-service wijzigen om een gekloonde instantie te kunnen gebruiken. Directorysynchronisatie wordt door het connectoronderdeel van de service afgehandeld en kan slechts op één connector tegelijk worden ingeschakeld.

Procedure

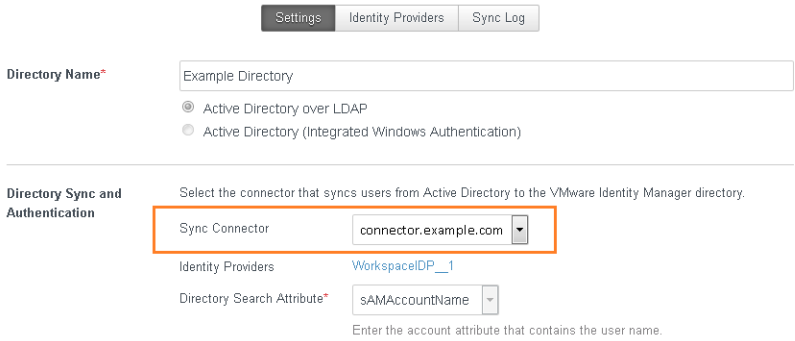
1 Meld u aan op de beheerconsole van VMware Identity Manager.

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 service-instantie.

U kunt deze informatie bekijken op de pagina **Installatie > Connectoren**. Op de pagina wordt het connectoronderdeel van elk van de virtual appliances van de service in uw cluster vermeld.

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



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

6 Klik op **Opslaan**.

Een knooppunt verwijderen uit een cluster

Als een knooppunt in een VMware Identity Manager-cluster niet correct werkt en u het niet kunt herstellen, kunt u het verwijderen uit de cluster met de opdracht Knooppunt verwijderen. De opdracht verwijdert de knooppuntvermeldingen uit de VMware Identity Manager-database.

U kunt de status van de knooppunten in uw cluster controleren in het Dashboard voor systeemdiagnose. Het bericht `Het huidige knooppunt heeft een ongeldige status` geeft aan dat het knooppunt niet correct werkt.

Belangrijk Maak spaarzaam gebruik van de opdracht Knooppunt verwijderen. Gebruik deze alleen als een knooppunt een onherstelbare status heeft en volledig moet worden verwijderd uit de VMware Identity Manager-implementatie.

Opmerking U kunt de opdracht Knooppunt verwijderen niet gebruiken om het laatste knooppunt in een cluster te verwijderen.

Connectoronderdeel ontkoppelen van domeinen, instellingen voor directorysynchronisatie en ingebouwde identiteitsprovider

Voordat u een knooppunt kunt verwijderen uit een VMware Identity Manager-cluster, moet u ervoor zorgen dat het connectoronderdeel van het knooppunt niet is toegevoegd aan domeinen, niet wordt gebruikt als synchronisatieconnector en niet is gekoppeld aan de ingebouwde identiteitsprovider.

Vereisten

U moet zich aanmelden als tenantbeheerder, oftewel een lokale beheerder bij de VMware Identity Manager-service. Een domeinbeheerder die is gesynchroniseerd vanuit de bedrijfsdirectory, heeft niet de nodige rechten.

Procedure

1 Meld u aan op de beheerconsole.

2 Klik op het tabblad **Identiteits- en toegangsbeheer** en klik vervolgens op **Installatie**.

De pagina Connectoren wordt geopend.

3 Als het connectoronderdeel van het knooppunt is toegevoegd aan het domein, verlaat u het domein.

a Zoek op de pagina Connectoren naar het connectoronderdeel van het knooppunt dat u wilt verwijderen.

Het connectoronderdeel heeft dezelfde naam als het knooppunt.

b Als in de kolom **Beschikbare opties** de knop **Domein verlaten** wordt weergegeven, klikt u op de knop om het domein te verlaten.

4 Als het connectoronderdeel van het knooppunt wordt gebruikt als synchronisatieconnector voor een directory, wijzigt u de instelling Synchronisatieconnector voor de directory.

a Controleer in de kolom **Gekoppelde directory** op de pagina Connectoren de directory's waaraan het connectoronderdeel is gekoppeld.

b Klik op een directorykoppeling.

c Controleer in het gedeelte **Directorysynchronisatie en -verificatie** van de directorypagina de waarde van de optie **Synchronisatieconnector**.

d Als het connectoronderdeel wordt gebruikt als synchronisatieconnector, selecteert u een andere connector voor de optie **Synchronisatieconnector** en klikt u op **Opslaan**.

e Herhaal deze stappen voor alle directory's waaraan het connectoronderdeel is gekoppeld.

5 Als het connectoronderdeel is gekoppeld aan de ingebouwde identiteitsprovider, verwijdert u het uit de identiteitsprovider.

a Bekijk op de pagina Connectoren in de kolom **Identiteitsprovider** de identiteitsproviders waaraan het connectoronderdeel is gekoppeld.

b Als de ingebouwde identiteitsprovider wordt vermeld, klikt u op de koppeling.

c Klik op de pagina voor de identiteitsprovider in het gedeelte **Connectoren** op het pictogram Verwijderen naast de connector.

Wat nu te doen

Verwijder het knooppunt uit de cluster.

Het knooppunt verwijderen uit de cluster

Nadat u het connectoronderdeel van het knooppunt hebt ontkoppeld van domeinen, instellingen voor directorysynchronisatie en de ingebouwde identiteitsprovider, kunt u het knooppunt verwijderen uit de cluster.

Opmerking U kunt de opdracht Verwijderen niet gebruiken om het laatste knooppunt in een cluster te verwijderen.

Vereisten

- Als u een knooppunt wilt verwijderen, moet u zich aanmelden als tenantbeheerder, oftewel een lokale beheerder bij de VMware Identity Manager-service. Een domeinbeheerder die is gesynchroniseerd vanuit de bedrijfsdirectory, heeft niet de nodige rechten.
- U hebt het connectoronderdeel van het knooppunt ontkoppeld van domeinen, instellingen voor directorysynchronisatie en, zo nodig, de ingebouwde identiteitsprovider. Zie “Connectoronderdeel ontkoppelen van domeinen, instellingen voor directorysynchronisatie en ingebouwde identiteitsprovider,” op pagina 87.

Procedure

1 Sluit de virtual machine van het knooppunt af.

a Meld u aan bij de vCenter Server-instantie.

b Klik met de rechtermuisknop op de virtual machine van het knooppunt en selecteer **Energie > Uitschakelen**.

2 Verwijder het knooppunt uit de load balancer.

3 Verwijder het knooppunt in de VMware Identity Manager-beheerconsole.

a Meld u bij de VMware Identity Manager-beheerconsole aan als lokale beheerder.

b Klik op de pijl omlaag op het tabblad **Dashboard** en selecteer **Dashboard voor systeemdiagnose**.

c Zoek het knooppunt dat u wilt verwijderen.

Voor het knooppunt wordt de volgende status weergegeven:

```
Het huidige knooppunt heeft een ongeldige status. Wilt u het verwijderen?
```

d Klik op de koppeling **Verwijderen** naast het bericht.

Het knooppunt wordt verwijderd uit het cluster. Vermeldingen voor het knoppunt worden verwijderd uit de VMware Identity Manager-database. Het knooppunt wordt ook verwijderd uit de ingesloten Elasticsearch- en Ehcache-clusters.

Wat nu te doen

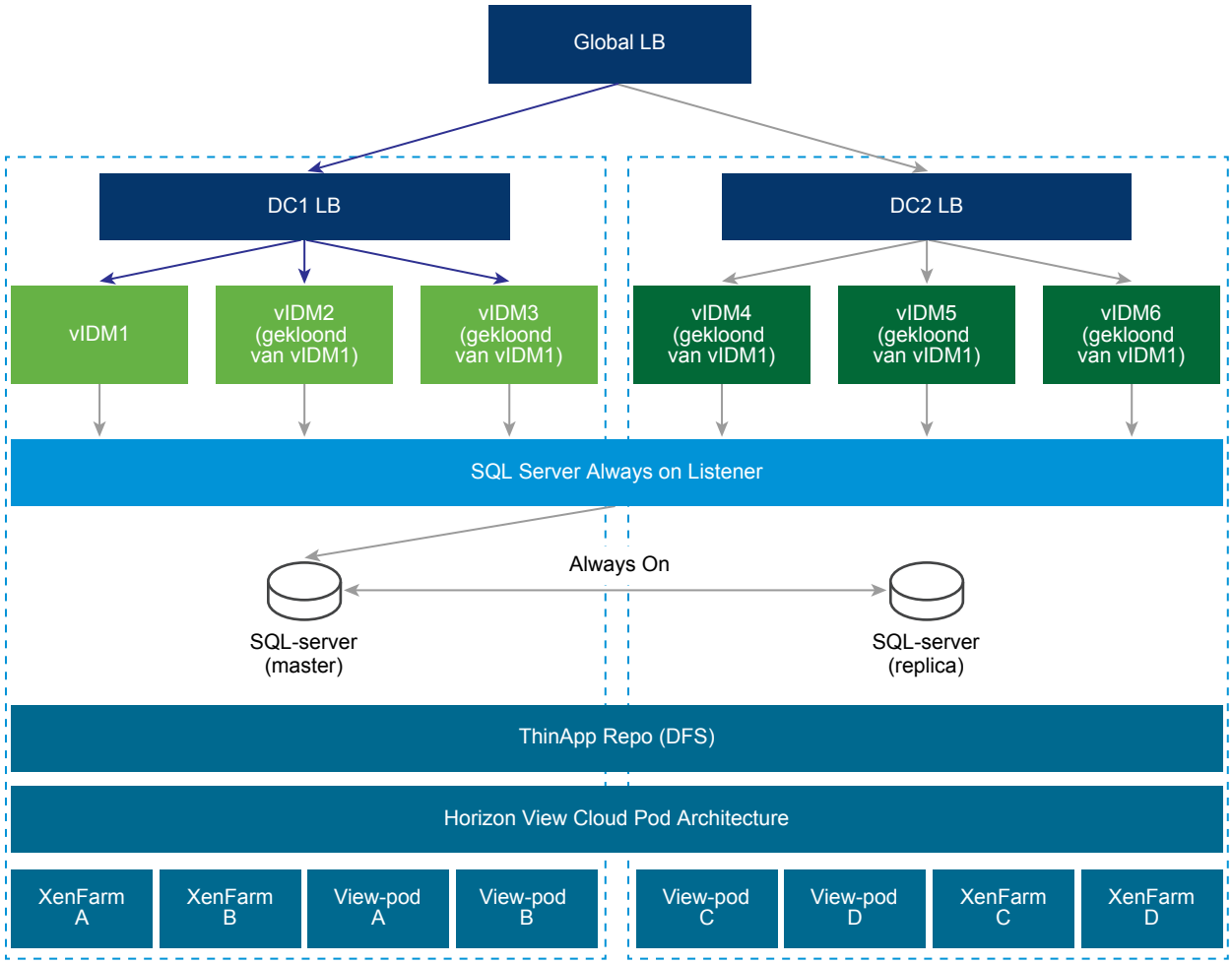
Wacht 5 tot 15 minuten tot de ingesloten Elasticsearch- en Ehcache-clusters stabiel zijn voordat u andere opdrachten uitvoert.

VMware Identity Manager implementeren in een secundair datacenter voor failover en redundantie

Als u mogelijkheden voor failover wilt bieden als het primaire VMware Identity Manager-datacenter niet meer beschikbaar is, moet VMware Identity Manager worden geïmplementeerd in een secundair datacenter.

Door een secundair datacenter te gebruiken, kunnen eindgebruikers zich aanmelden en applicaties gebruiken zonder uitvaltijd. Een secundair datacenter biedt beheerders ook de mogelijkheid om VMware Identity Manager te upgraden naar de volgende versie zonder uitvaltijd. Zie "VMware Identity Manager bijwerken zonder uitvaltijd," op pagina 99.

Hier wordt een typische implementatie met een tweede datacenter weergegeven.



Volg deze richtlijnen voor een implementatie met meerdere datacenters.

- Clusterimplementatie: u moet een reeks van drie of meer VMware Identity Manager virtual appliances als één cluster implementeren in het eerste datacenter en een andere reeks van drie of meer virtual appliances als een ander cluster in het tweede datacenter. Raadpleeg "Een secundair datacenter instellen," op pagina 91 voor meer informatie.
- Database: VMware Identity Manager maakt gebruik van de database om gegevens op te slaan. Voor een implementatie met meerdere datacenters is replicatie van de database tussen de twee datacenters cruciaal. Raadpleeg de documentatie die met de database is meegeleverd voor informatie over het instellen van een database in meerdere datacenters. Bij SQL Server wordt bijvoorbeeld het gebruik van Always On-implementatie aangeraden. Zie Overzicht van Always On-beschikbaarheidsgroepen (SQL Server) op de Microsoft-website voor meer informatie. VMware Identity Manager-functies verwachten een zeer lage latentie tussen de database en de VMware Identity Manager-toepassing. Om die reden wordt verwacht dat toepassingen in het ene datacenter verbinding maken met de database in hetzelfde datacenter.
- Niet actief-Actief: VMware Identity Manager ondersteunt geen Actief-Actief-implementaties waarbij gebruikers tegelijkertijd kunnen worden bediend door beide datacenters. Het secundaire datacenter is een hot stand-by-datacenter en het kan worden toegepast om eindgebruikers bedrijfscontinuïteit te bieden. De VMware Identity Manager-toepassingen in het secundaire datacenter staan in alleen-lezen-modus. Daarom werken de meeste beheerdersbewerkingen, zoals het toevoegen van gebruikers of apps, of gebruikers machtigen, niet meer na een fail-over naar dat datacenter.
- Terugvallen op primair: in de meeste foutscenario's kunt u terugvallen op het primaire datacenter zodra dat datacenter weer in de normale staat is hersteld. Zie "Failback naar primair datacenter," op pagina 98 voor informatie.
- Secundair promoveren naar primair: in geval van een langdurige storing van het datacenter kan het secundaire datacenter worden gepromoveerd naar primair. Zie "Het secundaire datacenter promoveren naar primair datacenter," op pagina 99 voor informatie.
- Fully Qualified Domain Name: de volledig gekwalificeerde domeinnaam om toegang te krijgen tot VMware Identity Manager moet in alle datacenters gelijk zijn.
- Audits: VMware Identity Manager maakt gebruik van Elasticsearch dat is geïntegreerd in de VMware Identity Manager-toepassing voor auditing, rapportage en het maken van directorysynchronisatielogboeken. Er moeten afzonderlijke Elasticsearch-clusters worden gemaakt in elk datacenter. Raadpleeg "Een secundair datacenter instellen," op pagina 91 voor meer informatie.
- Active Directory: VMware Identity Manager kan verbinding maken met Active Directory via de LDAP-API of met behulp van Geïntegreerde Windows-verificatie. Bij beide methoden kan VMware Identity Manager gebruikmaken van Active Directory SRV-records om de juiste domeincontroller in elk datacenter te bereiken.
- Windows-apps: VMware Identity Manager biedt ondersteuning van Windows-apps met behulp van ThinApp, en van Windows-apps en desktopcomputers die gebruikmaken van Horizon View- of Citrix-technologieën. Het is doorgaans belangrijk om deze bronnen te leveren vanuit een datacenter dat zich dichter bij de gebruiker bevindt, dit wordt ook Geo-Affinity genoemd. Houd rekening met het volgende in verband met Windows-bronnen:
  - ThinApps - VMware Identity Manager ondersteunt gedistribueerde Windows-bestandssystemen als ThinApp-repository. Gebruik de documentatie over gedistribueerde Windows-bestandssystemen om de juiste locatiespecifieke beleidsregels op te stellen.
  - Horizon View (met Cloud Pod Architecture) - VMware Identity Manager ondersteunt de Horizon Cloud Pod Architecture. Horizon Cloud Pod Architecture biedt Geo-Affinity door middel van algemene rechten. Zie "Cloud Pod Architecture-implementaties integreren" in *Bronnen instellen in VMware Identity Manager* voor meer informatie. Er hoeven geen aanvullende wijzigingen te worden doorgevoerd voor een VMware Identity Manager-implementatie in meerdere datacenters.

- Horizon View (zonder Cloud Pod Architecture) - Als Horizon Cloud Pod Architecture niet is ingeschakeld in uw omgeving, kunt u Geo-Affinity niet inschakelen. Na een fail-overgebeurtenis kunt u VMware Identity Manager handmatig inschakelen zodat Horizon View-bronnen worden gestart vanuit de View-pods die zijn geconfigureerd in het secundaire datacenter. Raadpleeg "Failovervolgorde van Horizon View en op Citrix gebaseerde bronnen configureren," op pagina 95 voor meer informatie.
- Citrix-bronnen - Net als in Horizon View (zonder Cloud Pod Architecture) kunt u Geo-Affinity niet inschakelen voor Citrix-bronnen. Na een fail-overgebeurtenis kunt u VMware Identity Manager handmatig inschakelen zodat Citrix-bronnen worden gestart vanuit de XenFarms die zijn geconfigureerd in het secundaire datacenter. Raadpleeg "Failovervolgorde van Horizon View en op Citrix gebaseerde bronnen configureren," op pagina 95 voor meer informatie.

Een secundair datacenter instellen

Het secundaire datacenter wordt doorgaans beheerd door een andere vCenter Server. Wanneer u het secundaire datacenter instelt, kunt u het volgende configureren en implementeren op basis van uw vereisten.

- VMware Identity Manager-appliances in het secundaire datacenter, gemaakt op basis van een OVA-bestand dat is geïmporteerd uit het primaire datacenter
- Load-balancer voor het secundaire datacenter
- Dubbele op Horizon View en Citrix gebaseerde bronnen en rechten
- Databaseconfiguratie
- Load-balancer of DNS-vermelding in de primaire en secundaire datacenters voor failover

Het primaire datacenter aanpassen voor replicatie

Voordat u het secundaire datacenter instelt, moet u het primaire datacenter voor Elasticsearch- en Ehcache-replicatie configureren op alle clusters.

Elasticsearch en Ehcache zijn geïntegreerd in de virtual VMware Identity Manager-appliance. Elasticsearch is een zoek- en analyse-engine die wordt gebruikt voor audits, rapporten en logboeken over directorysynchronisatie. Ehcache biedt mogelijkheden voor cache.

Configureer deze wijzigingen in alle knooppunten in de cluster op het primaire datacenter.

Vereisten

U hebt een VMware Identity Manager-cluster ingesteld in het primaire datacenter.

Procedure

1 Configureer Elasticsearch voor replicatie.

Maak deze wijzigingen op alle knooppunten van de cluster op het primaire datacenter.

a Schakel de crontaak voor Elasticsearch uit.

1 Bewerk het bestand `/etc/cron.d/hznelasticsearchsync`:

```
vi /etc/cron.d/hznelasticsearchsync
```

2 Noteer deze regel:

```
#*/1 * * * * root /usr/local/horizon/scripts/elasticsearchnodes.hzn
```

b Voeg de IP-adressen toe van alle knooppunten in de cluster op het primaire datacenter.

1 Bewerk het bestand `/etc/sysconfig/elasticsearch`.

```
vi /etc/sysconfig/elasticsearch
```

2 Voeg de IP-adressen toe van alle knooppunten in de cluster:

```
ES_UNICAST_HOSTS=IP–adres1,IP–adres2,IP–adres3
```

c Voeg FQDN van de load-balancer van de cluster van het secundaire datacenter toe aan het bestand `/usr/local/horizon/conf/runtime–config.properties`.

1 Bewerk het bestand `/usr/local/horizon/conf/runtime–config.properties`.

```
vi /usr/local/horizon/conf/runtime–config.properties
```

2 Voeg deze regel aan het bestand toe:

```
analytics.replication.peers=LB_FQDN_of_second_cluster
```

2 Configureer Ehcache voor replicatie.

Maak deze wijzigingen op alle knooppunten van de cluster op het primaire datacenter.

a `vi /usr/local/horizon/conf/runtime–config.properties`

b Voeg de FQDN toe van de andere knooppunten in de cluster. Voeg de FQDN niet toe voor het knooppunt dat u aan het bewerken bent. Scheidt de FQDN's met een dubbele punt.

```
ehcache.replication.rmi.servers=FQDNknooppunt2:FQDNknooppunt3
```

Bijvoorbeeld:

```
ehcache.replication.rmi.servers=server2.example.com:server3.example.com
```

3 Start de VMware Identity Manager-service opnieuw op alle knooppunten.

```
service horizon–workspace restart
```

4 Controleer of de cluster goed is ingesteld.

Voer deze opdrachten uit op alle knooppunten in de eerste cluster.

a Controleer de status van Elasticsearch.

```
curl 'http://localhost:9200/_cluster/health?pretty'
```

De opdracht moet een resultaat teruggeven dat vergelijkbaar is met het volgende.

```
        {
  "cluster_name" : "horizon",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
```

```
  "active_primary_shards" : 20,
  "active_shards" : 40,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0
}
```

Raadpleeg "Problemen met Elasticsearch oplossen," op pagina 110 als er zich problemen voordoen.

b Controleer of het bestand `/opt/vmware/horizon/workspace/logs/ horizon.log` deze regel bevat.

```
Added ehcache replication peer: //node3.example.com:40002
```

De hostnamen moeten de hostnamen van de andere knooppunten in de cluster zijn.

Wat nu te doen

Maak een cluster in het secundaire datacenter. Maak de knooppunten door het OVA-bestand van de eerste VMware Identity Manager virtual appliance van de cluster van het primaire datacenter te exporteren en te gebruiken voor de implementatie van de nieuwe virtual appliances in het secundaire datacenter.

VMware Identity Manager -virtual appliances in secundair datacenter maken

Om een VMware Identity Manager-cluster in het secundaire datacenter in te stellen, exporteert u het OVA-bestand van de oorspronkelijke VMware Identity Manager-toepassing in het primaire datacenter en gebruikt u het om toepassingen in het secundaire datacenter te implementeren.

Vereisten

- VMware Identity Manager-OVA-bestand dat is geëxporteerd van de oorspronkelijke VMware Identity Manager-toepassing in het primaire datacenter
- IP-adressen en DNS-records voor secundair datacenter

Procedure

1 Exporteer het OVA-bestand van de oorspronkelijke VMware Identity Manager-toepassing naar het primaire datacenter.

Zie de vSphere-documentatie voor informatie.

2 Implementeer in het secundaire datacenter het VMware Identity Manager-OVA-bestand dat is geëxporteerd om de nieuwe knooppunten te maken.

Zie de vSphere-documentatie voor informatie. Zie ook "Het OVA-bestand van VMware Identity Manager installeren," op pagina 19.

3 Nadat de VMware Identity Manager-apparaten zijn ingeschakeld, werkt u de configuratie van elk apparaat bij.

De VMware Identity Manager-toepassingen in het secundaire datacenter zijn identieke kopieën van de oorspronkelijke VMware Identity Manager-toepassing in het primaire datacenter. Synchroniseren naar Active Directory en naar bronnen die zijn geconfigureerd in het primaire datacenter, is uitgeschakeld.

Wat nu te doen

Ga naar de pagina's van Beheerconsole en configureer het volgende:

- Schakel Aan domein toevoegen in zoals is geconfigureerd in de oorspronkelijke VMware Identity Manager-toepassing in het primaire datacenter.

- Op de pagina Verificatieadapters voegt u de verificatiemethoden toe die zijn geconfigureerd in het primaire datacenter.
- Op de pagina Verificatiemethode van directory schakelt u Windows-verificatie in, als deze is geconfigureerd in het primaire datacenter.

Ga naar de pagina apparaatsinstellingen Certificaat installeren om door de certificaatautoriteit ondertekende certificaten toe te voegen en dupliceer de certificaten in de VMware Identity Manager-toepassingen in het primaire datacenter. Zie "SSL-certificaten gebruiken," op pagina 38.

Knooppunten in secundair datacenter configureren

Nadat u knooppunten in het secundaire datacenter heeft gemaakt met behulp van het OVA-bestand dat uit het primaire datacenter is geëxporteerd, configureert u de knooppunten.

Volg deze stappen voor elk knooppunt in het secundaire datacenter.

Procedure

- Werk de IP-tabellen bij.
  a. Werk in het bestand `/usr/local/horizon/scripts/updateiptables.hzn` de IP-adressen van alle knooppunten in het secundaire datacenter bij.
     1. `vi /usr/local/horizon/scripts/updateiptables.hzn`
     2. Vind en vervang de `ALL_IPS`-regel. Specificeer de IP-adressen met een spatie als scheidingsteken.

        `ALL_IPS="Node1_IPaddress Node2_IPaddress Node3_IPaddress"`
     3. Open de poorten door dit script uit te voeren.

        `/usr/local/horizon/scripts/updateiptables.hzn`

  b. Configureer de knooppunten voor Elasticsearch- en Ehcache-replicatie en controleer of deze correct zijn ingesteld.

     Zie de instructies in "Het primaire datacenter aanpassen voor replicatie," op pagina 91 en pas deze toe op de knooppunten in het secundaire datacenter.

     De cronjobs zijn al uitgeschakeld.

Het bestand runtime-config.properties bewerken in het secundaire datacenter

Als u een andere database gebruikt dan een SQL-server Always On-implementatie, moet u de `runtime-config.properties`-bestanden voor de VMware Identity Manager-toepassingen in het secundaire datacenter bewerken om de JDBC-URL te wijzigen zodat deze naar de database in het secundaire datacenter verwijst en om de toepassing te configureren voor alleen-lezen-toegang. Als u een SQL-server Always On-implementatie gebruikt, is deze stap niet vereist.

Voer deze wijzigingen door in elke VMware Identity Manager-toepassing in het secundaire datacenter.

Procedure

1. Meld u met behulp van een ssh-client als hoofdgebruiker aan bij het VMware Identity Manager-apparaat.
2. Open het bestand `runtime-config.properties` op `/usr/local/horizon/conf/runtime-config.properties`.
3. Wijzig de URL van de JDBC zodat deze verwijst naar de database voor het secundaire datacenter.

   Zie "VMware Identity Manager configureren om een externe database te gebruiken," op pagina 37.

4 Configureer of het VMware Identity Manager-apparaat alleen-lezen-toegang heeft.

   Voeg de regel `read.only.service=true` toe.

5 Start de Tomcat-server van het apparaat opnieuw.

   ```
   service horizon-workspace restart
   ```

Failovervolgorde van Horizon View en op Citrix gebaseerde bronnen configureren

Voor Horizon View en op Citrix gebaseerde bronnen moet u de failovervolgorde van bronnen configureren in zowel de primaire als de secundaire datacenters om de juiste bronnen van elk datacenter beschikbaar te maken.

U gebruikt de opdracht hznAdminTool om een databasetabel te maken met de failovervolgorde van bronnen in uw organisatie per service-instantie. De geconfigureerde failovervolgorde wordt gevolgd wanneer een bron wordt gestart. U voert de `hznAdminTool failoverConfiguration` uit in beide datacenters om de failovervolgorde in te stellen.

Vereisten

Wanneer VMware Identity Manager is geïmplementeerd in meerdere datacenters, worden dezelfde bronnen ook ingesteld in elk datacenter. Elke applicaties- of desktopgroep in de View-pods of op Citrix gebaseerde XenFarms wordt beschouwd als verschillende bron in de VMware Identity Manager-catalogus. Als u duplicatie van de bron in de catalogus wilt voorkomen, zorg dan dat u **Dubbele applicaties niet synchroniseren** hebt ingeschakeld op de pagina's View-groepen of Gepubliceerde apps - Citrix op de pagina Beheerconsole.

Procedure

1 Meld u met behulp van een ssh-client als hoofdgebruiker aan bij het VMware Identity Manager-apparaat.

2 Als u een lijst met de serverinstanties wilt weergeven, typt u `hznAdminTool serviceInstances`.

   Er wordt een lijst met de service-instanties met het toegewezen ID-nummer weergegeven, zoals in dit voorbeeld.

   ```
   {"id":103,"hostName":"ws4.domain.com","ipaddress":"10.142.28.92"}{"id":
   154,"hostName":"ws3.domain.com","ipaddress":"10.142.28.91"}{"id":
   1,"hostName":"ws1.domain.com","ipaddress":"10.143.104.176"}{"id":
   52,"hostName":"ws2.domain.com","ipaddress":"10.143.104.177"}
   ```

3 Voor elke service-instantie in uw organisatie configureert u de failovervolgorde voor bronnen op basis van View en Citrix.

   Typ `hznAdminTool failoverConfiguration –configType <configType> –configuration <configuration> –serviceInstanceId <serviceInstanceId> [–orgId <orgId>]`

Optie	Beschrijving
-configType	Typ het brontype dat wordt geconfigureerd voor failover. De waarden zijn `VIEW` of `XENAPP`.
-configuration	Typ de failovervolgorde. Voor configType VIEW typt u een door komma's gescheiden lijst van de hostnamen van de primaire View Connector Server die worden vermeld op de pagina View-groepen in de beheerconsole. Voor configType XENAPP typt u een door komma's gescheiden lijst met XenFarm-namen.

Optie	Beschrijving
-serviceInstanceId	Typ de ID van de service-instantie waarvoor u de configuratie hebt ingesteld. U kunt de ID vinden in de lijst die wordt weergegeven bij Stap 2, `"id":`
-orgId	(Optioneel). Als u dit leeg laat, wordt de configuratie ingesteld voor de standaardorganisatie.

Bijvoorbeeld, `hznAdminTool failoverConfiguration –configType VIEW –configuration pod1vcs1.domain.com,pod2vcs1.hs.trcint.com –orgId 1 –serviceInstanceId 1`.

Wanneer u deze opdracht typt voor VMware Identity Manager-instanties in het secundaire datacenter, draait u de volgorde van de View Connection Servers om. In dit voorbeeld zou de opdracht `hznAdminTool failoverConfiguration –configType VIEW –configuration pod2vcs1.hs.trcint.com, pod1vcs1.domain.com –orgId 1 –serviceInstanceId 103` zijn.

De databasetabel voor failover van bronnen is ingesteld voor elk datacenter.

Wat nu te doen

Als u de bestaande failoverconfiguratie van elk van de op View en Citrix gebaseerde bronnen wilt weergeven, voert u `hznAdminTool failoverConfigurationList –configType <configtype> –<orgId)` uit.

De waarde van <configtype> is VIEW of XENAPP. Het volgende voorbeeld is een uitvoer van `hznAdminTool failoverConfiguraitonList` met het configuratietype VIEW.

```
{"idOrganization":1,"serviceInstanceId":
52,"configType":"VIEW","configuration":"pod1vcs1.domain.com,pod2vcs1.domain.com"}
{"idOrganization":1,"serviceInstanceId":
103,"configType":"VIEW","configuration":"pod2vcs1.domain.com,pod1vcs1.domain.com"}
{"idOrganization":1,"serviceInstanceId":
154,"configType":"VIEW","configuration":"pod2vcs1.domain.com,pod1vcs1.domain.com"}
```

Configureer de database voor failover

Voor VMware Identity Manager is databasereplicatie geconfigureerd, zodat de gegevens consistent blijven over de databaseservers binnen het primaire datacenter en naar het secundaire datacenter.

U moet uw externe database configureren voor hoge beschikbaarheid. Configureer een master en slave database-architectuur, waarin de slave een exacte replica is van de master.

Raadpleeg de documentatie van uw externe database voor informatie.

Wanneer u SQL Server Always On gebruikt, gebruik dan de hostnaam of het IP-adres van de SQL Serverluisteraar wanneer u de database in elke VMware Identity Manager-toepassing configureert. Bijvoorbeeld:

`jdbc:sqlserver://<hostnaam_listener>;DatabaseName=saas`

Failover naar secundair datacenter

Wanneer er zich een fout in het primaire datacenter voordoet, kunt u een failover uitvoeren naar het secundaire datacenter. Voor het uitvoeren van een failover moet u de globale load-balancer of de DNS-record aanpassen om naar de load-balancer in het secundaire datacenter te wijzen.

Afhankelijk van de instelling van uw database bevinden de VMware Identity Manager-applicaties in het secundaire datacenter zich ofwel in de alleen-lezenmodus of in de lezen-schrijvenmodus. Voor alle databases, met uitzondering van de Always On-versie van de SQL-server, bevinden de VMware Identity Manager-applicaties zich in de alleen-lezenmodus. Daarom zijn de meeste beheerdersbewerkingen zoals het toepassen van gebruikers of apps of het machtigen van gebruikers niet beschikbaar.

Als u een Always On-implementatie van de SQL-server gebruikt, bevinden de VMware Identity Manager-applicaties in het secundaire datacenter zich in de lezen-schrijvenmodus.

Een DNS-record gebruiken om te regelen welk datacenter actief is

Als u een DNS-record (Domain Name System) gebruikt om gebruikersverkeer in uw datacenters te leiden, moet de DNS-record onder normale bedrijfsomstandigheden verwijzen naar een load-balancer in het primaire datacenter.

Als het primaire datacenter niet beschikbaar is, moet de DNS-record worden bijgewerkt zodat deze naar de load-balancer in het secundaire datacenter verwijst.

Als het primaire datacenter weer beschikbaar is, moet de DNS-record worden bijgewerkt zodat deze naar de load-balancer in het primaire datacenter verwijst.

De Time To Live instellen in de DNS-record

De instelling Time To Live (TTL) bepaalt hoe lang het duurt voordat DNS-gerelateerde informatie wordt vernieuwd in de cache. Voor een probleemloze failover van View-desktops en -applicaties zorgt u ervoor dat de instelling Time To Live (TTL) in de DNS-records kort is. Als de TTL-instelling te lang is ingesteld, kunnen gebruikers wellicht niet meteen na een failover toegang krijgen tot hun View-desktops en -applicaties. Als u snel vernieuwen van de DNS wilt inschakelen, stelt u de DNS-TTL in op 30 seconden.

VMware Identity Manager -activiteiten zijn niet beschikbaar in alleen-lezen-modus

De VMware Identity Manager gebruiken in alleen-lezen-modus is bedoeld voor een hoge beschikbaarheid zodat eindgebruikers toegang kunnen krijgen tot de bronnen in hun My Apps-portal. Sommige activiteiten in de VMware Identity Manager-beheerconsole en op andere pagina's voor beheerservices zijn wellicht niet beschikbaar in alleen-lezen-modus. Hieronder vindt u een gedeeltelijke lijst met algemene activiteiten die niet beschikbaar zijn.

Wanneer VMware Identity Manager wordt uitgevoerd in alleen-lezen-modus, kunnen er geen activiteiten met betrekking tot wijzigingen in Active Directory of de database worden gemaakt en werkt synchronisatie met de VMware Identity Manager-database niet.

Administratieve functies waarbij gegevens naar de database moeten worden geschreven, zijn op dit moment niet beschikbaar. U moet wachten tot VMware Identity Manager terugkeert in lees- en schrijfmodus.

Alleen-lezen-modus van VMware Identity Manager -beheerconsole

Hier volgen een aantal beperkingen van de beheerconsole in alleen-lezen-modus.

- Het toevoegen, verwijderen en bewerken van gebruikers en groepen op het tabblad **Gebruikers en groepen**
- Het toevoegen, verwijderen en bewerken van applicaties op het tabblad **Catalogus**
- Het toevoegen, verwijderen en bewerken van rechten van applicaties

- Gegevens van merkvermelding wijzigen
- Synchronisatie van directory's voor het toevoegen, verwijderen en bewerken van gebruikers en groepen
- Informatie over bronnen bewerken, waaronder View, XenApp en andere bronnen
- De pagina Verificatiemethoden bewerken

Opmerking De connectoronderdelen van de VMware Identity Manager-applicaties in het secundaire datacenter worden weergegeven in de beheerconsole. Zorg dat u geen connector van het secundaire datacenter als synchronisatieconnector selecteert.

Configuratiepagina's voor virtual appliance, alleen-lezen-modus

Hier volgen een aantal beperkingen van de configuratiepagina's voor de virtual appliance in alleen-lezen-modus.

- Het testen van de ingestelde databaseverbinding
- Het beheerderswachtwoord wijzigen op de pagina Wachtwoord wijzigen

Apps-portal voor eindgebruikers, alleen-lezen-modus

Wanneer VMware Identity Manager in alleen-lezen-modus staat, kunnen gebruikers zich aanmelden bij hun VMware Identity Manager-portal en hebben ze toegang tot hun bronnen. De volgende functies in de portal voor eindgebruikers zijn niet beschikbaar in alleen-lezen-modus.

- Het markeren van een bron als Favoriet of de Favoriet-markering van een bron verwijderen
- Bronnen toevoegen vanaf de pagina Catalogus of bronnen verwijderen via de startpagina
- De wachtwoorden ervan wijzigen via de apps-portal-pagina

Alleen-lezen-modus van VMware Identity Manager Windows-client

Wanneer VMware Identity Manager in alleen-lezen-modus staat, kunnen gebruikers geen nieuwe Windows-clients instellen. De bestaande Windows-clients blijven werken.

Failback naar primair datacenter

In de meeste scenario's waarbij sprake is van een storing kunt u een failback uitvoeren naar het primaire datacenter zodra dat datacenter weer functioneert.

Procedure

1 Pas de globale load-balancer of de DNS-record aan om naar de load-balancer in het primaire datacenter te wijzen.

Zie “Een DNS-record gebruiken om te regelen welk datacenter actief is,” op pagina 97.

2 Wis de cache in het secundaire datacenter.

U kunt REST API's gebruiken om de cache te wissen.

PAD: /SAAS/jersey/manager/api/removeAllCaches

Methode: POST

Toegestane rollen: alleen OPERATOR

Het secundaire datacenter promoveren naar primair datacenter

Indien er zich een uitgebreide fout in het datacenter voordoet, kunt u het secundaire datacenter promoveren naar primair.

Voor een Always On-implementatie van de SQL-server zijn geen wijzigingen vereist. Voor andere databaseconfiguraties moet u het bestand `runtime-config.properties` in de VMware Identity Manager-toepassingen in het secundaire datacenter bewerken om de toepassingen voor de lees-schrijfmodus te configureren.

Voer deze wijzigingen door in elke VMware Identity Manager-toepassing in het secundaire datacenter.

Procedure

1. Meld u met behulp van een ssh-client als hoofdgebruiker aan bij het VMware Identity Manager-apparaat.
2. Open het bestand `/usr/local/horizon/conf/runtime-config.properties` om te bewerken.
3. Wijzig de regel `read.only.service=true` in `read.only.service=false`.
4. Sla het bestand `runtime-config.properties` op.
5. Start de Tomcat-server van het apparaat opnieuw.

   ```
   service horizon-workspace restart
   ```

VMware Identity Manager bijwerken zonder uitvaltijd

Met een implementatie in meerdere datacenters kunt u VMware Identity Manager zonder uitvaltijd bijwerken naar de volgende versie. Gebruik deze aanbevolen werkstroom voor het uitvoeren van updates.

Raadpleeg het diagram in "VMware Identity Manager implementeren in een secundair datacenter voor failover en redundantie," op pagina 89 terwijl u deze stappen volgt.

Procedure

1. Wissel de omleiding van de Globale LB om zodat het verzoek naar de DC2 LB wordt verzonden.
2. Stop de databasereplicatie.
3. Werk de vIDM1-virtual appliance bij, werk vervolgens de vIDM2-virtual appliance bij, en werk vervolgens de vIDM 3-virtual appliance bij.
4. Test updates met behulp van DC1-LB.
5. Wanneer u tevreden bent, wisselt u de omleiding van de Global LB om zodat verzoeken naar DC1 LB worden verzonden.
6. Werk de vIDM4-virtual appliance bij, werk vervolgens de vIDM5-virtual appliance bij, en werk vervolgens de vIDM6-virtual appliance bij.
7. Test updates met behulp van DC2-LB.
8. Start de databasereplicatie.

Aanvullende connectorapplicaties installeren

7

De connector is een onderdeel van de VMware Identity Manager-service. Wanneer u een virtueel VMware Identity Manager-apparaat installeert, wordt er standaard altijd een connectoronderdeel meegeleverd.

De connector voert de volgende functies uit.

- Synchroniseert gebruikers- en groepsgegevens tussen uw bedrijfsdirectory en de corresponderende directory die u in de service maakt.
- Als deze wordt gebruikt als een identiteitsprovider, verifieert deze gebruikers naar de service.

  De connector is de standaardidentiteitsprovider.

Aangezien er al een connector beschikbaar is als onderdeel van de service, hoeft u in standaardimplementaties geen aanvullende connector te installeren.

In sommige scenario's is er echter wel een aanvullende connector vereist. Bijvoorbeeld:

- Als u meerdere directory's van het type Active Directory (Geïntegreerde Windows-verificatie) hebt, hebt u voor elke directory een aparte connector nodig.

  Een connectorinstantie kan aan meerdere directory's worden gekoppeld. Voor elke directory wordt een partitie in de connector gemaakt die de werker wordt genoemd. U kunt niet twee werkers van het type Geïntegreerde Windows-verificatie op dezelfde connectorinstantie hebben.
- Als u de toegang van gebruikers wilt beheren op basis van of ze zich aanmelden via een interne of externe locatie.
- Als u op certificaten gebaseerde verificatie wilt gebruiken, maar als uw load-balancer zodanig is geconfigureerd dat SSL wordt beëindigd bij de load-balancer. Voor certificaatverificatie is SSL pass-through bij de load-balancer vereist.

Als u een aanvullende connector wilt installeren, voert u de volgende taken uit.

- Download het OVA-pakket van de connector.
- Genereer een activatietoken in de service.
- Implementeer de connector van de virtual appliance.
- Configureer de connectorinstellingen.

Eventuele aanvullende connectoren die u implementeert, worden weergegeven in de gebruikersinterface van de service.

Dit hoofdstuk omvat de volgende onderwerpen:

- "Instellingen van Connector configureren," op pagina 103

Activeringscode voor connector genereren

Voordat u de connector van de virtual appliance implementeert, genereert u een activeringscode voor de nieuwe connector van de VMware Identity Manager-service. De activeringscode van de connector wordt gebruikt om de verbinding tussen de service en de connector tot stand te brengen.

Procedure

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

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

3 Klik op **Installatie**.

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

5 Geef een naam op voor de nieuwe connectorinstantie.

6 Klik op **Activeringscode genereren**.

De activeringscode wordt weergegeven in het veld **Activeringscode voor connector**.

7 Kopieer de activeringscode voor de connector en sla deze op.

U gebruikt de activeringscode wanneer u de wizard voor het instellen van de connector uitvoert.

Wat nu te doen

Installeer de connector van de virtual appliance.

Het OVA-bestand implementeren van de Connector

U downloadt het OVA-bestand van de Connector en implementeert het met de VMware vSphere Client of vSphere Web Client.

Vereisten

- Identificeer de DNS-records en hostnaam voor de OVA-implementatie van de Connector.
- 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.
- Download het OVA-bestand van de connector.

Procedure

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

2 Voer op de pagina's van OVF-sjabloon implementeren, de specifieke gegevens voor uw implementatie van de Connector in.

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.

Pagina	Beschrijving
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 te kunnen reageren op de vereisten 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 -apparaat, klikt u met de rechtermuisknop en selecteert u **Aan/uit > Inschakelen**.

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

Wat nu te doen

Gebruik de installatiewizard om de activeringscode en beheerderswachtwoorden toe te voegen.

Instellingen van Connector configureren

Nadat de OVA van de Connector is geïmplementeerd en geïnstalleerd, voert u de wizard Setup uit om het apparaat te activeren en om de beheerderswachtwoorden te configureren.

Vereisten

- U hebt de activeringscode voor de nieuwe connector. Zie "Activeringscode voor connector genereren," op pagina 102.
- Zorg ervoor dat het Connector-apparaat is ingeschakeld en dat u de URL van de Connector kent.
- Verzamel een lijst wachtwoorden om voor de Connector-beheerder, het hoofdaccount en het sshuser-account te gebruiken.

Procedure

1 U voert de installatiewizard uit door de URL van de Connector in te voeren. Deze URL wordt na de implementatie van OVA weergegeven op het tabblad Console.

2 Klik op **Doorgaan** op de welkomstpagina.

3 Maak sterke wachtwoorden voor de volgende beheerderaccounts voor de virtuele Connector-toepassing.

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. Gebruik deze account en bijbehorend wachtwoord om u aan te melden bij de Connector-services voor het beheren van de certificaten, toepassingswachtwoorden en syslog-configuratie. **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.

4 Klik op **Doorgaan**.

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

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

De configuratie van Connector is voltooid.

Wat nu te doen

Stel de omgeving van de service in conform uw behoeften. Als u bijvoorbeeld een extra connector hebt toegevoegd omdat u twee directory's met geïntegreerde Windows-verificatie wilt synchroniseren, maakt u de directory en koppelt u deze aan de nieuwe connector.

Configureer SSL-certificaten voor de Connector. Zie "SSL-certificaten gebruiken," op pagina 38.

Het ingebouwde KDC gebruiken

8

Voor de verificatiemethode Mobiele SSO voor iOS op door AirWatch beheerde iOS-apparaten kunt u het ingebouwde KDC gebruiken. U initialiseert het Key Distribution Center (KDC) in de appliance voordat u de verificatiemethode inschakelt in de beheerconsole.

Opmerking Wanneer u VMware Identity Manager integreert met AirWatch in een Windows-omgeving, gebruikt u de in de cloud gehoste KDC-service van VMware Identity Manager en niet het ingebouwde KDC. Voor gebruik van het KDC in de cloud moet de betreffende realmnaam worden geselecteerd op de pagina voor de iOS-verificatieadapter in de beheerconsole. Raadpleeg de Beheergids voor VMware Identity Manager.

Voordat u het KDC in VMware Identity Manager initialiseert, bepaalt u de realmnaam voor de KDC-server, of er subdomeinen aanwezig zijn in uw implementatie en of het KDC-standaardservercertificaat moet worden gebruikt of niet.

Gebied

Het gebied is de naam van een administratieve entiteit die verificatiegegevens bewaart. Het is belangrijk een beschrijvende naam te selecteren voor het Kerberos-verificatiegebied. De gebiedsnaam moet onderdeel zijn van een DNS-domein dat het bedrijf kan configureren.

De gebiedsnaam en de volledig gekwalificeerde domeinnaam (FQDN) die worden gebruikt om toegang te krijgen tot de VMware Identity Manager-service zijn onafhankelijk. Uw bedrijf moet de DNS-domeinen van zowel de gebiedsnaam als de FQDN regelen. Het is gebruikelijk dat de gebiedsnaam hetzelfde is als uw domeinnaam, ingevoerd met hoofdletters. Soms zijn de gebiedsnaam en het domein verschillend. Een realmnaam is bijvoorbeeld *EXAMPLE.NET* en *idm.example.com* is de VMware Identity Manager FQDN. In dit geval geeft u DNS-vermeldingen op voor de domeinen *example.net* en *example.com*.

De gebiedsnaam wordt door een Kerberos-client gebruikt om DNS-namen te genereren. Wanneer de naam bijvoorbeeld example.com is, is de aan Kerberos gerelateerde naam om contact te maken met de KDC via TCP *_kerberos._tcp.EXAMPLE.COM*.

Subdomeinen gebruiken

De VMware Identity Manager-service die is geïnstalleerd in een omgeving op locatie, kan het subdomein van de VMware Identity Manager FQDN gebruiken. Als uw VMware Identity Manager-site toegang heeft tot meerdere DNS-domeinen, configureert u de domeinen als locatie1.example.com, locatie2.example.com en locatie3.example.com. De waarde van het subdomein is in dit geval example.com, in kleine letters. Als u een subdomein in uw omgeving wilt configureren, werkt u samen met uw serviceondersteuningsteam.

KDC-servercertificaten gebruiken

Wanneer de KDC is geïnitialiseerd, worden er standaard een KDC-servercertificaat en een zelf ondertekend basiscertificaat gegenereerd. Het certificaat wordt gebruikt om het KDC-servercertificaat uit te geven. Dit basiscertificaat bevindt zich in het apparaatprofiel zodat het apparaat de KDC kan vertrouwen.

U kunt het KDC-servercertificaat handmatig genereren met behulp van een basis- of tussencertificaat van uw bedrijf. Neem contact op met uw serviceondersteuningsteam voor meer informatie over deze functie.

Download het rootcertificaat van de KDC-server via de VMware Identity Manager-beheerconsole om het te kunnen gebruiken in de AirWatch-configuratie van het iOS-apparaatbeheerprofiel.

Dit hoofdstuk omvat de volgende onderwerpen:

Het belangrijkste distributiecentrum in het apparaat initialiseren

Voordat u de mobiele SSO voor de iOS-verificatiemethode kunt gebruiken, moet u het belangrijkste distributiecentrum (KDC) in het VMware Identity Manager-apparaat initialiseren.

Als u het KDC wilt initialiseren, wijst u uw hostnaam van Identity Manager toe aan de Kerberos-gebieden. De domeinnaam wordt ingevoerd in hoofdletters. Als u meerdere Kerberos-gebieden configureert, gebruikt u beschrijvende namen die eindigen met uw domeinnaam van Identity manager om het gebied gemakkelijker te kunnen identificeren. Bijvoorbeeld: SALES.MY-IDENTITYMANAGER.EXAMPLE.COM. Als u subdomeinen configureert, typt u de naam van het subdomein in kleine letters in.

Vereisten

VMware Identity Manager is geïnstalleerd en geconfigureerd.

Gebiedsnaam is geïdentificeerd. Zie Hoofdstuk 8, "Het ingebouwde KDC gebruiken," op pagina 105.

Procedure

1 Stel SSH in het VMware Identity Manager-apparaat in als hoofdgebruiker.

2 Initialiseer het KDC. Voer `/etc/init.d/vmware-kdc init --realm {REALM.COM} --subdomain {sva-name.subdomain}` in.

   Bijvoorbeeld `/etc/init.d/vmware-kdc init --realm MY-IDM.EXAMPLE.COM --subdomain my-idm.example.com`

   Als u een load-balancer met meerdere Identity Manager-apparaten gebruikt, gebruikt u in beide gevallen de naam van de load-balancer.

3 Start de VMware Identity Manager-service opnieuw. Voer `service horizon-workspace restart` in.

4 Start de KDC-service. Voer `service vmware-kdc restart` in.

Wat nu te doen

Maak openbare DNS-vermeldingen. DNS-records moeten worden ingericht zodat de clients het KDC kunnen vinden. Zie "Openbare DNS-vermeldingen maken voor KDC met ingebouwde Kerberos," op pagina 107.

Openbare DNS-vermeldingen maken voor KDC met ingebouwde Kerberos

Nadat u KDC hebt geïnitialiseerd in VMware Identity Manager moet u openbare DNS-records maken zodat de clients van Kerberos de KDC kunnen vinden wanneer de ingebouwde Kerberos-verificatiefunctie is ingeschakeld.

De realmnaam van KDC wordt gebruikt als onderdeel van de DNS-naam voor de apparaatvermeldingen van VMware Identity Manager die worden gebruikt om de KDC-service te vinden. Eén SRV DNS-record is vereist voor elke VMware Identity Manager-site en twee A-adresvermeldingen.

Opmerking De AAAA-invoerwaarde is een IPv6-adres die een IPv4-adres codeert. Als de KDC niet adresseerbaar is via IPv6 en een IPv4-adres wordt gebruikt, moet de AAAA-vermelding mogelijk worden gespecificeerd in een strikte IPv6-notatie als `::ffff:175c:e147` op de DNS-server. U kunt een conversietool van IPv4 naar IPv6 gebruiken, zoals beschikbaar van Neustar.UltraTools om IPv4 te converteren naar de IPv6-adresnotatie.

Voorbeeld: DNS-recordvermeldingen voor KDC

In dit voorbeeld-DNS-record is de realm `EXAMPLE.COM`; de Fully Qualified Domain Name van VMware Identity Manager is `idm.example.com` en het IP-adres van VMware Identity Manager is `1.2.3.4`.

```
idm.example.com.               1800 IN  AAAA         ::ffff:1.2.3.4

idm.example.com.               1800 IN  A            1.2.3.4

_kerberos._tcp.EXAMPLE.COM          IN  SRV  10  0   88 idm.example.com.

_kerberos._udp.EXAMPLE.COM          IN  SRV  10  0   88 idm.example.com.
```

Installatie- en configuratieproblemen oplossen 9

De onderwerpen beschrijven oplossingen voor potentiële problemen die u kunt ondervinden wanneer u VMware Identity Manager installeert of configureert.

Dit hoofdstuk omvat de volgende onderwerpen:

Gebruikers kunnen geen applicaties starten of onjuiste verificatiemethode toegepast in omgevingen met gelijkmatige taakverdeling

Gebruikers kunnen geen applicaties starten vanaf de Workspace ONE-portal of de verkeerde verificatiemethode is toegepast in een omgeving met gelijkmatige taakverdeling.

Probleem

In een omgeving met gelijkmatige taakverdeling kunnen mogelijk de volgende problemen optreden:

- Gebruikers kunnen geen applicaties starten vanaf de Workspace ONE-portal nadat ze zich hebben aangemeld.
- De verkeerde verificatiemethode wordt aan gebruikers aangeboden voor verificatie.

Oorzaak

Deze problemen kunnen zich voordoen als het toegangsbeleid onjuist is vastgelegd. Het IP-adres van de client bepaalt welk toegangsbeleid wordt toegepast tijdens aanmelding en tijdens het starten van een applicatie. In een omgeving met gelijkmatige taakverdeling gebruikt VMware Identity Manager de kop X-Forwarded-For om het IP-adres van de client te bepalen. In sommige situaties kan een fout optreden.

Oplossing

Stel de eigenschap `service.numberOfLoadBalancers` in het bestand `runtime-config.properties` in voor elk van de knooppunten in uw VMware Identity Manager-cluster. De eigenschap bepaalt het aantal load balancers die het hoofd bieden aan de VMware Identity Manager-instanties.

Opmerking Het instellen van de eigenschap is optioneel.

1 Meld u aan bij de VMware Identity Manager-applicatie.

2 Bewerk het bestand `/usr/local/horizon/conf/runtime-config.properties` en voeg de volgende eigenschap toe.

```
service.numberOfLoadBalancers numberOfLBs
```

waarbij *numberOfLBs* het aantal load balancers is die het hoofd bieden aan de VMware Identity Manager-instanties.

3 Start de werkruimteservice opnieuw.

```
service horizon-workspace restart
```

Na synchronisatie van de directory worden geen leden in de groepen weergegeven

De synchronisatie van de directory is voltooid, maar er worden geen gebruikers weergegeven in gesynchroniseerde groepen.

Probleem

Nadat een directory handmatig of automatisch op basis van het synchronisatieschema is gesynchroniseerd, is het synchronisatieproces voltooid, maar worden er geen gebruikers in gesynchroniseerde groepen weergegeven.

Oorzaak

Dit probleem doet zich voor als u twee of meer knooppunten in een cluster hebt en er een tijdverschil van meer dan vijf seconden tussen de knooppunten bestaat.

Oplossing

1 Zorg ervoor dat er geen tijdverschil tussen de knooppunten zit. Gebruik dezelfde NTP-server op alle knooppunten in het cluster om de tijd te synchroniseren.

2 Start de service opnieuw op alle knooppunten.

```
service horizon-workspace restart
```

3 (Optioneel) Ga naar de beheerconsole, verwijder de groep, voeg de groep weer toe bij de synchronisatie-instellingen en synchroniseer de directory opnieuw.

Problemen met Elasticsearch oplossen

Gebruik deze informatie om problemen met Elasticsearch in een clusteromgeving op te lossen. Elasticsearch, een zoek- en analyse-engine die wordt gebruikt voor audits, rapportage en directorysynchronisatielogboeken, is geïntegreerd in de virtual VMware Identity Manager-appliance.

Problemen met Elasticsearch oplossen

U kunt de gezondheid van Elasticsearch verifiëren door de volgende opdracht in de VMware Identity Manager-toepassing te gebruiken.

```
curl 'http://localhost:9200/_cluster/health?pretty'
```

De opdracht moet een resultaat teruggeven dat vergelijkbaar is met het volgende.

```
        {
  "cluster_name" : "horizon",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
```

```
  "active_primary_shards" : 20,
  "active_shards" : 40,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0
}
```

Als Elasticsearch niet goed wil starten of als de status rood is, volgt u deze stappen om problemen op te lossen.

1 Zorg dat poort 9300 is geopend.

   a Werk de knooppuntgegevens bij door de IP-adressen van alle knooppunten in het cluster aan het bestand `/usr/local/horizon/scripts/updateiptables.hzn` toe te voegen:

   ```
   ALL_IPS="node1IPadd node2IPadd node3IPadd"
   ```

   b Voer het volgende script uit op alle knooppunten in het cluster.

   ```
   /usr/local/horizon/scripts/updateiptables.hzn
   ```

2 Start Elasticsearch opnieuw op alle knooppunten in het cluster.

   ```
   service elasticsearch restart
   ```

3 Bekijk de logboeken voor meer informatie.

   ```
   cd /opt/vmware/elasticsearch/logs
   ```

   ```
   tail –f horizon.log
   ```

Index