

vRealize Automation configureren

21 juli 2021

vRealize Automation 7.6

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

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

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

VMware Nederland B.V.
Key Office Papendorp
3e verdieping
Orteliuslaan 850
Utrecht
Nederland
Tel: +31 (0) 30-2849500
Fax: +31 (0) 30- 2849501
www.vmware.com/nl

Copyright © 2015-2021 VMware, Inc. Alle rechten voorbehouden. [Informatie over copyright en handelsmerken.](#)

Inhoud

vRealize Automation configureren 6

Bijgewerkte informatie 7

1 Externe voorbereidingen voor inrichting van een blueprint 8

- Uw omgeving voorbereiden voor beheer van vRealize Automation 8
 - Checklist voor de voorbereiding van de netwerk- en beveiligingsconfiguratie van NSX 10
 - Checklist voor het bieden van ondersteuning voor externe IPAM-providers 15
 - Checklist voor het configureren van Containers voor vRealize Automation 19
 - Uw vCloud Director-omgeving voorbereiden voor vRealize Automation 20
 - Uw vCloud Air-omgeving voorbereiden voor vRealize Automation 21
 - Vorbereiding van uw Amazon Web Services-omgeving 21
 - Functies voor netwerk en beveiliging in Red Hat OpenStack voorbereiden 29
 - Vorbereiding van uw SCVMM-omgeving 30
- Netwerk-naar-Azure VPC-connectiviteit configureren 31
- Vorbereiding op inrichting van machine 32
 - Voor te bereiden machine-inrichtingsmethode kiezen 32
 - Checklist voor het uitvoeren van Visual Basic-scripts tijdens inrichting 36
 - Gastagent voor vRealize Automation gebruiken bij de inrichting 37
 - Checklist voor de voorbereiding van inrichting door middel van klonen 46
 - vCloud Air- en vCloud Director-inrichting voorbereiden 61
 - Vorbereiding op inrichting met Linux Kickstart 62
 - Vorbereiding op inrichting met SCCM 65
 - WIM-inrichting voorbereiden 67
 - Inrichting met virtual machine-installatiekopie voorbereiden 76
 - Inrichting met installatiekopieën voor Amazon-machines voorbereiden 76
 - Scenario: vSphere-bronnen voorbereiden op machine-inrichting 79
- Vorbereiding op inrichting met Software 81
 - Inrichten van machines met Software voorbereiden 82
 - Scenario: een vSphere-sjabloon voorbereiden voor blueprints met kloonmachines en softwareonderdelen 86
 - Scenario: import van de blueprint van de vSphere-voorbeeldtoepassing voor Dukes Bank voorbereiden 90

2 Tenants en bronnen voorbereiden op de inrichting van blueprints 96

- Tenantinstellingen configureren 96
 - Configuratieopties kiezen voor Beheer van directory's 97
 - Externe connectoren voor beheer van directory's upgraden 169

Scenario: een Active Directory-koppeling voor een vRealize Automation met hoge zichtbaarheid configureren	177
Externe connectoren voor smartcardverificatie en verificatie via een externe identiteitsprovider in vRealize Automation configureren	180
Een Active Directory-koppeling maken met meerdere domeinen of forests	188
Groepen en gebruikersrollen configureren	190
Aanvullende tenants maken	198
Een tenant verwijderen	201
Configureren van beveiligingsinstellingen voor multi-tenants	202
Aangepaste merkvermelding configureren	202
Checklist voor meldingen configureren	204
Een aangepast RDP-bestand maken ter ondersteuning van RDP-verbindingen voor ingerichte machines	215
Scenario: datacenterlocaties toevoegen voor interregionale implementaties	216
vRealize Orchestrator configureren	218
Bronnen configureren	222
Checklist voor het configureren van IaaS-bronnen	222
XaaS-bronnen configureren	371
Containers maken en configureren	385
Aanvullende invoegtoepassingen installeren op de vRealize Orchestrator-standaardserver	410
Werken met een Active Directory-beleid	411
Gebruikersvoorkeuren voor meldingen en afgevaardigden	415

3 Serviceblueprints aanbieden aan gebruikers 416

Blueprints ontwerpen	416
Uw ontwerpbibliotheek opbouwen	418
Machineblueprints ontwerpen	421
Software-onderdelen ontwerpen	541
XaaS-blueprints en bronacties ontwerpen	555
Een blueprint publiceren	622
Werken met door ontwikkelaar gestuurde blueprints	623
Blueprints en inhoud exporteren en importeren	623
De opgegeven standalone blueprint downloaden en configureren	630
Blueprints en andere IaaS-inhoud maken in een omgeving met meerdere ontwikkelaars	630
Samengestelde blueprints samenstellen	631
Informatie over genest blueprintgedrag	633
Machine- en Software-componenten gebruiken bij het samenstellen van een blueprint.	636
Eigenschaftbindingen maken tussen blueprintonderdelen	638
Afhankelijkheden maken en de inrichtingsvolgorde regelen	639
Aanpassen van blueprint-aanvraagformulieren	640
Een aangepast aanvraagformulier met Active Directory-opties maken	644
Aangepaste veldeigenschappen voor formulierontwerper	653

vRealize Orchestrator-acties gebruiken in het ontwerpprogramma voor aangepaste formulieren	659
De elementen van het waardeselectieveld of boomstructuurselectieveld gebruiken in het ontwerpprogramma voor aangepaste formulieren	661
Het data grid-element gebruiken in het ontwerpprogramma voor aangepaste formulieren	663
Externe validatie gebruiken in het ontwerpprogramma voor aangepaste formulieren	668
Mislukte provisioning-aanvragen testen en problemen oplossen	672
Werking van de actie Hervatten	676
Vernietiging van een implementatie forceren na een mislukte vernietigingsaanvraag	678
Problemen oplossen met een mislukte implementatie die een vRealize Orchestrator werkstroom bevat	679
De servicecatalogus beheren	679
Checklist voor het configureren van de servicecatalogus	680
Een service maken	681
Werken met catalogusitems en acties	684
Rechten maken	687
Werken met goedkeuringsbeleid	696
Machine-inrichting aanvragen met behulp van een blueprint met parameters	728
Scenario: een CentOS met MySQL-toepassingsblueprint beschikbaar maken in de servicecatalogus	729
4 De catalogus gebruiken en implementaties beheren	734
Werken met de catalogus	735
Een catalogusaanvraag indienen	736
Werken met uw implementaties	738
Provisioning-aanvragen controleren	738
Geïmplementeerde catalogusitems beheren	742
Werken met de Inbox	790

vRealize Automation configureren

vRealize Automation configureren biedt informatie over het configureren van vRealize Automation en uw externe omgevingen ter voorbereiding van inrichting en catalogusbeheer met vRealize Automation.

Doelgroep

Deze informatie is bedoeld voor IT-professionals die verantwoordelijk zijn voor het configureren van de vRealize Automation-omgeving, alsmede voor infrastructuurbeheerders die bij de vRealize Automation-inrichting verantwoordelijk zijn voor het voorbereiden van de bijbehorende elementen in de bestaande infrastructuur. De informatie is bedoeld voor ervaren Windows- of Linux-systeembeheerders die bekend zijn met de technologie van virtuele apparaten en de acties in datacentra.

Bijgewerkte informatie

De volgende tabel bevat de wijzigingen voor *vRealize Automation configureren* die in deze versie van het product zijn aangebracht.

Revisie	Beschrijving
XX TBD 202X	Een metriekprovider configureren is bijgewerkt.
14 FEB 2020	<ul style="list-style-type: none">■ Computerbronnen bekijken en gegevensverzameling uitvoeren is bijgewerkt.■ Een NSX-T-endpoint maken en associëren met een vSphere-endpoint in vRealize Automation is bijgewerkt.
24 OKT 2019	<ul style="list-style-type: none">■ Problemen oplossen met onverwachte vermeldingen voor het filteren is toegevoegd.■ Kleine tekstbewerkingen en aanpassingen.
9 SEP 2019	<ul style="list-style-type: none">■ Microsoft Azure-endpointconfiguratie is toegevoegd.■ Kleine tekstbewerkingen.
18 JUL 2019	Optie voor doorvoeren verduidelijkt in Instellingen voor blueprunteigenschappen .
14 jun 2019	Kleine tekstbewerkingen.
30 MEI 2019	<ul style="list-style-type: none">■ Onderwerp toegevoegd om het gebruik van zoekopdrachten met jokertekens voor just-in-time-gebruikers te behandelen. Zie Zoekopdrachten met jokertekens gebruiken voor just-in-time-gebruikers.
7 MEI 2019	<ul style="list-style-type: none">■ Een aantal hyperlinks gecorrigeerd.■ Vorbereiding op inrichting met SCCM is bijgewerkt om recent toegevoegde configuratie-eigenschappen te beschrijven.
11 APR 2019	Eerste documentversie.

Externe voorbereidingen voor inrichting van een blueprint

1

Mogelijk moet u bij de inrichting met catalogusitems bepaalde elementen buiten vRealize Automation maken of voorbereiden. Als u bijvoorbeeld een catalogusitem voor de inrichting van een kloonmachine wilt aanbieden, moet u op uw hypervisor een sjabloon maken waarmee u kunt klonen.






Dit hoofdstuk omvat de volgende onderwerpen:

- [Uw omgeving voorbereiden voor beheer van vRealize Automation](#)
- [Netwerk-naar-Azure VPC-connectiviteit configureren](#)
- [Voorbereiding op inrichting van machine](#)
- [Voorbereiding op inrichting met Software](#)


Uw omgeving voorbereiden voor beheer van vRealize Automation

Afhankelijk van uw werkomgeving kan het aan te raden zijn enkele configuratiewijzigingen aan te brengen voordat u de omgeving onder vRealize Automation-beheer kunt plaatsen of voordat u bepaalde functies kunt implementeren.

Tabel 1-1. Uw omgeving voorbereiden voor integratie van vRealize Automation

Omgeving	Voorbereidingen
 NSX for vSphere en NSX-T	<p>Als u NSX for vSphere of NSX-T wilt gebruiken om netwerk-, beveiligings- en load balancer-functies te beheren van VM's die zijn ingericht met vRealize Automation, moet u uw NSX-instantie voorbereiden voor integratie. Zie Checklist voor de voorbereiding van de netwerk- en beveiligingsconfiguratie van NSX.</p>
 vCloud Director	<p>Installeer en configureer uw vCloud Director-instantie, stel vSphere- en cloudbronnen in en verkrijg of maak de juiste verificatiegegevens om vRealize Automation toegang te geven tot uw vCloud Director-omgeving. Zie Uw vCloud Director-omgeving voorbereiden voor vRealize Automation.</p>
 vCloud Air	<p>Registreer uw vCloud Air-account, stel uw vCloud Air-omgeving in en verkrijg of maak de juiste verificatiegegevens om vRealize Automation toegang te geven tot uw omgeving. Zie vCloud Air- en vCloud Director-inrichting voorbereiden.</p>
 Amazon Web Services	<p>Bereid elementen en gebruikersrollen voor in uw Amazon Web Services-omgeving voor gebruik in vRealize Automation en leer hoe Amazon Web Services-functies worden toegewezen aan vRealize Automation-functies. Zie Voorbereiding van uw Amazon Web Services-omgeving.</p>
<p>Microsoft Azure</p>	<p>Configureer netwerken om VPN-tunnels te gebruiken ter ondersteuning van softwareonderdelen op Azure-blueprints. Zie Netwerk-naar-Azure VPC-connectiviteit configureren.</p>
 Red Hat OpenStack	<p>Als u Red Hat OpenStack wilt gebruiken voor het beheer van netwerk- en beveiligingsfuncties van machines die zijn ingericht met vRealize Automation, bereidt u de Red Hat OpenStack-instantie voor op integratie. Zie Functies voor netwerk en beveiliging in Red Hat OpenStack voorbereiden.</p>

Tabel 1-1. Uw omgeving voorbereiden voor integratie van vRealize Automation (vervolg)

Omgeving	Vorbereidingen
 SCVMM	Configureer opslag, het netwerk en lees meer informatie over de beperkingen voor naamgeving van sjablonen en hardwareprofielen. Zie Vorbereiding van uw SCVMM-omgeving .
Externe IPAM-providers	Registreer een extern IPAM-providerpakket of invoegtoepassing, voer de configuratiewerkstromen uit en registreer de IPAM-oplossing als een nieuw vRealize Automation endpoint. Zie Checklist voor het bieden van ondersteuning voor externe IPAM-providers .
Alle overige omgevingen	U hoeft geen wijzigingen in uw omgeving aan te brengen. U kunt beginnen met het voorbereiden op het inrichten van machines door sjablonen, opstartomgevingen of installatiekopieën van machines te maken. Zie Vorbereiding op inrichting van machine .

Checklist voor de voorbereiding van de netwerk- en beveiligingsconfiguratie van NSX

Voordat u de netwerk- en beveiligingsopties van NSX kunt gebruiken in vRealize Automation, moet u het externe NSX for vSphere- of NSX-T-netwerk en de beveiligingsomgeving configureren die u wilt gebruiken.

Als u XaaS wilt gebruiken om de integratie van vRealize Automation en NSX for vSphere uit te breiden, installeert u de NSX-invoegtoepassing in vRealize Orchestrator. De invoegtoepassing biedt geen ondersteuning voor NSX-T.

Als voorbereiding op het gebruik van NSX-netwerk-, -beveiligings- en -load balancing-mogelijkheden in vRealize Automation, moet u, wanneer u NSX-beheerdersgegevens gebruikt, het NSX-beheerdersaccount gebruiken.

vRealize Automation ondersteunt NSX for vSphere en NSX-T. Raadpleeg de [NSX for vSphere-productdocumentatie](#) of [NSX-T-productdocumentatie](#) voor gerelateerde informatie over uw NSX-toepassing.

Vele netwerk- en beveiligingsinstellingen van NSX die u gebruikt in vRealize Automation worden extern geconfigureerd en beschikbaar gesteld nadat de gegevensverzameling is uitgevoerd op de computerbronnen.

Zie [Instellingen van netwerk- en beveiligingsonderdelen configureren in vRealize Automation](#) voor informatie over NSX-instellingen die u kunt configureren voor vRealize Automation-blueprints.

Tabel 1-2. Checklist voor voorbereiding van netwerk en beveiliging in NSX

Taak	Locatie	Details
<input type="checkbox"/> Configureer de NSX-netwerkinstellingen, inclusief instellingen voor gateway en transportzone.	Configureer de netwerkinstellingen in uw NSX -toepassing.	Afhankelijk van welk NSX-product u gebruikt, raadpleegt u de beheeronderwerpen in de volgende NSX-documentatie: <ul style="list-style-type: none"> ■ NSX for vSphere-productdocumentatie ■ NSX-T-productdocumentatie
<input type="checkbox"/> Maak NSX-beveiligingsbeleid, -tags en -groepen.	Configureer de beveiligingsinstellingen in uw NSX -toepassing.	Afhankelijk van welk NSX-product u gebruikt, raadpleegt u de beheeronderwerpen in de volgende NSX-documentatie: <ul style="list-style-type: none"> ■ NSX for vSphere-productdocumentatie ■ NSX-T-productdocumentatie

Tabel 1-2. Checklist voor voorbereiding van netwerk en beveiliging in NSX (vervolg)

Taak	Locatie	Details
<input type="checkbox"/> Configureer de NSX-instellingen voor load balancers.	Configureer de NSX load balancer-instellingen in uw NSX-toepassing.	<p>Afhankelijk van welk NSX-product u gebruikt, raadpleegt u de beheeronderwerpen in de volgende NSX-documentatie:</p> <ul style="list-style-type: none"> ■ NSX for vSphere-productdocumentatie ■ NSX-T-productdocumentatie <p>Zie ook Aangepaste eigenschappen voor netwerken in de PDF <i>Naslaggids voor aangepaste eigenschappen</i> op docs.vmware.com.</p>
<input type="checkbox"/> Voor overkoepelende virtual center-implementaties in NSX for vSphere controleert u of de NSX-computermanager de rol van primaire NSX-manager heeft.	Voor een vRealize Automation-inrichting moet de NSX-computermanager voor de regio waarvan de machine deel uitmaakt, de rol van primaire NSX-manager hebben.	<p>Zie Beheerdersvereisten voor het inrichten van universele NSX for vSphere-objecten.</p> <p>Zie de informatie over overkoepelende virtual center-implementaties, universele objecten en de rol van primaire NSX-manager in de NSX for vSphere-productdocumentatie.</p>

De NSX-invoegtoepassing installeren op vRealize Orchestrator

Om de NSX-invoegtoepassing te kunnen installeren, moet u het vRealize Orchestrator-installatiebestand downloaden, de vRealize Orchestrator-configuratie-interface gebruiken om het invoegtoepassingsbestand te uploaden en de invoegtoepassing installeren op een vRealize Orchestrator-server.

Raadpleeg de [vRealize Orchestrator-productdocumentatie](#) voor algemene informatie over het bijwerken van invoegtoepassingen en het oplossen van problemen.

Voorwaarden

Als u XaaS wilt gebruiken om de integratie van vRealize Automation en NSX for vSphere uit te breiden, installeert u de NSX-invoegtoepassing in vRealize Orchestrator. De invoegtoepassing biedt geen ondersteuning voor NSX-T.

Als u een ingesloten vRealize Orchestrator gebruikt die al een geïnstalleerde NSX-invoegtoepassing bevat, kunt u deze procedure overslaan.

- Controleer of u een ondersteunde vRealize Orchestrator-instantie uitvoert.
Zie *VMware vRealize Orchestrator installeren en configureren* in de [vRealize Orchestrator-productdocumentatie](#) voor informatie over het instellen van vRealize Orchestrator.
- Controleer of u over de verificatiegegevens beschikt voor een account met rechten om vRealize Orchestrator-invoegtoepassingen te installeren en om te verifiëren via vCenter Single Sign-On.
- Controleer of u de vRealize Orchestrator-client hebt geïnstalleerd en of u zich kunt aanmelden met beheerderverificatiegegevens.
- Bevestig dat de versie van de NSX-invoegtoepassing juist is in de [vRealize Automation-ondersteuningsmatrix](#).

Procedure

- 1 Download het invoegtoepassingsbestand naar een locatie die toegankelijk is vanaf de vRealize Orchestrator-server.

De naamindeling van het installatiebestand voor de invoegtoepassing, met correcte versiewaarden, is `o11nplugin-nsx-1.n.n.vmoapp`. Installatiebestanden van invoegtoepassingen voor NSX for vSphere zijn beschikbaar op de [downloadsite voor VMware-producten](#).

- 2 Open een browser en start de vRealize Orchestrator-configuratie-interface.
Een voorbeeld van de URL-indeling is `https://orchestrator_server.com:8283`.
- 3 Klik op **Invoegtoepassingen** in het linkervenster en schuif naar beneden naar de sectie voor het installeren van de nieuwe invoegtoepassing.

- 4 Blader in het tekstvak **Invoegtoepassingsbestand** naar het installatiebestand voor de invoegtoepassing en klik op **Uploaden en installeren**.

Het bestand moet de indeling .vmoapp hebben.

- 5 Als u daarom wordt gevraagd, accepteert u de licentieovereenkomst in het venster Een invoegtoepassing installeren.
- 6 Controleer in de sectie voor de installatiestatus van ingeschakelde invoegtoepassingen of de naam van de NSX-invoegtoepassing klopt.

Zie de [vRealize Automation-ondersteuningsmatrix](#) voor versie-informatie.

De status Invoegtoepassing wordt geïnstalleerd bij de volgende serveropstart wordt weergegeven.

- 7 Start de vRealize Orchestrator-serverservice opnieuw op.
- 8 Start de vRealize Orchestrator-configuratie-interface opnieuw op.
- 9 Klik op **Invoegtoepassingen** en controleer dat de status is gewijzigd in Installatie OK.
- 10 Start de vRealize Orchestrator-clienttoepassing, meld u aan en gebruik het tabblad **Werkstroom** om door de bibliotheek te bladeren naar de map NSX.

U kunt door de werkstromen bladeren die de NSX-invoegtoepassing biedt.

Wat nu te doen

Maak een vRealize Orchestrator-endpoint in vRealize Automation aan voor gebruik bij het uitvoeren van werkstromen. Zie [Een vRealize Orchestrator-endpoint maken](#).

Beheerdersvereisten voor het inrichten van universele NSX for vSphere-objecten

Om machines in te richten in een vCenter-overkoepelende NSX-omgeving bij gebruik van universele NSX-objecten, moet u deze inrichten in een vCenter Server waarin de NSX-computermanager de primaire rol vervult.

Er kunnen meerdere vCenter-servers aanwezig zijn in een vCenter-overkoepelende NSX for vSphere-omgeving, waarbij elke server moet worden gekoppeld aan een eigen NSX-manager. Eén NSX-manager krijgt de rol van primaire NSX-manager toegewezen, terwijl de rol van secundaire NSX-manager wordt toegewezen aan de andere managers.

De primaire NSX-manager kan universele objecten, zoals universele logische schakelopties, maken. Deze objecten worden gesynchroniseerd met de secundaire NSX-managers. U kunt deze objecten vanuit de secundaire NSX-managers bekijken, maar u kunt ze daar niet wijzigen. U moet de primaire NSX-manager gebruiken om universele objecten te beheren. De primaire NSX-manager kan worden gebruikt om iedere secundaire NSX-manager in de omgeving te configureren.

Zie *Overview of Cross-vCenter Networking and Security* in de *NSX Administration Guide* in de [NSX for vSphere-productdocumentatie](#) voor meer informatie over de vCenter-overkoepelende NSX-omgeving.

vRealize Automation ondersteunt lokale NSX-objecten, zoals lokale logische schakelopties, lokale Edge-gateways en lokale load balancers, beveiligingsgroepen en beveiligingstags voor een vSphere (vCenter)-endpoint dat is gekoppeld aan het NSX-endpoint van een primaire NSX-manager. Het ondersteunt ook een-op-een en een-op-veel NAT-netwerken met een universele transportzone, gerouteerde netwerken met een universele transportzone en universele gedistribueerde logische routers (DLR's) en een load balancer met ieder type netwerk.

vRealize Automation ondersteunt geen universele NSX-beveiligingsgroepen of -tags (bestaande of op aanvraag).

Gebruik een vCenter-specifieke lokale transportzone om lokale netwerken op aanvraag als primaire NSX-manager in te richten. U kunt vRealize Automation-reserveringen configureren voor gebruik van de lokale transportzone en virtuele kabels voor implementaties in de desbetreffende lokale vCenter Server.

Als u een verbinding maakt tussen een vSphere (vCenter)-endpoint en een bijbehorend endpoint van een secundaire NSX-manager, kunt u alleen lokale objecten inrichten en gebruiken.

vRealize Automation kan een universele logische NSX-schakeloptie van als extern netwerk verbruiken. Als een universele schakeloptie bestaat, worden de gegevens erover verzameld en wordt de schakeloptie vervolgens gekoppeld aan of verbruikt door iedere machine in de implementatie.

- Door een netwerk op aanvraag in te richten met een universele transportzone kan een nieuwe universele logische schakeloptie worden gemaakt.
- Door een netwerk op aanvraag in te richten met een universele transportzone voor de primaire NSX-manager, wordt een universele logische schakeloptie gemaakt.
- Het inrichten van een netwerk op aanvraag met een universele transportzone voor een secundaire NSX-manager mislukt, aangezien NSX geen universele logische schakeloptie kan maken op een secundaire NSX-manager.

Zie voor meer informatie over universele NSX-objecten het VMware Knowledge Base-artikel *Deployment of vRealize Automation blueprints with NSX objects fail (2147240)* op <http://kb.vmware.com/kb/2147240>.

Checklist voor het bieden van ondersteuning voor externe IPAM-providers

U kunt IP-adressen en bereiken voor gebruik in netwerkprofieldefinities verkrijgen van een ondersteunde externe IPAM-provider, zoals Infoblox.

Voordat u een extern IPAM-providerendpoint in een vRealize Automation-netwerkprofiel kunt maken en gebruiken, dient u een vRealize Orchestrator IPAM-providerinvoegtoepassing of -pakket te downloaden of op andere wijze te verkrijgen, de invoegtoepassing of het pakket te importeren, de vereiste werkstromen uit te voeren in vRealize Orchestrator en de IPAM-oplossing te registreren als een vRealize Automation-endpoint.

Voor een overzicht van het inrichtingsproces wanneer een externe IPAM-provider een reeks mogelijke IP-adressen moet leveren, raadpleegt u [Een vRealize Automation-implementatie inrichten met een externe IPAM-provider](#).

Tabel 1-3. Checklist voor het voorbereiden van ondersteuning voor externe IPAM-providers

Taak	Beschrijving	Details
<input type="checkbox"/> Verkrijg en importeer de vRealize Orchestrator-invoegtoepassing van de ondersteunde externe IPAM-provider.	<p>Download de invoegtoepassing of het pakket van de IPAM-provider, bijvoorbeeld de Infoblox IPAM-invoegtoepassing voor vRealize Orchestrator en bijbehorende documentatie van de VMware Solution Exchange (https://solutionexchange.vmware.com/store/category_groups/cloud-management) en importeer de invoegtoepassing of het pakket naar vRealize Orchestrator.</p> <p>Als de VMware Solution Exchange niet het benodigde pakket van de IPAM-provider bevat, kunt u uw eigen pakket maken met behulp van de SDK van de externe IPAM-provider en ondersteunende documentatie.</p> <p>Een versiespecifieke SDK van de externe IPAM-provider voor vRealize Automation, ondersteunende documentatie en bijbehorend starterspakket voor vRealize Orchestrator en vRealize Automation is beschikbaar op https://code.vmware.com/sdks of https://code.vmware.com/samples.</p>	<p>Zie Een pakket van de externe IPAM-provider verkrijgen en importeren in vRealize Orchestrator.</p>
<input type="checkbox"/> Voer de vereiste configuratiewerkstromen uit en registreer de externe IPAM-oplossing als een vRealize Automation-endpoint.	<p>Voer de vRealize Orchestrator-configuratiewerkstromen uit en registreer het IPAM-provider-endpointtype in vRealize Orchestrator.</p>	<p>Zie Werkstroom uitvoeren om externe IPAM-endpointtypes in vRealize Orchestrator te registreren.</p>

Een pakket van de externe IPAM-provider verkrijgen en importeren in vRealize Orchestrator

Ter voorbereiding van het definiëren en gebruiken van een extern IPAM-providerendpoint, moet u eerst het pakket van de externe IPAM-provider verkrijgen en importeren in vRealize Orchestrator.

U kunt een bestaande invoegtoepassing van een externe provider voor IP-adresbeheer downloaden, zoals Infoblox IPAM. U kunt ook uw eigen invoegtoepassing of pakket maken met behulp van een door VMware geleverd startpakket en begeleidende SDK-documentatie voor gebruik met een andere provider van een externe IPAM-oplossing, zoals BlueCat.

- Verkrijg de bestaande invoegtoepassing [Infoblox IPAM Plug-in for vRealize Orchestrator](#) en de ondersteunende documentatie van [marketplace.vmware.com](#). De download bevat ook documentatie voor het installeren en gebruiken van de invoegtoepassing.
- Maak uw eigen externe IPAM-oplossing door een SDK van een provider van externe IPAM-oplossingen, ondersteunende documentatie en een bijbehorend starterspakket voor vRealize Orchestrator en vRealize Automation op te halen en te gebruiken. Zie de pagina [vRealize Automation Example Third-Party IPAM Package](#) op [code.vmware.com/web/sdk](#).

Nadat u de invoegtoepassing of het pakket voor de externe IPAM-provider in vRealize Orchestrator hebt geïmporteerd, moet u de vereiste werkstromen uitvoeren en het IPAM-endpointtype registreren in vRealize Orchestrator.

Raadpleeg voor meer informatie over het importeren van invoegtoepassingen en pakketten en het uitvoeren van vRealize Orchestrator-werkstromen *Het gebruik van de VMware vRealize Orchestrator Client*. Raadpleeg voor meer informatie over het uitbreiden van vRealize Automation met vRealize Orchestrator-invoegtoepassingen, -pakketten en -werkstromen *Uitbreidbaarheid van levenscyclus*.

Voor deze stappenreeks wordt de Infoblox IPAM-invoegtoepassing als voorbeeld gebruikt. Uw stappenreeks verschilt mogelijk afhankelijk van de versie van uw vRealize Automation-invoegtoepassing.

Voorwaarden

- Download het pakket of de invoegtoepassing van [marketplace.vmware.com](#).
- Meld u aan bij vRealize Orchestrator met beheerdersbevoegdheden voor het importeren, configureren en registreren van een vRealize Orchestrator-invoegtoepassing of -pakket.

Procedure

- 1 Open de site [marketplace.vmware.com](#).
- 2 Zoek en download de invoegtoepassing of het pakket.

Importeer bijvoorbeeld de Infoblox-invoegtoepassing die ondersteuning biedt voor het externe IPAM-endpoint van Infoblox in vRealize Orchestrator en vRealize Automation 7.1 en hoger.

- a Selecteer **Infoblox** in de categorie **Publisher** en klik op **Apply**.
- b Selecteer [The Infoblox Plug-in for vRealize Orchestrator](#).
- c Klik op **Technische specificaties** en bekijk de vereisten.

- d Klik op **Try** voor meer informatie en om een e-mail met een koppeling naar de download te ontvangen.
- e Download het ZIP-bestand zoals wordt aangegeven in de instructies die u per e-mail hebt ontvangen.

Versie 4.0 en hoger van de invoegtoepassing ondersteunt vRealize Automation 7.1 en hoger. Het ZIP-bestand bevat ook documentatie over de invoegtoepassing.

- 3 Klik in vRealize Orchestrator op het tabblad **Beheerder** en klik op **Pakket importeren**.
- 4 Selecteer het pakket dat u wilt importeren.
- 5 Selecteer alle werkstromen en artefacten en klik op **Geselecteerde onderdelen importeren**.

Wat nu te doen

[Werkstroom uitvoeren om externe IPAM-endpointtypes in vRealize Orchestrator te registreren.](#)

Werkstroom uitvoeren om externe IPAM-endpointtypes in vRealize Orchestrator te registreren

Voer de registratiewerkstroom uit in vRealize Orchestrator ter ondersteuning van vRealize Automation-gebruik van de externe IPAM-provider en registreer het Infoblox IPAM-endpointtype voor gebruik in vRealize Automation.

Voorwaarden

- [Een pakket van de externe IPAM-provider verkrijgen en importeren in vRealize Orchestrator](#)
- Verzekert u ervan dat u bent aangemeld bij vRealize Orchestrator met bevoegdheid om werkstromen uit te voeren.
- Houd uw verificatiegegevens als vRealize Automation-beheerder bij de hand zodat u deze kunt invoeren wanneer u hierom wordt gevraagd in de registratiewerkstroom. Wanneer u IPAM-endpointtypes in vRealize Orchestrator registreert, wordt u gevraagd om verificatiegegevens voor de vRealize Automation-beheerder in te voeren.

Procedure

- 1 Klik in vRealize Orchestrator op het tabblad **Ontwerp**, selecteer **Beheerder > Bibliotheek** en selecteer **IPAM-servicepakket SDK**.

Ieder IPAM-providerpakket heeft een unieke naam en bevat unieke werkstromen. Elke provider levert een eigen registratiewerkstroom. Ofschoon de namen van de werkstromen in de pakketten van de providers op elkaar kunnen lijken, is de locatie van de werkstromen in vRealize Orchestrator mogelijk anders en specifiek voor de provider.

- 2 Voer voor dit voorbeeld de registratiewerkstroom **Register IPAM Endpoint** uit en geef het IPAM Infoblox-endpointtype op.

- 3** Wanneer u wordt verzocht vRealize Automation-verificatiegegevens in te voeren, voert u uw verificatiegegevens als vRealize Automation-beheerder in, bijvoorbeeld materiaal-beheerderverificatiegegevens.

U moet de registratiewerkstroom met systeembeheerder-aanmeldgegevens van vRealize Automation opgeven. Zelfs als een niet-systeembeheerder is aangemeld bij de vRealize Orchestrator-client, slaagt de registratie als de systeembeheerder-aanmeldgegevens van vRealize Automation worden opgegeven voor de werkstroom.

Resultaten

In dit voorbeeld registreert het pakket InfoBlox als nieuw IPAM-endpointtype in de vRealize Automation-endpointservice en stelt het het endpointtype beschikbaar voor het maken of bewerken van endpoints in vRealize Automation.

Opmerking Als de Infoblox IPAM-verbinding verdwijnt uit het tabblad vRealize Orchestrator**Inventaris** nadat u de vRealize Orchestrator-server opnieuw hebt opgestart via het vRealize Orchestrator Control Center. Als u dit probleem wilt oplossen, voert u de Create IPAM Connection-werkstroom uit via de menuvolgorde **vRO admin > Library > Infoblox > vRA > Helpers**. Vervolgens gaat u naar het tabblad vRealize Orchestrator**Inventaris**, selecteert u **Infoblox IPAM**, en vernieuwt u de pagina, zodat de Infoblox IPAM-verbinding wordt weergegeven.

Wat nu te doen

U kunt nu een nieuw IPAM Infoblox-endpointtype maken of een endpoint voor een willekeurig, extern pakket of een willekeurige, externe invoegtoepassing maken die u zojuist hebt geregistreerd in vRealize Automation. Zie [Een endpoint van een externe IPAM-provider maken](#).

Checklist voor het configureren van Containers voor vRealize Automation

Om aan de slag te gaan met Containers moet u eerst vRealize Automation-gebruikersrollen voor deze voorziening configureren.

Als u de containerdefinities hebt geconfigureerd in Containers, kunt u containeronderdelen aan een blueprint toevoegen en verder configureren.

Tabel 1-4. Checklist voor het configureren van Containers voor vRealize Automation

Taak	Details
Wijs de rollen van containerbeheerder en containerarchitect toe.	Zie de informatie over containerrollen in <i>Basisprincipes en concepten</i> .
Definieer de containerdefinities op het tabblad Containers van vRealize Automation.	Zie <i>vRealize Automation configureren</i> .
Voeg containeronderdelen en containernetwerkonderdelen toe aan blueprints via het tabblad Ontwerpen van vRealize Automation.	Zie <i>vRealize Automation configureren</i> .

Containers configureren met de vRealize Automation-toepassing

Informatie over de Xenon-service is toegankelijk in de vRealize AutomationvRealize Automation-toepassing (**vRA-instellingen > Xenon**).

Hier vindt u informatie over de Xenon-host VM, controlepoort en servicestatus. Verder vindt u informatie over de geclusterde Xenon-knooppunten.

U beheert de Xenon Linux-service met de volgende CLI-opdrachten in de vRealize Automation-toepassing.

Command	Beschrijving
service xenon-service status	Geeft aan of de service de status uitgevoerd of gestopt heeft.
service xenon-service start	Hiermee wordt de service gestart.
service xenon-service stop	Hiermee wordt de service gestopt.
service xenon-service restart	Hiermee wordt de service opnieuw gestart.
service xenon-service get_host	Toont de naam van de host waarop de service wordt uitgevoerd.
service xenon-service get_port	Toont de servicepoort.
service xenon-service status_cluster	Toont informatie over alle geclusterde knooppunten in een JSON-indeling.
service xenon-service reset	Verwijdert de directory waar alle configuratiebestanden van Xenon worden bewaard en start de service opnieuw op.

Containers clusteren

U kunt de Xenon-service gebruiken in combinatie met Containers voor vRealize Automation om knooppunten samen te voegen in een cluster. Als de knooppunten in een cluster zitten, worden ze automatisch met elkaar in verbinding gebracht wanneer de Xenon-service wordt gestart.

U kunt de clusterstatus controleren op het tabblad **Xenon** van de vRealize Automation-toepassing of door de volgende opdracht uit te voeren in een CLI:

```
service xenon-service status_cluster
```

Xenon werkt met een clustering op quorumbasis. Het quorum wordt berekend met behulp van de formule $(\text{number of nodes} / 2) + 1$.

Uw vCloud Director-omgeving voorbereiden voor vRealize Automation

Voordat u vCloud Director met vRealize Automation integreert, moet u uw vCloud Director-instantie installeren en configureren, uw vSphere- en cloudbronnen instellen en de juiste verificatiegegevens verkrijgen om vRealize Automation toegang te geven tot uw vCloud Director-omgeving.

Uw omgeving configureren

Configureer uw vSphere- en cloudbronnen, inclusief virtuele datacenters en netwerken. Raadpleeg de vCloud Director-documentatie voor meer informatie.

Vereiste verificatiegegevens voor de integratie

Maak of zoek verificatiegegevens voor een organisatiebeheerder of systeembeheerder waarmee vRealize Automation IaaS-beheerders uw vCloud Director-omgeving als endpoint onder vRealize Automation kunnen beheren.

Overwegingen bij gebruikersrollen

De vCloud Director-gebruikersrollen van een organisatie hoeven niet overeen te komen met de rollen van vRealize Automation-bedrijfsgroepen. Als de gebruikersaccount niet bestaat in vCloud Director, voert vCloud Director een zoekactie uit in de bijbehorende LDAP of Active Directory. Bestaat de gebruiker in het identiteitsarchief, dan wordt vervolgens een gebruikersaccount aangemaakt. Als geen gebruikersaccount kan worden gemaakt, wordt alleen een waarschuwing vastgelegd. Het inrichtingsproces zelf wordt verder voltooid. De ingerichte machine wordt vervolgens toegewezen aan de account waarmee het vCloud Director-endpoint is geconfigureerd.

Zie de vCloud Director-documentatie voor meer informatie over gebruikersbeheer met vCloud Director.

Uw vCloud Air-omgeving voorbereiden voor vRealize Automation

Voordat u vCloud Air met vRealize Automation integreert, moet u uw vCloud Air-account registreren, uw vCloud Air-omgeving instellen en de juiste verificatiegegevens verkrijgen om vRealize Automation toegang te geven tot uw omgeving.

Uw omgeving configureren

Configureer uw omgeving volgens de aanwijzingen in de vCloud Air-documentatie.

Vereiste verificatiegegevens voor de integratie

Maak of zoek beheerdersreferenties voor de virtuele infrastructuur of bijbehorende account waarmee vRealize Automation IaaS-beheerders uw vCloud Air-omgeving als endpoint onder vRealize Automation kunnen beheren.

Overwegingen bij gebruikersrollen

De vCloud Air-gebruikersrollen van een organisatie hoeven niet overeen te komen met de rollen van vRealize Automation-bedrijfsgroepen. Zie de vCloud Air-documentatie voor meer informatie over gebruikersbeheer met vCloud Air.

Vorbereiding van uw Amazon Web Services-omgeving

U moet elementen en gebruikersrollen in uw Amazon Web Services-omgeving voorbereiden, Amazon Web Services voorbereiden voor de communicatie met de gastagent en Software-bootstrapagent en weten hoe Amazon Web Services-functies worden toegewezen aan vRealize Automation-functies.

Amazon Web Services-gebruikersrollen en -verificatiegegevens die vereist zijn voor vRealize Automation

U moet verificatiegegevens in Amazon AWS configureren met de machtigingen die vereist zijn voor het beheer van uw omgeving door vRealize Automation.

vRealize Automation vereist toegangssleutels voor endpointverificatiegegevens en ondersteunt geen gebruikersnamen en wachtwoorden.

■ Autorisatie van rollen en machtigingen in Amazon Web Services

Hoewel de rol van Power User (Hoofdgebruiker) in AWS een AWS Directory Service-gebruiker of -groep volledige toegang tot AWS-services en -bronnen biedt, is deze rol niet vereist. Gebruikersrollen met mindere bevoegdheden worden ook ondersteund. Het AWS-beveiligingsbeleid dat aan de behoeften van vRealize Automation-functionaliiteit voldoet, is:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeImages",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeVolumes",

      "ec2:DescribeVpcAttribute",
      "ec2:DescribeAddresses",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeImageAttribute",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeVolumeStatus",
      "ec2:DescribeVpnConnections",
      "ec2:DescribeRegions",
      "ec2:DescribeTags",
      "ec2:DescribeVolumeAttribute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeNetworkInterfaceAttribute",

      "ec2:DisassociateAddress",
      "ec2:GetPasswordData",

      "ec2:ImportKeyPair",
      "ec2:ImportVolume",

      "ec2:CreateVolume",
      "ec2>DeleteVolume",
      "ec2:AttachVolume",
      "ec2:ModifyVolumeAttribute",
      "ec2:DetachVolume",
```

```

        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses",

        "ec2:CreateKeyPair",
        "ec2>DeleteKeyPair",

        "ec2:CreateTags",
        "ec2:AssociateAddress",
        "ec2:ReportInstanceState",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:MonitorInstances",
        "ec2:RebootInstances",
        "ec2:RunInstances",
        "ec2:TerminateInstances",

        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth"
    ],
    "Resource": "*"
}
}]

```

■ Verificatiegegevens in Amazon Web Services

Voor het beheer van gebruikers en groepen van Amazon Identity and Access Management (IAM) moeten voor u AWS-verificatiegegevens voor een beheerder met volledige toegangsrechten zijn geconfigureerd.

Wanneer u een AWS-endpoint in vRA maakt, wordt u gevraagd om een sleutel en geheime sleutel in te voeren. Voor het verkrijgen van de toegangssleutel die nodig is om het Amazon-endpoint te maken, moet de beheerder een sleutel aanvragen aan een gebruiker met AWS-verificatiegegevens voor een beheerder met volledige toegangsrechten of moet voor de beheerder het AWS-beleid voor een beheerder met volledige toegangsrechten worden geconfigureerd. Zie [Een Amazon-endpoint maken](#).

Voor informatie over het inschakelen van beleidsregels en rollen gaat u naar het gedeelte *AWS Identity and Access Management (IAM)* van de Amazon Web Services-productdocumentatie.

Amazon Web Services toestaan te communiceren met de Software-bootstragent en -gastagent

Als u toepassingsblueprints met Software wilt inrichten of als u over de mogelijkheid wilt beschikken om ingerichte machines verder aan te passen met de gastagent, moet u connectiviteit inschakelen tussen uw Amazon Web Services-omgeving, waarin uw machines worden ingericht, en uw vRealize Automation-omgeving, waarin de agenten pakketten downloaden en instructies ontvangen.

Wanneer u vRealize Automation gebruikt voor het inrichten van Amazon Web Services-machines met de vRealize Automation-gastagent en Software-bootstrapagent, moet u een netwerk-naar-Amazon VPC-verbinding instellen, zodat uw ingerichte machines kunnen communiceren met vRealize Automation voor het aanpassen van uw machines.

Raadpleeg de Amazon Web Services-documentatie voor meer informatie over de VPC-connectiviteitsopties voor Amazon Web Services.

Optionele functies van Amazon gebruiken

vRealize Automation ondersteunt diverse functies van Amazon, waaronder Amazon Virtual Private Cloud, elastische Load Balancers, elastische IP-adressen en Elastic Block-opslag.

Beveiligingsgroepen voor Amazon gebruiken

Geef minstens één beveiligingsgroep op wanneer u een Amazon-reservering maakt. Voor elke beschikbare regio moet minstens één beveiligingsgroep zijn opgegeven.

Een beveiligingsgroep functioneert als een firewall waarmee de toegang tot een machine wordt beheerd. Elke regio omvat ten minste een standaard beveiligingsgroep. Beheerders kunnen de Amazon Web Services Management Console gebruiken om extra beveiligingsgroepen te maken, poorten te configureren voor Microsoft Remote Desktop Protocol of SSH en een virtueel particulier netwerk in te stellen voor een Amazon VPN.

Wanneer u een Amazon-reservering maakt of een machineonderdeel configureert in de blueprint, kunt u kiezen uit de lijst met beveiligingsgroepen die beschikbaar zijn voor de opgegeven regio van de Amazon-account. Beveiligingsgroepen worden geïmporteerd tijdens de verzameling van gegevens.

Zie de documentatie bij Amazon voor informatie over het maken en gebruiken van beveiligingsgroepen in Amazon Web Services.

Amazon Web Services-regio's begrijpen

Elk Amazon Web Services-account wordt vertegenwoordigd door een cloudendpoint. Wanneer u een Amazon Elastic Cloud Computing-endpoint maakt in vRealize Automation, worden regio's verzameld als computerbronnen. Nadat de IaaS-beheerder computerbronnen selecteert voor een bedrijfsgroep, worden inventaris- en statusgegevens automatisch verzameld.

Bij de verzameling van inventarisgegevens, die automatisch eenmaal per dag plaatsvindt, worden gegevens verzameld over wat er op een computerbron staat, zoals de volgende gegevens:

- Elastische IP-adressen
- Elastische load balancers
- Elastische blokopslagvolumes

De verzameling van statusgegevens vindt standaard om de 15 minuten plaats. Hierbij worden gegevens verzameld over de status van beheerde instanties. Dit zijn instanties die vRealize Automation maakt. De volgende items zijn voorbeelden van statusgegevens:

- Windows-wachtwoorden
- Status van machines in load balancers
- Elastische IP-adressen

Een materiaalbeheerder kan de verzameling van inventaris- en statusgegevens initialiseren en deactiveren of de frequentie van de verzameling van inventaris- en statusgegevens wijzigen.

Virtuele privécloud van Amazon gebruiken

Amazon Virtual Private Cloud stelt u in staat om instanties van Amazon-machines in te richten in de privésectie van de Amazon Web Services-cloud.

Gebruikers van Amazon Web Services kunnen gebruikmaken van Amazon VPC om een virtuele topologie voor het netwerk te ontwerpen die voldoet aan uw specificaties. U kunt een Amazon VPC toewijzen in vRealize Automation. vRealize Automation houdt echter niet bij wat de kosten zijn van het gebruik van Amazon VPC.

Wanneer u een inrichting uitvoert met Amazon VPC, wordt door vRealize Automation ervan uitgegaan dat er een VPC-subnet is waarvan Amazon een primair IP-adres kan krijgen. Dit adres is statisch, totdat de instantie wordt afgesloten. U kunt ook de pool met elastische IP-adressen gebruiken om een elastisch IP-adres te koppelen aan een instantie in vRealize Automation. Hierdoor kan de gebruiker hetzelfde IP-adres blijven gebruiken als ze voortdurend een instantie in Amazon Web Services inrichten en ontkoppelen.

Gebruik de AWS Management Console om de volgende elementen te maken:

- Een Amazon VPC die internetgateways, een routingstabel, beveiligingsgroepen en subnetten en beschikbare IP-adressen omvat.
- Een Amazon Virtual Private Network voor het geval gebruikers zich willen aanmelden bij instanties van Amazon-machines die zich buiten AWS Management Console bevinden.

Gebruikers van vRealize Automation kunnen de volgende taken uitvoeren wanneer ze werken met een Amazon VPC:

- Een materiaalbeheerder kan een Amazon VPC toewijzen aan een cloudreservering. Zie [Een Amazon EC2-reservering maken](#).
- Een eigenaar van een machine kan een instantie van een Amazon-machine toewijzen aan een Amazon VPC.

Raadpleeg, voor meer informatie over het maken van een Amazon VPC, de documentatie bij Amazon Web Services.

Elastische Load Balancers gebruiken voor Amazon Web Services

Elastische Load Balancers verdelen het binnenkomende toepassingsverkeer over instanties van Amazon Web Services. Load Balancers van Amazon maakt verbeterde fouttolerantie en prestaties mogelijk

Amazon maakt elastische Load Balancers beschikbaar voor machines die zijn ingericht met blueprints van Amazon EC2.

De elastische Load Balancer moet beschikbaar zijn in Amazon Web Services, Amazon Virtual Private Network en de inrichtingslocatie. Als bijvoorbeeld een Load Balancer beschikbaar is in us-east1c en de machinelocatie is us-east1b, kan de machine geen gebruikmaken van de Load Balancer.

vRealize Automation maakt, beheert of controleert geen elastische Load Balancers.

Raadpleeg, voor informatie over het maken van elastische Load Balancers voor Amazon met behulp van de Amazon Web Services Management Console, de documentatie bij Amazon Web Services.

Elastische IP-adressen gebruiken voor Amazon Web Services

Als u een elastisch IP-adres gebruikt, kunt u snel een failover uitvoeren naar een andere machine in een dynamische Amazon Web Services-cloudomgeving. In vRealize Automation zijn elastische IP-adressen beschikbaar voor alle bedrijfsgroepen die over rechten in de regio beschikken.

Een beheerder kan elastische IP-adressen toewijzen aan uw account voor Amazon Web Services met behulp van de AWS Management Console. Er zijn twee groepen elastische IP-adressen in een bepaalde regio. Eén bereik is toegewezen voor instanties die niet tot Amazon VPC behoren en een ander bereik voor Amazon VPC's. Als u alleen de adressen toewijst in een regio die niet tot Amazon VPC behoort, zijn deze adressen niet beschikbaar in Amazon VPC. Het omgekeerde is ook waar. Als u alleen adressen in een Amazon VPC toewijst, zijn de adressen niet beschikbaar in een regio die niet bij Amazon VPC behoort.

Het elastische IP-adres wordt aan uw Amazon Web Services-account gekoppeld, niet aan een specifieke machine, maar het adres kan slechts door één machine tegelijk worden gebruikt. Het adres blijft gekoppeld aan uw account voor Amazon Web Services totdat u ervoor kiest om het vrij te geven. U kunt het adres vrijgeven, zodat het wordt toegewezen aan een specifieke instantie van een machine.

Een IaaS-architect kan een aangepaste eigenschap aan een blueprint toevoegen om een elastisch IP-adres aan machines toe te wijzen tijdens de inrichting. Machine-eigenaars en beheerders kunnen de elastische IP-adressen die aan machines zijn toegewezen, zien en machine-eigenaars of beheerders met bewerkinsrechten op machines kunnen een elastisch IP-adres toewijzen na de inrichting. Als het adres echter al is toegewezen aan een instantie van een machine en als deze instantie deel uitmaakt van de Amazon Virtual Private Cloud-implementatie, kan Amazon het adres niet toewijzen.

Zie de documentatie bij Amazon Web Services voor meer informatie over het maken en gebruiken van elastische IP-adressen van Amazon.

Elastic Block-opslag gebruiken voor Amazon Web Services

Amazon Elastic Block-opslag biedt opslagvolumes op blokniveau die u kunt gebruiken voor een instantie van een Amazon-machine en voor Amazon Virtual Private Cloud. Het opslagvolume kan langer behouden blijven dan mogelijk lijkt gezien de levensduur van de instantie van de bijbehorende Amazon-machine in de cloudomgeving van Amazon Web Services.

Wanneer u een Amazon Elastic Block-opslagvolume gebruikt samen met vRealize Automation, moet u rekening houden met de volgende overwegingen:

- U kunt geen bestaand Elastic Block-opslagvolume toevoegen wanneer u een instantie van een machine inricht. Als u echter een nieuw volume maakt en meer dan één machine aanvraagt, wordt het volume gemaakt en toegevoegd aan elke instantie. Als u bijvoorbeeld een volume maakt met de naam `volume_1` en u vraagt hiervoor drie machines aan, wordt een volume gemaakt voor elke machine. Er worden drie volumes met de naam `volume_1` gemaakt en toegevoegd aan elke machine. Elk volume beschikt over een unieke volume-id. Elk volume heeft dezelfde grootte en bevindt zich op dezelfde locatie.
- Het volume moet gebruikmaken van hetzelfde besturingssysteem en zich op dezelfde locatie bevinden als de machine waaraan u het volume toevoegt.
- vRealize Automation beheert het primaire volume niet van een instantie met een Elastic Block-opslagvolume.

Raadpleeg, voor meer informatie over Amazon Elastic Block-opslagvolumes en details over het inschakelen hiervan met Amazon Web Services Management Console, de documentatie bij Amazon Web Services.

Netwerk-naar-Amazon VPC-connectiviteit configureren voor een 'proof of concept'-omgeving

Als IT-professional die een omgeving moet instellen om vRealize Automation te evalueren, wilt u netwerk-naar-Amazon VPC-connectiviteit tijdelijk configureren om de functie vRealize Automation Software te ondersteunen.

Netwerk-naar-Amazon VPC-connectiviteit is alleen vereist als u de gastagent wilt gebruiken om ingerichte machines aan te passen, of als u Software-onderdelen in uw blueprints wilt opnemen. Voor een productieomgeving moet u deze connectiviteit officieel configureren via Amazon Web Services, maar omdat u in een 'proof of concept'-omgeving werkt, kunt u in plaats daarvan een tijdelijke netwerk-naar-Amazon VPC-connectiviteit configureren. U brengt de SSH-tunnel tot stand en configureert vervolgens een Amazon-reservering in vRealize Automation om deze door uw tunnel te leiden.

Voorwaarden

- Maak een Amazon Web Services-beveiligingsgroep genaamd `TunnelGroup` en configureer deze om toegang tot poort 22 toe te staan.

- Maak of identificeer een CentOS-machine in uw Amazon Web Services TunnelGroup-beveiligingsgroep en let op de volgende configuraties:
 - Administratieve gebruikersreferenties, bijvoorbeeld *root*.
 - Openbaar IP-adres.
 - Privé IP-adres.
- Maak of identificeer een CentOS-machine op hetzelfde lokale netwerk als uw vRealize Automation-installatie.
- Installeer OpenSSH SSHD Server op beide tunnelmachines.

Procedure

- 1 Meld u aan bij uw Amazon Web Services-tunnelmachine als de rootgebruiker of een gelijkaardig profiel.
- 2 Deactiveer iptables.

```
# service iptables save
# service iptables stop
# chkconfig iptables off
```

- 3 Bewerk `/etc/ssh/sshd_config` om `AllowTCPForwarding` en `GatewayPorts` in te schakelen.
- 4 Start de service opnieuw op.

```
/etc/init.d/sshd restart
```

- 5 Meld u aan bij de CentOS-machine op hetzelfde lokale netwerk als uw vRealize Automation-installatie als de rootgebruiker.
- 6 Roep de SSH-tunnel van de lokale netwerkmachine aan naar de Amazon Web Services-tunnelmachine.

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" \
-R 1442:vRealize_automation_appliance_fqdn:5480 \
-R 1443:vRealize_automation_appliance_fqdn:443 \
-R 1444:manager_service_fqdn:443 \
User of Amazon tunnel machine@Public IP Address of Amazon tunnel machine
```

U hebt doorsturen via poort geconfigureerd om uw Amazon Web Services-tunnelmachine toegang te geven tot vRealize Automation-bronnen, maar uw SSH-tunnel werkt niet tot u een Amazon-reservering hebt geconfigureerd om deze door de tunnel te leiden.

Wat nu te doen

- 1 Installeer de software-bootstrapagent en de gastagent op een Windows- of Linux-referentiemachine om een installatiekopie van een Amazon-machine te maken die uw architecten kunnen gebruiken om blueprints te maken. Zie [Voorbereiding op inrichting met Software](#).

- 2 Configureer uw Amazon-reservering in vRealize Automation om deze door uw SSH-tunnel te leiden. Zie [Scenario: een Amazon-reservering maken voor een omgeving om concepten te testen](#).

Functies voor netwerk en beveiliging in Red Hat OpenStack voorbereiden

vRealize Automation ondersteunt verschillende functies in OpenStack, waaronder beveiligingsgroepen en zwevende IP-adressen. Begrijp hoe deze functies werken in vRealize Automation en configureer ze in uw omgeving.

Beveiligingsgroepen voor OpenStack gebruiken

Met beveiligingsgroepen kunt u regels opgeven om het netwerkverkeer via bepaalde poorten te controleren.

Wanneer u een machine aanvraagt, kunt u beveiligingsgroepen opgeven in een reservering. U kunt ook een bestaande NSX-beveiligingsgroep of een beveiligingsgroep op aanvraag opgeven in het ontwerpcanvas.

Beveiligingsgroepen worden geïmporteerd tijdens de verzameling van gegevens.

Voor elke beschikbare regio moet minstens één beveiligingsgroep zijn opgegeven. Wanneer u een reservering maakt, worden de beschikbare beveiligingsgroepen waarover u kunt beschikken in die regio, weergegeven. Elke regio omvat ten minste een standaard beveiligingsgroep.

Extra beveiligingsgroepen moet worden beheerd in de basis van de bron. Voor meer informatie over het beheren van beveiligingsgroepen voor de verschillende machines, raadpleegt u de documentatie bij OpenStack.

Zwevende IP-adressen gebruiken met OpenStack

U kunt zwevende IP-adressen toewijzen aan een actieve virtuele instantie in OpenStack.

Om de toewijzing van zwevende IP-adressen in te schakelen, moet u Doorsturen via IP configureren en een zwevende IP-pool maken in Red Hat OpenStack. Raadpleeg de Red Hat OpenStack-documentatie voor meer informatie.

U moet rechten voor de acties Gekoppeld zwevend IP en Koppeling met zwevend IP ongedaan maken verlenen aan machine-eigenaars. De gebruikers met rechten kunnen vervolgens een zwevend IP-adres aan een ingerichte machine koppelen vanaf de externe netwerken die aan de machine zijn toegevoegd door een beschikbaar adres in de zwevende IP-adrespool te selecteren. Nadat een zwevend IP-adres aan een machine is gekoppeld, kan een vRealize Automation-gebruiker een optie Koppeling met zwevend IP ongedaan maken selecteren om de huidige toegewezen zwevende IP-adressen te bekijken en de koppeling van een adres met een machine ongedaan te maken.

Vorbereiding van uw SCVMM-omgeving

Voordat u sjablonen en hardwareprofielen voor SCVMM gaat maken voor gebruik bij het inrichten van een vRealize Automation-machine, moet u een goed begrip hebben van de beperkingen in de naamgeving voor sjablonen en hardwareprofielen en de netwerk- en opslaginstellingen voor SCVMM configureren.

Voor gerelateerde informatie over het voorbereiden van uw omgeving raadpleegt u informatie over vereisten voor SCVMM in *vRealize Automation installeren*.

Voor gerelateerde informatie over het inrichten van machines raadpleegt u [Een Hyper-V \(SCVMM\)-endpoint maken](#).

vRealize Automation biedt geen ondersteuning voor een implementatieomgeving waarin gebruik wordt gemaakt van een SCVMM-privécloudconfiguratie. vRealize Automation kan op dit moment niet verzamelen van, toewijzen aan of inrichten op basis van SCVM-privéclouds.

Naamgeving voor sjablonen en hardwareprofielen

Vanwege naamgevingsconventies die door SCVMM en vRealize Automation worden gebruikt voor sjablonen en hardwareprofielen, mogen de namen van sjablonen en hardwareprofielen niet beginnen met de woorden 'temporary' of 'profile'. De volgende termen worden bijvoorbeeld genegeerd bij het verzamelen van gegevens:

- TemporaryTemplate
- Temporary Template
- TemporaryProfile
- Temporary Profile
- Profile

Vereiste netwerkconfiguratie voor SCVMM-clusters

SCVMM-clusters geven virtuele netwerken alleen weer voor vRealize Automation, zodat er een een-op-een-relatie tussen de virtuele en logische netwerken moet bestaan. Wijs met behulp van de SCVMM-console elk logisch netwerk toe aan een virtueel netwerk en configureer uw SCVMM-cluster, zodat het virtuele netwerk wordt gebruikt voor toegang tot machines.

Vereiste opslagconfiguratie voor SCVMM-clusters

Op SCVMM Hyper-V-clusters worden door vRealize Automation uitsluitend op gedeelde volumes gegevens en inrichtingen verzameld. Met de SCVMM-console kunt u uw clusters zo configureren dat ze gebruik maken van de gedeelde bronvolumes gebruiken voor opslag.

Vereiste opslagconfiguratie voor standalone SCVMM-hosts

Voor standalone SCVMM-hosts worden door vRealize Automation gegevens en inrichtingen verzameld over het standaardpad naar virtual machine. Configureer met de SCVMM-console de standaardpaden naar de virtual machine voor uw standalone hosts.

Netwerk-naar-Azure VPC-connectiviteit configureren

U moet netwerk-naar-Azure-connectiviteit configureren als u softwareonderdelen in Azure-blueprints wilt gebruiken.

Voorwaarden

- Maak een Azure-beveiligingsgroep genaamd TunnelGroup en configureer deze om toegang tot poort 22 toe te staan.
- Maak of identificeer een machine, zoals een CentOS-machine, in uw Azure TunnelGroup-beveiligingsgroep en let op de volgende configuraties:
 - Administratieve gebruikersreferenties, bijvoorbeeld *root*.
 - Openbaar IP-adres.
 - Privé IP-adres.
- Maak of identificeer een CentOS-machine op hetzelfde lokale netwerk als uw vRealize Automation-installatie.
- Installeer OpenSSH SSHD Server op beide tunnelmachines.

Procedure

- 1 Meld u als de hoofdgebruiker of een gelijksoortig profiel aan bij uw Azure-tunnelmachine.
- 2 Deactiveer iptables.

```
# service iptables save
# service iptables stop
# chkconfig iptables off
```

- 3 Bewerk `/etc/ssh/sshd_config` om `AllowTCPForwarding` en `GatewayPorts` in te schakelen.
- 4 Start de service opnieuw op.

```
/etc/init.d/sshd restart
```

- 5 Meld u aan bij de CentOS-machine op hetzelfde lokale netwerk als uw vRealize Automation-installatie als de rootgebruiker.
- 6 Roep de SSH-tunnel aan van de lokale netwerkmachine naar de Azure-tunnelmachine.

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" \
-R 1442:vRealize_automation_appliance_fqdn:5480 \
-R 1443:vRealize_automation_appliance_fqdn:443 \
-R 1444:manager_service_fqdn:443 \
User of Azure tunnel machine@Public IP Address of Azure tunnel machine
```

U hebt doorsturen via poort geconfigureerd om uw Azure-tunnelmachine toegang te geven tot vRealize Automation-bronnen, maar uw SSH-tunnel werkt niet tot u een Azure-reservering hebt geconfigureerd om deze door de tunnel te leiden.

Wat nu te doen

- 1 Installeer de softwarebootstrapagent en de gastagent op een Windows- of Linux-referentiemachine om een installatiekopie van een Azure-machine te maken die uw architecten kunnen gebruiken om blueprints te maken. Zie [Voorbereiding op inrichting met Software](#).
- 2 Configureer uw Azure-reservering in vRealize Automation om deze door uw SSH-tunnel te leiden. Zie [Een reservering voor Microsoft Azure maken](#).

Voorbereiding op inrichting van machine

Afhankelijk van uw omgeving en de manier van machine-inrichting, kan het nodig zijn om onderdelen buiten vRealize Automation te configureren.

Zo kan het bijvoorbeeld nodig zijn om machinesjablonen of machine-images te configureren.

Ook kan het nodig zijn om instellingen voor NSX te configureren of vRealize Orchestrator-werkstromen uit te voeren.

Zie de *Referentie-architectuur* PDF in de [vRealize Automation-productdocumentatie](#) voor gerelateerde informatie over het opgeven van poorten tijdens het voorbereiden op de provisioning van machines.

Voor te bereiden machine-inrichtingsmethode kiezen

Voor de meeste methoden voor machine-inrichting moet u bepaalde elementen buiten vRealize Automation voorbereiden.

Tabel 1-5. Voor te bereiden machine-inrichtingsmethode kiezen

Scenario	Ondersteund endpoint	Agentondersteuning	Inrichtingsmethode	Voorbereiding vóór het inrichten
Configureer vRealize Automation om aangepaste Visual Basic-scripts uit te voeren als aanvullende stappen in de levenscyclus van de machine, ofwel voor of na de machine-inrichting. U kunt bijvoorbeeld een script vóór inrichting gebruiken om certificaten of beveiligingstokens te genereren voor de inrichting en vervolgens een script na inrichting gebruiken om de certificaten en tokens na de machine-inrichting te gebruiken.	U kunt Visual Basic-scripts met alle ondersteunde endpoints uitvoeren, behalve Amazon Web Services.	Hangt af van de gekozen inrichtingsmethode.	Ondersteund als aanvullende stap voor elke inrichtingsmethode, maar u kunt geen Visual Basic-scripts met Amazon Web Services-machines gebruiken.	Checklist voor het uitvoeren van Visual Basic-scripts tijdens inrichting
Richt toepassingsblueprints in die de installatie, configuratie en het levenscyclusbeheer automatiseren van middleware- en toepassingsimplementatieonderdelen, zoals Oracle, MySQL, WAR en databaseschema's.	<ul style="list-style-type: none"> ■ vSphere ■ vCloud Air ■ vCloud Director ■ Amazon Web Services 	<ul style="list-style-type: none"> ■ (Vereist) Gastagent ■ (Vereist) Software-bootstrapagent en gastagent 	<ul style="list-style-type: none"> ■ Klonen ■ Klonen (voor vCloud Air of vCloud Director) ■ Gekoppelde kloon ■ Installatiekopie van Amazon-machine 	Als u over de mogelijkheid wilt beschikken om Software-onderdelen te gebruiken in uw blueprints, bereidt u een inrichtingsmethode voor die de gastagent en Software-bootstrapagent ondersteunt. Zie Voorbereiding op inrichting met Software voor meer informatie over het voorbereiden voor Software.
Pas machines verder aan na het inrichten met behulp van de gastagent.	Alle virtuele endpoints en Amazon Web Services.	<ul style="list-style-type: none"> ■ (Vereist) Gastagent ■ (Optioneel) Software-bootstrapagent en gastagent 	Ondersteund voor alle inrichtingsmethoden, behalve virtual machine-installatiekopie.	Als u over de mogelijkheid wilt beschikken om machines na het inrichten aan te passen, selecteert u een inrichtingsmethode die de gastagent ondersteunt.
Machines inrichten zonder gastbesturingssysteem. U kunt een besturingssysteem installeren na de inrichting.	Alle virtual machine-endpoints.	Niet ondersteund	Basis	Niet vereist voor het uitvoeren van voorbereiding vóór het inrichten buiten vRealize Automation.

Tabel 1-5. Voor te bereiden machine-inrichtingsmethode kiezen (vervolg)

Scenario	Ondersteund endpoint	Agentondersteuning	Inrichtingsmethode	Vorbereiding vóór het inrichten
Een ruimtebesparende kopie inrichten van een virtual machine, een gekoppelde kloon genoemd. Gekoppelde klonen zijn gebaseerd op een momentopname van een VM en maken gebruik van een keten van deltaschijven om de verschillen met de oorspronkelijke machine vast te leggen.	vSphere	<ul style="list-style-type: none"> ■ (Optioneel) Gastagent ■ (Optioneel) Software-bootstrapagent en gastagent 	Gekoppelde kloon	<p>U moet een bestaande vSphere-virtual machine hebben.</p> <p>Als u Software wilt ondersteunen, moet u de gastagent en software-bootstrapagent installeren op de machine die u wilt klonen.</p> <p>Voordat u VM's van de gekoppelde kloon inricht, schakelt u VM-momentopname uit.</p>
Een ruimtebesparende kopie inrichten van een virtual machine door gebruik te maken van Net App FlexClone-technologie.	vSphere	(Optioneel) Gastagent	NetApp FlexClone	Zie Checklist voor de voorbereiding van inrichting door middel van klonen .
Machines inrichten door een bestaand sjabloonobject te klonen dat is gemaakt op basis van een bestaande Windows- of Linux-machine, de referentiemachine genoemd, en een aanpassingsobject.	<ul style="list-style-type: none"> ■ vSphere ■ KVM (RHEV) ■ SCVMM 	<ul style="list-style-type: none"> ■ (Optioneel) Gastagent ■ (Alleen optioneel voor vSphere) Software-bootstrapagent en gastagent 	Klonen	<p>Zie Checklist voor de voorbereiding van inrichting door middel van klonen.</p> <p>Als u Software wilt ondersteunen, moet u de gastagent en software-bootstrapagent installeren op de vSphere-machine die u wilt klonen.</p>
Richt vCloud Air- of vCloud Director-machines in door te klonen op basis van een sjabloon en het object aan te passen.	<ul style="list-style-type: none"> ■ vCloud Air ■ vCloud Director 	<ul style="list-style-type: none"> ■ (Optioneel) Gastagent ■ (Optioneel) Software-bootstrapagent en gastagent 	vCloud Air of vCloud Director klonen	<p>Zie vCloud Air- en vCloud Director-inrichting voorbereiden.</p> <p>Als u Software wilt ondersteunen, maakt u een sjabloon met de gastagent en de software-bootstrapagent. Voor vCloud Air configureert u een netwerkverbinding tussen uw vRealize Automation-omgeving en uw vCloud Air-omgeving.</p>

Tabel 1-5. Voor te bereiden machine-inrichtingsmethode kiezen (vervolg)

Scenario	Ondersteund endpoint	Agentondersteuning	Inrichtingsmethode	Vorbereiding vóór het inrichten
Richt een machine in door op te starten vanuit een ISO-image en vervolgens een Kickstart- of autoYaSt-configuratiebestand en een distributie-image voor Linux te gebruiken om het besturingssysteem op de machine te installeren.	<ul style="list-style-type: none"> ■ Alle virtuele endpoints. ■ Red Hat OpenStack 	Gastagent wordt geïnstalleerd als onderdeel van de instructies ter voorbereiding.	Linux Kickstart	Vorbereiding op inrichting met Linux Kickstart
Richt een machine in en geef vervolgens de besturing over aan een SCCM-takenreeks voor het opstarten op basis van een ISO-image, implementeer een Windows-besturingssysteem en installeer de vRealize Automation-gastagent.	Alle virtual machine-endpoints.	Gastagent wordt geïnstalleerd als onderdeel van de instructies ter voorbereiding.	SCCM	Vorbereiding op inrichting met SCCM
Richt een machine in door op te starten in een WinPE-omgeving en een besturingssysteem te installeren met behulp van een WIM-image (Windows Imaging File Format) van een bestaande Windows-referentiemachine.	<ul style="list-style-type: none"> ■ Alle virtuele endpoints. ■ Red Hat OpenStack 	Gastagent is vereist. Wanneer u de WinPE-image maakt, moet u handmatig de gastagent invoegen.	WIM	WIM-inrichting vorbereiden

Tabel 1-5. Voor te bereiden machine-inrichtingsmethode kiezen (vervolg)

Scenario	Ondersteund endpoint	Agentondersteuning	Inrichtingsmethode	Vorbereiding vóór het inrichten
Start een instantie met een image van een virtual machine.	Red Hat OpenStack	Niet ondersteund	Installatiekopie van virtual machine	Zie Inrichting met virtual machine-installatiekopie voorbereiden .
Start een instantie met een image van een Amazon-machine.	Amazon Web Services	<ul style="list-style-type: none"> ■ (Optioneel) Gastagent ■ (Optioneel) Software-bootstrapagent en gastagent 	Installatiekopie van Amazon-machine	<p>Koppel installatiekopieën en instantietypen van Amazon-machines aan uw Amazon Web Services-account.</p> <p>Als u ondersteuning van Software wilt bieden, maakt u een installatiekopie van een Amazon-machine met de gastagent en de software-bootstrapagent en configureert u netwerk-naar-VPC-connectiviteit tussen uw Amazon Web Services- en vRealize Automation-omgeving.</p>

Checklist voor het uitvoeren van Visual Basic-scripts tijdens inrichting

U kunt vRealize Automation configureren om uw aangepaste Visual Basic-scripts uit te voeren als aanvullende stappen in de levenscyclus van de machine, ofwel voor of na de machine-inrichting. U kunt bijvoorbeeld een script vóór inrichting gebruiken om certificaten of beveiligingstokens te genereren voor de inrichting en vervolgens een script na inrichting gebruiken om de certificaten en tokens na de machine-inrichting te gebruiken. U kunt Visual Basic-scripts uitvoeren zonder een inrichtingsmethode, maar u kunt geen Visual Basic-scripts zonder Amazon AWS-machines gebruiken.

Tabel 1-6. Checklist voor het uitvoeren van Visual Basic-scripts tijdens inrichting

Taak	Locatie	Details
<input type="checkbox"/> Installeer en configureer de EPI-agent voor Visual Basic-scripts.	Doorgaans de Manager Service-host	Zie <i>vRealize Automation installeren</i> .
<input type="checkbox"/> Maak uw Visual Basic-scripts.	Machine waarop de EPI-agent is geïnstalleerd	<p>vRealize Automation bevat een Visual Basic-voorbeeldscript <code>PrePostProvisioningExample.vbs</code> in de <code>Scripts</code>-submap van de EPI-agentinstallatiemap. Dit script bevat een koptekst om alle argumenten naar een woordenboek te laden, een hoofdtekst waarin u uw functies kunt opnemen en een voettekst om bijgewerkte aangepaste eigenschappen te retourneren naar vRealize Automation.</p> <p>Bij het uitvoeren van een Visual Basic-script, geeft de EPI-agent alle aangepaste eigenschappen van machines door als argumenten naar het script. Om bijgewerkte eigenschapswaarden te retourneren naar vRealize Automation, plaatst u deze eigenschappen in een woordenboek en roept u een functie aan die is opgegeven door vRealize Automation.</p>
<input type="checkbox"/> Verzamel de informatie die vereist is om scripts in blueprints op te nemen.	<p>Leg informatie vast en draag deze over naar uw infrastructuurarchitecten.</p> <p>Opmerking Een materiaalbeheerder kan een eigenschapsgroep maken door de eigenschapssets <code>ExternalPreProvisioningVbScript</code> en <code>ExternalPostProvisioningVbScript</code> te gebruiken om deze vereiste informatie door te geven. Op deze manier maakt u het voor blueprintarchitecten makkelijker om deze informatie goed in hun blueprints op te nemen.</p>	<ul style="list-style-type: none"> ■ Het volledige pad naar de Visual Basic-scripts, inclusief de bestandsnaam en de extensie. Bijvoorbeeld: <code>%System Drive %Program Files (x86)\VMware \vCAC Agents\EPI_Agents \Scripts\SendEmail.vbs</code>. ■ Om een script uit te voeren voor de inrichting, instrueert u infrastructuurarchitecten om het volledige pad naar het script op te geven als de waarde van de aangepaste eigenschap <code>ExternalPreProvisioningVbScript</code>. Om een script uit te voeren na de inrichting, moeten zij de aangepaste eigenschap <code>ExternalPostProvisioningVbScript</code> gebruiken.

Gastagent voor vRealize Automation gebruiken bij de inrichting

U kunt de gastagent op referentiemachines installeren om een machine verder aan te passen na de implementatie. U kunt de aangepaste eigenschappen van de gereserveerde gastagent

gebruiken om eenvoudige aanpassingen uit te voeren, zoals het toevoegen en formatteren van schijven. U kunt ook uw eigen aangepaste scripts maken voor de gastagent die kunnen worden uitgevoerd binnen het gastbesturingssysteem van een ingerichte machine.

Als u de implementatie hebt voltooid en de (eventuele) aanpassingsspecificatie uitvoert, zal de gastagent een XML-bestand (`c:\VRMGuestAgent\site\workitem.xml`) met alle aangepaste eigenschappen van de geïmplementeerde machine maken, alle taken conform de aangepaste eigenschappen van de gastagent voltooien en zichzelf vervolgens van de ingerichte machine verwijderen.

U kunt uw eigen aangepaste scripts schrijven die door de gastagent moeten worden uitgevoerd op machines die zijn geïmplementeerd, en de aangepaste eigenschappen op de blueprint van de machine gebruiken om de locatie van die scripts en de volgorde waarin ze moeten worden uitgevoerd, op te geven. U kunt ook aangepaste eigenschappen gebruiken op de blueprint van de machine, om de waarden van de aangepaste eigenschappen als parameters door te geven aan de scripts.

Zo kunt u bijvoorbeeld de gastagent gebruiken om de volgende aanpassingen uit te voeren op geïmplementeerde machines:

- Het IP-adres wijzigen
- Een station toevoegen of formatteren
- Beveiligingsscripts uitvoeren
- Een andere agent initialiseren, bijvoorbeeld Puppet of Chef

U kunt ook een gecodeerde tekenreeks opgeven als een aangepaste eigenschap in een opdrachtregelargument. Op die manier kunt u gecodeerde informatie bewaren die de gastagent kan decoderen en die deze begrijpt als een geldig opdrachtregelargument.

Opmerking De Linux-gastagent wijst statische IP-adressen toe tijdens het maken en klonen voor Linux Kickstart en PXE-inrichting met betrekking tot aangepaste eigenschappen van vRealize Automation in werkitems. De gastagent kan niet omgaan met het nieuwere consistente netwerknaamgevingsschema, zoals in Ubuntu 16.x, wanneer het statische IP-adressen toewijst.

Uw aangepaste scripts hoeven niet lokaal geïnstalleerd te zijn op de machine. Zo lang als de ingerichte machine netwerktoegang heeft tot de locatie van het script, kan de gastagent de scripts openen en uitvoeren. Hierdoor worden de onderhoudskosten verminderd, omdat u uw scripts kunt bijwerken zonder dat u alle sjablonen opnieuw hoeft samen te stellen.

U kunt beveiligingsinstellingen configureren door informatie op te geven in een reservering, blueprint of script van een gastagent. Als machines een gastagent vereisen, voegt u een beveiligingsregel toe aan de reservering of de blueprint.

Als u ervoor kiest om de gastagent te installeren om aangepaste scripts uit te voeren op machines die zijn ingericht, moeten uw blueprints over de juiste aangepaste eigenschappen van de gastagent beschikken. Als u de gastagent bijvoorbeeld installeert op een sjabloon voor klonen, een aangepast script maakt waarmee het IP-adres van de ingerichte machine wordt gewijzigd, en dit script in een gedeelde locatie plaatst, moet u een aantal aangepaste eigenschappen toevoegen aan uw blueprint.

Tabel 1-7. Aangepaste eigenschappen voor het wijzigen van het IP-adres van een ingerichte machine met een gastagent

Aangepaste eigenschap	Beschrijving
VirtualMachine.Admin.UseGuestAgent	Stel in op true (waar) om de gastagent te initialiseren wanneer de ingerichte machine is gestart.
VirtualMachine.Customize.WaitComplete	Stel dit in op Waar om te verhinderen dat de inrichtingswerkstroom werkitems verzendt naar de gastagent totdat alle aanpassingen zijn voltooid. Stel dit in op Onwaar om ervoor te zorgen dat werkitems worden gemaakt voordat de aanpassing is voltooid.

Tabel 1-7. Aangepaste eigenschappen voor het wijzigen van het IP-adres van een ingerichte machine met een gastagent (vervolg)

Aangepaste eigenschap	Beschrijving
VirtualMachine.SoftwareN.ScriptPath	<p>Geeft het volledige pad op naar het installatiescript van een toepassing. Het pad moet een geldig absoluut pad zijn zoals gezien door het gastbesturingssysteem en moet de naam van de scriptbestandsnaam bevatten.</p> <p>U kunt ook aangepaste eigenschapswaarden als parameters doorgeven naar het script door <code>{CustomPropertyName}</code> in de padtekenreeks toe te voegen. Als u bijvoorbeeld een aangepaste eigenschap hebt met de naam <code>ActivationKey</code> waarvan de waarde <code>1234</code> is, dan is het scriptpad <code>D:\InstallApp.bat -key {ActivationKey}</code>. De gastagent voert de opdracht <code>D:\InstallApp.bat -key 1234</code> uit. Uw scriptbestand kan vervolgens worden geprogrammeerd om deze waarde te accepteren en te gebruiken.</p> <p>Voeg <code>{Owner}</code> toe om de naam van de machine-eigenaar door te geven naar het script.</p> <p>Ook kunt u de waarden van aangepaste eigenschappen doorgeven als parameters voor het script door <code>{UwAangepasteEigenschap}</code> in de tekenreeks voor het pad in te voegen. Wanneer bijvoorbeeld de waarde <code>\\vra-scripts.mycompany.com\scripts\changeIP.bat</code> wordt opgegeven, wordt het script <code>changeIP.bat</code> uitgevoerd vanuit een gedeelde locatie. Maar als de waarde <code>\\vra-scripts.mycompany.com\scripts\changeIP.bat {VirtualMachine.Network0.Address}</code> wordt opgegeven, wordt het script <code>changeIP</code> uitgevoerd, maar wordt ook de waarde van de <code>VirtualMachine.Network0.Address</code>-eigenschap doorgegeven aan het script als een parameter.</p>
VirtualMachine.ScriptPath.Decrypt	<p>Hiermee kan vRealize Automation een versleutelde tekenreeks verkrijgen die als een goed geformatteerde aangepaste eigenschap van <code>VirtualMachine.SoftwareN.ScriptPath</code> wordt doorgegeven aan de opdrachtregel gagent.</p> <p>U kunt een versleutelde tekenreeks, zoals uw wachtwoord, als aangepaste eigenschap in een argument voor een opdrachtregel opgeven. Hierdoor kunt u versleutelde gegevens opslaan die de gastagent kan ontsleutelen en lezen als een geldig argument voor de opdrachtregel. De tekenreeks van de aangepaste eigenschap <code>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat password</code> is bijvoorbeeld niet veilig, omdat deze een daadwerkelijk wachtwoord bevat.</p> <p>Om het wachtwoord te versleutelen, kunt u een aangepaste eigenschap van vRealize Automation maken (bijvoorbeeld <code>MyPassword = password</code>), en versleuteling inschakelen door het beschikbare selectievakje in te</p>

Tabel 1-7. Aangepaste eigenschappen voor het wijzigen van het IP-adres van een ingerichte machine met een gastagent (vervolg)

Aangepaste eigenschap	Beschrijving
	<p>schakelen. De gastagent ontsleutelt de invoer [MijnWachtwoord] naar de waarde in de aangepaste eigenschap MyPassword en voert het script uit als <code>c:\dosomething.bat password</code>.</p> <ul style="list-style-type: none"> ■ Maak de aangepaste eigenschap MyPassword = wachtwoord, waarbij <i>wachtwoord</i> de waarde van uw daadwerkelijke wachtwoord is. Schakel versleuteling in door het beschikbare selectievakje in te schakelen. ■ Stel de aangepaste eigenschap VirtualMachine.ScriptPath.Decrypt in op VirtualMachine.ScriptPath.Decrypt = true. ■ Stel de aangepaste eigenschap VirtualMachine.Software0.ScriptPath in op VirtualMachine.Software0.ScriptPath = c:\dosomething.bat [MijnWachtwoord]. <p>Als u VirtualMachine.ScriptPath.Decrypt instelt op onwaar, of als u niet de aangepaste eigenschap VirtualMachine.ScriptPath.Decrypt maakt, wordt de tekenreeks tussen de vierkante haken ([en]) niet versleuteld.</p>

Zie *Naslaggids voor aangepaste eigenschappen* voor meer informatie over de aangepaste eigenschappen die u kunt gebruiken met de gastagent.

De gastagent configureren om een server te vertrouwen

Zorg dat het PEM-bestand met de openbare sleutel voor de vRealize Automation Manager Service-host in de juiste gastagentmap is geïnstalleerd. U weet dan zeker dat de gastagent op een veilige manier kan worden geconfigureerd om een server te vertrouwen.

Zoek op elke sjabloon de gastagentmap met het PEM-bestand `cert.pem` voor de Manager Service-host om een server te laten vertrouwen:

- Windows-gastagentmap op elke sjabloon die de gastagent gebruikt

```
C:\VRMGuestAgent\cert.pem
```

- Linux-gastagentmap op elke sjabloon die de gastagent gebruikt

```
/usr/share/gugent/cert.pem
```

Als het bestand `cert.pem` zich niet op deze locatie bevindt, kan de referentiemachine van de sjabloon de gastagent niet gebruiken. De beveiligingsvoorwaarde wordt bijvoorbeeld gebroken wanneer de VM al is gestart en u informatie over de openbare sleutel probeert te verzamelen met aangepaste scripts.

Mogelijk moet u, afhankelijk van de geconfigureerde omgeving, tevens met andere zaken rekening houden:

- Bij WIM-installaties moet u de inhoud van het PEM-bestand voor de openbare sleutel toevoegen aan een opdracht in het uitvoerbare bestand in de console en de gebruikersinterface. De consoleparameter is **/cert filename**.
- Bij RedHat Kickstart-installaties moet u de openbare sleutel in het voorbeeldbestand plakken. Anders wordt de gastagent niet uitgevoerd.
- Bij SCCM-installaties moet het bestand `cert.pem` in de map `VRMGuestAgent` worden geplaatst.
- Bij Linux vSphere-installaties moet het bestand `cert.pem` in de map `/usr/share/gugent` worden geplaatst.

Opmerking U kunt de software en gastagenten eventueel ook samen installeren door het volgende script te downloaden van <https://APPLIANCE/software/index.html>. Met dit script kunt u de acceptatie van de vingerafdruk van het SSL-certificaat afhandelen terwijl u de sjablonen maakt.

- Linux
`prepare_vra_template.sh`
- Windows
`prepare_vra_template.ps1`

Als u de software en de gastagent tegelijk installeert, hebt u de aanwijzingen in [De gastagent installeren op een Linux-referentiemachine](#) of [De gastagent installeren op een Windows-referentiemachine](#) niet nodig.

Het bestand `cert.pem` ophalen van de Manager Service-host

- 1 Ga op de Manager Service-host naar Systeembeheer en open Beheer van Internet Information Services (IIS).
- 2 Markeer de Manager Service-host in de boomstructuur aan de linkerkant.
- 3 Open Servercertificaten aan de rechterkant.
- 4 Zoek naar het certificaat waarvoor **Verleend aan** VMware vRA bevat en **Verleend door** VMware vRA bevat.
- 5 Klik met de rechtermuisknop op het certificaat en exporteer het.
- 6 Het opgeslagen certificaat heeft de indeling PFX. Als u dit certificaat wilt converteren naar PEM, gebruikt u OpenSSL vanaf de opdrachtregel.

```
openssl pkcs12 -in filename.pfx -out cert.pem -nodes
```

De gastagent installeren op een Linux-referentiemachine

Installeer de Linux-gastagent op uw referentiemachines om machines verder aan te passen na de implementatie.

Voorwaarden

- Identificeer of maak de referentiemachine.
- De gastagentbestanden die u downloadt bevatten zowel `tar.gz`- als RPM-pakketindelingen. Als uw besturingssysteem geen `tar.gz`- of RPM-bestanden kan installeren, gebruikt u een conversiehulpprogramma om de installatiebestanden te converteren naar uw gewenste pakketindeling.
- Breng vertrouwen tot stand tussen de gastagent en uw Manager Service-machine. Zie [De gastagent configureren om een server te vertrouwen](#).

Procedure

- 1 Ga naar de pagina van de beheerconsole voor de vRealize Automation-toepassing.
Bijvoorbeeld: `https://va-hostname.domain.com`.
- 2 Klik op de **pagina voor gast- en softwareagenten** in het gedeelte voor de installatie van onderdelen van vRealize Automation van de pagina.
Bijvoorbeeld: `https://va-hostname.domain.com/software/index.html`.
De pagina **Installatieprogramma's voor gast- en softwareagenten** wordt geopend, met koppelingen naar beschikbare downloads.
- 3 Klik op **Pakketten voor Linux-gastagenten** in het gedeelte voor installatieprogramma's van gastagenten van de pagina om het bestand `LinuxGuestAgentPkgs.zip` te downloaden en op te slaan.
- 4 Pak het gedownloade bestand `LinuxGuestAgentPkgs.zip` uit en maak de map `VraLinuxGuestAgent`.
- 5 Installeer het gastagentpakket dat overeenkomt met het gastbesturingssysteem dat u tijdens de inrichting implementeert.
 - a Ga naar de submap `VraLinuxGuestAgent` die overeenkomt met het gastbesturingssysteem dat moet worden geïmplementeerd bij de inrichting, bijvoorbeeld `rhel32`.
 - b Zoek naar uw gewenste pakketindeling of converteer een pakket naar uw gewenste pakketindeling.
 - c Installeer het gastagentpakket op uw referentiemachine.
Als u bijvoorbeeld de bestanden van het RPM-pakket wilt installeren, voert u `rpm -i gagent-gugent-7.1.0-4201531.i386.rpm` uit.

- 6 Configureer de gastagent om te communiceren met de Manager Service door `installgugent.sh` *Manager_Service_Hostname_fdqn:portnumber* *ssl platform* uit te voeren.

Het standaardpoortnummer voor de Manager Service is 443. Geaccepteerde platformwaarden zijn `ec2`, `vcd`, `vca` en `vsphere`.

Optie	Beschrijving
Als u een load balancer gebruikt	Voer de volledig gekwalificeerde domeinnaam en het poortnummer van uw Manager Service-load balancer in. Bijvoorbeeld: <pre>cd /usr/share/gugent ./installgugent.sh load_balancer_manager_service.mycompany.com:443 ssl ec2</pre>
Zonder load balancer	Voer de volledig gekwalificeerde domeinnaam en het poortnummer van uw Manager Service-machine in. Bijvoorbeeld: <pre>cd /usr/share/gugent ./installgugent.sh manager_service_machine.mycompany.com:443 ssl vsphere</pre>

- 7 Als geïmplementeerde machines niet al geconfigureerd zijn om het Manager Service SSL-certificaat te vertrouwen, moet u het bestand `cert.pem` op uw referentiemachine installeren om vertrouwen tot stand te brengen.
- Voor de meest veilige aanpak verkrijgt u het `cert.pem`-certificaat en installeert u het bestand handmatig op de referentiemachine.
 - Voor een eenvoudiger aanpak kunt u verbinding maken met de Manager Service-load balancer of Manager Service-machine en downloadt u het `cert.pem`-certificaat.

Optie	Beschrijving
Als u een load balancer gebruikt	Voer als rootgebruiker op de referentiemachine de volgende opdracht uit: <pre>echo openssl s_client -connect manager_service_load_balancer.mycompany.com:443 sed -ne '/- BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem</pre>
Zonder load balancer	Voer als rootgebruiker op de referentiemachine de volgende opdracht uit: <pre>echo openssl s_client -connect manager_service_machine.mycompany.com:443 sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem</pre>

- 8 Als u de gastagent installeert op een Ubuntu-besturingssysteem, maakt u symbolische koppelingen voor gedeelde objecten door een van de volgende opdrachtensets uit te voeren.

Optie	Beschrijving
64-bits systemen	<pre>cd /lib/x86_64-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>
32-bits systemen	<pre>cd /lib/i386-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>

Wat nu te doen

Converteer de referentiemachine naar een sjabloon om te klonen, een installatiekopie van een Amazon-machine of een momentopname die uw IaaS-architecten kunnen gebruiken voor het maken van blueprints.

De gastagent installeren op een Windows-referentiemachine

Installeer de vRealize Automation Windows-gastagent op een Windows-referentiemachine zodat deze als Windows-service wordt uitgevoerd en verdere aanpassing van machines mogelijk is.

Voorwaarden

- Identificeer of maak de referentiemachine.
- Breng vertrouwen tot stand tussen de gastagent en uw Manager Service-machine. Zie [De gastagent configureren om een server te vertrouwen](#).

Procedure

- 1 Ga naar de pagina **Guest and Software Agent Installers** van de vRealize Automation Appliance:
<https://vrealize-automation-appliance-FQDN/software>
- 2 Download het 32-bits of 64-bits uitvoerbaar bestand onder **Guest Agent Installers** en sla het bestand in de root van het station C: op.

Opmerking Er is een alternatief met opdrachtregels voor deze procedure voor de installatie van een gastagent. In plaats van de uitvoerbare bestanden te downloaden, kunt u naar **Installatieprogramma's voor Windows-software** gaan op de pagina met installatieprogramma's voor gast- en softwareagents. Hier kunt u het `prepare_vra_template.ps1` PowerShell-script downloaden en uitvoeren:

```
PowerShell -NoProfile -ExecutionPolicy Bypass -Command prepare_vra_template.ps1
```

- 3** Pak de Windows-gastagentbestanden uit door het uitvoerbare bestand uit te voeren.

Tijdens het uitpakken wordt C:\VRMGuestAgent gemaakt en worden de bestanden toegevoegd.

Wijzig de naam C:\VRMGuestAgent niet.

- 4** Configureer de gastagent om te communiceren met de Manager Service.
- Open een opdrachtprompt met verhoogde bevoegdheid.
 - Ga naar C:\VRMGuestAgent.
 - Plaats het vertrouwde PEM-bestand van Manager Service in de directory C:\VRMGuestAgent\ om de gastagent zodanig te configureren dat deze uw Manager Service-machine vertrouwt.
 - Voer `winservice -i -h Manager_Service_Hostname_fdqn:poortnummer -p ssl` uit.
- Het standaardpoortnummer voor de Manager Service is 443.

Optie	Beschrijving
Als u een load balancer gebruikt	Voer de volledig gekwalificeerde domeinnaam en het poortnummer van uw Manager Service-load balancer in. Bijvoorbeeld: <code>winservice -i -h load_balancer_manager_service.mycompany.com:443 -p ssl</code> .
Zonder load balancer	Voer de volledig gekwalificeerde domeinnaam en het poortnummer van uw Manager Service-machine in. Bijvoorbeeld: <code>winservice -i -h manager_service_machine.mycompany.com:443 -p ssl</code> .
Als u een installatiekopie van een Amazon-machine voorbereidt	U moet opgeven dat u Amazon gebruikt. Bijvoorbeeld: <code>winservice -i -h manager_service_machine.mycompany.com:443:443 -p ssl -c ec2</code>

Resultaten

De naam van de Windows-service is VCACGuestAgentService. U vindt het installatielogboek in VCAC-GuestAgentService.log in C:\VRMGuestAgent.

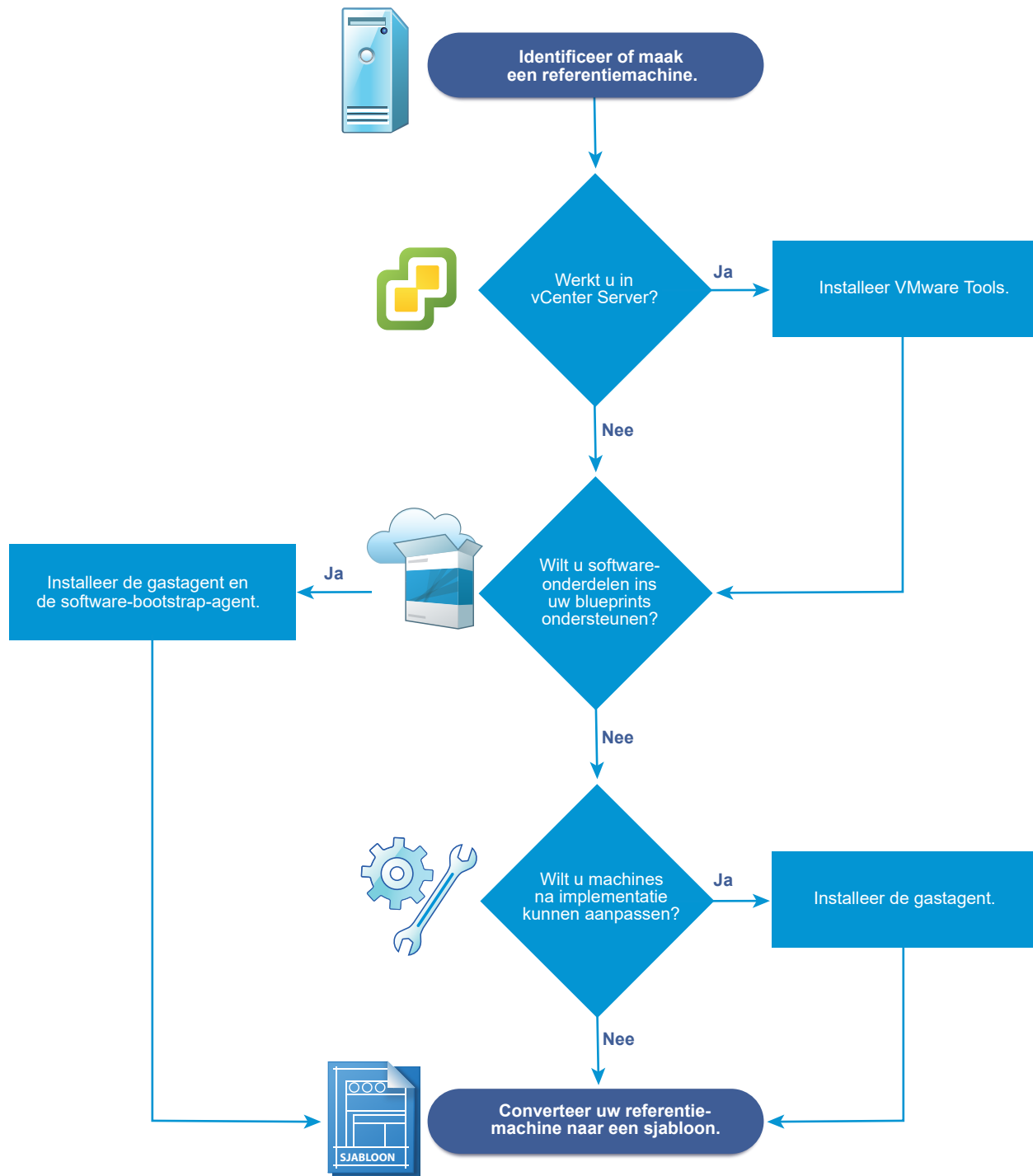
Wat nu te doen

Converteer de referentiemachine naar een sjabloon om te klonen, een image van een Amazon-machine of een momentopname die uw IaaS-architecten kunnen gebruiken voor het maken van blueprints.

Checklist voor de voorbereiding van inrichting door middel van klonen

U moet enige voorbereiding buiten vRealize Automation om verrichten om de sjabloon en aanpassingsobjecten te maken voor het klonen van Linux en Windows virtual machines.

Om te kunnen klonen is een sjabloon vereist, die wordt gemaakt op basis van een referentiemachine.



Als u een Windows-machine inricht door middel van klonen, kunt u de ingerichte machine alleen koppelen aan een Active Directory-domein via de aanpassingsspecificatie van vCenter Server of door een profiel voor een gastbesturingssysteem in de sjabloon voor SCVMM op te nemen. Machines die zijn ingericht door middel van klonen, kunnen niet in een Active Directory-container worden geplaatst tijdens de inrichting. U moet dit handmatig doen, nadat de inrichting gereed is.

Tabel 1-8. Checklist voor de voorbereiding van inrichting door middel van klonen

Taak	Locatie	Details
<input type="checkbox"/> Maak een referentiemachine of geef door welke machine dit is.	Hypervisor	Zie de documentatie die wordt aangeboden door uw hypervisor.
<input type="checkbox"/> (Optioneel) Als de kloonsjabloon Software-onderdelen moet ondersteunen, installeert u de vRealize Automation-gastagent en softwarebootstrapagent op uw referentiemachine.	Referentiemachine	Zie Een Windows-referentiemachine voorbereiden ter ondersteuning van Software voor Windows-referentiemachines. Zie Een Linux-referentiemachine voorbereiden ter ondersteuning van Software voor Linux-referentiemachines.
<input type="checkbox"/> (Optioneel) Als ondersteuning voor Software-onderdelen niet is vereist voor uw kloonsjabloon, maar u de geïmplementeerde machines wel wilt kunnen aanpassen, installeert u de vRealize Automationgastagent op uw referentiemachine.	Referentiemachine	Zie Gastagent voor vRealize Automation gebruiken bij de inrichting .
<input type="checkbox"/> Als u in een vCenter Server-omgeving werkt, installeert u VMware Tools op de referentiemachine.	vCenter Server	Zie de documentatie bij VMware Tools.
<input type="checkbox"/> Gebruik de referentiemachine om een sjabloon te maken om te klonen.	Hypervisor	De referentiemachine mag aan- of uitgezet worden. U bent bezig te klonen in vCenter Server. U kunt hiervoor direct een referentiemachine gebruiken zonder eerst een sjabloon te maken. Zie de documentatie die wordt aangeboden door uw hypervisor.
<input type="checkbox"/> Maak het aanpassingsobject om gekloonde machines te configureren door informatie van de System Preparation Utility toe te passen of de aanpassing van een versie van Linux uit te voeren.	Hypervisor	Als u een kloon uitvoert voor Linux kunt u de Linux-gastagent installeren en externe aanpassingsscripts uitvoeren, in plaats van een aanpassingsobject te maken. Als u kloont met vCenter Server moet u de aangepaste specificatie aanbieden, als het aanpassingsobject. Zie de documentatie die wordt aangeboden door uw hypervisor.
<input type="checkbox"/> Verzamel de informatie die vereist is om blueprints te maken, waarmee uw sjabloon kan worden gekloond.	Leg informatie vast en draag deze over naar uw IaaS-architecten.	Zie Checklist voor de voorbereiding op virtuele inrichting door middel van klonen .

Checklist voor de voorbereiding op virtuele inrichting door middel van klonen

Voltooi de checklist voor kennisoverdracht om informatie vast te leggen over de sjabloon, aanpassingen en aangepaste eigenschappen die vereist zijn om kloonblueprints te maken voor de sjablonen die u in uw omgeving hebt gemaakt. Niet al deze informatie is vereist voor elke implementatie. Gebruik deze checklist als leidraad of kopieer en plak de checklisttabellen naar een tekstverwerkingsprogramma voor bewerking.

Vereiste sjabloon- en reserveringsinformatie

Tabel 1-9. Checklist voor sjabloon- en reserveringsinformatie

Vereiste informatie	Mijn waarde	Details
Naam van sjabloon		
Reserveringen waarop de sjabloon beschikbaar is, of toe te passen reserveringsbeleid		Om fouten bij de inrichting te voorkomen, moet de sjabloon beschikbaar zijn voor alle reserveringen of moeten architecten een reserveringsbeleid gebruiken om de blueprint te beperken tot reserveringen waarvoor de sjabloon beschikbaar is.
(alleen vSphere) Type kloon dat voor deze sjabloon is aangevraagd		<ul style="list-style-type: none"> ■ Klonen ■ Gekoppelde kloon ■ NetApp FlexClone
Naam van aanpassingsspecificatie (Vereist voor klonen met statische IP-adressen)		<p>Zonder vSphere-aanpassingsspecificatie kunt u geen aanpassingen van Windows-machines uitvoeren.</p> <p>Zie Een Linux-machine verbinden met een Windows Active Directory-domein.</p>
(alleen SCVMM) ISO-naam		
(alleen SCVMM) Virtuele harde schijf		
(alleen SCVMM) Hardwareprofiel dat aan ingerichte machines moet worden toegevoegd		

Vereiste eigenschapsgroepen

U kunt de secties voor informatie over aangepaste eigenschappen van de checklist voltooien of u kunt eigenschapsgroepen maken en architecten vragen om uw eigenschapsgroepen aan hun blueprints toe te voegen in plaats van talloze afzonderlijke aangepaste eigenschappen.

Vereist vCenter Server-besturingssysteem

U moet de aangepaste eigenschap van het gastbesturingssysteem leveren voor vCenter Server-inrichting.

Tabel 1-10. vCenter Server-besturingssysteem

Aangepaste eigenschap	Mijn waarde	Beschrijving
VMware.VirtualCenter.OperatingSystem		Geeft de vCenter Server-gastbesturingssysteemversie (VirtualMachineGuestOsIdentificer) op waarmee vCenter Server de machine maakt. Deze besturingssysteemversie moet overeenkomen met de besturingssysteemversie die moet worden geïnstalleerd op de ingerichte machine. Beheerders kunnen eigenschapsgroepen maken met een of meer eigenschapssets, bijvoorbeeld VMware[OS_Version]Properties, die vooraf gedefinieerd zijn om de juiste VMware.VirtualCenter.OperatingSystem-waarden te bevatten. Deze eigenschap dient voor virtuele inrichting.

Visual Basic Script-informatie

Als u vRealize Automation hebt geconfigureerd om uw aangepaste Visual Basic Scripts als aanvullende stappen in de machinelevenscyclus uit te voeren, moet u informatie over de scripts in de blueprint opnemen.

Opmerking Een materiaalbeheerder kan een eigenschapsgroep maken door de eigenschapssets ExternalPreProvisioningVbScript en ExternalPostProvisioningVbScript te gebruiken om deze vereiste informatie door te geven. Op deze manier maakt u het voor blueprintarchitecten makkelijker om deze informatie goed in hun blueprints op te nemen.

Tabel 1-11. Visual Basic Script-informatie

Aangepaste eigenschap	Mijn waarde	Beschrijving
ExternalPreProvisioningVbScript		Voer een script uit vóór de inrichting. Voer het volledige pad naar het script in, inclusief de bestandsnaam en -extensie. <i>%System Drive%Program Files (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs.</i>
ExternalPostProvisioningVbScript		Voer een script uit na de inrichting. Voer het volledige pad naar het script in, inclusief de bestandsnaam en -extensie. <i>%System Drive%Program Files (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs</i>

Informatie over aanpassingsscript van Linux-gastagent

Als u uw Linux-sjabloon hebt geconfigureerd om de gastagent te gebruiken voor het uitvoeren van aanpassingsscripts, moet u informatie opnemen over de scripts in de blueprint.

Tabel 1-12. Checklist met informatie over aanpassingsscript van Linux-gastagent

Aangepaste eigenschap	Mijn waarde	Beschrijving
Linux.ExternalScript.Name		Geeft de naam op van een optioneel aanpassingsscript, bijvoorbeeld <code>config.sh</code> , dat de Linux-gastagent uitvoert nadat het besturingssysteem is geïnstalleerd. Deze eigenschap is beschikbaar voor Linux-machines die gekloond zijn vanaf sjablonen waarop de Linux-agent is geïnstalleerd. Als u een extern script opgeeft, moet u ook de locatie ervan opgeven met behulp van de eigenschappen <code>Linux.ExternalScript.LocationType</code> en <code>Linux.ExternalScript.Path</code> .
Linux.ExternalScript.LocationType		Geeft het locatietype op van het aanpassingsscript dat in de eigenschap <code>Linux.ExternalScript.Name</code> wordt genoemd. Dit kan <code>local</code> of <code>nfs</code> zijn. U moet ook de scriptlocatie opgeven met behulp van de eigenschap <code>Linux.ExternalScript.Path</code> . Als het locatietype <code>nfs</code> is, gebruikt u ook de eigenschap <code>Linux.ExternalScript.Server</code> .
Linux.ExternalScript.Server		Geeft de naam op van de NFS-server, bijvoorbeeld <code>lab-ad.lab.local</code> , waarop het externe Linux-aanpassingsscript dat in <code>Linux.ExternalScript.Name</code> wordt genoemd, zich bevindt.
Linux.ExternalScript.Path		Geeft het lokale pad op naar het Linux-aanpassingsscript of het exportpad naar de Linux-aanpassing op de NFS-server. De waarde moet beginnen met een slash en mag de bestandsnaam niet bevatten, bijvoorbeeld <code>/scripts/linux/config.sh</code> .

Andere aangepaste eigenschappen van de gastagent

Als u de gastagent op uw referentiemachine hebt geïnstalleerd, kunt u aangepaste eigenschappen gebruiken om machines verder aan te passen na de implementatie.

Tabel 1-13. Aangepaste eigenschappen voor het aanpassen van gekloonde machines met een gastagentchecklist

Aangepaste eigenschap	Mijn waarde	Beschrijving
<code>VirtualMachine.Admin.AddOwnerToAdmins</code>		Stel dit in op True (standaardwaarde) om de eigenaar van de machine, zoals opgegeven door de eigenschap <code>VirtualMachine.Admin.Owner</code> , toe te voegen aan de groep met lokale beheerders op de machine.
<code>VirtualMachine.Admin.AllowLogin</code>		Stel dit in op True (standaardwaarde) om de machine-eigenaar toe te voegen aan de groep met lokale Remote Desktop-gebruikers, zoals opgegeven door de eigenschap <code>VirtualMachine.Admin.Owner</code> .
<code>VirtualMachine.Admin.UseGuestAgent</code>		Als de gastagent geïnstalleerd is als een service op een sjabloon voor klonen, stelt u dit in op True op de machineblueprint om de gastagentservice in te schakelen op machines die gekloond zijn vanaf die sjabloon. Als de machine wordt gestart, wordt de gastagentservice gestart. Stel dit in op onwaar om de gastagent te deactiveren. Als dit is ingesteld op False, zal de uitgebreide kloonwerkstroom de gastagent niet gebruiken voor gastbesturingssysteemtaken, waardoor de functionaliteit ervan wordt beperkt tot <code>VMwareCloneWorkflow</code> . Als dit niet is opgegeven of als dit is ingesteld op iets anders dan False, zal de uitgebreide kloonwerkstroom werkitens naar de gastagent verzenden.
<code>VirtualMachine.DiskN.Active</code>		Stel dit in op True (standaardwaarde) om op te geven dat schijf <i>N</i> van de machine actief is. Stel dit in op False om op te geven dat schijf <i>N</i> van de machine niet actief is.
<code>VirtualMachine.DiskN.Label</code>		Geeft het label op voor schijf <i>N</i> van een machine. De maximumgrootte van het schijflabel is 32 tekens. De nummering van schijven moet opeenvolgend zijn. Als dit wordt gebruikt in combinatie met een gastagent, geeft dit het label op van schijf <i>N</i> van een machine in het gastbesturingssysteem.

Tabel 1-13. Aangepaste eigenschappen voor het aanpassen van gekloonde machines met een gastagentchecklist (vervolg)

Aangepaste eigenschap	Mijn waarde	Beschrijving
VirtualMachine.DiskN.Letter		Geeft de stationsletter of het koppelpunt van de schijf <i>N</i> van een machine op. De standaardwaarde is C. Als u bijvoorbeeld de letter D wilt opgeven voor Schijf 1, definieert u de aangepaste eigenschap als VirtualMachine.Disk1.Letter en voert u de waarde D in. De nummering van schijven moet opeenvolgend zijn. Als dit wordt gebruikt in combinatie met een gastagent, geeft deze waarde de stationsletter of het koppelpunt op waaronder een aanvullende schijf <i>N</i> wordt gekoppeld door de gastagent in het gastbesturingssysteem.
VirtualMachine.Admin.CustomizeGuestOSDelay		Geeft de tijd op die u moet wachten nadat de aanpassing is voltooid en voordat u de aanpassing van het gastbesturingssysteem kunt starten. De waarde moet de indeling UU:MM:SS hebben. Als de waarde niet is ingesteld, is de standaardwaarde één minuut (00:01:00). Als u ervoor kiest om deze aangepaste eigenschap niet op te nemen, kan de inrichting mislukken als de virtual machine opnieuw wordt opgestart voordat de gastagentwerkitems zijn voltooid.
VirtualMachine.Customize.WaitComplete		Stel dit in op Waar om te verhinderen dat de inrichtingswerkstroom werkitems verzendt naar de gastagent totdat alle aanpassingen zijn voltooid. Stel dit in op Onwaar om ervoor te zorgen dat werkitems worden gemaakt voordat de aanpassing is voltooid.
VirtualMachine.SoftwareN.Name		Geeft de beschrijvende naam op van de softwaretoepassing <i>N</i> die of het script dat moet worden geïnstalleerd of uitgevoerd tijdens inrichting. Dit is een optionele eigenschap die slechts ter informatie wordt gegeven. Deze heeft geen echte functie voor de uitgebreide kloonwerkstroom of de gastagent, maar is nuttig voor een aangepaste softwareselectie in een gebruikersinterface of voor rapportage over softwaregebruik.

Tabel 1-13. Aangepaste eigenschappen voor het aanpassen van gekloonde machines met een gastagentchecklist (vervolg)

Aangepaste eigenschap	Mijn waarde	Beschrijving
VirtualMachine.SoftwareN.ScriptPath		<p>Geeft het volledige pad op naar het installatiescript van een toepassing. Het pad moet een geldig absoluut pad zijn zoals gezien door het gastbesturingssysteem en moet de naam van de scriptbestandsnaam bevatten.</p> <p>U kunt ook aangepaste eigenschapswaarden als parameters doorgeven naar het script door <i>{CustomPropertyName}</i> in de padtekenreeks toe te voegen. Als u bijvoorbeeld een aangepaste eigenschap hebt met de naam <i>ActivationKey</i> waarvan de waarde 1234 is, dan is het scriptpad <i>D:\InstallApp.bat -key {ActivationKey}</i>. De gastagent voert de opdracht <i>D:\InstallApp.bat -key 1234</i> uit. Uw scriptbestand kan vervolgens worden geprogrammeerd om deze waarde te accepteren en te gebruiken.</p>
VirtualMachine.SoftwareN.ISOName		<p>Geeft het pad en de bestandsnaam van het ISO-bestand op ten opzichte van de datastorehoofdmap. De indeling is <i>/folder_name/subfolder_name/file_name.iso</i>. Als er geen waarde is opgegeven, wordt de ISO niet gekoppeld.</p>
VirtualMachine.SoftwareN.ISOLocation		<p>Geeft het opslagpad op dat het ISO-installatiekopiebestand bevat dat moet worden gebruikt door de toepassing of het script. Gebruik de indeling van het pad zoals het op de hostreservering wordt weergegeven, bijvoorbeeld <i>netapp-1:it_nfs_1</i>. Als er geen waarde is opgegeven, wordt de ISO niet gekoppeld.</p>

Aangepaste netwerkeigenschappen

U kunt de configuratie voor specifieke netwerkapparaten op een machine opgeven door aangepaste eigenschappen te gebruiken.

Veelgebruikte netwerkgerelateerde aangepaste eigenschappen worden weergegeven in de volgende tabel. Voor aanvullende en gerelateerde aangepaste eigenschappen raadpleegt u *Aangepaste eigenschappen voor kloonblueprints* en *Aangepaste eigenschappen voor netwerken* in *Naslaggids voor aangepaste eigenschappen*.

Tabel 1-14. Aangepaste eigenschappen voor netwerkconfiguratie

Aangepaste eigenschap	Mijn waarde	Beschrijving
VirtualMachine.NetworkN.Address		Geeft het IP-adres van netwerkkapparaat <i>N</i> op van een machine die is ingericht met een statisch IP-adres.
VirtualMachine.NetworkN.MacAddressType		<p>Geeft aan of het MAC-adres van netwerkkapparaat <i>N</i> wordt gegenereerd of door de gebruiker wordt gedefinieerd (statisch). Deze eigenschap is beschikbaar voor klonen.</p> <p>De standaardwaarde is 'genereren'. Als de waarde statisch is, moet u ook VirtualMachine.NetworkN.MacAddress gebruiken om het MAC-adres op te geven.</p> <p>Aangepaste eigenschappen met VirtualMachine.NetworkN zijn specifiek voor individuele blueprints en machines. Wanneer een machine wordt aangevraagd, wordt netwerken IP-adrestoewijzing uitgevoerd voordat de machine aan een reservering wordt toegewezen. Omdat blueprints niet noodzakelijk worden toegewezen aan een specifieke reservering, gebruikt u deze eigenschap niet op een reservering. Deze eigenschap wordt niet ondersteund voor NAT- of geleide netwerken op aanvraag.</p>

Tabel 1-14. Aangepaste eigenschappen voor netwerkconfiguratie (vervolg)

Aangepaste eigenschap	Mijn waarde	Beschrijving
VirtualMachine.NetworkN.MacAddress		<p>Geeft het MAC-adres van een netwerkkapparaat <i>N</i> op. Deze eigenschap is beschikbaar voor klonen.</p> <p>Als de waarde van VirtualMachine.NetworkN.MacAddressType wordt gegenereerd, bevat deze eigenschap het gegenereerde adres.</p> <p>Als de waarde van VirtualMachine.NetworkN.MacAddressType statisch is, geeft deze eigenschap het MAC-adres op. Voor virtual machines die zijn ingericht op ESX-serverhosts, moet het adres in het bereik liggen dat is opgegeven door VMware. Zie de vSphere-documentatie voor meer informatie.</p> <p>Aangepaste eigenschappen met VirtualMachine.NetworkN zijn specifiek voor individuele blueprints en machines. Wanneer een machine wordt aangevraagd, wordt netwerken IP-adrestoewijzing uitgevoerd voordat de machine aan een reservering wordt toegewezen. Omdat blueprints niet noodzakelijk worden toegewezen aan een specifieke reservering, gebruikt u deze eigenschap niet op een reservering. Deze eigenschap wordt niet ondersteund voor NAT- of geleide netwerken op aanvraag.</p>

Tabel 1-14. Aangepaste eigenschappen voor netwerkconfiguratie (vervolg)

Aangepaste eigenschap	Mijn waarde	Beschrijving
VirtualMachine.NetworkN.Name		<p>Geeft de naam op van het netwerk waarmee u verbinding wilt maken, bijvoorbeeld het netwerkkapparaat <i>N</i>, waaraan een machine is toegevoegd. Dit is gelijk aan een netwerkkinterfacekaart (NIC).</p> <p>Standaard wordt een netwerk toegewezen vanaf de netwerkpaden die beschikbaar zijn op de reservering waarop de machine is ingericht. Zie ook <code>VirtualMachine.NetworkN.AddressType</code>.</p> <p>U kunt controleren of een netwerkkapparaat verbonden is met een specifiek netwerk door de waarde van deze eigenschap in te stellen op de naam van een netwerk op een beschikbare reservering. Als u bijvoorbeeld eigenschappen opgeeft voor <i>N</i>= 0 en 1, krijgt u 2 NIC's en hun toegewezen waarde, op voorwaarde dat het netwerk geselecteerd is in de gekoppelde reservering.</p> <p>Aangepaste eigenschappen met <code>VirtualMachine.NetworkN</code> zijn specifiek voor blueprints en machines. Wanneer een machine wordt aangevraagd, wordt netwerk- en IP-adrestoewijzing uitgevoerd voordat de machine aan een reservering wordt toegewezen. Omdat blueprints niet noodzakelijk worden toegewezen aan een specifieke reservering, gebruikt u deze eigenschap niet op een reservering. Deze eigenschap wordt niet ondersteund voor NAT- of geleide netwerken op aanvraag.</p> <p>Zie het blogbericht Adding a Network Selection Drop-Down in vRA 7 voor een voorbeeld van hoe u deze aangepaste eigenschap kunt gebruiken om</p> <p><code>VirtualMachine.Network0.Name</code> dynamisch in te stellen op basis van een selectie van de gebruiker uit de lijst met vooraf gedefinieerde beschikbare netwerken.</p>

Tabel 1-14. Aangepaste eigenschappen voor netwerkconfiguratie (vervolg)

Aangepaste eigenschap	Mijn waarde	Beschrijving
VirtualMachine.NetworkN.PortID		<p>Geeft de poort-id op die moet worden gebruikt voor netwerkkapparaat <i>N</i> wanneer u een dvPort-groep gebruikt met een met vSphere gedistribueerde switch.</p> <p>Aangepaste eigenschappen met VirtualMachine.NetworkN zijn specifiek voor individuele blueprints en machines. Wanneer een machine wordt aangevraagd, wordt netwerk- en IP-adrestoewijzing uitgevoerd voordat de machine aan een reservering wordt toegewezen. Omdat blueprints niet noodzakelijk worden toegewezen aan een specifieke reservering, gebruikt u deze eigenschap niet op een reservering. Deze eigenschap wordt niet ondersteund voor NAT- of geleide netwerken op aanvraag.</p>
VirtualMachine.NetworkN.NetworkProfileName		<p>Geeft de naam op van een netwerkprofiel waarvan u een statisch IP-adres moet toewijzen aan netwerkkapparaat <i>N</i> of waarvan u het bereik met statische IP-adressen moet verkrijgen dat kan worden toegewezen aan netwerkkapparaat <i>N</i> van een gekloonde machine, waarbij <i>N</i>=0 is voor het eerste apparaat, 1 voor het tweede enzovoort.</p> <p>Het netwerkprofiel waarnaar de eigenschap verwijst, wordt gebruikt om een IP-adres toe te wijzen. De eigenschap bepaalt het netwerk waaraan de machine wordt gekoppeld, op basis van de reservering.</p>

Tabel 1-14. Aangepaste eigenschappen voor netwerkconfiguratie (vervolg)

Aangepaste eigenschap	Mijn waarde	Beschrijving
<ul style="list-style-type: none"> ■ VirtualMachine.NetworkN.SubnetMask ■ VirtualMachine.NetworkN.Gateway ■ VirtualMachine.NetworkN.PrimaryDns ■ VirtualMachine.NetworkN.SecondaryDns ■ VirtualMachine.NetworkN.PrimaryWins ■ VirtualMachine.NetworkN.SecondaryWins ■ VirtualMachine.NetworkN.DnsSuffix ■ VirtualMachine.NetworkN.DnsSearchSuffixes 		<p>Door een naam toe te voegen kunt u meerdere versies van een aangepaste eigenschap maken. De volgende eigenschappen kunnen bijvoorbeeld pools voor taakverdeling weergeven die zijn ingesteld voor algemeen gebruik, en machines met hoge, gemiddelde en lage prestatievereisten:</p> <ul style="list-style-type: none"> ■ VCNS.LoadBalancerEdgePool.Names ■ VCNS.LoadBalancerEdgePool.Names.moderate ■ VCNS.LoadBalancerEdgePool.Names.high ■ VCNS.LoadBalancerEdgePool.Names.low <p>Configureert kenmerken van het netwerkprofiel dat is opgegeven in VirtualMachine.NetworkN.NetworkProfileName.</p>
VCNS.LoadBalancerEdgePool.Names.name		<p>Geeft de NSX-pools voor taakverdeling op waaraan de virtual machine wordt toegewezen tijdens de inrichting. De virtual machine wordt toegewezen aan alle servicepoorten van alle opgegeven pools. De waarde is de naam van een <i>edge/pool</i> of een lijst met door komma's gescheiden namen van een <i>edge/pool</i>. Namen zijn hoofdlettergevoelig.</p> <p>Door een naam toe te voegen kunt u meerdere versies van een aangepaste eigenschap maken. De volgende eigenschappen kunnen bijvoorbeeld pools voor taakverdeling weergeven die zijn ingesteld voor algemeen gebruik, en machines met hoge, gemiddelde en lage prestatievereisten:</p> <ul style="list-style-type: none"> ■ VCNS.LoadBalancerEdgePool.Names ■ VCNS.LoadBalancerEdgePool.Names.moderate ■ VCNS.LoadBalancerEdgePool.Names.high ■ VCNS.LoadBalancerEdgePool.Names.low

Tabel 1-14. Aangepaste eigenschappen voor netwerkconfiguratie (vervolg)

Aangepaste eigenschap	Mijn waarde	Beschrijving
VCNS.SecurityGroup.Names.name		<p>Geeft de NSX-beveiligingsgroep(en) op waaraan de virtual machine wordt toegewezen tijdens de inrichting. De waarde is de naam van een beveiligingsgroep of een door komma's gescheiden lijst met namen. Namen zijn hoofdlettergevoelig.</p> <p>Door een naam toe te voegen kunt u meerdere versies van de eigenschap maken, die individueel of in combinatie met elkaar kunnen worden gebruikt. De volgende eigenschappen kunnen bijvoorbeeld beveiligingsgroepen weergeven die bedoeld zijn voor algemeen gebruik, voor het verkoopteam en voor ondersteuning:</p> <ul style="list-style-type: none"> ■ VCNS.SecurityGroup.Names ■ VCNS.SecurityGroup.Names.sale s ■ VCNS.SecurityGroup.Names.support
VCNS.SecurityTag.Names.name		<p>Geeft de NSX-beveiligingstag(s) op waaraan de virtual machine wordt gekoppeld tijdens de inrichting. De waarde is de naam van een beveiligingstag of een door komma's gescheiden lijst met namen. Namen zijn hoofdlettergevoelig.</p> <p>Door een naam toe te voegen kunt u meerdere versies van de eigenschap maken, die individueel of in combinatie met elkaar kunnen worden gebruikt. De volgende eigenschappen kunnen bijvoorbeeld beveiligingstags weergeven die bedoeld zijn voor algemeen gebruik, voor het verkoopteam en voor ondersteuning:</p> <ul style="list-style-type: none"> ■ VCNS.SecurityTag.Names ■ VCNS.SecurityTag.Names.sales ■ VCNS.SecurityTag.Names.support

Een Linux-machine verbinden met een Windows Active Directory-domein

Er zijn meerdere manieren om een Linux-machine te verbinden met een Windows Active Directory-domein wanneer u de machine inricht.

- Als u de machine door middel van klonen inricht, moet u ofwel een aanpassingsspecificatie (voor het inrichten van een vSphere- machine) gebruiken, ofwel een gastbesturingssysteemprofiel met een SCVMM-sjabloon toevoegen. Wanneer u de machine inricht, wordt deze met het opgegeven domein verbonden.
- Als u de machine niet door middel van klonen inricht, kunt u de instelling DNS-achtervoegsel in het bijbehorende netwerkprofiel van de blueprint gebruiken om het domein te identificeren. Voor een Windows-klooninrichting met een statische IP-adrestoewijzing *moet* u echter een vSphere-aanpassingsspecificatie gebruiken.
- Als u een vSphere-aanpassingsspecificatie gebruikt, worden de machines bij het inrichten verbonden met het domein dat in de aanpassingsspecificatie is geïdentificeerd, niet met het domein dat is opgegeven als DNS-achtervoegsel in het bijbehorende netwerkprofiel van de blueprint.

vSphere-aanpassingsspecificaties zijn vSphere-objecten die een vooraf gedefinieerde reeks voorwaarden voor instellingen van Windows- en Linux gastbesturingssystemen bevatten. U kunt de naam van een aanpassingsspecificatie toevoegen aan uw vRealize Automation-blueprint met behulp van de instelling **Aanpassingsspecificatie** op het tabblad **Versie-informatie** van de machine.

Zie de onderwerpen met betrekking tot aanpassingsspecificaties in de [vSphere-productdocumentatie](#), zoals *Aanpassingsspecificaties maken en beheren*, voor informatie over het maken van aanpassingsspecificaties in vSphere.

vCloud Air- en vCloud Director-inrichting voorbereiden

Om de inrichting van vCloud Air- en vCloud Director-machines met vRealize Automation voor te bereiden, moet u het virtuele datacenter van de organisatie configureren met behulp van sjablonen en aanpassingsobjecten.

Voor de inrichting van vCloud Air- en vCloud Director-bronnen met vRealize Automation moet de organisatie een sjabloon hebben die kan worden gekloond en een of meer machinebronnen bevat.

Alleen openbare sjablonen kunnen tussen organisaties worden gedeeld. Alleen gereserveerde sjablonen zijn als kloonbron beschikbaar voor vRealize Automation.

Opmerking Als u een blueprint maakt door een sjabloon te klonen, wordt de unieke id van die sjabloon aan de blueprint gekoppeld. De gekoppelde sjabloon wordt herkend wanneer de blueprint in de vRealize Automation-catalogus wordt gepubliceerd en voor de inrichting en gegevensverzameling wordt gebruikt. Als u de sjabloon in vCloud Air of vCloud Director verwijdert, zal de volgende vRealize Automation-inrichting en -gegevensverzameling mislukken omdat de bijbehorende sjabloon niet meer bestaat. In plaats van de sjabloon te verwijderen en opnieuw te maken, bijvoorbeeld om een bijgewerkte versie te uploaden, vervangt u de sjabloon via het sjabloonvervangingsproces van vCloud Air/vCloud Director. Als u vCloud Air of vCloud Director gebruikt om de sjabloon te vervangen (en deze dus niet verwijdert en opnieuw maakt), blijft de unieke id van de sjabloon behouden en kunt u de inrichting en gegevensverzameling onveranderd voortzetten.

In het volgende overzicht ziet u welke stappen u moet uitvoeren voordat u vRealize Automation kunt gebruiken om endpoints te maken en reserveringen en blueprints te definiëren. Voor meer informatie over deze beheertaken raadpleegt u de productdocumentatie van vCloud Air en vCloud Director.

- 1 Maak in vCloud Air of vCloud Director een sjabloon voor klonen en voeg deze toe aan de catalogus van de organisatie.
- 2 Gebruik de sjabloon in vCloud Air of vCloud Director om aangepaste instellingen voor onder meer wachtwoorden, het domein en scripts op te geven voor het gastbesturingssysteem op elke machine.

U kunt een aantal van deze instellingen overschrijven in vRealize Automation.

De mogelijke aanpassingen zijn afhankelijk van het gastbesturingssysteem van de bron.

- 3 Configureer in vCloud Air of vCloud Director de catalogus die met alle mensen in de organisatie wordt gedeeld.

Configureer in vCloud Air of vCloud Director de toegang van accountbeheerders voor de gewenste organisaties om de catalogus toegankelijk te maken voor alle gebruikers en groepen in de organisatie. Als deze deling niet wordt toegewezen, zijn de catalogussjablonen niet zichtbaar voor endpoint- of blueprintarchitecten in vRealize Automation.

- 4 Verzamel de volgende informatie, zodat u deze kunt opnemen in blueprints:
 - De naam van de vCloud Air- of vCloud Director-sjabloon.
 - De totale hoeveelheid opslagruimte die is opgegeven voor de sjabloon.

Vorbereiding op inrichting met Linux Kickstart

De inrichting met Linux Kickstart maakt gebruik van een configuratiebestand om een Linux-installatie op een nieuw ingerichte machine te automatiseren. Ter voorbereiding op de inrichting

moet u een opstartbare ISO-image en een Kickstart- of een autoYaST-configuratiebestand maken.

Hier volgt een overzicht op hoog niveau van de vereiste stappen om de inrichting met Linux Kickstart voor te bereiden:

- 1 Controleer of een DHCP-server beschikbaar is op het netwerk. vRealize Automation kan geen machines inrichten met behulp van de inrichting met Linux Kickstart tenzij DHCP beschikbaar is.
- 2 Bereid het configuratiebestand voor. In het configuratiebestand moet u de locatie opgeven van de vRealize Automation-server en het installatiepakket voor de Linux-agent. Zie [Vorbereiding van het voorbeeld van het configuratiebestand Linux Kickstart](#).
- 3 Bewerk het bestand `isolinux/isolinux.cfg` of `loader/isolinux.cfg` om de naam en locatie op te geven van het configuratiebestand en de juiste Linux-distributiebron.
- 4 Maak de opstartbare ISO-image en sla deze op de locatie op die door het virtualisatieplatform wordt vereist. Raadpleeg de documentatie die door uw hypervisor wordt aangeboden voor informatie over de vereiste locatie.
- 5 (Optioneel) Voeg scripts voor de aanpassing toe.
 - a Zie [Aangepaste scripts in een configuratiebestand voor Kickstart of autoYaST opgeven](#) als u in de configuratie scripts wilt opgeven voor aanpassing na installatie.
 - b Zie [Checklist voor het uitvoeren van Visual Basic-scripts tijdens inrichting](#) als u Visual Basic-scripts wilt oproepen vanuit de blueprint.
- 6 Verzamel de volgende informatie, zodat de architecten van blueprints deze kunnen opnemen in hun blueprints:
 - a De naam en de locatie van de ISO-image.
 - b Voor integraties met vCenter Server de versie van het gastbesturingssysteem voor vCenter Server waarmee vCenter Server de machine moet maken.

Opmerking U kunt een eigenschapsgroep maken waarvan de eigenschapset `BootIsoProperties` de vereiste ISO-informatie bevat. Hierdoor wordt het gemakkelijker om deze informatie op de juiste wijze op te nemen in blueprints.

Vorbereiding van het voorbeeld van het configuratiebestand Linux Kickstart

vRealize Automation bevat een aantal voorbeelden van configuratiebestanden die u kunt aanpassen en bewerken om aan uw behoeften te voldoen. Er zijn diverse wijzigingen vereist om deze bestanden te kunnen gebruiken.

Procedure

- 1 Ga naar de pagina van de beheerconsole voor de vRealize Automation-toepassing.
Bijvoorbeeld: `https://va-hostname.domain.com`.

- 2 Klik op de **pagina voor gast- en softwareagenten** in het gedeelte voor de installatie van onderdelen van vRealize Automation van de pagina.

Bijvoorbeeld: `https://va-hostname.domain.com/software/index.html`.

De pagina **Installatieprogramma's voor gast- en softwareagenten** wordt geopend, met koppelingen naar beschikbare downloads.

- 3 Klik op **Pakketten voor Linux-gastagenten** in het gedeelte voor installatieprogramma's van gastagenten van de pagina om het bestand `LinuxGuestAgentPkgs.zip` te downloaden en op te slaan.

- 4 Pak het gedownloade bestand `LinuxGuestAgentPkgs.zip` uit en maak de map `VraLinuxGuestAgent`.

- 5 Ga naar de submap `VraLinuxGuestAgent` die overeenkomt met het gastbesturingssysteem dat moet worden geïmplementeerd bij de inrichting.

Bijvoorbeeld: `rhel132`.

- 6 Open een bestand in de submap `samples` dat overeenkomt met uw doelsysteem.

Bijvoorbeeld, `samples/sample-https-rhel6-x86.cfg`.

- 7 Vervang alle instanties van de tekenreeks `host=dcac.example.net` door het IP-adres of de volledig gekwalificeerde domeinnaam en het poortnummer voor de Manager Service of de load balancer voor de Manager Service.

Platform	Vereiste indeling
vSphere ESXi	IP-adres, bijvoorbeeld: <code>—host=172.20.9.59</code>
vSphere ESX	IP-adres, bijvoorbeeld: <code>—host=172.20.9.58</code>
SUSE 10	IP-adres, bijvoorbeeld: <code>—host=172.20.9.57</code>
Alle overige	FQDN, bijvoorbeeld: <code>—host=mycompany-host1.mycompany.local:443</code>

- 8 Zoek elke instantie van `gugent.rpm` of `gugent.tar.gz` en vervang de URL `rpm.example.net` met de locatie van het gastagentpakket.

Bijvoorbeeld:

```
rpm -i nfs:172.20.9.59/suseagent/gugent.rpm
```

- 9 Sla het bestand op een locatie op die toegankelijk is voor nieuw ingerichte machines.

Aangepaste scripts in een configuratiebestand voor Kickstart of autoYaST opgeven

U kunt het configuratiebestand wijzigen zodat aangepaste scripts op nieuw ingerichte machines worden gekopieerd of geïnstalleerd. De Linux-agent voert de scripts uit op een specifiek punt in de werkstroom.

Uw script kan verwijzen naar een van de `/properties.xml`-bestanden in de map `/usr/share/gugent/site/werkitem`.

Voorwaarden

- Bereid een configuratiebestand voor Kickstart of autoYaST voor. Zie [Vorbereiding van het voorbeeld van het configuratiebestand Linux Kickstart](#).
- Uw script moet een waarde retourneren die niet nul is wanneer er fouten optreden, om fouten bij het inrichten van de machine te voorkomen.

Procedure

1 Maak of identificeer het script dat u wilt gebruiken.

2 Sla het script op als *NN_scriptnaam*.

Waarbij *NN* een getal met twee cijfers is. Bij de uitvoering van scripts wordt de volgorde van laag naar hoog gehanteerd. Als twee scripts hetzelfde nummer hebben, wordt bij het bepalen van de volgorde de alfabetische volgorde van de *scriptnaam* gebruikt.

3 Zorg ervoor dat uw script uitvoerbaar is.

4 Zoek de sectie voor na de installatie in het configuratiebestand voor Kickstart of autoYaST.

In Kickstart wordt dit aangegeven met `%post`. In autoYaST wordt dit aangegeven met `post-scripts`.

5 Wijzig de sectie voor na de installatie van het configuratiebestand, zodat uw script wordt gekopieerd in de gewenste map `/usr/share/gugent/site/werkitem`.

Aangepaste scripts worden meestal gebruikt voor een virtuele Kickstart of autoYaST met de werkitens SetupOS (voor het maken van een inrichting) en CustomizeOS (voor inrichting van een kloon), maar u kunt op elk moment in de werkstroom scripts laten uitvoeren.

U kunt bijvoorbeeld het configuratiebestand wijzigen, zodat het script `11_addusers.sh` naar de map `/usr/share/gugent/site/SetupOS` wordt gekopieerd op een nieuw ingerichte machine met de volgende opdracht:

```
cp nfs:172.20.9.59/linuxscripts/11_addusers.sh /usr/share/gugent/site/SetupOS
```

Resultaten

De Linux-agent voert het script uit in de volgorde die wordt opgegeven door de map voor het werkitem en de bestandsnaam van het script.

Vorbereiding op inrichting met SCCM

Door vRealize Automation wordt een nieuw ingerichte machine opgestart op basis van een ISO-image en wordt vervolgens de besturing overgegeven aan de opgegeven SCCM-takenreeks.

Vorbereiding van SCCM wordt ondersteund voor de implementatie van Windows-besturingssystemen. Linux wordt niet ondersteund. Softwaredistributie en updates worden niet ondersteund.

Standaard wordt een SCCM-machine geconfigureerd om elke 10 seconden na de inrichting het lidmaatschap in de toepasselijke verzameling te bevestigen. In sommige gevallen kan dit interval problemen veroorzaken met het registratieproces. Er zijn twee eigenschappen beschikbaar om het bevestigingsproces aan te passen. De eerste eigenschap wordt `SCCM refresh collection setting` genoemd. Deze eigenschap is standaard ingesteld op `true` om te bevestigen dat de machine een lidmaatschapscontrole uitvoert. Indien nodig kunt u deze instelling wijzigen in `false` om de machine zo te configureren dat de lidmaatschapscontrole wordt overgeslagen. De tweede eigenschap wordt `SCCM machine membership check interval` genoemd. Zoals is aangegeven, is het standaardinterval 10 seconden. U kunt echter een andere waarde instellen om het heractiveringsinterval te vergroten als u registratieproblemen ondervindt. U vindt beide eigenschappen in de algemene IaaS-instellingen onder **Infrastructuur > Beheer > Algemene instellingen**.

Hier volgt een overzicht op hoog niveau van de vereiste stappen om de inrichting met SCCM voor te bereiden:

- 1 Voor communicatie met SCCM is de NetBIOS-naam van de SCCM-server vereist.

Werk samen met uw netwerkbeheerder om ervoor te zorgen dat ten minste één Distributed Execution Manager (DEM) de FQDN van de SCCM-server kan herleiden naar zijn NetBIOS-naam.

U hoeft DEM's niet rechtstreeks in hetzelfde netwerk te plaatsen als de SCCM-server, maar DEM's moeten de SCCM-server kunnen bereiken via IP.
- 2 Maak een softwarepakket met daarin de vRealize Automation-gastagent. Zie [Een softwarepakket maken voor SCCM-inrichting](#).
- 3 Maak in SCCM de gewenste takenreeks voor de inrichting van de machine. De laatste stap moet het installeren van het softwarepakket zijn, dat u hebt gemaakt en dat de vRealize Automation-gastagent bevat. Zie de documentatie bij SCCM voor informatie over het maken van takenreeksen en het installeren van softwarepakketten.
- 4 Maak een opstartbare ISO-image voor de takenreeks, die zonder aan te raken, kan worden gestart. Standaard wordt door SCCM een opstartbare ISO-image gemaakt, die maar licht hoeft te worden aangeraakt. Voor informatie over de configuratie van SCCM voor ISO-images die niet hoeven te worden aangeraakt om te starten, raadpleegt u de documentatie bij SCCM.
- 5 Kopieer de ISO-image naar de locatie die door het virtualisatieplatform wordt vereist. Als u niet weet wat de juiste locatie is, raadpleegt u de documentatie die door uw hypervisor wordt aangeboden.
- 6 Verzamel de volgende informatie, zodat de architecten van blueprints deze kunnen opnemen in blueprints:
 - a De naam van de verzameling met deze takenreeks.

- b De volledig gekwalificeerde domeinnaam van de SCCM-server waarop de verzameling met de reeks zich bevindt.
- c De code van de site van de SCCM-server.
- d Referentiegegevens op beheerdersniveau voor de SCCM-server.
- e (Optioneel) Voor SCVMM-integraties, de ISO, de virtuele harde schijf of het hardwareprofiel waaraan de machines die worden ingericht, worden gekoppeld.

Een softwarepakket maken voor SCCM-inrichting

De laatste stap in uw volgorde van SCCM-taken is de installatie van een softwarepakket dat de vRealize Automation-gastagent bevat.

Procedure

- 1 Ga naar de pagina van de beheerconsole voor de vRealize Automation-toepassing.
Bijvoorbeeld: <https://va-hostname.domain.com>.
- 2 Klik op de **pagina voor gast- en softwareagenten** in het gedeelte voor de installatie van onderdelen van vRealize Automation van de pagina.
Bijvoorbeeld: <https://va-hostname.domain.com/software/index.html>.
De pagina **Installatieprogramma's voor gast- en softwareagenten** wordt geopend, met koppelingen naar beschikbare downloads.
- 3 Klik op Bestanden voor Windows-gastagenten (**32-bits**) of (**64-bits**) in het gedeelte voor de installatie van onderdelen van de pagina om het bestand `GuestAgentInstaller.exe` of `GuestAgentInstaller_x64.exe` te downloaden en op te slaan.
- 4 Pak de Windows-gastagentbestanden uit naar een locatie die beschikbaar is voor SCCM.
Hiermee wordt de directory `C:\VRMGuestAgent` gemaakt. Wijzig de naam van deze map niet.
- 5 Maak een softwarepakket vanaf het definitiebestand `SCCMPackageDefinitionFile.sms`.
- 6 Maak het softwarepakket beschikbaar op uw distributiepunt.
- 7 Selecteer de inhoud van de uitgepakte Windows-gastagentbestanden als uw bronbestanden.

WIM-inrichting voorbereiden

Richt een machine in door op te starten in een WinPE-omgeving en installeer vervolgens een besturingssysteem met behulp van een WIM-installatiekopie (Windows Imaging File Format) van een bestaande Windows-referentiemachine.

Hier volgt een algemeen overzicht van de vereiste stappen om de WIM-inrichting voor te bereiden:

- 1 Identificeer of maak het faseringsgebied. Het faseringsgebied moet een netwerkdirectory zijn die kan worden opgegeven als een UNC-pad of gekoppeld als een netwerkstation door
 - De referentiemachine.

- Het systeem waarin u de WinPE-image hebt gebouwd.
 - De virtualisatiehost waar u de machines inricht.
- 2 Zorg ervoor dat het netwerk een DHCP-server heeft. vRealize Automation kan geen machines inrichten met een WIM-image tenzij DHCP beschikbaar is.
 - 3 Identificeer of maak op het virtualisatieplatform de referentiemachine die u voor de inrichting wilt gebruiken. Zie [Vereisten voor referentiemachine bij inrichting van WIM](#) voor de vRealize Automation-vereisten. Zie de documentatie van uw hypervisor voor meer informatie over het maken van een referentiemachine.
 - 4 Gebruik de System Preparation Utility for Windows om het besturingssysteem van de referentiemachine voor te bereiden voor de implementatie. Zie [SysPrep-vereisten voor de referentiemachine](#).
 - 5 Maak de WIM-installatiekopie van de referentiemachine. De bestandsnaam van de WIM-installatiekopie mag geen spaties bevatten. Anders mislukt de inrichting.
 - 6 Maak een WinPE-installatiekopie met daarin de vRealize Automation-gastagent.
 - (Optioneel) Als u de ingerichte machines wilt aanpassen, maakt u desgewenst aangepaste scripts. Plaats deze in de bijbehorende werkitemdirectory.
 - Als u VirtIO gebruikt voor netwerk- of opslaginterfaces, moet u controleren of de benodigde stuurprogramma's zijn opgenomen in uw WinPE- en WIM-image. Zie [Voorbereiding op inrichting met WIM met VirtIO-stuurprogramma's](#).

Wanneer u de WinPE-image maakt, moet u handmatig de vRealize Automation-gastagent invoegen. Zie [De gastagent handmatig invoegen in een WinPE-installatiekopie](#).

- 7 Plaats de WinPE-installatiekopie op de vereiste locatie voor uw virtualisatieplatform. Als u de locatie niet kent, raadpleegt u de documentatie van de hypervisor.
- 8 Verzamel de volgende informatie om in de blueprint op te nemen:
 - a De naam en de locatie van de WinPE ISO-image.
 - b De naam van het WIM-bestand, het UNC-pad naar het WIM-bestand en de index die wordt gebruikt om de gewenste image uit het WIM-bestand te halen.
 - c De gebruikersnaam en het wachtwoord waarmee het pad naar de WIM-image kan worden toegewezen aan een netwerkstation op de machine die wordt ingericht.
 - d (Optioneel) Als u de standaardwaarde K niet wilt gebruiken, de letter van het station die voor het pad van de WIM-image is toegewezen op de machine die wordt ingericht.
 - e Voor integraties met vCenter Server de versie van het gastbesturingssysteem voor vCenter Server waarmee vCenter Server de machine moet maken.

- f (Optioneel) Voor SCVMM-integraties, de ISO, de virtuele harde schijf of het hardwareprofiel waaraan de machines die worden ingericht, worden gekoppeld.

Opmerking U kunt een eigenschapsgroep maken waarin al deze vereiste informatie is opgenomen. Met een eigenschapsgroep is het eenvoudiger om de vereiste informatie in de blueprints op te nemen.

Procedure

1 Vereisten voor referentiemachine bij inrichting van WIM

Bij inrichting van WIM moet een WIM-image worden gemaakt op basis van een referentiemachine. De referentiemachine moet voldoen aan de basisvereisten voor de WIM-image om te kunnen fungeren in de inrichting van vRealize Automation.

2 SysPrep-vereisten voor de referentiemachine

Een SysPrep-antwoordbestand bevat verschillende vereiste instellingen voor WIM-inrichtingen.

3 Voorbereiding op inrichting met WIM met VirtIO-stuurprogramma's

Als u VirtIO gebruikt voor netwerk- of opslaginterfaces, moet u controleren of de benodigde stuurprogramma's zijn opgenomen in uw WinPE- en WIM-image. VirtIO biedt doorgaans betere prestaties bij de inrichting met KVM (RHEV).

4 De gastagent handmatig invoegen in een WinPE-installatiekopie

U moet de vRealize Automation-gastagent handmatig invoegen in uw WinPE-image.

Vereisten voor referentiemachine bij inrichting van WIM

Bij inrichting van WIM moet een WIM-image worden gemaakt op basis van een referentiemachine. De referentiemachine moet voldoen aan de basisvereisten voor de WIM-image om te kunnen fungeren in de inrichting van vRealize Automation.

Hier volgt een overzicht op hoog niveau van de vereiste stappen om de referentiemachine voor te bereiden:

- 1 Als het besturingssysteem op uw referentiemachine Windows Server 2008 R2, Windows Server 2012, Windows 7 of Windows 8 is, wordt door de standaard installatie een kleine partitie op de harde schijf van het systeem gemaakt, naast de belangrijkste partitie. vRealize Automation ondersteunt het gebruik van WIM-images die zijn gemaakt op een referentiemachine met meerdere partities, niet. U moet deze partitie verwijderen tijdens het installatieproces.
- 2 Installeer NET 4.5 en Windows AIK (Automated Installation Kit) voor Windows 7 (inclusief WinPE 3.0) op de referentiemachine.
- 3 Als het besturingssysteem op de referentiemachine Windows Server 2003 of Windows XP is, met het wachtwoord voor de beheerder leeg worden gemaakt. (Er is dan geen wachtwoord.)
- 4 (Optioneel) Als u XenDesktop-integratie wilt inschakelen, moet u Citrix Virtual Desktop Agent installeren en configureren.

- 5 (Optioneel) Een WMI-agent (Windows Management Instrumentation) is vereist om bepaalde gegevens te verzamelen op een Windows-machine die wordt beheerd door vRealize Automation, bijvoorbeeld de status van de Active Directory van de eigenaar van de machine. Als u het beheer van de Windows-machines wilt laten slagen, moet u een WMI-agent installeren (meestal gebeurt dit op de Manager Service-host) en de agent activeren om gegevens van de Windows-machines te verzamelen. Zie *vRealize Automation installeren*.

SysPrep-vereisten voor de referentiemachine

Een SysPrep-antwoordbestand bevat verschillende vereiste instellingen voor WIM-inrichtingen.

Tabel 1-15. vereiste SysPrep-instellingen voor Windows Server- of Windows XP-referentiemachine

GuiUnattended-instellingen	Waarde
AutoLogon	Ja
AutoLogonCount	1
AutoLogonUsername	<i>username</i> (<i>username</i> en <i>password</i> zijn de verificatiegegevens voor de automatische aanmelding wanneer het gastbesturingssysteem van de nieuw ingerichte machine wordt opgestart. Doorgaans is dit de beheerdersaccount.)
AutoLogonPassword	<i>wachtwoord</i> voor AutoLogonUsername.

Tabel 1-16. Vereiste SysPrep-instellingen voor referentiemachine doe niet werken met Windows Server 2003 of Windows XP:

AutoLogon-instellingen	Waarde
Enabled	Ja
LogonCount	1

Tabel 1-16. Vereiste SysPrep-instellingen voor referentiemachine doe niet werken met Windows Server 2003 of Windows XP: (vervolg)

AutoLogon-instellingen	Waarde
Username	<i>username</i> <i>(username en password zijn de verificatiegegevens voor de automatische aanmelding wanneer het gastbesturingssysteem van de nieuw ingerichte machine wordt opgestart. Doorgaans is dit de beheerdersaccount.)</i>
Password	<i>wachtwoord</i> <i>(username en password zijn de verificatiegegevens voor de automatische aanmelding wanneer het gastbesturingssysteem van de nieuw ingerichte machine wordt opgestart. Doorgaans is dit de beheerdersaccount.)</i> Opmerking Voor referentiemachines die werken met een nieuwer Windows-platform dan Windows Server 2003/ Windows XP, gebruikt u de aangepaste eigenschap Sysprep.GuiUnattended.AdminPassword om het wachtwoord voor de automatische aanmelding in te stellen. U kunt dit het beste regelen door een aangepaste eigenschapsgroep te maken waarin deze aangepaste eigenschap is opgenomen. Tenant- en bedrijfsgroepbeheerders kunnen deze gegevens dan op de juiste wijze overnemen in hun blueprints.

Voorbereiding op inrichting met WIM met VirtIO-stuurprogramma's

Als u VirtIO gebruikt voor netwerk- of opslaginterfaces, moet u controleren of de benodigde stuurprogramma's zijn opgenomen in uw WinPE- en WIM-image. VirtIO biedt doorgaans betere prestaties bij de inrichting met KVM (RHEV).

Windows-stuurprogramma's voor VirtIO maken deel uit van de Red Hat Enterprise Virtualization en bevinden zich in de map `/usr/share/virtio-win` op het bestandssysteem van de Red Hat Enterprise Virtualization Manager. De stuurprogramma's maken ook deel uit van de Red Hat Enterprise Virtualization Guest Tools die zich in `/usr/share/rhev-guest-tools-iso/rhev-tools-setup.iso` bevinden.

Het proces op een hoog niveau voor het activeren van een op WIM gebaseerde inrichting met VirtIO-stuurprogramma's ziet er zo uit:

- 1 Maak een WIM-image op basis van een Windows-referentiemachine waarop de VirtIO-stuurprogramma's zijn geïnstalleerd of voeg de stuurprogramma's toe aan een bestaande WIM-image.
- 2 Kopieer de VirtIO-stuurprogrammabestanden en voeg de stuurprogramma's in in een WinPE-image.
- 3 Upload de WinPE ISO-image naar het Red Hat Enterprise Virtualization ISO-opslagdomein met de opdracht `rhev-m-iso-uploader`. Raadpleeg de documentatie bij Red Hat voor meer informatie over het beheer van ISO-images.

- 4 Maak een KVM (RHEV)-blueprint voor de inrichting van WIM en selecteer de optie WinPE ISO. De aangepaste eigenschap `VirtualMachine.Admin.DiskInterfaceType` moet worden opgenomen bij de waarde **VirtIO**. Een materiaalbeheerder kan deze informatie opnemen in een eigenschapsgroep, zodat deze ook wordt opgenomen in blueprints.

De aangepaste eigenschappen `Image.ISO.Location` en `Image.ISO.Name` worden niet gebruikt voor KVM (RHEV)-blueprints.

De gastagent handmatig invoegen in een WinPE-installatiekopie

U moet de vRealize Automation-gastagent handmatig invoegen in uw WinPE-image.

Voorwaarden

- Selecteer een Windows-systeem waarvan het faseringsgebied dat u hebt voorbereid, toegankelijk is en waarop .NET 4.5 en Windows Automated Installation Kit (AIK) voor Windows 7 (inclusief WinPE 3.0) zijn geïnstalleerd.
- Maak een WinPE.

Procedure

1 [De gastagent in een WinPE installeren](#)

U moet de gastagentbestanden handmatig naar uw WinPE-image kopiëren.

2 [Het bestand `doagent.bat` configureren](#)

Tot slot moet u het bestand `doagent.bat` configureren.

3 [Het bestand `doagentc.bat` configureren](#)

Tot slot moet u het bestand `doagentc.bat` configureren.

4 [De gastagenteigenschapsbestanden configureren](#)

U moet de gastagenteigenschapsbestanden handmatig configureren.

Procedure

1 [De gastagent in een WinPE installeren.](#)

2 [Het bestand `doagent.bat` configureren.](#)

3 [Het bestand `doagentc.bat` configureren.](#)

4 [De gastagenteigenschapsbestanden configureren.](#)

De gastagent in een WinPE installeren

U moet de gastagentbestanden handmatig naar uw WinPE-image kopiëren.

Voorwaarden

- Selecteer een Windows-systeem waarvan het faseringsgebied dat u hebt voorbereid, toegankelijk is en waarop .NET 4.5 en Windows Automated Installation Kit (AIK) voor Windows 7 (inclusief WinPE 3.0) zijn geïnstalleerd.

- Maak een WinPE.

Procedure

- ◆ Download en installeer de vRealize Automation-gastagent via https://vRealize_VA_Hostname_fqdn/software/index.html.
 - a Download `GugentZip_versie` naar het C-station op de referentiemachine.
Selecteer `GuestAgentInstaller.exe` (32-bits) of `GuestAgentInstaller_x64.exe` (64-bits), afhankelijk van de versie die geschikt is voor uw besturingssysteem.
 - b Klik met de rechtermuisknop op het bestand en selecteer **Eigenschappen**.
 - c Klik op **Algemeen**.
 - d Klik op **Blokking opheffen**.
 - e Pak de bestanden uit naar `C:\`.
Hiermee wordt de directory `C:\VRMGuestAgent` gemaakt. Wijzig de naam van deze map niet.

Wat nu te doen

[Het bestand `doagent.bat` configureren.](#)

Het bestand `doagent.bat` configureren

Tot slot moet u het bestand `doagent.bat` configureren.

Voorwaarden

[De gastagent in een WinPE installeren.](#)

Procedure

- 1 Ga naar de `VRMGuestAgent`-map in uw WinPE-installatiekopie.
Bijvoorbeeld: `C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent`.
- 2 Maak een kopie van het bestand `doagent-template.bat` en geef het de naam `doagent.bat`.
- 3 Open `doagent.bat` in een teksteditor.

- 4 Vervang alle instanties van de tekenreeks `#Dcac Hostname#` door de volledig gekwalificeerde domeinnaam en het poortnummer van de IaaS Manager Service-host.

Optie	Beschrijving
Als u een load balancer gebruikt	Voer de volledig gekwalificeerde domeinnaam en poort van de load balancer voor de IaaS Manager Service in. Bijvoorbeeld: <code>manager_service_LB.mycompany.com:443</code>
Zonder load balancer	Voer de volledig gekwalificeerde domeinnaam en poort in van de machine waarop de IaaS Manager Service is geïnstalleerd. Bijvoorbeeld: <code>manager_service.mycompany.com:443</code>

- 5 Vervang alle instanties van de tekenreeks `#Protocol#` door de tekenreeks `/ssl`.
- 6 Vervang alle instanties van de tekenreeks `#Comment#` door `REM` (`REM` moet worden gevolgd door een afsluitende spatie).
- 7 (Optioneel) Als u automatisch ondertekende certificaten gebruikt, verwijdert u opmerkingen voor de openssl-opdracht.

```
echo QUIT | c:\VRMGuestAgent\bin\openssl s_client -connect
```

- 8 Sla het bestand op en sluit het.
- 9 Bewerk het script `Startnet.cmd` voor uw WinPE om het `doagent.bat` op te nemen als een aangepast script.

Wat nu te doen

[Het bestand `doagentc.bat` configureren.](#)

Het bestand `doagentc.bat` configureren

Tot slot moet u het bestand `doagentc.bat` configureren.

Voorwaarden

[Het bestand `doagent.bat` configureren.](#)

Procedure

- 1 Ga naar de `VRMGuestAgent`-map in uw WinPE-installatiekopie.
Bijvoorbeeld: `C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent`.
- 2 Maak een kopie van het bestand `doagentsvc-template.bat` en geef het de naam `doagentc.bat`.
- 3 Open `doagentc.bat` in een teksteditor.
- 4 Verwijder alle instanties van de tekenreeks `#Comment#`.

- 5 Vervang alle instanties van de tekenreeks `#Dcac Hostname#` door de volledig gekwalificeerde domeinnaam en het poortnummer van de Manager Service-host.

De standaardpoort voor de Manager Service is 443.

Optie	Beschrijving
Als u een load balancer gebruikt	Voer de volledig gekwalificeerde domeinnaam en poort van de load balancer voor de Manager Service in. Bijvoorbeeld: <code>load_balancer_manager_service.mycompany.com:443</code>
Zonder load balancer	Voer de volledig gekwalificeerde domeinnaam en poort van de Manager Service in. Bijvoorbeeld: <code>manager_service.mycompany.com:443</code>

- 6 Vervang alle instanties van de tekenreeks `#errorlevel#` door het teken 1.
- 7 Vervang alle instanties van de tekenreeks `#Protocol#` door de tekenreeks `/ssl`.
- 8 Sla het bestand op en sluit het.

Wat nu te doen

[De gastagenteigenschapsbestanden configureren.](#)

De gastagenteigenschapsbestanden configureren

U moet de gastagenteigenschapsbestanden handmatig configureren.

Voorwaarden

[Het bestand `doagentc.bat` configureren.](#)

Procedure

- 1 Ga naar de VRMGuestAgent-map in uw WinPE-installatiekopie.
Bijvoorbeeld: `C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent`.
- 2 Maak een kopie van het bestand `gugent.properties` en geef het de naam `gugent.properties.template`.
- 3 Maak een kopie van het bestand `gugent.properties.template` en geef het de naam `gugentc.properties`.
- 4 Open `gugent.properties` in een teksteditor.
- 5 Vervang alle instanties van de tekenreeks `GuestAgent.log` door de tekenreeks `X:/VRMGuestAgent/GuestAgent.log`.
- 6 Sla het bestand op en sluit het.
- 7 Open `gugentc.properties` in een teksteditor.

- 8 Vervang alle instanties van de tekenreeks `GuestAgent.log` door de tekenreeks `C:/VRMGuestAgent/GuestAgent.log`.
- 9 Sla het bestand op en sluit het.

Inrichting met virtual machine-installatiekopie voorbereiden

U kunt instanties met OpenStack pas inrichten, nadat u de installatiekopieën en soorten voor virtual machines hebt geconfigureerd in de OpenStack-provider.

Images van virtual machines

U kunt een image van een virtual machine selecteren in een lijst met beschikbare images, wanneer u blueprints maakt voor een OpenStack-bron.

Een image van een virtual machine is een sjabloon die de softwareconfiguratie bevat, inclusief een besturingssysteem. Images van virtual machines worden beheerd door de OpenStack-provider en worden geïmporteerd tijdens het verzamelen van gegevens.

Als een image die wordt gebruikt in een blueprint, later wordt verwijderd uit de OpenStack-provider, wordt deze ook verwijderd uit de blueprint. Als alle images zijn verwijderd uit een blueprint, is de blueprint gedeactiveerd en kan deze niet meer worden gebruikt voor machineaanvragen, totdat de blueprint is bewerkt en er ten minste één image aan toe is gevoegd.

OpenStack-soorten

U kunt één of meer soorten selecteren wanneer u OpenStack-blueprints maakt.

OpenStack-soorten zijn virtuele hardwaresjablonen waarmee de specificaties van de bronnen worden gedefinieerd voor instanties in OpenStack. Soorten worden beheerd door de OpenStack-provider en worden geïmporteerd tijdens het verzamelen van gegevens.

Inrichting met installatiekopieën voor Amazon-machines voorbereiden

Bereid de installatiekopieën en instantietypen voor Amazon-machines voor in vRealize Automation.

Informatie over images van Amazon-machines

Wanneer u blueprints voor een Amazon-machine maakt, kunt u uit een lijst met beschikbare images een image van een Amazon-machine selecteren.

Een image van een Amazon-machine is een sjabloon die de softwareconfiguratie bevat, inclusief een besturingssysteem. Deze worden beheerd door Amazon Web Services-accounts. vRealize Automation beheert de instantietypes die beschikbaar zijn voor het inrichten.

De image van de Amazon-machine en het instantietype moeten beschikbaar zijn in de Amazon-regio. Niet alle instantietypes zijn beschikbaar in alle regio's.

U kunt een image van een Amazon-machine selecteren die wordt aangeboden door Amazon Web Services, een gebruikersgemeenschap of de site AWS Marketplace. U kunt ook uw eigen images van Amazon-machines maken en eventueel delen. Een image van een Amazon-machine kan worden gebruikt om één of meer instanties te starten.

De volgende overwegingen zijn van toepassing op images van Amazon-machines in de Amazon Web Services-accounts waarmee u cloudmachines gaat inrichten:

- In elke blueprint moet een image voor een Amazon-machine zijn opgegeven.
Een persoonlijke image van een Amazon-machine is beschikbaar voor een specifieke account en alle bijbehorende regio's. Een openbare image van een Amazon-machine is beschikbaar voor alle accounts, maar uitsluitend voor een specifieke regio voor elke account.
- Wanneer de blueprint wordt gemaakt, wordt de opgegeven image van de Amazon-machine geselecteerd uit de regio's waarvan de gegevens zijn verzameld. Als er meerdere Amazon Web Services-accounts beschikbaar zijn, moet de bedrijfsgroepbeheerder over rechten beschikken voor persoonlijke images van Amazon-machines. Aan de hand van de regio van de image van een Amazon-machine en de locatie van de opgegeven gebruiker wordt de inrichtingsaanvraag beperkt tot reserveringen die overeenkomen met de betreffende regio en locatie.
- Gebruik reserveringen en beleid om images van Amazon-machines te distribueren voor uw Amazon Web Services-accounts. Gebruik beleid om het inrichten vanaf een blueprint te beperken tot een bepaalde set reserveringen.
- vRealize Automation kan geen gebruikersaccounts maken op een cloudmachine. De eerste maal dat een eigenaar van een machine verbinding maakt met een cloudmachine, moet hij of zij zich aanmelden als beheerder en zijn of haar verificatiegegevens voor vRealize Automation toevoegen of een beheerder vragen om dat te doen. Hij of zij kan zich vervolgens aanmelden met zijn of haar verificatiegegevens voor vRealize Automation.

Als de image van de Amazon-machine telkens een nieuw wachtwoord voor de beheerder genereert als de machine wordt opgestart, wordt het wachtwoord op de pagina Machinerecord bewerken weergegeven. Als dit niet het geval is, kunt u het wachtwoord vinden in de Amazon Web Services-account. U kunt alle images voor Amazon-machines zo configureren dat het wachtwoord voor de beheerder opnieuw wordt gegenereerd als de machine wordt opgestart. U kunt ook informatie over het wachtwoord voor de beheerder doorgeven om gebruikers te ondersteunen die machines voor andere gebruikers inrichten.

- Om externe Microsoft Windows Management Instrumentation (WMI)-verzoeken op cloudmachines die zijn ingericht in Amazon Web Services-accounts toe te staan, dient u een Microsoft Windows Remote Management (WinRM)-agent in te schakelen om gegevens te verzamelen van Windows-machines die worden beheerd door vRealize Automation. Zie *vRealize Automation installeren*.
- Een persoonlijke image van een Amazon-machine kan vanuit meerdere tenants worden gezien.

Zie de onderwerpen *Amazon Machine Images (AMI)* in de Amazon-documentatie voor meer informatie.

Informatie over Amazon-instantietypes

Een IaaS-architect selecteert een of meer Amazon-instantietypen bij het maken van Amazon EC2-blueprints. Een IaaS-beheerder kan instantietypen toevoegen of verwijderen voor het beheren van de keuzen die beschikbaar zijn voor architecten.

Een Amazon EC2-instantie is een virtuele server waarop toepassingen kunnen worden uitgevoerd in Amazon Web Services. Instanties worden gemaakt aan de hand van een image van een Amazon-machine en door de juiste instantietypes te kiezen.

Als u een machine wilt inrichten voor een Amazon Web Services-account, wordt een instantietype toegepast op de opgegeven image van de Amazon-machine. De beschikbare instantietypen worden vermeld in de lijst wanneer architecten de blueprint voor Amazon EC2 maken. Architecten selecteren een of meer instantietypen en deze instantietypen worden keuzen die beschikbaar zijn voor de gebruiker wanneer deze aanvraagt een machine in te richten. De instantietypes moeten in de betreffende regio worden ondersteund.

Voor aanvullende informatie raadpleegt u de onderwerpen *Selecting Instance Types* en *Amazon EC2 Instance Details* in de Amazon-documentatie.

Een Amazon-instantietype toevoegen

Er worden verschillende instantietypen meegeleverd bij vRealize Automation voor gebruik met Amazon-blueprints. Een beheerder kan instantietypen toevoegen en verwijderen.

De instantietypen van machines die worden beheerd door IaaS-beheerders zijn beschikbaar voor blueprintarchitecten bij het maken of bewerken van een Amazon-blueprint. Installatiekopieën en instantietypen van Amazon-machines worden beschikbaar gemaakt via het Amazon Web Services-product.

Voorwaarden

Meld u aan bij vRealize Automation als een **IaaS-beheerder**.

Procedure

- 1 Klik op **Infrastructuur > Beheer > Instantietypen**.
- 2 Klik op **Nieuw**.
- 3 Voeg een nieuw instantietype toe en geef de volgende parameters op.

Informatie over de beschikbare Amazon-instantietypen en de instellingswaarden die u kunt opgeven voor deze parameters, is beschikbaar in de Amazon Web Services-documentatie in *EC2 Instance Types - Amazon Web Services (AWS)* op aws.amazon.com/ec2 en *Instance Types* op docs.aws.amazon.com.

- Naam
- API-naam

- Naam van type
- IO-prestatienaam
- CPU's
- Geheugen (GB)
- Opslag (GB)
- Rekeneenheden

4 Klik op het pictogram **Opslaan** ()

Resultaten

Wanneer IaaS-architecten Amazon Web Services-blueprints maken, kunnen ze uw aangepaste instantietypen gebruiken.

Wat nu te doen

Voeg de computerbronnen van uw endpoint toe aan een materiaalgroep. Zie [Een materiaalgroep maken](#).

Scenario: vSphere-bronnen voorbereiden op machine-inrichting

Als de vSphere-beheerder die sjablonen voor vRealize Automation maakt, wilt u de vSphere Web Client gebruiken om het klonen van CentOS-machines in vRealize Automation voor te bereiden.

U wilt een bestaande CentOS-referentiemachine converteren naar een vSphere-sjabloon zodat u en uw architecten blueprints kunnen maken voor het klonen van CentOS-machines in vRealize Automation. Om conflicten te voorkomen die zouden kunnen optreden bij de implementatie van meerdere virtual machines met identieke instellingen, wilt u ook een algemene aanpassingsspecificatie maken die u en uw architecten kunnen gebruiken om kloonblueprints voor Linux-sjablonen te maken.

Voorwaarden

Identificeer of maak een Linux CentOS-referentiemachine waarop VMware Tools is geïnstalleerd. Neem minstens één netwerkadapter op om een internetverbinding te bieden.

Procedure

1 [Scenario: uw CentOS-referentiemachine omzetten in een sjabloon voor Rainpole](#)

Met behulp van de vSphere Client converteert u uw bestaande CentOS-referentiemachine naar een vSphere-sjabloon waarnaar uw vRealize Automation IaaS-architecten kunnen verwijzen als basis voor hun kloonblueprints.

2 [Scenario: een aanpassingsspecificatie maken voor het klonen van Linux-machines](#)

Maak met behulp van de vSphere Client een standaard aanpassingsspecificatie die uw vRealize Automation IaaS-architecten kunnen gebruiken bij het maken van kloonblueprints voor Linux-machines.

Scenario: uw CentOS-referentiemachine omzetten in een sjabloon voor Rainpole

Met behulp van de vSphere Client converteert u uw bestaande CentOS-referentiemachine naar een vSphere-sjabloon waarnaar uw vRealize Automation IaaS-architecten kunnen verwijzen als basis voor hun kloonblueprints.

Procedure

- 1 Meld u aan bij uw referentiemachine als de hoofdgebruiker en bereid de machine voor op de conversie.

- a Verwijder de udev-persistentieregels.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- b Ingeschakelde machines die op basis van deze sjabloon zijn gekloond, hebben hun eigen unieke id's.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- c Schakel de machine uit.

```
shutdown -h now
```

- 2 Meld u aan bij de vSphere Web Client als een beheerder.
- 3 Klik op het tabblad **VM-opties**.
- 4 Klik met de rechtermuisknop op de referentiemachine en selecteer **Instellingen bewerken**.
- 5 Voer **Rainpole_centos_63_x86** in het tekstvak **VM-naam** in.
- 6 Hoewel uw referentiemachine CentOS als gastbesturingssysteem heeft, selecteert u **Red Hat Enterprise Linux 6 (64-bit)** in het vervolgkeuzemenu **Versie gastbesturingssysteem**.

Als u CentOS selecteert, functioneert uw sjabloon en de aangepaste specificatie mogelijk niet op de verwachte wijze.

- 7 Klik met de rechtermuisknop op uw referentiemachine **Rainpole_centos_63_x86** in de vSphere Web Client en selecteer **Sjabloon > Converteren naar sjabloon**.

Resultaten

vCenter Server markeert de referentiemachine Rainpole_centos_63_x86 als een sjabloon en geeft de taak weer in het venster Recente taken.

Wat nu te doen

Om conflicten te voorkomen die zouden kunnen optreden bij de implementatie van meerdere virtual machines met identieke instellingen, maakt u een algemene aanpassingsspecificatie die u en uw Rainpole-architecten kunnen gebruiken om kloonblueprints voor Linux-sjablonen te maken.

Scenario: een aanpassingsspecificatie maken voor het klonen van Linux-machines

Maak met behulp van de vSphere Client een standaard aanpassingsspecificatie die uw vRealize Automation IaaS-architecten kunnen gebruiken bij het maken van kloonblueprints voor Linux-machines.

Procedure

- 1 Klik op de startpagina op **Manager aanpassingsspecificatie** om de wizard te openen.
- 2 Klik op het pictogram **Nieuw**.
- 3 Geef de eigenschappen op.
 - a Selecteer **Linux** in het vervolgkeuzemenu **Besturingssysteem voor VM van doel**.
 - b Voer **Linux** in het tekstvak **Naam Specificatie aanpassing** in.
 - c Voer **Rainpole Linux klonen met vRealize Automation** in het tekstvak **Beschrijving** in.
 - d Klik op **Volgende**.
- 4 Stel de naam van de computer in.
 - a Selecteer **Naam van virtual machine gebruiken**.
 - b Voer in het tekstvak **Domeinnaam** het domein in waarop gekloonde machines zullen worden ingericht.
 - c Klik op **Volgende**.
- 5 Configureer de instellingen van de tijdzones.
- 6 Klik op **Volgende**.
- 7 Selecteer **Standaardnetwerkinstellingen gebruiken voor het gastbesturingssysteem, inclusief het inschakelen van DHCP voor alle netwerkinterfaces**.
- 8 Volg de prompts en geef de resterende vereiste informatie op.
- 9 Controleer in de pagina **Gereed om te voltooiën** uw selecties en klik op **Voltooiën**.

Vorbereiding op inrichting met Software

Gebruik Software om toepassingen en middleware te implementeren als deel van het vRealize Automation-inrichtingsproces voor vSphere-, vCloud Director-, vCloud Air-, Amazon Web Services- en Microsoft Azure-machines.

U kunt Software op machines implementeren als uw blueprint Software ondersteunt en als u de gastagent en de software-bootstrapagent op uw referentiemachines installeert voordat u deze converteert naar sjablonen, momentopnamen of machine images.

Zie de *Referentie-architectuur* PDF in de [vRealize Automation-productdocumentatie](#) voor gerelateerde informatie over het opgeven van poorten tijdens het voorbereiden op de provisioning van machines.

Tabel 1-17. Inrichtingsmethoden die Software ondersteunen

Machinetype	Vorbereiding
vSphere	Bij een kloonblueprint wordt een complete en onafhankelijke virtual machine ingericht op basis van een vCenter Server-sjabloon voor virtual machines. Als u wilt dat uw sjablonen voor klonen ondersteuning bieden voor Software-onderdelen, installeert u de gastagent en de software-bootstrapagent op uw referentiemachine wanneer u een sjabloon voorbereidt voor het klonen. Zie Checklist voor de voorbereiding van inrichting door middel van klonen .
vSphere	Met een gekoppelde kloonblueprint wordt een ruimtebesparende kopie van een vSphere-machine ingericht op basis van een momentopname met behulp van een keten van deltaschijven om de verschillen met de oorspronkelijke machine vast te leggen. Als u wilt dat uw gekoppelde kloonblueprints ondersteuning bieden voor Software-onderdelen, installeert u de gastagent en de software-bootstrapagent op de machine voordat u de momentopname maakt. Als uw momentopnamemachine is gekloond vanaf een sjabloon dat ondersteuning biedt voor Software, zijn de vereiste agenten al geïnstalleerd.
vCloud Director	Bij een kloonblueprint wordt een complete en onafhankelijke virtual machine ingericht op basis van een vCenter Server-sjabloon voor virtual machines. Als u wilt dat uw sjablonen voor klonen ondersteuning bieden voor Software-onderdelen, installeert u de gastagent en de software-bootstrapagent op uw referentiemachine wanneer u een sjabloon voorbereidt voor het klonen. Zie Checklist voor de voorbereiding van inrichting door middel van klonen .
vCloud Air	Bij een kloonblueprint wordt een complete en onafhankelijke virtual machine ingericht op basis van een vCenter Server-sjabloon voor virtual machines. Als u wilt dat uw sjablonen voor klonen ondersteuning bieden voor Software-onderdelen, installeert u de gastagent en de software-bootstrapagent op uw referentiemachine wanneer u een sjabloon voorbereidt voor het klonen. Zie Checklist voor de voorbereiding van inrichting door middel van klonen .
Amazon Web Services	Een image van een Amazon-machine is een sjabloon die de softwareconfiguratie bevat, inclusief een besturingssysteem. Als u een image van een Amazon-machine wilt maken die ondersteuning biedt voor Software, maakt u verbinding met een actieve Amazon Web Services-instantie die een EBS-volume gebruikt voor het hoofdapparaat. Installeer de gastagent en de software-bootstrapagent op de referentiemachine en maak een image van een Amazon-machine vanaf uw instantie. Als u wilt dat de gastagent en de Software-bootstrapagent werken op ingerichte machines, moet u netwerk-naar-VPC-connectiviteit configureren. Raadpleeg de documentatie bij Amazon Web Services voor instructies over het maken van door EBS ondersteunde images van Amazon-machines.
Microsoft Azure	Zie Instellingen voor Software-onderdelen -, Een blueprint maken voor Microsoft Azure - en Microsoft Azure-productdocumentatie voor informatie.

Inrichten van machines met Software voorbereiden

Als u Software-onderdelen wilt ondersteunen, moet u de gastagent en de Software-bootstrapagent op uw referentiemachine installeren voordat u deze omzet in een sjabloon voor klonen, een installatiekopie van een Amazon-machine maakt of een momentopname maakt.

Een Windows-referentiemachine voorbereiden ter ondersteuning van Software

U gebruikt één script voor installatie van de Java Runtime Environment, de gastagent en de Software-bootstrap-agent op een Windows-referentiemachine. U kunt vanuit de

referentiemachine een sjabloon maken voor klonen, een momentopname, of een installatiekopie van een Amazon machine die Software-onderdelen ondersteunt.

Software ondersteunt scriptverwerking van Windows CMD en PowerShell 2.0.

Belangrijk Het opstartproces mag niet worden onderbroken. Configureer de virtual machine zodanig dat niets het opstartproces van de virtual machine pauzeert voordat de aanmeldingsprompt wordt weergegeven. Controleer bijvoorbeeld of er geen processen of scripts om gebruikersinteractie vragen wanneer de virtual machine wordt gestart.

Voorwaarden

- Identificeer of maak een Windows-referentiemachine.
- Creëer een veilige vertrouwde relatie tussen de referentiemachine en de IaaS Manager Service-host. Zie [De gastagent configureren om een server te vertrouwen](#).
- Als u van plan bent om extern verbinding te maken met de machine voor probleemoplossing of om andere redenen, installeert u Externe bureaublad-services (Remote Desktop Services, RDS)
- Verwijder de artefacten van de netwerkconfiguratie uit de netwerkconfiguratiebestanden.

Procedure

- 1 Meld u aan bij de Windows-referentieserver als een beheerder.
- 2 Open in een browser de softwaredownloadpagina op de vRealize Automation-toepassing.
`https://vrealize-automation-appliance-FQDN/software`
- 3 Sla de ZIP-sjabloon op de Windows-server op.
`prepare_vra_template_windows.zip`
- 4 Pak de ZIP-inhoud uit naar een map en voer het batch-bestand uit.
`.\prepare_vra_template.bat`
- 5 Volg de aanwijzingen.
- 6 Wanneer u klaar bent, sluit u de Windows virtual machine af.

Resultaten

Het script verwijdert eventuele eerdere installaties van de Software-bootstrapagenten, en installeert de ondersteunde versies van de Java Runtime Environment, de gastagent en de Software-bootstrapagent.

Wat nu te doen

Converteer de referentiemachine naar een sjabloon voor klonen, een momentopname, of een installatiekopie van een Amazon-machine. In alle gevallen worden Software-onderdelen ondersteunt en infrastructuurarchitecten kunnen ze gebruiken bij het maken van blueprints.

Een Linux-referentiemachine voorbereiden ter ondersteuning van Software

U gebruikt één script om Java Runtime Environment, de gastagent en de Software bootstrap-agent te installeren op uw Linux-referentiemachine. U kunt vanuit de referentiemachine een sjabloon maken voor klonen, een momentopname, of een installatiekopie van een Amazon machine die Software-onderdelen ondersteunt.

Software ondersteunt scriptverwerking van Bash.

Belangrijk Het opstartproces mag niet worden onderbroken. Configureer de virtual machine zodanig dat niets het opstartproces van de virtual machine onderbreekt voordat de aanmeldingsprompt wordt weergegeven. Controleer bijvoorbeeld of er geen processen of scripts om gebruikersinteractie vragen wanneer de virtual machine wordt gestart.

Voorwaarden

- Identificeer of maak een Linux-referentiemachine.
- Controleer of de volgende opdrachten beschikbaar zijn, afhankelijk van uw Linux-systeem:
 - yum of apt-get
 - wget of curl
 - python
 - dmidecode indien gewenst door cloudproviders
 - Veelvoorkomende vereisten zoals sed, awk, perl, chkconfig, unzip en grep zijn afhankelijk van uw Linux-distributie

U kunt ook een editor gebruiken om het gedownloade `prepare_vra_template.sh`-script te inspecteren, wat laat zien welke opdrachten er worden gebruikt.

- Als u van plan bent om extern verbinding te maken tot de machine voor probleemoplossing of om andere redenen, installeert u OpenSSH.
- Verwijder de artefacten van de netwerkconfiguratie uit de netwerkconfiguratiebestanden.

Procedure

- 1 Meld u aan bij uw referentiemachine als de rootgebruiker.
- 2 Download het tar.gz-pakketsjabloon van de vRealize Automation-toepassing.

```
wget https://vrealize-automation-appliance-FQDN/software/download/prepare_vra_template_linux.tar.gz
```

Als uw omgeving gebruik maakt van automatisch ondertekende certificaten, hebt u mogelijk de optie `--no-check-certificate` nodig.

```
wget --no-check-certificate https://vrealize-automation-appliance-FQDN/software/download/prepare_vra_template_linux.tar.gz
```


3 Pak het pakket uit.

```
tar -xvf prepare_vra_template_linux.tar.gz
```

4 Zoek in de uitvoer van de untar naar het installatiescript en maak deze uitvoerbaar.

```
chmod +x prepare_vra_template.sh
```

5 Voer het installatiescript uit.

```
./prepare_vra_template.sh
```

Als u informatie over niet-interactieve opties en verwachte waarden nodig heeft, raadpleegt u de helpoptie van het script.

```
./prepare_vra_template.sh --help
```

6 Volg de aanwijzingen.

Nadat de installatie is voltooid, wordt een bevestiging weergegeven. Als er fouten en logboeken worden weergegeven, lost u de fouten op en voert u het script opnieuw uit.

7 Wanneer u klaar bent, sluit u de Linux virtual machine af.**Resultaten**

Het script verwijdt eventuele eerdere installaties van de Software-bootstrapagenten, en installeert de ondersteunde versies van de Java Runtime Environment, de gastagent en de Software-bootstrapagent.

Wat nu te doen

Converteer de referentiemachine op uw hypervisor of cloudprovider naar een sjabloon voor klonen, een momentopname of een installatiekopie van een Amazon-machine. In alle gevallen worden Software-onderdelen ondersteunt en infrastructuurarchitecten kunnen ze gebruiken bij het maken van blueprints.

Bestaande sjablonen voor virtual machines in vRealize Automation bijwerken

Als u uw sjablonen, images van Amazon-machines of momentopnamen bijwerkt naar de laatste versie van de bootstrapagent voor Windows Software of als u de bootstrapagent voor Linux Software handmatig bijwerkt naar de laatste versie zonder het script `prepare_vra_template.sh` te gebruiken, moet u alle bestaande versies en bijbehorende logboeken verwijderen.

Linux

Als u het script `prepare_vra_template.sh` uitvoert voor Linux-referentiemachines wordt de agent opnieuw ingesteld en worden eventueel aanwezige logboeken voorafgaand aan de nieuwe installatie verwijderd. Als u echter van plan bent de installatie handmatig uit te voeren, moet u zich als hoofdgebruiker aanmelden bij de referentiemachine en de opdracht uitvoeren om de artefacten opnieuw in te stellen en te verwijderen.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

Windows

Voor Windows-referentiemachines verwijdt u zowel de bestaande Software-agentbootstrap als de gastagent van vRealize Automation 6.0 of hoger en eventueel aanwezige runtime-logboekbestanden. Voer in een PowerShell-opdrachtvenster de opdrachten uit om de agent en artefacten te verwijderen.

```
c:\opt\vmware-appdirector\agent-bootstrap\appd_bootstrap_removal.bat
```

Scenario: een vSphere-sjabloon voorbereiden voor blueprints met kloonmachines en softwareonderdelen

Als vCenter Server-beheerder wilt u een vSphere-sjabloon voorbereiden waarmee uw vRealize Automation-architecten bijvoorbeeld Linux CentOS-machines kunnen klonen. U wilt dat de sjabloon geschikt is voor blueprints met softwareonderdelen. Daarom installeert u eerst de gastagent en software-bootstrapagent voordat u de referentiemachine omzet naar een sjabloon.

Voorwaarden

- Identificeer of maak een Linux CentOS-referentiemachine waarop VMware Tools is geïnstalleerd. Voeg ten minste één netwerkadapter toe zodat er zeker internetverbinding mogelijk is, mocht de blueprintarchitect deze voorziening niet toevoegen op blueprintniveau. Raadpleeg de documentatie bij vSphere voor informatie over het maken van virtual machines.
- U moet verbinding maken met een vCenter Server om een virtual machine naar een sjabloon te converteren. U kunt geen sjablonen maken als u een rechtstreekse verbinding maakt tussen vSphere Client en de host voor vSphere ESXi.

Procedure

1 [Scenario: uw referentiemachine voorbereiden op de aanpassingen van de gastagent en softwareonderdelen](#)

Als u wilt dat uw sjabloon softwareonderdelen kan ondersteunen, installeert u de bootstrap-agent van de software en de vereiste, de gastagent, op uw referentiemachine. De agenten zorgen ervoor dat vRealize Automation-architecten die uw sjabloon gebruiken, softwareonderdelen in hun blueprints kunnen invoegen.

2 [Scenario: uw CentOS-referentiemachine omzetten in een sjabloon](#)

Nadat u de gastagent en software-bootstrapagent op uw referentiemachine hebt geïnstalleerd, verandert u uw referentiemachine in een sjabloon die vRealize Automation-architecten kunnen gebruiken om kloonmachineblueprints te maken.

3 [Scenario: een aanpassingsspecificatie maken voor vSphere-klonen](#)

Maak een aanpassingsspecificatie die uw blueprintarchitecten kunnen gebruiken voor de sjabloon `cpb_centos_63_x84`.

Resultaten

U hebt de referentiemachine omgezet in een sjabloon met een aanpassingsspecificatie waarmee blueprintarchitecten vRealize Automation-blueprints kunnen maken voor het klonen van Linux CentOS-machines. Omdat u de Software-bootstrapagent en de gastagent op de referentiemachine hebt geïnstalleerd, kunnen architecten uw sjabloon gebruiken om blueprints te maken met complexe catalogusitems, inclusief Software-onderdelen of andere aanpassingen door de gastagent, zoals het uitvoeren van scripts of formatteren van schijven. Omdat u VMware Tools hebt geïnstalleerd, kunnen architecten en catalogusbeheerders gebruikers acties voor machines laten uitvoeren, zoals opnieuw configureren, momentopnamen maken, en opnieuw opstarten.

Wat nu te doen

Als u vRealize Automation-gebruikers, -groepen en -bronnen hebt geconfigureerd, kunt u de sjabloon en de aanpassingsspecificatie gebruiken om een machineblueprint voor klonen te maken. Zie [Een machineblueprint configureren](#).

Scenario: uw referentiemachine voorbereiden op de aanpassingen van de gastagent en softwareonderdelen

Als u wilt dat uw sjabloon softwareonderdelen kan ondersteunen, installeert u de bootstrap-agent van de software en de vereiste, de gastagent, op uw referentiemachine. De agenten zorgen ervoor dat vRealize Automation-architecten die uw sjabloon gebruiken, softwareonderdelen in hun blueprints kunnen invoegen.

Als u de procedure wilt vereenvoudigen, kunt u een vRealize Automation-script dat beide agenten installeert, downloaden en uitvoeren, in plaats van aparte pakketten te downloaden en te installeren.

Het script maakt ook verbinding met de Manager Service-instantie en downloadt het SSL-certificaat, waarmee u vertrouwen tot stand brengt tussen de Manager Service en de machines die zijn geïmplementeerd aan de hand van de sjabloon. Houd er rekening mee dat het downloaden van het certificaat via het script minder veilig is dan het Manager Service SSL-certificaat handmatig op te halen en te installeren op uw referentiemachine in `/usr/share/gugent/cert.pem`.

Procedure

- 1 Open een browser op de pagina van de vRealize Automation-toepassingssoftware.

`https://vrealize-automation-appliance-FQDN/software`

- 2 Download het gecomprimeerde (gzip) tar-bestand onder de Linux-software-installatieprogramma's.

`prepare_vra_template_linux.tar.gz`

- 3 Verplaats het tar-bestand naar een tijdelijke directory op de Linux-referentiemachine.

Als u het bestand wilt overdragen, kunt u een hulpprogramma zoals WinSCP uitvoeren of een andere methode gebruiken waarmee u bekend bent.

- 4 Meld u als rootgebruiker aan bij de opdrachtprompt op de Linux-referentiemachine.

Om een terminal te openen, kunt u de Remote Console op de machine starten vanuit vRealize Automation of een andere methode gebruiken waarmee u bekend bent.

- 5 Pak het tar-bestand uit vanuit de tijdelijke directory.

```
gunzip prepare_vra_template_linux.tar.gz
```

- 6 Pak de inhoud van het tar-bestand uit.

```
tar xvf prepare_vra_template_linux.tar
```

- 7 Ga naar de scriptdirectory.

```
cd prepare_vra_template_linux
```

- 8 Voer het script uit en volg de instructies.

```
./prepare_vra_template.sh
```

Als u niet-interactieve informatie over opties en waarden wilt, voert u in./

```
prepare_vra_template.sh --help.
```

Resultaten

Er wordt een bevestigingsbericht weergegeven wanneer de installatie is voltooid. Als er foutmeldingen en logboeken worden weergegeven, corrigeert u de fouten en voert u het script opnieuw uit.

Scenario: uw CentOS-referentiemachine omzetten in een sjabloon

Nadat u de gastagent en software-bootstrapagent op uw referentiemachine hebt geïnstalleerd, verandert u uw referentiemachine in een sjabloon die vRealize Automation-architecten kunnen gebruiken om kloonmachineblueprints te maken.

Nadat u de referentiemachine hebt geconverteerd naar een sjabloon, kunt u de sjabloon niet langer bewerken of inschakelen, tenzij u deze weer converteert naar een virtual machine.

Procedure

- 1 Meld u aan bij uw referentiemachine als de hoofdgebruiker en bereid de machine voor op de conversie.

- a Verwijder de udev-persistentieregels.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- b Ingeschakelde machines die op basis van deze sjabloon zijn gekloond, hebben hun eigen unieke id's.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- c Als u de referentiemachine opnieuw hebt opgestart of geconfigureerd nadat u de software-bootstrapagent hebt geïnstalleerd, moet u deze agent opnieuw instellen.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- d Schakel de machine uit.

```
shutdown -h now
```

- 2 Meld u aan bij de vSphere Web Client als een beheerder.
- 3 Klik met de rechtermuisknop op de referentiemachine en selecteer **Instellingen bewerken**.
- 4 Voer **cpb_centos_63_x84** in het tekstvak **VM-naam** in.
- 5 Hoewel uw referentiemachine CentOS als gastbesturingssysteem heeft, selecteert u **Red Hat Enterprise Linux 6 (64-bit)** in het vervolgkeuzemenu **Versie gastbesturingssysteem**.
Als u CentOS selecteert, functioneert uw sjabloon en de aangepaste specificatie mogelijk niet op de verwachte wijze.
- 6 Klik met de rechtermuisknop op de referentiemachine in vSphere Web Client en selecteer **Sjabloon > Converteren naar sjabloon**.

Resultaten

vCenter Server markeert de referentiemachine cpb_centos_63_x84 als een sjabloon en geeft de taak weer in het venster Recente taken. Als de vSphere-omgeving al onder het beheer van vRealize Automation staat, wordt uw sjabloon ontdekt wanneer de geautomatiseerde gegevensverzameling een volgende keer wordt uitgevoerd. Als u vRealize Automation nog niet hebt geconfigureerd, wordt de sjabloon verzameld tijdens dat proces.

Scenario: een aanpassingsspecificatie maken voor vSphere-klonen

Maak een aanpassingsspecificatie die uw blueprintarchitecten kunnen gebruiken voor de sjabloon cpb_centos_63_x84.

Procedure

- 1 Meld u aan bij de vSphere Web Client als een beheerder.
- 2 Klik op de startpagina op **Manager aanpassingsspecificatie** om de wizard te openen.
- 3 Klik op het pictogram **Nieuw**.
- 4 Klik op het pictogram **Nieuw**.
- 5 Geef de eigenschappen op.
 - a Selecteer **Linux** in het vervolgkeuzemenu **Besturingssysteem voor VM van doel**.
 - b Geef **Aangepaste spec.** op in het tekstvak **Naam aanpassingsspecificatie**.
 - c Voer **cpb-centos_63_x84 klonen met vRealize Automation** in het tekstvak **Beschrijving** in.
 - d Klik op **Volgende**.
- 6 Stel de naam van de computer in.
 - a Selecteer **Naam van virtual machine gebruiken**.
 - b Voer in het tekstvak **Domeinnaam** het domein in waarop gekloonde machines zullen worden ingericht.
 - c Klik op **Volgende**.
- 7 Configureer de instellingen van de tijdzones.
- 8 Klik op **Volgende**.
- 9 Selecteer **Standaardnetwerkinstellingen gebruiken voor het gastbesturingssysteem, inclusief het inschakelen van DHCP voor alle netwerkinterfaces**.

Materiaalbeheerders en infrastructuurarchitecten handelen netwerkinstellingen voor machines die worden ingericht, af door netwerkprofielen te maken en te gebruiken in vRealize Automation.
- 10 Volg de prompts en geef de resterende vereiste informatie op.
- 11 Controleer in de pagina **Gereed om te voltooien** uw selecties en klik op **Voltooien**.

Resultaten

Scenario: import van de blueprint van de vSphere-voorbeeldtoepassing voor Dukes Bank voorbereiden

Als vCenter Server-beheerder wilt u een vSphere CentOS 6.x Linux-sjabloon en specificatie voor aanpassing voorbereiden zodat u deze kunt gebruiken om de vRealize Automation-voorbeeldtoepassing voor Dukes Bank in te richten.

Als u ervoor wilt zorgen dat uw sjabloon de softwareonderdelen van de voorbeeldtoepassing ondersteunt, installeert u de gastagent en de software-bootstrapagent op uw Linux-referentiemachine voordat u deze converteert naar een sjabloon en een specificatie voor aanpassing maakt. U deactiveert SELinux op uw referentiemachine om ervoor te zorgen dat uw sjabloon de specifieke implementatie van MySQL ondersteunt die wordt gebruikt in de voorbeeldtoepassing voor Dukes Bank.

Voorwaarden

- Identificeer of maak een CentOS 6.x Linux-referentiemachine waarop VMware Tools is geïnstalleerd. Raadpleeg de documentatie bij vSphere voor informatie over het maken van virtual machines.
- U moet verbinding maken met een vCenter Server om een virtual machine naar een sjabloon te converteren. U kunt geen sjablonen maken als u een rechtstreekse verbinding maakt tussen vSphere Client en de host voor vSphere ESXi.

Procedure

1 [Scenario: uw referentiemachine voorbereiden voor de vSphere-voorbeeldtoepassing voor Dukes Bank](#)

Als u wilt dat uw sjabloon de voorbeeldtoepassing voor Dukes Bank ondersteunt, moet u zowel de gastagent als de software-bootstrapagent op uw referentiemachine installeren, zodat vRealize Automation de softwareonderdelen kan inrichten. Om het proces te vereenvoudigen, kunt u een vRealize Automation-script downloaden en uitvoeren, waarmee zowel de gastagent als de software-bootstrapagent tegelijk worden geïnstalleerd, zodat u beide pakketten niet afzonderlijk hoeft te downloaden en te installeren.

2 [Scenario: uw referentiemachine converteren naar een sjabloon voor de vSphere-toepassing voor Dukes Bank](#)

Nadat u de gastagent en de software-bootstrapagent hebt geïnstalleerd op uw referentiemachine, deactiveert u SELinux om ervoor te zorgen dat uw sjabloon de specifieke implementatie van MySQL ondersteunt die wordt gebruikt in de voorbeeldtoepassing voor Dukes Bank. U maakt van uw referentiemachine een sjabloon die u kunt gebruiken om de vSphere-voorbeeldtoepassing voor Dukes Bank in te richten.

3 [Scenario: een aangepaste specificatie maken voor het klonen van de vSphere-voorbeeldtoepassingsmachines voor Dukes Bank](#)

U maakt een aangepaste specificatie die u kunt gebruiken met de sjabloon voor machines van Dukes Bank.

Resultaten

U hebt een sjabloon en een specificatie voor aanpassing gemaakt voor uw referentiemachine die de vRealize Automation-voorbeeldtoepassing voor Dukes Bank ondersteunt.

Scenario: uw referentiemachine voorbereiden voor de vSphere-voorbeeldtoepassing voor Dukes Bank

Als u wilt dat uw sjabloon de voorbeeldtoepassing voor Dukes Bank ondersteunt, moet u zowel de gastagent als de software-bootstrapagent op uw referentiemachine installeren, zodat vRealize Automation de softwareonderdelen kan inrichten. Om het proces te vereenvoudigen, kunt u een vRealize Automation-script downloaden en uitvoeren, waarmee zowel de gastagent als de software-bootstrapagent tegelijk worden geïnstalleerd, zodat u beide pakketten niet afzonderlijk hoeft te downloaden en te installeren.

Procedure

- 1 Meld u aan bij uw referentiemachine als de rootgebruiker.
- 2 Download het installatiescript van uw vRealize Automation-toepassing.

```
wget https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

Als uw omgeving gebruik maakt van automatisch ondertekende certificaten, moet u wellicht de wget-optie `--no-check-certificate` gebruiken. Bijvoorbeeld:

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

- 3 Maak het script `prepare_vra_template.sh` uitvoerbaar.

```
chmod +x prepare_vra_template.sh
```

- 4 Voer het installatiescript `prepare_vra_template.sh` uit.

```
./prepare_vra_template.sh
```

U kunt de helpopdracht `./prepare_vra_template.sh --help` uitvoeren voor informatie over niet-interactieve opties en verwachte waarden.

- 5 Volg de prompts om de installatie te voltooien.

U krijgt een bevestiging te zien wanneer de installatie is geslaagd. Als er een foutmelding en logboeken in de console worden weergegeven, moet u de fouten oplossen en het installatiescript opnieuw uitvoeren.

Resultaten

U hebt zowel de software-bootstrapagent als de hiervoor vereiste gastagent geïnstalleerd om ervoor te zorgen dat de voorbeeldtoepassing voor Dukes Bank softwareonderdelen kan inrichten. Het script heeft ook verbinding gemaakt met uw instantie van Manager Service en heeft het SSL-certificaat gedownload waarmee een vertrouwensband kan worden gelegd tussen Manager Service en de machines die worden geïmplementeerd door uw sjabloon. Deze aanpak is minder veilig dan het ophalen van het SSL-certificaat van Manager Service en dit vervolgens handmatig op uw referentiemachine installeren in `/usr/share/gugent/cert.pem`. U kunt handmatig dit certificaat vervangen als veiligheid een hoge prioriteit heeft.

Scenario: uw referentiemachine converteren naar een sjabloon voor de vSphere-toepassing voor Dukes Bank

Nadat u de gastagent en de software-bootstrapagent hebt geïnstalleerd op uw referentiemachine, deactiveert u SELinux om ervoor te zorgen dat uw sjabloon de specifieke implementatie van MySQL ondersteunt die wordt gebruikt in de voorbeeldtoepassing voor Dukes Bank. U maakt van uw referentiemachine een sjabloon die u kunt gebruiken om de vSphere-voorbeeldtoepassing voor Dukes Bank in te richten.

Nadat u de referentiemachine hebt geconverteerd naar een sjabloon, kunt u de sjabloon niet langer bewerken of inschakelen, tenzij u deze weer converteert naar een virtual machine.

Procedure

1 Meld u aan bij uw referentiemachine als de rootgebruiker.

- a Bewerk het bestand `/etc/selinux/config` om SELinux te deactiveren.

```
SELINUX=disabled
```

Als u SELinux niet deactiveert, werkt het softwareonderdeel MySQL van de Dukes Bank-voorbeeldtoepassing mogelijk niet op de verwachte wijze.

- b Verwijder de udev-persistentieregels.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- c Ingeschakelde machines die op basis van deze sjabloon zijn gekloond, hebben hun eigen unieke id's.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- d Als u de referentiemachine opnieuw hebt opgestart of geconfigureerd nadat u de software-bootstrapagent hebt geïnstalleerd, moet u deze agent opnieuw instellen.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- e Schakel de machine uit.

```
shutdown -h now
```

2 Meld u aan bij de vSphere Web Client als een beheerder.

3 Klik met de rechtermuisknop op de referentiemachine en selecteer **Instellingen bewerken**.

4 Geef **dukes_bank_sjabloon** op in het tekstvak **Naam virtual machine**.

5 Als uw referentiemachine CentOS als gastbesturingssysteem heeft, selecteert u **Red Hat Enterprise Linux 6 (64-bit)** in het vervolgkeuzemenu **Versie gastbesturingssysteem**.

Als u CentOS selecteert, functioneert uw sjabloon en de aangepaste specificatie mogelijk niet op de verwachte wijze.

- 6 Klik op **OK**.
- 7 Klik met de rechtermuisknop op de referentiemachine in vSphere Web Client en selecteer **Sjabloon > Converteren naar sjabloon**.

Resultaten

vCenter Server markeert de referentiemachine `dukes_bank_sjabloon` als een sjabloon en geeft de taak weer in het venster Recente taken. Als de vSphere-omgeving al onder het beheer van vRealize Automation staat, wordt uw sjabloon ontdekt wanneer de geautomatiseerde gegevensverzameling een volgende keer wordt uitgevoerd. Als u vRealize Automation nog niet hebt geconfigureerd, wordt de sjabloon verzameld tijdens dat proces.

Scenario: een aangepaste specificatie maken voor het klonen van de vSphere-voorbeeldtoepassingsmachines voor Dukes Bank

U maakt een aangepaste specificatie die u kunt gebruiken met de sjabloon voor machines van Dukes Bank.

Procedure

- 1 Meld u aan bij de vSphere Web Client als een beheerder.
- 2 Klik op de startpagina op **Manager aanpassingsspecificatie** om de wizard te openen.
- 3 Klik op het pictogram **Nieuw**.
- 4 Geef de eigenschappen op.
 - a Selecteer **Linux** in het vervolgkeuzemenu **Besturingssysteem voor VM van doel**.
 - b Geef **voorbeeld_aangepaste_specificatie** op in het tekstvak **Naam Specificatie aanpassing**.
 - c Geef **Aangepaste specificatie voor Dukes Bank** op in het tekstvak **Beschrijving**.
 - d Klik op **Volgende**.
- 5 Stel de naam van de computer in.
 - a Selecteer **Naam van virtual machine gebruiken**.
 - b Geef het domein op waar u de voorbeeldtoepassing voor Dukes Bank wilt inrichten in het tekstvak **Domeinnaam**.
 - c Klik op **Volgende**.
- 6 Configureer de instellingen van de tijdzones.
- 7 Klik op **Volgende**.

- 8 Selecteer **Standaardnetwerkinstellingen gebruiken voor het gastbesturingssysteem, inclusief het inschakelen van DHCP voor alle netwerkinterfaces**.

Materiaalbeheerders en infrastructuurarchitecten handelen netwerkinstellingen voor machines die worden ingericht, af door netwerkprofielen te maken en te gebruiken in vRealize Automation.

- 9 Volg de prompts en geef de resterende vereiste informatie op.
- 10 Controleer in de pagina **Gereed om te voltooien** uw selecties en klik op **Voltooien**.

Resultaten

U hebt een sjabloon en een aangepaste specificatie gemaakt die u kunt gebruiken om de voorbeeldtoepassing voor Dukes Bank in te richten.

Wat nu te doen

- 1 Maak een extern netwerkprofiel ten behoeve van een gateway met een IP-adresbereik. Zie [Een extern netwerkprofiel maken via een externe IPAM-provider](#).
- 2 Koppel uw externe netwerkprofiel aan uw vSphere-reservering. Zie [Een reservering maken voor Hyper-V, KVM, SCVMM, vSphere of XenServer](#). Zonder extern netwerkprofiel kan de voorbeeldtoepassing niet juist worden ingericht.
- 3 Importeer de voorbeeldtoepassing voor Dukes Bank in uw omgeving. Zie [Scenario: de Dukes Bank voor vSphere-voorbeeldtoepassing importeren en configureren voor uw omgeving](#).

Tenants en bronnen voorbereiden op de inrichting van blueprints

2

U kunt meerdere tenantomgevingen configureren, met elk hun eigen gebruikersgroepen en unieke toegang tot bronnen die u onder het beheer van vRealize Automation brengt.

Dit hoofdstuk omvat de volgende onderwerpen:

- [Tenantinstellingen configureren](#)
- [Bronnen configureren](#)
- [Gebruikersvoorkeuren voor meldingen en afgevaardigden](#)

Tenantinstellingen configureren

Tenantbeheerders configureren tenantinstellingen zoals gebruikersverificatie en beheren gebruikersrollen en bedrijfsgroepen. Systeembeheerder en tenantbeheerders configureren opties zoals e-mailservers voor verwerking van meldingen en de merkvermelding voor de vRealize Automation-console.

De checklist voor het configureren van tenantinstellingen biedt een algemeen overzicht van de vereiste stappen voor de configuratie van de tenantinstellingen.

Tabel 2-1. Checklist voor het configureren van tenantinstellingen

Taak	vRealize Automation Rol	Details
<input type="checkbox"/> Maak lokale gebruikersaccounts en wijs een tenantbeheerder toe.	Systeembeheerder	Toegang tot de standaardtenant configureren
<input type="checkbox"/> Configureer Beheer van directory's om het beheer van tenantidentiteiten en de instellingen voor toegangscontrole in te stellen.	Tenantbeheerder	Configuratieopties kiezen voor Beheer van directory's
<input type="checkbox"/> Maak bedrijfsgroepen en aangepaste groepen en verleen gebruikers toegangsrechten voor de vRealize Automation-console.	Tenantbeheerder	Groepen en gebruikersrollen configureren
<input type="checkbox"/> (Optioneel) Maak extra tenants zodat gebruikers toegang hebben tot de juiste toepassingen en bronnen die zij nodig hebben om hun werkopdrachten te voltooien.	Systeembeheerder	Aanvullende tenants maken

Tabel 2-1. Checklist voor het configureren van tenantinstellingen (vervolg)

Taak	vRealize Automation Rol	Details
❑ (Optioneel) Configureer aangepaste merkvermelding op de aanmeld- en toepassingspagina's voor tenants van de vRealize Automation-console.	<ul style="list-style-type: none"> ■ Systeembeheerder ■ Tenantbeheerder 	Aangepaste merkvermelding configureren
❑ (Optioneel) Configureer vRealize Automation zodat gebruikers bij specifieke gebeurtenissen een melding ontvangen.	<ul style="list-style-type: none"> ■ Systeembeheerder ■ Tenantbeheerder 	Checklist voor meldingen configureren
❑ (Optioneel) Configureer vRealize Orchestrator om ondersteuning te bieden voor XaaS en andere uitbreidbaarheid.	<ul style="list-style-type: none"> ■ Systeembeheerder ■ Tenantbeheerder 	vRealize Orchestrator configureren
❑ (Optioneel) Maak een aangepast RDP-protocolbestand (Remote Desktop Protocol) dat IaaS-architecten gebruiken in blueprints voor het configureren van RDP-instellingen.	Systeembeheerder	Een aangepast RDP-bestand maken ter ondersteuning van RDP-verbindingen voor ingerichte machines
❑ (Optioneel) Definieer datacenterlocaties die door uw materiaalbeheerders en IaaS-architecten kunnen worden gebruikt zodat gebruikers de juiste locatie kunnen selecteren voor het inrichten wanneer ze machines aanvragen.	Systeembeheerder	Zie Scenario: datacenterlocaties toevoegen voor interregionale implementaties voor een voorbeeld van het toevoegen van datacenterlocaties.

Configuratieopties kiezen voor Beheer van directory's

U kunt de functies van Beheer van directory's van vRealize Automation gebruiken voor het configureren van een Active Directory-verbinding die voldoet aan uw vereisten voor gebruikersverificatie.

Beheer van directory's biedt een groot aantal opties die in hoge mate aangepaste gebruikersverificatie ondersteunen.

Tabel 2-2. Configuratieopties kiezen voor Beheer van directory's

Configuratieoptie	Procedure
Configureer een verbinding met uw Active Directory.	<ol style="list-style-type: none"> 1 Configureer een verbinding met uw Active Directory. Zie Een koppeling configureren voor Active Directory via een LDAP/IWA. 2 Als u vRealize Automation hebt geconfigureerd voor hoge beschikbaarheid, raadpleegt u Beheer van directory's configureren voor hoge beschikbaarheid.
(Optioneel) Verbeter de beveiliging van een directoryverbinding op basis van gebruikers-id en wachtwoord door integratie in twee richtingen met Active Directory Federated Services te configureren.	Een vertrouwensrelatie in twee richtingen configureren tussen vRealize Automation en Active Directory

Tabel 2-2. Configuratieopties kiezen voor Beheer van directory's (vervolg)

Configuratieoptie	Procedure
(Optioneel) Voeg gebruikers en groepen toe aan een bestaande Active Directory-verbinding.	Gebruikers of groepen toevoegen aan een Active Directory-verbinding.
(Optioneel) Bewerk het standaardbeleid om aangepaste regels toe te passen voor een Active Directory-verbinding.	Het toegangsbeleid voor gebruikers beheren.
(Optioneel) Configureer netwerkbereiken om de IP-adressen te beperken waarmee gebruikers zich bij het systeem kunnen aanmelden en beheer aanmeldbeperkingen (time-out, aantal aanmeldingspogingen voordat het systeem wordt vergrendeld).	Een netwerkbereik toevoegen of bewerken.

Overzicht van Beheer van directory's

Tenantbeheerders kunnen identiteitsbeheer voor tenants configureren en hebben toegang tot beheerinstellingen met de opties van Directory's beheren in de toepassingsconsole van vRealize Automation.

U kunt de volgende instellingen beheren via het tabblad **Beheer > Beheer van directory's**.

Tabel 2-3. Instellingen van Beheer van directory's

Instelling	Beschrijving
Directory's	<p>Op de pagina Directory's kunt u Active Directory-verbindingen configureren en beheren ter ondersteuning van gebruikersverificatie en -autorisatie voor vRealize Automation-tenants. U maakt een of meer directory's en vervolgens synchroniseert u deze directory's met uw Active Directory-implementatie. Op deze pagina wordt het aantal groepen en gebruikers weergegeven dat met de directory wordt gesynchroniseerd en het laatste tijdstip waarop is gesynchroniseerd. U kunt op Nu synchroniseren klikken om het synchroniseren van directory's handmatig te starten.</p> <p>Zie Beheer van directory's gebruiken om een Active Directory-verbinding te maken.</p> <p>Wanneer u op een directory klikt en vervolgens op de knop Synchronisatie-instellingen klikt, kunt u de synchronisatie-instellingen bewerken, naar de pagina Identiteitsproviders gaan en het synchronisatielogboek weergeven.</p> <p>Op de pagina met synchronisatie-instellingen voor directory's kunt u de synchronisatiefrequentie plannen, de lijst weergeven met domeinen die aan deze directory gekoppeld zijn, de lijst met toegewezen kenmerken wijzigen, de lijst bijwerken met gebruikers en groepen die worden gesynchroniseerd en de beveiligingsdoelen instellen.</p>
Connectoren	<p>Op de pagina Connectoren worden geïmplementeerde connectoren weergegeven voor uw bedrijfsnetwerk. Met een connector worden gebruikers- en groepsgegevens tussen Active Directory en de Directories Management-service gesynchroniseerd. Wanneer de connector als identiteitsprovider wordt gebruikt, worden gebruikers hiermee bij de service geverifieerd. Elke vRealize Automation-toepassing bevat standaard een connector. Zie Connectoren en connectorclusters beheren.</p>

Tabel 2-3. Instellingen van Beheer van directory's (vervolg)

Instelling	Beschrijving
Gebruikerskenmerken	Op de pagina Gebruikerskenmerken worden de standaard gebruikerskenmerken weergegeven die worden gesynchroniseerd in de directory. U kunt andere kenmerken toevoegen die u kunt toewijzen aan Active Directory-kenmerken. Zie Kenmerken selecteren om te synchroniseren met de directory .
Netwerkbereiken	Op deze pagina worden de netwerkbereiken weergegeven die voor uw systeem worden geconfigureerd. U configureert een netwerkbereik om gebruikers toegang te bieden via de betreffende IP-adressen. U kunt aanvullende netwerkbereiken toevoegen en u kunt bestaande bereiken bewerken. Zie Een netwerkbereik toevoegen of bewerken .
Identiteitsproviders	Op de pagina Identiteitsproviders worden de identiteitsproviders weergegeven die beschikbaar zijn in uw systeem. vRealize Automation-systemen bevatten een connector die fungeert als de standaardidentiteitsprovider en die voor de behoeften van de meeste gebruikers voldoende is. U kunt identiteitsproviderinstanties van derden toevoegen of een combinatie van beide gebruiken. Zie Een verbinding met een externe identiteitsprovider configureren .
Beleidsregels	Op de pagina Beleidsregels worden het standaardtoegangsbeleid en ander toegangsbeleid voor webtoepassingen dat u hebt gemaakt, weergegeven. Beleid bestaat uit een verzameling regels die criteria opgeven waaraan moet worden voldaan voordat gebruikers toegang krijgen tot toepassingsportals of webtoepassingen kunnen starten die voor deze gebruikers zijn ingeschakeld. Het standaardbeleid moet geschikt zijn voor de meeste vRealize Automation-implementaties, maar u kunt het naar wens aanpassen. Zie Het toegangsbeleid voor gebruikers beheren .

Belangrijke concepten in verband met Active Directory

Enkele concepten in verband met Active Directory zijn van groot belang voor inzicht in de manier waarop Directories Management wordt geïntegreerd met uw Active Directory-omgevingen.

Connector

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

- Synchroniseert gegevens van gebruikers en groepen tussen Active Directory en de service.
- Als deze wordt gebruikt als een identiteitsprovider, verifieert deze gebruikers naar de service.

De Connector is de standaardidentiteitsprovider. Als u wilt weten welke verificatiemethoden de Connector ondersteunt, raadpleegt u *VMware Identity Manager Administration*. U kunt ook identiteitsproviders van derden gebruiken die het SAML 2.0-protocol ondersteunen. Gebruik een identiteitsprovider van derden voor een verificatietype dat niet door de Connector wordt ondersteund of voor een verificatietype dat wel door de Connector wordt ondersteund, als de identiteitsprovider van derden de voorkeur heeft op basis van het beveiligingsbeleid van uw bedrijf.

Opmerking Ook als u identiteitsproviders van derden gebruikt, moet u de Connector gebruiken om gegevens van gebruikers en groepen te synchroniseren.

Directory

De Directories Management-service heeft een eigen concept van een directory, dat gebruikmaakt van Active Directory-kenmerken en -parameters om gebruikers en groepen te definiëren. U maakt een of meer directory's en vervolgens synchroniseert u deze directory's met uw Active Directory-implementatie. U kunt de volgende directorytypen maken in de service.

- **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.

De service heeft geen directe toegang tot Active Directory. Alleen de Connector heeft directe toegang tot Active Directory. 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 Active Directory en de service via een of meer werkers.

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

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.

Zie [Een koppeling configureren voor Active Directory via een LDAP/IWA](#) . Selecteer de optie Active Directory via LDAP wanneer u een directory aan de service toevoegt voor deze omgeving.

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.

Zie [Een koppeling configureren voor Active Directory via een LDAP/IWA](#) . Wanneer u een directory voor deze omgeving toevoegt, selecteert u de optie Active Directory (geïntegreerde Windows-verificatie).

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.

Zie [Een koppeling configureren voor Active Directory via een LDAP/IWA](#) . Wanneer u een directory voor deze omgeving toevoegt, selecteert u de optie Active Directory (geïntegreerde Windows-verificatie).

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.

Zie [Een koppeling configureren voor Active Directory via een LDAP/IWA](#) . 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.

Beheer van directory's gebruiken om een Active Directory-verbinding te maken

Nadat u vRealize Automation-tenants hebt gemaakt, moet u zich bij de systeemconsole aanmelden als een tenantbeheerder en moet u een Active Directory-verbinding maken om gebruikersverificatie te ondersteunen.

Er zijn drie opties voor Active Directory-communicatieprotocollen bij het configureren van een Active Directory-verbinding met behulp van Beheer van directory's.

- Active Directory via LDAP - Een Active Directory via LDAP-protocol ondersteunt standaard het opzoeken van de locatie van de DNS-service.

- Active Directory (met geïntegreerde Windows-verificatie) - Met Active Directory (met geïntegreerde Windows-verificatie) configureert u het domein waarvan u lid wilt worden. Active Directory via LDAP is geschikt voor implementaties met één domein. Gebruik Active Directory (met geïntegreerde Windows-verificatie) voor alle implementaties met meerdere domeinen en forests.
- OpenLDAP - U kunt de opensourceversie van LDAP gebruiken om gebruikersverificatie voor Beheer van directory's te ondersteunen.

Na het selecteren van een communicatieprotocol en het configureren van een Active Directory-verbinding, kunt u de domeinen opgeven die moeten worden gebruikt met de Active Directory-configuratie. Vervolgens kunt u de gebruikers en groepen selecteren die moeten worden gesynchroniseerd met de opgegeven configuratie.

Een koppeling configureren voor Active Directory via een LDAP/IWA

U kunt een koppeling voor Active Directory via LDAP/IWA configureren om ondersteuning voor gebruikersverificatie in te stellen. Daarbij gebruikt u Directories Management om een koppeling naar Active Directory te configureren die gebruikersverificatie biedt voor alle tenants, en selecteert u de gebruikers en groepen die u wilt synchroniseren met de Directories Management-directory.

Zie [Een OpenLDAP-directoryverbinding configureren](#) voor informatie en aanwijzingen voor het gebruik van OpenLDAP met Beheer van directory's.

Voor een Active Directory-configuratie (met geïntegreerde Windows-verificatie) 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, zullen deze leden ontbreken in de lokale domeingroep.

Opmerking Configureer Active Directory IWA-directory's eerst voor de standaardtenant en voeg deze vervolgens toe aan andere tenants.

Voorwaarden

- Selecteer de vereiste standaardkenmerken en voeg aanvullende kenmerken toe op de pagina Gebruikerskenmerken. Zie [Kenmerken selecteren om te synchroniseren met de directory](#).
- Lijst met de Active Directory-groepen en -gebruikers die u wilt synchroniseren vanuit Active Directory.
- Als de Active Directory toegang via SSL of STARTTLS vereist, is het root-CA-certificaat van de domeincontroller van Active Directory vereist.
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > Beheer van directory's > Directory's**.
- 2 Klik op **Directory toevoegen** en selecteer **Active Directory via LDAP/IWA toevoegen**.

- 3 Geef op de pagina Directory toevoegen het IP-adres op voor de Active Directory-server in het tekstvak **Naam van directory**.
- 4 Selecteer het juiste communicatieprotocol voor Active Directory met de keuzerondjes onder het tekstvak **Naam van directory**.

Optie	Beschrijving
Windows-verificatie	Selecteer Active Directory (Geïntegreerde Windows-verificatie) . 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.
LDAP	Selecteer Active Directory via LDAP . Voor Active Directory via LDAP is onder andere de basis-DN, de bindings-DN en het wachtwoord van de bindings-DN vereist.

- 5 Configureer de connector waarmee gebruikers uit de Active Directory worden gesynchroniseerd met de VMware Directories Management-directory in de sectie Directory synchroniseren en verifiëren.

Optie	Beschrijving
Connector voor synchronisatie	Selecteer de juiste connector die u voor uw systeem wilt gebruiken. Elke vRealize Automation-toepassing bevat een standaardconnector. Raadpleeg uw systeembeheerder als u hulp nodig hebt bij het kiezen van de juiste connector.
Verificatie	<p>Klik op het juiste keuzerondje om aan te geven of de geselecteerde connector ook voor verificatie moet worden gebruikt.</p> <p>Als u gebruikmaakt van Active Directory (Geïntegreerde Windows-verificatie), met een externe identiteitsprovider 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 Identiteitsprovider om de externe identiteitsprovider toe te voegen voor verificatie.</p> <p>Raadpleeg de <i>VMware Identity Manager Administration Guide</i> voor informatie over het gebruik van verificatieadapters zoals PasswordIpdAdapter, SecurIDAdapter en RadiusAuthAdapter.</p>
Zoekenmerken directory	<p>Selecteer het juiste accountkenmerk dat de gebruikersnaam bevat. VMware raadt aan het sAMAccount-kenmerk te gebruiken in plaats van userPrincipleName. Als u userPrincipleName voor synchronisatiebewerkingen gebruikt, werken integraties met software van tweede en derde partijen waarvoor een gebruikersnaam is vereist, mogelijk niet goed.</p> <p>Opmerking Als u sAMAccountName selecteert wanneer u een globale catalogus gebruikt, aangegeven door het selectievakje Deze directory heeft een globale catalogus in te schakelen in het gebied Serverlocatie, kunnen gebruikers zich niet aanmelden.</p>

- 6 Voer de juiste informatie in het tekstvak Serverlocatie in als u Active Directory via LDAP hebt gekozen of voer informatie in de tekstvakken Details domein koppelen in als u Active Directory (Geïntegreerde Windows-verificatie) hebt geselecteerd.

Optie	Beschrijving
Serverlocatie - Wordt weergegeven als Active Directory via LDAP is geselecteerd	<ul style="list-style-type: none"> Als u DNS-servicelocatie wilt gebruiken om domeinen in Active Directory te vinden, houdt u het selectievakje Deze directory ondersteunt DNS-servicelocatie ingeschakeld. <p>Opmerking U kunt de poorttoewijzing niet wijzigen in 636 als u deze optie selecteert.</p> <p>Samen met de directory wordt het bestand <code>domain_krb.properties</code> gemaakt, waaraan automatisch een lijst met domeincontrollers is toegevoegd. Zie Domeincontrollers selecteren.</p> <p>Als voor Active Directory de versleuteling STARTTLS is vereist, schakelt u het selectievakje Voor deze directory is vereist dat alle verbindingen STARTTLS gebruiken in de sectie Certificaten in en kopieert en plakt u het root-CA-certificaat van Active Directory in het veld SSL-certificaat.</p> <ul style="list-style-type: none"> Als de opgegeven Active Directory-instantie het opzoeken van de DNS-servicelocatie niet gebruikt, schakelt u het selectievakje naast Deze directory ondersteunt de DNS-servicelocatie in de velden van Serverlocatie uit en voert u de hostnaam en het poortnummer van de Active Directory-server in de daartoe bestemde tekstvakken in. <p>Schakel het selectievakje Deze directory heeft een globale catalogus in als de bijbehorende Active Directory gebruikmaakt van een globale catalogus. Een globale catalogus bevat een vertegenwoordiging van alle objecten in elk domein in een Active Directory-forest met meerdere domeinen.</p> <p>Zie de sectie Active Directory-omgeving met één forest en meerdere domeinen in Active Directory-omgevingen om de directory te configureren als globale catalogus.</p> <p>Als u voor Active Directory toegang via SSL nodig hebt, schakelt u het selectievakje Voor deze directory moeten alle verbindingen SSL gebruiken in onder het kopje Certificaten en geeft u het Active Directory SSL-certificaat op.</p> <p>Wanneer u deze optie selecteert, wordt automatisch poort 636 gebruikt en kan deze niet worden gewijzigd.</p> <p>Zorg ervoor dat het certificaat de PEM-indeling heeft en dat de regels 'BEGIN CERTIFICATE' en 'END CERTIFICATE' erin zijn opgenomen.</p>
Details voor deelnemen aan domein - Wordt weergegeven als Active Directory (met geïntegreerde Windows-verificatie) is geselecteerd	<p>Voer de vereiste verificatiegegevens in de tekstvakken Domeinnaam, Gebruikersnaam van domeinbeheerder en Wachtwoord van domeinbeheerder in.</p> <p>Als voor Active Directory de versleuteling STARTTLS is vereist, schakelt u het selectievakje Voor deze directory is vereist dat alle verbindingen STARTTLS gebruiken in de sectie Certificaten in en kopieert en plakt u het root-CA-certificaat van Active Directory in het veld SSL-certificaat.</p> <p>Zorg ervoor dat het certificaat de PEM-indeling heeft en dat de regels 'BEGIN CERTIFICATE' en 'END CERTIFICATE' erin zijn opgenomen.</p>

Optie	Beschrijving
	Als de directory gebruikmaakt van meerdere domeinen, 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.

- 7 Voer in de sectie Gebruikersgegevens binden de juiste verificatiegegevens in om synchronisatie van directory's mogelijk te maken.

Voor Active Directory via LDAP:

Optie	Beschrijving
Basis-DN	Voer de DN-naam voor de zoekbasis in. Bijvoorbeeld: cn=users,dc=corp,dc=local.
Bindings-DN	Voer de bindings-DN-naam in. Bijvoorbeeld cn=fritz infra,cn=users,dc=corp,dc=local

Voor Active Directory (met geïntegreerde Windows-verificatie):

Optie	Beschrijving
UPN van gebruiker van de binding	Voer de UPN-naam (User Principal Name) in van de gebruiker die het domein kan verifiëren. Bijvoorbeeld: gebruikersnaam@example.com.
Wachtwoord van de bindings-DN	Voer het wachtwoord van de bindingsgebruiker in.

- 8 Klik op **Verbinding testen** om de verbinding met de geconfigureerde directory te testen.

Deze knop wordt niet weergegeven als u Active Directory (met geïntegreerde Windows-verificatie) hebt geselecteerd.

- 9 Klik op **Opslaan en Volgende**.

De pagina De domeinen selecteren wordt weergegeven, met de lijst met domeinen.

- 10 Controleer en update de domeinen die worden vermeld voor de verbinding met Active Directory.

- Voor Active Directory (met geïntegreerde Windows-verificatie) selecteert u de domeinen die moeten worden gekoppeld aan deze Active Directory-verbinding.
- Voor Active Directory via LDAP wordt het beschikbare domein met een vinkje weergegeven.


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.

- 11 Klik op **Volgende**.

- 12** Controleer of de kenmerknamen van de Directories Management-directory zijn toegewezen aan de juiste Active Directory-kenmerken.

Als de kenmerknamen van de directory niet goed worden toegewezen, selecteert u het juiste Active Directory-kenmerk in het vervolgkeuzemenu.

- 13** Klik op **Volgende**.

- 14** Klik op  om de groepen te selecteren die u vanuit Active Directory met de directory wilt synchroniseren.

Wanneer u een groep toevoegt vanuit Active Directory, worden de leden van de groep aan de lijst Gebruikers toegevoegd als ze hierin nog niet worden vermeld. Wanneer u een groep synchroniseert, worden gebruikers die Domeingebruikers niet als hun primaire groep in Active Directory hebben, niet gesynchroniseerd.

Opmerking Het systeem van gebruikersverificatie van Directories Management importeert gegevens uit Active Directory bij het toevoegen van groepen en gebruikers. De snelheid van het systeem wordt beperkt door de mogelijkheden van Active Directory. Als gevolg hiervan kunnen importbewerkingen veel tijd in beslag nemen, afhankelijk van het aantal groepen en gebruikers dat wordt toegevoegd. Om het risico op vertragingen of problemen te beperken, raden we u aan het aantal groepen en gebruikers te beperken tot de groepen en gebruikers die vereist zijn voor het gebruik van vRealize Automation.


Als de prestaties van het systeem afnemen of fouten optreden, sluit u niet-vereiste toepassingen en zorgt u ervoor dat uw systeem voldoende geheugen toewijst aan Active Directory. Als de problemen zich blijven voordoen, kunt u de geheugentoewijzing voor Active Directory naar wens verhogen. Voor systemen met grote aantallen gebruikers en groepen moet u mogelijk de geheugentoewijzing voor Active Directory verhogen tot maximaal 24 GB.

- 15** Klik op **Volgende**.

- 16** Klik op  om aanvullende gebruikers toe te voegen.

De juiste waarden zijn als volgt:

- Eén gebruiker: **CN=username,CN=Users,OU=Users,DC=myCorp,DC=com**
- Meerdere gebruikers: **OU=Users,OU=myUnit,DC=myCorp,DC=com**

Als u gebruikers wilt uitsluiten, klikt u op  om een filter te maken waarmee bepaalde typen gebruikers worden uitgesloten. U selecteert het gebruikerskenmerk waarop moet worden gefilterd, de queryregel en de waarde.

- 17** Klik op **Volgende**.

- 18** Controleer de pagina om na te gaan hoeveel gebruikers en groepen worden gesynchroniseerd met de directory.

Als u wijzigingen wilt aanbrengen in gebruikers en groepen, klikt u op een van de koppelingen Bewerken.

Opmerking Zorg ervoor dat u gebruiker-DN's opgeeft die eerder onder de basis-DN waren opgegeven. Als de gebruikers-DN buiten de basis-DN ligt, worden gebruikers van die DN gesynchroniseerd, maar kunnen zij zich niet aanmelden.

- 19** Klik op **Naar Workspace pushen** om het synchroniseren met de directory te starten.

Resultaten

De verbinding met Active Directory is voltooid en de geselecteerde gebruikers en groepen worden aan de directory toegevoegd. U kunt nu gebruikers en groepen toewijzen aan de gewenste vRealize Automation-rollen door **Beheer > Gebruikers en groepen > Directory-gebruikers en -groepen** te selecteren. Raadpleeg [Rollen toewijzen aan directorygebruikers of -groepen](#) voor meer informatie.

Wat nu te doen

Als uw vRealize Automation-omgeving is geconfigureerd voor hoge beschikbaarheid, moet u Beheer van directory's specifiek configureren voor hoge beschikbaarheid. Zie [Beheer van directory's configureren voor hoge beschikbaarheid](#).

- 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 webtoepassingen aan de catalogus, kunt u nieuw toegangsbeleid maken.
- Pas aangepaste merkvermelding toe op de beheerconsole, de portaalpagina's van gebruikers en het aanmeldscherm.

Een OpenLDAP-directoryverbinding configureren

U kunt een OpenLDAP-directoryverbinding configureren met Beheer van directory's.

Er bestaan weliswaar verschillende LDAP-protocollen, maar OpenLDAP is het enige protocol dat is getest en goedgekeurd voor gebruik met vRealize Automation Beheer van directory's.

Om uw LDAP-directory te integreren, maakt u een overeenkomstige Directories Management-directory aan en synchroniseert u gebruikers en groepen van uw LDAP-directory met de Directories Management-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 Directories Management-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 Directories Management 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

Opmerking Beheer van directory's gebruikt de standaardpaginagrootte van 1500 voor LDAP-query's. Als u een OpenLDAP-directoryverbinding configureert, moet u de beheerextensie eenvoudige paginaresultaten voor OpenLDAP inschakelen om het aantal weergegeven resultaten te beperken. Het niet gebruiken van deze extensie kan fouten veroorzaken bij de synchronisatie van gebruikers en groepen.

Voorwaarden

- Controleer de configuratie op de pagina Gebruikerskenmerken en voeg overige kenmerken toe die u wilt synchroniseren. U wijst de Directories Management-kenmerken 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 als vereist markeert, behalve het kenmerk **userName**. De instellingen op de pagina Gebruikerskenmerken gelden voor alle directory's in de service. Wanneer een kenmerk als vereist is gemarkeerd, worden gebruikers zonder dat kenmerk niet gesynchroniseerd met de Directories Management-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 Directories Management**domein** wanneer u de Directories Management-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 Selecteer **Beheer > Beheer van directory's > Directory's**.
- 2 Klik op **Directory toevoegen** en selecteer **LDAP-directory toevoegen**.

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

Optie	Beschrijving
Directorynaam	Voer een naam in voor de Directories Management-directory.
Directorysynchronisatie en -verificatie	<p>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 Directories Management.</p> <p>Een connectoronderdeel is standaard altijd beschikbaar bij de Directories Management-service. Deze connector verschijnt in het vervolgkeuzemenu. Als u meerdere Directories Management-apparaten installeert voor hoge beschikbaarheid, verschijnt het connectoronderdeel van elk van die apparaten in de lijst.</p> <p>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.</p> <p>b In het veld Verificatie selecteert u Ja wanneer u deze LDAP-directory wilt gebruiken voor het verifiëren van gebruikers.</p> <p>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 Beheren > Beheer van directory's > Identiteitsproviders om de identiteitsprovider voor verificatie toe te voegen.</p> <p>c In de meeste configuraties laat u het selectievakje Aangepast van het tekstvak Zoekkenmerken directory standaard ingeschakeld. In het veld Aangepast zoekkenmerk directory specificeert u het LDAP-directorykenmerk dat wordt gebruikt voor de naam van gebruikers en groepen. Dit kenmerk vormt een unieke identificatie voor entiteiten, zoals gebruikers en groepen, op de LDAP-server. Bijvoorbeeld cn.</p> <p>d Als u DNS Service Location-opzoeken voor Active Directory wilt gebruiken, maakt u de volgende selecties.</p> <ul style="list-style-type: none"> ■ Schakel in de sectie Serverlocatie het selectievakje Deze directory ondersteunt DNS-servicelocatie in. <p>Beheer van directory's vindt en gebruikt optimale domeincontrollers. Als u geen gebruik wilt maken van de selectie van geoptimaliseerde domeincontrollers, gaat u door naar stap e.</p> <ul style="list-style-type: none"> ■ Als Active Directory STARTTLS-versleuteling vereist, schakelt u het selectievakje Deze directory vereist dat alle verbindingen SSL gebruiken in de sectie Certificaten in en kopieert en plakt u het root-CA-certificaat van Active Directory in het tekstvak SSL-certificaat. <p>Zorg ervoor dat het certificaat de PEM-indeling heeft en dat regels 'BEGIN CERTIFICATE' en 'END CERTIFICATE' erin zijn opgenomen.</p> <p>Opmerking Als de Active Directory STARTTLS vereist en u verstrekt het certificaat niet, kunt u de directory niet maken.</p> <p>e Als u DNS Service Location-opzoeken voor Active Directory niet wilt gebruiken, maakt u de volgende selecties.</p> <ul style="list-style-type: none"> ■ In de sectie Serverlocatie controleert u of het selectievakje Deze directory ondersteunt DNS-servicelocatie niet is ingeschakeld en

Optie	Beschrijving
	<p>voert u de serverhostnaam en het poortnummer van de Active Directory in. Zie de sectie Active Directory-omgeving met één forest en meerdere domeinen in Active Directory-omgevingen om de directory te configureren als globale catalogus.</p> <ul style="list-style-type: none"> ■ 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 <p>Zorg ervoor dat het certificaat de PEM-indeling heeft en dat regels 'BEGIN CERTIFICATE' en 'END CERTIFICATE' erin zijn opgenomen.</p> <p>Opmerking Als de Active Directory STARTTLS vereist en u verstrekt het certificaat niet, kunt u de directory niet maken.</p>
Serverlocatie	<p>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.</p> <p>Als u een cluster servers achter een load-balancer hebt, voert u in plaats daarvan de informatie van de load-balancer in.</p>
LDAP-configuratie	<p>Geef de zoekfilters en kenmerken van LDAP op die Directories Management kan gebruiken om uw LDAP-directory op te vragen. Standaardwaarden worden verstrekt op basis van het LDAP-kernschema.</p> <p>Query's filteren</p> <ul style="list-style-type: none"> ■ Groepen: het zoekfilter om groepsobjecten te verkrijgen. <p>Bijvoorbeeld: (objectClass=group)</p> <ul style="list-style-type: none"> ■ Bindingsgebruiker: het zoekfilter om een bindingsgebruikerobject te verkrijgen, ofwel de gebruiker die zich aan de directory kan binden. <p>Bijvoorbeeld: (objectClass=person)</p> <ul style="list-style-type: none"> ■ Gebruikers: het zoekfilter om gebruikers te verkrijgen om te synchroniseren. <p>Bijvoorbeeld: (&(objectClass=user)(objectCategory=person))</p> <p>Kenmerken</p> <ul style="list-style-type: none"> ■ Lidmaatschap: het kenmerk dat wordt gebruikt in uw LDAP-directory om leden van een groep te definiëren. <p>Bijvoorbeeld: lid</p> <ul style="list-style-type: none"> ■ Object-UUID: het kenmerk dat wordt gebruikt in uw LDAP-directory om de UUID van een gebruiker of groep te definiëren. <p>Bijvoorbeeld: entryUUID</p> <ul style="list-style-type: none"> ■ Distinguished Name: het kenmerk dat wordt gebruikt in uw LDAP-directory voor de DN-naam van een gebruiker of groep. <p>Bijvoorbeeld: entryDN</p>

Optie	Beschrijving
Certificaten	<p>Als voor uw LDAP-directory SSL-toegang is vereist, schakelt u het selectievakje Deze directory vereist dat alle verbindingen SSL gebruiken in. Kopieer vervolgens het basis-CA SSL-certificaat van de LDAP-directoryserver naar het tekstvak SSL-certificaat. Zorg ervoor dat het certificaat de PEM-indeling heeft en de regels "BEGIN CERTIFICATE" en "END CERTIFICATE" erin zijn opgenomen.</p> <p>Als de directory meerdere domeinen heeft, voegt u een voor een de root-CA-certificaten van alle domeinen toe.</p> <p>Controleer tot slot of het juiste poortnummer is opgegeven in het veld Serverpoort in de sectie Serverlocatie van de pagina.</p>
Bind-gebruikersdetails	<p>Basis DN: voer de DN in van waaruit zoekopdrachten worden gestart. Bijvoorbeeld cn=users,dc=example,dc=com</p> <p>Alle bijbehorende gebruikers moeten zich onder de Basis-DN bevinden. Gebruikers die niet op die locatie zijn ondergebracht, kunnen zich niet aanmelden, zelfs niet als ze lid zijn van een groep die in de Basis-DN is opgenomen.</p> <p>Bind DN: voer de DN in die wordt gebruikt om aan de LDAP-directory te binden. U kunt ook gebruikersnamen invoeren, maar voor de meeste implementaties is het beter een DN te gebruiken.</p> <hr/> <p>Opmerking Het gebruik van een gebruikersaccount van Bind DN met een wachtwoord dat niet verloopt, wordt aanbevolen.</p> <hr/> <p>Wachtwoord Bind-DN: voer het wachtwoord in voor de Bind DN-gebruiker.</p>

- 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.

- Klik op **Opslaan en Volgende**.

- Controleer of het juiste domein is geselecteerd op de pagina Domein selecteren en klik op **Volgende**.

- Verifieer op de pagina Kenmerken toewijzen of de Directories Management-kenmerken zijn toegewezen aan de juiste LDAP-kenmerken.

Deze kenmerken worden gesynchroniseerd voor gebruikers.

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

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

- Klik op **Volgende**.

- Klik op de pagina Groepen (gebruikers) selecteren om te synchroniseren op **+** om de groepen te selecteren die u vanuit de LDAP-directory wilt synchroniseren met de Directories Management-directory.

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

Wanneer u een groep toevoegt vanuit Active Directory, worden de leden van de groep aan de lijst Gebruikers toegevoegd als ze hierin nog niet worden vermeld. Wanneer u een groep synchroniseert, worden gebruikers die Domeingebruikers niet als hun primaire groep in Active Directory hebben, niet gesynchroniseerd.

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. Geneste groepen worden niet gesynchroniseerd; alleen de gebruikers die tot de geneste groepen behoren, worden gesynchroniseerd. In de directory van Directories Management 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 Directories Management als leden van de geselecteerde groep.

Als deze optie is gedeactiveerd 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 bronnen en tijd kost. Als u deze optie deactiveert, zorg er dan voor dat u alle groepen selecteert waarvan u de gebruikers wilt synchroniseren.

Opmerking Het systeem van gebruikersverificatie van Directories Management importeert gegevens uit Active Directory bij het toevoegen van groepen en gebruikers. De snelheid van het systeem wordt beperkt door de mogelijkheden van Active Directory. Als gevolg hiervan kunnen importbewerkingen lange tijd in beslag nemen, afhankelijk van het aantal groepen en gebruikers dat wordt toegevoegd. Om het risico op vertragingen of problemen te beperken, raden we u aan het aantal groepen en gebruikers te beperken tot de groepen en gebruikers die vereist zijn voor het gebruik van vRealize Automation.

Als de prestaties van het systeem afnemen of fouten optreden, sluit u niet-vereiste toepassingen en zorgt u ervoor dat uw systeem voldoende geheugen toewijst aan Beheer van directory's. Als de problemen zich blijven voordoen, kunt u de geheugentoewijzing voor Beheer van directory's naar wens verhogen. Voor systemen met grote aantallen gebruikers en groepen moet u mogelijk de geheugentoewijzing voor Beheer van directory's verhogen tot maximaal 24 GB.

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.

U kunt hier zowel organisatie-eenheden als afzonderlijke gebruikers toevoegen.

U kunt een filter maken waarmee bepaalde typen gebruikers worden uitgesloten. Selecteer het gebruikerskenmerk waarop moet worden gefilterd, de queryregel en de waarde.

12 Klik op **Volgende**.

- 13** 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.

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

Resultaten

De verbinding met de LDAP-directory wordt tot stand gebracht en gebruikers en groepen worden gesynchroniseerd van de LDAP-directory met de Directories Management-directory.

U kunt nu gebruikers en groepen toewijzen aan de gewenste vRealize Automation-rollen door **Beheer > Gebruikers en groepen > Directory-gebruikers en -groepen** te selecteren. Raadpleeg [Rollen toewijzen aan directorygebruikers of -groepen](#) voor meer informatie.

Beperkingen van LDAP-directory-integratie

Er zijn verschillende belangrijke beperkingen met betrekking tot LDAP-directory-integratie in het beheer van directory's.

- U kunt slechts één domein van een LDAP-directory-omgeving integreren
Om meerdere domeinen van een LDAP-directory te integreren, moet u extra Directories Management-mappen aanmaken, één voor elk domein.
- De volgende verificatiemethoden worden niet ondersteund voor Directories Management-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 Directories Management-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 Directories Management-service.

- Wanneer uw LDAP-directory meerdere groepen met dezelfde naam bevat, moet u voor deze groepen unieke namen specificeren in de Directories Management-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.

Beheer van directory's configureren voor hoge beschikbaarheid

U kunt Beheer van directory's gebruiken voor het configureren van een Active Directory-verbinding met hoge beschikbaarheid in vRealize Automation.

Elke vRealize Automation-toepassing bevat een connector die ondersteuning biedt voor gebruikersverificatie, hoewel er meestal maar één connector wordt geconfigureerd voor het uitvoeren van synchronisatie tussen directory's. Het maakt niet uit welke connector u kiest als de connector voor synchronisatie. Om hoge beschikbaarheid voor Beheer van directory's te ondersteunen, moet u handmatig een tweede connector configureren die overeenkomt met uw tweede vRealize Automation-toepassing, die verbinding maakt met uw identiteitsprovider en verwijst naar dezelfde Active Directory-instantie. Als er in deze configuratie een storing optreedt in een toepassing, neemt de andere het beheer van gebruikersverificatie over.

In een omgeving met hoge beschikbaarheid moeten alle knooppunten dezelfde verzameling Active Directory-directory's, gebruikers, verificatiemethoden, enz. bedienen. De meest directe methode om dit te bereiken, is door de identiteitsprovider te promoveren naar het cluster door de host van de load balancer in te stellen als de host van de identiteitsprovider. In deze configuratie worden alle verificatieaanvragen doorgeleid naar de load balancer, die de aanvragen doorstuurt naar een van de connectoren.

Een connector wordt ook gebruikt voor gebruikerssynchronisatie. Maar slechts één connector is geconfigureerd voor het uitvoeren van synchronisatie tussen directory's. Gesynchroniseerde gebruikers worden opgeslagen in de toepassingsdatabase, die door alle geclusterde knooppunten kan worden gelezen. Als er een probleem is met de connector die verantwoordelijk is voor directory-synchronisatie, zal de directory-synchronisatie niet meer werken. Om dit probleem op te lossen, moet de tenant-beheerder een andere connector handmatig vragen om de directory-synchronisatie uit te voeren met behulp van de gebruikersinterface van vRealize Automation. Zie [Directorysynchronisatie inschakelen op een tweede connector](#).

Zie [Connectoren en connectorclusters beheren](#) voor meer informatie over het werken met connectoren.

Voorwaarden

- Configureer de vRealize Automation-implementatie met ten minste twee instanties van de vRealize Automation-toepassing.
- Installeer vRealize Automation in de Enterprise-modus voor één domein met twee instanties van de vRealize Automation-toepassing.

- Installeer en configureer een geschikte load balancer voor uw vRealize Automation-implementatie.
- Configureer tenants en Beheer van directory's met behulp van een van de connectoren die worden geleverd bij de geïnstalleerde instanties van de vRealize Automation-toepassing. Zie [Tenantinstellingen configureren](#) voor meer informatie over het configureren van tenants.

Procedure

- 1 Meld u aan bij de load balancer voor uw vRealize Automation-implementatie als tenantbeheerder.

De URL van de load balancer is `<adres van load balancer>/vcac/org/naam_van_tenant`.
- 2 Selecteer **Beheer > Beheer van directory's > Identiteitsproviders**.
- 3 Klik op de identiteitsprovider die momenteel voor uw systeem wordt gebruikt.

De bestaande directory en connector die het basisidentiteitsbeheer voor uw systeem bieden, worden weergegeven.
- 4 Klik op de eigenschappenpagina van de identiteitsprovider op de vervolgkeuzelijst **Een connector toevoegen** en selecteer de connector die overeenkomt met uw secundaire vRealize Automation-toepassing.
- 5 Voer het juiste wachtwoord in het tekstvak **Wachtwoord bindings-DN** in dat wordt weergegeven wanneer u de connector selecteert.
- 6 Klik op **Connector toevoegen**.
- 7 De hoofdconnector wordt standaard weergegeven in het tekstvak **IdP-hostnaam**. Wijzig de hostnaam, zodat deze naar de load balancer wijst.

Directorysynchronisatie inschakelen op een tweede connector

In geval van een probleem met uw primaire connector wordt de verificatie automatisch afgehandeld door een andere connectorinstantie. In geval van een probleem bij directorysynchronisatie moet u de directory-instellingen wijzigen in Directorybeheer zodat de juiste secundaire connectorinstantie wordt gebruikt. U kunt de directorysynchronisatie slechts op één connector tegelijk inschakelen.

Procedure

- 1 Selecteer **Beheer > Beheer van directory's > Directory's**.
- 2 Selecteer de directory die was gekoppeld aan de oorspronkelijke connectorinstantie.

Opmerking U kunt deze informatie bekijken op de pagina **Directory > connectoren**

- 3 In het gedeelte Directorysynchronisatie en verificatie van de pagina Directory selecteert u een andere connectorinstantie in het vervolgkeuzemenu **Synchronisatieconnector**.
- 4 In het gedeelte Bind-gebruikersdetails voert u het wachtwoord van uw Active Directory bind-account in in het tekstvak **Bind DN-wachtwoord**.

5 Klik op **Opslaan**.

Een vertrouwensrelatie in twee richtingen configureren tussen vRealize Automation en Active Directory

Door een vertrouwensrelatie in twee richtingen te configureren tussen uw identiteitsprovider en Active Directory Federated Services kunt u de systeembeveiliging van een vRealize Automation Active Directory-basisverbinding verbeteren.

Als u een vertrouwensrelatie in twee richtingen tussen vRealize Automation en Active Directory wilt configureren, moet u een aangepaste identiteitsprovider maken en Active Directory-metagegevens toevoegen aan deze provider. U moet tevens het standaardbeleid wijzigen dat wordt gebruikt door uw vRealize Automation-implementatie. Ten slotte moet u Active Directory configureren voor het herkennen van uw identiteitsprovider.

Voorwaarden

- Controleer of u tenants hebt geconfigureerd voor uw vRealize Automation-implementatie en een geschikte Active Directory-verbinding hebt ingesteld ter ondersteuning van Active Directory-verificatie van gebruikers-id's en wachtwoorden.
- Active Directory is geïnstalleerd en geconfigureerd voor gebruik op uw netwerk.
- Haal de juiste ADFS-metagegevens (Active Directory Federated Services) op.
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Haal het bestand met federatieve metagegevens op.

U kunt dit bestand downloaden van <https://servernaam.domein/FederationMetadata/2007-06/FederationMetadata.xml>

- 2 Zoek het woord logout en bewerk de locatie van elke instantie, zodat deze wijst naar <https://servernaam.domein/adfs/ls/logout.aspx>

De volgende vermelding:

```
SingleLogoutService
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://servername.domain/adfs/ls/ "/>
```

Moet bijvoorbeeld worden gewijzigd in:

```
SingleLogoutService
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://servername.domain/adfs/ls/logout.aspx"/>
```

3 Maak een nieuwe identiteitsprovider voor uw implementatie.

- a Selecteer **Beheer > Beheer van directory's > Identiteitsproviders**.
- b Klik op **Identiteitsprovider toevoegen** en vul in de velden de vereiste gegevens in.

Optie	Beschrijving
Naam van identiteitsprovider	Geef een naam op voor de nieuwe identiteitsprovider
Identiteitsprovider metadata (URL of XML)	Plak hier de inhoud van het bestand met metagegevens van Active Directory Federated Services.
Beleid voor naam-id in SAML-aanvraag (optioneel)	Voer indien vereist een naam in voor het identiteitsbeleid in de SAML-aanvraag.
Gebruikers	Selecteer de domeinen waarvoor u gebruikers toegangsrechten wilt verlenen.
IDP-metagegevens verwerken	Klik hier om het door u toegevoegde metagegevensbestand te verwerken.
Netwerk	Selecteer de netwerkbereiken waartoe u gebruikers toegang wilt verlenen.
Verificatiemethoden	Voer een naam in voor de verificatiemethode die wordt gebruikt door deze identiteitsprovider.
SAML-context	Selecteer de juiste context voor uw systeem.
SAML-handtekeningcertificaat	Klik op de koppeling naast de kop SAML-metagegevens om de metagegevens voor Beheer van directory's te downloaden.

- c Sla het metagegevensbestand van Beheer van directory's op als `sp.xml`.
- d Klik op **Toevoegen**.

4 Voeg een regel toe aan het standaardbeleid.

- a Selecteer **Beheer > Beheer van directory's > Beleid**.
- b Klik op de naam van het standaardbeleid.
- c Klik op het pictogram **+** onder de kop **Beleidsregels** om een nieuwe regel toe te voegen.

Gebruik de opties op de pagina Een beleidsregel toevoegen om een regel te maken waarmee de juiste primaire en secundaire verificatiemethoden worden opgegeven voor een specifiek netwerkbereik en apparaat.

Als uw netwerkbereik bijvoorbeeld **Mijn machine** is en u toegang moet krijgen tot inhoud op **Alle apparaattypen**, moet u in een typische implementatie verificatie uitvoeren via de volgende methode: **ADFS-gebruikersnaam en -wachtwoord**.

- d Klik op **OK** om het bijgewerkte beleid op te slaan.
- e Sleep de nieuwe regel op de pagina Standaardbeleid naar de bovenkant van de tabel, zodat deze voorrang krijgt boven de bestaande regels.

- 5 Gebruik de beheerconsole van Active Directory Federated Services, of een ander geschikt hulpprogramma, om een Relying Party-vertrouwensrelatie in te stellen met de vRealize Automation-identiteitsprovider.

Voor het instellen van deze vertrouwensrelatie moet u de metagegevens van Directory's beheren importeren die u eerder hebt gedownload. Zie de Microsoft Active Directory-documentatie voor meer informatie over het configureren van Active Directory Federated Services voor vertrouwensrelaties in twee richtingen. Als onderdeel van dit proces moet u het volgende doen:

- Een Relying Party-vertrouwensrelatie instellen. Bij het instellen van deze vertrouwensrelatie moet u het XML-metagegevensbestand van de VMware Identity Provider-serviceprovider importeren die u hebt gekopieerd en opgeslagen.
- Maak een claimregel die de kenmerken die worden opgehaald uit LDAP in de regel Get Attributes omzet in de gewenste SAML-indeling. Nadat u de regel hebt gemaakt, bewerkt u de regel door de volgende tekst toe te voegen:

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/
format"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress", Properties["http://
schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"vmwareidentity.domain.com");
```

SAML-federatie configureren tussen Directories Management en SSO2

U kunt een SAML-federatie tot stand brengen tussen vRealize Automation Directories Management en systemen die SSO2 gebruiken om Single Sign-On te ondersteunen.

Breng federatie tot stand tussen Directories Management en SSO2 door een SAML-verbinding te maken tussen de twee partijen. Momenteel worden uitsluitend end-to-end-stromen ondersteund waarbij SSO2 als identiteitsprovider (IdP) dient en waarbij Directories Management als serviceprovider (SP) dient.

Voor SSO2-gebruikersverificatie moet hetzelfde account aanwezig zijn in zowel Directories Management als SSO2. De UserPrincipalName (UPN) van de gebruiker moet minimaal overeenkomen. Andere eigenschappen kunnen afwijken, omdat ze zijn vereist om het SAML-onderwerp te identificeren.

Voor lokale gebruikers in SSO2, zoals `admin@vsphere.local`, moeten er tevens overeenkomende accounts aanwezig zijn in Directories Management, waarbij de UPN van de gebruiker minimaal moet overeenkomen. Maak deze accounts handmatig of met behulp van een script en de lokale Directories Management-API's om gebruikers te maken.

Voor het instellen van SAML tussen SSO2 en Directories Management moeten de onderdelen Beheer van directory's en SSO worden geconfigureerd.

Tabel 2-4. Configuratie van onderdeel van SAML-federatie

Onderdeel	Configuratie
Beheer van directory's	Configureer SSO2 als externe identiteitsprovider op Directories Management en werk het standaardverificatiebeleid bij. U kunt een geautomatiseerd script maken voor het instellen van Directories Management.
SSO2-onderdeel	Configureer Directories Management als serviceprovider door het bestand Directories Managementsp.xml te importeren. Met dit bestand kunt u SSO2 configureren voor het gebruik van Directories Management als de serviceprovider (SP).

Voorwaarden

- Configureer tenants voor uw vRealize Automation-implementatie. Zie [Aanvullende tenants maken](#).
- Breng een geschikte Active Directory-koppeling tot stand om basisverificatie voor Active Directory gebruikers-ID's en wachtwoorden te ondersteunen.
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Download de metagegevens voor de SSO2-identiteitsprovider via de SSO2-gebruikersinterface.
 - a Meld u als beheerder aan bij vCenter via `https://<cloudvm-hostname>/`.
 - b Klik op de koppeling **Aanmelden bij vSphere Web Client**.
 - c Selecteer in het linkernavigatievenster de optie **Beheer > Single Sign On > Configuratie**.
 - d Klik op **Downloaden** naast de metagegevens voor de kop van uw SAML-serviceprovider. Het `vsphere.local.xml`-bestand moet nu worden gedownload.
 - e Kopieer de inhoud van het bestand `vsphere.local.xml`.
- 2 Op de pagina vRealize AutomationBeheer van directory's Identiteitsproviders maakt u een nieuwe Identiteitsprovider.
 - a Meld u bij vRealize Automation aan als **tenantbeheerder**.
 - b Selecteer **Beheer > Beheer van directory's > Identiteitsproviders**.

- c Klik op **Identiteitsprovider toevoegen** en geef de configuratiegegevens op.

Optie	Actie
Naam van identiteitsprovider	Geef een naam op voor de nieuwe identiteitsprovider.
Tekstvak Metagegevens van identiteitsprovider (URI of XML)	Plak de inhoud van uw SSO2 idp.xml-metagegevensbestand in het tekstvak en klik op IDP-metagegevens verwerken .
Beleid inzake naam-ID in SAML-verzoek (Optioneel)	Voer <code>http://schemas.xmlsoap.org/claims/UPN</code>
Gebruikers	Selecteer de domeinen waarvoor u gebruikers toegangsrechten wilt verlenen.
Netwerk	Selecteer de netwerkbereiken van waaruit u gebruikers toegangsprivileges wilt geven. Als u gebruikers wilt verifiëren op basis van een IP-adres, selecteert u Alle bereiken .
Verificatiemethoden	Geef een naam op voor de verificatiemethode. Gebruik vervolgens het vervolgkeuzemenu SAML-context aan de rechterkant om de verificatiemethode te koppelen aan <code>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</code> .
SAML-ondertekeningscertificaat	Klik op de koppeling naast de kop SAML-metagegevens om de metagegevens voor Beheer van directory's te downloaden.

- d Sla het metagegevensbestand van Beheer van directory's op als `sp.xml`.
- e Klik op **Toevoegen**.
- 3** Werk het betreffende verificatiebeleid bij op de beleidspagina in Beheer van directory's, zodat verificatie wordt doorverwezen naar de externe SSO2-identiteitsprovider.
- a Selecteer **Beheer > Beheer van directory's > Beleid**.
- b Klik op de naam van het standaardbeleid.
- c Klik op de verificatiemethode onder de kop **Beleidsregels** om de bestaande verificatieregel te bewerken.
- d Op de pagina Een beleidsregel bewerken wijzigt u de verificatiemethode van wachtwoord in de gewenste methode.

In dit geval moet de methode SSO2 zijn.
- e Klik op **Opslaan** om het bijgewerkte beleid op te slaan.
- 4** In het linkernavigatievenster selecteert u **Beheer > Single Sign On > Configuratie**, en klikt u op **Bijwerken** om het `sp.xml`-bestand te uploaden naar vSphere.

Gebruikers of groepen toevoegen aan een Active Directory-verbinding

U kunt gebruikers of groepen toevoegen aan een bestaande Active Directory-verbinding.

Het gebruikersverificatiesysteem van Beheer van directory's importeert gegevens uit Active Directory wanneer groepen en gebruikers worden toegevoegd. De snelheid van de gegevensoverdracht wordt beperkt door de mogelijkheden van Active Directory. Hierdoor kunnen acties veel tijd in beslag nemen, afhankelijk van het aantal groepen en gebruikers dat u hebt toegevoegd. U kunt problemen minimaliseren door de groepen en gebruikers te beperken tot alleen die groepen en gebruikers die nodig zijn voor een vRealize Automation-actie. Als er problemen optreden, sluit u alle overbodige toepassingen en controleert u of in uw implementatie voldoende geheugen is toegewezen aan Active Directory. Als het probleem zich herhaalt, verhoogt u de geheugentoewijzing voor Active Directory. Voor implementaties met een groot aantal gebruikers en groepen moet u mogelijk de geheugentoewijzing voor Active Directory verhogen tot maximaal 24 GB.

Wanneer u een vRealize Automation-implementatie met een groot aantal gebruikers en groepen synchroniseert, kunnen de SyncLog-gegevens mogelijk met vertraging beschikbaar worden. De tijdstempel in het logboekbestand kan verschillen van de voltooiingstijd die wordt weergegeven in de console.

Als leden van een groep niet in de lijst met gebruikers staan, worden de leden toegevoegd aan de lijst wanneer u de groep vanuit Active Directory toevoegt. Wanneer u een groep synchroniseert, worden gebruikers die Domeingebruikers niet als hun primaire groep in Active Directory hebben, niet gesynchroniseerd.

Opmerking Nadat u de actie hebt gestart, kunt u een synchronisatieactie niet annuleren.

Voorwaarden

- Connector is geïnstalleerd en de activeringscode is geactiveerd. Selecteer de vereiste standaardkenmerken en voeg aanvullende kenmerken toe op de pagina Gebruikerskenmerken.
- Lijst met de Active Directory-groepen en -gebruikers die u wilt synchroniseren vanuit Active Directory.
- Voor Active Directory via LDAP is onder andere de basis-DN, de bindings-DN en het wachtwoord van de bindings-DN vereist.
- 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.
- Als via SSL toegang wordt verkregen tot Active Directory, is een exemplaar van het SSL-certificaat vereist.
- Als u een Active Directory met meerdere forests hebt geïntegreerd met Windows-verificatie en de lokale domeingroep leden van verschillende forests bevat, doet u het volgende. Voeg de Bind-gebruiker toe aan de beheerdersgroep van de lokale domeingroep. Als de Bind-gebruiker niet wordt toegevoegd, ontbreken deze leden in de lokale domeingroep.
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > Beheer van directory's > Directory's**.
- 2 Klik op de gewenste directorynaam.
- 3 Klik op **Synchronisatie-instellingen** om een dialoogvenster met synchronisatieopties te openen.
- 4 Klik op het pictogram voor het wijzigen van de configuratie van een gebruiker of van een groep.

De groepsconfiguratie bewerken:

- Als u groepen wilt toevoegen, klikt u op het pictogram **+** om een nieuwe regel voor de definitie van een groeps-DN toe te voegen en voert u de betreffende groeps-DN in.
- Als u een DN-groepsdefinitie wilt verwijderen, klikt u op het pictogram **x** voor de gewenste groeps-DN.

De gebruikersconfiguratie bewerken:

- ◆ Als u gebruikers wilt toevoegen, klikt u op het pictogram **+** om een nieuwe regel voor de definitie van een DN-gebruiker toe te voegen en voert u de betreffende gebruikers-DN in.

Als u een DN-gebruikersdefinitie wilt verwijderen, klikt u op het pictogram **x** voor de gewenste gebruikers-DN.

- 5 Klik op **Opslaan** om uw wijzigingen op te slaan zonder uw updates onmiddellijk te synchroniseren. Klik op **Opslaan en synchroniseren** om uw wijzigingen op te slaan en uw updates onmiddellijk te synchroniseren.

Kenmerken selecteren om te synchroniseren met de directory

Wanneer u de Directories Management-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 indien nodig 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.

Raadpleeg [Gebruikerskenmerken beheren die vanuit Active Directory worden gesynchroniseerd](#) voor een lijst met de standaard toegewezen kenmerken.

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.

Procedure

- 1 Meld u als systeem- of tenantbeheerder aan bij vRealize Automation.
- 2 Klik op het tabblad **Beheer**.
- 3 Selecteer **Beheer van directory's > Gebruikerskenmerken**
- 4 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.
- 5 Voeg in de sectie Kenmerken de naam van het Directories Management-directorykenmerk toe aan de lijst.
- 6 Klik op **Opslaan**.
De standaardkenmerkstatus wordt bijgewerkt en de kenmerken die u hebt toegevoegd, worden aan de lijst Toegewezen kenmerken van de directory toegevoegd.
- 7 Nadat de directory is gemaakt, gaat u naar de pagina Identiteitsarchieven en selecteert u de directory.
- 8 Klik op **Synchronisatie-instellingen > Toegewezen kenmerken**.
- 9 Selecteer in het vervolgkeuzemenu voor de kenmerken die u hebt toegevoegd, het Active Directory-kenmerk waarnaar u wilt toewijzen.
- 10 Klik op **Opslaan**.

Resultaten

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

Geheugen toevoegen aan Beheer van directory's

Mogelijk moet u aanvullend geheugen toevoegen aan Directories Management, als u Active Directory-verbindingen hebt met grote hoeveelheden gebruikers of groepen.

Standaard is 4 GB aan geheugen toegewezen aan de Directories Management-service. Dit is voldoende voor veel kleine tot middelgrote implementaties. Als u een Active Directory-verbinding hebt die gebruikmaakt van grote hoeveelheden gebruikers of groepen, moet u mogelijk de geheugentoewijzing verhogen. Verhoogde geheugentoewijzing is bedoeld voor systemen met meer dan 100.000 gebruikers, die zijn onderverdeeld in 30 groepen, met 750 groepen in totaal. Voor dergelijke systemen raadt VMware aan de Directories Management-geheugentoewijzing te verhogen tot 6 GB.

Het geheugen voor Beheer van directory's wordt beheerd op basis van het totale geheugen dat is toegewezen aan de vRealize Automation-toepassing. In de volgende tabel ziet u de geheugentoewijzing voor relevante onderdelen.

Tabel 2-5. Geheugentoewijzing voor de vRealize Automation-toepassing

Geheugen voor virtual appliance	Geheugen voor vRA-service	Geheugen voor vIDM-service
18 GB	3,3 GB	4 GB
24 GB	4,9 GB	6 GB
30 GB	7,4 GB	9,1 GB

Opmerking Bij deze toewijzingen gaan we ervan uit dat alle standaardservices ingeschakeld en actief zijn voor de virtuele toepassing. De geheugentoewijzing kan worden gewijzigd wanneer bepaalde services worden gestopt.

Voorwaarden

- Een geschikte Active Directory-verbinding is geconfigureerd en werkt voor uw vRealize Automation-implementatie.

Procedure

- 1 Stop elke machine waarop een vRealize Automation-toepassing wordt uitgevoerd.
- 2 Verhoog de geheugentoewijzing voor de virtuele toepassing op elke machine.

Als u de standaardgeheugentoewijzing van 18 GB gebruikt, raadt VMware aan dat u de geheugentoewijzing verhoogt naar 24 GB.

- 3 Start de machines met de vRealize Automation-toepassing opnieuw op.

Configureer Just-In-Time-gebruikersprovisioning

U kunt Just-in-Time (JIT) provisioning configureren om te ondersteunen dat gebruikers toegevoegd kunnen worden zonder te synchroniseren met uw Active Directory.

Om Just-in-Time-provisioning te ondersteunen, moet u een externe identiteitsprovider toevoegen en daarmee een verbinding configureren binnen uw vRealize Automation-implementatie, om het beheer van directory's te integreren met andere SSO-providers via een SAML-protocol. Daarnaast moet u een nieuwe directory maken met de juiste naam, bijvoorbeeld JIT Directory.

Wanneer u Just-in-Time-provisioning inschakelt, kunt u Just-in-Time-gebruikers toevoegen aan een aangewezen aangepaste groep. Om deze functionaliteit te ondersteunen, maakt u een aangepaste groep met de juiste leden. Zie [Just-in-time-gebruikers met aangepaste groepen en regels toevoegen](#).

Opmerking Het is een best practice om Just-in-Time-provisioning niet te configureren op de standaard vsphere.local-tenant.

Voorwaarden

Configureer een geschikte externe identiteitsprovider om te gebruiken met JIT-provisioning.

Procedure

1 Maak een identiteitsprovider voor Just-in-Time-provisioning.

- a Selecteer **Beheer > Beheer van directory's > Identiteitsproviders**
- b Klik op **Identiteitsprovider toevoegen** en bewerk de instellingen van de identiteitsproviderinstantie waar relevant.
 - Maak voor Just-in-Time-provisioning een externe identiteitsprovider.
 - In de sectie Just-in-Time-directory maken, voer namen in voor de directory en een of meer domeinen.
 - U moet een netwerk selecteren om de externe identiteitsprovider te configureren.
 - Als u gebruikmaakt van een externe VMware Identity Manager identiteitsprovider, en u gebruikt `userPrincipalName` om gebruikers te verifiëren, moet u de configuratie van de naam-ID-toewijzing wijzigen voor `userPrincipalName` van de standaardwaarde `x509SubjectName` naar `unspecified`.

Zie [Een verbinding met een externe identiteitsprovider configureren](#) voor meer informatie over het maken van identiteitsproviders.

2 Configureer SAML op de Just-in-Time-identiteitsprovider.

- a Kopieer de IdP-metagegevens van uw identiteitsprovider.
- b Selecteer uw identiteitsprovider in vRealize Automation, en plak de IdP-metagegevens in het **tekstvak Metagegevens van Identiteitsprovider (URL of XML)**.
- c Klik op **Opslaan**.
- d Selecteer de juiste indeling in het vervolgkeuzemenu **Naam id-beleid in SAML-aanvraag (optioneel)**.

Bijvoorbeeld: als u het e-mailadres gebruikt als de unieke gebruikers-id, selecteert u `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`.
- e Selecteer de gewenste directory onder de titel Gebruikers.
- f Selecteer de netwerken waarvan deze identiteitsprovider gebruik moet maken onder de titel Netwerk.
- g Geef een geschikte naam op in het tekstvak **Verificatiemethoden**.
- h Selecteer `urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport` in de vervolgkeuzelijst **SAML-Context**
- i Klik met de rechtermuisknop op de koppeling **Metagegevens van de serviceprovider (SP)** en open deze in een tabblad van een nieuw browservenster.
- j Gebruik deze metagegevens om de SAML-verbinding naar uw identiteitsprovider te configureren.

Als u gebruikmaakt van VMware Identity Manager, zie dan de VMware Identity Manager-documentatie voor volledige instructies over het configureren van SAML.

3 Klik op **Toevoegen**.

De nieuwe directory wordt gemaakt met de Directorynaam die wordt opgegeven.

4 Configureer het vRealize Automation-toegangsbeleid.

- a Selecteer **Beheer > Beleid**.
- b Klik op het groene +-pictogram aan de rechterbovenkant van de tabel beleidsregels.
- c Stel de beleidsregel in die van toepassing moeten zijn op de relevante bereiken en apparaattypes.
- d Selecteer de verificatiemethode die u hebt gemaakt bij het configureren van de externe identiteitsprovider voor JIT-provisioning voor de verificatiemethode.

Gebruikerskenmerken beheren die vanuit Active Directory worden gesynchroniseerd

Op de pagina Gebruikerskenmerken van Beheer van directory's ziet u de gebruikerskenmerken die worden gesynchroniseerd met uw Active Directory-verbinding.

Wijzigingen die u aanbrengt en opslaat op de pagina Gebruikerskenmerken, worden toegevoegd aan de pagina Toegewezen kenmerken in de Directories Management-directory. De kenmerk wijzigingen worden bijgewerkt naar de directory bij de volgende synchronisatie naar Active Directory.

De pagina Gebruikerskenmerken geeft de standaarddirectorykenmerken weer die u kunt toewijzen 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.

Tabel 2-6. Active Directory-standaardkenmerken om te synchroniseren met de directory

Naam van directorykenmerk	Standaardtoewijzing aan Active Directory-kenmerk
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeid	employeeID
domain	canonicalName. Hiermee voegt u de Fully Qualified Domain Name van het object toe.
disabled (externe gebruiker uitgeschakeld)	userAccountControl. Gemarkerd met UF_Account_Disable. Wanneer een account is uitgeschakeld, kunnen gebruikers zich niet aanmelden om toegang te krijgen tot hun toepassingen en bronnen. De bronnen waarvoor gebruikers rechten hebben, zijn niet verwijderd uit het account, dus wanneer de markering uit het account is verwijderd, kunnen gebruikers zich aanmelden en toegang krijgen tot de bronnen waarvoor ze rechten hebben.
phone	telephoneNumber
lastName	sn

Tabel 2-6. Active Directory-standaardkenmerken om te synchroniseren met de directory (vervolg)

Naam van directorykenmerk	Standaardtoewijzing aan Active Directory-kenmerk
firstName	givenName
email	mail
Gebruikersnaam	sAMAccountNaam

De pagina Gebruikerskenmerken geeft de standaarddirectorykenmerken weer die u kunt toewijzen 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.

Tabel 2-7. Active Directory-standaardkenmerken om te synchroniseren met de directory

Naam van directorykenmerk	Standaardtoewijzing aan Active Directory-kenmerk
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeID	employeeID
domain	canonicalName. Hiermee voegt u de Fully Qualified Domain Name van het object toe.
disabled (externe gebruiker uitgeschakeld)	userAccountControl. Gemarkerd met UF_Account_Disable. Wanneer een account is uitgeschakeld, kunnen gebruikers zich niet aanmelden om toegang te krijgen tot hun toepassingen en bronnen. De bronnen waarvoor gebruikers rechten hebben, zijn niet verwijderd uit het account, dus wanneer de markering uit het account is verwijderd, kunnen gebruikers zich aanmelden en toegang krijgen tot de bronnen waarvoor ze rechten hebben.
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
Gebruikersnaam	sAMAccountNaam

Connectoren en connectorclusters beheren

Op de pagina Connectoren worden geïmplementeerde connectoren weergegeven voor uw bedrijfsnetwerk. Met een connector worden gebruikers- en groepsgegevens tussen Active Directory en de Directories Management-service gesynchroniseerd. Wanneer de connector als identiteitsprovider wordt gebruikt, worden gebruikers hiermee bij de service geverifieerd.

In vRealize Automation bevat elke vRealize Automation-toepassing-toepassing een eigen connector. Deze zijn geschikt voor de meeste implementaties.

Wanneer u een directory koppelt aan een connectorinstantie, wordt door de connector een partitie gemaakt voor de gekoppelde directory, die we een werker noemen. Een connectorinstantie kan meerdere gekoppelde werkers hebben. Elke werker fungeert als identiteitsprovider. Door de connector worden gebruikers- en groepsgegevens gesynchroniseerd tussen Active Directory en de service via een of meer werkers. U kunt verificatiemethoden definiëren en configureren per werker.

U kunt verschillende aspecten van een Active Directory-verbinding beheren via de pagina Connectoren. De pagina bevat een tabel en verschillende knoppen waarmee u enkele beheertaken kunt uitvoeren.

- Selecteer in de kolom Werker een werker om de gegevens van de connector weer te geven en ga naar de pagina Verificatieadapters om de status van de beschikbare verificatiemethoden weer te geven. Zie [Alternatieve producten voor gebruikersverificatie integreren in Beheer van directory's](#) voor informatie over verificatie.
- Selecteer in de kolom Identiteitsprovider de IDP die u wilt weergeven, bewerken of deactiveren. Zie [Een verbinding met een externe identiteitsprovider configureren](#).
- Open in de kolom Gekoppelde directory de directory die aan deze werker is gekoppeld.
- Klik op **Deelnemen aan domein** om de connector te koppelen aan een specifiek Active Directory-domein. Als u Kerberos-verificatie configureert, moet u bijvoorbeeld deelnemen aan het Active Directory-domein dat gebruikers bevat of dat een vertrouwensrelatie heeft met het domein dat de gebruikers bevat.
- Wanneer u een directory configureert met Active Directory met geïntegreerde Windows-verificatie, wordt de connector lid van het domein op basis van de configuratiegegevens.

Connectoren in een geclusterde omgeving

In een gedistribueerde vRealize Automation-implementatie voeren alle beschikbare connectoren alle vereiste gebruikersautorisaties uit, terwijl één toegewezen connector alle configuratiesynchronisaties uitvoert. Doorgaans omvat synchronisatie toevoegingen, verwijderingen of wijzigingen aan de gebruikersconfiguratie en verloopt de synchronisatie automatisch zolang alle connectoren beschikbaar zijn. Er zijn bepaalde specifieke situaties waarin automatische synchronisatie mogelijk niet plaatsvindt.

Voor wijzigingen met betrekking tot directoryconfiguratie, zoals Basis-DN, probeert vRealize Automation updates automatisch naar alle connectoren in een cluster te pushen. Als een connector om een bepaalde reden onbruikbaar of onbereikbaar is, zal die connector de update niet ontvangen, zelfs wanneer deze weer online werkt. Om configuratiewijzigingen te implementeren in connectoren die deze mogelijk niet automatisch hebben ontvangen, moeten systeembeheerders de wijzigingen handmatig opslaan in alle toepasselijke connectoren.

Voor wijzigingen met betrekking tot het directoriesynchronisatieprofiel probeert vRealize Automation updates ook automatisch naar alle connectoren te pushen. Als de synchronisatieconnector operationeel is, wordt de update opgeslagen en naar alle beschikbare autorisatieconnectoren gepusht. Als een of meer connectoren onbereikbaar zijn, ontvangt de systeembeheerder een waarschuwing dat niet alle connectoren zijn bijgewerkt. Als de

synchronisatieconnector onbruikbaar is, mislukt de update en leidt dit tot een fout. Als de systeembeheerder de connector wijzigt die als de synchronisatieconnector is toegewezen, ontvangt de nieuwe synchronisatieconnector de nieuwste beschikbare profielinformatie en wordt die informatie gepusht naar alle toepasselijke, en beschikbare, connectoren.

Een connectormachine toevoegen aan een domein

In sommige gevallen moet u mogelijk een machine met een connector van Beheer van directory's toevoegen aan een domein.

Bij Active Directory via LDAP-directory's maakt u eerst de directory en voegt u vervolgens de controller aan het domein toe. 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 de bijbehorende 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

Als u een computer lid maakt van een domein, wordt een computerobject gemaakt op de standaardlocatie van Active Directory.

Als u niet over de juiste rechten beschikt om computers lid te maken van een domein of als het beleid van uw organisatie een aangepaste locatie voor het computerobject vereist, vraagt u de beheerder het object te maken en voegt u de connectormachine toe aan het domein.

Procedure

- 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. U moet de hostnaam van de connector opgeven. Zorg dat u de volledig gekwalificeerde domeinnaam invoert, bijvoorbeeld `server.example.com`.

U ziet de hostnaam in de kolom Hostnaam op de pagina Connectoren van de beheerconsole. Selecteer **Beheer > Beheer van directory's > Connectoren**.

- 2 Als het computerobject is gemaakt, klikt u op **Aan domein toevoegen** op de pagina Connectoren om de machine lid te maken van het domein. Gebruik hiervoor een van de beschikbare gebruikersaccounts voor domeinen in Beheer van directory's.

Domeincontrollers selecteren

Beheer van directory's houdt een dynamische lijst met domeincontrollers bij waarvoor geen gebruikersconfiguratie is vereist.

Beheer van directory's vernieuwt regelmatig domeincontrollers en detecteert en ordent ze opnieuw op basis van LDAP Ping, en slaat deze op in een domain_krb.properties-bestand en een aangepast krb5.conf-bestand. De beste domeincontroller staat bovenaan in de lijst en wordt daarom voor alle doeleinden gebruikt, zoals verificatie en synchronisatiebewerkingen. Als deze domeincontroller niet binnen 10 ms reageert, wordt de lijst met domeincontrollers opnieuw vernieuwd. Hierdoor gebruikt Beheer van directory's altijd optimale domeincontrollers, zelfs in geval van storingen van domeincontrollers.

Toegangsbeleid beheren

Het Directories Management-beleid bestaat uit een verzameling regels die criteria opgeven waaraan moet worden voldaan, zodat gebruikers toegang kunnen krijgen tot hun toepassingsportal of opgegeven webtoepassingen kunnen starten.

U maakt de regel als onderdeel van een beleid. Met elke regel in een beleid kan de volgende informatie worden opgegeven.

- Het netwerkbereik van waaruit gebruikers zich mogen aanmelden, zoals binnen of buiten het bedrijfsnetwerk.
- Het apparaattype dat toegang krijgt via dit beleid.
- De volgorde waarin de ingeschakelde verificatiemethoden worden toegepast.
- Het aantal uren dat de verificatie geldig is.
- Aangepast bericht Toegang geweigerd.

Opmerking Het beleid beheert de periode die een webtoepassingsessie duurt niet. Het beheert de hoeveelheid tijd die gebruiker krijgen om een webtoepassing te starten.

De Directories Management-service bevat standaardbeleid dat u kunt bewerken. Met dit beleid wordt toegang tot de service als geheel beheerd. Zie [Het standaardtoegangsbeleid toepassen](#). U kunt aanvullend beleid maken voor het beheren van toegang tot specifieke webtoepassingen. Als u geen beleid toepast op een webtoepassing, is het standaardbeleid van toepassing.

Instellingen voor toegangsbeleid configureren

Een beleid bevat een of meer toegangsregels. Elke regel bestaat uit instellingen die u kunt configureren voor het beheer van gebruikerstoegang tot toepassingsportals als geheel of tot opgegeven webtoepassingen.

Netwerkbereik

U bepaalt de gebruikersbasis voor elke regel door een netwerkbereik op te geven. Een netwerkbereik bestaat uit een of meer IP-bereiken. U maakt netwerkbereiken op het tabblad Identiteits- en toegangsbeheer op de pagina Installatie > Netwerkbereiken voordat u toegangsbeleidsets configureert.

Apparaatype

Selecteer het type apparaat dat de regel beheert. De clienttypen zijn Webbrowser, Clientapp voor identiteitsbeheer, iOS, Android en Alle apparaattypen.

Groepen toevoegen

U kunt verschillende beleidsregels toepassen voor verificatie op basis van het lidmaatschap van uw gebruikers. Om groepen gebruikers toe te wijzen om in te loggen via een specifieke verificatiestroom, kunt u groepen toevoegen aan de toegangsbeleidsregel. U kunt groepen synchroniseren vanuit uw bedrijfsdirectory of lokale groepen die u hebt gemaakt in de beheerdersconsole. Groepsnamen moeten uniek zijn binnen een domein.

Om groepen te gebruiken in toegangsbeleidsregels, configureert u een nieuw beleid vanaf de pagina Beheer van directory's > Beleid en selecteert u de gewenste groepen voor het beleid. Het beleid moet worden toegewezen op de pagina Gebruikerskenmerken en vervolgens met de directory worden gesynchroniseerd.

Wanneer groepen worden gebruikt in een toegangsbeleidsregel, verandert de gebruikersaanmelding voor de gebruiker. In plaats van gebruikers te vragen hun domein te selecteren en vervolgens hun inloggegevens in te voeren, wordt een pagina weergegeven met de vraag om hun unieke ID in te voeren. Directories Management vindt de gebruiker in de interne database op basis van de unieke ID en geeft de verificatiepagina weer die in die regel is geconfigureerd.

Wanneer een groep niet is geselecteerd, is de toegangsbeleidsregel van toepassing op alle gebruikers. Wanneer u toegangsbeleidsregels configureert die regels op basis van groepen en een regel voor alle gebruikers omvatten, moet u ervoor zorgen dat de regel die voor alle gebruikers is ingesteld de laatste regel is die wordt vermeld in het gedeelte Beleidsregels van het beleid.

Raadpleeg de documentatie van VMware Identity Manager over Inlogervaring met behulp van de unieke identificatie voor meer informatie over hoe regels op gebruikers worden toegepast.

Verificatiemethoden

Stel de prioriteit van de verificatiemethoden voor de beleidsregel in. De verificatiemethoden worden toegepast in de volgorde waarin ze worden weergegeven. De eerste identiteitsproviderinstantie die voldoet aan de verificatiemethode en de netwerkbereikconfiguratie in het beleid, wordt geselecteerd, en de gebruikersverificatieaanvraag wordt naar de identiteitsproviderinstantie doorgestuurd voor verificatie. Als de verificatie mislukt, wordt de volgende verificatiemethode in de lijst geselecteerd. Als certificaatverificatie wordt gebruikt, moet deze methode de eerste verificatiemethode in de lijst zijn.

U kunt toegangsbeleidsregels configureren om te eisen dat gebruikers verificatiegegevens via twee verificatiemethoden opgeven voordat ze zich kunnen aanmelden. Als een of beide verificatiemethoden mislukken en er ook alternatieve methoden zijn geconfigureerd, dan worden de gebruikers gevraagd om hun verificatiegegevens in te voeren voor de volgende verificatiemethoden die zijn geconfigureerd. De volgende twee scenario's beschrijven hoe verificatieketens werken.

- In het eerste scenario is de toegangsbeleidsregel geconfigureerd zodat gebruikers verificatie moeten uitvoeren met hun wachtwoord en hun Kerberos-verificatiegegevens. Alternatieve verificatie wordt ingesteld om het wachtwoord en de RADIUS-verificatiegegevens te vereisen voor verificatie. Een gebruiker voert het wachtwoord correct in, maar voert niet de juiste Kerberos-verificatiegegevens in. Omdat de gebruiker het juiste wachtwoord heeft ingevoerd, geldt de alternatieve verificatieaanvraag alleen voor de RADIUS-verificatiegegevens. De gebruiker moet het wachtwoord niet opnieuw invoeren.
- In het tweede scenario is de toegangsbeleidsregel geconfigureerd zodat gebruikers verificatie moeten uitvoeren met hun wachtwoord en hun Kerberos-verificatiegegevens. Alternatieve verificatie wordt ingesteld om RSA SecurID en een RADIUS te vereisen voor verificatie. Een gebruiker voert het wachtwoord correct in, maar voert niet de juiste Kerberos-verificatiegegevens in. De alternatieve verificatieaanvraag geldt zowel voor de RSA SecurID-verificatiegegevens als voor de RADIUS-verificatiegegevens.

Lengte van verificatiesessie

Voor elke regel stelt u de lengte in waarin deze verificatie geldig is. De waarde bepaalt de maximale hoeveelheid tijd waarover gebruikers sinds hun laatste verificatiegebeurtenis beschikken om toegang te krijgen tot hun portaal of om een specifieke webtoepassing te starten. Een waarde van 4 in een webtoepassingsregel bijvoorbeeld geeft gebruikers vier uur tijd om de webtoepassing te starten tenzij ze een andere verificatiegebeurtenis starten die de tijd verlengt.

Aangepast toegang geweigerd-bericht

Wanneer gebruikers zich proberen aan te melden en dit mislukt als gevolg van ongeldige verificatiegegevens, een onjuiste configuratie of een systeemfout, wordt een toegang geweigerd-bericht weergegeven. Het standaardbericht is

Toegang geweigerd omdat geen geldige verificatiemethoden zijn gevonden.

U kunt een aangepast foutbericht maken voor elke toegangsbeleidsregel, die het standaardbericht vervangt. Het aangepaste bericht kan tekst bevatten en een koppeling voor een bericht met een actieverzoek. Als bijvoorbeeld in een beleid voor het beheren van mobiele apparaten een gebruiker zich probeert aan te melden met een niet-geregistreerd apparaat, kan het volgende aangepaste foutbericht worden weergegeven:

Registreer uw apparaat om toegang te krijgen tot bedrijfsbronnen door te klikken op de koppeling aan het einde van dit bericht. Neem contact op met ondersteuning voor hulp als uw apparaat al is geregistreerd.

Voorbeeld van standaardbeleid

Het volgende beleid dient als voorbeeld van hoe u het standaardbeleid kunt configureren voor het beheer van toegang tot de toepassingsportal. Zie [Het toegangsbeleid voor gebruikers beheren](#).

De beleidsregels worden geëvalueerd in de weergegeven volgorde. U kunt de volgorde van het beleid wijzigen door de regel in de sectie Beleidsregels te slepen en neer te zetten.

In de volgende use case wordt dit beleidsvoorbeeld gebruikt voor alle toepassingen.

STANDAARDBELEID

* Naam beleid: default_access_policy_set

Omschrijving: Default access policy set

Van toepassing op: Alle toepassingen

Beleidsregels

U kunt een lijst met regels maken voor de toegang tot deze webtoepassingen. Selecteer voor elke regel het IP-netwerkbereik, het type apparaten waarmee toepassingen kunnen worden gebruikt, de methoden en verificatievolgorde, en het maximale aantal uren dat gebruikers de toepassing kunnen gebruiken voordat herverificatie nodig is.

Netwerkbereik	Apparaattype	Verificatiemethode	Herverificatie	
ALLE BEREIKEN	Webbrowser	Password	8 Uur/juren	✗ +
ALLE BEREIKEN	Identity Manager Client-app	Password	2160 Uur/juren	✗ +

Opslaan Annuleren

- Voor het interne netwerk (intern netwerkbereik) worden twee verificatiemethoden geconfigureerd voor de regel, namelijk Kerberos en wachtwoordverificatie als de alternatieve methode. Om toegang tot het portaal met apps te krijgen vanaf een intern netwerk, probeert de service eerst gebruikers te verifiëren met Kerberos-verificatie, omdat dit de eerste verificatiemethode is die in de regel wordt weergegeven. Als dit mislukt, worden de gebruikers gevraagd om hun Active Directory-wachtwoord in te voeren. Gebruikers melden zich aan met een browser en hebben nu toegang tot hun gebruikersportalen voor een sessie van acht uur.
 - Voor toegang vanaf het externe netwerk (alle bereiken) wordt slechts één verificatiemethode geconfigureerd, namelijk RSA SecurID. Om toegang tot het portaal met apps te krijgen vanaf een extern netwerk, moeten gebruikers zich aanmelden met SecurID. Gebruikers melden zich aan met een browser en hebben nu toegang tot hun portalen met apps voor een sessie van vier uur.
- Als een gebruiker toegang probeert te krijgen tot een bron, behalve voor webtoepassingen die worden gedekt door een webtoepassingsspecifiek beleid, is het standaardportaaltoegangsbeleid van toepassing.

De tijd voor herverificatie voor dergelijke bronnen bijvoorbeeld komt overeen met de tijd voor herverificatie van de beleidsregel voor standaardtoegang. Als de tijd voor een gebruiker die zich bij het portaal met apps aanmeldt, acht uur is volgens de standaardtoegangsbeleidsregel, en de gebruiker probeert een bron te starten tijdens de sessie, dan wordt de toepassing opgestart zonder dat de gebruiker zich opnieuw moet verifiëren.

Configureer een op een groep gebaseerd toegangsbeleid

U kunt een op een groep gebaseerd toegangsbeleid configureren om op groepstaken gebaseerde inlogbevoegdheden te beheren.

Beheer van Directory's bevat standaardtoegangsbeleidsregels die ondersteuning bieden voor alle groepen en alle netwerkbereiken. U kunt deze beleidsregels aanpassen om ze beperkter te maken of u kunt nieuwe beleidsregels ter ondersteuning van verschillende inlogbeleidsregels maken.

Procedure

1 Voeg groepen toe aan het gewenste beleid.

a Selecteer **Beheer > Beheer van directory's > Beleid**.

b U kunt het standaardtoegangsbeleid openen of een nieuw beleid maken.

c Bewerk de beleidsregel die is geconfigureerd met een toesteltype van Web Browser.

Als u een beleid wilt bewerken, klikt u op de Verificatiemethode. Standaard zijn er twee beleidsregels die van toepassing zijn op alle IP-adressen en alle gebruikers.

De pagina Beleidsregel bewerken wordt geopend voor het geselecteerde beleid. U kunt verschillende parameters bewerken, zoals het Netwerkbereik, het Apparaattype, Verificatiemethoden en andere regelparameters voor het beleid.

d Klik op **Groepen bewerken** op de pagina Beleidsregel bewerken om alle groepen te bekijken die beschikbaar zijn voor gebruik met het beleid.

Op deze pagina ziet u alle groepen die zijn gekoppeld aan de tenant.

e Selecteer de groepen die u wilt koppelen aan het beleid.

f Klik op **OK**.

De geselecteerde groepen worden op de pagina Beleidsregel bewerken weergegeven.

g Klik op **OK** op de pagina Beleidsregel bewerken om de wijzigingen in de beleidsregel op te slaan.

De pagina Beleidsregels wordt weergegeven met het aantal groepen die voor het beleid zijn geselecteerd.

h Klik op **Opslaan** op de pagina Beleidsregels.

2 Configureer een Netwerkbereik voor het groepsbeleid.

- a Selecteer **Beheer > Beheer van directory's > Netwerkbereiken**.

Standaard is er een vooraf gedefinieerde instelling van **All Ranges** die alle IP-adressen voor alle netwerkbereiken omvat. U kunt een nieuw netwerkbereik maken of een van de bestaande netwerkbereiken bewerken.

- b Klik op **Netwerkbereik toevoegen**.

De pagina Netwerkbereik bewerken wordt weergegeven.

- c Voer een **Naam** in voor het nieuwe netwerkbereik en voeg een **Beschrijving** toe, indien nodig.

Resultaten

Wanneer gebruikers zich aanmelden bij vRealize Automation, moeten ze het domein selecteren en een geldige gebruikersnaam en wachtwoord invoeren. Als een groep is opgegeven in het beleid dat van toepassing is, moeten geldige gebruikers nog steeds een gebruikersnaam en wachtwoord invoeren.


Webtoepassingsspecifiek beleid beheren

Wanneer u webtoepassingen toevoegt aan de catalogus, kunt u voor webtoepassingen specifiek toegangsbeleid maken. U kunt bijvoorbeeld een beleid maken met regels voor een webtoepassing dat opgeeft welke IP-adressen toegang hebben tot de toepassing, met welke verificatiemethoden en hoe lang ze toegang hebben voordat ze opnieuw moeten worden geverifieerd.

Het volgende voor webtoepassingen specifieke beleid biedt een voorbeeld van een beleid dat u kunt maken voor het beheer van toegang tot opgegeven webtoepassingen.

Voorbeeld 1 Strikt webtoepassingsspecifiek beleid

In dit voorbeeld wordt een nieuw beleid gemaakt en toegepast op een gevoelige webtoepassing.



Sensitive Web Application
 To be applied to Web application that should have limited access.

Beleid verwijderen

Naam beleid*

Omschrijving

Van toepassing op

Selecteer de toepassingen uit de catalogus waarop dit beleid van toepassing is.

Apps bewerken

Beleidsregels

U kunt een lijst met regels maken voor toegang tot deze toepassingen. Selecteer voor elke regel het IP-netwerkbereik, het type apparaten waarmee toepassingen kunnen worden gebruikt, de methoden en verificatievolgorde, en het maximale aantal uren dat gebruikers de toepassing kunnen gebruiken voordat herverificatie nodig is.

Netwerkbereik	Apparaattype	Verificatiemethode	Herverificatie	Groepen	
Internal Network	Webbrowser	Probeer eerst: Kerberos en nog 1 back-up(s)...	8 uur/uren	Alle gebruikers	✗ +
ALLE BEREIKEN	Webbrowser	SecurID	4 uur/uren	Alle gebruikers	✗ +

Opslaan

Annuleren

- Om toegang te krijgen tot de service van buiten het bedrijfsnetwerk, moet de gebruiker zich aanmelden met RSA SecurID. De gebruiker meldt zich aan met een browser en heeft nu toegang tot de toepassingsportal voor een sessie van vier uur, zoals geboden door de standaardtoegangsregel.
- Na vier uur probeert de gebruiker een webtoepassing te starten waarop het beleid voor gevoelige webtoepassingen is toegepast.
- De service controleert de regels in het beleid en past het beleid toe met het netwerkbereik ALL RANGES, omdat de gebruikersaanvraag afkomstig is uit een webbrowser en uit het ALL RANGES-netwerkbereik.

De gebruiker heeft zich aangemeld met de RSA SecurID-verificatiemethode, maar de sessie is zojuist verlopen. De gebruiker wordt omgeleid, zodat deze zich opnieuw kan verifiëren. Dankzij de hernieuwde verificatie heeft de gebruiker opnieuw een sessie van vier uur en kan deze de toepassing starten. Tijdens de volgende vier uur kan de gebruiker doorgaan met het starten van de toepassing zonder dat deze zich opnieuw moet verifiëren.

Voorbeeld 2 Strikter webtoepassingsspecifiek beleid

Als u een striktere regel wilt toepassen op extra gevoelige webtoepassingen, kunt u na een uur hernieuwde verificatie met SecurID vereisen op elk willekeurig apparaat. Hieronder volgt een voorbeeld van hoe dit type toegangsbeleidsregels wordt geïmplementeerd.

- De gebruiker meldt zich van binnen het bedrijfsnetwerk aan met de wachtwoordverificatiemethode.

De gebruiker heeft nu acht uur lang toegang tot de toepassingsportal, zoals bepaald in Voorbeeld 1.

- 2 De gebruiker probeert onmiddellijk een webtoepassing te starten waarop de beleidsregel uit Voorbeeld 2 is toegepast. Hiervoor is RSA SecurID-verificatie vereist.
- 3 De gebruiker wordt omgeleid naar een identiteitsprovider die RSA SecurID-verificatie biedt.
- 4 Nadat de gebruiker zich heeft aangemeld, wordt de toepassing door de service gestart en wordt de verificatiegebeurtenis opgeslagen.

De gebruiker kan een uur lang doorgaan met het starten van deze toepassing, maar wordt na een uur gevraagd zich opnieuw te verifiëren, zoals bepaald in de beleidsregel.

Het toegangsbeleid voor gebruikers beheren

vRealize Automation wordt geleverd met een standaardtoegangsbeleid voor gebruikers dat u ongewijzigd kunt gebruiken of naar wens kunt bewerken voor het beheer van tenanttoegang tot toepassingen.

vRealize Automation wordt geleverd met standaardtoegangsbeleid voor gebruikers en u kunt geen nieuw beleid toevoegen. U kunt het bestaande beleid bewerken om regels toe te voegen.

Voorwaarden

- Selecteer of configureer de juiste identiteitsproviders voor uw implementatie. Zie [Een verbinding met een externe identiteitsprovider configureren](#).
- Configureer het juiste netwerkbereik voor uw implementatie. Zie [Een netwerkbereik toevoegen of bewerken](#).
- Configureer de juiste verificatiemethoden voor uw implementatie. Zie [Alternatieve producten voor gebruikersverificatie integreren in Beheer van directory's](#).
- Als u het standaardbeleid wilt bewerken (om gebruikerstoegang tot de service als geheel te beheren), moet u deze configureren voordat u specifiek beleid voor webtoepassingen maakt.
- Voeg webtoepassingen toe aan de catalogus. De webtoepassingen moeten op de pagina Catalogus worden weergegeven voordat u een beleid kunt toevoegen.
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > Beheer van directory's > Beleid**.
- 2 Klik op **Beleid bewerken** om een nieuw beleid toe te voegen.
- 3 Voeg een beleidsnaam en -beschrijving toe in de respectievelijke tekstvakken.
- 4 Klik in het gedeelte Van toepassing op op **Selecteren** en selecteer de webtoepassingen die aan dit beleid gekoppeld zijn op de pagina die wordt weergegeven.
- 5 Klik op **+** om een regel toe te voegen in het gedeelte Beleidsregels.

De pagina Een beleidsregel toevoegen wordt weergegeven.

- a Selecteer het netwerkbereik dat op deze regel moet worden toegepast.
- b Selecteer het type apparaat dat toegang heeft tot de webtoepassingen voor deze regel.

- c Selecteer de verificatiemethoden die moeten worden gebruikt in de volgorde waarin de methoden moeten worden toegepast.
- d Geef het aantal uur op dat een webtoepassingssessie geopend moet blijven.
- e Klik op **Opslaan**.

6 Configureer naar wens aanvullende regels.

7 Klik op **Opslaan**.

Aanvullende identiteitsproviderverbindingen configureren

U kunt indien nodig aanvullende identiteitsproviderverbindingen configureren voor de ondersteuning van andere identiteitsbeheerscenario's, waaronder aanvullende ingebouwde identiteitsproviders en externe identiteitsproviders.

U kunt drie soorten identiteitsproviderverbindingen maken met Beheer van directory's.

- Externe IdP maken - Gebruik dit item om een verbinding met een externe identiteitsprovider te maken. Zorg ervoor dat u over het volgende beschikt voordat u een externe identiteitsproviderinstantie toevoegt.
 - Controleer of de instanties van derden compatibel zijn met SAML 2.0 en of de service de instantie van derden kan bereiken.
 - Zorg dat u de vereiste metagegevensinformatie van derden hebt en deze kunt toevoegen wanneer u de identiteitsprovider configureert in de beheerconsole. De metagegevensinformatie die u verkrijgt uit de instantie van derden is de URL voor de metagegevens of zijn de volledige metagegevens zelf.
- Workspace-IdP maken - Wanneer u een connector inschakelt om gebruikers te verifiëren tijdens het configureren van Beheer van directory's, wordt een Workspace-IdP gemaakt aangezien de identiteitsprovider en wachtwoordverificatie zijn ingeschakeld. U kunt aanvullende Workspace-identiteitsproviders achter verschillende load balancers configureren.
- Ingebouwde IdP maken - Ingebouwde identiteitsproviders gebruiken de interne mechanismen voor Beheer van directory's om verificatie te ondersteunen. U kunt ingebouwde identiteitsproviders configureren om verificatiemethoden te gebruiken waarvoor het gebruik van een connector op locatie niet is vereist. Wanneer u de ingebouwde identiteitsprovider configureert, koppelt u de verificatiemethoden voor gebruik met de provider.
- [Een verbinding met een externe identiteitsprovider configureren](#)
vRealize Automation wordt geleverd met een standaardverbindingsinstantie voor een identiteitsprovider. Mogelijk willen gebruikers aanvullende verbindingen met de identiteitsprovider maken om just-in-time-gebruikersinrichting of andere aangepaste configuraties te ondersteunen.

- [Extra Workspace-identiteitsproviders configureren](#)

Bij het configureren van een connector voor Beheer van directory's om gebruikers te verifiëren, wordt een Workspace-IdP gemaakt en wordt wachtwoordverificatie ingeschakeld.

- [Verbinding met een ingebouwde identiteitsprovider configureren](#)

U kunt meerdere ingebouwde identiteitsproviders configureren en er verificatiemethoden aan koppelen.

Een verbinding met een externe identiteitsprovider configureren

vRealize Automation wordt geleverd met een standaardverbindingsinstantie voor een identiteitsprovider. Mogelijk willen gebruikers aanvullende verbindingen met de identiteitsprovider maken om just-in-time-gebruikersinrichting of andere aangepaste configuraties te ondersteunen.

vRealize Automation wordt geleverd met een standaardidentiteitsprovider. In de meeste gevallen is de standaardprovider voldoende voor klantbehoeften. Als u een bestaande zakelijke oplossing voor identiteitsbeheer gebruikt, kunt u een aangepaste identiteitsprovider instellen om gebruikers door te verwijzen naar uw bestaande identiteitsoplossing.

Als u een aangepaste identiteitsprovider gebruikt, maakt Beheer van directory's gebruik van SAML-metagegevens van die provider om een vertrouwensrelatie tot stand te brengen met de provider. Nadat deze relatie tot stand is gebracht, koppelt Beheer van directory's de gebruikers van de SAML-bevestiging op basis van de onderwerpsnaam-id aan de lijst met interne vRealize Automation-gebruikers.

Voorwaarden

- Configureer het netwerkbereik dat u wilt doorverwijzen naar deze identiteitsproviderinstantie voor verificatie. Zie [Een netwerkbereik toevoegen of bewerken](#).
- Toegang tot het document met metagegevens van derden. Dit kan de URL naar de metagegevens zijn of kunnen de metagegevens zelf zijn.
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > Beheer van directory's > Identiteitsproviders**.

Op deze pagina worden alle geconfigureerde identiteitsproviders weergegeven.

- 2 Klik op **Identiteitsprovider toevoegen**.

Er wordt een menu weergegeven met opties voor de identiteitsprovider.

- 3 Selecteer **Externe IdP maken**.

4 Voer de juiste informatie in om de identiteitsprovider te configureren.

Optie	Beschrijving
Naam van identiteitsprovider	Voer een naam in voor deze identiteitsproviderinstantie.
SAML-metagegevens	<p>Voeg het IdPs XML-metagegevensdocument van derden toe om een vertrouwensrelatie tot stand te brengen met de identiteitsprovider.</p> <ol style="list-style-type: none"> 1 Voer de URL voor de SAML-metagegevens of de XML-inhoud in het tekstvak in. 2 Klik op IdP-metagegevens verwerken. De NameID-indelingen die worden ondersteund door de IdP worden geëxtraheerd uit de metagegevens en worden toegevoegd aan de tabel Naam-id-indeling. 3 Selecteer in de kolom Naam-id-waarde het gebruikerskenmerk in de service dat moet worden toegewezen aan de weergegeven id-indelingen. U kunt aangepaste indelingen voor de naam-id van derden toevoegen en toewijzen aan de waarden voor de gebruikerskenmerken in de service. 4 (Optioneel) Selecteer de stringindeling voor de NameIDPolicy-antwoord-id.
Gebruikers	Selecteer de Directories Management-directory's van de gebruikers die verificatie kunnen uitvoeren met deze identiteitsprovider.
Just-in-time-gebruikersinrichting	<p>Selecteer de betreffende opties om just-in-time-inrichting met een geschikte externe identiteitsprovider te ondersteunen.</p> <p>Voer de directorynaam in voor gebruik bij just-in-time-inrichting.</p> <p>Voer een of meer domeinen in die bestaan binnen de externe identiteitsprovider die u wilt gebruiken voor de just-in-time-inrichting.</p>
Netwerk	<p>De bestaande netwerkbereiken die zijn geconfigureerd in de service worden weergegeven.</p> <p>Selecteer de netwerkbereiken voor de gebruikers, op basis van hun IP-adressen, die u wilt doorverwijzen naar deze identiteitsproviderinstantie voor verificatie.</p>
Verificatiemethoden	Voeg de verificatiemethoden toe die worden ondersteund door de derde identiteitsprovider. Selecteer de contextklasse voor SAML-verificatie die de verificatiemethode ondersteunt.
SAML-handtekeningcertificaat	Klik op Metagegevens van serviceprovider (SP) om de URL weer te geven naar de metagegevens van de SAML-serviceprovider van Directories Management. Kopieer de URL en sla deze op. Deze URL wordt geconfigureerd wanneer u de SAML-bevestiging bewerkt in de identiteitsprovider van derden voor het toewijzen van Directories Management-gebruikers.
Hostnaam	Als het veld Hostnaam wordt weergegeven, voert u de hostnaam in waarnaar de identiteitsprovider voor verificatie wordt doorverwezen. Als u een niet-standaardpoort gebruikt die niet 443 is, kunt u dit instellen als Hostnaam:Poort. Bijvoorbeeld: myco.example.com:8443.

5 Klik op **Toevoegen**.

Wat nu te doen

- Kopieer de metagegevens van de Directories Management-serviceprovider die zijn vereist voor het configureren van de instantie van de identiteitsprovider van derden en sla deze op. Deze metagegevens zijn beschikbaar in het gedeelte SAML-handtekeningcertificaat van de pagina Identiteitsprovider.

- Voeg de verificatiemethode van de identiteitsprovider toe aan het standaardbeleid voor de services.

Zie de *Bronnen instellen in Directories Management*-handleiding voor informatie over het toevoegen en aanpassen van bronnen die u aan de catalogus toevoegt.

Extra Workspace-identiteitsproviders configureren

Bij het configureren van een connector voor Beheer van directory's om gebruikers te verifiëren, wordt een Workspace-IdP gemaakt en wordt wachtwoordverificatie ingeschakeld.

U kunt extra connectoren configureren om te functioneren achter meerdere load balancers. Wanneer in uw implementatie meerdere load balancers aanwezig zijn, kunt u extra Workspace-identiteitsproviders voor verificatie configureren in elke configuratie van een load balancer.

Procedure

- 1 Selecteer **Beheer > Beheer van directory's > Identiteitsproviders**.

Op deze pagina worden alle geconfigureerde identiteitsproviders weergegeven.

- 2 Klik op **Identiteitsprovider toevoegen**.

Er wordt een menu weergegeven met opties voor de identiteitsprovider.

- 3 Selecteer **Workspace-IdP maken**.

- 4 Voer de juiste informatie in om de identiteitsprovider te configureren.

Optie	Beschrijving
Naam van identiteitsprovider	Voer de naam van deze ingebouwde identiteitsproviderinstantie in.
Gebruikers	Selecteer de gebruikers die u wilt verifiëren. De geconfigureerde directory's worden weergegeven.
Gebruikers	Selecteer de groep van gebruikers die zich kunnen verifiëren met deze Workspace-identiteitsprovider.
Netwerk	De bestaande netwerkbereiken die zijn geconfigureerd in de service worden weergegeven. Selecteer het netwerkbereik voor de gebruikers op basis van de IP-adressen die u voor verificatie wilt omleiden naar deze identiteitsproviderinstantie.
Verificatiemethoden	<p>Verificatiemethoden die zijn geconfigureerd voor de service, worden weergegeven. Schakel het selectievakje in voor de verificatiemethoden die u wilt koppelen aan deze identiteitsprovider.</p> <p>Voor apparaatcompliance en wachtwoordverificatie met AirWatch en AirWatch Connector moet u ervoor zorgen dat de optie is ingeschakeld op de configuratiepagina van AirWatch.</p>

- 5 Klik op **Toevoegen**.

Verbinding met een ingebouwde identiteitsprovider configureren

U kunt meerdere ingebouwde identiteitsproviders configureren en er verificatiemethoden aan koppelen.

Voorwaarden

Als u ingebouwde Kerberos-verificatie gebruikt, downloadt u het KDC-uitgevercertificaat voor gebruik bij de AirWatch-configuratie van het iOS-apparaatbeheerprofiel.

Procedure

1 Selecteer **Beheer > Beheer van directory's > Identiteitsproviders**.

Op deze pagina worden alle geconfigureerde identiteitsproviders weergegeven.

2 Klik op **Identiteitsprovider toevoegen**.

Er wordt een menu weergegeven met opties voor de identiteitsprovider.

3 Selecteer **Ingebouwde IdP maken**.

4 Voer de juiste informatie in om de identiteitsprovider te configureren.

Optie	Beschrijving
Naam van identiteitsprovider	Voer de naam van deze ingebouwde identiteitsproviderinstantie in.
Gebruikers	Selecteer de gebruikers die u wilt verifiëren. De geconfigureerde directory's worden weergegeven.
Netwerk	De bestaande netwerkbereiken die zijn geconfigureerd in de service worden weergegeven. Selecteer het netwerkbereik voor de gebruikers op basis van de IP-adressen die u voor verificatie wilt omleiden naar deze identiteitsproviderinstantie.
Verificatiemethoden	De verificatiemethoden die zijn geconfigureerd voor de service, worden weergegeven. Schakel het selectievakje in voor de verificatiemethoden die u wilt koppelen aan deze identiteitsprovider. Voor apparaatcompliance en wachtwoordverificatie met AirWatch en AirWatch Connector moet u ervoor zorgen dat de juiste optie is ingeschakeld op de configuratiepagina van AirWatch.

5 Klik op **Toevoegen**.

Alternatieve producten voor gebruikersverificatie integreren in Beheer van directory's

Bij het initieel configureren van Beheer van directory's gebruikt u normaal gesproken de connectoren die worden geleverd bij de bestaande vRealize Automation-infrastructuur voor het maken van een Active Directory-verbinding voor verificatie op basis van een gebruikers-id en een wachtwoord en voor beheer. U kunt Beheer van directory's echter ook integreren met andere oplossingen voor verificatie zoals Kerberos of RSA SecurID.

De identiteitsproviderinstantie kan de Directories ManagementConnector-instantie, identiteitsproviderinstanties van derden of een combinatie van beide zijn.

De identiteitsproviderinstantie die u bij de Directories Management-service gebruikt, maakt een federatie-autoriteit in het netwerk die met de service communiceert door middel van SAML 2.0-stellingen.

Wanneer u de Directories Management-service voor de eerste keer implementeert, is de connector de eerste identiteitsprovider voor de service. Uw bestaande Active Directory-infrastructuur wordt gebruikt voor gebruikersverificatie en -beheer.

De volgende verificatiemethoden worden ondersteund. U configureert deze verificatiemethoden via de beheerdersconsole.

Tabel 2-8. Typen gebruikersverificatie die worden ondersteund door Beheer van directory's

Verificatietypen	Beschrijving
Wachtwoord (implementatie op locatie)	Zonder een configuratie nadat Active Directory is geconfigureerd, ondersteunt Directories Management Active Directory-wachtwoordverificatie. Deze methode verifieert gebruikers direct op Active Directory.
Kerberos voor desktops	Kerberos-verificatie biedt domeingebruikers met single sign-in toegang tot hun apps-portal. Gebruikers hoeven zich niet opnieuw aan te melden nadat ze zich hebben aangemeld bij het netwerk.
Certificaat (implementatie op locatie)	Op certificaat gebaseerde verificatie kan worden geconfigureerd om clients toe te staan verificatie uit te voeren met certificaten op hun desktop- en mobiele apparaten of om een smartcardadapter te gebruiken voor verificatie. Op certificaat gebaseerde verificatie is gebaseerd op wat de gebruiker heeft en wat de persoon kent. Een X.509-certificaat maakt gebruik van de infrastructuurstandaard met openbare sleutel om te controleren of een openbare sleutel in het certificaat aan de gebruiker toebehoort.
RSA SecurID (implementatie op locatie)	Als RSA SecurID-verificatie is geconfigureerd, is Directories Management geconfigureerd als de verificatieagent in de RSA SecurID-server. RSA SecurID-verificatie vereist dat gebruikers een tokengebaseerd verificatiesysteem gebruiken. RSA SecurID is een verificatiemethode voor gebruikers die toegang maken tot Directories Management buiten het bedrijfsnetwerk.
RADIUS (implementatie op locatie)	RADIUS-verificatie biedt tweeledige verificatieopties. U stelt de RADIUS-server in die toegankelijk is voor de Directories Management-service. Als gebruikers zich aanmelden met hun gebruikersnaam en wachtwoordcode, wordt een toegangsaanvraag naar de RADIUS-server verzonden voor verificatie.
RSA Adaptive Authentication (implementatie op locatie)	RSA-verificatie biedt een sterkere, meervoudige verificatie dan alleen de verificatie met gebruikersnaam en wachtwoord op Active Directory. Wanneer RSA Adaptive Authentication is ingeschakeld, worden de risico-indicatoren die worden vermeld in het risicobeleid ingesteld in de RSA-beleidsbeheertoepassing. De Directories Management-serviceconfiguratie van adaptieve verificatie wordt gebruikt om de vereiste verificatieprompts te bepalen.
Mobiele SSO (voor iOS)	Mobiele SSO voor iOS-verificatie wordt gebruikt voor single sign-on-verificatie voor door AirWatch beheerde iOS-apparaten. Mobiele SSO voor iOS-verificatie maakt gebruik van een Key Distribution Center (KDC) dat deel uitmaakt van de Directories Management-service. U moet de KDC-service starten in de VMware Identity Manager-service voordat u deze verificatiemethode inschakelt.

Tabel 2-8. Typen gebruikersverificatie die worden ondersteund door Beheer van directory's (vervolg)

Verificatietypen	Beschrijving
Mobiele SSO (voor Android)	Mobiele SSO voor Android-verificatie wordt gebruikt voor single sign-on-verificatie voor door AirWatch beheerde Android-apparaten. Er wordt een proxyservice ingesteld tussen de Directories Management-service en AirWatch om het certificaat op te halen via AirWatch voor de verificatie.
Wachtwoord (AirWatch-connector)	De AirWatch Cloud Connector kan worden geïntegreerd met de Directories Management-service voor gebruikerswachtwoordverificatie. U configureert de Directories Management-service om gebruikers in de AirWatch-map te synchroniseren.

Gebruikers worden geverifieerd op basis van de verificatiemethoden, de standaardregels in het toegangsbeleid, netwerkbereiken en de instantie van de identiteitsprovider die u configureert. Nadat de verificatiemethoden zijn geconfigureerd, maakt u toegangsbeleidsregels die de te gebruiken verificatiemethoden per apparaattypen opgeven.

- [SecurID configureren voor Directories Management](#)

Wanneer u een RSA SecurID-server configureert, moet u de informatie voor de Directories Management-service toevoegen als verificatieagent op de RSA SecurID-server en de RSA SecurID-servergegevens configureren voor de Directories Management-service.

- [RADIUS configureren voor Directories Management](#)

U kunt Directories Management zo configureren dat van gebruikers wordt vereist dat ze RADIUS-verificatie (Remote Authentication Dial-In User Service) gebruiken. U configureert de RADIUS-serverinformatie met de Directories Management-service.

- [Een certificaat- of smartcardadapter configureren voor gebruik met Beheer van directory's](#)

U kunt x509-certificaatverificatie configureren, zodat clients zich kunnen verifiëren met certificaten op hun bureaublad en mobiele apparaten of een smartcardadapter kunnen gebruiken voor verificatie. De certificaatverificatie wordt gebaseerd op wat de gebruiker heeft (de privésleutel of smartcard) en wat de persoon weet (het wachtwoord voor de privésleutel of de pincode van de smartcard). Een X.509-certificaat maakt gebruik van de PKI-standaard (Public Key Infrastructure) om te controleren of een openbare sleutel in het certificaat eigendom is van de gebruiker. Bij smartcardverificatie sluiten gebruikers de smartcard aan op de computer en voeren ze een pincode in.

- [Een identiteitsproviderinstantie van derden configureren voor verificatie van gebruikers](#)

U kunt een identiteitsprovider van derden configureren voor het verifiëren van gebruikers in de Directories Management-service.

- [Verificatiemethoden beheren die op gebruikers worden toegepast](#)

De Directories Management-service probeert gebruikers te verifiëren op basis van de verificatiemethoden, het standaardtoegangsbeleid, de netwerkbereiken en de identiteitsproviderinstanties die u configureert.

■ Kerberos configureren voor Directories Management

Kerberos-verificatie biedt gebruikers die zijn aangemeld bij het Active Directory-domein toegang tot hun appsportal zonder dat ze om aanvullende verificatiegegevens worden gevraagd. U moet Windows-verificatie inschakelen, zodat het Kerberos-protocol interacties kan beveiligen tussen de browser van gebruikers en de Directories Management-service. U hoeft Active Directory niet direct te configureren om Kerberos in uw implementatie te laten werken.

SecurID configureren voor Directories Management

Wanneer u een RSA SecurID-server configureert, moet u de informatie voor de Directories Management-service toevoegen als verificatieagent op de RSA SecurID-server en de RSA SecurID-servergegevens configureren voor de Directories Management-service.

Wanneer u SecurID configureert voor het leveren van aanvullende beveiliging, moet u controleren of het netwerk correct is geconfigureerd voor uw Directories Management-implementatie. Met name voor SecurID moet u nagaan of de juiste poort open staat, zodat SecurID gebruikers van buiten uw netwerk kan verifiëren.

Nadat u de installatiewizard voor de Directories Management- hebt uitgevoerd en de Active Directory-verbinding hebt geconfigureerd, beschikt u over de vereiste informatie voor het voorbereiden van de RSA SecurID-server. Nadat u de RSA SecurID-server hebt voorbereid voor Directories Management, schakelt u SecurID in de beheerconsole in.

■ De RSA SecurID-server voorbereiden

De RSA SecurID-server moet worden geconfigureerd met informatie over de Directories Management-appliance als de verificatieagent. De vereiste informatie bestaat uit de hostnaam en de IP-adressen voor netwerkinterfaces.

■ RSA SecurID-verificatie configureren

Nadat Beheer van directory's is geconfigureerd als verificatieagent op de RSA SecurID-server, moet u de RSA SecurID-configuratiegegevens toevoegen aan de connector.

De RSA SecurID-server voorbereiden

De RSA SecurID-server moet worden geconfigureerd met informatie over de Directories Management-appliance als de verificatieagent. De vereiste informatie bestaat uit de hostnaam en de IP-adressen voor netwerkinterfaces.

Voorwaarden

- Controleer of een van de volgende RSA Authentication Manager-versies is geïnstalleerd en werkt op het bedrijfsnetwerk: RSA AM 6.1.2, 7.1 SP2 en hoger en 8.0 en hoger. De Directories Management-server gebruikt AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51 (Agent API 8.1 SP1), dat alleen de voorafgaande versies van RSA Authentication Manager (de RSA SecurID-server) ondersteunt. Raadpleeg de RSA-documentatie voor meer informatie over het installeren en configureren van RSA Authentication Manager (RSA SecurID-server).

Procedure

- 1 Voeg de Directories Management Connector als verificatieagent toe op een ondersteunde versie van de RSA SecurID-server. Geef de volgende informatie op.

Optie	Beschrijving
Hostnaam	De hostnaam van Directories Management.
IP-adres	Het IP-adres van Directories Management.
Alternatief IP-adres	Als verkeer van de connector wordt doorgeleid door een NAT-apparaat (Network Address Translation) voordat het de RSA SecurID-server bereikt, voert u het privé IP-adres in van de appliance.

- 2 Download het gecomprimeerde configuratiebestand en extraheer het bestand `sdconf.rec`.
Dit bestand moet u later uploaden wanneer u RSA SecurID in Directories Management configureert.

Wat nu te doen

Ga naar de beheerconsole en selecteer de connector op de installatiepagina's van het tabblad Identiteits- en toegangsbeheer. Selecteer de connector en configureer SecurID op de pagina Verificatieadapter.

RSA SecurID-verificatie configureren

Nadat Beheer van directory's is geconfigureerd als verificatieagent op de RSA SecurID-server, moet u de RSA SecurID-configuratiegegevens toevoegen aan de connector.

Voorwaarden

- Controleer of de RSA Authentication Manager (de RSA SecurID-server) correct is geïnstalleerd en geconfigureerd.
- Download het gecomprimeerde bestand van de RSA SecurID-server en pak het serverconfiguratiebestand uit.

Procedure

- 1 Ga als tenantbeheerder naar **Beheer > Beheer van directory's > Connectoren**
- 2 Selecteer op de pagina Connectoren de koppeling Werker voor de connector die wordt geconfigureerd met RSA SecurID.
- 3 Klik op **Verificatieadapters** en klik vervolgens op **SecurID-IDP-adapter**.
U wordt omgeleid naar de aanmeldpagina van het identiteitsbeheer.
- 4 Klik op de pagina Verificatieadapters in de rij SecurID-IDP-adapter op **Bewerken**.
- 5 Configureer de pagina SecurID-verificatieadapter.

De informatie die wordt gebruikt en de bestanden die worden gegenereerd op de RSA SecurID-server, zijn vereist wanneer u de SecurID-pagina configureert.

Optie	Actie
Naam	Een naam is vereist. De standaardnaam is SecurID-IDP-adapter. U kunt dit wijzigen.
SecurID inschakelen	Schakel dit vakje in om SecurID-verificatie in te schakelen.
Aantal toegestane verificatiepogingen	Voer het maximum aantal mislukte aanmeldingspogingen in bij het gebruik van het RSA SecurID-token. De standaardwaarde is vijf pogingen.
Connectoradres	Voer het IP-adres van de connectorinstantie in. De waarde die u invoert, moet overeenkomen met de waarde die u hebt gebruikt toen u de connectortoepassing als verificatieagent hebt toegevoegd aan de RSA SecurID-server. Als voor uw SecurID-server een waarde is toegewezen aan de prompt Alternatief IP-adres, dan voert u deze waarde in als het IP-adres van de connector. Als er geen alternatief IP-adres is toegewezen, voert u de waarde in die is toegewezen aan de prompt IP-adres.
Agent-IP-adres	Voer de waarde in die is toegewezen aan de prompt IP-adres in de RSA SecurID-server.
Serverconfiguratie	Upload het RSA SecurID-serverconfiguratiebestand. Eerst moet u het gecomprimeerde bestand downloaden van de RSA SecurID-server en het serverconfiguratiebestand, dat standaard <code>sdconf.rec</code> wordt genoemd, uitpakken.
Knooppuntgeheim	Als u het veld voor het knooppuntgeheim leeg laat, kan het knooppuntgeheim automatisch worden gegenereerd. Wij raden u aan het knooppuntgeheimbestand op de RSA SecurID-server te wissen en het knooppuntgeheimbestand niet opzettelijk te uploaden. Zorg ervoor dat het knooppuntgeheimbestand op de RSA SecurID-server en op de serverconnectorinstantie altijd overeenkomen. Als u het knooppuntgeheim op één locatie wijzigt, moet u dit ook op de andere locatie wijzigen.

6 Klik op **Opslaan**.

Wat nu te doen

Voeg de verificatiemethode toe aan het standaardtoegangsbeleid. Ga naar **Beheer > Beheer van directory's > Beleid** en klik op **Standaardbeleid bewerken**, zodat u de standaardbeleidsregels kunt bewerken en de SecurID-verificatiemethode in de correcte verificatievolgorde kunt toevoegen aan de regel.

RADIUS configureren voor Directories Management

U kunt Directories Management zo configureren dat van gebruikers wordt vereist dat ze RADIUS-verificatie (Remote Authentication Dial-In User Service) gebruiken. U configureert de RADIUS-serverinformatie met de Directories Management-service.

RADIUS-ondersteunt een groot aantal alternatieve opties voor tweeledige op tokens gebaseerde verificatie. Omdat tweeledige verificatieoplossingen als RADIUS werken met verificatiebeheerders die op afzonderlijke servers geïnstalleerd zijn, moet u de RADIUS-server configureren en toegankelijk maken voor de identiteitsbeheerservice.

Wanneer gebruikers zich aanmelden bij hun My Apps-portal en RADIUS-verificatie ingeschakeld is, wordt een speciaal aanmeldingsdialoogvenster weergegeven. Gebruikers voeren hun gebruikersnaam en wachtwoord voor RADIUS-verificatie in dit dialoogvenster in. Als de RADIUS-server antwoordt met een toegangscontrole, wordt door de identiteitsbeheerservice een dialoogvenster weergegeven waarin om een tweede wachtwoordcode wordt gevraagd. Ondersteuning voor RADIUS-toegangscontrole is momenteel beperkt tot het vragen om tekstinput.

Nadat een gebruiker verificatiegegevens heeft opgegeven in het dialoogvenster kan de RADIUS-server een sms-bericht, een e-mail of een tekst met behulp van een ander out-of-band-mechanisme sturen naar de mobiele telefoon van de gebruiker met een code. De gebruiker kan deze tekst en code in het aanmeldingsdialoogvenster invoeren om de verificatie te voltooien.

Als de RADIUS-server de mogelijkheid biedt om gebruikers uit Active Directory te importeren, kan eindgebruikers worden gevraagd om Active Directory-verificatiegegevens op te geven voordat ze worden gevraagd om de gebruikersnaam en de wachtwoordcode voor RADIUS-verificatie.

De RADIUS-server voorbereiden

Stel de RADIUS-server in en configureer deze voor het accepteren van RADIUS-aanvragen van de Directories Management-service.

Raadpleeg de installatiehandleidingen van uw RADIUS-leverancier voor informatie over het instellen van de RADIUS-server. Schrijf de RADIUS-configuratiegegevens op, omdat u deze informatie gebruikt bij het configureren van RADIUS in de service. Zie [RADIUS-verificatie configureren in Beheer van directory's](#) als u het type RADIUS-informatie wilt bekijken dat is vereist voor het configureren van Directories Management.

U kunt een secundaire RADIUS-verificatieserver instellen die moet worden gebruikt voor het leveren van hoge beschikbaarheid. Als de primaire RADIUS-server niet reageert binnen de servertime-out die is geconfigureerd voor RADIUS-verificatie, wordt de aanvraag omgeleid naar de secundaire server. Als de primaire server niet reageert, ontvangt de secundaire server alle toekomstige verificatieaanvragen.

RADIUS-verificatie configureren in Beheer van directory's

U schakelt de RADIUS-software in op een verificatiebeheerserver. Voor RADIUS-verificatie volgt u de configuratiedocumentatie van de leverancier.

Voorwaarden

Installeer en configureer de RADIUS-software op een verificatieserver. Voor RADIUS-verificatie volgt u de configuratiedocumentatie van de leverancier.

U moet de volgende RADIUS-serverinformatie kennen om RADIUS op de service te configureren.

- IP-adres of DNS-naam van de RADIUS-server.
- Verificatiepoortnummers. De verificatiepoort is doorgaans 1812.
- Verificatietype. De verificatietypen omvatten PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP1, MSCHAP2 (Microsoft Challenge Handshake Authentication Protocol, versies 1 en 2).

- RADIUS gedeeld geheim dat wordt gebruikt voor versleuteling en ontsleuteling in RADIUS-protocolberichten.
- Specifieke time-out- en pogingswaarden zijn vereist voor RADIUS-verificatie.
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > Beheer van directory's > Connectoren**.
- 2 Selecteer op de pagina Connectoren de koppeling Werker voor de connector die wordt geconfigureerd voor RADIUS-verificatie.
- 3 Klik op **Verificatieadapters** en klik vervolgens op **RADIUS-verificatieadapter**.
U wordt omgeleid naar de aanmeldpagina van het identiteitsbeheer.
- 4 Klik op **Bewerken** om deze velden te configureren op de pagina Verificatieadapter.

Optie	Actie
Naam	Een naam is vereist. De standaardnaam is RADIUS-verificatieadapter. U kunt dit wijzigen.
RADIUS-adapter inschakelen	Schakel dit vakje in om RADIUS-verificatie in te schakelen.
Aantal toegestane verificatiepogingen	Voer het maximum aantal mislukte aanmeldingspogingen in bij het gebruik van RADIUS bij de aanmelding. De standaardwaarde is vijf pogingen.
Aantal pogingen voor RADIUS-server	Geef het totale aantal nieuwe pogingen op. Als de primaire server niet reageert, wacht de service gedurende de geconfigureerde tijd voordat een nieuwe poging wordt gedaan.
Hostnaam/adres van RADIUS-server	Voer de hostnaam of het IP-adres van de RADIUS-server in.
Verificatiepoort	Voer het RADIUS-verificatiepoortnummer in. Dit is doorgaans 1812.
Accountingpoort	Voer 0 in voor het poortnummer. De accountingpoort wordt op dit ogenblik niet gebruikt.
Verificatietype	Voer het verificatieprotocol in dat door de RADIUS-server wordt ondersteund. PAP, CHAP, MSCHAP1, of MSCHAP2.
Gedeeld geheim	Voer het gedeeld geheim in dat wordt gebruikt tussen de RADIUS-server en de VMware Identity Manager-service.
Servertime-out in seconden	Voer de RADIUS-servertime-out in seconden in, waarna een nieuwe poging wordt verzonden als de RADIUS-server niet reageert.

Optie	Actie
Voorvoegsel van realm	(Optioneel) De gebruikersaccountlocatie wordt de realm genoemd. Als u een tekenreeks voor het realmvoorvoegsel opgeeft, wordt de tekenreeks aan het begin van de gebruikersnaam geplaatst wanneer de naam naar de RADIUS-server wordt verzonden. Als de gebruikersnaam bijvoorbeeld wordt ingevoerd als jdoe en het realmvoorvoegsel DOMAIN-A\ wordt opgegeven, dan wordt de gebruikersnaam DOMAIN-A\jdoe naar de RADIUS-server verzonden. Als u deze velden niet configureert, dan wordt alleen de ingevoerde gebruikersnaam verzonden.
Achtervoegsel van realm	(Optioneel) Als u een realmachtervoegsel opgeeft, wordt de tekenreeks aan het einde van de gebruikersnaam geplaatst. Als het achtervoegsel bijvoorbeeld @myco.com is, dan wordt de gebruikersnaam jdoe@myco.com naar de RADIUS-server verzonden.
Hint voor wachtwoord zin van aanmeldpagina	Voer de teksttekenreeks in die moet worden weergegeven in het bericht op de gebruikersaanmeldpagina om gebruikers te vragen de juiste RADIUS-wachtwoordcode in te voeren. Als dit veld bijvoorbeeld is geconfigureerd met Eerst AD-wachtwoord en vervolgens SMS-wachtwoordcode , dan bevat het bericht op de aanmeldpagina Voer eerst uw AD-wachtwoord in en vervolgens de SMS-wachtwoordcode . De standaard teksttekenreeks is RADIUS-wachtwoordcode .

5 U kunt een secundaire RADIUS-server voor hoge beschikbaarheid inschakelen.

Configureer de secundaire server zoals beschreven in stap 4.

6 Klik op **Opslaan**.

Wat nu te doen

Voeg de RADIUS-verificatiemethode toe aan het standaardtoegangsbeleid. Selecteer **Beheer > Beheer van directory's > Beleid** en klik op **Standaardbeleid bewerken**, zodat u de standaardbeleidsregels kunt bewerken en de RADIUS-verificatiemethode in de correcte verificatievolgorde kunt toevoegen aan de regel.

Een certificaat- of smartcardadapter configureren voor gebruik met Beheer van directory's

U kunt x509-certificaatverificatie configureren, zodat clients zich kunnen verifiëren met certificaten op hun bureaublad en mobiele apparaten of een smartcardadapter kunnen gebruiken voor verificatie. De certificaatverificatie wordt gebaseerd op wat de gebruiker heeft (de privésleutel of smartcard) en wat de persoon weet (het wachtwoord voor de privésleutel of de pincode van de smartcard). Een X.509-certificaat maakt gebruik van de PKI-standaard (Public Key Infrastructure) om te controleren of een openbare sleutel in het certificaat eigendom is van de gebruiker. Bij smartcardverificatie sluiten gebruikers de smartcard aan op de computer en voeren ze een pincode in.

De smartcardcertificaten worden gekopieerd naar het lokale certificaatarchief op de computer van de gebruiker. De certificaten in het lokale certificaatarchief zijn beschikbaar voor alle browsers die op de computer van deze gebruiker draaien, met enkele uitzonderingen.

Opmerking Wanneer certificaatverificatie is geconfigureerd en de servicetoepassing is ingesteld achter een load balancer, moet u zich ervan verzekeren dat in de configuratie van de connector SSL pass-through bij de load balancer is opgenomen, en niet het beëindigen van SSL bij de load balancer. Deze configuratie zorgt ervoor dat de SSL-handdruk plaatsvindt tussen de connector en de client om het certificaat door te geven aan de connector. U kunt extra connectoren configureren achter een andere load balancer die is geconfigureerd met SSL-passthrough en certificaatverificatie op deze connectoren inschakelen en configureren.

User Principal Name gebruiken voor certificaatverificatie

U kunt certificaattoewijzing gebruiken in Active Directory. Aanmeldingen met een certificaat en smartcard gebruiken de UPN (User Principal Name) uit de Active Directory om gebruikersaccounts te valideren. De Active Directory-accounts van gebruikers die verificatie proberen uit te voeren in de Directories Management-service, moeten een geldige UPN hebben die overeenkomt met de UPN in het certificaat.

U kunt de Directories Management- configureren zodat een e-mailadres wordt gebruikt voor het valideren van het gebruikersaccount als de UPN niet bestaat in het certificaat.

U kunt ook een alternatief UPN-type inschakelen dat moet worden gebruikt.

Certificeringsinstantie vereist voor verificatie

Als u aanmelden via certificaatverificatie wilt toestaan, moeten basis- en tussencertificaten worden geüpload naar de Directories Management-.

De certificaten worden gekopieerd naar het lokale certificaatarchief op de computer van de gebruiker. De certificaten in het lokale certificaatarchief zijn beschikbaar voor alle browsers die actief zijn op de computer van deze gebruiker, met enkele uitzonderingen, en zijn daarom beschikbaar voor een Directories Management-instantie in de browser.

Voor smartcardverificatie verzendt de Directories Management-service een lijst met vertrouwde certificeringsinstanties (CA of Certificate Authority) naar de browser wanneer een gebruiker een verbinding initieert met de Directories Management-instantie. De browser vergelijkt de lijst met vertrouwde CA's met de beschikbare gebruikerscertificaten, selecteert een geschikt certificaat en vraagt de gebruiker de pincode voor een smartcard in te voeren. Als er meerdere geldige gebruikerscertificaten beschikbaar zijn, wordt de gebruiker gevraagd een certificaat te selecteren.

Als een gebruiker geen verificatie kan uitvoeren, zijn de basis-CA en de tussenliggende CA mogelijk niet correct ingesteld. Het kan ook zijn dat de service niet opnieuw is opgestart nadat de basis- en tussenliggende CA's naar de server zijn geüpload. In deze gevallen kan de browser de geïnstalleerde certificaten niet weergeven, kan de gebruiker geen correct certificaat selecteren en mislukt de certificaatverificatie.

Certificaatintrekkingscontrole gebruiken

U kunt certificaatintrekkingscontrole configureren om te voorkomen dat gebruikers waarvan de gebruikerscertificaten zijn ingetrokken, verificatie kunnen uitvoeren. Certificaten worden vaak

ingetrokken wanneer een gebruiker een organisatie verlaat, een smartcard verliest of van de ene naar de andere afdeling verhuist.

Certificaatintrekkingscontrole met certificaatintrekkingslijsten (CRL's) en met het Online Certificate Status Protocol (OCSP) wordt ondersteund. Een CRL is een lijst met ingetrokken certificaten die gepubliceerd wordt door de certificeringsinstantie die de certificaten heeft uitgegeven. OCSP is een certificaatvalidatieprotocol dat wordt gebruikt om de intrekkingsstatus van een certificaat te verkrijgen.

U kunt certificaatintrekkingscontrole configureren op de pagina Connectoren > Verificatieadapters > Certificaatverificatieadapter van de beheerconsole wanneer u certificaatverificatie configureert.

U kunt zowel CRL als OCSP configureren in dezelfde configuratie van de certificaatverificatieadapter. Wanneer u beide typen van certificaatintrekking configureert en het selectievakje CRL gebruiken als OCSP mislukt is ingeschakeld, wordt OCSP eerst ingeschakeld. Als OCSP mislukt, valt de intrekkingscontrole terug op CRL. Intrekkingscontrole valt niet terug op OCSP als CRL mislukt.

Aanmelden met CRL-controle

Als u certificaatintrekking inschakelt, dan gebruikt de Directories Management-server een CRL om de intrekkingsstatus van een gebruikerscertificaat te bepalen.

Als een certificaat wordt ingetrokken, mislukt de verificatie via het certificaat.

Aanmelden met OCSP-certificaatcontrole

Als u OCSP-intrekkingscontrole configureert, dan verzendt Directories Management een aanvraag naar een OCSP-responder om de intrekkingsstatus van een specifiek gebruikerscertificaat te bepalen. De Directories Management-server gebruikt het OCSP-handtekeningcertificaat om te controleren of de antwoorden die van de OCSP-responder worden ontvangen, authentiek zijn.

Als het certificaat is ingetrokken, mislukt de verificatie.

U kunt de verificatie configureren zodat deze terugvalt op CRL-controle als deze geen antwoord van de OCSP-responder ontvangt of als het antwoord ongeldig is.

Certificaatverificatie configureren voor Beheer van directory's

U activeert en configureert verificatie via een certificaat via de functie Beheer van directory's van de vRealize Automation-beheerconsole.

Opmerking Een systeembeheerder moet een externe connector voor uw vRealize Automation-implementatie configureren als u externe identiteitsproviders zoals Keberos of smartcardverificatie gebruikt.

Voorwaarden

- Haal het basiscertificaat en de tussencertificaten op van de certificeringsinstantie die de certificaten die door uw gebruikers worden voorgesteld, heeft ondertekend.

- (Optioneel) Lijst met object-id's (OID's) van geldige certificaatbeleidsregels voor certificaatverificatie.
- Voor intrekingscontrole, de bestandslocatie van de CRL, de URL van de OCSP-server.
- (Optioneel) Bestandslocatie van handtekeningcertificaat van OCSP-antwoord.
- Inhoud van toestemmingsformulier bij het inschakelen van een toestemmingsformulier voor weergave vóór de verificatie.

Procedure

- 1 Ga als tenantbeheerder naar **Beheer > Beheer van directory's > Connectoren**
- 2 Selecteer op de pagina Connectoren de koppeling Werker voor de connector die wordt geconfigureerd.
- 3 Klik op **Verificatieadapters** en klik vervolgens op **Certificaatverificatieadapter**.
U wordt omgeleid naar de aanmeldpagina van het identiteitsbeheer.
- 4 Klik in de rij Certificaatverificatieadapter op **Bewerken**.
- 5 Configureer de pagina Certificaatverificatieadapter.

Opmerking Een sterretje geeft aan dat dit veld moet worden ingevuld. Alle overige velden zijn optioneel.

Optie	Beschrijving
*Naam	Een naam is vereist. De standaardnaam is Certificaatverificatieadapter. U kunt deze naam wijzigen.
Certificaatadapter inschakelen	Schakel het selectievakje in om certificaatverificatie in te schakelen.
*Basis- en tussen-CA-certificaten	Selecteer de certificaatbestanden die moeten worden geüpload. U kunt meerdere basis-CA-certificaten en tussen-CA-certificaten die gecodeerd zijn als DER of PEM, selecteren.
Geüploade CA-certificaten	<p>De geüploade certificaatbestanden worden weergegeven in de sectie Geüploade CA-certificaten van het formulier.</p> <p>U moet de service opnieuw opstarten om de nieuwe certificaten beschikbaar te maken.</p> <p>Klik op Web Service opnieuw opstarten om de service opnieuw op te starten en de certificaten aan de vertrouwde service toe te voegen.</p> <p>Opmerking Door de service opnieuw op te starten, wordt de certificaatverificatie niet ingeschakeld. Nadat de service opnieuw is opgestart, gaat u verder met de configuratie van deze pagina. Door aan het einde van de pagina op Opslaan te klikken, wordt de certificaatverificatie op de service ingeschakeld.</p>
E-mail gebruiken als certificaat geen UPN bevat	Als de User Principal Name (UPN) niet bestaat in het certificaat, schakelt u dit selectievakje in om het kenmerk E-mailadres te gebruiken als de extensie van de Alternatieve naam voor onderwerp om gebruikersaccounts te valideren.

Optie	Beschrijving
Certificaatbeleid geaccepteerd	Maak een lijst met object-id's die worden geaccepteerd in de certificaatbeleidextensies. Voer de object-id's (OID's) in voor het certificaatuitgiftebeleid. Klik op Waarde toevoegen om aanvullende OID's toe te voegen.
Certificaatintrekking inschakelen	Schakel het selectievakje in om certificaatintrekkingscontrole in te schakelen. Dit voorkomt dat gebruikers waarvan de gebruikerscertificaten zijn ingetrokken, verificatie kunnen uitvoeren.
CRL van certificaten gebruiken	Schakel het selectievakje in om de certificaatintrekkingslijst (CRL) te gebruiken die werd gepubliceerd door de certificeringsinstantie die de certificaten heeft uitgegeven om de status van een certificaat (ingetrokken of niet-ingetrokken) te valideren.
Locatie van CRL	Voer het serverbestandspad of het lokale bestandspad in waarvan de CRL moet worden opgehaald.
OCSP-intrekking inschakelen	Schakel het selectievakje in om het certificaatvalidatieprotocol Online Certificate Status Protocol (OCSP) te gebruiken om de intrekkingstatus van een certificaat op te halen.
CRL gebruiken als OCSP mislukt	Als u zowel CRL als OCSP configureert, kunt u dit vakje inschakelen om terug te vallen op CRL als de OCSP-controle niet beschikbaar is.
OCSP-nonce verzenden	Schakel dit selectievakje in als u wilt dat de unieke id van de OCSP-aanvraag in het antwoord wordt verzonden.
OCSP URL	Als u OCSP-intrekking inschakelt, voert u het OCSP-serveradres voor intrekkingscontrole in.
Handtekeningcertificaat van OCSP-responder	Voer het pad in naar het OCSP-certificaat voor de responder, <i>/path/to/file.cer</i> .
Toestemmingsformulier inschakelen vóór verificatie	Schakel dit selectievakje in om een pagina met een toestemmingsformulier te laten weergeven voordat gebruikers zich bij het portaal Mijn apps aanmelden met behulp van certificaatverificatie.
Inhoud van toestemmingsformulier	Typ in dit tekstvak de tekst die in het toestemmingsformulier moet worden weergegeven.

6 Klik op **Opslaan**.

Wat nu te doen

- Voeg de verificatiemethode via een certificaat toe aan het standaardtoegangsbeleid. Ga naar **Beheer > Beheer van directory's > Beleid** en klik op **Standaardbeleid bewerken** om de standaardbeleidsregels te bewerken, Certificaat toe te voegen en dit de eerste verificatiemethode te maken voor het standaardbeleid. Certificaat moet de eerste verificatiemethode zijn die in de beleidsregel wordt weergegeven. Anders mislukt certificaatverificatie.

- Als Certificaatverificatie is geconfigureerd en de servertoepassing wordt ingesteld achter een load balancer, dan zorgt u ervoor dat de Directories ManagementConnector is geconfigureerd met SSL-passthrough op de load balancer en dat deze niet is geconfigureerd om SSL op de load balancer te beëindigen. Deze configuratie zorgt ervoor dat de SSL-handshake plaatsvindt tussen de connector en de client om het certificaat door te geven naar de connector.

Een identiteitsproviderinstantie van derden configureren voor verificatie van gebruikers

U kunt een identiteitsprovider van derden configureren voor het verifiëren van gebruikers in de Directories Management-service.

Voer de volgende taken uit voordat u de beheerconsole gebruikt voor het toevoegen van de identiteitsproviderinstantie van derden.

- Controleer of de instanties van derden compatibel zijn met SAML 2.0 en of de service de instantie van derden kan bereiken.
- Zorg dat u de vereiste metagegevensinformatie van derden hebt en deze kunt toevoegen wanneer u de identiteitsprovider configureert in de beheerconsole. De metagegevensinformatie die u verkrijgt uit de instantie van derden is de URL voor de metagegevens of zijn de volledige metagegevens zelf.

Een verbinding met een externe identiteitsprovider configureren

vRealize Automation wordt geleverd met een standaardverbindinginstantie voor een identiteitsprovider. Mogelijk willen gebruikers aanvullende verbindingen met de identiteitsprovider maken om just-in-time-gebruikersinrichting of andere aangepaste configuraties te ondersteunen.

vRealize Automation wordt geleverd met een standaardidentiteitsprovider. In de meeste gevallen is de standaardprovider voldoende voor klantbehoeften. Als u een bestaande zakelijke oplossing voor identiteitsbeheer gebruikt, kunt u een aangepaste identiteitsprovider instellen om gebruikers door te verwijzen naar uw bestaande identiteitsoplossing.

Als u een aangepaste identiteitsprovider gebruikt, maakt Beheer van directory's gebruik van SAML-metagegevens van die provider om een vertrouwensrelatie tot stand te brengen met de provider. Nadat deze relatie tot stand is gebracht, koppelt Beheer van directory's de gebruikers van de SAML-bevestiging op basis van de onderwerpsnaam-id aan de lijst met interne vRealize Automation-gebruikers.

Voorwaarden

- Configureer het netwerkbereik dat u wilt doorverwijzen naar deze identiteitsproviderinstantie voor verificatie. Zie [Een netwerkbereik toevoegen of bewerken](#).
- Toegang tot het document met metagegevens van derden. Dit kan de URL naar de metagegevens zijn of kunnen de metagegevens zelf zijn.
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

1 Selecteer **Beheer > Beheer van directory's > Identiteitsproviders**.

Op deze pagina worden alle geconfigureerde identiteitsproviders weergegeven.

2 Klik op **Identiteitsprovider toevoegen**.

Er wordt een menu weergegeven met opties voor de identiteitsprovider.

3 Selecteer **Externe IdP maken**.

4 Voer de juiste informatie in om de identiteitsprovider te configureren.

Optie	Beschrijving
Naam van identiteitsprovider	Voer een naam in voor deze identiteitsproviderinstantie.
SAML-metagegevens	<p>Voeg het IdPs XML-metagegevensdocument van derden toe om een vertrouwensrelatie tot stand te brengen met de identiteitsprovider.</p> <ol style="list-style-type: none"> Voer de URL voor de SAML-metagegevens of de XML-inhoud in het tekstvak in. Klik op IdP-metagegevens verwerken. De NameID-indelingen die worden ondersteund door de IdP worden geëxtraheerd uit de metagegevens en worden toegevoegd aan de tabel Naam-id-indeling. Selecteer in de kolom Naam-id-waarde het gebruikerskenmerk in de service dat moet worden toegewezen aan de weergegeven id-indelingen. U kunt aangepaste indelingen voor de naam-id van derden toevoegen en toewijzen aan de waarden voor de gebruikerskenmerken in de service. (Optioneel) Selecteer de stringindeling voor de NameIDPolicy-antwoord-id.
Gebruikers	Selecteer de Directories Management-directory's van de gebruikers die verificatie kunnen uitvoeren met deze identiteitsprovider.
Just-in-time-gebruikersinrichting	<p>Selecteer de betreffende opties om just-in-time-inrichting met een geschikte externe identiteitsprovider te ondersteunen.</p> <p>Voer de directorynaam in voor gebruik bij just-in-time-inrichting.</p> <p>Voer een of meer domeinen in die bestaan binnen de externe identiteitsprovider die u wilt gebruiken voor de just-in-time-inrichting.</p>
Netwerk	<p>De bestaande netwerkbereiken die zijn geconfigureerd in de service worden weergegeven.</p> <p>Selecteer de netwerkbereiken voor de gebruikers, op basis van hun IP-adressen, die u wilt doorverwijzen naar deze identiteitsproviderinstantie voor verificatie.</p>
Verificatiemethoden	Voeg de verificatiemethoden toe die worden ondersteund door de derde identiteitsprovider. Selecteer de contextklasse voor SAML-verificatie die de verificatiemethode ondersteunt.

Optie	Beschrijving
SAML-handtekeningcertificaat	Klik op Metagegevens van serviceprovider (SP) om de URL weer te geven naar de metagegevens van de SAML-serviceprovider van Directories Management. Kopieer de URL en sla deze op. Deze URL wordt geconfigureerd wanneer u de SAML-bevestiging bewerkt in de identiteitsprovider van derden voor het toewijzen van Directories Management-gebruikers.
Hostnaam	Als het veld Hostnaam wordt weergegeven, voert u de hostnaam in waarnaar de identiteitsprovider voor verificatie wordt doorverwezen. Als u een niet-standaardpoort gebruikt die niet 443 is, kunt u dit instellen als Hostnaam:Poort. Bijvoorbeeld: myco.example.com:8443.

5 Klik op **Toevoegen**.

Wat nu te doen

- Kopieer de metagegevens van de Directories Management-serviceprovider die zijn vereist voor het configureren van de instantie van de identiteitsprovider van derden en sla deze op. Deze metagegevens zijn beschikbaar in het gedeelte SAML-handtekeningcertificaat van de pagina Identiteitsprovider.
- Voeg de verificatiemethode van de identiteitsprovider toe aan het standaardbeleid voor de services.

Zie de *Bronnen instellen in Directories Management*-handleiding voor informatie over het toevoegen en aanpassen van bronnen die u aan de catalogus toevoegt.

Verificatiemethoden beheren die op gebruikers worden toegepast

De Directories Management-service probeert gebruikers te verifiëren op basis van de verificatiemethoden, het standaardtoegangsbeleid, de netwerkbereiken en de identiteitsproviderinstanties die u configureert.

Wanneer gebruikers zich proberen aan te melden, evalueert de service de regels van het standaardtoegangsbeleid om de beleidsregel te selecteren die moet worden toegepast. De verificatiemethoden worden toegepast in de volgorde waarin ze in de regel worden weergegeven. De eerste identiteitsproviderinstantie die aan de vereisten van de regel voor de verificatiemethode en het netwerkbereik voldoet, wordt geselecteerd en de aanvraag voor gebruikersverificatie wordt doorgestuurd naar de identiteitsproviderinstantie voor verificatie. Als de verificatie mislukt, wordt de volgende verificatiemethode die in de regel is geconfigureerd, toegepast.

U kunt regels toevoegen die de te gebruiken verificatiemethodes opgeven per apparaattype of per apparaattype en afkomstig uit een bepaald netwerkbereik. U kunt bijvoorbeeld een regel configureren waarmee gebruikers die zich met iOS-apparaten via een bepaald netwerk aanmelden, verplicht zijn zichzelf te verifiëren met behulp van RSA SecurID, en een andere regel waarmee alle apparaattypen die worden aangemeld via het interne netwerk-IP-adres moeten worden geverifieerd met behulp van hun wachtwoord.

Een netwerkbereik toevoegen of bewerken

U kunt de netwerkbereiken beheren door de IP-adressen op te geven waarmee gebruikers zich via een Active Directory-verbinding kunnen aanmelden. U kunt de netwerkbereiken die u maakt toevoegen aan specifieke instanties van de netwerkproviders en aan de regels van het toegangsbeleid.

Definieer netwerkbereiken voor uw Directories Management-implementatie op basis van uw netwerktopologie.

Eén netwerkbereik, met de naam ALL RANGES, wordt als standaardbereik gemaakt. Dit netwerkbereik omvat elk IP-adres dat op internet beschikbaar is, van 0.0.0.0 tot en met 255.255.255.255. Zelfs als uw implementatie maar één netwerkproviderinstantie heeft, kunt u het IP-adresbereik wijzigen en andere bereiken toevoegen, met als doel het uitsluiten of toevoegen van specifieke IP-adressen van of aan het standaardnetwerkbereik. U kunt andere netwerkbereiken maken met specifieke IP-adressen die u voor een bepaald doeleinde kunt toepassen.

Opmerking Het standaardnetwerkbereik, ALL RANGES, en de beschrijving hiervan, 'een netwerk voor alle bereiken', kunt u bewerken. U kunt de naam en beschrijving wijzigen en hiervoor zelfs een andere taal gebruiken, door op de naam van het netwerkbereik te klikken op de pagina Netwerkbereiken.

Voorwaarden

- U hebt tenants voor uw vRealize Automation-implementatie geconfigureerd en een geschikte Active Directory-verbinding ingesteld ter ondersteuning van Active Directory-verificatie van gebruikers-id's en wachtwoorden.
- Active Directory is geïnstalleerd en geconfigureerd voor gebruik op uw netwerk.
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > Beheer van directory's > Netwerkbereiken**.
- 2 Bewerk een bestaand netwerkbereik of voeg een nieuw netwerkbereik toe.

Optie	Beschrijving
Een bestaand bereik bewerken	Klik op de naam van het netwerkbereik dat u wilt bewerken.
Een bereik toevoegen	Klik op Netwerkbereik toevoegen om een nieuw bereik toe te voegen.

- 3 Vul het formulier in.

Formulieritem	Beschrijving
Naam	Geef een naam op voor het netwerkbereik.
Beschrijving	Geef een beschrijving op voor het netwerkbereik.

Formulieritem	Beschrijving
Pods weergeven	De optie Pods weergeven is alleen zichtbaar wanneer de weergavemodule is ingeschakeld. URL voor clienttoegang van host. Geef de juiste toegangs-URL voor de Horizon Client voor het netwerkbereik op. Poort voor clienttoegang Geef het juiste toegangspoortnummer voor de Horizon Client voor het netwerkbereik op.
IP-bereiken	Wijzig IP-bereiken of voeg IP-bereiken toe totdat alle gewenste (en geen ongewenste) IP-adressen zijn opgenomen.

Wat nu te doen

- Koppel elk netwerkbereik aan de identiteitsproviderinstantie.
- Koppel netwerkbereiken naar wens aan een toegangsbeleidsregel. Zie [Instellingen voor toegangsbeleid configureren](#).

Kenmerken selecteren om te synchroniseren met de directory

Wanneer u de Directories Management-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 indien nodig 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.

Raadpleeg [Gebruikerskenmerken beheren die vanuit Active Directory worden gesynchroniseerd](#) voor een lijst met de standaard toegewezen kenmerken.

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.

Procedure

- 1 Meld u als systeem- of tenantbeheerder aan bij vRealize Automation.
- 2 Klik op het tabblad Beheer.
- 3 Selecteer **Beheer van directory's > Gebruikerskenmerken**
- 4 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.
- 5 Voeg in de sectie Kenmerken de naam van het Directories Management-directorykenmerk toe aan de lijst.

6 Klik op **Opslaan**.

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

7 Nadat de directory is gemaakt, gaat u naar de pagina Identiteitsarchieven en selecteert u de directory.**8** Klik op **Synchronisatie-instellingen > Toegewezen kenmerken**.**9** Selecteer in het vervolgkeuzemenu voor de kenmerken die u hebt toegevoegd, het Active Directory-kenmerk waarnaar u wilt toewijzen.**10** Klik op **Opslaan**.**Resultaten**

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

Het standaardtoegangsbeleid toepassen

De Directories Management-service bevat een standaardtoegangsbeleid waarmee toegang van gebruikers tot hun toepassingsportals wordt beheerd. U kunt het beleid wijzigen door de beleidsregels naar wens aan te passen.

Wanneer u verificatiemethoden inschakelt die geen wachtwoorden verifiëren, moet u het standaardbeleid bewerken en de ingeschakelde verificatiemethode toevoegen aan de beleidsregels.

Voor elke regel in het standaardtoegangsbeleid moet aan een set criteria worden voldaan. Als dit het geval is, krijgt de gebruiker toegang tot de toepassingsportal. U past een netwerkbereik toe, selecteert welk type gebruiker toegang heeft tot inhoud en selecteert de verificatiemethode die moet worden gebruikt. Zie [Toegangsbeleid beheren](#).

Het aantal pogingen dat een service doet om een gebruiker aan te melden met een bepaalde verificatiemethode varieert. De service doet slechts een verificatiepoging voor Kerberos- of certificaatverificatie. Als de gebruiker niet bij de poging kan worden aangemeld, wordt de volgende verificatiemethode in de regel geprobeerd. Het maximale aantal mislukte aanmeldingspogingen voor Active Directory-wachtwoordverificatie en RSA SecurID-verificatie is standaard ingesteld op vijf. Wanneer voor een gebruiker vijf mislukte aanmeldingspogingen worden bereikt, probeert de service de gebruiker aan te melden met de volgende verificatiemethode in de lijst. Wanneer de verificatiemethoden zijn uitgeput, wordt door de service een foutbericht weergegeven.

Verificatiemethoden toepassen op beleidsregels

In de standaardbeleidsregels wordt alleen de verificatiemethode voor wachtwoorden geconfigureerd. U moet de beleidsregels bewerken voor het selecteren van de andere verificatiemethoden die u hebt geconfigureerd en het instellen van de volgorde waarin de verificatiemethoden worden gebruikt voor verificatie.

Voorwaarden

Schakel de verificatiemethoden in die door uw organisatie worden ondersteund en configureer deze. Zie [Alternatieve producten voor gebruikersverificatie integreren in Beheer van directory's](#).

Procedure

- 1 Selecteer **Beheer > Beheer van directory's > Beleid**.
- 2 Klik om het standaardtoegangsbeleid om dit te bewerken.
- 3 Als u een beleidsregel wilt bewerken, klikt u op de te bewerken verificatiemethode in de kolom Verificatiemethode van Beleidsregels.

Als u een nieuwe beleidsregel wilt toevoegen, klikt u op het **+**-pictogram.

- 4 Klik op **Opslaan** en klik opnieuw op **Opslaan** op de pagina Beleid.

Beleidsregel bewerken

- 5 Klik op **Opslaan** en klik opnieuw op **Opslaan** op de pagina Beleid.

Kerberos configureren voor Directories Management

Kerberos-verificatie biedt gebruikers die zijn aangemeld bij het Active Directory-domein toegang tot hun appsportal zonder dat ze om aanvullende verificatiegegevens worden gevraagd. U moet Windows-verificatie inschakelen, zodat het Kerberos-protocol interacties kan beveiligen tussen de browser van gebruikers en de Directories Management-service. U hoeft Active Directory niet direct te configureren om Kerberos in uw implementatie te laten werken.

Momenteel worden interacties tussen de browser van een gebruiker en de service alleen door Kerberos geverifieerd op het Windows-besturingssysteem. Bij toegang tot de service vanaf andere besturingssystemen wordt niet van Kerberos-verificatie gebruikgemaakt.

■ [Kerberos-verificatie configureren](#)

Als u de Directories Management-service wilt configureren voor het leveren van Kerberos-verificatie, moet u deelnemen aan het domein en Kerberos-verificatie inschakelen op de Directories Management-connector.

■ [Internet Explorer configureren voor toegang tot de webinterface](#)

U moet de Internet Explorer-browser configureren als Kerberos is geconfigureerd voor uw implementatie en u gebruikers toegang wilt verlenen tot de webinterface via Internet Explorer.

- [Firefox configureren voor toegang tot de webinterface](#)

U moet de Firefox-browser configureren als Kerberos is geconfigureerd voor uw implementatie en u gebruikers toegang wilt verlenen tot de webinterface via Firefox.

- [De Chrome-browser configureren voor toegang tot de webinterface](#)

U moet de Chrome-browser configureren als Kerberos is geconfigureerd voor uw implementatie en u gebruikers toegang wilt verlenen tot de webinterface via de Chrome-browser.

Kerberos-verificatie configureren

Als u de Directories Management-service wilt configureren voor het leveren van Kerberos-verificatie, moet u deelnemen aan het domein en Kerberos-verificatie inschakelen op de Directories Management-connector.

Voorwaarden

- Implementeer NSX Edge in vCenter en configureer een NSX load balancer. Zie *Taakverdeling voor vRealize Automation* voor informatie over het instellen van een load balancer.
- Maak uw domein lid van de hoofdtentant. U moet dit doen voordat u directoryverbindingen maakt in afzonderlijke tenants.
 - Meld u aan bij de standaardtenant als administrator@vsphere.local.
 - Maak een lokale gebruiker met de naam TestUser en voer TestUser in als beheerder van de tenant.
 - Selecteer **Beheer > Beheer van directory's > Connectoren**.
 - Selecteer Aan domein toevoegen voor elke applianceconnector.
 - Aan domein toevoegen. Selecteer Aangepast domein en voer het domein in waarmee u wilt dat de tenant verbinding maakt, samen met de verificatiegegevens en de OU om verbinding te maken.
- Stel directoryverbindingen in voor standaardtenants en voor niet-standaardtenants. Kerberos-verificatie werkt met Geïntegreerde Windows-verificatie en met Active Directory via LDAP. Zie [Een koppeling configureren voor Active Directory via een LDAP/IWA](#) en [Een OpenLDAP-directoryverbinding configureren](#).
- Zorg ervoor dat de hostnaam van het vRealize Automation-knooppunt overeenkomt met het Active Directory-domein waaraan dit is toegevoegd. Als vRealize Automation bijvoorbeeld wordt toegevoegd aan een Active Directory-realm met de naam COMPANY.COM, moet de hostnaam node.company.com zijn.
- Configureer een identiteitsprovider voor de werkplek. Zorg ervoor dat alle knooppunten in uw implementatie zijn geregistreerd in de identiteitsprovider voor de werkplek en dat de naam van uw load balancer is gedefinieerd.
 - Selecteer **Beheer > Beheer van directory's > Identiteitsproviders**.
 - Selecteer de koppeling van de juiste identiteitsprovider.

Bijvoorbeeld: WorkspaceIDP__1.

- c Klik op de koppeling voor de identiteitsprovider en zoek de geconfigureerde IdP-hostnaam. Leg de hostnaam vast omdat u deze nodig hebt bij het configureren van uw webbrowsers.
 - d Registreer alle toepasselijke knooppunten in de identiteitsprovider voor de werkplek en voer de FQDN van de load balancer in voor de hostnaam.
 - e Klik op **Opslaan**.
- Configureer de tenantdirectory voor de standaardtenant. Zie 'Toegang tot de standaardtenant configureren' in *vRealize Automation installeren*

Procedure

- 1 Ga als tenantbeheerder naar **Beheer > Beheer van directory's > Connectoren**.
- 2 Klik op de pagina Connectoren voor de connector die wordt geconfigureerd voor Kerberos-verificatie op **Aan domein toevoegen**.
- 3 Voer op de pagina Aan domein toevoegen de informatie in voor het Active Directory-domein.

Optie	Beschrijving
Domein	Voer de Fully Qualified Domain Name (volledig gekwalificeerde domeinnaam) van de Active Directory in. De domeinnaam die u invoert, moet hetzelfde Windows-domein zijn als de connectorserver.
Domeingebruiker	Voer de gebruikersnaam in van een account in de Active Directory dat rechten heeft om systemen aan dat Active Directory-domein toe te voegen.
Domeinwachtwoord	Voer het wachtwoord in dat aan de AD-gebruikersnaam is gekoppeld. Dit wachtwoord wordt niet opgeslagen door Directories Management

Klik op **Opslaan**.

De pagina Aan domein toevoegen wordt vernieuwd en geeft een bericht weer dat u aan het domein bent toegevoegd.

- 4 Klik in de kolom Werker voor de connector op **Verificatieadapters**.
- 5 Klik op **Kerberos-IDP-adapter**
U wordt omgeleid naar de aanmeldpagina van het identiteitsbeheer.
- 6 Klik op **Bewerken** in de rij Kerberos-IDP-adapter en configureer de Kerberos-verificatiepagina.

Optie	Beschrijving
Naam	Een naam is vereist. De standaardnaam is Kerberos-IDP-adapter. U kunt dit wijzigen.
Directory-UID-kenmerk	Voer het accountkenmerk in dat de gebruikersnaam bevat.

Optie	Beschrijving
Windows-verificatie inschakelen	Selecteer dit om verificatie-interacties uit te breiden tussen de browsers van gebruikers en Directories Management.
NTLM inschakelen	Selecteer dit alleen om op het NTLM-protocol (NT LAN Manager) gebaseerde verificatie in te schakelen als uw Active Directory-infrastructuur vertrouwt op NTLM-verificatie.
Omleiden inschakelen	Selecteer dit als round robin-DNS en load balancers geen Kerberos-ondersteuning hebben. Verificatieaanvragen worden omgeleid naar de hostnaam voor omleiding. Als dit geselecteerd is, voert u de hostnaam voor omleiding in het tekstvak Hostnaam omleiding in. Dit is doorgaans de hostnaam van de service.

7 Klik op **Opslaan**.

8 Configureer Kerberos-verificatie op alle toepasselijke knooppunten.

a Selecteer **Beheer > Beheer van directory's > Connectoren**.

Op deze pagina worden de momenteel geconfigureerde connectoren weergegeven. Standaard wordt alleen wachtwoordverificatie geconfigureerd.

b Klik op de hyperlink van de werker die aan de eerste vRealize Automation-toepassing is gekoppeld.

c Klik op de koppeling KerberosIdpAdapter om de verificatiepagina te openen.

Mogelijk moet u uw wachtwoord invoeren en de KerberosIdpAdapter-koppeling opnieuw starten.

d Geef het Directory-UID-kenmerk op en voer de standaardwaarde sMAAccountName in.

e Schakel de selectievakjes **Windows-verificatie inschakelen** en **Doorverwijzen inschakelen** in.

f Schakel **NTLM** niet in, omdat dit alleen nodig is voor oudere domeincontrollers.

g Voer de naam in van de VA1-appliance voor de omleidingshostnaam.

h Klik op **Opslaan**.

9 Configureer een standaardtoegangsbeleid. Kerberos-configuratie vereist drie aspecten van het toegangsbeleid: Kerberos, wachtwoord, lokaal wachtwoord.

a Selecteer **Beheer > Beheer van directory's > Beleid**.

b Selecteer default_access_policy_set.

c Klik op de waarde met de hyperlink voor het wachtwoord onder de titel Verificatiemethoden op de balk van de webbrowser.

d Klik op de groene +-pictogrammen om nieuwe verificatiemethoden te maken voor Kerberos, wachtwoord en wachtwoord (lokale directory).

e Selecteer voor elke verificatiemethode ALLE BEREIKEN als het netwerkbereik van de gebruikers en Webbrowser als de toegangsmethode voor inhoud van de gebruiker.

- f Wijzig de eerste verificatiemethode in Kerberos en stel de failback-methode in op wachtwoord.
- g Klik op **Opslaan** en klik vervolgens op **OK**.

Internet Explorer configureren voor toegang tot de webinterface

U moet de Internet Explorer-browser configureren als Kerberos is geconfigureerd voor uw implementatie en u gebruikers toegang wilt verlenen tot de webinterface via Internet Explorer.

Kerberos-verificatie werkt samen met Directories Management op Windows-besturingssystemen.

Opmerking Implementeer deze stappen voor Kerberos niet op andere besturingssystemen.

Voorwaarden

Configureer de Internet Explorer-browser voor elke gebruiker of bied gebruikers instructies voor configuratie nadat u Kerberos hebt geconfigureerd.

Procedure

- 1 Controleer of u bij Windows bent aangemeld als gebruiker in het domein.
- 2 Schakel automatische aanmelding in Internet Explorer in.
 - a Selecteer **Extra > Internetopties > Beveiliging**.
 - b Klik op **Aangepast niveau**.
 - c Selecteer **Alleen automatisch aanmelden in de intranetzone**.
 - d Klik op **OK**.
- 3 Controleer of deze instantie van de virtuele toepassing van de connector onderdeel uitmaakt van de lokale intranetzone.
 - a Gebruik Internet Explorer om de aanmeldings-URL voor de Directories Management- te openen via *https://myconnectorhost.domain/authenticate/*.
 - b Controleer de zone in de rechterbenedenhoek, op de statusbalk van het browservenster.
Als de zone Lokaal intranet is, is de configuratie van Internet Explorer voltooid.
- 4 Als de zone niet Lokaal intranet is, voegt u de aanmeldings-URL voor de Directories Management- toe aan de intranetzone.
 - a Selecteer **Extra > Internetopties > Beveiliging > Lokaal intranet > Sites**.
 - b Selecteer **Intranetnetwerk automatisch detecteren**.
Als deze optie niet eerder was ingeschakeld, is inschakelen mogelijk voldoende voor het toevoegen van de aan de intranetzone.
 - c (Optioneel) Als u **Intranetnetwerk automatisch detecteren** hebt geselecteerd, klikt u op **OK** totdat alle dialoogvensters zijn gesloten.

- d Klik op **Geavanceerd** in het dialoogvenster Lokaal intranet.
Een tweede dialoogvenster met de naam Lokaal intranet wordt geopend.
 - e Voer de -URL van Directories Management in het tekstvak **Deze website aan de zone toevoegen** in.
https://myconnectorhost.domain/authenticate/
 - f Klik op **Toevoegen > Sluiten > OK**.
- 5** Controleer of Internet Explorer de Windows-verificatie mag doorgeven aan de vertrouwde site.
- a Klik in het dialoogvenster Internetopties op het tabblad **Geavanceerd**.
 - b Selecteer **Geïntegreerde Windows-verificatie inschakelen**.
Deze optie wordt pas van kracht nadat u Internet Explorer opnieuw hebt gestart.
 - c Klik op **OK**.
- 6** Meld u aan bij de webinterface om toegang te controleren.
Als Kerberos-verificatie slaagt, gaat de test-URL naar de webinterface.

Resultaten

Het Kerberos-protocol beveiligt alle interacties tussen deze instantie van de Internet Explorer-browser en Directories Management. Gebruikers kunnen vervolgens Single Sign-On-toegang gebruiken voor hun My Apps-portal.

Firefox configureren voor toegang tot de webinterface

U moet de Firefox-browser configureren als Kerberos is geconfigureerd voor uw implementatie en u gebruikers toegang wilt verlenen tot de webinterface via Firefox.

Kerberos-verificatie werkt samen met Directories Management op Windows-besturingssystemen.

Voorwaarden

Configureer de Firefox-browser voor elke gebruiker of biedt gebruikers instructies voor configuratie nadat u Kerberos hebt geconfigureerd.

Procedure

- 1** Voer `about:config` in het URL-tekstvak van de Firefox-browser in om toegang te krijgen tot de geavanceerde instellingen.
- 2** Klik op **Ik zal voorzichtig zijn, dat beloof ik!**.
- 3** Dubbelklik op **network.negotiate-auth.trusted-uris** in de kolom met de naam van de voorkeur.
- 4** Voer de -URL voor Directories Management in het tekstvak in.
https://myconnectorhost.domain.com
- 5** Klik op **OK**.

- 6 Dubbelklik op **network.negotiate-auth.delegation-uris** in de kolom met de naam van de voorkeur.
- 7 Voer de -URL voor Directories Management in het tekstvak in.
https://myconnectorhost.domain.com/authenticate/
- 8 Klik op **OK**.
- 9 Test de Kerberos-functies door u via de Firefox-browser aan te melden met de aanmeldings-URL van de . Bijvoorbeeld: *https://myconnectorhost.domain.com/authenticate/*.

Als Kerberos-verificatie slaagt, gaat de test-URL naar de webinterface.

Resultaten

Het Kerberos-protocol beveiligt alle interacties tussen deze instantie van de Firefox-browser en Directories Management. Gebruikers kunnen vervolgens Single Sign-On-toegang gebruiken voor hun My Apps-portal.

De Chrome-browser configureren voor toegang tot de webinterface

U moet de Chrome-browser configureren als Kerberos is geconfigureerd voor uw implementatie en u gebruikers toegang wilt verlenen tot de webinterface via de Chrome-browser.

Kerberos-verificatie werkt samen met Directories Management op Windows-besturingssystemen.

Opmerking Implementeer deze stappen voor Kerberos niet op andere besturingssystemen.

Voorwaarden

- Configureer Kerberos.
- Omdat Chrome de configuratie van Internet Explorer gebruikt voor het inschakelen van Kerberos-verificatie, moet u Internet Explorer configureren om het gebruik van de Internet Explorer-configuratie door Chrome toe te staan. Zie de Google-documentatie voor informatie over het configureren van Chrome voor Kerberos-verificatie.

Procedure

- 1 Test de Kerberos-functies in de Chrome-browser.
- 2 Meld u aan bij Directories Management op *https://myconnectorhost.domain.com/authenticate/*.

Als Kerberos-verificatie slaagt, maakt de test-URL verbinding met de webinterface.

Resultaten

Als alle met Kerberos verwante configuraties correct zijn, beveiligt het betreffende protocol (Kerberos) alle interacties tussen deze instantie van de Chrome-browser en Directories Management. Gebruikers kunnen Single Sign-On-toegang gebruiken voor hun My Apps-portal.

Externe connectoren voor beheer van directory's upgraden

Als u een externe connector gebruikt met uw configuratie van vRealize Automation-beheer van directory's, dient u deze connector mogelijk te upgraden.

U dient mogelijk een externe connector te upgraden wanneer u de versie van uw vRealize Automation-implementatie upgradet of als een nieuwe connectorversie een functie biedt die u wilt.

Deze documentatie is alleen van toepassing op gebruikers die aanvullende standalone externe connectortoepassingen hebben geïmplementeerd. In vRealize Automation worden bijvoorbeeld externe connectortoepassingen gebruikt met kaartverificatie.

Standaard gebruikt de connector de VMware-website voor de upgradeprocedure. Hiervoor moet de connectortoepassing over een internetverbinding beschikken. Indien nodig, moet u ook proxyserverinstellingen voor de connectortoepassing configureren.

Als uw connectortoepassing geen internetverbinding heeft, kunt u de upgrade offline uitvoeren. Voor een offline-upgrade downloadt u het upgradepakket en stelt u een lokale webserver in om het upgradebestand te hosten.

Doelgroep

Deze informatie is bedoeld voor iedereen die Beheer van directory's installeert, upgradet en configureert. De informatie is geschreven voor ervaren systeembeheerders van Windows en Linux die vertrouwd zijn met virtuele machinetechnologie.

De upgrade van een externe connector voorbereiden

Als u de upgrade van een connector wilt voorbereiden, moet u controleren welke upgrades beschikbaar zijn en de instellingen van de proxyserver configureren voor de appliance, indien van toepassing.

■ [Online zoeken naar een upgrade voor een externe connector](#)

Als uw connectortoepassing verbinding met internet heeft, kunt u controleren op de beschikbaarheid van online-upgrades vanaf de toepassing.

■ [Proxyserverinstellingen configureren voor de externe connectortoepassing](#)

De connectortoepassing heeft toegang tot de VMware-updateservers via internet. Als uw netwerkconfiguratie internettoegang biedt met behulp van een HTTP-proxy, moet u de proxyinstellingen aanpassen voor de toepassing.

Online zoeken naar een upgrade voor een externe connector

Als uw connectortoepassing verbinding met internet heeft, kunt u controleren op de beschikbaarheid van online-upgrades vanaf de toepassing.

Procedure

- 1 Meld u aan op de connectortoepassing als hoofdgebruiker.

- 2 Voer de volgende opdracht uit.

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

- 3 Voer de volgende opdracht uit om te controleren of een online-upgrade beschikbaar is.

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

Proxyserverinstellingen configureren voor de externe connectortoepassing

De connectortoepassing heeft toegang tot de VMware-updateservers via internet. Als uw netwerkconfiguratie internettoegang biedt met behulp van een HTTP-proxy, moet u de proxyinstellingen aanpassen voor de toepassing.

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.

Voorwaarden

- Controleer of u over het hoofdwachtwoord voor de connectortoepassing beschikt.
- Controleer of u over de proxyservergegevens beschikt.

Procedure

- 1 Meld u aan op de connectortoepassing als hoofdgebruiker.
- 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 virtual connectortoepassing om de nieuwe proxyinstellingen te gebruiken.

```
service horizon-workspace restart
```

Resultaten

De VMware-updateservers zijn nu beschikbaar voor de connectortoepassing.

Een externe connector online upgraden

U kunt een externe connector voor Beheer van directory's online upgraden als u een geschikte verbinding hebt.

Voorwaarden

- Controleer of de connectortoepassing `vapp-updates.vmware.com` kan omzetten en bereiken op poort 80 via HTTP.
- Controleer of een connectorupgrade bestaat. Voer de geschikte opdracht uit om te controleren op upgrades. Zie Controleren op de beschikbaarheid van een Directories Management-onlineconnectorupgrade.
- Controleer of minstens 2 GB vrije schijfruimte beschikbaar is op de primaire rootpartitie van de toepassing.
- Controleer of de connector correct is geconfigureerd.
- Maak een momentopname van uw connectortoepassing om er een back-up van te maken. Voor meer informatie over het maken van momentopnamen raadpleegt u de vSphere-documentatie.
- Als een HTTP-proxyserver vereist is voor uitgaande HTTP-toegang, configureert u de proxyserverinstellingen voor de connectortoepassing. Zie Proxyserverinstellingen voor de Directories Management-connectorupgrade configureren.

Procedure

- 1 Meld u aan op de connectortoepassing als hoofdgebruiker.

- 2 Voer de volgende opdracht uit.

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

- 3 Voer de volgende opdracht uit om te controleren of een online-upgrade beschikbaar is.

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

- 4 Voer de volgende opdracht uit om de toepassing bij te werken.

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

Berichten die tijdens de upgrade worden weergegeven, worden opgeslagen in het `update.log`-bestand op `/opt/vmware/var/log/update.log`.

- 5 Voer de opdracht `updatemgr.hzn check` opnieuw uit om te controleren of er geen nieuwere update beschikbaar is.

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

- 6 Controleer de versie van de geüpgradede toepassing.

```
vamcli version --appliance
```

De nieuwe versie wordt weergegeven.

- 7 Start de connectortoepassing opnieuw.
reboot

Een externe connector offline upgraden

Als uw bestaande connectortoepassing voor vRealize Automation-beheer van directory's geen verbinding met internet kan maken voor een upgrade, kunt u een offline-upgrade uitvoeren. U moet een upgradeopslagplaats op een lokale webserver maken en de connectortoepassing configureren zodat deze de lokale webserver gebruikt voor de upgrade.

Voorwaarden

- Controleer of een connectorupgrade bestaat. Raadpleeg de website My VMware-downloads op my.vmware.com voor upgrades.
- Controleer of minstens 2 GB vrije schijfruimte beschikbaar is op de primaire rootpartitie van de toepassing.
- Controleer of de connector correct is geconfigureerd.
- Maak een momentopname van uw connectortoepassing om er een back-up van te maken. Voor meer informatie over het maken van momentopnamen raadpleegt u de vSphere-documentatie.
- Configureer de connectortoepassing om een lokale webserver te gebruiken om het upgradebestand te hosten. Zie Een lokale webserver voorbereiden voor een offline-upgrade.

Procedure

1 Een lokale webserver voorbereiden voor een offline-upgrade

Voordat u de offlineconnectorupgrade start, bereidt u de lokale webserver voor door een directorystructuur met een subdirectory voor de connectortoepassing te maken.

2 De connector configureren en de offline-upgrade uitvoeren

Configureer de connectortoepassing om te verwijzen naar de lokale webserver om een offline-upgrade uit te voeren. Voer vervolgens de upgrade van de toepassing uit.

Een lokale webserver voorbereiden voor een offline-upgrade

Voordat u de offlineconnectorupgrade start, bereidt u de lokale webserver voor door een directorystructuur met een subdirectory voor de connectortoepassing te maken.

Voorwaarden

- Download het bestand `identity-manager-connector-versionNumber-buildNumber-updaterepo.zip` van My VMware. Ga naar my.vmware.com, navigeer naar de downloadpagina van VMware Identity Manager, en download het bestand dat wordt weergegeven onder **VMware Identity Manager Connector offline upgrade package**.

- Als u een IIS-webserver gebruikt, configureert u de webserver om speciale tekens in bestandsnamen toe te staan. U configureert dit in het gedeelte **Aanvraagfiltering** door de optie **Dubbele aanhalingstekens toestaan** te selecteren.

Procedure

- 1 Maak een directory op de webserver op `http://YourWebServer/VM/` en kopieer het gedownloade ZIP-bestand naar deze directory.
- 2 Controleer of uw webserver MIME-typen bevat voor `.sig` (tekst/zonder opmaak) en `.sha256` (tekst/zonder opmaak).

Zonder deze MIME-typen kan uw webserver niet controleren op updates.

- 3 Pak het bestand uit.

De inhoud van het uitgepakte ZIP-bestand wordt aangeboden door `http://YourWebServer/VM/`.

De uitgepakte inhoud van het bestand bevat de volgende subdirectory's: `/manifest` en `/package-pool`.

- 4 Voer de volgende opdracht `updateLocal.hzn` uit om te controleren of de URL geldige update-inhoud bevat.

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

De connector configureren en de offline-upgrade uitvoeren

Configureer de connectortoepassing om te verwijzen naar de lokale webserver om een offline-upgrade uit te voeren. Voer vervolgens de upgrade van de toepassing uit.

Voorwaarden

Bereid een lokale webserver voor op een offline-upgrade.

Procedure

- 1 Meld u aan op de connectortoepassing als hoofdgebruiker.
- 2 Voer de volgende opdracht uit om een upgradeopslagplaats te configureren die een lokale webserver gebruikt.

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

Opmerking Om de configuratie ongedaan te maken en de mogelijkheid om een online-upgrade uit te voeren, te herstellen, kunt u de volgende opdracht uitvoeren.

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

3 Voer de upgrade uit.

- a Voer de volgende opdracht uit.

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

- b Voer de volgende opdracht uit om de versie van de beschikbare upgrade te controleren.

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

- c Voer de volgende opdracht uit om de connector bij te werken.

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

Berichten die tijdens de upgrade worden weergegeven, worden opgeslagen in het `update.log`-bestand op `/opt/vmware/var/log/update.log`.

- d Voer de opdracht
- `updatemgr.hzn check`
- opnieuw uit.

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

- e Controleer de versie van de geüpgradede toepassing.

```
vamcli version --appliance
```

De opdracht zou de nieuwe versie moeten weergeven.

- f Start de connectortoepassing opnieuw.

Voer in de opdrachtregel bijvoorbeeld de volgende opdracht uit.

```
reboot
```

Resultaten

De connectorupgrade is voltooid.

Instellingen configureren na een upgrade naar een externe connector

Als u een upgrade naar connector 2016.3.1.0 of hoger hebt uitgevoerd, moet u bepaalde instellingen mogelijk aanpassen.

Opnieuw lid worden van domein met Kerberos-verificatie

Als u Kerberos-verificatie of Active Directory (met geïntegreerde Windows-verificatie) gebruikt, moet u het domein verlaten en er opnieuw lid van worden. Dit is vereist voor alle virtuele toepassingen van de connector in uw implementatie.

- 1 Selecteer
- Beheer > Beheer van directory's > Connectoren**
- .

- 2 Op de pagina Connectoren voor elke connector die wordt gebruikt voor Kerberos-verificatie of een Active Directory-directory (met geïntegreerde Windows-verificatie), klikt u op **Verwijderen uit domein**.
- 3 Om lid te worden van het domein moet u Active Directory-verificatiegegevens hebben met deelnamerechten voor het domein. Raadpleeg [Een connectormachine toevoegen aan een domein](#) voor meer informatie.
- 4 Als u Kerberos-verificatie gebruikt, schakelt u de Kerberos-verificatieadapter opnieuw in. Om toegang te krijgen tot de pagina Verificatieadapters, klikt u op de pagina Connectoren op de juiste koppeling in de kolom **Werker** en selecteert u het tabblad **Verificatieadapters**.
- 5 Controleer of de andere verificatieadapters die u gebruikt, zijn ingeschakeld.

Domeinpagina bijwerken

Als u Active Directory (met geïntegreerde Windows-verificatie) of Active Directory via LDAP gebruikt met de optie **Deze directory ondersteunt DNS-servicelocatie** ingeschakeld, slaat u de pagina Domeinen van de directory op.

- 1 Selecteer **Beheer > Beheer van directory's > Directory's**.
- 2 Selecteer de directory die u wilt bewerken.
- 3 Geef het wachtwoord voor de Bind DN-gebruiker op en klik op **Opslaan**.
- 4 Klik op **Synchronisatie-instellingen** aan de linkerkant van de pagina en selecteer het tabblad **Domeinen**.
- 5 Klik op **Opslaan**.

DNS-servicelocatie en domeincontrollers

Opmerking In connector 2016.3.1.0 en later wordt een `domain_krb.properties`-bestand automatisch gemaakt en gevuld met domeincontrollers wanneer een directory met ingeschakelde DNS-servicelocatie wordt gemaakt. Wanneer u de pagina Domeinen na de upgrade opslaat, en u een `domain_krb.properties`-bestand in uw originele implementatie had, wordt het bestand bijgewerkt met domeinen die u mogelijk opeenvolgend hebt toegevoegd en die zich niet in het bestand bevonden. Als u geen `domain_krb.properties`-bestand in uw originele implementatie had, wordt het bestand gemaakt en automatisch gevuld met domeincontrollers. Zie [Domeincontrollers selecteren](#) voor meer informatie over het bestand `domain_krb.properties`.

Fouten bij het upgraden van externe connector oplossen

U kunt problemen bij het upgraden van de externe connector voor vRA-beheer van directory's oplossen door de foutenlogboeken te controleren. Als de connector niet opstart, kunt u deze terugzetten naar een vorige instantie door terug te draaien naar een momentopname.

■ De upgradefoutenlogboeken controleren

Los problemen op die optreden tijdens de upgrade door de foutenlogboeken te controleren. Upgradelogboekbestanden bevinden zich in de directory `/opt/vmware/var/log`.

■ Terugdraaien naar momentopnamen van connector

Als de connector niet correct wordt opgestart na een upgrade en u het probleem niet kunt oplossen door de upgradefoutenlogboeken te controleren en de upgradeopdracht opnieuw uit te voeren, kunt u terugdraaien naar een eerdere connectorinstantie.

■ Een logboekbestandsbundel verzamelen

U kunt een bundel van logboekbestanden verzamelen om te verzenden naar VMware-ondersteuning. U ontvangt de bundel van de connectorconfiguratiepagina.

De upgradefoutenlogboeken controleren

Los problemen op die optreden tijdens de upgrade door de foutenlogboeken te controleren. Upgradelogboekbestanden bevinden zich in de directory `/opt/vmware/var/log`.

Als er fouten optreden, kan de connector mogelijk niet worden gestart na de upgrade.

Procedure

- 1 Meld u aan bij de connectortoepassing.
- 2 Ga naar de directory `/opt/vmware/var/log`.
- 3 Open het bestand `update.log` en controleer de foutberichten.
- 4 Los de problemen op en voer de upgradeopdracht opnieuw uit. De upgradeopdracht wordt hervat vanaf het punt waar deze was gestopt.

Opmerking U kunt ook terugdraaien naar een momentopname en de update opnieuw uitvoeren.

Terugdraaien naar momentopnamen van connector

Als de connector niet correct wordt opgestart na een upgrade en u het probleem niet kunt oplossen door de upgradefoutenlogboeken te controleren en de upgradeopdracht opnieuw uit te voeren, kunt u terugdraaien naar een eerdere connectorinstantie.

Procedure

- ◆ Keer terug naar een van de momentopnamen die u hebt gemaakt als een back-up van uw originele connectorinstantie. Raadpleeg de vSphere-documentatie voor meer informatie.

Een logboekbestandsbundel verzamelen

U kunt een bundel van logboekbestanden verzamelen om te verzenden naar VMware-ondersteuning. U ontvangt de bundel van de connectorconfiguratiepagina.

De volgende logboekbestanden worden verzameld in de bundel.

Tabel 2-9. Logboekbestanden

Onderdeel	Locatie van logboekbestand	Beschrijving
Apache Tomcat-logboeken (catalina.log)	/opt/vmware/horizon/workspace/logs/catalina.log	Apache Tomcat registreert berichten die niet in andere logboekbestanden zijn geregistreerd.
Configurator-logboeken (configurator.log)	/opt/vmware/horizon/workspace/logs/configurator.log	Aanvragen die de configurator van de REST-client en de webinterface ontvangt.
Connector-logboeken (connector.log)	/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.

Procedure

- 1 Meld u aan bij de connectorconfiguratiepagina op <https://connectorURL:8443/cfg/logs>.
- 2 Klik op **Logboekbundel voorbereiden**.
- 3 Download de bundel en verzend deze naar VMware-ondersteuning.

Scenario: een Active Directory-koppeling voor een vRealize Automation met hoge zichtbaarheid configureren

Als tenantbeheerder wilt u een directoryverbinding met Active Directory via LDAP configureren om gebruikersverificatie voor uw vRealize Automation-implementatie met hoge beschikbaarheid te ondersteunen.

Elke vRealize Automation-toepassing bevat een connector die ondersteuning biedt voor gebruikersverificatie, hoewel er meestal maar één connector wordt geconfigureerd voor het uitvoeren van synchronisatie tussen directory's. Het maakt niet uit welke connector u kiest als de connector voor synchronisatie. Om hoge beschikbaarheid voor Beheer van directory's te ondersteunen, moet u een tweede connector configureren die overeenkomt met uw tweede vRealize Automation-toepassing, die verbinding maakt met uw identiteitsprovider en verwijst naar dezelfde Active Directory-instantie. Als er in deze configuratie een storing optreedt in een toepassing, neemt de andere het beheer van gebruikersverificatie over.

In een omgeving met hoge beschikbaarheid moeten alle knooppunten dezelfde verzameling Active Directory-directory's, gebruikers, verificatiemethoden, enz. bedienen. De meest directe methode om dit te bereiken, is door de identiteitsprovider te promoveren naar het cluster door de host van de load balancer in te stellen als de host van de identiteitsprovider. In deze configuratie worden alle verificatieaanvragen doorgeleid naar de load balancer, die de aanvragen doorstuurt naar een van de connectoren.

Voorwaarden

- Installeer een gedistribueerde vRealize Automation-implementatie met de juiste load balancers. Zie *vRealize Automation installeren*.
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > Beheer van directory's > Directory's**.
- 2 Klik op **Directory toevoegen**.
- 3 Geef uw specifieke Active Directory-accountinstellingen op en accepteer de standaardopties.

Optie	Voorbeeldinvoer
Directorynaam	Voeg het IP-adres van de domeinnaam van uw active directory toe.
Connector voor synchronisatie	Elke vRealize Automation-toepassing bevat een connector. Gebruik een van de beschikbare connectors.
Basis-DN	Voer de DN (Distinguished Name) in van het beginpunt voor zoekopdrachten in de directoryserver. Bijvoorbeeld: cn=users,dc=corp,dc=local.
Bindings-DN	Voer de volledige DN (Distinguished Name) in, inclusief de CN (Common Name) van een gebruikersaccount op Active Directory dat over rechten beschikt om naar gebruikers te zoeken. Bijvoorbeeld: cn=config_admin infra,cn=users,dc=corp,dc=local.
Wachtwoord van de bindings-DN	Voer het wachtwoord in voor het account op Active Directory dat over rechten beschikt om naar gebruikers te zoeken.

- 4 Klik op **Verbinding testen** om de verbinding met de geconfigureerde directory te testen.
Als de verbinding mislukt, controleert u uw invoer in alle velden en neemt u indien nodig contact op met uw systeembeheerder.
- 5 Klik op **Opslaan en Volgende**.
De pagina Selecteer de domeinen met de lijst met domeinen wordt weergegeven.
- 6 Laat het standaarddomein geselecteerd en klik op **Volgende**.
- 7 Controleer of de kenmerknamen zijn toegewezen aan de juiste Active Directory-kenmerken.
Als dit niet het geval is, selecteert u het juiste Active Directory-kenmerk in het vervolgkeuzemenu. Klik op **Volgende**.
- 8 Selecteer de groepen en de gebruikers die u wilt synchroniseren.
 - a Klik op het pictogram **Toevoegen (+)**.
 - b Voer het gebruikersdomein in en klik op **Groepen zoeken**.
Bijvoorbeeld: **cn=users,dc=corp,dc=local.**
 - c Schakel het selectievakje **Alles selecteren** in.

- d Klik op **Selecteren**.
 - e Klik op **Volgende**.
 - f Klik op **+** om aanvullende gebruikers toe te voegen. Voer ze bijvoorbeeld in als:
CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com.

Om gebruikers uit te sluiten, klikt u op + om een filter te maken om bepaalde typen van gebruikers uit te sluiten. U selecteert het gebruikerskenmerk waarop moet worden gefilterd, de queryregel en de waarde.
 - g Klik op **Volgende**.
- 9** Controleer de pagina om te bekijken of de gebruikers en de groepen worden gesynchroniseerd in de directory en klik op **Directory synchroniseren**.
- De procedure voor het synchroniseren van directory's neemt wat tijd in beslag, maar dit vindt plaats op de achtergrond en u kunt blijven doorwerken.
- 10** Configureer een tweede connector om een hoge beschikbaarheid te ondersteunen.
- a Meld u aan bij de load balancer voor uw vRealize Automation-implementatie als tenantbeheerder.

De URL van de load balancer is *adres van load balancer/vcac/org/naam_van_tenant*.
 - b Selecteer **Beheer > Beheer van directory's > Identiteitsproviders**.
 - c Klik op de identiteitsprovider die momenteel voor uw systeem wordt gebruikt.

De bestaande directory en connector die het basisidentiteitsbeheer voor uw systeem bieden, worden weergegeven.
 - d Klik op het vervolgkeuzemenu **Een connector toevoegen** en selecteer de connector die overeenkomt met uw secundaire vRealize Automation-toepassing.
 - e Voer het juiste wachtwoord in het tekstvak **Wachtwoord bindings-DN** in dat wordt weergegeven wanneer u de connector selecteert.
 - f Klik op **Connector toevoegen**.
 - g Wijzig de hostnaam, zodat deze naar uw load balancer wijst.

Resultaten

U hebt uw zakelijke Active Directory verbonden met vRealize Automation en u hebt Beheer van directory's geconfigureerd voor een hoge beschikbaarheid.

Wat nu te doen

Om uitgebreide beveiliging te bieden, kunt u vertrouwen in twee richtingen tussen uw identiteitsprovider en uw Active Directory configureren. Zie [Een vertrouwensrelatie in twee richtingen configureren tussen vRealize Automation en Active Directory](#).

Externe connectoren voor smartcardverificatie en verificatie via een externe identiteitsprovider in vRealize Automation configureren

Een systeembeheerder moet een externe connector voor uw vRealize Automation-implementatie configureren met behulp van Beheer van directory's als u externe identiteitsproviders met certificaatverificatie of smartcardverificatie gebruikt. De procedure in dit document kan ook in grote lijnen worden toegepast op alle soorten certificaatverificatie.

Beheer van directory's ondersteunt meerdere identiteitsproviders en connectorclusters voor elke geconfigureerde Active Directory. Als u verificatie via een externe identiteitsprovider en smartcardverificatie wilt gebruiken, kunt u een afzonderlijke externe connector of een connectorcluster met een geschikte identiteitsprovider instellen achter een load balancer die SSL-passthrough toestaat. Raadpleeg [Connectoren en connectorclusters beheren](#) voor meer informatie.

Zie [Externe connectoren voor beheer van directory's upgraden](#) voor informatie over het bijwerken van een externe connector.

Er zijn verschillende certificaatconfiguraties beschikbaar voor smartcardverificatie. Zie [Een certificaat- of smartcardadapter configureren voor gebruik met Beheer van directory's](#).

Voorwaarden

- Configureer een geschikte Active Directory-verbinding voor uw vRealize Automation-implementatie.
- Download het vereiste OVA-bestand voor het configureren van een connector van [VMware vRealize Automation Tools and SDK](#).
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

1 [Een token voor connectoractivering genereren](#)

Als u de virtuele connectortoepassing wilt implementeren voor smartcardverificatie, moet u eerst een activeringscode voor de nieuwe connector genereren vanuit de vRealize Automation-console. De activeringscode wordt gebruikt om de verbinding tussen Beheer van directory's en de connector in te stellen.

2 [Het OVA-bestand van de connector implementeren](#)

Als u het OVA-bestand van de connector hebt gedownload, kunt u het implementeren met de VMware vSphere Client of vSphere Web Client.

3 [Connectorinstellingen configureren](#)

Als u het OVA-bestand van de connector hebt geïmplementeerd, moet u de installatiewizard uitvoeren om de toepassing te activeren en de beheerderswachtwoorden configureren.

4 Openbare certificeringsinstantie toepassen

Wanneer Beheer van directory's is geïnstalleerd, wordt een standaard SSL-certificaat gegenereerd. U kunt dit standaardcertificaat gebruiken voor testdoeleinden, maar voor een productieomgeving dient u commerciële SSL-certificaten te genereren en installeren.

5 Een Workspace-identiteitsprovider maken

U moet een Workspace-identiteitsprovider maken voor een externe connector.

6 Certificaatverificatie en standaardregels voor toegangsbeleid configureren

U moet de externe connector met een Active Directory en domein configureren voor vRealize Automation.

Een token voor connectoractivering genereren

Als u de virtuele connectortoepassing wilt implementeren voor smartcardverificatie, moet u eerst een activeringscode voor de nieuwe connector genereren vanuit de vRealize Automation-console. De activeringscode wordt gebruikt om de verbinding tussen Beheer van directory's en de connector in te stellen.

U kunt een afzonderlijke connector of een connectorcluster configureren. Als u een connectorcluster wilt gebruiken, herhaalt u deze procedure voor elke gewenste connector.

Voorwaarden

- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

1 Selecteer **Beheer > Beheer van directory's > Connectoren**.

2 Klik op **Connector toevoegen**.

3 Voer de naam van de nieuwe connector in het tekstvak **Naam connector** in.

4 Klik op **Activeringscode genereren**.

De activeringscode voor de connector verschijnt in het vak **Activeringscode connector**.

5 Kopieer de activeringscode bij de configuratie van de connector met behulp van het OVA-bestand.

6 Klik op **OK**.

Het OVA-bestand van de connector implementeren

Als u het OVA-bestand van de connector hebt gedownload, kunt u het implementeren met de VMware vSphere Client of vSphere Web Client.

U implementeert het OVA-bestand met behulp van de vSphere Client of de vSphere Web Client.

Voorwaarden

- 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 vereiste OVA-bestand voor het configureren van een connector van [VMware vRealize Automation Tools and SDK](#).

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 virtuele toepassing. Dit moet een unieke naam in de inventarismap zijn van maximaal 80 tekens. Namen zijn hoofdlettergevoelig. Selecteer een locatie voor de virtuele toepassing.
Host / Cluster	Selecteer de host of cluster waar de geïmplementeerde sjabloon wordt uitgevoerd.
Bronpool	Selecteer de bronpool.
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.
Netwerktoeewijzing	Wijs de netwerken in uw omgeving toe aan de netwerken van de OVF-sjabloon.
Eigenschappen	<ol style="list-style-type: none"> 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. <p>Belangrijk Als u een van deze vier adresvelden niet invult en geen hostnaam opgeeft, wordt DHCP gebruikt.</p> <p>U stelt DHCP in door de adresvelden leeg te laten.</p>
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 -toepassing, klikt u met de rechtermuisknop en selecteert u **Aan/uit > Inschakelen**.

De -toepassing wordt geïnitieerd. Op het tabblad **Console** kunt u de details bekijken. Wanneer de virtuele toepassing is geïnitieerd, 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.

Connectorinstellingen configureren

Als u het OVA-bestand van de connector hebt geïmplementeerd, moet u de installatiewizard uitvoeren om de toepassing te activeren en de beheerderswachtwoorden configureren.

Voorwaarden

- U hebt een activeringscode voor de connector gegenereerd.
- Zorg ervoor dat de connectortoepassing is ingeschakeld en dat u de connector-URL kent.
- Maak een lijst met wachtwoorden die worden gebruikt voor de connectorbeheerder, rootaccount en sshuser-account.

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 welkomspagina.

- 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
Toepassingsbeheerder	Maak het wachtwoord voor de toepassingsbeheerder. De gebruikersnaam is admin . U kunt deze naam niet wijzigen. Gebruik dit 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 admingebruiker moet minstens zes tekens lang zijn.
Rootaccount	De Connector-toepassing is geïnstalleerd op basis van een standaardhoofd wachtwoord 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**.
- 6 Als u een zelfondertekend certificaat gebruikt op de interne connector van vRealize Automation, kunt u het betreffende certificaat ophalen door de volgende opdracht uit te voeren op de vRealize Automation-toepassing: `cat /etc/apache2/server-cert.pem`

Selecteer het tabblad **SSL beëindigen op load balancer** en klik op de koppeling van / `horizon_workspace_rootca.pem`.

De activeringscode wordt gecontroleerd en de verbinding tussen de service en connectorinstantie wordt gemaakt. Daarmee is de configuratie van de connector 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.

Openbare certificeringsinstantie toepassen

Wanneer Beheer van directory's is geïnstalleerd, wordt een standaard SSL-certificaat gegenereerd. U kunt dit standaardcertificaat gebruiken voor testdoeleinden, maar voor een productieomgeving dient u commerciële SSL-certificaten te genereren en installeren.

Als Beheer van directory's naar een load balancer verwijst, wordt het SSL-certificaat toegepast op de load balancer.

U moet **Deze sleutel markeren als exporteerbaar** inschakelen wanneer u een certificaat importeert.

U hoeft alleen de CN, of de sitedomeinnaam van de certificaatautoriteit, op te geven als u een aanvraag voor certificaatondertekening voor een aangepast certificaat genereert.

Voorwaarden

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 Meld u op de volgende locatie aan als admingebruiker bij de beheerpagina van de toepassing van de connector:

`https://myconnector.mycompany:8443/cfg`

- 2 Klik in de beheerconsole op **Apparaatinstellingen**.

De configuratie van de virtual appliance is standaard geselecteerd.

- 3 Klik op **Configuraties beheren**.

- 4 Voer het wachtwoord van de admingebruiker voor de VMware Identity Manager-server in.

- 5 Selecteer **Certificaat installeren**.

- 6 Selecteer **Aangepast certificaat** op het tabblad SSL beëindigen op **Identity Manager-toepassing**.

- 7 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.

- 8 Plak de persoonlijke sleutel in het tekstvak Persoonlijke sleutel. Kopieer alle inhoud vanaf ----BEGIN RSA PRIVATE KEY tot en met ---END RSA PRIVATE KEY.

- 9 Klik op **Opslaan**.

Voorbeeld: Voorbeelden van certificaten

Voorbeeld van certificaatketen

-----BEGIN CERTIFICATE-----

jiQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+

...

...

...

W53+O05j5xsxzDJfWr1lqBIFF/OkIYCPcyK1

Voorbeeld van certificaatketen

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

WdR9Vpg3WQT5+C3HU17bUOwvhp/rjIQvt90+

...

...

...

O05j5xsxzDJfWr1lqBIFF/OkIYCPW53+cyK1

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

dR9Vpg3WQTjIQvt9W5+C3HU17bUOwvhp/r0+

...

...

...

5j5xsxzDJfWr1lqW53+O0BIFF/OkIYCPcyK1

-----END CERTIFICATE-----

Voorbeeld van persoonlijke sleutel

-----BEGIN RSA PRIVATE KEY-----

jIQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+

...

...

...

1lqBIFFW53+O05j5xsxzDJfWr/OkIYCPcyK1

-----END RSA PRIVATE KEY-----

Een Workspace-identiteitsprovider maken

U moet een Workspace-identiteitsprovider maken voor een externe connector.

Voorwaarden

- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > Beheer van directory's > Identiteitsproviders**.
- 2 Selecteer **Identiteitsprovider toevoegen**.
- 3 Selecteer **Workspace-IdP maken**.
- 4 Geef een naam voor de nieuwe identiteitsprovider op in het veld **Naam van identiteitsprovider**.

- 5 Selecteer de directory voor de gebruikers die deze identiteitsprovider gebruiken.
De directory die u selecteert, bepaalt welke connectoren beschikbaar zijn voor de identiteitsprovider.
- 6 Selecteer de externe connector(en) die u hebt ingesteld voor de smartcardverificatie.

Opmerking Als de implementatie achter een load balancer wordt uitgevoerd, voert u de URL van de load balancer in.

- 7 Selecteer het netwerk dat toegang moet hebben tot de identiteitsprovider.
- 8 Klik op **Toevoegen**.

Certificaatverificatie en standaardregels voor toegangsbeleid configureren

U moet de externe connector met een Active Directory en domein configureren voor vRealize Automation.

Voorwaarden

Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > Beheer van directory's > Connectoren**.
- 2 Selecteer de gewenste connector in de kolom **Werker**.
De geselecteerde werker wordt weergegeven in het tekstvak **Naam werker** op het tabblad **Connectordetails** en het type connector in het tekstvak **Connectortype**.
- 3 Zorg ervoor dat de connector is gekoppeld aan de gewenste Active Directory door die directory op te geven in het tekstvak **Gekoppelde directory**.
- 4 Geef de juiste domeinnaam op in het tekstvak **Gekoppelde domeinen**.
- 5 Selecteer het tabblad **AuthAdapters** en schakel CertificateAuthAdapter in.
- 6 Configureer de gewenste certificaatverificatie voor uw implementatie.
Zie [Certificaatverificatie configureren voor Beheer van directory's](#).
- 7 Selecteer **Beheer > Beheer van directory's > Beleid**.
- 8 Klik op **Standaardbeleid bewerken**.
- 9 Voeg Certificaat toe als beleidsregel en stel dit in als eerste verificatiemethode.
Certificaat moet de eerste verificatiemethode zijn die in de beleidsregel wordt weergegeven. Anders mislukt certificaatverificatie.

Een Active Directory-koppeling maken met meerdere domeinen of forests

Als systeembeheerder moet u een Active Directory-koppeling met meerdere domeinen of forests configureren.

De procedure voor het configureren van een Active Directory-koppeling met meerdere domeinen of forests is nagenoeg hetzelfde. Voor een koppeling met meerdere forests is vertrouwen in twee richtingen vereist tussen alle van toepassing zijnde domeinen.

Voorwaarden

- Installeer een gedistribueerde vRealize Automation-implementatie met de juiste load balancers. Zie *vRealize Automation installeren*.
- Meld u bij vRealize Automation aan als **tenantbeheerder**.
- Configureer de juiste domeinen en Active Directory-forests voor uw implementatie.

Procedure

- 1 Selecteer **Beheer > Beheer van directory's > Directory's**.
- 2 Klik op **Directory toevoegen**.
- 3 Op de pagina Directory toevoegen geeft u een naam op voor de Active Directory-server in het tekstvak **Directorynaam**.
- 4 Selecteer **Active Directory (Geïntegreerde Windows-verificatie)** onder de kop **Directorynaam**.
- 5 Configureer de connector waarmee gebruikers uit de Active Directory worden gesynchroniseerd met de VMware Directories Management-directory in de sectie Directory synchroniseren en verifiëren.

Optie	Beschrijving
Connector voor synchronisatie	Selecteer de juiste connector die u voor uw systeem wilt gebruiken. Elke vRealize Automation-toepassing bevat een standaardconnector. Raadpleeg uw systeembeheerder als u hulp nodig hebt bij het kiezen van de juiste connector.
Verificatie	Klik op het juiste keuzerondje om aan te geven of de geselecteerde connector ook voor verificatie moet worden gebruikt.
Zoekkenmerken directory	Selecteer het juiste accountkenmerk dat de gebruikersnaam bevat.

Afhankelijk van de configuratie van uw implementatie moeten er één of meer connectoren beschikbaar zijn voor gebruik.

- 6** Geef de juiste verificatiegegevens voor het toevoegen van domeinen op in de tekstvakken **Domeinnaam**, **Gebruikersnaam van domeinbeheerder** en **Wachtwoord van domeinbeheerder**.

U kunt bijvoorbeeld het volgende opgeven: **Domeinnaam**: `hs.trcint.com`, **Gebruikersnaam van domeinbeheerder**: `devadmin`, **Wachtwoord van domeinbeheerder**: `xxxx`.

- 7** In het gedeelte **Details van bindingsgebruiker** geeft u de juiste verificatiegegevens voor Active Directory (Geïntegreerde Windows-verificatie) op om het synchroniseren van directory's te vereenvoudigen.

Optie	Beschrijving
UPN van gebruiker van de binding	Voer de UPN-naam (User Principal Name) in van de gebruiker die het domein kan verifiëren. Bijvoorbeeld: <code>gebruikersnaam@example.com</code> .
Wachtwoord van de bindings-DN	Voer het wachtwoord van de bindingsgebruiker in.

- 8** Klik op **Opslaan en Volgende**.

De pagina De domeinen selecteren wordt weergegeven, met de lijst met domeinen.


- 9** Klik op de juiste selectievakjes om de gewenste domeinen te selecteren voor uw systeemimplementatie.

- 10** Klik op **Volgende**.

- 11** Controleer of de kenmerknamen van de Directories Management-directory zijn toegewezen aan de juiste Active Directory-kenmerken.

Als de kenmerknamen van directory's op een onjuiste manier zijn toegewezen, selecteert u het juiste Active Directory-kenmerk in het vervolgkeuzemenu.


- 12** Klik op **Volgende**.


- 13** Klik op  om de groepen te selecteren die u vanuit Active Directory met de directory wilt synchroniseren.

Wanneer u een Active Directory-groep toewijst, worden leden van die groep die niet in de lijst Gebruikers staan, toegevoegd.

Opmerking Het systeem van gebruikersverificatie van Directories Management importeert gegevens uit Active Directory bij het toevoegen van groepen en gebruikers. De snelheid van het systeem wordt beperkt door de mogelijkheden van Active Directory. Als gevolg hiervan kunnen importbewerkingen lange tijd in beslag nemen, afhankelijk van het aantal groepen en gebruikers dat wordt toegevoegd. Om het risico op vertragingen of problemen te beperken, raden we u aan het aantal groepen en gebruikers te beperken tot de groepen en gebruikers die vereist zijn voor het gebruik van vRealize Automation. Als de prestaties van het systeem afnemen of fouten optreden, sluit u niet-vereiste toepassingen en zorgt u ervoor dat uw systeem voldoende geheugen toewijst aan Active Directory. Als de problemen zich blijven voordoen, kunt u de geheugentoewijzing voor Active Directory naar wens verhogen. Voor systemen met grote aantallen gebruikers en groepen moet u mogelijk de geheugentoewijzing voor Active Directory verhogen tot maximaal 24 GB.

- 14** Klik op **Volgende**.

- 15** Klik op  om aanvullende gebruikers toe te voegen. Voer ze bijvoorbeeld in als:
CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com.

Als u gebruikers wilt uitsluiten, klikt u op  om een filter te maken waarmee bepaalde typen gebruikers worden uitgesloten. U selecteert het gebruikerskenmerk waarop moet worden gefilterd, de queryregel en de waarde.

- 16** Klik op **Volgende**.

- 17** Controleer de pagina om na te gaan hoeveel gebruikers en groepen worden gesynchroniseerd met de directory.

Als u wijzigingen wilt aanbrengen in gebruikers en groepen, klikt u op een van de koppelingen Bewerken.

- 18** Klik op **Naar Workspace pushen** om het synchroniseren met de directory te starten.

Wat nu te doen

Groepen en gebruikersrollen configureren

Tenantbeheerders kunnen bedrijfspgroepen en aangepaste groepen maken en gebruikers toegangsrechten verlenen voor de vRealize Automation-console.

Rollen toewijzen aan directorygebruikers of -groepen

Tenantbeheerders verlenen toegangsrechten aan gebruikers door rollen toe te wijzen aan gebruikers of groepen.

U kunt gebruikers of groepen toestaan een pipeline te wijzigen en te activeren door rechten toe te wijzen aan de betreffende gebruikers en groepen. Wanneer u gebruikers en groepen de rol van Release Manager toewijst, kunnen ze de pipeline wijzigen en activeren. Wanneer u gebruikers en groepen de rol van Release Engineer toewijst, kunnen ze de pipeline activeren. Zie de handleiding *Werken met vRealize Code Stream* voor meer informatie.

Voorwaarden

Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > Gebruikers en groepen > Gebruikers en groepen directory**.
- 2 Typ een gebruikers- of groepsnaam in het vak **Zoeken** en druk op Enter.
Gebruik geen apenstaartje (@), backslash (\) of slash (/) in een naam. U kunt uw zoekopdracht optimaliseren door de volledige gebruikers- of groepsnaam in de notatie gebruiker@domein te typen.
- 3 Klik op de naam van de gebruiker of groep waaraan u rollen wilt toewijzen.
- 4 Selecteer één of meer rollen uit de lijst Voeg rollen aan deze gebruiker toe.
De lijst Machtigingen voor geselecteerde rollen geeft aan welke specifieke machtigingen u toekent.
- 5 (Optioneel) Klik op **Volgende** om meer informatie over de gebruiker of groep weer te geven.
- 6 Loop op de pagina **Details van gebruiker** op het tabblad **Algemeen** door de lijst met rollen om de gebruiker toe te voegen.
 - a Selecteer het vakje **Release Manager** om de gebruiker het recht te geven een pipeline aan te passen en te activeren.
 - b Selecteer het vakje **Release Engineer** om de gebruiker het recht te geven een pipeline te activeren.
- 7 Klik op **Bijwerken**.

Resultaten

Gebruikers die momenteel zijn aangemeld bij vRealize Automation, moeten zich afmelden en zich opnieuw aanmelden bij vRealize Automation voordat ze naar de pagina's kunnen navigeren waartoe ze toegang hebben gekregen.

Wat nu te doen

U kunt ook uw eigen aangepaste groepen maken met gebruikers en groepen in uw Active Directory-verbindingen. Zie [Een aangepaste groep maken](#).

Een aangepaste groep maken

Tenantbeheerders kunnen aangepaste groepen maken door andere aangepaste groepen, identiteitsarchiefgroepen en individuele identiteitsarchiefgebruikers te combineren. Aangepaste

groepen bieden meer gedetailleerde controle over de toegang in vRealize Automation dan bedrijfsgroepen die overeenkomen met een line of business, afdeling of andere organisatie-eenheid.

Met aangepaste groepen kunt u toegangsrechten voor taken op een meer gedetailleerde basis dan de standaardgroepstoewijzingen van vRealize Automation verlenen. U wilt bijvoorbeeld een aangepaste groep maken als u tenantbeheerders wilt toestaan om te bepalen wie specifieke machtigingen binnen de tenant heeft.

U kunt rollen toewijzen aan uw aangepaste groep, maar dit is niet in alle gevallen noodzakelijk. U kunt bijvoorbeeld een aangepaste groep met de naam Machinespecificatiegoedkeurders maken voor gebruik voor alle voorlopige machinegoedkeuringen. U kunt ook aangepaste groepen maken om aan uw bedrijfsgroepen toe te wijzen zodat u alle groepen op één plaats kunt beheren. In deze gevallen hoeft u geen rollen toe te wijzen.

Voorwaarden

Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

1 Selecteer **Beheer > Gebruikers en groepen > Aangepaste groepen**.

2 Klik op **Nieuw**.

3 Geef een naam voor de groep op in het tekstvak **Naam**.

Aangepaste groepsnamen mogen niet de combinatie van een puntkomma (;) gevolgd door een gelijkteken (=) bevatten.

4 (Optioneel) Geef een beschrijving op in het tekstvak **Beschrijving**.

5 Selecteer één of meer rollen uit de lijst Voeg rollen toe aan deze groep.

De lijst Machtigingen voor geselecteerde rollen geeft aan welke specifieke machtigingen u toekent.

6 Klik op **Volgende**.

7 Voeg gebruikers en groepen toe om uw aangepaste groep te maken.

a Typ een gebruikers- of groepsnaam in het vak **Zoeken** en druk op Enter.

Gebruik geen apenstaartje (@), backslash (\) of slash (/) in een naam. U kunt uw zoekopdracht optimaliseren door de volledige gebruikers- of groepsnaam in de notatie gebruiker@domein te typen.

b Selecteer de gebruiker of groep die u aan uw aangepaste groep wilt toevoegen.

8 Klik op **Voltooien**.

Resultaten

Gebruikers die momenteel zijn aangemeld bij vRealize Automation, moeten zich afmelden en zich opnieuw aanmelden bij vRealize Automation voordat ze naar de pagina's kunnen navigeren waartoe ze toegang hebben gekregen.

Just-in-time-gebruikers met aangepaste groepen en regels toevoegen

U kunt vRealize Automation-gebruikers toevoegen aan een implementatie zonder toegang tot Active Directory met behulp van just-in-time-gebruikersinrichting. Om just-in-time-inrichting aan te roepen voor nieuwe gebruikers, moet u regels maken om de van toepassing zijnde aangepaste groep te vullen.

Bij de eerste aanmelding wordt aan just-in-time-gebruikers groepslidmaatschap toegewezen dat dynamisch gebaseerd is op regels die u maakt op de pagina van de wizard Geavanceerd groepslidmaatschap. U kunt na de eerste aanmelding groepslidmaatschappen toewijzen op de gebruikelijke wijze. De tweede pagina van deze wizard bevat vier selectievakken voor het maken van regels op basis van verschillende criteria waarmee just-In-time-gebruikers worden gedefinieerd.

In het selectievak voor de eerste regel bijvoorbeeld kunt u Domein selecteren als een criterium en vervolgens selecteert u Komt overeen met in het tweede vak. Daarna voert u een domein in het vak voor de derde regel in. Met deze selecties maakt u een regel voor gebruikers op basis van just-in-time-lidmaatschap die gekoppeld zijn aan het opgegeven domein. Het derde selectievak is een invoervak voor vrije tekst en u kunt hier alle informatie invoeren die logisch gerelateerd is aan de selecties in de eerste twee selectievakken.

Opmerking Bij het configureren van just-in-time-gebruikers geeft de indelingstoewijzing voor `NameId` een kenmerk op waarmee een gebruiker op unieke wijze wordt geïdentificeerd. Dit kenmerk dat als `NameId` wordt gebruikt, moet uniek zijn voor de gebruiker en het kenmerk zelf moet worden opgegeven als onderdeel van de SAML-claim. Als u het kenmerk `NameId` of de waarde van `NameId` wijzigt, resulteert dit in een fout tijdens een aanmeldingspoging. Bijvoorbeeld: als u `NameId` toewijst aan de `SAMAccountName` van de gebruiker met de indeling `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` voor `NameID`, moet u de `SAMAccountName` ook afzonderlijk opgeven. De gebruikersnaam en de waarde van `SAMAccountName` mogen nooit worden gewijzigd.

vRealize Automation ondersteunt het gebruik van zoekopdrachten met jokertekens om just-in-time-gebruikers te configureren. Zie [Zoekopdrachten met jokertekens gebruiken voor just-in-time-gebruikers](#) voor meer informatie over het inschakelen en gebruiken van zoekopdrachten met jokertekens.

Opmerking U kunt meerdere regels maken om just-in-time-gebruikers toe te voegen op basis van verschillende criteria. Als u meerdere regels maakt, kunt u het regelselectievak

Overeenkomst gebruiken dat zich boven de belangrijkste regelvakken bevindt om op te geven of bij het toevoegen van just-in-time-gebruikers overeenkomst met een, meerdere of alle regels moet worden afgedwongen door vRealize Automation.

Procedure

- 1 Selecteer **Beheer > Gebruikers en groepen > Aangepaste groepen** en zoek naar een bestaande groep, bijvoorbeeld een groep die geschikt is voor de just-in-time-gebruikers.

Raadpleeg [Een aangepaste groep maken](#) voor meer informatie.

Klik in de groeprij, maar niet op de naam van de groep.

- 2 Klik op **Geavanceerd lidmaatschap**.

Indien gewenst kunt u individuele gebruikers toevoegen op de pagina Gebruikers toevoegen aan groep.

- 3 Klik op **Volgende** om de pagina met Groepsregels te bekijken.

- 4 Gebruik de overeenkomst- en regelselectievakken om een of meerdere regels te maken volgens uw gebruikersconfiguratie.

In de drie belangrijkste regelselectievakken onder het regelselectievak **Overeenkomst** klikt u op de pijlen-omlaag en voert u informatie in om vervolgkeuzelijsten te activeren waarmee u de gewenste regel kunt maken. Denk eraan dat u de tekens * en \ kunt gebruiken zoals hierboven beschreven.

- 5 Klik op **Volgende**.

- 6 Als u gebruikers van de groep wilt uitsluiten, zoek die gebruikers dan op en voeg ze toe aan de pagina Gebruikers uitsluiten van groep.

- 7 Klik op **Volgende**.

- 8 Controleer de groepsconfiguratie op de pagina Controleren, en klik op **Opslaan** om uw regels en configuratie op te slaan en te implementeren.

Resultaten

Just-in-time-gebruikers worden toegevoegd op basis van de door u gemaakte regels.

Zoekopdrachten met jokertekens gebruiken voor just-in-time-gebruikers

vRealize Automation ondersteunt regels voor het gebruik van zoekopdrachten met jokertekens om just-in-time-gebruikers te configureren.

Het gebruik van zoekopdrachten met jokertekens inschakelen

Het gebruik van zoekopdrachten met jokertekens is standaard niet ingeschakeld. Als u het gebruik van zoekopdrachten met jokertekens wilt inschakelen, moet u de juiste REST API-opdracht als volgt uitvoeren.

```
PUT:- https://{VRA_HOSTNAME}/SAAS/t/VSPHERE.LOCAL/jersey/manager/api/system/config/
isDynamicGroupWildcardEnabled
Content-Type: application/vnd.vmware.horizon.manager.systemconfigparameter+json
Accept: application/vnd.vmware.horizon.manager.systemconfigparameter+json
Authorization: HZN <token> (edited)
{
  "name": "isDynamicGroupWildcardEnabled",
```

```
"values": {
  "values": [
    "true"
  ]
}
```

Het HZN-token dat moet worden geleverd aan de API die de configuratie van jokertekens inschakelt, moet het token voor de beheerdersgebruiker in de vsphere.local-tenant zijn.

Kenmerken in de SAML-bevestiging toewijzen aan vRealize Automation-gebruikerskenmerken

De kenmerknaam in de SAML-bevestiging moet volledig overeenkomen met de kenmerknaam die is gedefinieerd op de pagina Gebruikerskenmerken van vRealize Automation. Het SAML-kenmerk dat de voornaam van de gebruiker bevat, moet de naam firstName zijn en de achternaam moet de naam lastName krijgen, enz. Als de identiteitsprovider aanvullende gebruikerskenmerken verzendt die niet zijn gedefinieerd op de pagina Gebruikerskenmerken, moet de beheerder die kenmerken toevoegen aan de pagina. Bijvoorbeeld: als de identiteitsprovider informatie over lidmaatschap van gebruikersgroepen in het SAML-kenmerk groups of memberof verzendt, moet u de gebruikerskenmerken groups of memberof in vRealize Automation toevoegen. Zorg ervoor dat u exacte hoofdletters gebruikt voor de kenmerknamen.

Opmerking Als u een tekenreeks zoals Group_Name wilt identificeren in het kenmerk met meerdere waarden dat lidmaatschap van een gebruikersgroep definieert, maakt u een jokerteken als *Group_Name*.

Voor de voorwaarden Overeenkomst en Geen overeenkomst kunt u een * als jokerteken gebruiken om de tekenpatroonovereenkomst in de regel op te nemen. Als u bijvoorbeeld <userinput>*Smi*</userinput> invoert, worden Smith, Smiley, Smirnoff en andere soortgelijke varianten geselecteerd, inclusief namen met smi in het midden. Als u alle exacte overeenkomsten voor een patroon wilt vinden, typt u een backslash (\) vóór de * wanneer u het patroon invoert. Bijvoorbeeld: met <userinput>*Adam* </userinput> vindt u alle namen die exact overeenkomen met het patroon Adam*. U kunt * overal in de woordgroep gebruiken, gevolgd en voorafgegaan door een willekeurig teken, inclusief * & *.

Een bedrijfsgroep maken

Bedrijfsgroepen worden gebruikt om een reeks services en bronnen te associëren met een reeks gebruikers. Deze groepen komen vaak overeen met een branche, afdeling of andere organisatorische eenheid. U kunt een bedrijfsgroep maken om reserveringen te configureren en gebruikers rechten te verlenen om servicecatalogusitems in te richten voor bedrijfsgroepleden.

Om meerdere gebruikers toe te voegen aan een bedrijfsgroepsrol, kunt u meerdere individuele gebruikers toevoegen of u kunt meerdere gebruikers tegelijk toevoegen door een identiteitsarchiefgroep of een aangepaste groep aan een rol toe te voegen. U kunt bijvoorbeeld een aangepaste groep Verkoopondersteuningsteam maken en die groep toevoegen aan de ondersteunende rol. U kunt ook bestaande gebruikersgroepen van een identiteitsarchief gebruiken. De gebruikers en groepen die u kiest moeten geldig zijn in het identiteitsarchief.

Ter ondersteuning van vCloud Director-integratie moeten dezelfde bedrijfsgroepleden in de vRealize Automation-bedrijfsgroep ook lid zijn van de vCloud Director-organisatie.

Nadat de tenantbeheerder de bedrijfsgroep heeft gemaakt, heeft de bedrijfsgroepbeheerder het recht om het e-mailadres van de beheerder en de leden te wijzigen. De tenantbeheerder kan alle opties wijzigen.

Voor deze procedure gaan we ervan uit dat IaaS is geïnstalleerd en geconfigureerd.

Voorwaarden

- Meld u bij vRealize Automation aan als **tenantbeheerder**.
- Als u machines die zijn gemaakt door leden van een bedrijfsgroep wilt toevoegen aan een bepaalde organisatie-eenheid van Active Directory, moet u het Active Directory-beleid configureren. Zie [Een Active Directory-beleid maken](#). U kunt het beleid toepassen wanneer u de bedrijfsgroep maakt of later toevoegen.
- Als u een standaardvoorvoegsel voor machines wilt opgeven voor de groep die is voorbereid op ingerichte machinenaamen, vraag dan een voorvoegsel aan bij een materiaalbeheerder. Zie [Machinevoorvoegsels configureren](#). Machinevoorvoegsels zijn niet van toepassing op XaaS-aanvragen.

Procedure

- 1 Selecteer **Beheer > Gebruikers en groepen > Bedrijfsgroepen**.
- 2 Klik op het pictogram **Nieuw** (+).
- 3 Configureer de gegevens voor de bedrijfsgroep.

Optie	Beschrijving
Naam	Voer de naam van de bedrijfsgroep in.
Beschrijving	Voer de beschrijving in.
E-mails met waarschuwing over de capaciteit verzenden naar	Voer een of meer e-mailadressen van gebruikers in die waarschuwingmeldingen over de capaciteit moeten ontvangen. E-mailaliasadressen worden niet ondersteund. Elk e-mailadres moet bij een specifieke gebruiker horen. Scheid meerdere vermeldingen van elkaar met een komma. Bijvoorbeeld JoeAdmin@mycompany.com,WeiMgr@mycompany.com .
Active Directory-beleid	Selecteer het Active Directory-standaardbeleid voor de bedrijfsgroep.

- 4 Voeg aangepaste eigenschappen toe.
- 5 Klik op **Volgende** om door te gaan naar de pagina Leden.

- 6 Voer een gebruikersnaam of een aangepaste gebruikersgroepnaam in en druk op Enter.

U kunt een of meer personen of aangepaste gebruikersgroepen toevoegen aan de bedrijfsgroep. U kunt de gebruikers nu opgeven of u kunt lege bedrijfsgroepen maken en deze later invullen.

Optie	Beschrijving
Rol groepsbeheerder	Kan rechten maken en goedkeuringsbeleid voor de groep toewijzen.
Ondersteunende rol	Kan servicecatalogusitems aanvragen en beheren namens de andere leden van de bedrijfsgroep.
Rol voor gedeelde toegang	Kan acties gebruiken en uitvoeren op bronnen die worden geïmplementeerd door andere bedrijfsgroepsleden.
Gebruikersrol	Kan servicecatalogusitems aanvragen waarvoor rechten zijn verleend.

- 7 Klik op **Volgende** om door te gaan naar de pagina Infrastructuur.

- 8 Configureer de standaardinfrastructuuropties.

Optie	Beschrijving
Standaardvoorvoegsel machine	<p>Selecteer een vooraf geconfigureerd machinevoorvoegsel voor de bedrijfsgroep.</p> <p>Dit voorvoegsel wordt gebruikt door machineblueprints. Als voor de blueprint een standaardvoorvoegsel wordt gebruikt en u dat hier niet opgeeft, wordt er een machinevoorvoegsel gemaakt op basis van de bedrijfsgroepnaam. Het wordt aanbevolen om een standaardvoorvoegsel op te geven. U kunt blueprints gewoon met specifieke voorvoegsels configureren of toestaan dat servicecatalogusgebruikers deze overschrijven wanneer ze een blueprint aanvragen.</p> <p>XaaS-blueprints maken geen gebruik van standaardmachinevoorvoegsels. Als u hier een voorvoegsel configureert en een XaaS-blueprint een recht verleent voor deze bedrijfsgroep, is dit niet van invloed op het inrichten van een XaaS-machine.</p>
Active Directory-container	<p>Geef een Active Directory-container op. Deze optie is alleen van toepassing op WIM-inrichting.</p> <p>Voor andere inrichtingsmethoden zijn extra configuratiestappen vereist om ingerichte machines samen te voegen in een AD-container.</p>

- 9 Klik op **Voltooien**.

Resultaten

Tenantbeheerders kunnen bronnen toewijzen aan uw bedrijfsgroep via het maken van een reservering. Bedrijfsgroepbeheerders kunnen rechten maken voor leden van de bedrijfsgroep.

Wat nu te doen

- Maak een reservering voor uw bedrijfsgroep op basis van de locatie waarop de bedrijfsgroep machines inricht. Zie [Een reserveringsscenario kiezen](#).

- Als de catalogusitems gepubliceerd zijn en de service bestaat, kunt u een recht maken voor de bedrijfsgroepleden. Zie [Gebruikers rechten verlenen voor services, catalogusitems en acties](#).

Problemen oplossen met trage weergave van groepsleden

De leden van de bedrijfsgroep of aangepaste groep worden traag weergegeven wanneer u de details van een groep wilt bekijken.

Probleem

Wanneer u gebruikersinformatie weergeeft in omgevingen met grote aantallen gebruikers, worden de namen van gebruikers traag in de gebruikersinterface geladen.

Oorzaak

De vertraging bij het laden van de namen vindt plaats in omgevingen met een grote Active Directory-omgeving.

Oplossing

- ◆ Om de belasting voor het ophalen van de gegevens te verkleinen, raden we u aan waar mogelijk Active Directory-groepen of aangepaste groepen te gebruiken in plaats van honderden afzonderlijke leden op naam toe te voegen.

Problemen oplossen met onverwachte vermeldingen voor het filteren

In de lijst met bedrijfsgroepen die wordt gebruikt voor het maken van filterselecties, worden onverwachte of dubbele vermeldingen weergegeven.

Probleem

U hebt wijzigingen aangebracht in bedrijfsgroepen onder **Beheer > Gebruikers en groepen > Bedrijfsgroepen**. Wanneer u op de pagina Implementaties probeert de implementaties per bedrijfsgroep te filteren, worden in de lijst met beschikbare bedrijfsgroepen die worden gefilterd, geen van uw wijzigingen of onverwachte resultaten, zoals dubbele bedrijfsgroepen, weergegeven.

Oorzaak

Het systeem controleert slechts één keer per 30 minuten op wijzigingen.

Oplossing

Wacht tot 30 minuten en vernieuw de lijst met bedrijfsgroepen voor filterselectie door de browser te vernieuwen.

Aanvullende tenants maken

Als systeembeheerder kunt u aanvullende vRealize Automation-tenants maken, zodat gebruikers toegang krijgen tot de vereiste toepassingen en bronnen voor het voltooien van werktaken.

Een tenant is een groep gebruikers met specifieke privileges die werken in een softwareinstantie. Een standaard vRealize Automation-tenant wordt meestal gemaakt tijdens systeeminstallatie en de eerste configuratie. Hierna kunnen beheerders aanvullende tenants maken, zodat gebruikers zich kunnen aanmelden en hun werktaken kunnen voltooien. Beheerders kunnen zoveel tenants maken als vereist voor gebruik van het systeem. Bij het maken van tenants moeten beheerders basisconfiguratiegegevens opgeven, zoals de naam, de aanmeldings-URL, lokale gebruikers en beheerders. Na het configureren van deze basisgegevens voor de tenant, moet de tenantbeheerder zich aanmelden en een correcte Active Directory-verbinding instellen met de functie Beheer van directory's, op het tabblad Beheer van de vRealize Automation-console. Daarnaast kunnen tenantbeheerders aangepaste merkvermelding toepassen op tenants.

Voorwaarden

Meld u aan bij de vRealize Automation-console als **systeembeheerder**.

Procedure

1 (Optioneel) Tenantinformatie opgeven

Als u een nieuwe tenant configureert, moet u eerst opgeven onder welke naam u deze aan vRealize Automation wilt toevoegen en vervolgens de tenantspecifieke toegangs-URL maken.

2 (Optioneel) Lokale gebruikers configureren

De vRealize Automation-systeembeheerder moet lokale gebruikers configureren voor elke toepasselijke tenant.

3 (Optioneel) Beheerders aanstellen

U kunt een of meer tenantbeheerders en IaaS-beheerders aanstellen uit de identiteitsarchieven die u voor een tenant hebt geconfigureerd.

Tenantinformatie opgeven

Als u een nieuwe tenant configureert, moet u eerst opgeven onder welke naam u deze aan vRealize Automation wilt toevoegen en vervolgens de tenantspecifieke toegangs-URL maken.

Voorwaarden

Meld u aan bij de vRealize Automation-console als **systeembeheerder**.

Procedure

- 1 Selecteer **Beheer > Tenants**.
- 2 Klik op het pictogram **Nieuw** (+).
- 3 Geef een naam op in het tekstvak **Naam**.
- 4 (Optioneel) Geef een beschrijving op in het tekstvak **Beschrijving**.

- 5 Voer een unieke id voor de tenant in in het tekstvak **URL-naam**.

Dit URL-token wordt gebruikt om een tenantspecifieke id toe te voegen aan de URL van de vRealize Automation-console.

Voer bijvoorbeeld **mytenant** in om de URL `https://vrealize-appliance-hostname.domain.name/vcac/org/mytenant` te maken.

Opmerking In vRealize Automation 7.0 en 7.1 mag u alleen kleine letters gebruiken voor de URL van de tenant.

- 6 (Optioneel) Voer een e-mailadres in in het tekstvak **E-mail contactpersoon**.

- 7 Klik op **Indienen en volgende**.

Lokale gebruikers configureren

De vRealize Automation-systeembeheerder moet lokale gebruikers configureren voor elke toepasselijke tenant.

Nadat een beheerder de algemene informatie voor een tenant heeft opgegeven, wordt het tabblad Lokale gebruikers actief. De beheerder kan nu gebruikers toewijzen die toegang hebben tot de tenant. Wanneer tenantconfiguratie is voltooid, kunnen lokale tenantgebruikers zich aanmelden bij hun respectievelijke tenants om werktaken te voltooien.

Opmerking Nadat u een gebruiker hebt toegevoegd, kunt u de configuratie van deze gebruiker niet meer wijzigen. Als u iets moet wijzigen in de gebruikersconfiguratie, moet u de gebruiker verwijderen en opnieuw maken.

Procedure

- 1 Klik op de knop **Toevoegen** op het tabblad Lokale gebruikers.
- 2 Voer de voor- en achternaam van de gebruikers in de velden **Voornaam** en **Achternaam** van het dialoogvenster Details van gebruiker in.
- 3 Voer het e-mailadres van de gebruiker in het veld **E-mail** in.
- 4 Voer de gebruikers-id en het wachtwoord voor de gebruiker in de velden **Gebruikersnaam** en **Wachtwoord** in.
- 5 Klik op de knop **Toevoegen**.
- 6 Herhaal deze stappen voor alle vereiste lokale gebruikers van de tenant.

Resultaten

De opgegeven lokale gebruikers worden voor de tenant aangemaakt.

Beheerders aanstellen

U kunt een of meer tenantbeheerders en IaaS-beheerders aanstellen uit de identiteitsarchieven die u voor een tenant hebt geconfigureerd.

Tenantbeheerders zijn verantwoordelijk voor het configureren van tenantspecifieke merkvermelding, evenals het beheren van identiteitsarchieven, gebruikers, groepen, rechten en gedeelde blueprints in de context van hun tenant. IaaS-beheerders zijn verantwoordelijk voor het configureren van endpoints voor infrastructuurbronnen in IaaS, het aanstellen van materiaalbeheerders en het controleren van IaaS-logboeken.

Voorwaarden

- Voordat u IaaS-beheerders aanstelt, moet u IaaS installeren. Zie *vRealize Automation installeren* voor meer informatie over het installeren van IaaS.

Procedure

- 1 Voer de naam van een gebruiker of groep in in het zoekvak **Tenantbeheerders** en druk op Enter.

Voor snellere resultaten voert u de volledige gebruikers- of groepsnaam in, bijvoorbeeld myAdmins@mycompany.domain. Herhaal deze stap om aanvullende tenantbeheerders aan te duiden.

- 2 Als u IaaS hebt geïnstalleerd, voert u de naam van een gebruiker of groep in in het zoekvak **IaaS-beheerders** en drukt u op Enter.

Voor snellere resultaten voert u de volledige gebruikers- of groepsnaam in, IaaSAdmins@mycompany.domain. Herhaal deze stap om aanvullende infrastructuurbeheerders aan te duiden.

- 3 Klik op **Toevoegen**.

Een tenant verwijderen

De systeembeheer kan ongewenste tenants uit vRealize Automation verwijderen.

Als u een tenant verwijdert, wordt deze direct uit de vRealize Automation-interface verwijderd. Het kan echter enige uren duren voordat de tenant volledig uit uw implementatie is verwijderd. Als u een tenant verwijdert en een andere tenant met dezelfde URL wilt maken, moet u na de verwijdering enkele uren wachten voordat u de nieuwe tenant maakt.

Voorwaarden

Meld u aan bij de vRealize Automation-console als **systeembeheerder**.

Procedure

- 1 Selecteer **Beheer > Tenants**.
- 2 Selecteer de tenant die u wilt verwijderen.

Klik niet op de naam van de tenant om deze te selecteren. In dat geval opent u de tenant om te bewerken.

- 3 Klik op **Verwijderen**.

Resultaten

De tenant wordt uit uw vRealize Automation-implementatie verwijderd.

Configureren van beveiligingsinstellingen voor multi-tenants

U kunt de beschikbaarheid van NSX-beveiligingsobjecten bepalen voor verschillende tenants in een omgeving met multi-tenants.

Wanneer u een NSX-beveiligingsobject maakt, kan de standaardbeschikbaarheid algemeen zijn, wat betekent dat deze beschikbaar is in alle tenants waarvoor het gekoppelde endpoint een reservering heeft, of verborgen voor alle gebruikers behalve de beheerder.

De beschikbaarheid van beveiligingsobjecten voor verschillende tenants is afhankelijk van de vraag of het gekoppelde endpoint een reservering of een reserveringsbeleid in de tenant heeft.

De manier waarop u de beschikbaarheid beheert van nieuwe beveiligingsobjecten in tenants en het gedrag dat wordt weergegeven in de bestaande beveiligingsobjecten ten opzichte van cross-tenants, na een upgrade naar deze release van vRealize Automation, wordt samengevat in het gerelateerde onderwerp [Tenanttoegang voor beveiligingsobjecten beheren in vRealize Automation](#).

Aangepaste merkvermelding configureren

Met vRealize Automation kunt u een aangepaste merkvermelding opnemen op de aanmeld- en toepassingspagina's van de tenant.

Een aangepaste merkvermelding kan betrekking hebben op tekst- en achtergrondkleuren, logo's, de bedrijfsnaam, het privacybeleid, copyrightvermeldingen en andere relevante informatie die u op de aanmeld- of toepassingspagina's van de tenant wilt weergeven.

Aangepaste merkvermelding voor aanmeldingspagina van tenant

U gebruikt de pagina Merkvermelding op aanmeldscherm om een aangepaste merkvermelding toe te passen op de vRealize Automation-aanmeldpagina's van de tenants.

U kunt de standaardmerkvermelding van vRealize Automation overnemen voor de aanmeldpagina van de tenants of een aangepaste merkvermelding definiëren op de pagina Merkvermelding op aanmeldscherm. Houd er rekening mee dat de aangepaste merkvermelding op dezelfde wijze wordt toegepast in al uw tenanttoepassingen.

Op deze pagina kunt u de merkvermelding voor de aanmeldpagina's van alle tenants instellen.

U ziet de huidig geïmplementeerde merkvermelding voor tenantaanmeldingen in het voorbeeldvenster van de pagina Merkvermelding op aanmeldscherm.

Opmerking Nadat u de nieuwe merkvermelding voor tenantaanmeldingspagina's hebt opgeslagen, kan het tot vijf minuten duren voordat deze op alle aanmeldpagina's zichtbaar is.

Voorwaarden

Als u een aangepast logo of andere afbeelding wilt gebruiken voor uw merkvermelding, moeten de bijbehorende bestanden voor u beschikbaar zijn.

Procedure

- 1 Meld u als systeem- of tenantbeheerder aan bij vRealize Automation.
- 2 Klik op het tabblad **Beheer**.
- 3 Selecteer **Merkvermelding > Merkvermelding op aanmeldscher**
- 4 Als u een logoafbeelding wilt toevoegen, klikt u op de knop **Uploaden** naast het veld Logo, navigeert u naar de gewenste map en selecteert u het afbeeldingsbestand van het logo.
- 5 Als u nog een afbeelding wilt toevoegen, klikt u op de knop **Uploaden** onder het veld Afbeelding (optioneel), navigeert u naar de gewenste map en selecteert u nog een afbeeldingsbestand.
- 6 Als u de achtergrondkleuren wilt aanpassen, geeft u de juiste hexadecimale codes op in de velden voor de **achtergrondkleur**, **impressumkleur**, **achtergrondkleur van aanmeldknop** en **voorggrondkleur van aanmeldknop**.

U kunt indien nodig een lijst met hexadecimale kleurcodes vinden op internet.

- 7 Klik op **Opslaan** om de instellingen toe te passen.

Resultaten

Tenantgebruikers zien de aangepaste merkvermelding nu op hun aanmeldpagina's.

Aangepaste merkvermelding voor tenanttoepassingen

U gebruikt de pagina Merkvermelding voor toepassing om een aangepaste merkvermelding toe te passen op de vRealize Automation-tenanttoepassingen.

U kunt de standaardmerkvermelding van vRealize Automation overnemen voor de toepassingen van uw gebruikers of een aangepaste merkvermelding definiëren op de pagina Merkvermelding voor toepassing. Op deze pagina kunt u de merkvermelding voor de titel en voettekst van de toepassingspagina's instellen. Houd er rekening mee dat de aangepaste merkvermelding op dezelfde wijze wordt toegepast in al uw gebruikerstoepassingen.

U ziet de huidig geïmplementeerde merkvermelding voor titels en voetteksten onder aan de pagina Merkvermelding voor toepassing.

Voorwaarden

Als u een aangepast logo wilt gebruiken voor uw merkvermelding, moet het bijbehorende afbeeldingsbestand beschikbaar zijn voor u.

Procedure

- 1 Meld u als systeem- of tenantbeheerder aan bij vRealize Automation.

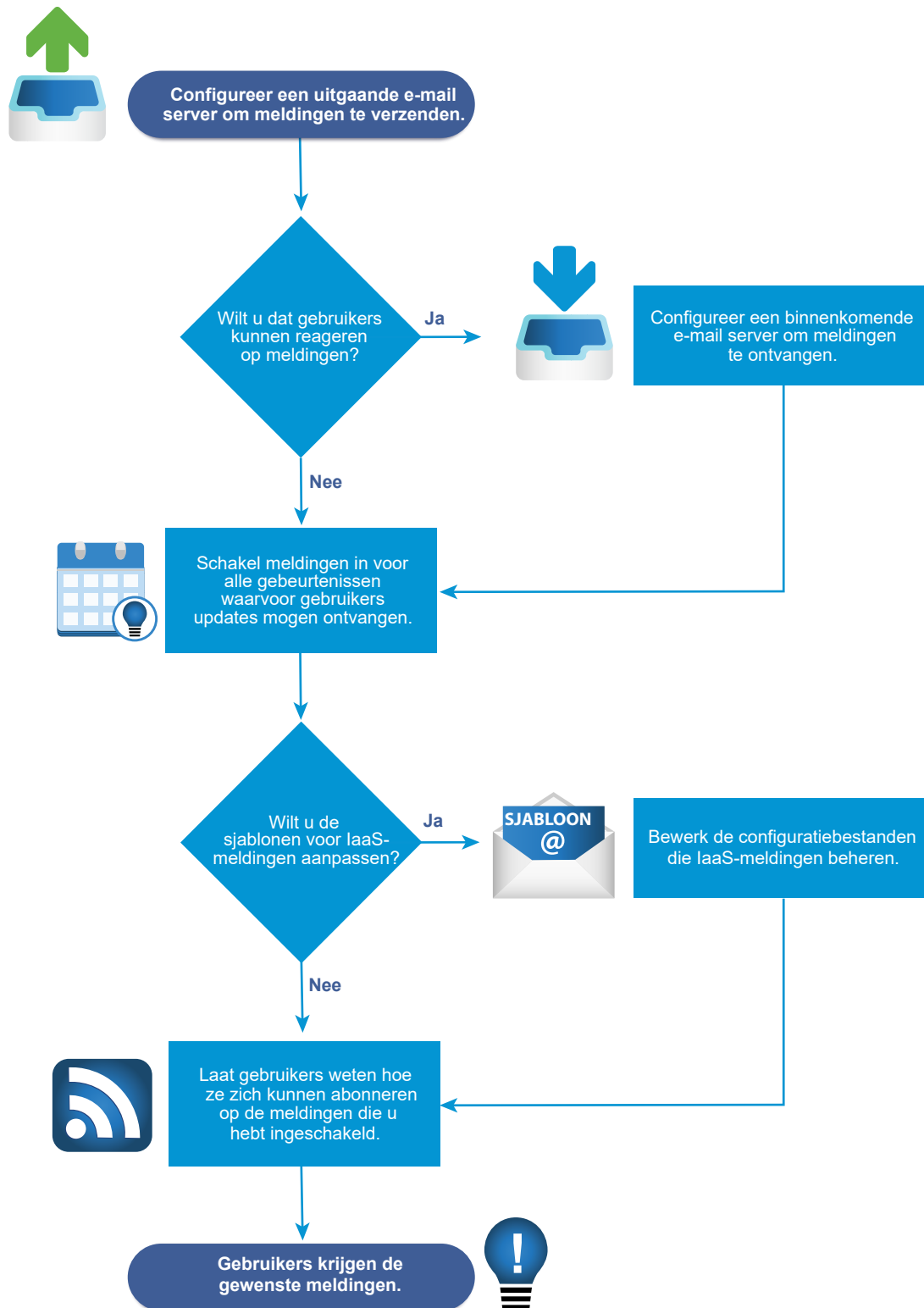
- 2 Klik op het tabblad **Beheer**.
- 3 Selecteer **Merkvermelding > Merkvermelding voor toepassing**
- 4 Klik op het tabblad **Titel** (als het nog niet actief is).
- 5 Als u de standaardmerkvermelding van vRealize Automation wilt gebruiken, klikt u op het selectievakje **Standaardwaarde gebruiken**.
- 6 Als u een aangepaste merkvermelding wilt implementeren, maakt u de gewenste keuzes in de velden op de tabbladen **Titel** en **Voettekst**.
 - a Klik op de knop **Bladeren** van het veld **Logo in titel**, navigeer naar de gewenste map en selecteer het afbeeldingsbestand van het logo.
 - b Typ de gewenste bedrijfsnaam in het veld **Bedrijfsnaam**.
De opgegeven naam voor het bedrijf verschijnt wanneer de gebruiker de muisaanwijzer op het logo plaatst.
 - c Typ de gewenste naam in het veld **Productnaam**.
De naam die u hier invoert, wordt weergegeven in de toepassingstitel naast het logo.
 - d Voer in het veld **Hexadecimale achtergrondkleur** de gewenste hexadecimale kleurcode voor de achtergrondkleur van de toepassingsperimeter in.
U kunt indien nodig een lijst met hexadecimale kleurcodes vinden op internet.
 - e Voer in het veld **Hexadecimale tekstkleur** de gewenste hexadecimale kleurcode voor de tekstkleur in.
U kunt indien nodig een lijst met hexadecimale tekstkleuren vinden op internet.
 - f Klik op **Volgende** om naar het tabblad Voettekst te gaan.
 - g Typ de gewenste tekst in het veld **Copyrightvermelding**.
 - h Typ in het veld **Koppeling naar privacybeleid** de koppeling naar de verklaring inzake het privacybeleid van uw bedrijf.
 - i Typ in het veld **Koppeling naar contactgegevens** de gewenste contactgegevens voor het bedrijf.
- 7 Klik op **Bijwerken** om de geconfigureerde merkvermelding te implementeren.

Resultaten

Tenantgebruikers zien de aangepaste merkvermelding nu op hun toepassingspagina's.

Checklist voor meldingen configureren

U kunt vRealize Automation configureren zodat gebruikers bij specifieke gebeurtenissen een melding ontvangen. Gebruikers kunnen zelf kiezen welke meldingen ze willen ontvangen, maar ze hebben daarbij alleen de keuze uit de gebeurtenissen waarvoor u een melding wilt triggeren.



De checklist voor het configureren van meldingen geeft een algemeen overzicht van de stappen die zijn vereist om meldingen te configureren en bevat koppelingen naar beslissingspunten of gedetailleerde instructies voor elke stap.

Tabel 2-10. Checklist voor meldingen configureren

Taak	Vereiste rol	Details
<input type="checkbox"/> Een server voor uitgaande e-mail configureren voor de verzending van meldingen.	<ul style="list-style-type: none"> ■ Systeembeheerders configureren algemene standaardserver. ■ Tenantbeheerders configureren servers voor hun tenants. 	<p>Zie Een tenantspecifieke uitgaande e-mailserver toevoegen als u voor de eerste maal een server voor uw tenant configureert. Zie Standaard uitgaande e-mailserver voor systeem overschrijven als u een algemene standaardserver moet overschrijven.</p> <p>Zie Een algemene uitgaande e-mailserver maken als u algemene standaardserver voor alle tenants wilt configureren.</p>
<input type="checkbox"/> (Optioneel) Een server voor inkomende e-mail configureren zodat gebruikers op de meldingen kunnen reageren en de taak kunnen voltooien.	<ul style="list-style-type: none"> ■ Systeembeheerders configureren algemene standaardserver. ■ Tenantbeheerders configureren servers voor hun tenants. 	<p>Zie Een tenantspecifieke binnenkomende e-mailserver toevoegen als u voor de eerste maal een server voor uw tenant configureert.</p> <p>Zie Standaard inkomende e-mailserver voor systeem overschrijven als u een algemene standaardserver moet overschrijven.</p> <p>Zie Een algemene binnenkomende e-mailserver maken als u een algemene standaardserver voor alle tenants wilt configureren.</p>
<input type="checkbox"/> (Optioneel) Opgeven wanneer een e-mailmelding moet worden verzonden voordat de vervaldatum van een machine wordt bereikt.	Systeembeheerder	<p>Zie De datum voor e-mailmeldingen voor het verlopen van machines aanpassen.</p>
<input type="checkbox"/> Selecteren welke vRealize Automation-gebeurtenissen een melding voor gebruikers triggeren. Gebruikers kunnen zich alleen inschrijven voor meldingen van gebeurtenissen waarvoor u een melding wilt triggeren.	Tenantbeheerder	<p>Zie Meldingen configureren.</p>

Tabel 2-10. Checklist voor meldingen configureren (vervolg)

Taak	Vereiste rol	Details
<input type="checkbox"/> (Optioneel) Sjablonen configureren voor meldingen die naar machine-eigenaren worden verzonden en specifiek betrekking hebben op gebeurtenissen met hun machine, zoals het einde van de leaseperiode.	Iedereen met toegang tot de map \Templates onder de vRealize Automation-serverinstallatiemap (doorgaans %SystemDrive%\Program Files x86\VMware\VCAC\Server) kan de sjablonen voor deze e-mailmeldingen configureren.	Zie Sjablonen voor automatische IaaS-e-mails configureren .
<input type="checkbox"/> Uw gebruikers worden automatisch geabonneerd op de geconfigureerde meldingen. U kunt, indien nodig, uw gebruikers instructies geven over hoe ze zich kunnen abonneren op de meldingen die u heeft ingeschakeld. Ze hebben de keuze om zich alleen in te schrijven voor meldingen die van belang zijn voor hun rol.	Alle gebruikers	Zie Abonneren op aankondigingen .

Algemene e-mailservers configureren voor meldingen

Tenantbeheerders kunnen e-mailservers beheren als deel van het configureren van meldingen voor hun eigen tenants. Als systeembeheerder kunt u algemene binnenkomende en uitgaande e-mailservers instellen die als systeemstandaarden aan alle tenants worden weergegeven. Als tenantbeheerders deze instellingen niet overschrijven voordat ze meldingen inschakelen, gebruikt vRealize Automation de algemeen geconfigureerde e-mailservers.

Een algemene binnenkomende e-mailserver maken

Systeembeheerders maken een algemene binnenkomende e-mailserver om binnenkomende e-mailmeldingen, zoals goedkeuringsantwoorden, af te handelen. U kunt slechts één binnenkomende server maken. Deze verschijnt als standaardoptie voor alle tenants. Als tenantbeheerders deze instellingen niet overschrijven voordat ze meldingen inschakelen, gebruikt vRealize Automation de algemeen geconfigureerde e-mailserver.

Voorwaarden

Meld u aan bij de vRealize Automation-console als **systeembeheerder**.

Procedure

- 1 Selecteer **Beheer > E-mailservers**.
- 2 Klik op het pictogram **Toevoegen** (+).

- 3 Selecteer **E-mail – Binnenkomend**.
- 4 Klik op **OK**.
- 5 Geef een naam op in het tekstvak **Naam**.
- 6 (Optioneel) Geef een beschrijving op in het tekstvak **Beschrijving**.
- 7 (Optioneel) Schakel het selectievakje **SSL** in om SSL voor de beveiliging te gebruiken.
- 8 Kies een serverprotocol.
- 9 Geef de naam van de server op in het tekstvak **Servernaam**.
- 10 Typ het poortnummer van de server in het tekstvak **Serverpoort**.
- 11 Typ de naam voor de map voor e-mails in het tekstvak **Mapnaam**.
Deze optie is alleen vereist als u het serverprotocol IMAP hebt gekozen.
- 12 Voer in het tekstvak **Gebruikersnaam** een gebruikersnaam in.
- 13 Voer een wachtwoord in het tekstvak **Wachtwoord** in.
- 14 Typ het e-mailadres waar vRealize Automation-gebruikers antwoorden naar kunnen sturen in het tekstvak **E-mailadres**.
- 15 (Optioneel) Selecteer **Verwijderen van server** als u alle verwerkte e-mails van de server wilt verwijderen die door de meldingsservice zijn opgehaald.
- 16 Kies of vRealize Automation automatische certificaten van de e-mailserver kan accepteren.
- 17 Klik op **Testverbinding**.
- 18 Klik op **Toevoegen**.

Een algemene uitgaande e-mailserver maken

Systeembeheerders maken een algemene uitgaande e-mailserver om uitgaande e-mailmeldingen af te handelen. U kunt slechts één uitgaande server maken. Deze verschijnt als standaardoptie voor alle tenants. Als tenantbeheerders deze instellingen niet overschrijven voordat ze meldingen inschakelen, gebruikt vRealize Automation de algemeen geconfigureerde e-mailserver.

Voorwaarden

Meld u aan bij de vRealize Automation-console als **systeembeheerder**.

Procedure

- 1 Selecteer **Beheer > E-mailservers**.
- 2 Klik op het pictogram **Toevoegen** (+).
- 3 Selecteer **E-mail – Uitgaand**.
- 4 Klik op **OK**.
- 5 Geef een naam op in het tekstvak **Naam**.

- 6 (Optioneel) Geef een beschrijving op in het tekstvak **Beschrijving**.
- 7 Geef de naam van de server op in het tekstvak **Servernaam**.
- 8 Kies een coderingsmethode.
 - Klik op **SSL gebruiken**.
 - Klik op **TLS gebruiken**.
 - Klik op **Geen** om ongecodeerde berichten te verzenden.
- 9 Typ het poortnummer van de server in het tekstvak **Serverpoort**.
- 10 (Optioneel) Schakel het selectievakje **Vereist** in, als voor de server verificatie vereist is.
 - a Typ in het tekstvak **Gebruikersnaam** een gebruikersnaam.
 - b Typ een wachtwoord in het tekstvak **Wachtwoord**.
- 11 Typ het e-mailadres waardoor e-mails van vRealize Automation schijnbaar verzonden moeten zijn, in het tekstvak **Adres afzender**.

Dit e-mailadres hoort bij de door u opgegeven gebruikersnaam en het bijbehorende wachtwoord.
- 12 Kies of vRealize Automation automatische certificaten van de e-mailserver kan accepteren.
- 13 Klik op **Testverbinding**.
- 14 Klik op **Toevoegen**.

Een tenantspecifieke uitgaande e-mailserver toevoegen

Tenantbeheerders kunnen een uitgaande e-mailserver toevoegen om meldingen te verzenden voor het voltooiën van werkitens, zoals goedkeuringen.

Elke tenant kan slechts één uitgaande e-mailserver hebben. Als uw systeembeheerder al een algemene uitgaande e-mailserver heeft geconfigureerd, gaat u naar [Standaard uitgaande e-mailserver voor systeem overschrijven](#).

Voorwaarden

- Meld u bij vRealize Automation aan als **tenantbeheerder**.
- Als de e-mailserver verificatie vereist, moet de opgegeven gebruiker zich in een identiteitsarchief en de bedrijfsgroep bevinden.

Procedure

- 1 Selecteer **Beheer > Meldingen > E-mailservers**.
- 2 Klik op het pictogram **Toevoegen** (+).
- 3 Selecteer **E-mail – Uitgaand**.
- 4 Klik op **OK**.

- 5 Geef een naam op in het tekstvak **Naam**.
- 6 (Optioneel) Geef een beschrijving op in het tekstvak **Beschrijving**.
- 7 Geef de naam van de server op in het tekstvak **Servernaam**.
- 8 Kies een coderingsmethode.
 - Klik op **SSL gebruiken**.
 - Klik op **TLS gebruiken**.
 - Klik op **Geen** om ongecodeerde berichten te verzenden.
- 9 Typ het poortnummer van de server in het tekstvak **Serverpoort**.
- 10 (Optioneel) Schakel het selectievakje **Vereist** in, als voor de server verificatie vereist is.
 - a Typ in het tekstvak **Gebruikersnaam** een gebruikersnaam.
 - b Typ een wachtwoord in het tekstvak **Wachtwoord**.
- 11 Typ het e-mailadres waardoor e-mails van vRealize Automation schijnbaar verzonden moeten zijn, in het tekstvak **Adres afzender**.

Dit e-mailadres hoort bij de door u opgegeven gebruikersnaam en het bijbehorende wachtwoord.
- 12 Kies of vRealize Automation automatische certificaten van de e-mailserver kan accepteren.

Deze optie is alleen beschikbaar als u codering hebt ingeschakeld.
 - Klik op **Ja** om automatische certificaten te accepteren.
 - Klik op **Nee** om automatische certificaten te weigeren.
- 13 Klik op **Testverbinding**.
- 14 Klik op **Toevoegen**.

Een tenantspecifieke binnenkomende e-mailserver toevoegen

Tenantbeheerders kunnen een binnenkomende e-mailserver toevoegen zodat gebruikers kunnen reageren op meldingen voor het voltooien van werkitens, zoals goedkeuringen.

Elke tenant kan slechts één binnenkomende e-mailserver hebben. Als uw systeembeheerder al een algemene binnenkomende e-mailserver heeft geconfigureerd, gaat u naar [Standaard inkomende e-mailserver voor systeem overschrijven](#).

Voorwaarden

- Meld u bij vRealize Automation aan als **tenantbeheerder**.
- Controleer of de opgegeven gebruiker in een identiteitsarchief en de bedrijfsgroep aanwezig is.

Procedure

- 1 Selecteer **Beheer > Meldingen > E-mailservers**.

- 2 Klik op het pictogram **Toevoegen** (+).
- 3 Selecteer **E-mail - Binnenkomend** en klik op **OK**.
- 4 Configureer de volgende opties voor binnenkomende e-mailservers.

Optie	Actie
Naam	Voer een naam in voor de binnenkomende e-mailserver.
Beschrijving	Voer een beschrijving in voor de binnenkomende e-mailserver.
Beveiliging	Schakel het selectievakje SSL gebruiken in.
Protocol	Kies een serverprotocol.
Servernaam	Voer de servernaam in.
Serverpoort	Voer het serverpoortnummer in.

- 5 Typ de naam voor de map voor e-mails in het tekstvak **Mapnaam**.
Deze optie is alleen vereist als u het serverprotocol IMAP hebt gekozen.
- 6 Voer in het tekstvak **Gebruikersnaam** een gebruikersnaam in.
- 7 Voer een wachtwoord in het tekstvak **Wachtwoord** in.
- 8 Typ het e-mailadres waar vRealize Automation-gebruikers antwoorden naar kunnen sturen in het tekstvak **E-mailadres**.
- 9 (Optioneel) Selecteer **Verwijderen van server** als u alle verwerkte e-mails van de server wilt verwijderen die door de meldingsservice zijn opgehaald.
- 10 Kies of vRealize Automation automatische certificaten van de e-mailserver kan accepteren.
Deze optie is alleen beschikbaar als u codering hebt ingeschakeld.
 - Klik op **Ja** om automatische certificaten te accepteren.
 - Klik op **Nee** om automatische certificaten te weigeren.
- 11 Klik op **Testverbinding**.
- 12 Klik op **Toevoegen**.

Standaard uitgaande e-mailserver voor systeem overschrijven

Als de systeembeheerder een standaard uitgaande e-mailserver voor het systeem heeft geconfigureerd, kan de tenantbeheerder deze algemene instelling overschrijven.

Voorwaarden

Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > Meldingen > E-mailservers**.
- 2 Selecteer de uitgaande e-mailserver.

- 3 Klik op **Alles overschrijven**.
- 4 Geef een naam op in het tekstvak **Naam**.
- 5 (Optioneel) Geef een beschrijving op in het tekstvak **Beschrijving**.
- 6 Geef de naam van de server op in het tekstvak **Servernaam**.
- 7 Kies een coderingsmethode.
 - Klik op **SSL gebruiken**.
 - Klik op **TLS gebruiken**.
 - Klik op **Geen** om ongecodeerde berichten te verzenden.
- 8 Typ het poortnummer van de server in het tekstvak **Serverpoort**.
- 9 (Optioneel) Schakel het selectievakje **Vereist** in, als voor de server verificatie vereist is.
 - a Typ in het tekstvak **Gebruikersnaam** een gebruikersnaam.
 - b Typ een wachtwoord in het tekstvak **Wachtwoord**.
- 10 Typ het e-mailadres waardoor e-mails van vRealize Automation schijnbaar verzonden moeten zijn, in het tekstvak **Adres afzender**.

Dit e-mailadres hoort bij de door u opgegeven gebruikersnaam en het bijbehorende wachtwoord.
- 11 Kies of vRealize Automation automatische certificaten van de e-mailserver kan accepteren.

Deze optie is alleen beschikbaar als u codering hebt ingeschakeld.
 - Klik op **Ja** om automatische certificaten te accepteren.
 - Klik op **Nee** om automatische certificaten te weigeren.
- 12 Klik op **Testverbinding**.
- 13 Klik op **Toevoegen**.

Standaard inkomende e-mailserver voor systeem overschrijven

Als de systeembeheerder een standaard inkomende e-mailserver voor het systeem heeft geconfigureerd, kunnen tenantbeheerders deze algemene instelling overschrijven.

Voorwaarden

Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > Meldingen > E-mailservers**.
- 2 Selecteer de inkomende e-mailserver in de tabel E-mailservers.
- 3 Klik op **Alles overschrijven**.

- 4 Voer de volgende opties in voor de inkomende e-mailserver.

Optie	Actie
Naam	Voer de naam in van de inkomende e-mailserver.
Beschrijving	Voer een beschrijving in voor de binnenkomende e-mailserver.
Beveiliging	Schakel het selectievakje SSL in om SSL voor de beveiliging te gebruiken.
Protocol	Kies een serverprotocol.
Servernaam	Voer de servernaam in.
Serverpoort	Voer het serverpoortnummer in.

- 5 Typ de naam voor de map voor e-mails in het tekstvak **Mapnaam:**.
Deze optie is alleen vereist als u het serverprotocol IMAP hebt gekozen.
- 6 Voer in het tekstvak **Gebruikersnaam** een gebruikersnaam in.
- 7 Voer een wachtwoord in het tekstvak **Wachtwoord** in.
- 8 Typ het e-mailadres waar vRealize Automation-gebruikers antwoorden naar kunnen sturen in het tekstvak **E-mailadres**.
- 9 (Optioneel) Selecteer **Verwijderen van server** als u alle verwerkte e-mails van de server wilt verwijderen die door de meldingsservice zijn opgehaald.
- 10 Kies of vRealize Automation automatische certificaten van de e-mailserver kan accepteren.
Deze optie is alleen beschikbaar als u codering hebt ingeschakeld.
- Klik op **Ja** om automatische certificaten te accepteren.
 - Klik op **Nee** om automatische certificaten te weigeren.
- 11 Klik op **Testverbinding**.
- 12 Klik op **Toevoegen**.

Standaard-mailservers voor systeem terugzetten

Tenantbeheerders die de standaardservers voor het systeem overschrijven kunnen de oorspronkelijke instellingen terugzetten.

Voorwaarden

Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > Meldingen > E-mailservers**.
- 2 Selecteer de e-mailserver die u wilt terugzetten.
- 3 Klik op **Terugzetten naar Alles**.
- 4 Klik op **Ja**.

Meldingen configureren

Elke gebruiker bepaalt of hij of zij meldingen wilt ontvangen, maar tenantbeheerders bepalen welke gebeurtenissen meldingen triggeren.

Voorwaarden

- Meld u bij vRealize Automation aan als **tenantbeheerder**.
- Controleer of een tenantbeheerder of systeembeheerder een uitgaande e-mailserver heeft geconfigureerd. Zie [Een tenantspecifieke uitgaande e-mailserver toevoegen](#).

Procedure

- 1 Selecteer **Beheer > Meldingen > Scenario's**.
- 2 Selecteer een of meer meldingen.
- 3 Klik op **Activeren**.

Resultaten

Gebruikers die zich in hun voorkeursinstellingen abonneren op meldingen, ontvangen nu de meldingen.

De datum voor e-mailmeldingen voor het verlopen van machines aanpassen

U kunt opgeven wanneer een e-mailmelding moet worden verzonden voordat de verloopdatum van een machine wordt bereikt.

U kunt de instelling wijzigen waarmee het aantal dagen vóór de verloopdatum van een machine wordt gedefinieerd waarop door vRealize Automation een e-mailmelding wordt verzonden. De gebruikers worden door de e-mail op de hoogte gesteld van het verlopen van de machine. De standaardinstelling is 7 dagen voorafgaand aan het verlopen van de machine.

Procedure

- 1 Meld u aan bij de vRealize Automation-server met verificatiegegevens met beheerderstoegang.
- 2 Ga naar het bestand `/etc/vcac/setenv-user` en open dit.
- 3 Voeg de volgende regel toe aan het bestand om het aantal dagen voorafgaand aan het verlopen van de machine op te geven, waarbij met 3 in dit voorbeeld 3 dagen voorafgaand aan het verlopen van de machine wordt bedoeld.

```
VCAC_OPTS="$VCAC_OPTS -Dlease.enforcement.prearchive.notification.days=3"
```

- 4 Start de vCAC-services op de virtual appliance opnieuw, zodat de volgende opdracht wordt uitgevoerd:

```
service vcac-server restart
```

Wat nu te doen

Als u werkt in een omgeving met een load balancer voor hoge beschikbaarheid, herhaalt u deze procedure voor alle virtual appliances in de omgeving voor hoge beschikbaarheid.

Sjablonen voor automatische IaaS-e-mails configureren

U kunt meldingse-mails zodanig configureren dat ze naar eigenaren van machines worden verzonden en informatie bieden over verschillende vRealize Automation-gebeurtenissen in verband met hun machines.

De gebeurtenissen die meldingen activeren, kunnen betrekking hebben op vervaldatum of naderende vervaldatum van archiveringsperioden en de lease van virtual machines.

Raadpleeg voor meer informatie over het configureren en het in- of uitschakelen van e-mailmeldingen van vRealize Automation de volgende blogartikelen en Knowledge Base-artikelen:

- [E-mails aanpassen in vRealize Automation](#)
- [E-mailsjablonen aanpassen in vRealize Automation \(2088805\)](#)
- [Voorbeelden voor het aanpassen van e-mailsjablonen in vRealize Automation \(2102019\)](#)

Abonneren op aankondigingen

Als uw beheerders aankondigingen hebben geconfigureerd, bent u automatisch geabonneerd. Aankondigingsgebeurtenissen kunnen onder meer de geslaagde voltooiing van een catalogusaanvraag of een vereiste goedkeuring omvatten.

Als u handmatig moet abonneren, kunt u uw meldingen inschakelen.

Voorwaarden

Meld u aan bij vRealize Automation.

Procedure

- 1 Klik op **Voorkeuren**.
- 2 Schakel het selectievakje **Ingeschakeld** in voor het protocol e-mail in de tabel Aankondigingen.
- 3 Klik op **Toepassen**.
- 4 Klik op **Sluiten**.

Een aangepast RDP-bestand maken ter ondersteuning van RDP-verbindingen voor ingerichte machines

Systeembeheerders kunnen een aangepast RDP-protocolbestand (Remote Desktop Protocol) maken dat IaaS-architecten gebruiken in blueprints voor het configureren van RDP-instellingen. U maakt het RDP-bestand en biedt architecten de volledige padnaam voor het bestand, zodat ze

het aan blueprints kunnen toevoegen. Vervolgens kunnen catalogusbeheerders gebruikers rechten verlenen voor de RDP-actie.

Opmerking Als u Internet Explorer gebruikt met Verbeterde beveiliging ingeschakeld, kunt u `.rdp`-bestanden niet downloaden.

Voorwaarden

Meld u aan bij de IaaS Manager Service als een beheerder.

Procedure

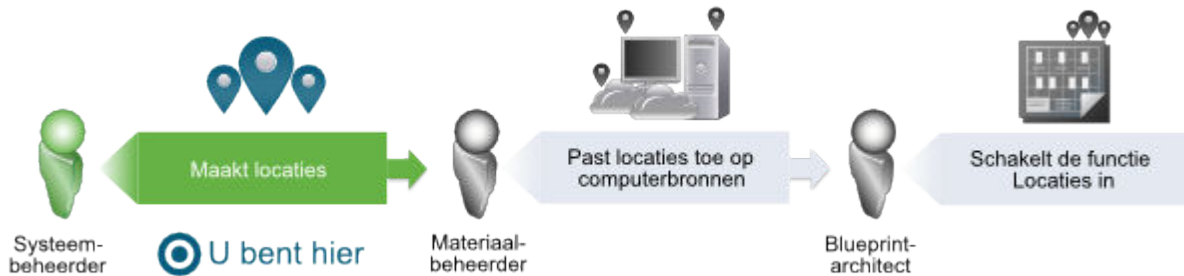
- 1 Stel uw huidige directory in op `<vRA_installation_dir>\Rdp`.
- 2 Kopieer het bestand `Default.rdp` en wijzig de naam in `Console.rdp` in dezelfde directory.
- 3 Open het bestand `Console.rdp` in een editor.
- 4 Voeg RDP-instellingen toe aan het bestand.
Bijvoorbeeld: **connect to console:i:1**.
- 5 Als u in een gedistribueerde omgeving werkt, meldt u zich aan als gebruiker met beheerdersrechten bij de IaaS-hostmachine waarop het Model Manager-websiteonderdeel is geïnstalleerd.
- 6 Kopieer het bestand `Console.rdp` naar de directory `vRA_installation_dir\Server\Website\Rdp`.
- 7 Voeg een individuele aangepaste eigenschap `VirtualMachine.Rdp.File` toe aan de blueprint.

Uw IaaS-architecten kunnen de aangepaste RDP-eigenschappen toevoegen aan Windows-machineblueprints. Vervolgens kunnen catalogusbeheerders gebruikers rechten verlenen voor de actie Verbinding maken via RDP. Zie [Ondersteuning voor RDP-verbinding toevoegen aan Windows-machineblueprints](#).

Scenario: datacenterlocaties toevoegen voor interregionale implementaties

Als systeembeheerder wilt u locaties opgeven voor de datacenters in Londen en Boston, zodat uw materiaalbeheerders de juiste locaties kunnen toepassen op computerbronnen in elk datacenter. Wanneer uw blueprintarchitecten blueprints maken, kunnen ze locatiefuncties inschakelen, zodat gebruikers de optie hebben om machines in te richten in Londen of Boston bij het invullen van aanvraagformulieren voor catalogusitems.

U hebt een datacenter in Londen en een datacenter in Boston en u wilt voorkomen dat gebruikers in Boston machines inrichten op de infrastructuur in Londen en omgekeerd. Om ervoor te zorgen dat uw gebruikers in Boston machines inrichten op uw infrastructuur voor Boston (en gebruikers in Londen de infrastructuur van Londen gebruiken), is het aan te raden gebruikers de juiste locatie te laten selecteren voor de inrichting wanneer ze machines aanvragen.



U kunt datacenterlocaties in het xml-bestand niet filteren op basis van de tenant of bedrijfsgroep. Wanneer u in een omgeving met meerdere tenants werkt, kunt u filteren op eigenschapsdefinities op basis van de tenant of bedrijfsgroep. Zie blogpost [How to use dynamic property definitions](#) (Gebruik van dynamische eigenschapsdefinities) voor informatie over het gebruik van eigenschapsdefinities.

Procedure

- 1 Meld u aan bij de IaaS-webserverhost met behulp van beheerderverificatiegegevens.
Dit is de machine waarop u het IaaS-websiteonderdeel hebt geïnstalleerd.
- 2 Bewerk het bestand `WebSite\XmlData\DataCenterLocations.xml` in de installatiedirectory voor Windows Server (doorgaans `%SystemDrive%\Program Files x86\VMware\VCAC\Server`).
- 3 Bewerk het gedeelte `CustomDataType` van het bestand om gegevensnaamvermeldingen te maken voor elke locatie.

```

<CustomDataType>
  <Data Name="London" Description="London datacenter" />
  <Data Name="Boston" Description="Boston datacenter" />
</CustomDataType>
  
```

- 4 Sla het bestand op en sluit het.
- 5 Start de Manager Service opnieuw op.
- 6 Als u meer dan een IaaS-webserverhost hebt, herhaalt u deze procedure op elke redundante instantie.

Resultaten

Uw materiaalbeheerder kan de juiste locatie toepassen op computerbronnen in elk datacenter. Zie [Scenario: een locatie toewijzen aan een computerbron voor interregionale implementaties](#).

Wat nu te doen

U kunt de eigenschap `Vrm.DataCenter.Location` toevoegen aan een blueprint of de optie **Locatie op verzoek weergeven** in de blueprint inschakelen, zodat de gebruiker een datacenterlocatie moet opgeven bij de aanvraag van een machine-inrichting.

vRealize Orchestrator configureren

vRealize Orchestrator is een automatiserings- en beheerengine die vRealize Automation uitbreidt voor ondersteuning van XaaS en die nog andere uitbreidingsmogelijkheden biedt. U kunt de vRealize Orchestrator-server configureren en gebruiken die vooraf in de vRealize Automation-appliance is geconfigureerd, of u kunt vRealize Orchestrator als een externe serverinstantie implementeren en die externe instantie associëren met vRealize Automation.

Met vRealize Orchestrator kunnen beheerders en architecten complexe automatiseringstaken ontwikkelen met behulp van het werkstroomontwerpprogramma en toegang krijgen tot de werkstromen van vRealize Automation en deze uitvoeren.

Met vRealize Orchestrator krijgt u toegang tot externe technologieën en toepassingen via vRealize Orchestrator-invoegtoepassingen en kunt u deze beheren.

Als u vRealize Automation configureert voor het gebruik van vRealize Orchestrator, kunnen vRealize Orchestrator-werkstromen worden gepubliceerd in de vRealize Orchestrator-servicecatalogus als onderdeel van het beheer van XaaS-blueprints.

Als u werkstromen wilt uitvoeren om het beheer van IaaS-machines uit te breiden, moet u vRealize Orchestrator als endpoint configureren.

Configuratieprivileges

Systeem- en tenantbeheerders kunnen vRealize Automation configureren voor het gebruik van een externe of de ingesloten vRealize Orchestrator-server.

Bovendien kunnen systeembeheerders ook bepalen welke werkstroommappen beschikbaar zijn voor elke tenant.

Tenantbeheerders kunnen de vRealize Orchestrator-invoegtoepassingen configureren als endpoint.

Rol	Privileges in verband met vRealize Orchestrator
Systeembeheerders	<ul style="list-style-type: none"> ■ Configureer de vRealize Orchestrator-server voor alle tenants. ■ Geef de standaard vRealize Orchestrator-werkstroommappen per tenant op.
Tenantbeheerders	<ul style="list-style-type: none"> ■ Configureer de vRealize Orchestrator-server voor de eigen tenant. ■ Voeg vRealize Orchestrator-invoegtoepassingen toe als endpoints.

De ingesloten vRealize Orchestrator-server configureren

De vRealize Automation-toepassing bevat een vooraf geconfigureerde instantie van vRealize Orchestrator.

Voorwaarden

Implementeer de vRealize Automation-toepassing. Voor meer informatie raadpleegt u *De vRealize Automation-appliance implementeren* in *vRealize Automation installeren*.

Procedure

- 1 Meld u aan bij de vRealize Automation-console als **systeembeheerder** of **tenantbeheerder**.
- 2 Selecteer **Beheer > VRO-configuratie > Serverconfiguratie**.
- 3 Klik op **Gebruik de standaard Orchestrator-server**.

Resultaten

Verbindingen met de ingesloten vRealize Orchestrator-server worden nu geconfigureerd. De map met **VCAC**-werkstromen en de verwante acties van het hulpprogramma worden automatisch geïmporteerd. De map met **VCAC > ASD**-werkstromen bevat werkstromen voor het configureren van endpoints en het maken van brontoewijzingen.

Meld u aan bij het vRealize Orchestrator Control Center

Als u de configuratie wilt bewerken van de standaard vRealize Orchestrator-instantie die is ingesloten in vRealize Automation, moet u zich aanmelden bij het vRealize Orchestrator Control Center.

De configuratieservices van de ingesloten vRealize Orchestrator-instantie worden automatisch gestart.

Opmerking U kunt controleren of de configuratie automatisch start door de opdracht `chkconfig vco-configurator` uit te voeren vanuit de opdrachtregelconsole van vRealize Orchestrator Appliance. Als de service `off` meldt, voert u de opdracht `chkconfig vco-configurator on` uit en start u de appliance opnieuw op.

Procedure

- 1 Maak verbinding met de vRealize Automation URL in een webbrowser.
- 2 Klik op **vRealize Orchestrator Control Center**.
U wordt omgeleid naar `https://vra-vd-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter`.
- 3 Voer de rootverificatiegegevens van uw vRealize Automation-omgeving in.

Aanmelden bij de vRealize Orchestrator-client

Om algemene beheertaken uit te voeren of werkstromen te bewerken en maken in de vRealize Orchestrator-standaardinstantie, moet u zich aanmelden bij de vRealize Orchestrator-client.

De vRealize Orchestrator-clientinterface is ontworpen voor ontwikkelaars met beheerdersrechten die werkstromen, acties en andere aangepaste elementen willen ontwikkelen.

Procedure

- 1 Maak verbinding met de vRealize Automation URL in een webbrowser.
- 2 Aanmelden bij de HTML5-gebaseerde vRealize Orchestrator-client.
 - a Klik op **vRealize Orchestrator Client**.
 - b Voer de gebruikersnaam en het wachtwoord van de vRealize Orchestrator-client in en klik op **Aanmelden**.

De verificatiegegevens bestaan uit de gebruikersnaam en het wachtwoord van de standaard tenantbeheerder.

- 3 Aanmelden bij de vRealize Orchestrator Legacy Client.

- a Klik op **vRealize Orchestrator Legacy Client**.
Het clientbestand wordt gedownload.
- b Klik op het gedownloade bestand en volg de prompts.
- c Selecteer in het venster **Beveiligingswaarschuwing** een optie om de certificaatwaarschuwing af te handelen.

De vRealize Orchestrator-client communiceert met de vRealize Orchestrator-server met behulp van een SSL-certificaat. Een vertrouwde certificeringsinstantie ondertekent het certificaat niet tijdens de installatie. U ontvangt een beveiligingswaarschuwing telkens wanneer u verbinding maakt met de vRealize Orchestrator-server.

Optie	Beschrijving
Doorgaan	Ga door met behulp van het huidige SSL-certificaat. Het waarschuwingsbericht wordt opnieuw weergegeven wanneer u opnieuw verbinding maakt met dezelfde vRealize Orchestrator-server of wanneer u probeert een werkstroom te synchroniseren met een externe vRealize Orchestrator-server.
Annuleren	Sluit het venster en stop het aanmeldingsproces.

- d Klik op **Uitvoeren**.
- e Typ het IP-adres of de domeinnaam van de vRealize Automation-appliance in het tekstvak **Hostnaam** en **443** als het standaard poortnummer op de aanmeldingspagina van vRealize Orchestrator.
Voer bijvoorbeeld *vrealize_automation_appliance_ip:443* in.
- f Voer de gebruikersnaam en het wachtwoord van de vRealize Orchestrator-client in en klik op **Aanmelden**.

De verificatiegegevens bestaan uit de gebruikersnaam en het wachtwoord van de standaard tenantbeheerder.

Wat nu te doen

Gebruik de vRealize Orchestrator-client om werkstromen te ontwikkelen en uit te voeren en exporteer uw inhoud naar andere vRealize Orchestrator-omgevingen met behulp van pakketten. Zie *De VMware vRealize Orchestrator Client gebruiken* en *Ontwikkelen met VMware vRealize Orchestrator*.

Een externe vRealize Orchestrator-server configureren

U kunt vRealize Automation instellen om een externe vRealize Orchestrator-server te gebruiken.

Systeembeheerders kunnen de standaard vRealize Orchestrator-server globaal voor alle tenants configureren. Tenantbeheerders kunnen de vRealize Orchestrator-server alleen voor hun tenants configureren.

Voor verbindingen met instanties van externe vRealize Orchestrator-servers is vereist dat het gebruikersaccount het recht Weergeven en Uitvoeren heeft in vRealize Orchestrator.

- Single Sign-On-verificatie. De gebruikersinformatie wordt doorgegeven aan vRealize Orchestrator met de XaaS-aanvraag en de gebruiker wordt het recht Weergeven en Uitvoeren verleend voor de aangevraagde werkstroom.
- Basisverificatie. Het geleverde gebruikersaccount moet lid zijn van een vRealize Orchestrator-groep met het recht Weergeven en Uitvoeren of moet lid zijn van de groep vcoadmins.

Voorwaarden

- Installeer en configureer een externe vRealize Orchestrator-toepassing. Zie *vRealize Orchestrator installeren en configureren* in de [vRealize Orchestrator-productdocumentatie](#).
- Meld u aan bij de vRealize Automation-console als **systeembeheerder** of **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > vRO-configuratie > Serverconfiguratie**.
- 2 Klik op **Gebruik een externe Orchestrator-server**.
- 3 Voer een naam in en desgewenst een beschrijving.
- 4 Voer het IP-adres of de DNS-naam in van de machine waarop de vRealize Orchestrator-server wordt uitgevoerd in het tekstvak **Host**.

Opmerking Als de externe vRealize Orchestrator is geconfigureerd voor gebruik in de clustermodus, voert u het IP-adres of de hostnaam van de virtuele server met de load balancer in die de clientaanvragen distribueert onder de vRealize Orchestrator-servers in het cluster.

- 5 Voer het poortnummer in voor communicatie met de externe vRealize Orchestrator-server in het tekstvak **Poort**.

8281 is het standaardpoortnummer voor vRealize Orchestrator.

6 Selecteer het verificatietype.

Optie	Beschrijving
Single Sign-On	Maakt verbinding met de vRealize Orchestrator-server met vCenter Single Sign-On. Deze optie is alleen van toepassing als u vRealize Orchestrator en vRealize Automation hebt geconfigureerd voor het gebruik van een gemeenschappelijke instantie van vCenter Single Sign-On.
Basis	Maakt verbinding met de vRealize Orchestrator-server met de gebruikersnaam en het wachtwoord dat u invoert in de tekstvakken Gebruikersnaam en Wachtwoord . Het account dat u opgeeft moet lid zijn van de vRealize Orchestrator-groep vcoadmins of moet lid zijn van een groep met het recht Weergeven en Uitvoeren.

7 Klik op **Testverbinding**.

8 Klik op **OK**.

9 Importeer het pakket `xaas.package`.

- Meld u als **root** aan bij de vRealize Automation-appliance.
- Zoek het pakket `xaas.package` in de map `/usr/lib/vcac/content/o11n/`.
- Importeer het pakket `xaas.package` in de externe client.

Resultaten

U hebt de verbinding met de externe vRealize Orchestrator-server geconfigureerd en de map met **VCAC**-werkstromen en de verwante acties van het hulpprogramma geïmporteerd. De map met **VCAC > ASD**-werkstromen bevat werkstromen voor het configureren van endpoints en het maken van brontoewijzingen.

Wat nu te doen

[Aanmelden bij de vRealize Orchestrator-client.](#)

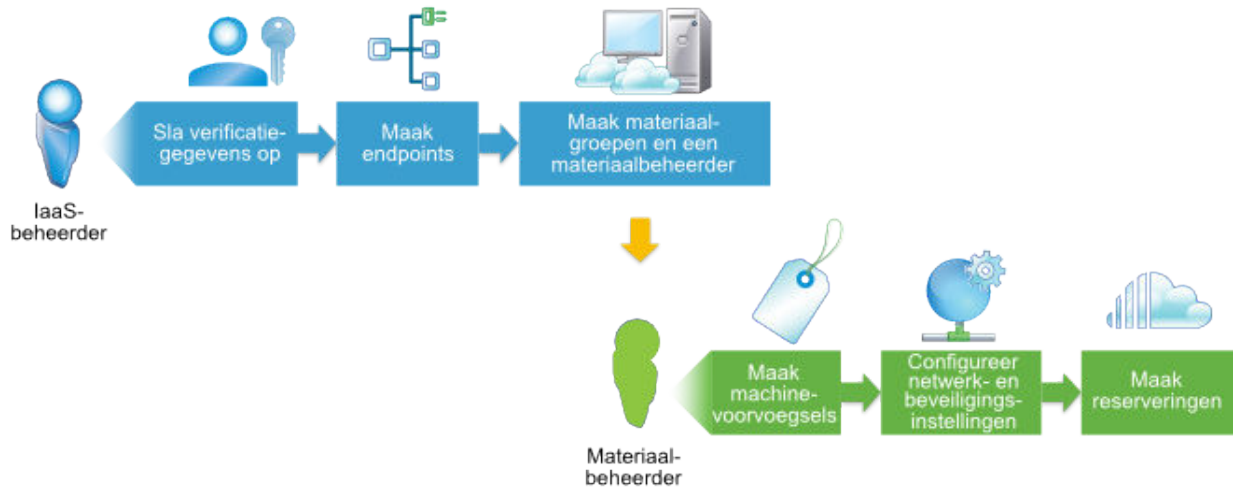
Bronnen configureren

U kunt bronnen zoals endpoints, reserveringen en netwerkprofielen configureren ten behoeve van de blueprintdefinitie en machine-inrichting met vRealize Automation.

Checklist voor het configureren van IaaS-bronnen

IaaS-beheerders en materiaalbeheerders configureren IaaS-bronnen om de bestaande infrastructuur met vRealize Automation te integreren en infrastructurele bronnen toe te wijzen aan vRealize Automation-bedrijfsgroepen.

De checklist voor het configureren van IaaS-bronnen biedt een algemeen overzicht van de vereiste stappen voor de IaaS-bronconfiguratie.



Tabel 2-11. Checklist voor het configureren van IaaS-bronnen

Taak	vRealize Automation Rol	Details
<input type="checkbox"/> Endpoints voor de infrastructuur maken om bronnen onder vRealize Automation-beheer te brengen.	IaaS-beheerder	Een endpointscenario kiezen.
<input type="checkbox"/> Een materiaalgroep maken waarin infrastructuurbronnen groepsgewijs worden geordend en een of meer beheerders van die bronnen aanwijzen als vRealize Automation-materiaalbeheerders.	IaaS-beheerder	Een materiaalgroep maken.
<input type="checkbox"/> Machinevoorvoegsels configureren voor de namen van machines die worden ingericht met behulp van vRealize Automation.	Materiaalbeheerder	Machinevoorvoegsels configureren.
<input type="checkbox"/> (Optioneel) Netwerkprofielen maken om netwerkinstellingen voor ingerichte machines te configureren.	Materiaalbeheerder	Een netwerkprofiel maken in vRealize Automation.
<input type="checkbox"/> Infrastructurele bronnen toewijzen aan bedrijfsgroepen door reserveringen en optioneel profielen voor reserveringen en opslagreserveringen te maken.	<ul style="list-style-type: none"> ■ IaaS-beheerder indien ook geconfigureerd als materiaalbeheerder ■ Materiaalbeheerder 	Reserveringen en reserveringsbeleid configureren.

Endpoints configureren

U kunt de endpoints die vRealize Automation toestemming geven om met uw infrastructuur te communiceren maken en configureren.

Endpointdefinities zijn ingedeeld in categorieën op basis van type:

- Cloud

De categorie cloud bevat de endpointtypen vCloud Air, vCloud Director, Amazon EC2 en OpenStack

- IPAM

Deze categorie is alleen zichtbaar als u een extern IPAM-endpointtype, zoals Infoblox IPAM, hebt geregistreerd in een vRealize Orchestrator-werkstroom.

- Beheer

Deze categorie bevat alleen het endpoint vRealize Operations Manager.

- Netwerk en beveiliging

Deze categorie bevat de endpointtypen Proxy en NSX.

Een proxyendpoint kan worden geassocieerd met een Amazon-, vCloud Air-, of vCloud Director- endpoint.

Een NSX-endpoint kan worden geassocieerd met een vSphere-endpoint.

- Orkestratie

Deze categorie bevat alleen het endpoint vRealize Orchestrator.

- Opslag

Deze categorie bevat het NetApp ONTAP-endpoint.

- Virtueel

De virtuele categorie bevat de endpointtypen vSphere, Hyper-V (SCVMM) en KVM (RHEV).

U kunt aanvullende endpointtypen configureren in vRealize Orchestrator en deze gebruiken met ondersteunde endpointtypen in vRealize Automation. U kunt ook endpoints importeren en exporteren met behulp van een programma.

Zie [Overwegingen bij het werken met bijgewerkte of gemigreerde endpoints](#) voor informatie over werken met endpoints na een upgrade of migratie.

Een endpointscenario kiezen

Kies een endpointscenario op basis van het doelendpointtype.

Zie [Naslaginformatie endpointinstellingen](#) voor meer informatie over beschikbare endpointinstellingen.

Tabel 2-12. Een endpointscenario kiezen

Endpoint	Meer informatie
vSphere	Zie Een vSphere-endpoint in vRealize Automation maken en koppelen aan NSX .
NSX	Zie Een NSX for vSphere-endpoint maken en associëren met een vSphere-endpoint in vRealize Automation of Een NSX-T-endpoint maken en associëren met een vSphere-endpoint in vRealize Automation .

Tabel 2-12. Een endpointscenario kiezen (vervolg)

Endpoint	Meer informatie
vCloud Air (abonnement of op aanvraag)	Zie Een vCloud Air-endpoint maken .
vCloud Director	Zie Een vCloud Director-endpoint maken .
vRealize Orchestrator	Zie Een vRealize Orchestrator-endpoint maken .
vRealize Operations	Zie Een vRealize Operations Manager-endpoint maken .
Derde IPAM-provider	Zie Een endpoint van een externe IPAM-provider maken .
Microsoft Azure	Zie Een Microsoft Azure-endpoint maken .
Puppet	Zie Een Puppet-endpoint maken .
Amazon	Zie Een Amazon-endpoint maken en Een Amazon-instantiotype toevoegen .
OpenStack	Zie Een OpenStack-endpoint maken .
Proxy	Een proxyendpoint maken en associëren met een cloud-endpoint
Hyper-V (SCVMM)	Zie Een Hyper-V (SCVMM)-endpoint maken .
KVM (RHEV)	Zie Naslaginformatie endpointinstellingen .
NetApp ONTAP	Zie Ruimtebesparende opslag voor virtuele inrichting en Naslaginformatie endpointinstellingen .
Hyper-V (stand-alone), XenServer of Xen Pool Master	Zie Een Hyper-V-, XenServer- of Xen Pool-endpoint maken .
Endpoints importeren	Zie Endpoints via een programma importeren of exporteren .

Naslaginformatie endpointinstellingen

Met endpointinstellingen kunt u locaties en verificatiegegevens voor toegang definiëren voor gegevensverzameling en implementatie van de servicecatalogus.

Tabblad Algemeen

De meeste vRealize Automation-endpoints hebben de volgende opties. Instellingen die uniek zijn voor een bepaald endpointtype zijn als zodanig aangeduid.

Tabel 2-13. Instellingen tabblad **Algemeen**

Instelling	Beschrijving
Naam	Voer de naam van het endpoint in.
Beschrijving	Voer de beschrijving van het endpoint in.

Tabel 2-13. Instellingen tabblad **Algemeen** (vervolg)

Instelling	Beschrijving
Adres	<p>Voer het adres van het endpoint in. Gebruik hiervoor de endpoint-specifieke adresindeling.</p> <ul style="list-style-type: none"> ■ In het geval van een KVM (RHEV)- of NetApp ONTAP-endpoint, moet het adres een van de volgende indelingen hebben: <ul style="list-style-type: none"> ■ <code>https://FQDN</code> ■ <code>https://IP-adres</code> <p>Bijvoorbeeld: <code>https://mycompany-kvmrhev1.mycompany.local</code> of <code>netapp-1.mycompany.local</code>.</p> ■ In het geval van een OpenStack-endpoint, moet het adres de indeling <code>https:// FQDN/powervc/openstack/ service</code> hebben. Bijvoorbeeld: <code>https://openstack.mijnbedrijf.com/powervc/openstack/admin</code>. ■ In het geval van een OpenStack-endpoint, moet het adres een van de volgende indelingen hebben. <ul style="list-style-type: none"> ■ <code>https://FQDN:500</code> ■ <code>https://IP-adres:500</code> ■ In het geval van een vSphere-endpoint, moet het adres de indeling <code>https://host/sdk</code> hebben. ■ In het geval van een NSX-endpoint, moet het adres de indeling <code>https://host</code> hebben. ■ In het geval van een vRealize Orchestrator endpoint, moet het adres gebruikmaken van het https-protocol en de volledig gekwalificeerde naam of het IP-adres van de vRealize Orchestrator-server en het poortnummer van vRealize Orchestrator, bijvoorbeeld <code>https://vrealize-automation-appliance-hostname:443/vco</code>. ■ In het geval van een vRealize Operations-endpoint, moet het adres de indeling <code>https://host/suite-api</code> hebben.
Geïntegreerde verificatiegegevens	<p>Als u uw vSphere geïntegreerde verificatiegegevens gebruikt, hoeft u geen gebruikersnaam en wachtwoord in te voeren.</p> <p>Deze instelling is alleen van toepassing op vSphere-endpoints.</p>
Gebruikersnaam	Voer de gebruikersnaam op beheerdersniveau in de endpoint-specifieke indeling in die u voor het endpoint hebt opgeslagen, zoals voorgesteld in de gebruikersinterface.
Wachtwoord	Voer het wachtwoord met beheerdersbevoegdheden in dat u hebt opgeslagen voor het endpoint.
OpenStack-project	<p>Voer een OpenStack-tenantnaam in.</p> <p>Deze instelling is alleen van toepassing op OpenStack-endpoints.</p>
Organisatie	<p>Als u een organisatiebeheerder bent, kunt u een vCloud Director-organisatienaam invoeren.</p> <p>Deze instelling is alleen van toepassing op vCloud Director.</p>
Toegangssleutel-id	<p>Voer de Amazon AWS-sleutel-id in.</p> <p>Deze instelling is alleen van toepassing op Amazon-endpoints.</p>
Geheime toegangssleutel	<p>Voer uw geheime toegangssleutel van Amazon AWS in.</p> <p>Deze instelling is alleen van toepassing op Amazon-endpoints.</p>

Tabel 2-13. Instellingen tabblad **Algemeen** (vervolg)

Instelling	Beschrijving
Poort	Voer de poortwaarde in voor het maken van een verbinding met het adres van het proxyendpoint. Deze instelling is alleen van toepassing op proxyendpoints.
Prioriteit	Voer een prioriteitswaarde in, in de vorm van een geheel getal groter dan of gelijk aan 1. Hoe lager de waarde, des te hoger de prioriteit. De prioriteitswaarde is geassocieerd met de ingesloten, aangepaste eigenschap VMware.VCenterOrchestrator.Priority . Deze instelling is alleen van toepassing op vRealize Orchestrator-endpoints.

Tabblad Eigenschappen

Alle endpointtypen hebben een prioriteitentabblad voor het vastleggen van aangepaste eigenschappen of groepen en instellingen van eigenschappen. Zie *Naslaggids voor aangepaste eigenschappen* voor voorbeelden van aangepaste eigenschappen voor specifieke endpointtypen.

Tabblad Associatie

U kunt een associatie met een NSX-endpoint of een proxyendpoint maken, afhankelijk van het endpoint dat u wilt associëren. U kunt een vSphere-endpoint associëren met een NSX-endpoint om NSX-instellingen toe te wijzen aan het vSphere-endpoint. U kunt ook een vCloud Air-, vCloud Director- of Amazon-endpoint associëren met een proxyendpoint om proxy-instellingen toe te wijzen aan het vCloud Air-, vCloud Director- of Amazon-endpoint.

Testverbinding

Met de bewerking Testverbinding kunt u de verificatiegegevens, het endpointadres van de host en het certificaat voor een vSphere-, NSX- of vRealize Operations Manager-endpoint valideren. Zie [Overwegingen bij het gebruik van Testverbinding](#).

Een vSphere-endpoint in vRealize Automation maken en koppelen aan NSX

U kunt vSphere-endpoints in vRealize Automation maken die met vCenter communiceren om computerbronnen te ontdekken, gegevens te verzamelen en machines in te richten. U kunt ook NSX-instellingen koppelen aan het vSphere-endpoint door aan een NSX for vSphere-endpoint, een of meer NSX-T-endpoints of beide NSX-endpointtypen te koppelen.

Als u een vSphere-endpoint aan NSX for vSphere- en NSX-T-endpoints koppelt, kunt u NSX for vSphere en NSX-T voor verschillende clusters configureren in één vCenter:

- Een IaaS-beheerder kan een vSphere-endpoint koppelen aan zowel een NSX for vSphere-endpoint als een NSX-T-endpoint.
- Een materiaalbeheerder kan een reservering voor NSX for vSphere of NSX-T maken, afhankelijk van de computerbron.
- Een blueprint-architect kan blueprints ontwerpen die ofwel NSX for vSphere-specifiek of NSX-T-specifiek zijn. Beide typen blueprints kunnen in dezelfde vCenter-omgeving worden geïmplementeerd.

U kunt een associatie maken tussen vSphere- en NSX-endpoints. Associaties omvatten:

- Eén vSphere-endpoint gekoppeld aan één NSX for vSphere-endpoint.
- Eén vSphere-endpoint gekoppeld aan meerdere NSX-T-endpoints.
- Eén NSX-T-endpoint gekoppeld aan meerdere vSphere-endpoints.
- Eén NSX for vSphere-endpoint gekoppeld aan één vSphere-endpoint.
- Eén vSphere-endpoint gekoppeld aan één NSX for vSphere-endpoint en één NSX-T-endpoint.

Wanneer een vSphere-endpoint is gekoppeld aan zowel een NSX for vSphere-endpoint als een NSX-T-endpoint, wordt het cluster beheerd door NSX for vSphere of door NSX-T. De NSX Manager wordt bepaald door vRealize Automation wanneer gegevens voor het endpoint worden verzameld en er een relatie tot stand wordt gebracht. U kunt het type NSX-platform zien dat een specifiek cluster beheert door de kolom **NSX-type** op de pagina **Computerbronnen** te controleren.

Voor informatie over het maken van NSX-endpoints die zijn gekoppeld aan een vSphere-endpoint, raadpleegt u [Een NSX for vSphere-endpoint maken en associëren met een vSphere-endpoint in vRealize Automation](#) of [Een NSX-T-endpoint maken en associëren met een vSphere-endpoint in vRealize Automation](#).

Zie [Overwegingen bij het gebruik van Testverbinding](#) voor informatie over het valideren van de endpointverbinding en het certificaatvertrouwen.

Als u een upgrade hebt uitgevoerd of bent gemigreerd van een vSphere-endpoint dat gebruikmaakte van een NSX Manager, wordt er een nieuw NSX-endpoint gemaakt dat een associatie bevat tussen het vSphere-endpoint waarvoor een upgrade is uitgevoerd en een nieuw NSX-endpoint.

Voorwaarden

- Meld u aan bij vRealize Automation als een **laaS-beheerder**.
- U moet een vSphere-proxyagent installeren om uw vSphere-endpoint te beheren. De naam van de agent en de naam van het endpoint moeten overeenkomen. Raadpleeg voor meer informatie over het installeren van de agent *vRealize Automation installeren*.
- Als u een vSphere-endpoint wilt gebruiken voor het implementeren van VM's van OVF-sjablonen, controleert u of uw verificatiegegevens de vSphere-bevoegdheid `VApp.Import` omvatten in de vCenter Server die is gekoppeld aan het endpoint.

Met de bevoegdheid `VApp.Import` kunt u een vSphere-machine implementeren met behulp van instellingen die worden geïmporteerd uit een OVF. Meer informatie over deze vSphere-bevoegdheid vindt u in de [vSphere SDK-documentatie](#).

Als het OVF wordt gehost op een website, raadpleegt u [Een proxyendpoint maken voor de website van de OVF-host](#).

- Als u aanvullende NSX-netwerk- en -beveiligingsinstellingen wilt configureren voor het vSphere-endpoint, maakt u een NSX for vSphere- of NSX-T-endpoint. U kunt een associatie maken met uw NSX-endpoint wanneer u een vSphere-endpoint maakt of bewerkt.

Procedure

- 1 Selecteer **Infrastructuur > Endpoints > Endpoints**.

- 2 Selecteer **Nieuw > Virtual > vSphere**.

- 3 Geef een naam op in het tekstvak **Naam**.

De naam moet overeenkomen met de endpointnaam die tijdens de installatie is opgegeven voor de vSphere-proxyagent. Als de naam niet overeenkomt, mislukt de gegevensverzameling.

- 4 (Optioneel) Geef een beschrijving op in het tekstvak **Beschrijving**.

- 5 Typ de URL voor de vCenter Server-instantie in het tekstvak **Adres**.

De URL moet van het type **https://hostname/sdk** of **https://IP_address/sdk** zijn.

Bijvoorbeeld **https://vsphereA/sdk**.

- 6 Voer uw vSphere-gebruikersnaam en -wachtwoord op beheerdersniveau in of gebruik uw geïntegreerde vSphere-verificatiegegevens.

Geef verificatiegegevens waarmee u bevoegd bent om aangepaste kenmerken te wijzigen.

De indeling van de gebruikersnaam is *domein\gebruikersnaam*.

Als u het serviceaccount van de vSphere-proxyagent wilt gebruiken om verbinding te maken met vCenter Server, selecteert u **Geïntegreerde verificatiegegevens gebruiken**.

Als u uw vSphere geïntegreerde verificatiegegevens gebruikt, hoeft u geen gebruikersnaam en wachtwoord in te voeren.

- 7 (Optioneel) Klik op **Eigenschappen** en voeg opgegeven aangepaste eigenschappen, eigenschapsgroepen of uw eigen eigenschapsdefinities voor het endpoint toe.

- 8 (Optioneel) Klik op **Associaties** en maak een associatie met een bestaand NSX for vSphere of NSX-T-endpoint om NSX-netwerkinstellingen en -beveiligingsinstellingen voor het endpoint te configureren.

U moet ten minste één NSX-endpoint hebben om een associatie te maken.

- 9 (Optioneel) Klik op **Testverbinding** om de verificatiegegevens, het endpointadres van de host en het certificaatvertrouwen te valideren. De actie controleert ook of de beheerservice en -agent actief zijn zodat gegevens voor het endpoint kunnen worden verzameld. De actie **OK** test op dezelfde voorwaarden.

De actie **Testverbinding** retourneert informatie over een van de volgende voorwaarden:

- Certificaatfout

Als het certificaat niet wordt gevonden, vertrouwd of is verlopen, wordt u gevraagd een vingerafdruk van het certificaat te accepteren. Als u de vingerafdruk niet accepteert, kunt u het endpoint wel opslaan maar mislukt de inrichting van de machine mogelijk.

- Agentfout

De gekoppelde vSphere-agent is niet gevonden. Voor een succesvolle test moet de agent actief zijn.

- Hostfout

Het opgegeven endpointadres is niet bereikbaar of de gekoppelde beheerservice is niet actief. Voor een succesvolle test moet de managementservice actief zijn.

- Verificatiegegevensfout

De opgegeven combinatie van gebruikersnaam en wachtwoord is ongeldig voor het endpoint op het opgegeven adres.

- Timeout

De testactie kan niet worden voltooid in de toegestane tijdsperiode van twee minuten.

Als de actie **Testverbinding** mislukt, kunt u het endpoint wel opslaan maar mislukt de inrichting van de machine mogelijk.

Als er een probleem is met een vertrouwd certificaat, bijvoorbeeld als het certificaat is verlopen, wordt u gevraagd een vingerafdruk van het certificaat te accepteren.

10 Klik op **OK** om het endpoint op te slaan.

De actie **OK** test op dezelfde voorwaarden als de actie **Testverbinding**. Als een van de vorige voorwaarden wordt gevonden, wordt een bericht geretourneerd. Als er kan worden opgeslagen, wordt de fout weergegeven op het scherm zodat u die kunt controleren.

Resultaten

vRealize Automation verzamelt gegevens van uw endpoint en ontdekt uw rekenbronnen.

Opmerking Wijzig de naam van vSphere-datacenters niet na de eerste gegevensverzameling, anders kan de inrichting mislukken.

Zie [Computerbronnen bekijken en gegevensverzameling uitvoeren](#) voor meer informatie.

Wat nu te doen

Voeg de computerbronnen van uw endpoint toe aan een materiaalgroep. Zie [Een materiaalgroep maken](#).

Een NSX for vSphere-endpoint maken en associëren met een vSphere-endpoint in vRealize Automation

U kunt een NSX for vSphere-endpoint maken en dit associëren met een bestaand vSphere-endpoint in vRealize Automation.

U kunt een NSX for vSphere-endpoint koppelen aan een vSphere-endpoint.

U kunt een associatie maken tussen vSphere- en NSX-endpoints. Associaties omvatten:

- Eén vSphere-endpoint gekoppeld aan één NSX for vSphere-endpoint.
- Eén vSphere-endpoint gekoppeld aan meerdere NSX-T-endpoints.
- Eén NSX-T-endpoint gekoppeld aan meerdere vSphere-endpoints.
- Eén NSX for vSphere-endpoint gekoppeld aan één vSphere-endpoint.
- Eén vSphere-endpoint gekoppeld aan één NSX for vSphere-endpoint en één NSX-T-endpoint.

Wanneer een vSphere-endpoint is gekoppeld aan zowel een NSX for vSphere-endpoint als een NSX-T-endpoint, wordt het cluster beheerd door NSX for vSphere of door NSX-T. De NSX Manager wordt bepaald door vRealize Automation wanneer gegevens voor het endpoint worden verzameld en er een relatie tot stand wordt gebracht. U kunt het type NSX-platform zien dat een specifiek cluster beheert door de kolom **NSX-type** op de pagina **Computerbronnen** te controleren.

Zie [Overwegingen bij het gebruik van Testverbinding](#) voor informatie over het valideren van de endpointverbinding en het certificaatvertrouwen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **IaaS-beheerder**.
- U moet een vSphere-proxyagent installeren om uw vSphere-endpoint te beheren en u moet exact dezelfde naam gebruiken voor uw endpoint en agent. Raadpleeg voor meer informatie over het installeren van de agent *vRealize Automation installeren*.
- Configureer uw NSX for vSphere-netwerkinstellingen. Zie [Instellingen van netwerk- en beveiligingsonderdelen configureren in vRealize Automation](#).
- [Een vSphere-endpoint in vRealize Automation maken en koppelen aan NSX](#).

Als voorbereiding op het gebruik van NSX-netwerk-, -beveiligings- en -load balancing-mogelijkheden in vRealize Automation, moet u, wanneer u NSX-beheerdersgegevens gebruikt, het NSX-beheerdersaccount gebruiken.

Procedure

- 1 Selecteer **Infrastructuur > Endpoints > Endpoints**.
- 2 Selecteer **Nieuw > Netwerk en beveiliging > NSX**.
- 3 Geef een naam op in het tekstvak **Naam**.
- 4 (Optioneel) Geef een beschrijving op in het tekstvak **Beschrijving**.
- 5 Typ de URL voor de NSX for vSphere-instantie in het tekstvak **Adres**.

De URL moet van het type **https://hostname** of **https://IP_address** zijn.

Bijvoorbeeld, **https://abx.nsx-manager.local/**.

- 6 Voer de gebruikersnaam en het wachtwoord met beheerdersbevoegdheden voor NSX in die zijn opgeslagen voor het NSX for vSphere-endpoint.
- 7 (Optioneel) Klik op **Eigenschappen** en voeg opgegeven aangepaste eigenschappen, eigenschapsgroepen of uw eigen eigenschapsdefinities voor het endpoint toe.
- 8 Klik op **Associaties** en selecteer een bestaand vSphere-endpoint om de NSX for vSphere-netwerkinstellingen en -beveiligingsinstellingen te koppelen aan een bestaand vSphere-endpoint.

U moet het vSphere-endpoint maken voordat u de associatie kunt maken.

Een vSphere-endpoint kan slechts aan één type netwerk- en beveiligingsplatform gekoppeld zijn: NSX for vSphere of NSX-T.

U kunt een NSX for vSphere-endpoint slechts aan één vSphere-endpoint koppelen. De associatiebeperking betekent dat u een universeel netwerk op aanvraag niet kunt inrichten en toevoegen aan vSphere-machines die op verschillende vCenters zijn ingericht.

Wanneer de associatie is voltooid, geeft de kolom Beschrijving op de pagina het associatietype van NSX for vSphere aan.

- 9 (Optioneel) Klik op **Testverbinding** om de verificatiegegevens, het endpointadres van de host en het certificaatvertrouwen te valideren. De actie controleert ook of de beheerservice en -agent actief zijn zodat gegevens voor het endpoint kunnen worden verzameld. De actie **OK** test op dezelfde voorwaarden.

De actie **Testverbinding** retourneert informatie over een van de volgende voorwaarden:

- **Certificaatfout**

Als het certificaat niet wordt gevonden, vertrouwd of is verlopen, wordt u gevraagd een vingerafdruk van het certificaat te accepteren. Als u de vingerafdruk niet accepteert, kunt u het endpoint wel opslaan maar mislukt de inrichting van de machine mogelijk.

- **Agentfout**

De gekoppelde vSphere-agent is niet gevonden. Voor een succesvolle test moet de agent actief zijn.

- **Hostfout**

Het opgegeven endpointadres is niet bereikbaar of de gekoppelde beheerservice is niet actief. Voor een succesvolle test moet de managementservice actief zijn.

- **Verificatiegegevensfout**

De opgegeven combinatie van gebruikersnaam en wachtwoord is ongeldig voor het endpoint op het opgegeven adres.

- **Timeout**

De testactie kan niet worden voltooid in de toegestane tijdsperiode van twee minuten.

Als de actie **Testverbinding** mislukt, kunt u het endpoint wel opslaan maar mislukt de inrichting van de machine mogelijk.

Als er een probleem is met een vertrouwd certificaat, bijvoorbeeld als het certificaat is verlopen, wordt u gevraagd een vingerafdruk van het certificaat te accepteren.

10 Klik op **OK** om het endpoint op te slaan.

De actie **OK** test op dezelfde voorwaarden als de actie **Testverbinding**. Als een van de vorige voorwaarden wordt gevonden, wordt een bericht geretourneerd. Als er kan worden opgeslagen, wordt de fout weergegeven op het scherm zodat u die kunt controleren.

Resultaten

vRealize Automation verzamelt gegevens van uw endpoint en ontdekt uw rekenbronnen.

Zie [Computerbronnen bekijken en gegevensverzameling uitvoeren](#) voor informatie over het uitvoeren van een gegevensverzameling voor bestaande endpoints na de eerste gegevensverzameling.

Wat nu te doen

Voeg de computerbronnen van uw endpoint toe aan een materiaalgroep. Zie [Een materiaalgroep maken](#).

Een NSX-T-endpoint maken en associëren met een vSphere-endpoint in vRealize Automation

U kunt een NSX-T-endpoint maken en dit associëren met een bestaand vSphere-endpoint in vRealize Automation.

vRealize Automation gebruikt basisverificatie om verbinding te maken met het NSX-T-endpoint.

Om fouttolerantie en hoge beschikbaarheid in implementaties mogelijk te maken, vertegenwoordigt elk NSX-T-datacentereindpunt een cluster van drie NSX-managers.

- vRealize Automation kan verwijzen naar een van de NSX-managers. Met deze optie ontvangt een NSX-manager de API-aanroepen van vRealize Automation.
- vRealize Automation kan verwijzen naar het virtuele IP-adres van het cluster. Met deze optie neemt een NSX-manager de controle over van het VIP. Die manager ontvangt de API-aanroepen van vRealize Automation. In geval van een storing neemt een ander knooppunt in het cluster de controle over van het VIP en ontvangt het de API-aanroepen van vRealize Automation.

Voor meer informatie over VIP-configuratie, zie *Configure a Virtual IP (VIP) Address for a Cluster* in de *NSX-T Data Center Installation Guide* in de [documentatie voor VMware NSX-T Data Center](#).

- vRealize Automation kan naar het VIP van een load balancer verwijzen om de aanroepen naar de drie NSX-managers te verdelen. Met deze optie ontvangen alle drie NSX-managers API-aanroepen van vRealize Automation.

U kunt het VIP op een load balancer van derden of op een load balancer van NSX-T configureren.

Voor grote omgevingen kunt u deze optie gebruiken om de vRealize Automation API-oproepen tussen de drie NSX-managers te splitsen.

Gebruik deze informatie als u het NSX-T-endpoint in stap 5 opgeeft.

U kunt een NSX-T-endpoint koppelen aan een of meer vSphere-endpoints.

U kunt een associatie maken tussen vSphere- en NSX-endpoints. Associaties omvatten:

- Eén vSphere-endpoint gekoppeld aan één NSX for vSphere-endpoint.
- Eén vSphere-endpoint gekoppeld aan meerdere NSX-T-endpoints.
- Eén NSX-T-endpoint gekoppeld aan meerdere vSphere-endpoints.
- Eén NSX for vSphere-endpoint gekoppeld aan één vSphere-endpoint.
- Eén vSphere-endpoint gekoppeld aan één NSX for vSphere-endpoint en één NSX-T-endpoint.

Wanneer een vSphere-endpoint is gekoppeld aan zowel een NSX for vSphere-endpoint als een NSX-T-endpoint, wordt het cluster beheerd door NSX for vSphere of door NSX-T. De NSX Manager wordt bepaald door vRealize Automation wanneer gegevens voor het endpoint worden verzameld en er een relatie tot stand wordt gebracht. U kunt het type NSX-platform zien dat een specifiek cluster beheert door de kolom **NSX-type** op de pagina **Computerbronnen** te controleren.

Wanneer u een blueprint implementeert die een NSX-T-endpoint bevat, wijst de implementatie een tag toe aan NSX-T-onderdelen in de implementatie. De naam van de tag en de naam van de implementatie komen overeen.

Zie [Overwegingen bij het gebruik van Testverbinding](#) voor informatie over het valideren van de endpointverbinding en het certificaatvertrouwen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **laaS-beheerder**.
- U moet een vSphere-proxyagent installeren om uw vSphere-endpoint te beheren en u moet exact dezelfde naam gebruiken voor uw endpoint en agent. Raadpleeg voor meer informatie over het installeren van de agent *vRealize Automation installeren*.
- Configureer uw NSX-T-netwerkinstellingen. Zie [Instellingen van netwerk- en beveiligingsonderdelen configureren in vRealize Automation](#).
- [Een vSphere-endpoint in vRealize Automation maken en koppelen aan NSX](#).

Als voorbereiding op het gebruik van NSX-netwerk-, -beveiligings- en -load balancing-mogelijkheden in vRealize Automation, moet u, wanneer u NSX-beheerdersgegevens gebruikt, het NSX-beheerdersaccount gebruiken.

Procedure

- 1 Selecteer **Infrastructuur > Endpoints > Endpoints**.

- 2 Selecteer **Nieuw > Netwerk en beveiliging > NSX-T**.
- 3 Geef een naam op in het tekstvak **Naam**.
- 4 (Optioneel) Geef een beschrijving op in het tekstvak **Beschrijving**.
- 5 Voer de URL voor de NSX-T-endpointbeheerinstantie of VIP (zie boven) in het tekstvak **Adres** in.

De URL moet van het type **https://hostname** of **https://IP_address** zijn.

Bijvoorbeeld **https://abx-nsxt3-manager.local**.

- 6 Voer de gebruikersnaam en het wachtwoord met beheerdersbevoegdheden voor NSX in die zijn opgeslagen voor het NSX-T-endpoint.
- 7 (Optioneel) Klik op **Eigenschappen** en voeg opgegeven aangepaste eigenschappen, eigenschapsgroepen of uw eigen eigenschapsdefinities voor het endpoint toe.
- 8 Klik op **Associaties** en selecteer een bestaand vSphere-endpoint om de NSX-T-netwerkinstellingen en -beveiligingsinstellingen te koppelen aan een bestaand vSphere-endpoint.

U moet het vSphere-endpoint maken voordat u de associatie kunt maken.

Een vSphere-endpoint kan slechts aan één type netwerk- en beveiligingsplatform gekoppeld zijn: NSX for vSphere of NSX-T.

U kunt een NSX-T-endpoint koppelen aan meer dan één vSphere-endpoint. Eén NSX-T-instantie kan meerdere ESX-clusters op verschillende vCenters beheren.

Wanneer de associatie is voltooid, geeft de kolom Beschrijving op de pagina het associatietype van NSX-T aan.

- 9 (Optioneel) Klik op **Testverbinding** om de verificatiegegevens, het endpointadres van de host en het certificaatvertrouwen te valideren. De actie controleert ook of de beheerservice en -agent actief zijn zodat gegevens voor het endpoint kunnen worden verzameld. De actie **OK** test op dezelfde voorwaarden.

De actie **Testverbinding** retourneert informatie over een van de volgende voorwaarden:

- **Certificaatfout**

Als het certificaat niet wordt gevonden, vertrouwd of is verlopen, wordt u gevraagd een vingerafdruk van het certificaat te accepteren. Als u de vingerafdruk niet accepteert, kunt u het endpoint wel opslaan maar mislukt de inrichting van de machine mogelijk.

- **Agentfout**

De gekoppelde vSphere-agent is niet gevonden. Voor een succesvolle test moet de agent actief zijn.

- **Hostfout**

Het opgegeven endpointadres is niet bereikbaar of de gekoppelde beheerservice is niet actief. Voor een succesvolle test moet de managementservice actief zijn.

- Verificatiegegevensfout

De opgegeven combinatie van gebruikersnaam en wachtwoord is ongeldig voor het endpoint op het opgegeven adres.

- Timeout

De testactie kan niet worden voltooid in de toegestane tijdsperiode van twee minuten.

Als de actie **Testverbinding** mislukt, kunt u het endpoint wel opslaan maar mislukt de inrichting van de machine mogelijk.

Als er een probleem is met een vertrouwd certificaat, bijvoorbeeld als het certificaat is verlopen, wordt u gevraagd een vingerafdruk van het certificaat te accepteren.

10 Klik op **OK** om het endpoint op te slaan.

De actie **OK** test op dezelfde voorwaarden als de actie **Testverbinding**. Als een van de vorige voorwaarden wordt gevonden, wordt een bericht geretourneerd. Als er kan worden opgeslagen, wordt de fout weergegeven op het scherm zodat u die kunt controleren.

Resultaten

vRealize Automation verzamelt gegevens van uw endpoint en ontdekt uw rekenbronnen.

Zie [Computerbronnen bekijken en gegevensverzameling uitvoeren](#) voor informatie over het uitvoeren van een gegevensverzameling voor bestaande endpoints na de eerste gegevensverzameling.

Wat nu te doen

Voeg de computerbronnen van uw endpoint toe aan een materiaalgroep. Zie [Een materiaalgroep maken](#).

Een vCloud Air-endpoint maken

U kunt een vCloud Air-endpoint maken voor een OnDemand- of abonnementsservice. Optioneel kunt u proxyinstellingen koppelen aan het vCloud Director-endpoint door een proxyendpoint te koppelen.

Voor informatie over de vCloud Air-beheerconsole raadpleegt u de vCloud Air-documentatie.

Opmerking Reserveringen die zijn gedefinieerd voor vCloud Air-endpoints en vCloud Director-endpoints bieden geen ondersteuning voor het gebruik van netwerkprofielen voor het inrichten van machines.

Voor vCloud Air-endpoints moeten de organisatiennaam en de vDC-naam identiek zijn voor een vCloud Air-abonnementinstantie.

Zie [Een proxyendpoint maken en associëren met een cloud-endpoint](#) voor informatie over het koppelen van proxyinstellingen aan uw endpoint.

Voorwaarden

- Meld u aan bij vRealize Automation als een **IaaS-beheerder**.

- Zorg ervoor dat u de machtiging **virtuele-infrastructuurbeheerder** hebt voor uw vCloud Air-abonnementsservice of OnDemand-account.
- Als u extra beveiliging wilt configureren en verbindingen via een proxyserver wilt afdwingen, maakt u een proxyendpoint. U kunt een proxyendpoint koppelen wanneer u het vCloud Director-endpoint maakt. Zie [Een proxyendpoint maken en associëren met een cloud-endpoint](#).

Procedure

- 1 Selecteer **Infrastructuur > Endpoints > Endpoints**.
- 2 Selecteer **Nieuw > Cloud > vCloud Air**.
- 3 Voer een naam in en desgewenst een beschrijving.
- 4 Accepteer het standaard-vCloud Air-endpointadres in het tekstvak **Adres** of voer een nieuw adres is.

Het standaard-vCloud Air-endpointadres is `https://vca.vmware.com`, zoals opgegeven in de algemene eigenschap `Default URL for vCloud Air endpoint`.

- 5 Voer uw gebruikersnaam en wachtwoord op beheerdersniveau in.

De verificatiegegevens moeten die van de beheerder van de abonnementsservice of OnDemand-account voor vCloud Air zijn.

De indeling van de gebruikersnaam is `domein\gebruikersnaam`.

Geef de verificatiegegevens op van een organisatiebeheerder die het recht geven om verbinding te maken via VMware Remote Console.

- 6 (Optioneel) Klik op **Eigenschappen** en voeg opgegeven aangepaste eigenschappen, eigenschapsgroepen of uw eigen eigenschapsdefinities voor het endpoint toe.
- 7 (Optioneel) Klik op **Associaties** en maak een associatie met een bestaand Proxy-endpoint om extra beveiliging te configureren en af te dwingen dat verbindingen via een proxyserver gaan.

U moet ten minste één Proxy-endpoint hebben om een associatie te maken.

- 8 Klik op **OK**.

Wat nu te doen

[Een materiaalgroep maken](#).

Een vCloud Director-endpoint maken

U kunt een vCloud Director-endpoint maken om alle vCloud Director Virtual Datacenters (vDC's) in uw omgeving te beheren of u kunt afzonderlijke endpoints maken om elke vCloud Director-organisatie te beheren. Optioneel kunt u proxyinstellingen koppelen aan het vCloud Director-endpoint door een proxyendpoint te koppelen.

Voor informatie over organisatie-vDC's raadpleegt u de vCloud Director-documentatie.

Maak niet één enkel endpoint en afzonderlijke organisatie-endpoints voor dezelfde vCloud Director-instantie.

vRealize Automation gebruikt een proxyagent om vSphere-bronnen te beheren.

Opmerking Reserveringen die zijn gedefinieerd voor vCloud Air-endpoints en vCloud Director-endpoints bieden geen ondersteuning voor het gebruik van netwerkprofielen voor het inrichten van machines.

Lease-informatie voor vCloud Director-machines moet worden opgegeven in vRealize Automation, niet in vCloud Director. Als u lease-informatie opgeeft in vCloud Director, zal deze lease-informatie niet worden herkend of gebruikt in vRealize Automation. Voer lease-informatie voor vCloud Director-machines in uw vRealize Automation blueprint in, niet in vCloud Director.

Zie [Een proxyendpoint maken en associëren met een cloud-endpoint](#) voor informatie over het koppelen van proxyinstellingen aan uw endpoint.

Voorwaarden

- Meld u aan bij vRealize Automation als een **laaS-beheerder**.
- Als u extra beveiliging wilt configureren en verbindingen via een proxyserver wilt afdwingen, maakt u een proxyendpoint. U kunt een proxyendpoint koppelen wanneer u het vCloud Director-endpoint maakt. Zie [Een proxyendpoint maken en associëren met een cloud-endpoint](#).

Procedure

1 Selecteer **Infrastructuur > Endpoints > Endpoints**.

2 Selecteer **Nieuw > Cloud > vCloud Director**.

3 Voer een naam in en desgewenst een beschrijving.

4 Typ de URL van de vCloud Director-server in het tekstvak **Adres**.

De URL moet van het type *FQDN* of *IP_address* zijn.

Bijvoorbeeld <https://mycompany.com>.

5 Voer uw gebruikersnaam en wachtwoord op beheerdersniveau in.

- Om verbinding te maken met de vCloud Director-server en de organisatie op te geven waarvoor de gebruiker de beheerdersrol heeft, gebruikt u de verificatiegegevens van de organisatiebeheerder. Met deze verificatiegegevens kan het endpoint alleen toegang krijgen tot de gekoppelde organisatie-vDC's. U kunt endpoints toevoegen voor elke aanvullende organisatie in de vCloud Director-instantie om te integreren met vRealize Automation.
- Om toegang te krijgen tot alle organisatie-vDC's in de vCloud Director-instantie, gebruikt u verificatiegegevens van een systeembeheerder voor een vCloud Director en laat u het tekstvak **Organisatie** leeg.

- 6 Als u een organisatiebeheerder bent, kunt u een vCloud Director-organisatienaam invoeren in het tekstvak **Organisatie**.

Optie	Beschrijving
Alle organisatie-vCD's ontdekken	Als u vCloud Director hebt geïmplementeerd in een privécloud, kunt u het tekstvak Organisatie leeg laten zodat de toepassing alle beschikbare organisatie-vDC's kan ontdekken.
Afzonderlijke endpoints voor elke organisatie-vCD	Typ een vCloud Director-organisatienaam in het tekstvak Organisatie .

De **Organisatie**naam komt overeen met de naam van uw vCloud Director-organisatie, die mogelijk ook wordt weergegeven als de naam van uw Virtual Datacenter (vDC). Als u een Virtual Private Cloud gebruikt, dan is deze naam een unieke id in de indeling M123456789-12345. In een aangewezen cloud is dit de opgegeven naam van de doel-vDC.

Als u direct op systeemniveau verbinding maakt met vCloud Director, en bijvoorbeeld het veld Organisatie leeg laat, hebt u verificatiegegevens van een systeembeheerder nodig. Als u een organisatie invoert voor het endpoint, hebt u verificatiegegevens van een organisatiebeheerder voor die organisatie nodig.

Geef de verificatiegegevens op die het recht geven om verbinding te maken via VMware Remote Console.

- Geef de verificatiegegevens van een systeembeheerder op om alle organisaties met één endpoint te beheren.
- Als u elk virtual datacenter (vDC) van een organisatie met een afzonderlijk endpoint wilt beheren, maakt u voor elk vDC afzonderlijke verificatiegegevens voor organisatiebeheer.

Maak niet één enkel systeem-endpoint en afzonderlijke organisatie-endpoints voor dezelfde vCloud Director-instantie.

- 7 (Optioneel) Klik op **Eigenschappen** en voeg opgegeven aangepaste eigenschappen, eigenschapsgroepen of uw eigen eigenschapsdefinities voor het endpoint toe.
- 8 (Optioneel) Klik op **Associaties** en maak een associatie met een bestaand Proxy-endpoint om extra beveiliging te configureren en af te dwingen dat verbindingen via een proxyserver gaan.

U moet ten minste één Proxy-endpoint hebben om een associatie te maken.

- 9 Klik op **OK**.

Wat nu te doen

[Een materiaalgroep maken.](#)

Een Amazon-endpoint maken

U kunt een endpoint maken om verbinding te maken met een Amazon-instantie. U kunt desgewenst proxy-instellingen associëren met het Amazon-endpoint door associatie met een proxyendpoint.

vRealize Automation biedt verschillende Amazon-instantietypen voor het maken van blueprints, maar als u uw eigen instantietypen wilt importeren, raadpleegt u [Een Amazon-instantietype toevoegen](#).

Zie [Een proxyendpoint maken en associëren met een cloud-endpoint](#) voor informatie over het koppelen van proxyinstellingen aan uw endpoint.

Voorwaarden

- Meld u aan bij vRealize Automation als een **IaaS-beheerder**.
- Als u extra beveiliging wilt configureren en verbindingen via een proxyserver wilt afdwingen, maakt u een proxyendpoint. U kunt een associatie maken met een proxyendpoint op het moment dat u een Amazon-endpoint maakt. Zie [Een proxyendpoint maken en associëren met een cloud-endpoint](#).

Procedure

- 1 Selecteer **Infrastructuur > Endpoints > Endpoints**.
- 2 Selecteer **Nieuw > Cloud > Amazon EC2**.
- 3 Voer een naam in en desgewenst een beschrijving.
Doorgaans geeft deze naam het Amazon-account op dat overeenkomt met dit endpoint.
- 4 Voer de toegangssleutel-id met beheerdersrechten voor het Amazon-endpoint in.
Er kan slechts één endpoint aan een Amazon-toegangssleutel-id worden gekoppeld.
Voor het verkrijgen van de toegangssleutel die nodig is om het Amazon-endpoint te maken, moet u een sleutel aanvragen aan een gebruiker met AWS-verificatiegegevens voor een beheerder met volledige toegangsrechten of moet voor u het AWS-beleid voor een beheerder met volledige toegangsrechten worden geconfigureerd. Zie de documentatie van Amazon voor meer informatie.
- 5 Voer de geheime toegangssleutel voor het Amazon-endpoint in.
- 6 (Optioneel) Klik op **Eigenschappen** en voeg opgegeven aangepaste eigenschappen, eigenschapsgroepen of uw eigen eigenschapsdefinities voor het endpoint toe.
- 7 (Optioneel) Klik op **Associaties** en maak een associatie met een bestaand Proxy-endpoint om extra beveiliging te configureren en af te dwingen dat verbindingen via een proxyserver gaan.
U moet ten minste één Proxy-endpoint hebben om een associatie te maken.
- 8 Klik op **OK**.

Resultaten

Nadat u het endpoint hebt gemaakt, begint vRealize Automation met het verzamelen van gegevens uit de Amazon Web Services-regio's.

Wat nu te doen

Voeg de computerbronnen van uw endpoint toe aan een materiaalgroep. Zie [Een materiaalgroep maken](#).

Een Amazon-instantiotype toevoegen

Er worden verschillende instantietypen meegeleverd bij vRealize Automation voor gebruik met Amazon-blueprints. Een beheerder kan instantietypen toevoegen en verwijderen.

De instantietypen van machines die worden beheerd door IaaS-beheerders zijn beschikbaar voor blueprintarchitecten bij het maken of bewerken van een Amazon-blueprint. Installatiekopieën en instantietypen van Amazon-machines worden beschikbaar gemaakt via het Amazon Web Services-product.

Voorwaarden

Meld u aan bij vRealize Automation als een **IaaS-beheerder**.

Procedure

1 Klik op **Infrastructuur > Beheer > Instantietypen**.

2 Klik op **Nieuw**.

3 Voeg een nieuw instantiotype toe en geef de volgende parameters op.

Informatie over de beschikbare Amazon-instantietypen en de instellingswaarden die u kunt opgeven voor deze parameters, is beschikbaar in de Amazon Web Services-documentatie in *EC2 Instance Types - Amazon Web Services (AWS)* op aws.amazon.com/ec2 en *Instance Types* op docs.aws.amazon.com.

- Naam
- API-naam
- Naam van type
- IO-prestatienaam
- CPU's
- Geheugen (GB)
- Opslag (GB)
- Rekeneenheden

4 Klik op het pictogram **Opslaan** (.

Resultaten

Wanneer IaaS-architecten Amazon Web Services-blueprints maken, kunnen ze uw aangepaste instantietypen gebruiken.

Wat nu te doen

Voeg de computerbronnen van uw endpoint toe aan een materiaalgroep. Zie [Een materiaalgroep maken](#).

Een proxyendpoint maken en associëren met een cloud-endpoint

U kunt een proxyendpoint maken en de proxy-instellingen ervan associëren met een vCloud Air-, vCloud Director- of Amazon-endpoint.

Als u een upgrade hebt uitgevoerd of bent gemigreerd van een vCloud Air-, vCloud Director- of Amazon-endpoint dat gebruikmaakte van een proxymanager, wordt er een nieuw vCloud Air-, vCloud Director- of Amazon-endpoint gemaakt dat een associatie bevat tussen het vCloud Air-, vCloud Director- of Amazon-endpoint en een nieuw proxyendpoint.

Voorwaarden

- Meld u aan bij vRealize Automation als een **laaS-beheerder**.
- Maak een van de volgende endpointtypen:
 - [Een vCloud Air-endpoint maken](#)
 - [Een Amazon-endpoint maken](#)
 - [Een vCloud Director-endpoint maken](#)

U moet ten minste een vCloud Air-, vCloud Director- of Amazon-endpoint hebben om een associatie te maken van het proxyendpoint.

Procedure

- 1 Selecteer **Infrastructuur > Endpoints > Endpoints**.
- 2 Selecteer **Nieuw > Netwerk en beveiliging > Proxy**.
- 3 Geef een naam op in het tekstvak **Naam**.
- 4 (Optioneel) Geef een beschrijving op in het tekstvak **Beschrijving**.
- 5 Typ de URL voor het geïnstalleerde proxyendpoint in het tekstvak **Adres**.
- 6 Voer het poortnummer in dat moet worden gebruikt om verbinding te maken met de proxyserver in het tekstvak **Poort**.
- 7 Voer uw gebruikersnaam en wachtwoord op beheerdersniveau in.
- 8 (Optioneel) Klik op **Eigenschappen** en voeg opgegeven aangepaste eigenschappen, eigenschapsgroepen of uw eigen eigenschapsdefinities voor het endpoint toe.
- 9 Klik op **Associaties** en selecteer een of meer endpoints om de proxyinstellingen te koppelen aan een vCloud Air-, vCloud Director- of Amazon-endpoint.

U moet ten minste één vCloud Air-, vCloud Director- of Amazon-endpoint hebben om een associatie te maken.

U kunt het Proxy-endpoint koppelen aan meer dan één endpoint.

10 Klik op **OK**.

Resultaten

vRealize Automation verzamelt gegevens van uw endpoint en ontdekt uw rekenbronnen.

Wat nu te doen

Voeg de computerbronnen van uw endpoint toe aan een materiaalgroep. Zie [Een materiaalgroep maken](#).

Een proxyendpoint maken voor de website van de OVF-host

Wanneer een OVF-bestand op een website wordt gehost, kunt u een proxyendpoint maken en dit gebruiken om OVF te importeren in een vSphere-machineonderdeel in een blueprint of als waardeset voor een image-onderdeelprofiel.

Zie [Een vSphere-endpoint in vRealize Automation maken en koppelen aan NSX](#) en [Een blueprint configureren om in te richten vanaf een OVF](#) voor informatie over het configureren van een OVF-implementatie.

Voorwaarden

- Meld u aan bij vRealize Automation als een **laaS-beheerder**.

Procedure

- 1** Selecteer **Infrastructuur > Endpoints > Endpoints**.
- 2** Selecteer **Nieuw > Netwerk en beveiliging > Proxy**.
- 3** Geef een naam op in het tekstvak **Naam**.
- 4** (Optioneel) Geef een beschrijving op in het tekstvak **Beschrijving**.
- 5** Voer in het tekstvak **Adres** de URL in van de website waarop het OVF-bestand wordt gehost.
- 6** Voer in het tekstvak **Poort** het poortnummer in dat moet worden gebruikt om verbinding te maken met de proxyserver van de website.
- 7** Voer uw gebruikersnaam en wachtwoord op beheerdersniveau in.
- 8** (Optioneel) Klik op **Eigenschappen** en voeg opgegeven aangepaste eigenschappen, eigenschapsgroepen of uw eigen eigenschapsdefinities voor het endpoint toe.
- 9** Klik op **OK**.

Resultaten

U kunt nu het endpoint gebruiken om de website te definiëren waarop een OVF beschikbaar is. Zie voor meer informatie: [Blueprintinstellingen definiëren voor een vSphere-onderdeel met behulp van een OVF-bestand](#) en [Een imagewaardeset voor een onderdeelprofiel definiëren met behulp van een OVF](#).

Een vRealize Orchestrator-endpoint maken

U kunt een vRealize Orchestrator-endpoint maken om dit te verbinden met een vRealize Orchestrator-server.

U kunt meerdere endpoints configureren om verbinding te maken op verschillende vRealize Orchestrator-servers, maar u moet voor elk endpoint een prioriteit configureren.

Bij het uitvoeren van vRealize Orchestrator-werkstromen, wordt door vRealize Automation geprobeerd de vRealize Orchestrator-endpoint met de hoogste prioriteit als eerste uit te voeren. Als die endpoint niet bereikbaar is, dan wordt doorgedaan met de endpoint met de op een na hoogste prioriteit, totdat een vRealize Orchestrator-server beschikbaar is om de werkstroom uit te voeren.

Voorwaarden

- Meld u aan bij vRealize Automation als een **laaS-beheerder**.

Procedure

- 1 Selecteer **Infrastructuur > Endpoints > Endpoints**.
- 2 Selecteer **Nieuw > Orkestratie > vCenter Orchestrator**.
- 3 Voer een naam in en desgewenst een beschrijving.
- 4 Voer een URL in met de volledig gekwalificeerde naam of het IP-adres van de vRealize Orchestrator-server en het poortnummer voor vRealize Orchestrator.

Het transportprotocol moet HTTPS zijn. Als er geen poort wordt opgegeven, wordt de standaardpoort 443 gebruikt.

Als u de standaardinstantie voor vRealize Orchestrator wilt gebruiken die is ingesloten in de toepassing vRealize Automation, typt u

`https://vrealize-automatiseringstoepassing-hostnaam:443/vco`.

- 5 Typ uw vRealize Orchestrator-verificatiegegevens in de vakken **Gebruikersnaam** en **Wachtwoord** om een verbinding te maken met het vRealize Orchestrator endpoint.

De verificatiegegevens die u gebruikt moeten over het recht Uitvoeren beschikken voor elke vRealize Orchestrator-werkstroom die kan worden geroepen vanuit laaS.

Als u de standaardinstantie voor vRealize Orchestrator wilt gebruiken die is ingesloten in de toepassing vRealize Automation, is de gebruikersnaam **administrator@vsphere.local** en wordt het beheerderswachtwoord dat is opgegeven bij het configureren van SSO als wachtwoord gebruikt.

- 6 Voer een geheel getal in dat groter is dan of gelijk is aan 1 in het tekstvak **Prioriteit**.
Hoe lager de waarde, des te hoger de prioriteit.
- 7 (Optioneel) Klik op **Eigenschappen** en voeg opgegeven aangepaste eigenschappen, eigenschapsgroepen of uw eigen eigenschapsdefinities voor het endpoint toe.
- 8 Klik op **OK**.

vRealize Orchestrator-endpoints configureren voor netwerken

Als u vRealize Automation-werkstromen gebruikt om vRealize Orchestrator-werkstromen aan te roepen, moet u de vRealize Orchestrator-instantie of -server als een endpoint configureren.

Voor informatie over het toevoegen van een vRealize Orchestrator-endpoint raadpleegt u [Een vRealize Orchestrator-endpoint maken](#).

U kunt een vRealize Orchestrator-endpoint koppelen aan een machineblueprint, om er zo voor te zorgen dat alle nieuwe vRealize Orchestrator-werkstromen voor machines die zijn ingericht op basis van die blueprint worden ingericht met die endpoint.

vRealize Automation bevat standaard een ingesloten instantie voor vRealize Orchestrator. Het wordt aanbevolen dat u de ingesloten instantie als uw vRealize Orchestrator-endpoint gebruikt voor het uitvoeren van vRealize Automation-werkstromen in een productie- of testomgeving of voor het maken van een 'proof of concept'.

Wij raden u verder aan dit vRealize Orchestrator-endpoint te gebruiken bij het uitvoeren van vRealize Automation-werkstromen in een productieomgeving.

De vRealize Orchestrator-invoegtoepassing wordt automatisch geïnstalleerd bij vRealize Orchestrator 7.1 en later. Er is geen afzonderlijke vRealize Orchestrator-invoegtoepassing om te installeren.

Een vRealize Operations Manager-endpoint maken

U kunt een vRealize Operations Manager-endpoint maken om dit te verbinden met een vRealize Operations Manager-hostsuite-API.

Raadpleeg [Overwegingen bij het gebruik van Testverbinding](#) voor informatie over het valideren van de vRealize Operations Manager-verbinding en vertrouwen in certificaten.

Voorwaarden

- Meld u aan bij vRealize Automation als een **laaS-beheerder**.

Procedure

- 1 Selecteer **Infrastructuur > Endpoints > Endpoints**.
- 2 Selecteer **Nieuw > Management > vRealize Operations Manager**.
- 3 Voer een naam in en desgewenst een beschrijving.
- 4 Typ de URL voor de vRealize Operations Manager-server in het tekstvak **Adres**.
De URL moet de indeling: **https://hostnaam/suite-api** hebben.
- 5 Voer uw verificatiegegevens met gebruikersnaam en wachtwoord voor vRealize Operations Manager in.
- 6 (Optioneel) Klik op **Eigenschappen** en voeg opgegeven aangepaste eigenschappen, eigenschapsgroepen of uw eigen eigenschapsdefinities voor het endpoint toe.

- 7 (Optioneel) Klik op **Testverbinding** om de verificatiegegevens, het endpointadres van de host en het certificaatvertrouwen te valideren. De actie controleert ook of de beheerservice en -agent actief zijn zodat gegevens voor het endpoint kunnen worden verzameld. De actie **OK** test op dezelfde voorwaarden.

De actie **Testverbinding** retourneert informatie over een van de volgende voorwaarden:

- **Certificaatfout**

Als het certificaat niet wordt gevonden, vertrouwd of is verlopen, wordt u gevraagd een vingerafdruk van het certificaat te accepteren. Als u de vingerafdruk niet accepteert, kunt u het endpoint wel opslaan maar mislukt de inrichting van de machine mogelijk.

- **Agentfout**

De gekoppelde vSphere-agent is niet gevonden. Voor een succesvolle test moet de agent actief zijn.

- **Hostfout**

Het opgegeven endpointadres is niet bereikbaar of de gekoppelde beheerservice is niet actief. Voor een succesvolle test moet de managementservice actief zijn.

- **Verificatiegegevensfout**

De opgegeven combinatie van gebruikersnaam en wachtwoord is ongeldig voor het endpoint op het opgegeven adres.

- **Timeout**

De testactie kan niet worden voltooid in de toegestane tijdsperiode van twee minuten.

Als de actie **Testverbinding** mislukt, kunt u het endpoint wel opslaan maar mislukt de inrichting van de machine mogelijk.

Als er een probleem is met een vertrouwd certificaat, bijvoorbeeld als het certificaat is verlopen, wordt u gevraagd een vingerafdruk van het certificaat te accepteren.

- 8 Klik op **OK**.

Een endpoint van een externe IPAM-provider maken

Als u een IPAM-endpointtype van derden hebt geregistreerd en geconfigureerd in vRealize Orchestrator, kunt u een endpoint voor die IPAM-provider maken in vRealize Automation.

Als u een vRealize Orchestrator-pakket hebt geïmporteerd voor het inrichten van een externe IPAM-oplossing en als u het IPAM-endpointtype hebt geregistreerd in vRealize Orchestrator, kunt u dat IPAM-endpointtype selecteren wanneer u een vRealize Automation-endpoint maakt.

Opmerking Dit voorbeeld is gebaseerd op gebruik van de IPAM-invoegtoepassing van Infoblox. Deze invoegtoepassing kan worden gedownload op de VMware Solution Exchange. U kunt deze procedure ook gebruiken als u uw eigen IPAM-providerpakket hebt gemaakt met behulp van de door VMware geleverde SDK voor IPAM-oplossingen. De procedure voor het importeren en configureren van uw eigen IPAM-pakket van derden is dezelfde procedure als bij de voorwaarden is beschreven.

Het eerste IPAM-endpoint voor vRealize Automation wordt gemaakt wanneer u het type endpoint registreert voor de invoegtoepassing van de IPAM-provider in vRealize Orchestrator.

Voorwaarden

- Een pakket van de externe IPAM-provider verkrijgen en importeren in vRealize Orchestrator.
- [Werkstroom uitvoeren om externe IPAM-endpointtypes in vRealize Orchestrator te registreren.](#)
- Meld u aan bij vRealize Automation als een **IaaS-beheerder**.

Maak voor dit voorbeeld een Infoblox IPAM-endpoint met behulp van een endpointtype dat u hebt geregistreerd in vRealize Orchestrator voor de invoegtoepassing of het pakket van een derde IPAM-provider.

Procedure

- 1 Selecteer **Infrastructuur > Endpoints > Endpoints**.

- 2 Selecteer **Nieuw > IPAM > IPAM-endpointtype**.

Selecteer een endpointtype van een geregistreerde externe IPAM-provider zoals Infoblox. Endpoints van externe IPAM-providers zijn alleen beschikbaar als u een vRealize Orchestrator-pakket van derden hebt geïmporteerd en de pakketwerkstromen uitvoert om het endpointtype te registreren.

Voor Infoblox IPAM worden alleen primaire IPAM-endpointtypen vermeld. U kunt secundaire IPAM-endpointtypen opgeven door aangepaste eigenschappen te gebruiken.

Selecteer voor dit voorbeeld een endpointtype van een geregistreerde IPAM-provider zoals **Infoblox NIOS**.

- 3 Voer een naam in en desgewenst een beschrijving.
- 4 Voer in het tekstvak **Adres** de locatie van het geregistreerde IPAM-endpoint in met het voor de provider specifieke URL-formaat, zoals `https://hostnaam/naam`.

U maakt bijvoorbeeld diverse IPAM-endpoints, zoals `https://nsx62-scale-infoblox` en `https://nsx62-scale-infoblox2`, wanneer u het IPAM-endpointtype hebt geregistreerd in vRealize Orchestrator. Voer een primair geregistreerd endpointtype in. Als u ook een of meer secundaire IPAM-endpoints wilt opgeven, kunt u aangepaste eigenschappen gebruiken om de uitbreidbare kenmerken te emuleren die specifiek voor de IPAM-provider zijn.

- 5 Voer de gebruikersnaam en het wachtwoord in die vereist zijn om toegang te krijgen tot het account van de IPAM-oplossingsprovider.

U hebt de verificatiegegevens voor de account van de IPAM-provider nodig om het endpoint te maken, configureren en bewerken wanneer u in vRealize Automation werkt. vRealize Automation gebruikt de verificatiegegevens van het IPAM-endpoint om te communiceren met het opgegeven endpointtype zoals Infoblox, om IP-adressen toe te wijzen en andere bewerkingen uit te voeren. Dit gedrag is vergelijkbaar met de manier waarop vRealize Automation verificatiegegevens voor het endpoint van vSphere gebruikt.

- 6** (Optioneel) Klik op **Eigenschappen** en voeg endpointeigenschappen toe die relevant zijn voor de specifieke IPAM-oplossingsprovider.

Elke IPAM-provider, zoals Infoblox en Bluecat, maakt gebruik van uitbreidbare kenmerken die u kunt emuleren door aangepaste eigenschappen van vRealize Automation te gebruiken. Infoblox gebruikt bijvoorbeeld uitbreidbare kenmerken om onderscheid te maken tussen primaire en secundaire endpoints.

- 7** Klik op **OK**.

Wat nu te doen

Voeg de computerbronnen van uw endpoint toe aan een materiaalgroep. Zie [Een materiaalgroep maken](#).

Een Microsoft Azure-endpoint maken

U kunt een Microsoft Azure-endpoint maken om een geverifieerde verbinding tussen vRealize Automation en een Azure-implementatie te vergemakkelijken.

Een endpoint brengt een verbinding tot stand met een bron, in dit geval een Azure-instantie, die u kunt gebruiken voor het maken van blueprints voor virtual machines. U moet een Azure-endpoint hebben om te gebruiken als basis van blueprints voor het inrichten van Azure virtual machines. Als u meerdere Azure-abonnementen gebruikt, hebt u voor elke abonnements-id een endpoint nodig.

U kunt ook rechtstreeks een Azure-verbinding tot stand brengen vanuit vRealize Orchestrator door middel van de opdracht Een Azure-verbinding toevoegen onder **Bibliotheek > Azure > Configuratie** in de vRealize Orchestrator-workflowstructuur. In de meeste gevallen is de hierin beschreven verbinding door middel van de endpoint-configuratie de beste optie.

Azure-endpoints worden ondersteund door vRealize Orchestrator- en XaaS-functionaliteit. U kunt een Azure-endpoint maken, verwijderen en bewerken. Als u een bestaand endpoint wijzigt en gedurende meerdere uren geen updates uitvoert op de Azure-portal via de bijgewerkte verbinding, kunnen er problemen optreden. U moet de service vRealize Orchestrator opnieuw starten met behulp van de opdracht service vco-service restart. Als u dat niet doet, kunnen er fouten optreden.

Voorwaarden

- Configureer een Microsoft Azure-instantie en verkrijg een geldig Microsoft Azure-abonnement waarvan u de abonnements-id kunt gebruiken. Zie [Microsoft Azure-endpointconfiguratie](#) voor meer informatie over het configureren van Azure en het verkrijgen van een abonnements-id.
- Controleer of uw vRealize Automation-implementatie ten minste één tenant en één bedrijfsgroep heeft.
- Maak een Active Directory-toepassing zoals beschreven in <https://azure.microsoft.com/nl-nl/documentation/articles/resource-group-create-service-principal-portal>.

- Noteer de volgende Azure-gegevens. U hebt deze nodig tijdens de configuratie van het endpoint en de blueprint.
 - abonnements-id
 - tenant-id
 - naam opslagaccount
 - naam brongroep
 - locatie
 - naam virtual machine
 - clienttoepassings-id
 - geheime sleutel clienttoepassing
 - image-URN van virtual machine
- De vRealize Automation Azure-implementatie ondersteunt een subset van de regio's die door Microsoft Azure worden ondersteund. Zie [Door Azure ondersteunde regio's](#).
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > vRO-configuratie > Endpoints**.
- 2 Klik op het pictogram **Nieuw (+)**.
- 3 Klik op het tabblad Invoegtoepassing op het vervolgkeuzemenu **Invoegtoepassing** en selecteer **Azure**.
- 4 Klik op **Volgende**.
- 5 Voer een naam in en desgewenst een beschrijving.
- 6 Klik op **Volgende**.
- 7 Vul de tekstvakken op het tabblad Details in voor het endpoint.

Parameter	Beschrijving
Verbindingsinstellingen	
Verbindingsnaam	De unieke naam voor de nieuwe endpointverbinding. Deze naam wordt weergegeven in de vRealize Orchestrator-interface om u te helpen een bepaalde verbinding te identificeren.
Azure-abonnements-id	De id voor uw Azure-abonnement. Met deze id worden de opslagaccounts, virtual machines en andere Azure-bronnen waar u toegang toe hebt gedefinieerd.
Azure-omgeving	De geografische regio voor de geïmplementeerde Azure-bron. vRealize Automation ondersteunt alle huidige Azure-regio's op basis van de abonnements-id.

Parameter	Beschrijving
Instellingen bronbeheerder	
URI voor Azure-service	Dit is de URI die u nodig hebt voor toegang tot uw Azure-instantie. De standaardwaarde van <code>https://management.azure.com/</code> is doorgaans geschikt voor veel normale implementaties. Dit vakje wordt automatisch ingevuld wanneer u een omgeving selecteert.
Tenant-id	Dit is de Azure-tenant-id die het endpoint moet gebruiken.
Client-id	Dit is de Azure-client-id die het endpoint moet gebruiken. Deze wordt toegewezen wanneer u een Active Directory-toepassing maakt.
Clientgeheim	De sleutel die wordt gebruikt voor de Azure-client-id. Deze sleutel wordt toegewezen wanneer u een Active Directory-toepassing maakt.
Opslag-URI voor Azure	De URI via welke u toegang krijgt tot de opslaginstantie van Azure. Dit vakje wordt automatisch ingevuld wanneer u een omgeving selecteert.
Proxy-instellingen	
Proxy-host	Als uw bedrijf een proxyserver gebruikt, geeft u de hostnaam van die server op.
Proxypoort	Als uw bedrijf een proxyserver gebruikt, geeft u het poortnummer van die server op.

- 8** (Optioneel) Klik op Eigenschappen en voeg opgegeven aangepaste eigenschappen, eigenschapsgroepen of uw eigen eigenschapsdefinities toe.

- 9** Klik op **Voltooien**.

Wat nu te doen

Maak de toepasselijke brongroepen, opslagaccounts en netwerkbeveiligingsgroepen in Azure. Indien uw implementatie dit vereist, moet u tevens load balancers maken.

Actie	Opties
Een relevante brongroep maken	<ul style="list-style-type: none"> ■ Maak de brongroep via het Azure-portal. Raadpleeg de Azure-documentatie voor specifieke instructies. ■ Gebruik de van toepassing zijnde vRealize Orchestrator-werkstroom in de brongroep Bibliotheek/Azure/Bron/Maken. ■ Maak en publiceer in vRealize Automation een XaaS-blueprint die de vRealize Orchestrator-werkstroom bevat. U kunt de brongroep aanvragen nadat u deze aan de service en rechten hebt gekoppeld. <p>Opmerking Het brontype Brongroep wordt niet ondersteund of beheerd door vRealize Automation.</p>
Een Azure Storage-account maken	<ul style="list-style-type: none"> ■ Gebruik Azure om een opslagaccount te maken. Raadpleeg de Azure-documentatie voor specifieke instructies. ■ Gebruik de van toepassing zijnde vRealize Orchestrator-werkstroom in het opslagaccount Bibliotheek/Azure/Opslag/Maken. ■ Maak en publiceer in vRealize Automation een XaaS-blueprint die de vRealize Orchestrator-werkstroom bevat. U kunt het opslagaccount aanvragen nadat u dit aan de service en rechten hebt gekoppeld.
Een Azure-netwerkbeveiligingsgroep maken	<ul style="list-style-type: none"> ■ Gebruik Azure om een beveiligingsgroep te maken. Raadpleeg de Azure-documentatie voor specifieke instructies. ■ Gebruik de van toepassing zijnde vRealize Orchestrator-werkstroom in de beveiligingsgroep Bibliotheek/Azure/Netwerk/Netwerk maken. ■ Maak en publiceer in vRealize Automation een XaaS-blueprint die de vRealize Orchestrator-werkstroom bevat. U kunt de beveiligingsgroep aanvragen nadat u deze aan de service en rechten hebt gekoppeld.

Microsoft Azure-endpointconfiguratie

U moet informatie verzamelen en een bepaalde configuratie uitvoeren om een Microsoft Azure-endpoint in vRealize Automation te maken.

Procedure

- 1 Zoek en noteer de id's van uw Microsoft Azure-abonnement en tenant.
 - Abonnements-id: klik op het pictogram Abonnementen op de werkbalk links in Azure Portal om de abonnements-id weer te geven.
 - Tenant-id: klik op het Help-pictogram en selecteer Diagnostische gegevens weergeven in Azure Portal. Zoek naar de tenant en noteer de id wanneer u deze hebt gevonden.

- 2 U kunt een nieuw opslagaccount en een brongroep maken om aan de slag te gaan. U kunt deze ook later in blueprints maken.
 - Opslagaccount: gebruik de volgende procedure om een account te configureren.
 - 1 Zoek in Azure Portal het pictogram Opslagaccounts op de zijbalk. Zorg ervoor dat het juiste abonnement is geselecteerd en klik op **Toevoegen**. U kunt ook zoeken naar opslagaccount in het Azure-zoekveld.
 - 2 Voer de vereiste informatie voor het opslagaccount in. U hebt uw abonnements-id nodig.
 - 3 Selecteer of u een bestaande brongroep wilt gebruiken of een nieuwe wilt maken. Noteer de naam van uw brongroep. U hebt deze later nodig.

Opmerking Sla de locatie van uw opslagaccount op. U hebt deze later nodig.

- 3 Maak een virtueel netwerk. Als u een geschikt bestaand netwerk hebt, kunt u ook dat netwerk selecteren.

Als u een netwerk maakt, moet u Een bestaande brongroep gebruiken selecteren en de groep opgeven die u in de vorige stap hebt gemaakt. Selecteer ook dezelfde locatie die u eerder hebt opgegeven. Microsoft Azure implementeert geen virtual machines of andere objecten als de locatie niet overeenkomt voor alle applianceonderdelen die door het object worden gebruikt.

 - a Zoek het pictogram Virtueel netwerk in het linkerpaneel en klik erop of zoek naar virtueel netwerk. Zorg ervoor dat u het juiste abonnement selecteert en klik op **Toevoegen**.
 - b Voer een unieke naam voor het nieuwe virtuele netwerk in en noteer deze voor later.
 - c Voer het juiste IP-adres voor uw virtuele netwerk in in het veld **Adresruimte**.
 - d Zorg ervoor dat het juiste abonnement is geselecteerd en klik op **Toevoegen**.
 - e Voer de overige basisinformatie voor de configuratie in.
 - f U kunt de andere opties desgewenst wijzigen, maar voor de meeste configuraties kunt u de standaardinstellingen behouden.
 - g Klik op **Maken**.
- 4 Stel een Azure Active Directory-toepassing in zodat vRealize Automation kan verifiëren.
 - a Zoek het pictogram Active Directory in het linkermenu van Azure en klik erop.
 - b Klik op **App-registraties** en selecteer **Toevoegen**.
 - c Typ een naam voor uw toepassing die voldoet aan de Azure-naamvalidatie.
 - d Behoud de selectie van Web-app/-API als toepassingstype.
 - e De aanmeldings-URL kan alles zijn dat geschikt is voor uw gebruik.
 - f Klik op **Maken**.

- 5 Maak een geheime sleutel om de applicatie in vRealize Automation te verifiëren.
 - a Klik op de naam van uw toepassing in Azure.
Noteer uw toepassings-id voor later gebruik.
 - b Klik op **Alle instellingen** in het volgende paneel en selecteer sleutels in de lijst met instellingen.
 - c Voer een beschrijving voor de nieuwe sleutel in en kies een duur.
 - d Klik op **Opslaan** en zorg ervoor dat u de sleutelwaarde kopieert naar een veilige locatie, omdat u deze later niet meer kunt ophalen.
 - e Selecteer in het linkermenu **API-machtigingen** voor de applicatie en klik op **Toevoegen** om een nieuwe machtiging te maken.
 - f Selecteer Azure Service Management op de pagina Een API selecteren.
 - g Klik op **Gedelegeerde machtigingen**.
 - h Selecteer user_impersonation onder Machtigingen selecteren en klik vervolgens op **Machtigingen toevoegen**.
- 6 Autoriseer uw Active Directory-toepassing om verbinding te maken met uw Azure-abonnement zodat u virtual machines kunt implementeren en beheren.
 - a Klik in het linkermenu op het pictogram Abonnementen en selecteer uw nieuwe abonnement.
Mogelijk moet u op de tekst van de naam klikken om het paneel te laten doorschuiven.
 - b Selecteer de optie Toegangsbeheer (IAM) om de machtigingen voor uw abonnement te zien.
 - c Klik op **Toevoegen** onder de kop Een roltoewijzing toevoegen.
 - d Kies Bijdrager in de vervolgkeuzelijst Rol.
 - e Behoud de standaardselectie in de vervolgkeuzelijst Toegang toewijzen.
 - f Typ de naam van uw applicatie in het vak Selecteren.
 - g Klik op **Opslaan**.
 - h Voeg extra rollen toe zodat uw nieuwe applicatie de rollen Eigenaar, Bijdrager en Lezer heeft.
 - i Klik op **Opslaan**.

Wat nu te doen

U moet de hulpprogramma's voor de opdrachtregelinterface van Microsoft Azure installeren. Deze hulpprogramma's zijn vrij beschikbaar voor zowel Windows- als Mac-besturingssystemen. Raadpleeg de Microsoft-documentatie voor meer informatie over het downloaden en installeren van deze hulpprogramma's.

Wanneer u de opdrachtregelinterface hebt geïnstalleerd, moet u zich verifiëren bij uw nieuwe abonnement.

- 1 Open een terminalvenster en typ uw Microsoft Azure-aanmelding. U ontvangt een URL en een korte code waarmee u zich kunt verifiëren.
- 2 Voer in een browser de code in die u van de toepassing op uw toestel hebt ontvangen.
- 3 Voer uw verificatiecode in en klik op **Doorgaan**.
- 4 Selecteer uw Azure-account en meld u aan.

Als u meerdere abonnementen hebt, kunt u er met de opdracht `azure account set <subscription-name>` voor zorgen dat het juiste abonnement is geselecteerd.

- 5 Voordat u doorgaat, moet u de Microsoft.Compute-provider registreren bij uw nieuwe Azure-abonnement met de opdracht `azure provider register microsoft.compute`.

Als er een time-out optreedt voor de opdracht en een fout wordt geretourneerd wanneer u deze voor het eerst uitvoert, voert u deze opnieuw uit.

Wanneer u de configuratie hebt voltooid, kunt u de opdracht `azure vm image list` gebruiken om de namen van beschikbare images van virtual machines op te halen. U kunt de gewenste image kiezen, de opgegeven URN voor de image vastleggen en deze later in blueprints gebruiken.

Een Puppet-endpoint maken

U kunt een Puppet-endpoint maken om het toevoegen van Puppet-configuratiebeheeronderdelen aan virtuele vSphere-machines te ondersteunen. Met deze onderdelen kunt u met een Puppet Master configuratiebeheer op virtuele machines forceren.

Een endpoint brengt een verbinding met een externe bron tot stand, in dit geval een instantie van Puppet Master. Dankzij het endpoint kunt u Puppet-configuratiebeheeronderdelen op de blueprints van de virtuele vSphere-machine plaatsen. Ingerichte virtuele machines gebaseerd op deze blueprints hebben een Puppet-agent die beheer door de geassocieerde Puppet Master mogelijk maakt.

Zie <https://www.youtube.com/watch?v=P-VglzE9o-o> voor meer informatie over de Puppet-invoegtoepassing en een demo van de configuratie.

Voorwaarden

- Installeer en configureer Puppet Enterprise voor uw omgeving.
- Download en installeer de Puppet-invoegtoepassingsversie 3.0 op uw vRealize Orchestrator-implementatie. U kunt de invoegtoepassing downloaden van <https://marketplace.vmware.com/vsx/solutions/puppet-plugin-for-vrealize-automation?ref=search>. Zie https://docs.puppet.com/pe/latest/vro_intro.html voor informatie over het installeren en gebruiken van de invoegtoepassing.

Procedure

- 1 Selecteer **Beheer > vRO-configuratie > Endpoints**.

- 2 Klik op het pictogram **Nieuw** (+).
- 3 Klik op het tabblad Invoegtoepassing op het vervolgkeuzemenu **Invoegtoepassing** en selecteer **Puppet-invoegtoepassing**.
- 4 Klik op **Volgende**.
- 5 Voer een naam in en desgewenst een beschrijving.
- 6 Klik op **Volgende**.
- 7 Vul de tekstvakken op het tabblad **Details** in voor het endpoint.

Parameter	Beschrijving
Weergavenaam voor deze Puppet Master	De naam van de Puppet Master die is geassocieerd met de endpointverbinding. Deze naam wordt weergegeven in de vRealize Orchestrator-interface om u te helpen een bepaalde verbinding te identificeren.
Hostnaam of IP-adres	De FQDN-naam die of het IP-adres van de Puppet Master dat door dit endpoint wordt gebruikt.
SSH-poort	De poort die is gedefinieerd voor gebruik met veilige communicatie voor deze Puppet Master.
SSH RBAC en gebruikersnaam	De op rollen gebaseerde gebruikersnaam voor toegangscontrole die is vereist om verbinding te maken met de Puppet Master.
SSH en RBAC-wachtwoord	De op rollen gebaseerde gebruikersnaam voor toegangscontrole die is vereist voor veilige configuratie met de Puppet Master.
Sudo gebruiken voor shellopdrachten op deze master?	Selecteer deze optie als u wilt dat beheerders sudo-opdrachten kunnen gebruiken op Linux-servers voor beveiligingsopties op virtuele machines die zijn gebaseerd op dit endpoint.

- 8 Klik op **OK**.

Resultaten

U kunt nu Puppet-configuratiebeheeronderdelen toevoegen aan vSphere-blueprints zodat u virtuele vSphere-machines kunt implementeren die Puppet-agenten bevatten.

Een Ansible-endpoint maken

U kunt een Ansible-endpoint maken om het toevoegen van Ansible-configuratiebeheeronderdelen aan virtuele vSphere-machines te ondersteunen. Met deze onderdelen kunt u met een Ansible Tower configuratiebeheer op virtuele machines forceren.

Voorwaarden

- Installeer en configureer een geschikte Ansible Tower voor uw omgeving.

- Download en installeer de Ansible-invoegtoepassing op uw vRealize Orchestrator-implementatie. De plug-in is beschikbaar via <https://marketplace.vmware.com/vsx/solutions/sovlabs-ansible-tower-plugin-in-for-vra-cm-framework-1?ref=search>.

Procedure

- 1 Selecteer **Beheer > vRO-configuratie > Endpoints**.
- 2 Klik op het pictogram **Nieuw**.
- 3 Klik op het tabblad Invoegtoepassing op het vervolgkeuzemenu **Invoegtoepassing** en selecteer de Ansible-invoegtoepassing.
- 4 Klik op **Volgende**.
- 5 Voer een naam en desgewenst een beschrijving in op het tabblad Endpoint.
- 6 Klik op **Volgende**.
- 7 Vul de tekstvakken op de tabbladen Details in voor het endpoint.

Tabblad Details	Beschrijving
Configuratie van Ansible Tower-endpoint	<p>Voeg de configuratiegegevens voor het endpoint toe.</p> <ul style="list-style-type: none"> ■ Configuratie van Ansible Tower-endpoint: geef de naam en het IP-adres of de hostnaam op in de juiste tekstvakken. ■ Configuratie van verificatiegegevens voor Ansible Tower: geef de verificatiegegevens op voor de Ansible Tower die met dit endpoint is gekoppeld. ■ SSL-certificaat importeren: kies of u wilt dat het Ansible Tower-certificaat stilzwijgend door vRealize Orchestrator wordt geaccepteerd.
Toegang tot de Ansible Tower-host	Geef indien van toepassing de SSH-verificatiegegevens op voor de Ansible Tower-machine zodat een geïmplementeerde machine ermee verbinding kan maken om een aangepast dynamische-inventarisscript te configureren.
Instelling van organisatie en inventaris	Configureer de naam van uw organisatie en de inventaris. Voeg configuratiewaarden voor de dynamische inventaris toe.
Filters en groepen	Configureer eigenschappenfilters voor sleutelparen en dynamische Ansible-groepen.
Prompt bij opstartvervangingen (optioneel)	Configureer opties voor Ansible-taken, alsook machine-, sjabloon- en inventarisoptyes.
Omzetting van vRA-eigenschappen	Geef indien nodig de gewenste vervangende tekenreeks op die Ansible moet gebruiken tijdens het verwerken van aangepaste eigenschappen na de inrichting.

- 8 Klik op **Voltooien**.

Een Hyper-V (SCVMM)-endpoint maken

U kunt endpoints maken om vRealize Automation toestemming te geven om te communiceren met uw SCVMM-omgeving en computerbronnen te ontdekken, gegevens te verzamelen en machines in te richten.

Voorwaarden

- Meld u aan bij vRealize Automation als een **IaaS-beheerder**.
- U moet een DEM-agent installeren en configureren om uw Hyper-V (SCVMM)-endpoint te beheren. Zie de vereisten voor SCVMM in de *vRealize Automation installeren* voor meer informatie.

Zie [Voorbereiding van uw SCVMM-omgeving](#) voor gerelateerde informatie.

Procedure

- 1 Selecteer **Infrastructuur > Endpoints > Endpoints**.
- 2 Selecteer **Nieuw > Virtual > Hyper-V (SCVMM)**.
- 3 Geef een naam op in het tekstvak **Naam**.
- 4 (Optioneel) Geef een beschrijving op in het tekstvak **Beschrijving**.
- 5 Typ de URL voor het endpoint in het tekstvak **Adres**.
De URL moet van het type *FQDN* of *IP_address* zijn.
Bijvoorbeeld **mycompany-scvmm1.mycompany.local**.
- 6 Voer de gebruikersnaam en het wachtwoord op beheerniveau in die u voor dit endpoint hebt opgeslagen.
Als u de verificatiegegevens nog niet hebt opgeslagen, dan kunt u dit nu doen.
- 7 (Optioneel) Klik op **Eigenschappen** en voeg opgegeven aangepaste eigenschappen, eigenschapsgroepen of uw eigen eigenschapsdefinities voor het endpoint toe.
- 8 Klik op **OK**.

Resultaten

vRealize Automation verzamelt gegevens van uw endpoint en ontdekt uw rekenbronnen.

Wat nu te doen

Voeg de computerbronnen van uw endpoint toe aan een materiaalgroep. Zie [Een materiaalgroep maken](#).

Een OpenStack-endpoint maken

U maakt een endpoint zodat vRealize Automation kan communiceren met uw OpenStack-instantie.

Voorwaarden

- Meld u aan bij vRealize Automation als een **IaaS-beheerder**.

- Controleer of uw vRealize Automation-DEM's zijn geïnstalleerd op een machine die voldoet aan de OpenStack- of PowerVC-vereisten. Zie *vRealize Automation installeren*.
- Controleer of uw OpenStack-versie momenteel wordt ondersteund. Zie *Ondersteuningsmatrix voor vRealize Automation*.

Nadat u een upgrade hebt uitgevoerd of bent gemigreerd van een eerdere vRealize Automation-installatie en het verzamelen van gegevens mislukt voor OpenStack-endpoints, kunt u de aangepaste `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name`-eigenschap toevoegen aan elk Keystone V3 OpenStack-endpoint om een geldige domeinnaam op te geven en het verzamelen van gegevens mogelijk te maken.

Procedure

- 1 Selecteer **Infrastructuur > Endpoints > Endpoints**.
- 2 Selecteer **Nieuw > Cloud > OpenStack**.
- 3 Voer een naam in en desgewenst een beschrijving.
- 4 Typ de URL voor het endpoint in het tekstvak **Adres**.

Optie	Beschrijving
PowerVC	De URL moet de notatie <code>http://myPowerVC.com:5000</code> of <code>http://FQDN:5000</code> hebben.
OpenStack	De URL moet de indeling <code>FQDN:5000</code> of <code>IP_address:5000</code> hebben. Neem het achtervoegsel <code>/v2.0</code> niet op in het endpointadres.

- 5 Voer uw gebruikersnaam en wachtwoord op beheerdersniveau in.
De verificatiegegevens die u opgeeft, moeten over de beheerdersrol beschikken in de OpenStack-tenant die gekoppeld is aan het endpoint.
- 6 Typ een OpenStack-tenantnaam in het tekstvak **OpenStack-project**.
Als u meerdere endpoints met verschillende OpenStack-tenants instelt, maakt u reserveringsbeleidsregels voor elke tenant. Dit zorgt ervoor dat machines worden ingericht op de juiste tenantbronnen.
- 7 Klik op **Eigenschappen** en voeg opgegeven aangepaste eigenschappen, eigenschapsgroepen of uw eigen eigenschapsdefinities voor het endpoint toe.
Als Keystone V3 in gebruik is, voert u de aangepaste eigenschap `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` toe om een specifiek domein aan te duiden.
- 8 Klik op **OK**.

Resultaten

vRealize Automation verzamelt gegevens van uw endpoint en ontdekt uw rekenbronnen.

Wat nu te doen

Voeg de computerbronnen van uw endpoint toe aan een materiaalgroep. Zie [Een materiaalgroep maken](#).

Een Hyper-V-, XenServer- of Xen Pool-endpoint maken

U kunt endpoints maken om vRealize Automation toestemming te geven om te communiceren met de Hyper-V-, XenServer- of Xen Pool-hoofdomgeving, en computerbronnen te ontdekken, gegevens te verzamelen en machines in te richten.

Voorwaarden

- Meld u aan bij vRealize Automation als een **IaaS-beheerder**.
- Een systeembeheerder moet een proxyagent installeren met opgeslagen verificatiegegevens die overeenkomen met uw endpoint. Zie *vRealize Automation installeren*.

Procedure

- 1 Selecteer **Infrastructuur > Endpoints > Agenten**.
- 2 Typ de volledig gekwalificeerde DNS-naam van uw Hyper-V-server, Xen-server of Xen-hoofdpool in het tekstvak **Computerbron**.

Opmerking In geval van een Xen-poolendpoint moet u de naam van de hoofdpool invoeren. Om dubbele vermeldingen te voorkomen in de vRealize Automation-tabel met computerbronnen, geeft u een adres op dat overeenkomt met het geconfigureerde hoofdadres van de Xen-pool. Als het hoofdadres van de Xen-pool bijvoorbeeld de hostnaam bevat, voert u de hostnaam en niet de FQDN in. Als het hoofdadres van de Xen-pool gebruikmaakt van FQDN, voert u de FQDN in.

- 3 Selecteer de proxyagent die uw systeembeheerder voor dit endpoint heeft geïnstalleerd in het vervolgkeuzemenu **Naam proxyagent**.
- 4 (Optioneel) Geef een beschrijving op in het tekstvak **Beschrijving**.
- 5 Klik op **OK**.

Resultaten

vRealize Automation verzamelt gegevens van uw endpoint en ontdekt uw rekenbronnen.

Wat nu te doen

Voeg de computerbronnen van uw endpoint toe aan een materiaalgroep. Zie [Een materiaalgroep maken](#).

Overwegingen bij het gebruik van Testverbinding

Met de bewerking Testverbinding kunt u de verificatiegegevens, het endpointadres van de host en het certificaat voor een vSphere-, NSX for vSphere-, NSX-T- en vRealize Operations Manager-endpoint valideren.

De actie controleert ook of de beheerservice en -agent actief zijn zodat gegevens voor het endpoint kunnen worden verzameld.

De actie **Testverbinding** retourneert informatie over een van de volgende voorwaarden:

- **Certificaatfout**

Als het certificaat niet wordt gevonden, vertrouwd of is verlopen, wordt u gevraagd een vingerafdruk van het certificaat te accepteren. Als u de vingerafdruk niet accepteert, kunt u het endpoint wel opslaan maar mislukt de inrichting van de machine mogelijk.

- **Agentfout**

De gekoppelde vSphere-agent is niet gevonden. Voor een succesvolle test moet de agent actief zijn.

- **Hostfout**

Het opgegeven endpointadres is niet bereikbaar of de gekoppelde beheerservice is niet actief. Voor een succesvolle test moet de managementservice actief zijn.

- **Verificatiegegevensfout**

De opgegeven combinatie van gebruikersnaam en wachtwoord is ongeldig voor het endpoint op het opgegeven adres.

- **Timeout**

De testactie kan niet worden voltooid in de toegestane tijdsperiode van twee minuten.

Als u foutmeldingen krijgt wanneer u **Verbinding testen** uitvoert op geüpgradede of gemigreerde endpoints, raadpleegt u [Overwegingen bij het werken met bijgewerkte of gemigreerde endpoints](#) voor de benodigde stappen om vertrouwen in certificaten in te stellen.

Endpoints via een programma importeren of exporteren

Als u via het programma endpoints wilt importeren en exporteren in vRealize Automation 7.3 of later, moet u ofwel nieuwe REST API's voor de vRealize Automation-endpointconfiguratieservice ofwel vRealize CloudClient gebruiken.

De vRealize CloudClient-documentatie bevat alle van toepassing zijnde informatie voor het opmaken van opdrachtregels, voorbeelden en gebruik.

U kunt de vRealize CloudClient-toepassing en documentatie downloaden van de vRealize CloudClient-productpagina van de <https://developercenter.vmware.com/tool/cloudclient>.

Computerbronnen bekijken en gegevensverzameling uitvoeren

U kunt de machine en de computingbron bekijken die zijn geassocieerd met een specifiek endpoint. U kunt de gegevensverzameling ook handmatig starten.

Voorwaarden

Controleer of ten minste één endpoint aanwezig is.

Procedure

1 Selecteer **Infrastructuur > Endpoints > Endpoints**.

Gebruikers die niet over IaaS-beheerdersrechten beschikken, kunnen **Infrastructuur > Computerbronnen > Computerbronnen** selecteren om bronnen weer te geven en gegevensverzameling uit te voeren vanaf de computerbron.

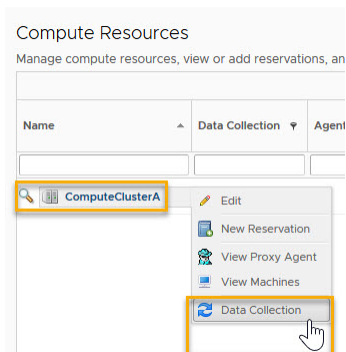
2 Selecteer **Infrastructuur > Endpoints > Endpoints**.

3 Selecteer een bestaande endpointrij en klik op **Acties**.

Selecteer een van de volgende beschikbare acties.

- Klik op **Computingbronnen weergeven** om de pagina **Infrastructuur > Computingbronnen** te openen. U kunt deze pagina gebruiken voor het bekijken en bewerken van instellingen voor computingbronnen. U kunt ook een gegevensverzameling uitvoeren voor een geselecteerde computerbron op de pagina **Computerbronnen**.
- Klik op **Machines weergeven** om de pagina **Infrastructuur > Beheerde machines** te openen.
- Klik op **Gegevensverzameling** om de pagina Gegevensverzameling te openen en te beginnen met de gegevensverzameling voor het endpoint. U kunt de pagina vernieuwen om de huidige status van de aanvraag weer te geven.

U kunt een gegevensverzameling uitvoeren vanaf de gekoppelde computerbron van het endpoint. Bijvoorbeeld: als u een gegevensverzameling wilt uitvoeren voor een bestaand NSX-T-endpoint, gebruikt u **Infrastructuur > Computerbronnen > Computerbronnen** om bronnen weer te geven en klikt u vervolgens op **Gegevensverzameling** om de pagina **Gegevensverzameling** voor de computerbron te openen. Zoek het gewenste endpoint in de lijst en klik op **Nu aanvragen**.



Overwegingen bij het werken met bijgewerkte of gemigreerde endpoints

Nadat u een lagere versie dan vRealize Automation 7.3 hebt geüpgraded of gemigreerd, is het belangrijk dat u de volgende overwegingen begrijpt en de nodige maatregelen kunt nemen.

Deze informatie geldt voor endpoints die zijn geüpgraded of gemigreerd naar deze versie van vRealize Automation.

- Wanneer u een upgrade uitvoert of migreert van een versie van vRealize Automation vóór 7.3, wordt elk vCloud Air-, vCloud Director- en Amazon-endpoint dat proxyinstellingen bevat geassocieerd met een nieuw proxyendpoint dat de proxyinstellingen bevat.

Na de upgrade of migratie is de nieuwe naam van het proxyendpoint Proxy_YYYYY, waarbij YYYYY door middel van een formule wordt berekend op basis van de URL, poort- en verificatiegegevens. Als u dezelfde proxyinstellingen (bijvoorbeeld dezelfde URL, poort en verificatiegegevens) hebt gebruikt voor een ander endpoint (bijvoorbeeld een vCloud Air- of Amazon-endpoint), is er na de upgrade of migratie nog slechts één proxyendpoint en een associatie tussen het vCloud Air- en Amazon-endpoint en het nieuwe proxyendpoint. Een proxyendpoint kan worden geassocieerd met meer dan één Amazon-, vCloud Air- of vCloud Director-endpoint.

- Wanneer u een upgrade uitvoert of migreert van vSphere-endpoints die NSX-beheerdersinstellingen bevatten, wordt elk vSphere-endpoint geassocieerd met een nieuw NSX-endpoint dat de NSX-beheerdersinstellingen bevat.

Na de upgrade of migratie is de naam van het NSX-endpoint NSX_XXXXX, waarbij XXXXX staat voor de naam van het bovenliggende vSphere-endpoint in de versie van vRealize Automation ouder dan 7.3.

- Wanneer de upgrade of migratie van vRealize Automation is voltooid, kan een infrastructuurbeheerder de namen van de nieuwe NSX- en proxyendpoints wijzigen.
- De standaardbeveiligingsinstelling voor bijgewerkte of gemigreerde endpoints is om uitsluitend vertrouwde certificaten te accepteren.
- Na de upgrade of migratie van een eerdere installatie van vRealize Automation, moet u als u niet-vertrouwde certificaten hebt gebruikt, de volgende stappen uitvoeren voor alle vSphere- en NSX-endpoints om certificaatvalidatie mogelijk te maken. Anders mislukken de endpointbewerkingen en zijn certificaatfouten het gevolg. Zie voor meer informatie de VMware Knowledge Base-artikelen *Communicatie met endpoint is verbroken na de upgrade naar vRA 7.3 (2150230)* op <http://kb.vmware.com/kb/2150230> en *Hoe u vCenter Server-rootcertificaten kunt downloaden en installeren om Web Browser-certificaatwaarschuwingen te vermijden (2108294)* op <http://kb.vmware.com/kb/2108294>.

- a Meld u na de upgrade of migratie aan bij de vRealize Automation vSphere-agentmachine en start uw vSphere-agenten opnieuw op. U doet dit op het tabblad **Services**.
Bij een migratie worden mogelijk niet alle agenten opnieuw opgestart. Start ze handmatig opnieuw op als dit nodig is.
- b Wacht tot er minimaal één pingrapport is voltooid. Een pingrapport is na een of twee minuten voltooid.
- c Meld u als IaaS-beheerder aan bij vRealize Automation wanneer de vSphere-agenten zijn begonnen met het verzamelen van gegevens.

- d Klik op **Infrastructuur > Endpoints > Endpoints**.
- e Bewerk een vSphere-endpoint en klik op **Testverbinding**.
- f Als er een certificaatvraag wordt weergegeven, klikt u op **OK** om het certificaat te accepteren.

Als er geen certificaatvraag wordt weergegeven, is het certificaat op dat moment mogelijk al juist opgeslagen in een vertrouwde hoofdautoriteit van de Windows-machine die als host van het endpoint fungeert, bijvoorbeeld als een proxyagentmachine of DEM-machine.

- g Klik op **OK** om het certificaat te accepteren en het endpoint op te slaan.
- h Herhaal deze procedure voor elk endpoint van vSphere.
- i Herhaal deze procedure voor elk endpoint van NSX.
- j Navigeer naar **Infrastructuur > Computerbronnen**, klik met de rechtermuisknop op uw **vCenter**-computerbron en voer **Gegevensverzameling** uit.

Als de actie **Testverbinding** succesvol is maar bepaalde onderdelen van het verzamelen van gegevens of van de inrichting mislukken, kunt u hetzelfde certificaat installeren op alle agentmachines die het endpoint bedienen en op alle DEM-machines. Of verwijder het certificaat van bestaande machines en herhaal de vorige procedure voor het endpoint waar dit fout gaat.

- De vRealize Automation REST API's waarmee programmatisch endpoints zijn gemaakt, bewerkt en verwijderd in vRealize Automation 7.2 en eerder, worden niet meer ondersteund in vRealize Automation 7.3 en later. Als u programmatisch endpoints wilt maken, bewerken en verwijderen in vRealize Automation 7.3 of later, moet u de nieuwe endpoint-configuratie-service-REST-API's voor vRealize Automation of vRealize CloudClient gebruiken.
- Nadat u een upgrade hebt uitgevoerd of bent gemigreerd van een eerdere vRealize Automation-installatie en het verzamelen van gegevens mislukt voor OpenStack-endpoints, kunt u de aangepaste `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name`-eigenschap toevoegen aan elk Keystone V3 OpenStack-endpoint om een geldige domeinnaam op te geven en het verzamelen van gegevens mogelijk te maken.
- Wanneer u een upgrade uitvoert van een extern IPAM-endpoint zoals Infoblox IPAM, wordt het vRealize Orchestrator-pakket dat de `RegisterIPAMEndpoint`-werkstroom bevat bijgewerkt. Het kan nodig zijn de werkstroom in vRealize Orchestrator opnieuw uit te voeren nadat de vRealize Automation-upgrade is voltooid.
- Als u verificatiegegevens voor meerdere endpoints wilt wijzigen, kunt u de endpoints afzonderlijk bewerken of vRealize CloudClient gebruiken om ze in een keer bij te werken.
- Voor bepaalde endpointtypen, zoals vCloud Air en vCloud Director, kan niet rechtstreeks een upgrade of migratie van vRealize Automation 6.2.x worden uitgevoerd naar vRealize Automation 7.3 of hoger.

- Als op de pagina **Infrastructuur > Endpoints** geen endpoints worden weergegeven of slechts bepaalde endpointtypen en endpoints worden weergegeven nadat u een upgrade of migratie naar vRealize Automation 7.3 hebt uitgevoerd, raadpleegt u [Knowledge Base-artikel 2150252](#) voor een tijdelijke oplossing.

Overwegingen bij het verwijderen van endpoints

U kunt bepaalde endpointtypen onder bepaalde voorwaarden verwijderen.

- U kunt endpoints waarvoor geen gegevens zijn verzameld verwijderen.
- U kunt een OpenStack-, Amazon- of VRO-endpoint verwijderen als er gegevens voor zijn verzameld, maar er geen reserveringen voor bestaan. Andere typen endpoints kunnen niet worden verwijderd als er gegevens voor zijn verzameld.
- U kunt een IPAM-endpoint van derden verwijderen als er geen associatie naar een netwerkprofiel voor bestaat.
- Wanneer een vSphere-endpoint wordt verwijderd, worden in de bevestigingsprompt de volgende afhankelijkheden gemeld:
 - Voor het endpoint zijn gegevens verzameld.
 - Naar het endpoint wordt verwezen in een reservering die is toegewezen aan een computerbron. U kunt een endpoint waarnaar wordt verwezen in een reservering niet verwijderen. Voor reserveringen is een computerbron vereist.
 - Het endpoint bevat een sjabloon waarnaar wordt verwezen in een bestaande blueprint. De blueprint wordt niet verwijderd wanneer u het endpoint verwijdert.
 - Het endpoint wordt gebruikt door virtual machines die in gebruik zijn.
- U kunt endpoints via een programma verwijderen door ofwel de nieuwe REST API's CREATE, EDIT en DELETE van de vRealize Automation- endpointconfiguratieservice te gebruiken die zijn geïntroduceerd in vRealize Automation 7.3 of door vRealize CloudClient te gebruiken. U kunt geen endpoints verwijderen via de REST API's voor de endpointconfiguratieservice van versies ouder dan vRealize Automation 7.3.

Problemen oplossen wanneer er geen gekoppelde endpoint voor vSphere kan worden gevonden

Wanneer de gegevensverzameling mislukt voor een vSphere-endpoint, wordt dit mogelijk veroorzaakt doordat de naam van de proxy en de naam van het endpoint niet overeenkomen.

Probleem

Gegevensverzameling voor een vSphere-endpoint mislukt. De logboekberichten retourneren een fout die er ongeveer zo uitziet:

Deze uitzondering is opgetreden: de gekoppelde endpoint 'vCenter' is niet gevonden.

Oorzaak

De endpointnaam die u configureert in vRealize Automation, moet overeenkomen met de endpointnaam die is opgegeven voor de vSphere-proxyagent tijdens de installatie. De gegevensverzameling voor een vSphere-endpoint mislukt als de naam van de endpoint niet overeenstemt met de naam van de proxyagent. Totdat een endpoint met een overeenstemmende naam wordt geconfigureerd, retourneren de logboekberichten een fout die er ongeveer zo uitziet:

Deze uitzondering is opgetreden: de gekoppelde endpoint '*verwachte endpointnaam*' is niet gevonden.

Oplossing

- 1 Selecteer **Infrastructuur > Controle > Logboek**.
- 2 Zoek naar een foutbericht Kan gekoppeld endpoint niet vinden.

Bijvoorbeeld:

Deze uitzondering is opgetreden: de gekoppelde endpoint '*verwachte endpointnaam*' is niet gevonden.

- 3 Bewerk de endpoint voor vSphere zodat de verwachte naam van de endpoint overeenstemt met de naam in het logboekbericht.
 - a Selecteer **Infrastructuur > Endpoints > Endpoints**.
 - b Klik op de naam van de endpoint die u wilt bewerken.
 - c Geef de verwachte naam van de endpoint op in het tekstvak **Naam**.
 - d Klik op **OK**.

Oplossing

De proxyagent kan communiceren met de endpoint en de gegevensverzameling is geslaagd.

Een materiaalgroep maken

U kunt infrastructuurbronnen in materiaalgroepen onderbrengen en een of meer materiaalbeheerders aanwijzen die de bronnen in de materiaalgroep beheren.

Materiaalgroepen zijn vereist voor virtuele en cloud-endpoints. U kunt meerdere gebruikers de rol van materiaalbeheerder geven door deze een voor een toe te voegen of een identiteitsarchiefgroep of aangepaste groep als materiaalbeheerder te kiezen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **IaaS-beheerder**.
- Maak ten minste één endpoint. Zie [Een endpointscenario kiezen](#).

Procedure

- 1 Selecteer **Infrastructuur > Endpoints > Materiaalgroepen**.

- 2 Klik op het pictogram **Nieuw** (+).
- 3 Geef een naam op in het tekstvak **Naam**.
- 4 (Optioneel) Geef een beschrijving op in het tekstvak **Beschrijving**.
- 5 Geef een gebruikersnaam of het e-mailadres van een gebruiker op in het tekstvak **Materiaalbeheerders**, klik op het pictogram Zoeken en selecteer het opgegeven e-mailadres.
Herhaal deze stap om meerdere gebruikers toe te voegen.
- 6 Selecteer een of meer **computerbronnen** die u in de materiaalgroep wilt opnemen.
Bij de gegevensverzameling worden alleen bronnen opgehaald die aanwezig zijn in de clusters die u voor de materiaalgroep hebt geselecteerd. Zo worden bijvoorbeeld alleen de sjablonen uit de geselecteerde clusters opgehaald en beschikbaar gesteld voor kloonbewerkingen op reserveringen die u voor bedrijfsgroepen maakt.
- 7 Klik op **OK**.

Resultaten

Vervolgens kunnen de materiaalbeheerders machinevoorvoegsels maken. Zie [Machinevoorvoegsels configureren](#).

Gebruikers die momenteel zijn aangemeld bij vRealize Automation, moeten zich afmelden en zich opnieuw aanmelden bij vRealize Automation voordat ze naar de pagina's kunnen navigeren waartoe ze toegang hebben gekregen.

Machinevoorvoegsels configureren

U kunt machinevoorvoegsels maken voor de namen van machines die worden ingericht met behulp van vRealize Automation. Een machinevoorvoegsel is vereist wanneer u machineonderdelen definieert op het ontwerpcanvas van een blueprint.

Een voorvoegsel is een basisnaam gevolgd door een teller met een specifiek aantal cijfers. Bij het laatste cijfer in de reeks keert vRealize Automation weer terug naar het eerste nummer.

Machinevoorvoegsels moeten aan de volgende beperkingen voldoen:

- Ze mogen alleen bestaan uit niet-hoofdlettergevoelige ASCII-letters a t/m z, de cijfers 0 t/m 9 en een koppelteken (-).
- Ze mogen niet met een koppelteken beginnen.
- Er mogen geen andere symbolen, interpunctietekens of spaties worden gebruikt.
- Ze mogen niet langer zijn dan 15 tekens, inclusief cijfers, zodat ze de Windows-limiet van 15 tekens voor hostnamen niet overschrijden.

Langere hostnamen worden afgekapt bij de inrichting van een machine en bijgewerkt zodra de volgende gegevensverzameling wordt uitgevoerd. Bij een WIM-inrichting worden de namen echter niet afgekapt. Daardoor zal de inrichting mislukken wanneer de opgegeven naam langer is dan 15 tekens.

- vRealize Automation biedt geen ondersteuning aan meerdere virtual machines met dezelfde naam die in één instantie worden gebruikt. Als de gekozen naamgevingsconventie ertoe leidt dat machinenaamen elkaar overlappen, zal vRealize Automation een machine met een redundante naam niet inrichten. Indien mogelijk probeert vRealize Automation de reeds gebruikte naam over te slaan en een nieuwe machinenaam te genereren op basis van het opgegeven machinevoorvoegsel. De inrichting mislukt als er geen unieke naam kan worden gegenereerd.

Voorwaarden

Meld u aan bij vRealize Automation als een **materiaalbeheerder**.

Procedure

- 1 Klik op **Infrastructuur > Beheer > Machinevoorvoegsels**.
- 2 Klik op het pictogram **Nieuw** (+).
- 3 Typ het machinevoorvoegsel in het tekstvak **Naam**.
- 4 Geef op of het machinevoorvoegsel wordt weergegeven in alle tenants of alleen in de huidige tenant in de kolom **Zichtbaarheid**.
- 5 Voer in het tekstvak **Aantal cijfers** het aantal cijfers van het machinevoorvoegsel in.
- 6 Voer in het tekstvak **Volgend nummer** het beginnummer van de teller in.
- 7 Klik op het pictogram **Opslaan** (✓).

Resultaten

Tenantbeheerders kunnen bedrijfsgroepen maken waarmee gebruikers bij de aanvraag van machines toegang krijgen tot vRealize Automation.

Een netwerkprofiel maken in vRealize Automation

Een netwerkprofiel bevat IP-gegevens, zoals een gateway, subnet en adresbereik. vRealize Automation gebruikt vSphere DHCP of een opgegeven IPAM-provider om IP-adressen toe te wijzen aan de machines die erdoor worden ingericht op basis van de instellingen voor netwerkprofielen.

U kunt een netwerkprofiel maken om het type van het beschikbare netwerk te definiëren. U kunt externe netwerkprofielen en -sjablonen maken voor profielen voor NAT-netwerken (Network Address Translation) op aanvraag en geleide of private netwerken op aanvraag. De profielen kunnen logische schakelopties voor NSX en de geschikte routeringsinstellingen voor een netwerkpad opbouwen.

Netwerkprofielen worden gebruikt om netwerkinstellingen te configureren wanneer machines worden ingericht. Ook bepalen netwerkprofielen de configuratie van NSX Edge-apparaten die worden gemaakt wanneer u machines inricht.

Beschikbare netwerktypen

De volgende netwerktypen zijn beschikbaar wanneer u een netwerkprofiel definieert:

- Bestaand netwerk
- Geleid netwerk op aanvraag
- NAT-netwerk op aanvraag
- Privaat netwerk op aanvraag (alleen NSX for vSphere)

Tabel 2-14. Beschikbare netwerktypen voor een vRealize Automation-netwerkprofiel

Netwerktipe	Beschrijving
Extern	<p>Bestaand netwerk dat is geconfigureerd op de vSphere-server. Deze zijn het externe gedeelte van de NAT- en geleide netwerktypen. Een extern netwerkprofiel kan een bereik definiëren van statische IP-adressen die beschikbaar zijn op het externe netwerk.</p> <p>U kunt IP-bereiken gebruiken die afkomstig zijn uit het geleverde VMware IPAM-endpoint of van een endpoint van een externe IPAM-serviceprovider dat u hebt geregistreerd en geconfigureerd in vRealize Orchestrator, zoals Infoblox IPAM. Een IP-bereik wordt gemaakt van een IP-blok tijdens de toewijzing.</p> <p>Een extern netwerkprofiel met een statisch IP-bereik is een voorwaarde voor NAT- en geleide netwerken.</p> <p>Zie Een extern netwerkprofiel maken voor een bestaand netwerk.</p>
NAT	<p>Netwerk op aanvraag dat wordt gemaakt tijdens het inrichten. NAT-netwerken die één set IP-adressen gebruiken voor externe communicatie en een andere set voor interne communicatie.</p> <p>Met een-op-een NAT-netwerken wordt aan elke virtual machine een extern IP-adres van het externe netwerkprofiel en een intern IP-adres van het NAT-netwerkprofiel toegewezen. Met een-op-veel NAT-netwerken delen alle machines één IP-adres van het externe netwerkprofiel voor externe communicatie.</p> <p>U kunt IP-bereiken gebruiken die afkomstig zijn uit het geleverde VMware IPAM-endpoint of van een endpoint van een externe IPAM-serviceprovider dat u hebt geregistreerd en geconfigureerd in vRealize Orchestrator, zoals Infoblox IPAM. Een IP-bereik wordt gemaakt van een IP-blok tijdens de toewijzing.</p> <p>Een NAT-netwerkprofiel definieert lokale en externe netwerken die een omzettingstabel gebruiken voor onderlinge communicatie.</p> <p>Zie Een NAT-netwerkprofiel maken voor een netwerk op aanvraag.</p>

Tabel 2-14. Beschikbare netwerktypen voor een vRealize Automation-netwerkprofiel (vervolg)

Netwerktipe	Beschrijving
Geleid	<p>Netwerk op aanvraag dat wordt gemaakt tijdens het inrichten. Geleide netwerken bevatten een routeerbare IP-ruimte die wordt verdeeld tussen subnetten die aan elkaar gekoppeld zijn met DLR (Distributed Logical Router).</p> <p>Aan elk nieuw geleid netwerk wordt het volgende beschikbare subnet toegewezen en dit wordt gekoppeld aan andere geleide netwerken die hetzelfde netwerkprofiel gebruiken. De virtual machines die zijn ingericht met geleide netwerken die hetzelfde geleide netwerkprofiel hebben, kunnen communiceren met elkaar en het externe netwerk.</p> <p>U kunt IP-bereiken gebruiken die afkomstig zijn uit het geleverde VMware IPAM-endpoint of van een endpoint van een externe IPAM-serviceprovider dat u hebt geregistreerd en geconfigureerd in vRealize Orchestrator, zoals Infoblox IPAM. Een IP-bereik wordt gemaakt van een IP-blok tijdens de toewijzing.</p> <p>Een geleid netwerkprofiel definieert een routeerbare ruimte en beschikbare subnetten.</p> <p>Zie Een gerouteerd netwerkprofiel maken voor een netwerk op aanvraag.</p>
Privé (alleen NSX for vSphere)	<p>Netwerk op aanvraag dat wordt gemaakt tijdens het inrichten. Deze optie is alleen beschikbaar voor NSX for vSphere. Deze optie is niet beschikbaar voor NSX-T.</p> <p>Private netwerken omvatten de volgende overwegingen:</p> <ul style="list-style-type: none"> ■ Private netwerken hebben geen binnenkomende of uitgaande connectiviteit. Er wordt geen Edge ingericht voor private netwerken. ■ U kunt een profiel voor een privaat netwerk met of zonder statische IP-adressen of -bereiken maken. DHCP en een externe IPAM worden niet ondersteund in private netwerken. <p>Zie Een profiel voor een privaat netwerk maken voor een netwerk op aanvraag in vRealize Automation.</p>

Voor NSX-informatie over netwerken raadpleegt u de [documentatie voor VMware NSX Data Center for vSphere](#) en de [documentatie voor VMware NSX-T Data Center](#).

Voor gerelateerde informatie over het configureren van netwerk en beveiliging voor NSX-T in vRealize Automation raadpleegt u het VMware-blogartikel [Application Networking and Security with vRealize Automation and NSX-T](#).

Meegeleverde of externe IPAM gebruiken

Netwerkprofielen ondersteunen ook externe IP-adresbeheerproviders (IP Address Management, IPAM) zoals Infoblox. Wanneer u een netwerkprofiel voor IPAM configureert, kunnen de machines die u hebt ingericht hun IP-adresgegevens en gerelateerde informatie zoals DNS en gateway ophalen van de geconfigureerde IPAM-oplossing. U kunt een extern IPAM-pakket voor een externe provider zoals Infoblox gebruiken om een IPAM-endpoint te definiëren dat u wilt gebruiken met een netwerkprofiel.

Opmerking Als u een IPAM-provider van derden gebruikt en wilt opgeven op welk netwerk uw machine moet worden geïmplementeerd, gebruikt u een apart netwerkprofiel voor elk VLAN om het bekende probleem zoals beschreven in het [Knowledge Base-artikel 2148656](#) te vermijden.

Als u geen externe IPAM-provider gebruikt maar in plaats daarvan het door vRealize Automation geleverde IPAM-endpoint gebruikt, kunt u de bereiken van IP-adressen opgeven waarvan de netwerkprofielen gebruik kunnen maken. Elk IP-adres in de opgegeven bereiken die aan een machine zijn toegewezen, wordt vrijgemaakt voor hertoewijzing wanneer de machine wordt vernietigd. U kunt een netwerkprofiel maken om een bereik van statische IP-adressen te definiëren die aan machines kunnen worden toegewezen. Als u virtual machines inricht door te klonen of door kickstart-/autoYaST-inrichting te gebruiken, kan de machine-eigenaar die de aanvraag doet, statische IP-adressen van een vooraf bepaald bereik toewijzen.

Een netwerkprofiel opgeven in een reservering of blueprint

U geeft een extern netwerkprofiel op wanneer u reserveringen en blueprints maakt. In een reservering kunt u een netwerkprofiel toewijzen aan een netwerkpad en kunt u een van deze paden opgeven voor een machineonderdeel in een blueprint. U kunt een netwerkprofiel vervolgens toewijzen aan een specifiek netwerkpad in een reservering. Voor sommige machineonderdeeltypen, zoals vSphere, kunt u een netwerkprofiel toewijzen wanneer u blueprints maakt of bewerkt.

U kunt een profiel voor een bestaand netwerk en een profiel voor een netwerk op aanvraag maken wanneer u netwerkadapters en load balancers definieert voor de vSphere-machine.

Als u een netwerkprofiel opgeeft in een reservering en een blueprint, krijgen de blueprintwaarden voorrang.

Wijzigingen aanbrengen na de implementatie van de blueprint

U kunt het netwerkprofiel van een geïmplementeerde virtual machine niet wijzigen, maar u kunt wel het netwerk wijzigen waarmee de VM is verbonden. Als het netwerk is geassocieerd met een ander netwerkprofiel, wijst vRealize Automation een IP-adres van het betreffende netwerkprofiel toe aan de VM. De VM blijft het oude IP-adres gebruiken totdat u het IP-adres op het gastbesturingssysteem bijwerkt. Als u de handeling Opnieuw configureren uitvoert op de geïmplementeerde VM moet u het IP-adres van het gastbesturingssysteem bijwerken.

Netwerkprofielen gebruiken om IP-adresbereiken te beheren

U kunt netwerkprofielen gebruiken om statische IP-adressen uit een vooraf gedefinieerd bereik toe te wijzen aan virtual machines die worden ingericht door te klonen of door gebruik te maken van Linux Kickstart of autoYaST of machines in de cloud op te nemen die zijn ingericht in OpenStack met behulp van Kickstart.

Standaard wordt in vRealize Automation DHCP (Dynamic Host Configuration Protocol) gebruikt om IP-adressen toe te wijzen aan ingerichte machines.

U kunt netwerkprofielen maken om een reeks statische IP-adressen te definiëren die u kunt toewijzen aan machines. U kunt deze netwerkprofielen vervolgens toewijzen aan specifieke netwerkpaden in een reservering. Machines die worden ingericht door te klonen of door kickstart of autoYaST en zijn gekoppeld aan een netwerkpad met een bijbehorend netwerkprofiel worden voorzien van een toegewezen statisch IP-adres. Voor inrichting met een statische IP-adrestoewijzing moet u een aanpassingsspecificatie gebruiken.

U kunt een netwerkprofiel toewijzen aan een vSphere-machineonderdeel in een blueprint door een bestaand netwerkonderdeel NAT op aanvraag of een geleid netwerkonderdeel op aanvraag aan het ontwerpcanvas toe te voegen en een netwerkprofiel te selecteren waarmee het vSphere-machineonderdeel moet worden verbonden. U kunt ook netwerkprofielen toewijzen aan blueprints door gebruik te maken van de aangepaste eigenschap `VirtualMachine.NetworkN.ProfileName`, waar *N* de netwerk-id is.

U kunt desgewenst het geleverde vRealize Automation IPAM-endpoint of een geregistreerd en geconfigureerd endpoint van een externe IPAM-serviceprovider in uw netwerkprofiel gebruiken om IP-adressen op te halen en te configureren. Raadpleeg [Checklist voor het bieden van ondersteuning voor externe IPAM-providers](#) voor informatie over externe IPAM-vereisten.

Als u een endpoint van een externe IPAM-serviceprovider in een netwerkprofiel selecteert, haalt vRealize Automation IP-bereiken uit het geregistreerde endpoint van de externe IPAM-provider, zoals Infoblox. Daarna wijst het IP-waarden van dat endpoint toe. Het opgegeven bereik subnetmasker wordt gebruikt om subnetten van het IP-blok toe te wijzen.

Als u een netwerkprofiel opgeeft in een reservering en een blueprint, krijgen de blueprintwaarden voorrang.

CSV-bestandsindeling voor het importeren van netwerkprofiel-IP-adressen

U kunt IP-adresnetwerkbereiken importeren naar een vRealize Automation-netwerkprofiel door gebruik te maken van een goed opgemaakt CSV-bestand.

De vermeldingen in het CSV-bestand moeten voldoen aan de volgende indeling.

CSV-veld	Beschrijving
<code>ip_address</code>	Een IP-adres in IPv4-indeling.
<code>machine_name</code>	Naam van een beheerde machine in vRealize Automation. Als het veld leeg is, is er standaard geen naam. Als het veld leeg is, kan de veldwaarde status niet Toegewezen zijn.
<code>status</code>	Toegewezen of Niet-toegewezen, hoofdlettergevoelig. Als het veld leeg is, is de standaardwaarde Niet-toegewezen. Als de status Toegewezen is, kan het veld <code>machine_name</code> niet leeg zijn.
<code>NIC_offset</code>	Een niet-negatief geheel getal. De NIC-offset geeft weer aan welke virtual machine-NIC het IP-adres is toegewezen. Als een virtual machine meer dan één IP-adres toewijst voor verschillende NIC's, is er een IP-adresvermelding voor elke NIC die de overeenkomstige NIC-offset bevat. Met de instelling 0 wordt geen offset opgegeven.

In het volgende voorbeeld wordt een machine weergegeven met IP-adres 100.10.100.1, de naam `mymachine01`, de status toegewezen en geen NIC-offset.

```
100.10.100.1,mymachine01,Unallocated,0
```

Scenario: IP-adressen uit een CSV-bestand importeren naar een netwerkprofiel

U kunt IP-adressen aan een netwerkprofielbereik toevoegen door een goed opgemaakt CSV-bestand te importeren. Ook kunt u de adressen in het netwerkprofielbereik wijzigen door het bereik in vRealize Automation te bewerken of door een gewijzigd of ander CSV-bestand te importeren.

U kunt de IP-adressen toevoegen aan een netwerkprofielbereik of erin wijzigen door ze uit een CSV-bestand te importeren of door ze handmatig in te voeren. U kunt in plaats daarvan IP-adressen laten toewijzen door een externe IPAM-provider.

- Importeer een initieel bereik van IP-adressen in een vRealize Automation-netwerkprofiel.
- Pas de geïmporteerde waarden toe om het eerste benoemde netwerkbereik in het netwerkprofiel te maken.
- Verwijder een of meer IP-adressen uit het netwerkbereik vRealize Automation.
- Importeer een gewijzigd of ander CSV-bestand om te zien hoe de netwerkbereikwaarden worden gewijzigd.

U kunt de optie **Importeren uit CSV** niet gebruiken voor netwerkprofielen die gebruikmaken van een extern IPAM-endpoint omdat de IP-adressen worden beheerd door de externe IPAM-provider, niet door vRealize Automation.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Maak een CSV-bestand met IP-adressen die u naar een netwerkbereik wilt importeren. Zie [Een extern netwerkprofiel maken via een externe IPAM-provider](#) en [CSV-bestandsindeling voor het importeren van netwerkprofiel-IP-adressen](#).

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Netwerkprofielen**.
- 2 Klik op **Nieuwen** selecteer een type netwerkprofiel in het vervolgkeuzemenu.
Voor dit voorbeeld selecteert u *Extern*.
- 3 Voer in het tekstvak **NaamMijn netwerkprofiel met CSV** in.
- 4 Voer in het tekstvak **BeschrijvingIP-adressen netwerkbereik testen met CSV** in.
De optie voor het importeren van het CSV-bestand is van toepassing op instellingen op de tabbladpagina's **Netwerkbereiken** en **IP-adressen**.
- 5 (Optioneel) Selecteer een geconfigureerd IPAM-endpoint als dit beschikbaar is. Als er geen endpoint beschikbaar is, slaat u deze stap over.
- 6 Voer in de tekstvakken **Subnetmasker** en **Gateway** een geschikte IP-adreswaarde in.
- 7 Klik op het tabblad **DNS**.
- 8 Voer relevante informatie in zoals een DNS-achtervoegsel en klik op het tabblad **Netwerkbereiken**.

De optie **Importeren uit CSV** is beschikbaar wanneer u op het tabblad **Netwerkbereiken** klikt.

- 9 Als u handmatig een nieuwe netwerkbereiknaam en IP-adresbereik wilt invoeren, klikt u op **Nieuw**, of als u IP-informatie uit een correct opgemaakt CSV-bestand wilt importeren, klikt u op **Importeren uit CSV**.

■ Klik op **Nieuw**.

- Voer een nieuwe naam voor het netwerkbereik in.
- Voer een nieuwe netwerkbereikbeschrijving in.
- Voer het eerste IP-adres van het bereik in.
- Voer het laatste IP-adres van het bereik in.

■ Klik op **Importeren uit CSV**.

- Ga naar het CSV-bestand en selecteer het of verplaats het CSV-bestand naar het dialoogvenster **Importeren uit CSV**.

Een rij in het CSV-bestand heeft de indeling *ip_address, machine_name, status, NIC_offset*. Bijvoorbeeld:

```
100.10.100.1,mymachine01,Allocated,0
```

CSV-veld	Beschrijving
ip_address	Een IP-adres in IPv4-indeling.
machine_name	Naam van een beheerde machine in vRealize Automation. Als het veld leeg is, is er standaard geen naam. Als het veld leeg is, kan de veldwaarde status niet Toegewezen zijn.
status	Toegewezen of Niet-toegewezen, hoofdlettergevoelig. Als het veld leeg is, is de standaardwaarde Niet-toegewezen. Als de status Toegewezen is, kan het veld machine_name niet leeg zijn.
NIC_offset	Een niet-negatief geheel getal. De NIC-offset geeft weer aan welke virtual machine-NIC het IP-adres is toegewezen. Als een virtual machine meer dan één IP-adres toewijst voor verschillende NIC's, is er een IP-adresvermelding voor elke NIC die de overeenkomstige NIC-offset bevat. Met de instelling 0 wordt geen offset opgegeven.

- Klik op **Toepassen**.

- 10 Klik op **OK**.

De IP-adressen in het bereik verschijnen in de gedefinieerde IP-adressenlijst.

De IP-adressen worden weergegeven wanneer u op **Toepassen** klikt of nadat u het netwerkprofiel hebt opgeslagen en vervolgens bewerkt.

- 11 Als u de IP-adresgegevens voor de opgegeven bereikadresruimte wilt weergeven, klikt u op het tabblad **IP-adressen**.

Als u de IP-adresinformatie hebt geïmporteerd uit een CSV-bestand, wordt de bereiknaam gegenereerd als *Geïmporteerd uit CSV*.

- 12** (Optioneel) Als u IP-adresvermeldingen wilt filteren, selecteert u een IP-adres in het vervolgkeuzemenu **Netwerkbereik**.

U kunt informatie tonen over de gedefinieerde netwerkbereiken, de netwerkbereiken die zijn geïmporteerd uit een CSV-bestand of een benoemd netwerkbereik.

Wat nu te doen

Als u opnieuw IP-adressen uit een CSV-bestand importeert, worden de vorige IP-adressen vervangen door de gegevens uit het geïmporteerde CSV-bestand.

Een extern netwerkprofiel maken voor een bestaand netwerk

U kunt externe netwerkprofielen maken om de netwerkinstellingen op te geven om bestaande netwerken te configureren voor de inrichting van machines, inclusief de configuratie van NSX Edge-apparaten die tijdens het inrichten worden gebruikt.

U kunt het meegeleverde endpoint voor de vRealize Automation IPAM-provider gebruiken of het endpoint van een externe IPAM-provider, zoals Infoblox, dat u hebt geregistreerd in vRealize Orchestrator.

Een extern netwerkprofiel maken met het meegeleverde IPAM-endpoint

U kunt een extern netwerkprofiel maken om externe netwerkeigenschappen en een bereik van statische IP-adressen te definiëren die moeten worden gebruikt bij het inrichten van machines op een bestaand netwerk.

U kunt een of meer netwerkbereiken van statische IP-adressen in het netwerkprofiel definiëren voor gebruik bij het inrichten van een machine. Als u geen bereik opgeeft, kunt u een netwerkprofiel gebruiken als netwerkreserveringsbeleid om een reserveringsnetwerkpad te selecteren voor de netwerkkaart van een virtual machine (vNIC).

Zie [Een extern netwerkprofiel maken via een externe IPAM-provider](#) voor informatie over het maken van een extern netwerkprofiel en het gebruik van een endpoint van een externe IPAM-provider.

Procedure

1 [Informatie voor externe netwerkprofielen opgeven via het meegeleverde IPAM-endpoint](#)

Met een extern netwerkprofiel identificeert u netwerkeigenschappen en instellingen voor een bestaand netwerk. Een extern netwerkprofiel is een vereiste van NAT- en geleide netwerkprofielen.

2 [IP-bereiken voor externe netwerkprofielen configureren via het meegeleverde IPAM-endpoint](#)

U kunt een of meer netwerkbereiken van statische IP-adressen in het netwerkprofiel definiëren voor gebruik bij het inrichten van een machine. Als u geen bereik opgeeft, kunt u een netwerkprofiel gebruiken als netwerkreserveringsbeleid om een reserveringsnetwerkpad te selecteren voor de netwerkkaart van een virtual machine (vNIC).

Wat nu te doen

U kunt een netwerkprofiel toewijzen aan een netwerkpad in een reservering of een architect van blueprints kan het netwerkprofiel in een blueprint opgeven. U kunt het externe netwerkprofiel gebruiken wanneer u een on-demand NAT of geleid netwerkprofiel wilt maken.

Informatie voor externe netwerkprofielen opgeven via het meegeleverde IPAM-endpoint
Met een extern netwerkprofiel identificeert u netwerkeigenschappen en instellingen voor een bestaand netwerk. Een extern netwerkprofiel is een vereiste van NAT- en geleide netwerkprofielen.

Voor meer informatie over hoe u een extern netwerkprofiel kunt maken door IPAM-adresgegevens te verkrijgen van een geregistreerd extern IPAM-endpoint zoals Infoblox, raadpleegt u [Checklist voor het bieden van ondersteuning voor externe IPAM-providers](#) en [Een extern netwerkprofiel maken via een externe IPAM-provider](#). Voer de volgende procedure uit om een netwerkprofiel te maken met behulp van het VMware interne IPAM-endpoint.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Netwerkprofielen**.
- 2 Klik op **Nieuw** en selecteer **Extern** in het vervolgkeuzemenu.
- 3 Voer een naam in en desgewenst een beschrijving.
- 4 Accepteer de standaardwaarde **IPAM-endpoint** voor het opgegeven endpoint **vRealize Automation IPAM**.
- 5 Voer een IP-subnetmasker in het tekstveld **Subnetmasker** in.

Het subnetmasker bepaalt de grootte van de volledige routeerbare adresruimte die u voor uw netwerkprofiel wilt definiëren.
Voer bijvoorbeeld 255.255.0.0 in.
- 6 Voer een adres van een geleide gateway in, bijvoorbeeld 10.10.110.1, in het tekstvak **Gateway**.

Het IP-adres van de gateway dat is gedefinieerd in het netwerkprofiel, wordt toegekend aan de NIC tijdens de toewijzing. De gateway is vereist voor NAT-netwerkprofielen.

De standaardgateway van de DHCP-server voor NSX-T komt overeen met de NAT een-op-veel-standaardgateway. De standaardgateway van de IP-pool komt overeen met de NAT één-op-veel standaardgateway in vRealize Automation.

Als geen waarde is opgegeven in het tekstvak **Gateway** in het netwerkprofiel, moet u de aangepaste eigenschap `VirtualMachine.Network0.Gateway` gebruiken om een gateway toe te wijzen.
- 7 Klik op het tabblad **DNS**.

8 Voer indien nodig de DNS- en WINS-waarden in.

Gebruik DNS-waarden voor de naamregistratie en -omzetting. De waarden zijn optioneel voor interne IPAM. De waarden worden geleverd door de externe IPAM-provider voor externe IPAM.

- a (Optioneel) Voer een **Primaire DNS**-serverwaarde in.
- b (Optioneel) Voer een **Secundaire DNS**-serverwaarde in.
- c (Optioneel) Voer een waarde voor **DNS-achtervoegsels** in.
- d (Optioneel) Voer een waarde voor **DNS-zoekachtervoegsels** in.
- e (Optioneel) Voer een **Preferred WINS**-serverwaarde in.
- f (Optioneel) Voer een **Alternate WINS**-serverwaarde in.

Wat nu te doen

U kunt IP-bereiken configureren voor statische IP-adressen. Zie [IP-bereiken voor externe netwerkprofielen configureren via het meegeleverde IPAM-endpoint](#).

IP-bereiken voor externe netwerkprofielen configureren via het meegeleverde IPAM-endpoint
U kunt een of meer netwerkbereiken van statische IP-adressen in het netwerkprofiel definiëren voor gebruik bij het inrichten van een machine. Als u geen bereik opgeeft, kunt u een netwerkprofiel gebruiken als netwerkreserveringsbeleid om een reserveringsnetwerkpad te selecteren voor de netwerkkaart van een virtual machine (vNIC).

U kunt IP-bereikwaarden handmatig definiëren vanuit een geïmporteerd CSV-bestand of door IP-adressen te gebruiken die door een externe IPAM-provider worden geleverd. U kunt handmatig gedefinieerde IP-bereiken combineren met IP-adressen die zijn geïmporteerd via CSV. U kunt bijvoorbeeld sommige bereiken definiëren met behulp van de gebruikersinterface en andere importeren vanuit een CSV-bestand.

Als u een tweede keer importeert vanuit een CSV-bestand, ongeacht de naam van het CSV-bestand, worden de IP-bereiken die zijn geïmporteerd vanuit het vorige CSV-bestand gewist en wordt de nieuwe IP-bereikinformatie toegevoegd. De vorige import wordt dus overschreven wanneer u twee of meer keer importeert. U kunt het proces van het bijwerken van een CSV-bestand en opnieuw importeren van dat CSV-bestand in het netwerkprofiel onbeperkt herhalen.

Als in een extern netwerkprofiel geen IP-bereiken zijn gedefinieerd, kunt u dit gebruiken om op te geven welk netwerk wordt gekozen voor een virtuele netwerkkaart (vNIC). Als u het bestaande netwerkprofiel gebruikt in een geleid of NAT-netwerkprofiel, moet het ten minste één statisch IP-bereik bevatten.

Voorwaarden

[Informatie voor externe netwerkprofielen opgeven via het meegeleverde IPAM-endpoint](#).

Procedure

1 Klik op het tabblad **Netwerkbereiken**.

- 2 Als u handmatig een nieuwe netwerkbereiknaam en IP-adresbereik wilt invoeren, klikt u op **Nieuw**, of als u IP-informatie uit een correct opgemaakt CSV-bestand wilt importeren, klikt u op **Importeren uit CSV**.

■ Klik op **Nieuw**.

- Voer een nieuwe naam voor het netwerkbereik in.
- Voer een nieuwe netwerkbereikbeschrijving in.
- Voer het eerste IP-adres van het bereik in.
- Voer het laatste IP-adres van het bereik in.

■ Klik op **Importeren uit CSV**.

- Ga naar het CSV-bestand en selecteer het of verplaats het CSV-bestand naar het dialoogvenster **Importeren uit CSV**.

Een rij in het CSV-bestand heeft de indeling *ip_address, machine_name, status, NIC_offset*. Bijvoorbeeld:

```
100.10.100.1,mymachine01,Allocated,0
```

CSV-veld	Beschrijving
ip_address	Een IP-adres in IPv4-indeling.
machine_name	Naam van een beheerde machine in vRealize Automation. Als het veld leeg is, is er standaard geen naam. Als het veld leeg is, kan de veldwaarde status niet Toegewezen zijn.
status	Toegewezen of Niet-toegewezen, hoofdlettergevoelig. Als het veld leeg is, is de standaardwaarde Niet-toegewezen. Als de status Toegewezen is, kan het veld machine_name niet leeg zijn.
NIC_offset	Een niet-negatief geheel getal. De NIC-offset geeft weer aan welke virtual machine-NIC het IP-adres is toegewezen. Als een virtual machine meer dan één IP-adres toewijst voor verschillende NIC's, is er een IP-adresvermelding voor elke NIC die de overeenkomstige NIC-offset bevat. Met de instelling 0 wordt geen offset opgegeven.

- Klik op **Toepassen**.

- 3 Klik op **OK**.

De IP-adressen in het bereik verschijnen in de gedefinieerde IP-adressenlijst.

De IP-adressen worden weergegeven wanneer u op **Toepassen** klikt of nadat u het netwerkprofiel hebt opgeslagen en vervolgens bewerkt.

- 4 Als u de IP-adresgegevens voor de opgegeven bereikadresruimte wilt weergeven, klikt u op het tabblad **IP-adressen**.

Als u de IP-adresinformatie hebt geïmporteerd uit een CSV-bestand, wordt de bereiknaam gegenereerd als *Geïmporteerd uit CSV*.

- 5 (Optioneel) Als u IP-adresvermeldingen wilt filteren, selecteert u een IP-adres in het vervolgkeuzemenu **Netwerkbereik**.

U kunt informatie tonen over de gedefinieerde netwerkbereiken, de netwerkbereiken die zijn geïmporteerd uit een CSV-bestand of een benoemd netwerkbereik.

- 6 (Optioneel) Als u IP-adressen wilt filteren die overeenkomen met de IP-status, selecteert u een statustype in het vervolgkeuzemenu **IP-status**.

Voor IP-adressen die verlopen of vernietigd zijn, kunt u klikken op **Herstellen** om deze adressen voor toewijzing beschikbaar te maken. U dient het profiel op te slaan om het herstel uit te voeren. Het kan een minuut duren voordat de kolom Status is bijgewerkt van Expired of Destroyed naar Allocated.

- 7 Klik op **OK** om het netwerkprofiel te voltooien.

Resultaten

U kunt een netwerkprofiel toewijzen aan een netwerkpad in een reservering of een architect van blueprints kan het netwerkprofiel in een blueprint opgeven. Als u een extern netwerkprofiel hebt gemaakt, kunt u het externe netwerkprofiel gebruiken als u een NAT- of geleid netwerkprofiel maakt.

Een extern netwerkprofiel maken via een externe IPAM-provider

Als u een IPAM-oplossing van derden hebt geïmporteerd, geconfigureerd en geregistreerd in vRealize Orchestrator, kunt u deze gebruiken om IP-adressen op te halen van die externe provider.

U kunt een extern netwerkprofiel maken dat een endpoint van een geregistreerde externe IPAM-provider gebruikt om de instellingen voor de gateway, het subnetmasker en DHCP/WINS op te halen.

U kunt een of meer netwerkbereiken van statische IP-adressen in het netwerkprofiel definiëren voor gebruik bij het inrichten van een machine. Als u geen bereik opgeeft, kunt u een netwerkprofiel gebruiken als netwerkeserveringsbeleid om een reserveringsnetwerkpad te selecteren voor de netwerkkaart van een virtual machine (vNIC).

Zie [Een extern netwerkprofiel maken met het meegeleverde IPAM-endpoint](#) voor informatie over het maken van een extern netwerkprofiel zonder een IPAM-provider te gebruiken of door het endpoint van de opgegeven interne IPAM-provider te gebruiken.

Procedure

- 1 [Informatie opgeven over een extern netwerkprofiel met behulp van een extern IPAM-endpoint](#)

Met een extern netwerkprofiel identificeert u netwerkeigenschappen en instellingen voor een bestaand netwerk. Een extern netwerkprofiel is een vereiste van NAT- en geleide netwerkprofielen. Als u een IPAM-endpoint hebt geregistreerd en geconfigureerd in vRealize Orchestrator, kunt u aangeven dat IP-adresinformatie moet worden verstrekt door een IPAM-provider.

2 IP-bereiken voor externe netwerkprofielen configureren via een IPAM-endpoint van derden

U kunt een of meer netwerkbereiken van statische IP-adressen in het netwerkprofiel definiëren voor gebruik bij het inrichten van een machine. Als u geen bereik opgeeft, kunt u een netwerkprofiel gebruiken als netwerkreserveringsbeleid om een reserveringsnetwerkpad te selecteren voor de netwerkkaart van een virtual machine (vNIC).

Wat nu te doen

U kunt een netwerkprofiel toewijzen aan een netwerkpad in een reservering of een architect van blueprints kan het netwerkprofiel in een blueprint opgeven. U kunt het externe netwerkprofiel gebruiken wanneer u een on-demand NAT of geleid netwerkprofiel wilt maken.

Informatie opgeven over een extern netwerkprofiel met behulp van een extern IPAM-endpoint
Met een extern netwerkprofiel identificeert u netwerkeigenschappen en instellingen voor een bestaand netwerk. Een extern netwerkprofiel is een vereiste van NAT- en geleide netwerkprofielen. Als u een IPAM-endpoint hebt geregistreerd en geconfigureerd in vRealize Orchestrator, kunt u aangeven dat IP-adresinformatie moet worden verstrekt door een IPAM-provider.

Voorwaarden

- Verzeker u ervan dat u een invoegtoepassing van een externe IPAM-provider hebt geïmporteerd en geconfigureerd in vRealize Orchestrator en een endpointtype van de IPAM-provider hebt geregistreerd in vRealize Orchestrator. In dit voorbeeld is de ondersteunde externe IPAM-oplossingsprovider Infoblox. Zie [Checklist voor het bieden van ondersteuning voor externe IPAM-providers](#).
- [Een endpoint van een externe IPAM-provider maken](#).
- Configureer de vRealize Orchestrator Appliance met de geregistreerde IPAM-endpointwerkstroom als de standalone Orchestrator in de global tenant (administrator@vsphere.local).
- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Netwerkprofielen**.
- 2 Klik op **Nieuw** en selecteer **Extern** in het vervolgkeuzemenu.
- 3 Voer een naam in en desgewenst een beschrijving.
- 4 Als u één of meer endpoints van een externe IPAM-provider hebt geconfigureerd, selecteert u een extern IPAM-endpoint in het vervolgkeuzemenu **IPAM-endpoint**.

Als u een endpoint van een externe IPAM-provider selecteert dat u hebt geregistreerd in vRealize Orchestrator, verkrijgt u IP-adressen van de opgegeven IPAM-serviceprovider.

Wat nu te doen

U kunt nu netwerkbereiken definiëren voor IP-adressen voor het afronden van de netwerkprofieldefinitie.

IP-bereiken voor externe netwerkprofielen configureren via een IPAM-endpoint van derden
U kunt een of meer netwerkbereiken van statische IP-adressen in het netwerkprofiel definiëren voor gebruik bij het inrichten van een machine. Als u geen bereik opgeeft, kunt u een netwerkprofiel gebruiken als netwerkeserveringsbeleid om een reserveringsnetwerkpad te selecteren voor de netwerkkaart van een virtual machine (vNIC).

U kunt IP-bereiken definiëren door de IP-adressen te gebruiken die zijn geleverd door een externe IPAM-provider.

vRealize Automation slaat alleen bereik-ID's op in de externe IPAM in de database, geen bereikdetails. Als u een netwerkprofiel op deze pagina of op een blueprint bewerkt, roept vRealize Automation de IPAM-service aan om bereikdetails op te halen op basis van de geselecteerde bereik-ID's.

Opmerking Er is een bekend probleem met bepaalde externe IPAM-providers waarbij een time-out kan plaatsvinden bij een query tijdens het weergeven van de netwerkbereiken, wat resulteert in een lege lijst. U kunt deze time-out voorkomen door zoekcriteria op te stellen en de gegevens over het netwerkbereik te verkrijgen.

Afhankelijk van uw IPAM-provider kunt u bijvoorbeeld een eigenschap genaamd VLAN aan elk netwerk in de toepassing van de IPAM-provider toevoegen en aan die eigenschap een waarde toekennen, zoals 4. U kunt vervolgens filteren op de eigenschap en de waarde, bijvoorbeeld VLAN=4, in het tekstvak **Netwerkbereik selecteren** op de profielpagina van het vRealize Automation-netwerk.

Een alternatieve methode is de time-outinstelling te verhogen door middel van de volgende procedure:

- 1 Open het bestand `/etc/vcac/webapps/o11n-gateway-service/WEB-INF/classes/META-INF/spring/root/o11n-gateway-service-context.xml` in elk van de vRealize Automation-toepassingsknooppunten.
 - 2 Wijzig de time-outwaarde van 30 seconden naar een hoger getal.
 - 3 Start de vcac-server opnieuw op door service `vcac-server` `restart` in te voeren.
-

Voorwaarden

[Informatie opgeven over een extern netwerkprofiel met behulp van een extern IPAM-endpoint.](#)

Procedure

- 1 Als u een netwerkbereik wilt maken of een bestaand netwerkbereik wilt selecteren, klikt u op het tabblad **Netwerkbereiken**.
- 2 Selecteer een adresruimte uit de lijst met alle adresruimten die beschikbaar zijn voor het endpoint via het vervolgkeuzemenu **Adresruimte**.

- 3 Klik op **Toevoegen** en selecteer een of meer beschikbare netwerkbereiken voor de specifieke adresruimte.

Als u een netwerkbereik selecteert, kan dit resulteren in een lege lijst als u een externe IPAM-provider gebruikt. Bekijk voor details het Knowledge Base-artikel 2148656 op <http://kb.vmware.com/kb/2148656>.

- 4 Klik op **OK**.

De IP-adressen in het bereik verschijnen in de gedefinieerde IP-adressenlijst.

De IP-adressen worden weergegeven wanneer u op **Toepassen** klikt of nadat u het netwerkprofiel hebt opgeslagen en vervolgens bewerkt.

- 5 Klik op **OK** om het netwerkprofiel te voltooien.

Wat nu te doen

U kunt een netwerkprofiel toewijzen aan een netwerkpad in een reservering of een architect van blueprints kan het netwerkprofiel in een blueprint opgeven.

Een gerouteerd netwerkprofiel maken voor een netwerk op aanvraag

U kunt een gerouteerd netwerkprofiel op aanvraag maken dat de geleverde vRealize Automation-IPAM-endpoint gebruikt of een correct geconfigureerd en geregistreerd IPAM-endpoint van derden.

Een geleid netwerkprofiel staat voor een routeerbare IP-ruimte die over meerdere netwerken is verdeeld. In elk geleide netwerk wordt het volgende beschikbare subnet toegewezen in de routeerbare IP-ruimte. Een geleid netwerk heeft toegang tot alle andere geleide netwerken die hetzelfde netwerkprofiel gebruiken. Elk geleid subnet heeft toegang tot alle andere subnets die zijn gemaakt met behulp van hetzelfde netwerkprofiel.

Bij een externe IPAM-provider wordt de routeerbare IP-ruimte gemaakt en beheerd door de externe IPAM-provider. De netwerkbeheerder gebruikt een externe IPAM-provider om een routeerbare IP-ruimte te definiëren en er een IP-blok voor te maken. U kunt één of meer IP-blokken selecteren die zijn verkregen van de externe IPAM-provider als u een gerouteerd netwerkprofiel maakt of bewerkt.

Om een nieuwe instantie van het geleide netwerkprofiel van de externe IPAM-provider toe te wijzen, verstuurt vRealize Automation een oproep naar de provider om het volgende beschikbare subnet te reserveren en een bereik te maken van IP-blokken conform het geleide netwerkprofiel en de subnetgrootte. Het resulterende bereik wordt gebruikt voor het toewijzen van IP-adressen aan machines die samen met het NAT-netwerk worden geïmplementeerd.

Een geleid netwerkprofiel maken met het meegeleverde IPAM-endpoint

Als u een geleid netwerkprofiel gebruikt met het meegeleverde IPAM-endpoint, kunt u een routeerbare IP-ruimte met beschikbare subnetten definiëren voor een geleid netwerk op aanvraag.

Via het meegeleverde vRealize Automation IPAM-endpoint kunt u bereiken van statische IP-adressen en een basis-IP-adres voor het geleide netwerkprofiel maken.

U kunt IP-bereiken gebruiken die afkomstig zijn uit het geleverde VMware IPAM-endpoint of van een endpoint van een externe IPAM-serviceprovider dat u hebt geregistreerd en geconfigureerd in vRealize Orchestrator, zoals Infoblox IPAM. Een IP-bereik wordt gemaakt van een IP-blok tijdens de toewijzing.

Procedure

1 [Informatie opgeven voor een geleid netwerkprofiel met het vRealize Automation IPAM-endpoint](#)

De netwerkprofielinformatie identificeert de geleide netwerkeigenschappen, het onderliggende externe netwerkprofiel ervan en andere waarden die bij de inrichting van het netwerk worden gebruikt, wanneer gebruik wordt gemaakt van het geleverde IPAM-endpoint.

2 [IP-bereiken configureren voor een geleid netwerkprofiel met het vRealize Automation IPAM-endpoint](#)

U kunt een of meer bereiken van statische IP-adressen definiëren voor gebruik bij het inrichten van een netwerk.

Informatie opgeven voor een geleid netwerkprofiel met het vRealize Automation IPAM-endpoint
De netwerkprofielinformatie identificeert de geleide netwerkeigenschappen, het onderliggende externe netwerkprofiel ervan en andere waarden die bij de inrichting van het netwerk worden gebruikt, wanneer gebruik wordt gemaakt van het geleverde IPAM-endpoint.

Zie [Informatie opgeven voor een geleid netwerkprofiel met een extern IPAM-endpoint](#) als u een geleid netwerkprofiel wilt maken met een IPAM-endpoint van derden.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Maak een extern netwerkprofiel. Zie [Een extern netwerkprofiel maken met het meegeleverde IPAM-endpoint](#).

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Netwerkprofielen**.
- 2 Klik op **Nieuw** en selecteer **Geleid** in het vervolgkeuzemenu.
- 3 Voer een naam in en desgewenst een beschrijving.
- 4 Accepteer de standaardwaarde **IPAM-endpoint** voor het opgegeven endpoint **vRealize Automation IPAM**.
- 5 Selecteer een bestaand extern netwerkprofiel in het vervolgkeuzemenu **Extern netwerkprofiel**.

- 6 Voer het subnetmasker in het tekstveld **Subnetmasker** in dat is gekoppeld aan het externe netwerkprofiel.

Het subnetmasker bepaalt de grootte van de volledige routeerbare adresruimte die voor uw netwerkprofiel moet worden gedefinieerd.

Voer bijvoorbeeld 255.255.0.0 in.

- 7 Selecteer een waarde in het vervolgkeuzemenu van het tekstvak **Bereik subnetmasker**.

Voer bijvoorbeeld 255.255.255.0 in.

Het subnetmaskerbereik definieert hoe u de netwerkruimte in afzonderlijke adresblokken wilt partitioneren. De blokken worden toegewezen aan elke implementatie-instantie van het netwerkprofiel.

Voor elke implementatie die gebruikmaakt van een geleid netwerkprofiel gebruikt u een bereik. Het aantal beschikbare geleide bereiken is gelijk aan het subnetmasker gedeeld door het bereik subnetmasker, bijvoorbeeld $255.255.0.0 / 255.255.255.0 = 256$.

- 8 Voer het eerste beschikbare IP adres in het tekstveld **Basis-IP** in.

Deze optie is niet beschikbaar voor externe endpoints.

Voer bijvoorbeeld 120.120.0.1 in.

- 9 Klik op het tabblad **DNS**.

- 10 Voer indien nodig de DNS- en WINS-waarden in.

Gebruik DNS-waarden voor de naamregistratie en -omzetting. De waarden zijn optioneel voor interne IPAM. De waarden worden geleverd door de externe IPAM-provider voor externe IPAM.

- a (Optioneel) Voer een **Primaire DNS**-serverwaarde in.
- b (Optioneel) Voer een **Secundaire DNS**-serverwaarde in.
- c (Optioneel) Voer een waarde voor **DNS-achtervoegsels** in.
- d (Optioneel) Voer een waarde voor **DNS-zoekachtervoegsels** in.
- e (Optioneel) Voer een **Preferred WINS**-serverwaarde in.
- f (Optioneel) Voer een **Alternate WINS**-serverwaarde in.

Wat nu te doen

[IP-bereiken configureren voor een geleid netwerkprofiel met het vRealize Automation IPAM-endpoint.](#)

IP-bereiken configureren voor een geleid netwerkprofiel met het vRealize Automation IPAM-endpoint

U kunt een of meer bereiken van statische IP-adressen definiëren voor gebruik bij het inrichten van een netwerk.

Tijdens inrichting wijst elk nieuw geleid netwerk het volgende beschikbare bereik toe en gebruikt het dit als zijn IP-ruimte.

Voorwaarden

[Informatie opgeven voor een geleid netwerkprofiel met het vRealize Automation IPAM-endpoint.](#)

Procedure

- 1 Als u een netwerkbereik wilt maken of een bestaand netwerkbereik wilt selecteren, klikt u op het tabblad **Netwerkbereiken**.
- 2 Klik op **Bereiken genereren** om netwerkbereiken te genereren op basis van het subnetmasker, het subnetmasker van het bereik en de basisinformatie over het IP-adres dat u op het tabblad Algemeen hebt ingevoerd.

Te beginnen met het basis-IP-adres genereert vRealize Automation bereiken op basis van het bereik van het subnetmasker.

vRealize Automation genereert bijvoorbeeld bereiken van 255 IP-adressen als het subnetmasker 255.255.0.0 is en het subnetmasker van het bereik 255.255.255.0 is met de naam Range1 tot en met Rangen.

- 3 Klik op **OK**.

Een geleid netwerkprofiel maken met een IPAM-endpoint van derden

Wanneer u een geleid netwerkprofiel gebruikt met een IPAM-endpoint van derden, wordt een routeerbare IP-ruimte gemaakt en beheerd door de externe IPAM-provider.

Wanneer u een IPAM-endpoint van derden in uw gerouteerde netwerkprofiel gebruikt, maakt die provider nieuwe IP-bereiken voor elke instantie van het netwerk op aanvraag.

U kunt IP-bereiken gebruiken die afkomstig zijn uit het geleverde VMware IPAM-endpoint of van een endpoint van een externe IPAM-serviceprovider dat u hebt geregistreerd en geconfigureerd in vRealize Orchestrator, zoals Infoblox IPAM. Een IP-bereik wordt gemaakt van een IP-blok tijdens de toewijzing.

Procedure

- 1 [Informatie opgeven voor een geleid netwerkprofiel met een extern IPAM-endpoint](#)

De netwerkprofielinformatie identificeert de geleide netwerkeigenschappen, het onderliggende externe netwerkprofiel ervan en andere waarden die bij de inrichting van het netwerk worden gebruikt, wanneer gebruik wordt gemaakt van een extern IPAM-endpoint.

- 2 [IP-bereiken configureren voor een geleid netwerkprofiel met een extern IPAM-endpoint](#)

U kunt een of meer benoemde bereiken van statische IPv4-netwerkadressen beheren voor gebruik bij het inrichten van een netwerk.

Informatie opgeven voor een geleid netwerkprofiel met een extern IPAM-endpoint

De netwerkprofielinformatie identificeert de geleide netwerkeigenschappen, het onderliggende externe netwerkprofiel ervan en andere waarden die bij de inrichting van het netwerk worden gebruikt, wanneer gebruik wordt gemaakt van een extern IPAM-endpoint.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Maak een extern netwerkprofiel. Zie [Een extern netwerkprofiel maken met het meegeleverde IPAM-endpoint](#) of [Een extern netwerkprofiel maken via een externe IPAM-provider](#).
- Een extern IPAM-endpoint maken en configureren. Zie [Een endpoint van een externe IPAM-provider maken](#).

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Netwerkprofielen**.
- 2 Klik op **Nieuw** en selecteer **Geleid** in het vervolgkeuzemenu.
- 3 Voer een naam in en desgewenst een beschrijving.
- 4 Als u één of meer endpoints van een externe IPAM-provider hebt geconfigureerd, selecteert u een extern IPAM-endpoint in het vervolgkeuzemenu **IPAM-endpoint**.

Als u een endpoint van een externe IPAM-provider selecteert dat u hebt geregistreerd in vRealize Orchestrator, verkrijgt u IP-adressen van de opgegeven IPAM-serviceprovider.

- 5 Selecteer een bestaand extern netwerkprofiel in het vervolgkeuzemenu **Extern netwerkprofiel**.

Alleen externe netwerkprofielen die zijn geconfigureerd om gebruik te maken van het opgegeven IPAM-endpoint zijn in de lijst opgenomen en beschikbaar voor selectie.

- 6 Om te bepalen hoeveel netwerksubnetten moeten worden gemaakt, selecteert u een waarde in het vervolgkeuzemenu van het tekstvak **Bereik subnetmasker**.

Voer bijvoorbeeld 255.255.255.0 in.

Het bereik subnetmasker definieert hoe u die ruimte in afzonderlijke adresblokken wilt opdelen die worden toegewezen aan elke implementatie-instantie van dat netwerkprofiel. Wanneer u een waarde kiest voor het bereik subnetmasker, moet u rekening houden met het aantal implementaties waarin u het geleide netwerk verwacht te gebruiken.

Een bereik wordt gebruikt voor elke implementatie waarin een geleid netwerkprofiel wordt gebruikt. Het aantal beschikbare geleide bereiken is gelijk aan het subnetmasker gedeeld door het bereik subnetmasker, bijvoorbeeld $255.255.0.0/255.255.255.0 = 256$.

- 7 Klik op het tabblad **IP-blokken** om een adresruimte te definiëren en één of meer benoemde bereiken van statische IPv4-netwerkadressen te beheren.

De beschikbare IP-blokken vormen de bron voor de IP-bereiken die u maakt of toewijst voor omleiding op aanvraag.

Wat nu te doen

[IP-bereiken configureren voor een geleid netwerkprofiel met een extern IPAM-endpoint.](#)

IP-bereiken configureren voor een geleid netwerkprofiel met een extern IPAM-endpoint

U kunt een of meer benoemde bereiken van statische IPv4-netwerkadressen beheren voor gebruik bij het inrichten van een netwerk.

Tijdens inrichting wijst elk nieuw geleid netwerk het volgende beschikbare bereik toe en gebruikt het dit toegewezen bereik als zijn IP-ruimte. De IP-blokken worden verkregen van de externe IPAM-provider. Tijdens de inrichting krijgt het geleide netwerk een subnetmasker toegewezen uit het blok dat overeenkomt met het aangeboden bereik aan subnetmaskers.

Voorwaarden

Informatie opgeven voor een geleid netwerkprofiel met een extern IPAM-endpoint.

Procedure

- 1 Als u de beschikbare IP-blokken bij het inrichten wilt beperken, selecteert u een adresruimte in het vervolgkeuzemenu **Adresruimte**.

U kunt geen adresruimte selecteren nadat u IP-blokken hebt toegevoegd. Een geleid netwerkprofiel kan niet meer dan één adresruimte omvatten.

- 2 Voeg een of meer IP-blokken of IPAM-providerbereiken toe.

De IP-blokken worden opgehaald bij de externe IPAM-provider.

Als u een netwerkbereik selecteert, kan dit resulteren in een lege lijst als u een externe IPAM-provider gebruikt. Bekijk voor details het Knowledge Base-artikel 2148656 op <http://kb.vmware.com/kb/2148656>.

- a Klik op **Toevoegen**.
- b Klik op **Zoeken**.
- c Voer de zoeksyntaxis in of selecteer IP-blokken in het vervolgkeuzemenu.
- d Klik op **OK**.

- 3 Klik op **Toepassen**.

- 4 Klik op **OK**.

Een NAT-netwerkprofiel maken voor een netwerk op aanvraag

U kunt een profiel voor een NAT-netwerk op aanvraag maken dat de geleverde vRealize Automation-IPAM-endpoint gebruikt of een correct geconfigureerd en geregistreerd IPAM-endpoint van derden.

Een NAT-netwerkprofiel maken met het meegeleverde IPAM-endpoint

U kunt een profiel voor een NSX NAT-netwerk op aanvraag maken dat betrekking heeft op een extern netwerkprofiel. Wanneer het meegeleverde vRealize Automation IPAM-endpoint wordt gebruikt, kunt u bereiken met statische IP- en DHCP-adressen aan het NAT-netwerkprofiel toewijzen.

NAT-netwerken gebruiken één set IP-adressen voor externe communicatie en een andere set voor interne communicatie. Externe IP-adressen worden toegewezen vanuit een extern netwerkprofiel, terwijl interne NAT IP-adressen worden gedefinieerd door een NAT-netwerkprofiel. Wanneer u een nieuw NAT-netwerk inricht, wordt een nieuwe instantie van het NAT-netwerkprofiel gemaakt waarmee IP-adressen aan machines worden toegewezen.

U kunt IP-bereiken gebruiken die afkomstig zijn uit het geleverde VMware IPAM-endpoint of van een endpoint van een externe IPAM-serviceprovider dat u hebt geregistreerd en geconfigureerd in vRealize Orchestrator, zoals Infoblox IPAM. Een IP-bereik wordt gemaakt van een IP-blok tijdens de toewijzing.

Voor een NAT een-op-veel-netwerk kunt u NAT-regels definiëren die kunnen worden geconfigureerd wanneer u een NAT-netwerkonderdeel aan de blueprint toevoegt. U kunt een NAT-regel wijzigen wanneer u het NAT-netwerk in een implementatie bewerkt.

Procedure

1 [Informatie opgeven voor een NAT-netwerkprofiel met het vRealize Automation IPAM-endpoint](#)

Het netwerkprofiel identificeert de eigenschappen van het NAT-netwerk op aanvraag, het onderliggende externe netwerkprofiel, het NAT-type en andere waarden die bij de inrichting van het netwerk worden gebruikt met behulp van de ingebedde vRealize Automation IPAM.

2 [IP-bereiken configureren voor een NAT-netwerkprofiel met het vRealize Automation IPAM-endpoint](#)

U kunt een of meer bereiken van statische IP-adressen definiëren voor gebruik bij het inrichten van een netwerk.

Informatie opgeven voor een NAT-netwerkprofiel met het vRealize Automation IPAM-endpoint

Het netwerkprofiel identificeert de eigenschappen van het NAT-netwerk op aanvraag, het onderliggende externe netwerkprofiel, het NAT-type en andere waarden die bij de inrichting van het netwerk worden gebruikt met behulp van de ingebedde vRealize Automation IPAM.

Zie [Informatie opgeven voor een NAT-netwerkprofiel met een extern IPAM-endpoint](#) als u een NAT-netwerkprofiel wilt maken dat gebruikmaakt van een extern IPAM-endpoint.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Maak een extern netwerkprofiel. Zie [Een extern netwerkprofiel maken met het meegeleverde IPAM-endpoint](#).

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Netwerkprofielen**.
- 2 Klik op **Nieuw** en selecteer **NAT** in het vervolgkeuzemenu.
- 3 Voer een naam in en desgewenst een beschrijving.

- 4 Accepteer de standaardwaarde **IPAM-endpoint** voor het opgegeven endpoint **vRealize Automation IPAM**.
- 5 Selecteer een bestaand extern netwerkprofiel in het vervolgkeuzemenu **Extern netwerkprofiel**.
- 6 Kies een een-op-een of een-op-veel type netwerkadresvertaling in het vervolgkeuzemenu **NAT-type**.

Optie	Beschrijving
Een-op-een	<p>Wijs een extern, statisch IP-adres toe aan elke netwerkadapter. Elke machine heeft toegang tot het externe netwerk en is bereikbaar vanuit het externe netwerk.</p> <p>Alle externe IP-adressen die aan een NSX Edge-uplink zijn toegewezen, moeten deel uitmaken van hetzelfde subnet. Wanneer u NAT één-op-één gebruikt in vRealize Automation, mag het overeenkomende externe netwerkprofiel alleen IP-bereiken bevatten die binnen één subnet bestaan.</p>
Een-op-veel	<p>Eén extern IP-adres wordt gedeeld door alle machines in het netwerk. Een interne machine kan gebruikmaken van DHCP of statische IP-adressen. Elke machine heeft toegang tot het externe netwerk maar geen enkele machine is bereikbaar vanuit het externe netwerk. Als u deze optie selecteert, wordt het selectievakje Ingeschakeld in de DHCP-groep ingeschakeld.</p> <p>Voor NSX for vSphere kunt u met het type netwerkadresomzetting NAT een-op-veel NAT-regels definiëren wanneer u een NAT-netwerkonderdeel aan een blueprint toevoegt.</p> <p>NSX for vSphere ondersteunt een-op-een en een-op-veel NAT-netwerken, maar NSX-T ondersteunt alleen een-op-veel NAT-netwerken.</p>

- 7 Voer een IP-subnetmasker in het tekstveld **Subnetmasker** in.
Het subnetmasker bepaalt de grootte van de volledige routeerbare adresruimte die u voor uw netwerkprofiel wilt definiëren.
Voer bijvoorbeeld 255.255.0.0 in.
- 8 Voer een adres van een geleide gateway in, bijvoorbeeld 10.10.110.1, in het tekstvak **Gateway**.
Het IP-adres van de gateway dat is gedefinieerd in het netwerkprofiel, wordt toegekend aan de NIC tijdens de toewijzing. De gateway is vereist voor NAT-netwerkprofielen.
De standaardgateway van de DHCP-server voor NSX-T komt overeen met de NAT een-op-veel-standaardgateway. De standaardgateway van de IP-pool komt overeen met de NAT één-op-veel standaardgateway in vRealize Automation.
Als geen waarde is opgegeven in het tekstvak **Gateway** in het netwerkprofiel, moet u de aangepaste eigenschap `VirtualMachine.Network0.Gateway` gebruiken om een gateway toe te wijzen.
- 9 (Optioneel) Schakel in de DHCP-groep het selectievakje **Ingeschakeld** in en voer de waarden voor **eerste IP-bereik** en **laatste IP-bereik** in.
U kunt het selectievakje alleen inschakelen, als u het NAT-type hebt ingesteld op een-op-veel.

Voor NSX-T komt het eerste IP-adres in het IP-poolbereik overeen met het IP-adres van de DHCP-server dat is gedefinieerd met de instelling <FirstIpInPool>/<subnetMaskOfNat>. De IP-pool in NSX-T start met het tweede IP-adres.

- 10** (Optioneel) Stel een DHCP-leasetijd in om te definiëren hoe lang een machine een IP-adres kan gebruiken.
- 11** Klik op het tabblad **DNS**.
- 12** Voer indien nodig de DNS- en WINS-waarden in.

Gebruik DNS-waarden voor de naamregistratie en -omzetting. De waarden zijn optioneel voor interne IPAM. De waarden worden geleverd door de externe IPAM-provider voor externe IPAM.

- a (Optioneel) Voer een **Primaire DNS**-serverwaarde in.
- b (Optioneel) Voer een **Secundaire DNS**-serverwaarde in.
- c (Optioneel) Voer een waarde voor **DNS-achtervoegsels** in.
- d (Optioneel) Voer een waarde voor **DNS-zoekachtervoegsels** in.
- e (Optioneel) Voer een **Preferred WINS**-serverwaarde in.
- f (Optioneel) Voer een **Alternate WINS**-serverwaarde in.

Wat nu te doen

[IP-bereiken configureren voor een NAT-netwerkprofiel met het vRealize Automation IPAM-endpoint.](#)

IP-bereiken configureren voor een NAT-netwerkprofiel met het vRealize Automation IPAM-endpoint

U kunt een of meer bereiken van statische IP-adressen definiëren voor gebruik bij het inrichten van een netwerk.

U kunt de IP-adressen aan het begin en einde van het netwerkbereik ook overlappen met de DHCP-adressen. Als u een profiel probeert op te slaan met adresbereiken die overlappen, wordt in vRealize Automation een validatiefout weergegeven.

Voorwaarden

[Informatie opgeven voor een NAT-netwerkprofiel met het vRealize Automation IPAM-endpoint.](#)

Procedure

- 1** Als u een netwerkbereik wilt maken of een bestaand netwerkbereik wilt selecteren, klikt u op het tabblad **Netwerkbereiken**.

- 2 Als u handmatig een nieuwe netwerkbereiknaam en IP-adresbereik wilt invoeren, klikt u op **Nieuw**, of als u IP-informatie uit een correct opgemaakt CSV-bestand wilt importeren, klikt u op **Importeren uit CSV**.

■ Klik op **Nieuw**.

- a Voer een nieuwe naam voor het netwerkbereik in.
- b Voer een nieuwe netwerkbereikbeschrijving in.
- c Voer het eerste IP-adres van het bereik in.
- d Voer het laatste IP-adres van het bereik in.

■ Klik op **Importeren uit CSV**.

- a Ga naar het CSV-bestand en selecteer het of verplaats het CSV-bestand naar het dialoogvenster **Importeren uit CSV**.

Een rij in het CSV-bestand heeft de indeling *ip_address, machine_name, status, NIC_offset*. Bijvoorbeeld:

```
100.10.100.1,mymachine01,Allocated,0
```

CSV-veld	Beschrijving
ip_address	Een IP-adres in IPv4-indeling.
machine_name	Naam van een beheerde machine in vRealize Automation. Als het veld leeg is, is er standaard geen naam. Als het veld leeg is, kan de veldwaarde status niet Toegewezen zijn.
status	Toegewezen of Niet-toegewezen, hoofdlettergevoelig. Als het veld leeg is, is de standaardwaarde Niet-toegewezen. Als de status Toegewezen is, kan het veld machine_name niet leeg zijn.
NIC_offset	Een niet-negatief geheel getal. De NIC-offset geeft weer aan welke virtual machine-NIC het IP-adres is toegewezen. Als een virtual machine meer dan één IP-adres toewijst voor verschillende NIC's, is er een IP-adresvermelding voor elke NIC die de overeenkomstige NIC-offset bevat. Met de instelling 0 wordt geen offset opgegeven.

- b Klik op **Toepassen**.

- 3 Klik op **OK**.

De IP-adressen in het bereik verschijnen in de gedefinieerde IP-adressenlijst.

De IP-adressen worden weergegeven wanneer u op **Toepassen** klikt of nadat u het netwerkprofiel hebt opgeslagen en vervolgens bewerkt.

- 4 Als u de IP-adressen voor het benoemde netwerkbereik wilt weergeven, klikt u op het tabblad **IP-adressen**.

- 5 (Optioneel) Als u IP-adresvermeldingen wilt filteren, selecteert u een IP-adres in het vervolgkeuzemenu **Netwerkbereik**.

U kunt informatie tonen over de gedefinieerde netwerkbereiken, de netwerkbereiken die zijn geïmporteerd uit een CSV-bestand of een benoemd netwerkbereik.

- 6 (Optioneel) Als u IP-adressen wilt filteren die overeenkomen met de IP-status, selecteert u een statustype in het vervolgkeuzemenu **IP-status**.

Voor IP-adressen die verlopen of vernietigd zijn, kunt u klikken op **Herstellen** om deze adressen voor toewijzing beschikbaar te maken. U dient het profiel op te slaan om het herstel uit te voeren. Het kan een minuut duren voordat de kolom Status is bijgewerkt van Expired of Destroyed naar Allocated.

- 7 Klik op **OK**.

Een NAT-netwerkprofiel maken met een extern IPAM-endpoint in vRealize Automation

U kunt een profiel voor een NSX NAT-netwerk op aanvraag maken dat betrekking heeft op een extern netwerkprofiel in vRealize Automation. Wanneer u een profiel voor een NSX NAT-netwerk gebruikt met een externe IPAM-provider, wordt er een IP-ruimte gemaakt en beheerd door de externe IPAM-provider.

Wanneer u een IPAM-endpoint van derden in uw NAT-netwerkprofiel gebruikt, maakt de provider nieuwe IP-bereiken voor elke instantie van het netwerk op aanvraag. Er wordt voor elke instantie van het netwerk een interne set IP-adressen gemaakt die worden gedefinieerd met een of meer bereiken in het endpoint van de externe IPAM-provider. De IP-bereiken wijzen IP-adressen toe voor de machines in het netwerk in dezelfde implementatie. Omdat er in een afzonderlijke adresruimte geen dubbele IP-adressen kunnen worden gedefinieerd, maakt de provider voor elke instantie van het netwerk een nieuwe adresruimte. Wanneer een NAT-netwerk wordt vernietigd, worden ook de bijbehorende adresbereiken vernietigd op het endpoint van de IPAM-provider en in de nieuwe adresruimte.

U kunt IP-bereiken gebruiken die afkomstig zijn uit het geleverde VMware IPAM-endpoint of van een endpoint van een externe IPAM-serviceprovider dat u hebt geregistreerd en geconfigureerd in vRealize Orchestrator, zoals Infoblox IPAM. Een IP-bereik wordt gemaakt van een IP-blok tijdens de toewijzing.

Voor een NAT een-op-veel-netwerk kunt u NAT-regels definiëren die kunnen worden geconfigureerd wanneer u een NAT-netwerkonderdeel aan de blueprint toevoegt. U kunt een NAT-regel wijzigen wanneer u het NAT-netwerk in een implementatie bewerkt.

Procedure

1 Informatie opgeven voor een NAT-netwerkprofiel met een extern IPAM-endpoint

De netwerkprofielinformatie identificeert de NAT-netwerkeigenschappen, het onderliggende externe netwerkprofiel ervan en andere waarden die bij de inrichting van het netwerk worden gebruikt, wanneer gebruik wordt gemaakt van een extern IPAM-endpoint.

2 IP-bereiken voor een NAT-netwerkprofiel configureren met een IPAM-endpoint van derden

U kunt een of meer IP-adresbereiken definiëren voor gebruik bij het inrichten van een netwerk met NAT.

Informatie opgeven voor een NAT-netwerkprofiel met een extern IPAM-endpoint

De netwerkprofielinformatie identificeert de NAT-netwerkeigenschappen, het onderliggende externe netwerkprofiel ervan en andere waarden die bij de inrichting van het netwerk worden gebruikt, wanneer gebruik wordt gemaakt van een extern IPAM-endpoint.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Maak een extern netwerkprofiel. Zie [Een extern netwerkprofiel maken met het meegeleverde IPAM-endpoint](#) of [Een extern netwerkprofiel maken via een externe IPAM-provider](#).
- Maak en configureer een extern IPAM-endpoint. Zie [Een endpoint van een externe IPAM-provider maken](#).

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Netwerkprofielen**.
- 2 Klik op **Nieuw** en selecteer **NAT** in het vervolgkeuzemenu.
- 3 Voer een naam in en desgewenst een beschrijving.
- 4 Als u één of meer endpoints van een externe IPAM-provider hebt geconfigureerd, selecteert u een extern IPAM-endpoint in het vervolgkeuzemenu **IPAM-endpoint**.

Als u een endpoint van een externe IPAM-provider selecteert dat u hebt geregistreerd in vRealize Orchestrator, verkrijgt u IP-adressen van de opgegeven IPAM-serviceprovider.

- 5 Selecteer een bestaand extern netwerkprofiel in het vervolgkeuzemenu **Extern netwerkprofiel**.

Alleen externe netwerkprofielen die zijn geconfigureerd om gebruik te maken van het opgegeven IPAM-endpoint zijn in de lijst opgenomen en beschikbaar voor selectie.

- 6 Kies een een-op-een of een-op-veel type netwerkadresvertaling in het vervolgkeuzemenu **NAT-type**.

Optie	Beschrijving
Een-op-een	<p>Wijs een extern, statisch IP-adres toe aan elke netwerkadapter. Elke machine heeft toegang tot het externe netwerk en is bereikbaar vanuit het externe netwerk.</p> <p>Alle externe IP-adressen die aan een NSX Edge-uplink zijn toegewezen, moeten deel uitmaken van hetzelfde subnet. Wanneer u NAT één-op-één gebruikt in vRealize Automation, mag het overeenkomende externe netwerkprofiel alleen IP-bereiken bevatten die binnen één subnet bestaan.</p>
Een-op-veel	<p>Eén extern IP-adres wordt gedeeld door alle machines in het netwerk. Een interne machine kan alleen gebruikmaken van statische IP-adressen. Elke machine heeft toegang tot het externe netwerk maar geen enkele machine is bereikbaar vanuit het externe netwerk.</p> <p>DHCP wordt niet ondersteund wanneer NAT met een externe IPAM-provider wordt gebruikt.</p> <p>Voor NSX for vSphere kunt u met het type netwerkadresomzetting NAT een-op-veel NAT-regels definiëren wanneer u een NAT-netwerkonderdeel aan een blueprint toevoegt.</p> <p>NSX for vSphere ondersteunt een-op-een en een-op-veel NAT-netwerken, maar NSX-T ondersteunt alleen een-op-veel NAT-netwerken.</p>

- 7 Voer een IP-subnetmasker in het tekstveld **Subnetmasker** in.

Het subnetmasker bepaalt de grootte van de volledige routeerbare adresruimte die u voor uw netwerkprofiel wilt definiëren.

Voer bijvoorbeeld 255.255.0.0 in.

- 8 Voer een adres van een geleide gateway in, bijvoorbeeld 10.10.110.1, in het tekstvak **Gateway**.

Het IP-adres van de gateway dat is gedefinieerd in het netwerkprofiel, wordt toegekend aan de NIC tijdens de toewijzing. De gateway is vereist voor NAT-netwerkprofielen.

De standaardgateway van de DHCP-server voor NSX-T komt overeen met de NAT een-op-veel-standaardgateway. De standaardgateway van de IP-pool komt overeen met de NAT één-op-veel standaardgateway in vRealize Automation.

Als geen waarde is opgegeven in het tekstvak **Gateway** in het netwerkprofiel, moet u de aangepaste eigenschap `VirtualMachine.Network0.Gateway` gebruiken om een gateway toe te wijzen.

- 9 Klik op het tabblad **DNS**.

10 Voer indien nodig de DNS- en WINS-waarden in.

Gebruik DNS-waarden voor de naamregistratie en -omzetting. De waarden zijn optioneel voor interne IPAM. De waarden worden geleverd door de externe IPAM-provider voor externe IPAM.

- a (Optioneel) Voer een **Primaire DNS**-serverwaarde in.
- b (Optioneel) Voer een **Secundaire DNS**-serverwaarde in.
- c (Optioneel) Voer een waarde voor **DNS-achtervoegsels** in.
- d (Optioneel) Voer een waarde voor **DNS-zoekachtervoegsels** in.
- e (Optioneel) Voer een **Preferred WINS**-serverwaarde in.
- f (Optioneel) Voer een **Alternate WINS**-serverwaarde in.

Wat nu te doen

[IP-bereiken voor een NAT-netwerkprofiel configureren met een IPAM-endpoint van derden.](#)

IP-bereiken voor een NAT-netwerkprofiel configureren met een IPAM-endpoint van derden

U kunt een of meer IP-adresbereiken definiëren voor gebruik bij het inrichten van een netwerk met NAT.

Voorwaarden

[Informatie opgeven voor een NAT-netwerkprofiel met een extern IPAM-endpoint.](#)

Procedure

- 1** Als u een netwerkbereik wilt maken of een bestaand netwerkbereik wilt selecteren, klikt u op het tabblad **Netwerkbereiken**.
- 2** Klik op **Nieuw** en definieer een netwerkbereik.
 - a Voer een netwerkbereik en een beschrijving in.
 - b Voer een eerste en laatste IP-adres in om het bereik te definiëren.
 - c Klik op **Toepassen**.

3 Klik op **OK**.

De IP-adressen in het bereik verschijnen in de gedefinieerde IP-adressenlijst.

De IP-adressen worden weergegeven wanneer u op **Toepassen** klikt of nadat u het netwerkprofiel hebt opgeslagen en vervolgens bewerkt.

- 4** Als u de IP-adressen voor het benoemde netwerkbereik wilt weergeven, klikt u op het tabblad **IP-adressen**.
- 5** (Optioneel) Als u IP-adresvermeldingen wilt filteren, selecteert u een IP-adres in het vervolgkeuzemenu **Netwerkbereik**.

U kunt informatie tonen over de gedefinieerde netwerkbereiken, de netwerkbereiken die zijn geïmporteerd uit een CSV-bestand of een benoemd netwerkbereik.

- 6 (Optioneel) Als u IP-adressen wilt filteren die overeenkomen met de IP-status, selecteert u een statustype in het vervolgkeuzemenu **IP-status**.

Voor IP-adressen die verlopen of vernietigd zijn, kunt u klikken op **Herstellen** om deze adressen voor toewijzing beschikbaar te maken. U dient het profiel op te slaan om het herstel uit te voeren. Het kan een minuut duren voordat de kolom Status is bijgewerkt van Expired of Destroyed naar Allocated.

- 7 Klik op **OK**.

Een profiel voor een privaat netwerk maken voor een netwerk op aanvraag in vRealize Automation

U kunt een privaat netwerk maken voor NSX for vSphere dat gebruikmaakt van de IPAM-specificatie die wordt geleverd door vRealize Automation.

U kunt een profiel voor een privaat netwerk op aanvraag maken voor NSX for vSphere dat betrekking heeft op een extern netwerkprofiel.

Private netwerken zijn niet beschikbaar voor NSX-T.

Private netwerken zijn niet beschikbaar voor externe IPAM.

U kunt een of meer bereiken van statische IP-adressen definiëren voor gebruik bij het inrichten van een netwerk.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Netwerkprofielen**.
- 2 Klik op **Nieuw** en selecteer **Privaat** in het vervolgkeuzemenu.
- 3 Voer een naam in en desgewenst een beschrijving.
- 4 Accepteer de standaardwaarde **IPAM-endpoint** voor het opgegeven endpoint **vRealize Automation IPAM**.
- 5 Selecteer de tenant-ID als hierom wordt gevraagd.
- 6 Voer een IP-subnetmasker in het tekstveld **Subnetmasker** in.
 Het subnetmasker bepaalt de grootte van de volledige routeerbare adresruimte die u voor uw netwerkprofiel wilt definiëren.
 Voer bijvoorbeeld 255.255.0.0 in.
- 7 Voer een adres van een geleide gateway in, bijvoorbeeld 10.10.110.1 in het tekstvak **Gateway**.
 Het IP-adres van de gateway dat is gedefinieerd in het netwerkprofiel, wordt toegekend aan de NIC tijdens de toewijzing. Als geen waarde is opgegeven in het tekstvak **Gateway** in het netwerkprofiel, moet u de aangepaste eigenschap `VirtualMachine.Network0.Gateway` gebruiken om een gateway toe te wijzen.

8 Klik op het tabblad **DNS**.

9 Voer indien nodig de DNS- en WINS-waarden in.

Als u een profiel probeert op te slaan met adresbereiken die overlappen, wordt in vRealize Automation een validatiefout weergegeven.

10 Als u een netwerkbereik wilt maken of een bestaand netwerkbereik wilt selecteren, klikt u op het tabblad **Netwerkbereiken**.

11 Als u handmatig een nieuwe netwerkbereiknaam en IP-adresbereik wilt invoeren, klikt u op **Nieuw**, of als u IP-informatie uit een correct opgemaakt CSV-bestand wilt importeren, klikt u op **Importeren uit CSV**.

■ Klik op **Nieuw**.

- a Voer een nieuwe naam voor het netwerkbereik in.
- b Voer een nieuwe netwerkbereikbeschrijving in.
- c Voer het eerste IP-adres van het bereik in.
- d Voer het laatste IP-adres van het bereik in.

■ Klik op **Importeren uit CSV**.

- a Ga naar het CSV-bestand en selecteer het of verplaats het CSV-bestand naar het dialoogvenster **Importeren uit CSV**.

Een rij in het CSV-bestand heeft de indeling *ip_address, machine_name, status, NIC_offset*. Bijvoorbeeld:

```
100.10.100.1,mymachine01,Allocated,0
```

CSV-veld	Beschrijving
ip_address	Een IP-adres in IPv4-indeling.
machine_name	Naam van een beheerde machine in vRealize Automation. Als het veld leeg is, is er standaard geen naam. Als het veld leeg is, kan de veldwaarde status niet Toegewezen zijn.
status	Toegewezen of Niet-toegewezen, hoofdlettergevoelig. Als het veld leeg is, is de standaardwaarde Niet-toegewezen. Als de status Toegewezen is, kan het veld machine_name niet leeg zijn.
NIC_offset	Een niet-negatief geheel getal. De NIC-offset geeft weer aan welke virtual machine-NIC het IP-adres is toegewezen. Als een virtual machine meer dan één IP-adres toewijst voor verschillende NIC's, is er een IP-adresvermelding voor elke NIC die de overeenkomstige NIC-offset bevat. Met de instelling 0 wordt geen offset opgegeven.

- b Klik op **Toepassen**.

12 Klik op **OK**.

De IP-adressen in het bereik verschijnen in de gedefinieerde IP-adressenlijst.

De IP-adressen worden weergegeven wanneer u op **Toepassen** klikt of nadat u het netwerkprofiel hebt opgeslagen en vervolgens bewerkt.

- 13** Als u de IP-adressen voor het benoemde netwerkbereik wilt weergeven, klikt u op het tabblad **IP-adressen**.

- 14** (Optioneel) Als u IP-adresvermeldingen wilt filteren, selecteert u een IP-adres in het vervolgkeuzemenu **Netwerkbereik**.

U kunt informatie tonen over de gedefinieerde netwerkbereiken, de netwerkbereiken die zijn geïmporteerd uit een CSV-bestand of een benoemd netwerkbereik.

- 15** (Optioneel) Als u IP-adressen wilt filteren die overeenkomen met de IP-status, selecteert u een statustype in het vervolgkeuzemenu **IP-status**.

Voor IP-adressen die verlopen of vernietigd zijn, kunt u klikken op **Herstellen** om deze adressen voor toewijzing beschikbaar te maken. U dient het profiel op te slaan om het herstel uit te voeren. Het kan een minuut duren voordat de kolom Status is bijgewerkt van Expired of Destroyed naar Allocated.

- 16** Klik op **OK**.

IP-adressen vrijgeven door ingerichte machines te vernietigen

Wanneer u een implementatie vernietigt, worden de IP-adressen verwijderd. De toegewezen IP-adressen, bijvoorbeeld de IP-adressen in een netwerkprofielbereik, worden vrijgegeven en zijn daarna weer beschikbaar voor inrichting.

Wanneer u een machine met een statisch IP-adres vernietigt, kan dat IP-adres weer gebruikt worden door andere machines. Ongebruikte adressen zijn mogelijk niet direct beschikbaar, omdat het proces waarmee statische IP-adressen worden hersteld, maar een keer per 30 minuten wordt uitgevoerd.

Als u gebruik maakt van een externe IPAM-provider, worden door vRealize Automation de bijbehorende IP-adressen verwijderd doordat de vRealize Orchestrator-werkstroom wordt toegepast op de invoegtoepassing of het pakket van de externe IPAM-provider.

Reserveringen en reserveringsbeleid configureren

Met een vRealize Automation-reservering kunt u beleidsregels, prioriteiten en quotas definiëren waarmee de plaatsing van machines bij inrichtingsaanvragen wordt bepaald.

Een reserveringsbeleid beperkt de machine-inrichting tot een subset van beschikbare reserveringen. Met een opslagreserveringsbeleid kunnen architecten van blueprints machinevolumes aan verschillende datastores toewijzen.

Voor een goede inrichting moet de reservering voldoende beschikbare opslag hebben. De beschikbare opslag van de reservering is afhankelijk van:

- Hoeveel opslag in de datastore en/of het cluster beschikbaar is.
- Hoeveel van die opslag is gereserveerd voor die datastore en/of dat cluster.
- Hoeveel van die opslag al is toegewezen in vRealize Automation

Zelfs als bijvoorbeeld vCenter Server opslag beschikbaar heeft voor de datastore en/of het cluster, zal de inrichting mislukken met een fout van het type 'Geen reservering beschikbaar om toe te wijzen...' als er te weinig opslag is gereserveerd. De toegewezen opslag op een reservering is afhankelijk van het aantal VM's (ongeacht hun status) op die specifieke reservering. Zie het VMware Knowledge Base-artikel *Machine XXX: Geen reservering beschikbaar om binnen de groep XXX toe te wijzen. In totaal werd XX GB aan opslag aangevraagd (2151030)* op <http://kb.vmware.com/kb/2151030> voor meer informatie.

Reserveringen

U kunt een vRealize Automation-reservering maken om inrichtingsbronnen in de materiaalgroep toe te wijzen aan een specifieke bedrijfsgroep.

U kunt bijvoorbeeld reserveringen gebruiken om op te geven dat een deel van de geheugen-, CPU-, netwerk- en opslagbronnen van één computerbron tot een specifieke bedrijfsgroep behoren of dat bepaalde machines worden toegewezen aan een specifieke bedrijfsgroep.

U gebruikt een netwerkreserveringsbeleid om de netwerkcommunicaties voor blueprintimplementaties te beheren. Wanneer u machine-inrichting aanvraagt, wordt het reserveringsbeleid gebruikt om de reserveringen te groeperen die voor de implementatie in aanmerking kunnen komen.

U kunt geen reserveringen delen tussen meerdere bedrijfsgroepen.

Opmerking Opslagruimte en geheugen die door middel van een reservering zijn toegewezen aan een ingerichte machine, worden vrijgemaakt wanneer de machine waaraan ze zijn gekoppeld, in vRealize Automation wordt verwijderd door de actie Vernietigen. De opslagruimte en het geheugen worden niet vrijgemaakt als de machine wordt verwijderd in de vCenter Server.

U kunt een reservering maken voor de volgende machinetypen:

- vSphere
- vCloud Air
- vCloud Director
- Amazon EC2
- Microsoft Azure
- Hyper V (SCVMM)
- Hyper-V Standalone
- KVM (RHEV)
- OpenStack
- XenServer

U kunt beveiligingsinstellingen configureren door informatie op te geven in een reservering, blueprint of script van een gastagent. Als machines een gastagent vereisen, voegt u een beveiligingsregel toe aan de reservering of de blueprint.

Een reserveringsscenario kiezen

U kunt reserveringen maken om bronnen toe te wijzen aan bedrijfsgroepen. Afhankelijk van uw scenario kan de procedure voor het maken van een reservering verschillen.

Kies een reserveringsscenario op basis van het beoogde endpointtype.

Elke bedrijfsgroep moet minstens één reservering hebben zodat de leden van die groep machines van dat type kunnen inrichten. Een bedrijfsgroep met een OpenStack-reservering maar geen Amazon-reservering kan bijvoorbeeld geen machine van Amazon aanvragen. In dit voorbeeld moet aan de bedrijfsgroep specifiek een reservering voor Amazon-bronnen zijn toegewezen.

Tabel 2-15. Een reserveringsscenario kiezen

Scenario	Procedure
Een vSphere-reservering maken.	Een reservering maken voor Hyper-V, KVM, SCVMM, vSphere of XenServer
Een reservering maken om bronnen voor een vCloud Air-endpoint toe te wijzen	Een vCloud Air-reservering maken
Een reservering maken om bronnen voor een vCloud Director-endpoint toe te wijzen	Een vCloud Director-reservering maken
Een reservering maken om bronnen toe te wijzen op een Amazon-bron (met of zonder het gebruik van de virtuele privécloud van Amazon)	Een Amazon EC2-reservering maken
Een reservering maken om bronnen op een OpenStack-bron toe te wijzen.	Een OpenStack-reservering maken
Een reservering maken om bronnen voor Hyper-V toe te wijzen	Een reservering maken voor Hyper-V, KVM, SCVMM, vSphere of XenServer
Een reservering maken om bronnen voor KVM toe te wijzen	Een reservering maken voor Hyper-V, KVM, SCVMM, vSphere of XenServer
Een reservering maken om bronnen op een OpenStack-bron toe te wijzen	Een OpenStack-reservering maken
Een reservering maken om bronnen voor SCVMM toe te wijzen	Een reservering maken voor Hyper-V, KVM, SCVMM, vSphere of XenServer
Een reservering maken om bronnen voor XenServer toe te wijzen	Een reservering maken voor Hyper-V, KVM, SCVMM, vSphere of XenServer
Een reservering maken om bronnen voor Microsoft Azure toe te wijzen	Een reservering voor Microsoft Azure maken

Reserveringen voor cloudcategorieën maken

Een reservering van het type cloudcategorie biedt toegang tot de inrichtingsservices van een cloudserviceaccount voor een specifieke vRealize Automation-bedrijfsgroep. Beschikbare cloudreserveringstypen zijn onder meer Amazon, OpenStack, vCloud Air en vCloud Director.

Een reservering is een deel van de geheugen-, CPU-, netwerk- en opslagbronnen van een computerbron dat aan een specifieke vRealize Automation-bedrijfsgroep wordt toegewezen.

Een bedrijfsgroep kan meerdere reserveringen op één endpoint hebben of reserveringen op meerdere endpoints.

Het toewijzingsmodel voor een reservering is afhankelijk van het toewijzingsmodel in het gekoppelde datacenter. Beschikbare toewijzingsmodellen zijn toewijzingspool, betalen-naar-gebruik en reserveringspool. Zie de vCloud Director- of vCloud Air-documentatie voor informatie over toewijzingsmodellen.

Naast het definiëren van het deel van materiaalbronnen dat aan de bedrijfsgroep is toegewezen, kan een reservering beleidsregels, prioriteiten en quotums definiëren die de plaatsing van machines bepaalt.

Voor een goede inrichting moet de reservering voldoende beschikbare opslag hebben. De beschikbare opslag van de reservering is afhankelijk van:

- Hoeveel opslag in de datastore en/of het cluster beschikbaar is.
- Hoeveel van die opslag is gereserveerd voor die datastore en/of dat cluster.
- Hoeveel van die opslag al is toegewezen in vRealize Automation

Zelfs als bijvoorbeeld vCenter Server opslag beschikbaar heeft voor de datastore en/of het cluster, zal de inrichting mislukken met een fout van het type 'Geen reservering beschikbaar om toe te wijzen...' als er te weinig opslag is gereserveerd. De toegewezen opslag op een reservering is afhankelijk van het aantal VM's (ongeacht hun status) op die specifieke reservering. Zie het VMware Knowledge Base-artikel *Machine XXX: Geen reservering beschikbaar om binnen de groep XXX toe te wijzen. In totaal werd XX GB aan opslag aangevraagd (2151030)* op <http://kb.vmware.com/kb/2151030> voor meer informatie.

Informatie over de selectielogica voor cloudreserveringen

Wanneer een lid van een bedrijfsgroep een inrichtingsaanvraag maakt voor een cloudmachine, wordt door vRealize Automation een machine geselecteerd uit de reserveringen die beschikbaar zijn voor die bedrijfsgroep. Amazon, OpenStack, vCloud Air en vCloud Director behoren onder meer tot de cloudreserveringen.

De reservering waarvoor een machine wordt ingericht, moet aan de volgende criteria voldoen:

- De reservering moet gebruikmaken van hetzelfde type platform als de blueprint waaruit de machine is aangevraagd.
- De reservering moet geactiveerd zijn.
- De reservering moet resterende capaciteit in het machinequotum hebben of over een onbeperkt machinequotum beschikken.

Het toegewezen machinequotum omvat uitsluitend machines die zijn ingeschakeld. Als een reservering bijvoorbeeld beschikt over een quotum van 50 en er 40 machines zijn ingericht waarvan slechts 20 zijn ingeschakeld, is 40 procent van het quotum van de reservering toegewezen en niet 80 procent.

- De reservering moet over de beveiligingsgroepen beschikken die zijn opgegeven in de aanvraag voor de machine.

- De reservering moet zijn gekoppeld aan een regio met de image van de machine, die is opgegeven in de blueprint.
- De reservering moet over voldoende niet-toegewezen geheugen en opslagbronnen beschikken om de machine in te richten.

In een reservering voor Betalen-naar-gebruik, kunnen de bronnen onbeperkt zijn.

- Voor Amazon-machines wordt in de aanvraag opgegeven wat de beschikbaarheidszone is en of de machine moet worden ingericht met een subnet in een VPC-locatie (Virtual Private Cloud) of in een niet-VPC-locatie. De reservering moet over een vergelijkbaar netwerktype beschikken (VPC of niet-VPC).
- Als in de aanvraag voor vCloud Air of vCloud Director een toewijzingsmodel is opgegeven, moet het virtuele datacenter dat is gekoppeld aan de reservering over hetzelfde toewijzingsmodel beschikken.
- De organisatie die voor vCloud Director of vCloud Air is opgegeven, moet geactiveerd zijn.
- Eventuele blueprintsjablonen moeten voor de reservering beschikbaar zijn. Als het reserveringsbeleid is toegewezen aan meer dan één bron, moeten de sjablonen openbaar zijn.
- Als de cloudprovider netwerkselectie ondersteunt en de blueprint specifieke netwerkinstellingen bevat, moet de reservering over dezelfde netwerken beschikken.

Als voor de blueprint of de reservering een netwerkprofiel voor toewijzing van statische IP-adressen is opgegeven, moet een IP-adres beschikbaar zijn om toe te wijzen aan de nieuwe machine.

- Als in de aanvraag een toewijzingsmodel is opgegeven, moet het toewijzingsmodel voor de reservering overeenstemmen met het toewijzingsmodel in de aanvraag.
- Als in de blueprint een reserveringsbeleid is opgegeven, moet de reservering onderdeel uitmaken van dat reserveringsbeleid.

Een reserveringsbeleid is een manier om te garanderen dat de geselecteerde reservering voldoet aan de extra vereisten voor de inrichting van machines op basis van een specifieke blueprint. Als een blueprint bijvoorbeeld gebruikmaakt van een specifieke image van een machine, kunt u het reserveringsbeleid gebruiken om de inrichting te beperken tot reserveringen die zijn gekoppeld aan regio's die over de vereiste image beschikken.

Als er geen reservering beschikbaar is die aan alle selectiecriteria voldoet, mislukt de inrichting.

Als er meerdere reserveringen voldoen aan alle criteria, wordt op de volgende wijze bepaald welke reservering wordt gebruikt om een aangevraagde machine in te richten:

- Een reservering met een lagere prioriteit wordt geselecteerd voor een reservering met een hogere prioriteit.
- Als er meerdere reserveringen dezelfde prioriteit hebben, wordt de reservering geselecteerd waarvoor het laagste percentage machinequotum is toegewezen.

- Als er meerdere reserveringen zijn met dezelfde prioriteit en hetzelfde quotumgebruik, worden machines evenredig gedistribueerd onder de reserveringen.

Opmerking De round-robin-selectie van netwerkprofielen wordt niet ondersteund, round-robin-selectie van netwerken (indien aanwezig) wordt ondersteund, en kan worden gekoppeld aan verschillende netwerkprofielen.

Als er meerdere opslagpaden beschikbaar zijn voor een reservering met voldoende capaciteit om de machinevolumes in te richten, worden de opslagpaden geselecteerd op basis van de volgende logica.

- Een opslagpad met een lagere prioriteit wordt geselecteerd voor een opslagpad met een hogere prioriteit.
- Als in de blueprint of aanvraag een opslagreserveringsbeleid is opgegeven, moet het opslagpad onderdeel uitmaken van dat opslagreserveringsbeleid.

Als de aangepaste eigenschap `VirtualMachine.DiskN.StorageReservationPolicyMode` is ingesteld op Niet exact en er geen opslagpad met voldoende capaciteit beschikbaar is in het opslagreserveringsbeleid, wordt de inrichting voortgezet met een opslagpad dat buiten het opgegeven opslagreserveringsbeleid valt. De standaardwaarde van `VirtualMachine.DiskN.StorageReservationPolicyMode` is Exact.

- Als er meerdere opslagpaden zijn met dezelfde prioriteit, worden de machines evenredig gedistribueerd over de opslagpaden.

Een Amazon EC2-reservering maken

U moet bronnen aan machines toewijzen door een reservering te maken voordat leden van een bedrijfsgroep machine-inrichting kunnen aanvragen.

U kunt werken met Amazon-reserveringen voor Amazon Virtual Private Cloud of Amazon niet-VPC. Amazon Web Services-gebruikers kunnen een Amazon Virtual Private Cloud maken om een virtuele netwerktopologie te ontwerpen volgens uw specificaties. Als u van plan bent om Amazon VPC te gebruiken, moet u een Amazon VPC toewijzen aan een vRealize Automation-reservering.

Wanneer u een Amazon-reservering maakt of een machineonderdeel configureert in de blueprint, kunt u kiezen uit de lijst met beveiligingsgroepen die beschikbaar zijn voor de opgegeven Amazon-regio. Beveiligingsgroepen worden geïmporteerd tijdens de verzameling van gegevens.

Opmerking Nadat u een reservering hebt gemaakt, kunt u de koppelingen met bedrijfsgroepen of computerbronnen niet meer wijzigen.

Voor meer informatie over het maken van een Amazon VPC met behulp van de AWS Management Console raadpleegt u de Amazon Web Services-documentatie.

Procedure

1 [Amazon-reserveringsinformatie opgeven](#)

Elke reservering is geconfigureerd voor een specifieke bedrijfsgroep zodat deze toegang krijgt om machines aan te vragen op een opgegeven computerbron.

2 [Bron- en netwerkinstellingen opgeven voor Amazon-reserveringen](#)

Geef bron- en netwerkinstellingen op voor het inrichten van machines vanaf deze vRealize Automation-reservering.

3 [Aangepaste eigenschappen en waarschuwingen voor Amazon-reserveringen opgeven](#)

U kunt aangepaste eigenschappen koppelen aan een vRealize Automation-reservering. U kunt ook waarschuwingen configureren om e-mailmeldingen te verzenden wanneer er weinig reserveringsbronnen zijn.

Amazon-reserveringsinformatie opgeven

Elke reservering is geconfigureerd voor een specifieke bedrijfsgroep zodat deze toegang krijgt om machines aan te vragen op een opgegeven computerbron.

Opmerking Nadat u een reservering hebt gemaakt, kunt u de koppelingen met bedrijfsgroepen of computerbronnen niet meer wijzigen.

U kunt bepalen hoe reserveringen worden weergegeven, tijdens het toevoegen, bewerken of verwijderen, door gebruik te maken van de optie **Filteren op categorie** op de pagina Reserveringen. Houd er rekening mee dat reserveringen van testagenten niet worden weergegeven in de lijst met reserveringen wanneer u filtert op categorie.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Controleer of de tenantbeheerder ten minste één bedrijfsgroep heeft gemaakt.
- Controleer of er een computerbron bestaat.
- Configureer de netwerkinstellingen.
- (Optioneel) Configureer de informatie over een netwerkprofiel.
- Controleer of u toegang hebt tot een gewenst Amazon-netwerk. Als u bijvoorbeeld VPC wilt gebruiken, controleert u of u toegang hebt tot een Amazon VPC-netwerk (virtuele privécloud).
- Controleer of er vereiste sleutelparen bestaan. Zie [Sleutelparen beheren](#).

Procedure

1 Selecteer **Infrastructuur > Reserveringen > Reserveringen**.

- 2 Klik op het pictogram **Nieuw** (+) en selecteer het type reservering dat u wilt maken.
Selecteer **Amazon EC2**.
- 3 Geef een naam op in het tekstvak **Naam**.
- 4 Selecteer een tenant in het vervolgkeuzemenu **Tenant**.
- 5 Selecteer een bedrijfsgroep in het vervolgkeuzemenu **Bedrijfsgroep**.
Alleen gebruikers in deze bedrijfsgroep kunnen machines inrichten met behulp van deze reservering.
- 6 (Optioneel) Selecteer een reserveringsbeleid in het vervolgkeuzemenu **Reserveringsbeleid**.
Voor deze optie is vereist dat er minimaal één reserveringsbeleid bestaat. U kunt de reservering later bewerken om een reserveringsbeleid op te geven.
U kunt een reserveringsbeleid gebruiken om de inrichting te beperken tot bepaalde reserveringen.
- 7 Geef een getal op in het tekstvak **Prioriteit** om de prioriteit voor de reservering in te stellen.
De prioriteit wordt gebruikt wanneer er meer dan een reservering bestaat voor de bedrijfsgroep. Een reservering met de prioriteit 1 wordt eerder ingericht dan een reservering met de prioriteit 2.
- 8 (Optioneel) Schakel het selectievakje **Deze reservering inschakelen** uit als u niet wilt dat deze reservering actief is.

Resultaten

Verlaat deze pagina niet. Uw reservering is niet compleet.

Bron- en netwerkinstellingen opgeven voor Amazon-reserveringen

Geef bron- en netwerkinstellingen op voor het inrichten van machines vanaf deze vRealize Automation-reservering.

Wanneer u een Amazon-reservering maakt of een machineonderdeel configureert in de blueprint, kunt u kiezen uit de lijst met beveiligingsgroepen die beschikbaar zijn voor de opgegeven regio van de Amazon-account. Beveiligingsgroepen worden geïmporteerd tijdens de verzameling van gegevens. Een beveiligingsgroep functioneert als een firewall waarmee de toegang tot een machine wordt beheerd. Elke regio omvat ten minste een standaard beveiligingsgroep. Beheerders kunnen de Amazon Web Services Management Console gebruiken om extra beveiligingsgroepen te maken, poorten te configureren voor Microsoft Remote Desktop Protocol of SSH en een virtueel particulier netwerk in te stellen voor een Amazon VPN. Zie de documentatie bij Amazon voor informatie over het maken en gebruiken van beveiligingsgroepen in Amazon Web Services.

Voor gerelateerde informatie over load balancers raadpleegt u *vRealize Automation configureren*.

Voorwaarden

Amazon-reserveringsinformatie opgeven.

Procedure

- 1 Klik op het tabblad **Bronnen**.
- 2 Selecteer een computerbron waarop u machines wilt inrichten in het vervolgkeuzemenu **Computerbron**.

De beschikbare Amazon-regio's worden weergegeven.

- 3 (Optioneel) Geef een getal op in het tekstvak **Machinequotum** om het maximum aantal machines in te stellen dat kan worden ingericht voor deze reservering.

Alleen machines die zijn ingeschakeld worden meegeteld in het quotum. Laat het tekstvak leeg om geen beperkingen te stellen aan de reservering.

- 4 Selecteer een methode om sleutelparen toe te wijzen aan computerinstanties in het vervolgkeuzemenu **Sleutelpaar**.

Optie	Beschrijving
Niet opgegeven	Hiermee wordt het gedrag bepaald van het sleutelpaar op het niveau van de blueprint in plaats van het niveau van de reservering.
Automatisch gegenereerd per bedrijfspgroep	Elke machine die in dezelfde bedrijfspgroep wordt ingericht, heeft hetzelfde sleutelpaar, inclusief machines die in andere reserveringen worden ingericht wanneer de machines dezelfde computerbron en bedrijfspgroep hebben. Omdat sleutelparen die op deze manier worden gegenereerd, zijn gekoppeld aan een bedrijfspgroep, worden de sleutelparen verwijderd wanneer de bedrijfspgroep wordt verwijderd.
Automatisch gegenereerd per machine	Elke machine heeft een uniek sleutelpaar. Dit is de veiligste methode omdat er geen sleutelparen worden gedeeld tussen machines onderling.
Specifiek sleutelpaar	Elke machine die wordt ingericht voor deze reservering, heeft hetzelfde sleutelpaar. Blader naar een sleutelpaar dat u voor deze reservering wilt gebruiken.

- 5 Als u **Specifiek sleutelpaar** hebt geselecteerd in het vervolgkeuzemenu **Sleutelpaar**, selecteert u een waarde voor het sleutelpaar in het vervolgkeuzemenu **Specifiek sleutelpaar**.
- 6 In een configuratie voor een virtuele privécloud van Amazon schakelt u het selectievakje **Toewijzen aan een subnet in een VPC** in. Anders laat u het selectievakje uitgeschakeld.

Als u **Toewijzen aan een subnet in een VPC** selecteert, worden de volgende opties voor locaties of subnetten, beveiligingsgroepen en load balancers weergegeven in een snelmenu in plaats van op dezelfde pagina.

Geef bij een VPC-reservering de beveiligingsgroepen en subnetten op voor elke VPC die in de reservering is opgenomen.

- 7 Selecteer een of meer beschikbare locaties (niet-VPC) of subnetten (VPC) in de lijst **Locaties** of **Subnetten**.

Selecteer elke beschikbare locatie of subnet dat u beschikbaar wilt maken voor inrichting.

- 8 Selecteer één of meer beveiligingsgroepen die kunnen worden toegewezen aan een machine tijdens de inrichting, in de lijst **Beveiligingsgroepen**.

Selecteer elke beveiligingsgroep die tijdens de inrichting aan een machine kan worden toegewezen. Voor elke beschikbare regio moet minstens één beveiligingsgroep zijn opgegeven.

- 9 Selecteer één of meer beschikbare Load Balancers in de lijst **Load Balancers**.

Als u de functie elastische load balancer gebruikt, selecteert u een of meer beschikbare load balancers die van toepassing zijn op de geselecteerde locaties of subnetten.

Resultaten

U kunt de reservering nu opslaan door te klikken op **Opslaan**. Of u kunt aangepaste eigenschappen toevoegen om nog nauwkeuriger te bepalen hoe reserveringsspecificaties worden weergegeven. U kunt ook waarschuwingse-mails configureren, zodat u meldingen ontvangt wanneer de hoeveelheid bronnen voor de reservering beneden een bepaald peil daalt. Aangepaste eigenschappen en waarschuwingen voor Amazon-reserveringen opgeven
U kunt aangepaste eigenschappen koppelen aan een vRealize Automation-reservering. U kunt ook waarschuwingen configureren om e-mailmeldingen te verzenden wanneer er weinig reserveringsbronnen zijn.

Aangepaste eigenschappen en waarschuwingse-mails zijn optionele configuraties voor de reservering. Als u geen koppelingen wilt maken voor de aangepaste eigenschappen of waarschuwingen wilt instellen, klikt u op **Opslaan** om het maken van de reservering te beëindigen.

U kunt nu zoveel aangepaste eigenschappen toevoegen als er nodig zijn.

Als het zo is geconfigureerd, kunnen waarschuwingen dagelijks worden gegenereerd, in plaats van bij het bereiken van de opgegeven drempelwaardes.

Belangrijk Meldingen worden alleen verzonden als waarschuwingse-mails zijn geconfigureerd en meldingen zijn ingeschakeld.

Voorwaarden

[Bron- en netwerkinstellingen opgeven voor Amazon-reserveringen.](#)

Procedure

- 1 Klik op het tabblad **Eigenschappen**.
- 2 Klik op **Nieuw**.
- 3 Geef een geldige naam op voor de aangepaste eigenschap.

- 4 Geef indien nodig een waarde op voor de eigenschap.
- 5 Klik op **Opslaan**.
- 6 (Optioneel) Voeg extra aangepaste eigenschappen toe.
- 7 Klik op het tabblad **Waarschuwingen**.
- 8 Schakel het selectievakje **Waarschuwingen over capaciteit** in om de waarschuwingen te configureren die worden verzonden.
- 9 Gebruik de schuifregelaar om de drempelwaarde in te stellen voor de toewijzing van de beschikbare bronnen.
- 10 Voer in het tekstvak **Ontvangers** de AD-gebruikers- of groepsnamen (geen e-mailadressen) in om waarschuwingmeldingen te ontvangen.

Voer op elke regel een naam in. Druk op Enter om de verschillende vermeldingen te scheiden.
- 11 Selecteer **Waarschuwingen naar groepsbeheerder sturen** om groepsbeheerders toe te voegen aan de ontvangers van waarschuwingse-mails.

De e-mailwaarschuwingen worden verzonden naar de gebruikers in de lijst **E-mails van beheerder versturen aan** voor de bedrijfsgroep.
- 12 Geef een herinneringsfrequentie (dagen) op.
- 13 Klik op **Opslaan**.

Resultaten

De reservering wordt opgeslagen en weergegeven in de lijst Reserveringen.

Wat nu te doen

U kunt optioneel een reserveringsbeleid configureren of beginnen met de voorbereiding van de inrichting.

Gebruikers die het recht hebben om blueprints te maken, kunnen deze nu maken.

Een OpenStack-reservering maken

U moet bronnen aan machines toewijzen door een reservering te maken voordat leden van een bedrijfsgroep machine-inrichting kunnen aanvragen.

Maak een OpenStack-reservering.

Procedure

1 [OpenStack-reserveringsinformatie opgeven](#)

Elke reservering is geconfigureerd voor een specifieke bedrijfsgroep zodat deze toegang krijgt om machines aan te vragen op een opgegeven computerbron.

2 Bron- en netwerkinstellingen opgeven voor OpenStack-reserveringen

Geef bron- en netwerkinstellingen op die beschikbaar zijn voor -machines die vanaf deze vRealize Automation-reservering zijn ingericht.

3 Aangepaste eigenschappen en waarschuwingen voor OpenStack-reserveringen opgeven

U kunt aangepaste eigenschappen koppelen aan een vRealize Automation-reservering. U kunt ook waarschuwingen configureren om e-mailmeldingen te verzenden wanneer er weinig reserveringsbronnen zijn.

OpenStack-reserveringsinformatie opgeven

Elke reservering is geconfigureerd voor een specifieke bedrijfsgroep zodat deze toegang krijgt om machines aan te vragen op een opgegeven computerbron.

Opmerking Nadat u een reservering hebt gemaakt, kunt u de koppelingen met bedrijfsgroepen of computerbronnen niet meer wijzigen.

U kunt bepalen hoe reserveringen worden weergegeven, tijdens het toevoegen, bewerken of verwijderen, door gebruik te maken van de optie **Filteren op categorie** op de pagina Reserveringen. Houd er rekening mee dat reserveringen van testagenten niet worden weergegeven in de lijst met reserveringen wanneer u filtert op categorie.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Controleer of de tenantbeheerder ten minste één bedrijfsgroep heeft gemaakt.
- Controleer of er een computerbron bestaat.
- Controleer of er optionele beveiligingsgroepen of zwevende IP-adressen zijn geconfigureerd.
- Controleer of er vereiste sleutelparen bestaan. Zie [Sleutelparen beheren](#).
- Controleer of er een computerbron bestaat.
- Configureer de netwerkinstellingen.

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Reserveringen**.
- 2 Klik op het pictogram **Nieuw** (+) en selecteer het type reservering dat u wilt maken.
Selecteer **OpenStack**.
- 3 Geef een naam op in het tekstvak **Naam**.
- 4 Selecteer een tenant in het vervolgkeuzemenu **Tenant**.
- 5 Selecteer een bedrijfsgroep in het vervolgkeuzemenu **Bedrijfsgroep**.

Alleen gebruikers in deze bedrijfsgroep kunnen machines inrichten met behulp van deze reservering.

- 6** (Optioneel) Selecteer een reserveringsbeleid in het vervolgkeuzemenu **Reserveringsbeleid**.

Voor deze optie is vereist dat er minimaal één reserveringsbeleid bestaat. U kunt de reservering later bewerken om een reserveringsbeleid op te geven.

U kunt een reserveringsbeleid gebruiken om de inrichting te beperken tot bepaalde reserveringen.

- 7** Geef een getal op in het tekstvak **Prioriteit** om de prioriteit voor de reservering in te stellen.

De prioriteit wordt gebruikt wanneer er meer dan een reservering bestaat voor de bedrijfsgroep. Een reservering met de prioriteit 1 wordt eerder ingericht dan een reservering met de prioriteit 2.

- 8** (Optioneel) Schakel het selectievakje **Deze reservering inschakelen** uit als u niet wilt dat deze reservering actief is.

Resultaten

Verlaat deze pagina niet. Uw reservering is niet compleet.

Bron- en netwerkinstellingen opgeven voor OpenStack-reserveringen

Geef bron- en netwerkinstellingen op die beschikbaar zijn voor -machines die vanaf deze vRealize Automation-reservering zijn ingericht.

Voorwaarden

[OpenStack-reserveringsinformatie opgeven.](#)

Procedure

- 1** Klik op het tabblad **Bronnen**.
- 2** Selecteer een computerbron waarop u machines wilt inrichten in het vervolgkeuzemenu **Computerbron**.

Alleen sjablonen die zich op het geselecteerde cluster bevinden, kunnen worden gekloond met deze reservering.

Tijdens het inrichten worden machines in een host geplaatst die is verbonden met de lokale opslag. Als de reservering gebruikmaakt van de lokale opslag, worden alle machines die door de reservering zijn ingericht, in de host geplaatst die deze lokale opslag bevat. Als u echter de aangepaste `VirtualMachine.Admin.ForceHost`-eigenschap gebruikt, die een machine forceert om te worden ingericht op een andere host, mislukt de inrichting. De inrichting mislukt ook als de sjabloon aan de hand waarvan de machine is gekloond zich op de lokale opslag bevindt, en is gekoppeld aan een machine in een ander cluster. In dit geval mislukt de inrichting omdat de sjabloon niet toegankelijk is.

- 3** (Optioneel) Geef een getal op in het tekstvak **Machinequotum** om het maximum aantal machines in te stellen dat kan worden ingericht voor deze reservering.

Alleen machines die zijn ingeschakeld worden meegeteld in het quotum. Laat het tekstvak leeg om geen beperkingen te stellen aan de reservering.

- 4 Selecteer een methode om sleutelparen toe te wijzen aan computerinstanties in het vervolgkeuzemenu **Sleutelpaar**.

Optie	Beschrijving
Niet opgegeven	Hiermee wordt het gedrag bepaald van het sleutelpaar op het niveau van de blueprint in plaats van het niveau van de reservering.
Automatisch gegenereerd per bedrijfsgroep	Elke machine die in dezelfde bedrijfsgroep wordt ingericht, heeft hetzelfde sleutelpaar, inclusief machines die in andere reserveringen worden ingericht wanneer de machines dezelfde computerbron en bedrijfsgroep hebben. Omdat sleutelparen die op deze manier worden gegenereerd, zijn gekoppeld aan een bedrijfsgroep, worden de sleutelparen verwijderd wanneer de bedrijfsgroep wordt verwijderd.
Automatisch gegenereerd per machine	Elke machine heeft een uniek sleutelpaar. Dit is de veiligste methode omdat er geen sleutelparen worden gedeeld tussen machines onderling.
Specifiek sleutelpaar	Elke machine die wordt ingericht voor deze reservering, heeft hetzelfde sleutelpaar. Blader naar een sleutelpaar dat u voor deze reservering wilt gebruiken.

- 5 Als u **Specifiek sleutelpaar** hebt geselecteerd in het vervolgkeuzemenu **Sleutelpaar**, selecteert u een waarde voor het sleutelpaar in het vervolgkeuzemenu **Specifiek sleutelpaar**.
- 6 Selecteer één of meer beveiligingsgroepen die kunnen worden toegewezen aan een machine tijdens de inrichting, in de lijst **Beveiligingsgroepen**.
- 7 Klik op het tabblad **Netwerk**.
- 8 Configureer een netwerkpad voor machines die worden ingericht met behulp van deze reservering.
- a (Optioneel) Als de optie beschikbaar is, selecteert u een opslagendpoint in het vervolgkeuzemenu **Endpoint**.
- De optie FlexClone wordt weergegeven in de kolom endpoint als een NetApp ONTAP-endpoint bestaat en er een virtuele host is. Als er een NetApp ONTAP-endpoint is, wordt op de reserveringspagina het endpoint weergegeven dat is gekoppeld aan het opslagpad. Wanneer u een endpoint voor een opslagpad toevoegt, bijwerkt of verwijdert, wordt deze wijziging weergegeven in alle betreffende reserveringen.
- Wanneer u een endpoint voor een opslagpad toevoegt, bijwerkt of verwijdert, wordt deze wijziging weergegeven in de reserveringspagina.
- b Selecteer een of meer **netwerkadapters** voor de machines die moeten worden ingericht voor deze reservering.

- c (Optioneel) Selecteer een beschikbaar **netwerkprofiel** voor elke geselecteerde netwerkadapter.
- d (Optioneel) Als de geavanceerde instellingen beschikbaar zijn, selecteert u een **transportzone** en een of meer **laag 0 logische routers** die moeten worden gebruikt bij het implementeren van een blueprint die load balancers bevat.

Met een transportzone wordt aangegeven welke clusters de netwerkadapters omvatten. Als u een transportzone opgeeft in een reservering en in een blueprint, moeten de waarden voor de transportzone overeenkomen.

U kunt meer dan één netwerkadapter selecteren in een reservering, maar er wordt slechts één netwerk gebruikt bij de inrichting van een machine.

Resultaten

U kunt de reservering nu opslaan door te klikken op **Opslaan**. Of u kunt aangepaste eigenschappen toevoegen om nog nauwkeuriger te bepalen hoe reserveringsspecificaties worden weergegeven. U kunt ook waarschuwingse-mails configureren, zodat u meldingen ontvangt wanneer de hoeveelheid bronnen voor de reservering beneden een bepaald peil daalt. Aangepaste eigenschappen en waarschuwingen voor OpenStack-reserveringen opgeven. U kunt aangepaste eigenschappen koppelen aan een vRealize Automation-reservering. U kunt ook waarschuwingen configureren om e-mailmeldingen te verzenden wanneer er weinig reserveringsbronnen zijn.

Aangepaste eigenschappen en waarschuwingse-mails zijn optionele configuraties voor de reservering. Als u geen koppelingen wilt maken voor de aangepaste eigenschappen of waarschuwingen wilt instellen, klikt u op **Opslaan** om het maken van de reservering te beëindigen.

U kunt nu zoveel aangepaste eigenschappen toevoegen als er nodig zijn.

Belangrijk Meldingen worden alleen verzonden als waarschuwingse-mails zijn geconfigureerd en meldingen zijn ingeschakeld.

Als het zo is geconfigureerd, kunnen waarschuwingen dagelijks worden gegenereerd, in plaats van bij het bereiken van de opgegeven drempelwaardes.

Voorwaarden

[Bron- en netwerkinstellingen opgeven voor OpenStack-reserveringen.](#)

Procedure

- 1 Klik op het tabblad **Eigenschappen**.
- 2 Klik op **Nieuw**.
- 3 Geef een geldige naam op voor de aangepaste eigenschap.
- 4 Geef indien nodig een waarde op voor de eigenschap.
- 5 Klik op **Opslaan**.

- 6 (Optioneel) Voeg extra aangepaste eigenschappen toe.
- 7 Klik op het tabblad **Waarschuwingen**.
- 8 Schakel het selectievakje **Waarschuwingen over capaciteit** in om de waarschuwingen te configureren die worden verzonden.
- 9 Gebruik de schuifregelaar om de drempelwaarde in te stellen voor de toewijzing van de beschikbare bronnen.
- 10 Voer in het tekstvak **Ontvangers** de AD-gebruikers- of groepsnamen (geen e-mailadressen) in om waarschuwingmeldingen te ontvangen.

Voer op elke regel een naam in. Druk op Enter om de verschillende vermeldingen te scheiden.
- 11 Selecteer **Waarschuwingen naar groepsbeheerder sturen** om groepsbeheerders toe te voegen aan de ontvangers van waarschuwingse-mails.

De e-mailwaarschuwingen worden verzonden naar de gebruikers in de lijst **E-mails van beheerder versturen aan** voor de bedrijfsgroep.
- 12 Geef een herinneringsfrequentie (dagen) op.
- 13 Klik op **Opslaan**.

Resultaten

De reservering wordt opgeslagen en weergegeven in de lijst Reserveringen.

Wat nu te doen

U kunt optioneel een reserveringsbeleid configureren of beginnen met de voorbereiding van de inrichting.

Gebruikers die het recht hebben om blueprints te maken, kunnen deze nu maken.

Een vCloud Air-reservering maken

U moet bronnen aan machines toewijzen door een vRealize Automation-reservering te maken voordat leden van een bedrijfsgroep machine-inrichting kunnen aanvragen.

Elke bedrijfsgroep moet minstens één reservering hebben zodat de leden van die groep machines van dat type kunnen inrichten.

Procedure

1 vCloud Air-reserveringsinformatie opgeven

U kunt voor alle afzonderlijke vCloud Air-machineabonnementen of OnDemand-bronnen een reservering maken. Elke reservering is geconfigureerd voor een specifieke bedrijfsgroep om deze toegang te verlenen voor het aanvragen van machines.

2 Bron- en netwerkinstellingen opgeven voor een vCloud Air-reservering

Geef bron- en netwerkinstellingen op die beschikbaar zijn voor vCloud Air-machines die vanaf deze vRealize Automation-reservering zijn ingericht.

3 Aangepaste eigenschappen en waarschuwingen voor een vCloud Air-reservering opgeven

U kunt aangepaste eigenschappen koppelen aan een vRealize Automation-reservering. U kunt ook waarschuwingen configureren om e-mailmeldingen te verzenden wanneer er weinig reserveringsbronnen zijn.

vCloud Air-reserveringsinformatie opgeven

U kunt voor alle afzonderlijke vCloud Air-machineabbonnementen of OnDemand-bronnen een reservering maken. Elke reservering is geconfigureerd voor een specifieke bedrijfsgroep om deze toegang te verlenen voor het aanvragen van machines.

U kunt bepalen hoe reserveringen worden weergegeven, tijdens het toevoegen, bewerken of verwijderen, door gebruik te maken van de optie **Filteren op categorie** op de pagina Reserveringen. Houd er rekening mee dat reserveringen van testagenten niet worden weergegeven in de lijst met reserveringen wanneer u filtert op categorie.

Opmerking Nadat u een reservering hebt gemaakt, kunt u de koppelingen met bedrijfsgroepen of computerbronnen niet meer wijzigen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Controleer of de tenantbeheerder ten minste één bedrijfsgroep heeft gemaakt.
- Controleer of er een computerbron bestaat.
- Configureer de netwerkinstellingen.
- (Optioneel) Configureer de informatie over een netwerkprofiel.

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Reserveringen**.
- 2 Klik op het pictogram **Nieuw** (+) en selecteer het type reservering dat u wilt maken.
De beschikbare cloudreserveringstypes zijn Amazon, OpenStack, vCloud Air en vCloud Director.
Selecteer **vCloud Air**.
- 3 Geef een naam op in het tekstvak **Naam**.
- 4 Selecteer een tenant in het vervolgkeuzemenu **Tenant**.
- 5 Selecteer een bedrijfsgroep in het vervolgkeuzemenu **Bedrijfsgroep**.
Alleen gebruikers in deze bedrijfsgroep kunnen machines inrichten met behulp van deze reservering.
- 6 (Optioneel) Selecteer een reserveringsbeleid in het vervolgkeuzemenu **Reserveringsbeleid**.
Voor deze optie is vereist dat er minimaal één reserveringsbeleid bestaat. U kunt de reservering later bewerken om een reserveringsbeleid op te geven.

U kunt een reserveringsbeleid gebruiken om de inrichting te beperken tot bepaalde reserveringen.

- 7 Geef een getal op in het tekstvak **Prioriteit** om de prioriteit voor de reservering in te stellen.

De prioriteit wordt gebruikt wanneer er meer dan een reservering bestaat voor de bedrijfsgroep. Een reservering met de prioriteit 1 wordt eerder ingericht dan een reservering met de prioriteit 2.

- 8 (Optioneel) Schakel het selectievakje **Deze reservering inschakelen** uit als u niet wilt dat deze reservering actief is.

Resultaten

Verlaat deze pagina niet. Uw reservering is niet compleet.

Bron- en netwerkinstellingen opgeven voor een vCloud Air-reservering

Geef bron- en netwerkinstellingen op die beschikbaar zijn voor vCloud Air-machines die vanaf deze vRealize Automation-reservering zijn ingericht.

De beschikbare brontoewijzingsmodellen voor machines die zijn ingericht vanaf een vCloud Director-reservering zijn Toewijzingspool, Betalen-naar-gebruik en Reserveringspool. Voor Betalen-naar-gebruik hoeft u geen opslag- of geheugenhoeveelheden op te geven, maar u moet wel een prioriteit opgeven voor het opslagpad. Voor informatie over deze toewijzingsmodellen raadpleegt u de vCloud Air-documentatie.

U kunt een standaardopslagprofiel of opslagprofiel op schijfniveau opgeven. Schijfopslag op meerdere niveaus is beschikbaar op vCloud Air-endpoints.

Voor integraties die gebruikmaken van SDRS-opslag (Storage Distributed Resource Scheduler), kunt u een opslagcluster selecteren zodat SDRS automatisch de opslaglocatie en taakverdeling kan afhandelen van machines die worden ingericht vanuit deze reservering. De automatiseringsmodus voor SDRS moet worden ingesteld op Automatisch. Selecteer anders een datastore binnen het cluster om het gedrag van standalone datastores te leren kennen. SDRS wordt niet ondersteund op FlexClone-opslagapparaten.

Opmerking Reserveringen die zijn gedefinieerd voor vCloud Air-endpoints en vCloud Director-endpoints bieden geen ondersteuning voor het gebruik van netwerkprofielen voor het inrichten van machines.

Voorwaarden

[vCloud Director-reserveringsinformatie opgeven.](#)

Procedure

- 1 Klik op het tabblad **Bronnen**.
- 2 Selecteer een computerbron waarop u machines wilt inrichten in het vervolgkeuzemenu **Computerbron**.

Alleen sjablonen die zich op het geselecteerde cluster bevinden, kunnen worden gekloond met deze reservering.

3 Selecteer een toewijzingsmodel.**4** (Optioneel) Geef een getal op in het tekstvak **Machinequotum** om het maximum aantal machines in te stellen dat kan worden ingericht voor deze reservering.

Alleen machines die zijn ingeschakeld worden meegeteld in het quotum. Laat het tekstvak leeg om geen beperkingen te stellen aan de reservering.

5 Geef de hoeveelheid geheugen (in GB) op die moet worden toegewezen aan deze reservering in de tabel Geheugen.

De waarde van het totale geheugen voor de reservering wordt bepaald aan de hand van de geselecteerde computerbron.

6 Selecteer één of meer opslagpaden in de lijst.

De beschikbare opties voor opslagpaden worden bepaald aan de hand van de geselecteerde computerbron.

a Geef een waarde op in het tekstvak **Deze reservering is gereserveerd** om aan te geven hoeveel opslagruimte moet worden toegewezen aan deze reservering.

b Geef een waarde op in het tekstvak **Prioriteit** om de prioriteitswaarde op te geven voor het opslagpad in verhouding tot andere opslagpaden die betrekking hebben op deze reservering.

De prioriteit wordt gebruikt voor meerdere opslagpaden. Een opslagpad met de prioriteit 0 wordt gebruikt voordat een pad met de prioriteit 1 wordt gebruikt.

c Klik op de optie **Uitschakelen** als u een opslagpad niet wilt laten gebruiken door deze reservering.

d Herhaal deze stap om indien nodig andere clusters en datastores te configureren.

7 Klik op het tabblad **Netwerk**.**8** Configureer een netwerkpad voor machines die worden ingericht met behulp van deze reservering.

a (Optioneel) Als de optie beschikbaar is, selecteert u een opslagendpoint in het vervolgkeuzemenu **Endpoint**.

De optie FlexClone wordt weergegeven in de kolom endpoint als een NetApp ONTAP-endpoint bestaat en er een virtuele host is. Als er een NetApp ONTAP-endpoint is, wordt op de reserveringspagina het endpoint weergegeven dat is gekoppeld aan het opslagpad. Wanneer u een endpoint voor een opslagpad toevoegt, bijwerkt of verwijdt, wordt deze wijziging weergegeven in alle betreffende reserveringen.

Wanneer u een endpoint voor een opslagpad toevoegt, bijwerkt of verwijdt, wordt deze wijziging weergegeven in de reserveringspagina.

b Selecteer een of meer **netwerkadapters** voor de machines die moeten worden ingericht voor deze reservering.

- c (Optioneel) Selecteer een beschikbaar **netwerkprofiel** voor elke geselecteerde netwerkadapter.
- d (Optioneel) Als de geavanceerde instellingen beschikbaar zijn, selecteert u een **transportzone** en een of meer **laag 0 logische routers** die moeten worden gebruikt bij het implementeren van een blueprint die load balancers bevat.

Met een transportzone wordt aangegeven welke clusters de netwerkadapters omvatten. Als u een transportzone opgeeft in een reservering en in een blueprint, moeten de waarden voor de transportzone overeenkomen.

U kunt meer dan één netwerkadapter selecteren in een reservering, maar er wordt slechts één netwerk gebruikt bij de inrichting van een machine.

Resultaten

U kunt de reservering nu opslaan door te klikken op **Opslaan**. Of u kunt aangepaste eigenschappen toevoegen om nog nauwkeuriger te bepalen hoe reserveringsspecificaties worden weergegeven. U kunt ook waarschuwingse-mails configureren, zodat u meldingen ontvangt wanneer de hoeveelheid bronnen voor de reservering beneden een bepaald peil daalt. Aangepaste eigenschappen en waarschuwingen voor een vCloud Air-reservering opgeven. U kunt aangepaste eigenschappen koppelen aan een vRealize Automation-reservering. U kunt ook waarschuwingen configureren om e-mailmeldingen te verzenden wanneer er weinig reserveringsbronnen zijn.

Aangepaste eigenschappen en waarschuwingse-mails zijn optionele configuraties voor de reservering. Als u geen koppelingen wilt maken voor de aangepaste eigenschappen of waarschuwingen wilt instellen, klikt u op **Opslaan** om het maken van de reservering te beëindigen.

U kunt nu zoveel aangepaste eigenschappen toevoegen als er nodig zijn.

Als het zo is geconfigureerd, kunnen waarschuwingen dagelijks worden gegenereerd, in plaats van bij het bereiken van de opgegeven drempelwaarden.

Belangrijk Meldingen worden alleen verzonden als waarschuwingse-mails zijn geconfigureerd en meldingen zijn ingeschakeld.

Voor reserveringen die gebruikmaken van Betalen-naar-gebruik en waarvoor geen beperkingen zijn ingesteld, worden geen waarschuwingen afgegeven.

Voorwaarden

[Bron- en netwerkinstellingen opgeven voor een vCloud Air-reservering](#)

Procedure

- 1 Klik op het tabblad **Eigenschappen**.
- 2 Klik op **Nieuw**.
- 3 Geef een geldige naam op voor de aangepaste eigenschap.

- 4 Geef indien nodig een waarde op voor de eigenschap.
- 5 (Optioneel) Schakel het selectievakje **Gecodeerd** in om de waarde van de eigenschap te versleutelen.
- 6 (Optioneel) Schakel het selectievakje **Vragen aan gebruiker** in om ervoor te zorgen dat de gebruiker een waarde moet opgeven.
Deze optie kan niet worden overschreven tijdens het inrichten.
- 7 Klik op **Opslaan**.
- 8 (Optioneel) Voeg extra aangepaste eigenschappen toe.
- 9 Klik op het tabblad **Waarschuwingen**.
- 10 Schakel het selectievakje **Waarschuwingen over capaciteit** in om de waarschuwingen te configureren die worden verzonden.
- 11 Gebruik de schuifregelaar om de drempelwaarde in te stellen voor de toewijzing van de beschikbare bronnen.
- 12 Voer in het tekstvak **Ontvangers** de AD-gebruikers- of groepsnamen (geen e-mailadressen) in om waarschuwingmeldingen te ontvangen.
Voer op elke regel een naam in. Druk op Enter om de verschillende vermeldingen te scheiden.
- 13 Selecteer **Waarschuwingen naar groepsbeheerder sturen** om groepsbeheerders toe te voegen aan de ontvangers van waarschuwingse-mails.
De e-mailwaarschuwingen worden verzonden naar de gebruikers in de lijst **E-mails van beheerder versturen aan** voor de bedrijfsgroep.
- 14 Geef een herinneringsfrequentie (dagen) op.
- 15 Klik op **Opslaan**.

Resultaten

De reservering wordt opgeslagen en weergegeven in de lijst Reserveringen.

Een vCloud Director-reservering maken

U moet bronnen aan machines toewijzen door een vRealize Automation-reservering te maken voordat leden van een bedrijfsgroep machine-inrichting kunnen aanvragen.

Elke bedrijfsgroep moet minstens één reservering hebben zodat de leden van die groep machines van dat type kunnen inrichten.

Procedure

1 [vCloud Director-reserveringsinformatie opgeven](#)

U kunt een reservering maken voor elk vCloud Director virtueel datacenter (VDC) van een organisatie. Elke reservering is geconfigureerd voor een specifieke bedrijfsgroep zodat deze toegang krijgt om machines aan te vragen op een opgegeven computerbron.

2 Bron- en netwerkinstellingen opgeven voor een vCloud Director-reservering

Geef bron- en netwerkinstellingen op die beschikbaar zijn voor vCloud Director-machines die vanaf deze vRealize Automation-reservering zijn ingericht.

3 Aangepaste eigenschappen en waarschuwingen voor vCloud Director-reserveringen opgeven

U kunt aangepaste eigenschappen koppelen aan een vRealize Automation-reservering. U kunt ook waarschuwingen configureren om e-mailmeldingen te verzenden wanneer er weinig reserveringsbronnen zijn.

Wat nu te doen

U kunt optioneel een reserveringsbeleid configureren of beginnen met de voorbereiding van de inrichting.

Gebruikers die het recht hebben om blueprints te maken, kunnen deze nu maken.

vCloud Director-reserveringsinformatie opgeven

U kunt een reservering maken voor elk vCloud Director virtueel datacenter (VDC) van een organisatie. Elke reservering is geconfigureerd voor een specifieke bedrijfsgroep zodat deze toegang krijgt om machines aan te vragen op een opgegeven computerbron.

U kunt bepalen hoe reserveringen worden weergegeven, tijdens het toevoegen, bewerken of verwijderen, door gebruik te maken van de optie **Filteren op categorie** op de pagina Reserveringen. Houd er rekening mee dat reserveringen van testagenten niet worden weergegeven in de lijst met reserveringen wanneer u filtert op categorie.

Opmerking Nadat u een reservering hebt gemaakt, kunt u de koppelingen met bedrijfsgroepen of computerbronnen niet meer wijzigen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Controleer of de tenantbeheerder ten minste één bedrijfsgroep heeft gemaakt.
- Controleer of er een computerbron bestaat.
- Configureer de netwerkinstellingen.
- (Optioneel) Configureer de informatie over een netwerkprofiel.

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Reserveringen**.
- 2 Klik op het pictogram **Nieuw** (+) en selecteer het type reservering dat u wilt maken.
De beschikbare cloudreserveringstypes zijn Amazon, OpenStack, vCloud Air en vCloud Director.
Selecteer **vCloud Director**.

3 Geef een naam op in het tekstvak **Naam**.

4 Selecteer een tenant in het vervolgkeuzemenu **Tenant**.

5 Selecteer een bedrijfsgroep in het vervolgkeuzemenu **Bedrijfsgroep**.

Alleen gebruikers in deze bedrijfsgroep kunnen machines inrichten met behulp van deze reservering.

6 (Optioneel) Selecteer een reserveringsbeleid in het vervolgkeuzemenu **Reserveringsbeleid**.

Voor deze optie is vereist dat er minimaal één reserveringsbeleid bestaat. U kunt de reservering later bewerken om een reserveringsbeleid op te geven.

U kunt een reserveringsbeleid gebruiken om de inrichting te beperken tot bepaalde reserveringen.

7 Geef een getal op in het tekstvak **Prioriteit** om de prioriteit voor de reservering in te stellen.

De prioriteit wordt gebruikt wanneer er meer dan een reservering bestaat voor de bedrijfsgroep. Een reservering met de prioriteit 1 wordt eerder ingericht dan een reservering met de prioriteit 2.

8 (Optioneel) Schakel het selectievakje **Deze reservering inschakelen** uit als u niet wilt dat deze reservering actief is.

Resultaten

Verlaat deze pagina niet. Uw reservering is niet compleet.

Bron- en netwerkinstellingen opgeven voor een vCloud Director-reservering

Geef bron- en netwerkinstellingen op die beschikbaar zijn voor vCloud Director-machines die vanaf deze vRealize Automation-reservering zijn ingericht.

De beschikbare brontoewijzingsmodellen voor machines die zijn ingericht vanaf een vCloud Director-reservering zijn Toewijzingspool, Betalen-naar-gebruik en Reserveringspool. Voor Betalen-naar-gebruik hoeft u geen opslag- of geheugenhoeveelheden op te geven, maar u moet wel een prioriteit opgeven voor het opslagpad. Voor informatie over deze toewijzingsmodellen raadpleegt u de vCloud Director-documentatie.

U kunt een standaardopslagprofiel of opslagprofiel op schijfniveau opgeven. Schijfopslag op meerdere niveaus is beschikbaar voor vCloud Director 5.6-endpoints en hoger. Schijfopslag op meerdere niveaus wordt niet ondersteund voor vCloud Director 5.5-endpoints.

Voor integraties die gebruikmaken van SDRS-opslag (Storage Distributed Resource Scheduler), kunt u een opslagcluster selecteren zodat SDRS automatisch de opslaglocatie en taakverdeling kan afhandelen van machines die worden ingericht vanuit deze reservering. De automatiseringsmodus voor SDRS moet worden ingesteld op Automatisch. Selecteer anders een datastore binnen het cluster om het gedrag van standalone datastores te leren kennen. SDRS wordt niet ondersteund op FlexClone-opslagapparaten.

Opmerking Reserveringen die zijn gedefinieerd voor vCloud Air-endpoints en vCloud Director-endpoints bieden geen ondersteuning voor het gebruik van netwerkprofielen voor het inrichten van machines.

Voorwaarden

[vCloud Director-reserveringsinformatie opgeven.](#)

Procedure

1 Klik op het tabblad **Bronnen**.

2 Selecteer een computerbron waarop u machines wilt inrichten in het vervolgkeuzemenu **Computerbron**.

Alleen sjablonen die zich op het geselecteerde cluster bevinden, kunnen worden gekloond met deze reservering.

3 Selecteer een toewijzingsmodel.

4 (Optioneel) Geef een getal op in het tekstvak **Machinequotum** om het maximum aantal machines in te stellen dat kan worden ingericht voor deze reservering.

Alleen machines die zijn ingeschakeld worden meegeteld in het quotum. Laat het tekstvak leeg om geen beperkingen te stellen aan de reservering.

5 Geef de hoeveelheid geheugen (in GB) op die moet worden toegewezen aan deze reservering in de tabel Geheugen.

De waarde van het totale geheugen voor de reservering wordt bepaald aan de hand van de geselecteerde computerbron.

6 Selecteer één of meer opslagpaden in de lijst.

De beschikbare opties voor opslagpaden worden bepaald aan de hand van de geselecteerde computerbron.

a Geef een waarde op in het tekstvak **Deze reservering is gereserveerd** om aan te geven hoeveel opslagruimte moet worden toegewezen aan deze reservering.

b Geef een waarde op in het tekstvak **Prioriteit** om de prioriteitswaarde op te geven voor het opslagpad in verhouding tot andere opslagpaden die betrekking hebben op deze reservering.

De prioriteit wordt gebruikt voor meerdere opslagpaden. Een opslagpad met de prioriteit 0 wordt gebruikt voordat een pad met de prioriteit 1 wordt gebruikt.

- c Klik op de optie **Uitschakelen** als u een opslagpad niet wilt laten gebruiken door deze reservering.
- d Herhaal deze stap om indien nodig andere clusters en datastores te configureren.

7 Klik op het tabblad **Netwerk**.

8 Configureer een netwerkpad voor machines die worden ingericht met behulp van deze reservering.

- a (Optioneel) Als de optie beschikbaar is, selecteert u een opslagendpoint in het vervolgkeuzemenu **Endpoint**.

De optie FlexClone wordt weergegeven in de kolom endpoint als een NetApp ONTAP-endpoint bestaat en er een virtuele host is. Als er een NetApp ONTAP-endpoint is, wordt op de reserveringspagina het endpoint weergegeven dat is gekoppeld aan het opslagpad. Wanneer u een endpoint voor een opslagpad toevoegt, bijwerkt of verwijdert, wordt deze wijziging weergegeven in alle betreffende reserveringen.

Wanneer u een endpoint voor een opslagpad toevoegt, bijwerkt of verwijdert, wordt deze wijziging weergegeven in de reserveringspagina.

- b Selecteer een of meer **netwerkadapters** voor de machines die moeten worden ingericht voor deze reservering.
- c (Optioneel) Selecteer een beschikbaar **netwerkprofiel** voor elke geselecteerde netwerkadapter.
- d (Optioneel) Als de geavanceerde instellingen beschikbaar zijn, selecteert u een **transportzone** en een of meer **laag 0 logische routers** die moeten worden gebruikt bij het implementeren van een blueprint die load balancers bevat.

Met een transportzone wordt aangegeven welke clusters de netwerkadapters omvatten. Als u een transportzone opgeeft in een reservering en in een blueprint, moeten de waarden voor de transportzone overeenkomen.

U kunt meer dan één netwerkadapter selecteren in een reservering, maar er wordt slechts één netwerk gebruikt bij de inrichting van een machine.

Resultaten

U kunt de reservering nu opslaan door te klikken op **Opslaan**. Of u kunt aangepaste eigenschappen toevoegen om nog nauwkeuriger te bepalen hoe reserveringsspecificaties worden weergegeven. U kunt ook waarschuwingse-mails configureren, zodat u meldingen ontvangt wanneer de hoeveelheid bronnen voor de reservering beneden een bepaald peil daalt. Aangepaste eigenschappen en waarschuwingen voor vCloud Director-reserveringen opgeven. U kunt aangepaste eigenschappen koppelen aan een vRealize Automation-reservering. U kunt ook waarschuwingen configureren om e-mailmeldingen te verzenden wanneer er weinig reserveringsbronnen zijn.

Aangepaste eigenschappen en waarschuwingse-mails zijn optionele configuraties voor de reservering. Als u geen koppelingen wilt maken voor de aangepaste eigenschappen of waarschuwingen wilt instellen, klikt u op **Opslaan** om het maken van de reservering te beëindigen.

U kunt nu zoveel aangepaste eigenschappen toevoegen als er nodig zijn.

Als het zo is geconfigureerd, kunnen waarschuwingen dagelijks worden gegenereerd, in plaats van bij het bereiken van de opgegeven drempelwaarden.

Belangrijk Meldingen worden alleen verzonden als waarschuwingse-mails zijn geconfigureerd en meldingen zijn ingeschakeld.

Voor reserveringen die gebruikmaken van Betalen-naar-gebruik en waarvoor geen beperkingen zijn ingesteld, worden geen waarschuwingen afgegeven.

Voorwaarden

[Bron- en netwerkinstellingen opgeven voor een vCloud Director-reservering.](#)

Procedure

- 1 Klik op het tabblad **Eigenschappen**.
- 2 Klik op **Nieuw**.
- 3 Geef een geldige naam op voor de aangepaste eigenschap.
- 4 Geef indien nodig een waarde op voor de eigenschap.
- 5 (Optioneel) Schakel het selectievakje **Gecodeerd** in om de waarde van de eigenschap te versleutelen.
- 6 (Optioneel) Schakel het selectievakje **Vragen aan gebruiker** in om ervoor te zorgen dat de gebruiker een waarde moet opgeven.

Deze optie kan niet worden overschreven tijdens het inrichten.
- 7 Klik op **Opslaan**.
- 8 (Optioneel) Voeg extra aangepaste eigenschappen toe.
- 9 Klik op het tabblad **Waarschuwingen**.
- 10 Schakel het selectievakje **Waarschuwingen over capaciteit** in om de waarschuwingen te configureren die worden verzonden.
- 11 Gebruik de schuifregelaar om de drempelwaarde in te stellen voor de toewijzing van de beschikbare bronnen.
- 12 Voer in het tekstvak **Ontvangers** de AD-gebruikers- of groepsnamen (geen e-mailadressen) in om waarschuwing meldingen te ontvangen.

Voer op elke regel een naam in. Druk op Enter om de verschillende vermeldingen te scheiden.

- 13** Selecteer **Waarschuwingen naar groepsbeheerder sturen** om groepsbeheerders toe te voegen aan de ontvangers van waarschuwingse-mails.

De e-mailwaarschuwingen worden verzonden naar de gebruikers in de lijst **E-mails van beheerder versturen aan** voor de bedrijfsgroep.

- 14** Geef een herinneringsfrequentie (dagen) op.

- 15** Klik op **Opslaan**.

Resultaten

De reservering wordt opgeslagen en weergegeven in de lijst Reserveringen.

Een reservering voor Microsoft Azure maken

Maak een Azure-reservering voor een specifieke bedrijfsgroep om gebruikers in die groep de mogelijkheid te geven Azure virtual machines aan te vragen op een specifieke computerbron.

Als uw implementatie ondersteuning biedt voor Single Sign-On via een VPN-tunnel, kunt u via de instellingen op het tabblad Eigenschappen ondersteuning configureren voor deze functionaliteit met virtuele Azure-machines.

Opmerking Het tabblad Waarschuwingen is niet van toepassing wanneer u een Azure-reservering maakt. U kunt dit negeren. Nadat u een reservering hebt gemaakt, kunt u de bedrijfsgroepkoppelingen niet meer wijzigen. Ook is er in tegenstelling tot andere typen machines geen directe koppeling tussen een Azure-reservering en een blueprint.

U kunt bepalen hoe reserveringen worden weergegeven, tijdens het toevoegen, bewerken of verwijderen, door gebruik te maken van de optie **Filteren op categorie** op de pagina Reserveringen. Houd er rekening mee dat reserveringen van testagenten niet worden weergegeven in de lijst met reserveringen wanneer u filtert op categorie.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Controleer of de tenantbeheerder ten minste één bedrijfsgroep heeft gemaakt.
- (Optioneel) Configureer de informatie over een netwerkprofiel.
- Controleer of u toegang hebt tot de benodigde Azure-bronnen.
- Controleer of er vereiste sleutelparen bestaan. Zie *vRealize Automation configureren* voor meer informatie over sleutelparen.
- Verkrijg een geldige Azure-abonnement-id die overeenkomt met de id die is gebruikt met het betreffende Azure-endpoint. Als u meerdere Azure-abonnementen gebruikt, moet u voor elk abonnement een reservering maken.

- Als uw implementatie via een VPN-tunnel ondersteuning biedt voor Single Sign-On, moet u de juiste VPC-connectiviteit configureren voordat u een reservering maakt. Zie [Netwerk-naar-Azure VPC-connectiviteit configureren](#).

Procedure

1 [Gegevens van Microsoft Azure Basic-reserveringen configureren](#)

Geef basisgegevens op voor een Microsoft Azure-reservering.

2 [Brongegevens configureren voor Azure-reservering](#)

Wanneer u een Azure-reservering installeert, kunt u gegevens over de brongroep en opslagaccount toewijzen op basis van de gebruikte Azure-instantie. Wanneer u een reservering installeert, zal de inrichtingslogica van vRealize Automation bij de inrichting van virtual machines bronnen, zoals brongroepen en opslagaccounts, proberen toe wijzen op basis van de brongegevens van die reservering.

3 [Azure-eigenschappen configureren](#)

U kunt aangepaste eigenschappen toevoegen aan een Azure-reservering om opties te ondersteunen zoals VPN-tunneling ten behoeve van communicatie tussen meerdere netwerken. Deze functionaliteit maakt ook het toevoegen van softwareonderdelen aan blueprints mogelijk.

4 [Netwerkgegevens configureren voor een Azure-reservering](#)

U kunt in een Azure-reservering gegevens configureren voor het virtuele netwerk en de load balancer van een virtual machine.

Gegevens van Microsoft Azure Basic-reserveringen configureren

Geef basisgegevens op voor een Microsoft Azure-reservering.

Alle informatie op de pagina met reserveringsgegevens is vereist behalve het reserveringsbeleid. Alle informatie op de volgende Azure-reserveringspagina's is optioneel.

Procedure

1 Selecteer **Infrastructuur > Beheer > Reserveringen**.

2 Klik op het pictogram **Nieuw** (+) en selecteer het type reservering dat u wilt maken. Selecteer **Azure**.

3 Geef een naam op in het tekstvak **Naam**.

4 Selecteer een bedrijfsgroep in het vervolgkeuzemenu **Bedrijfsgroep**.

Alleen gebruikers in deze bedrijfsgroep kunnen machines inrichten met behulp van deze reservering.

5 Negeer het tekstvak **Reserveringsbeleid**. Dit is niet van toepassing op Azure-reserveringen.

- 6 Geef een getal op in het tekstvak **Prioriteit** om de prioriteit voor de reservering in te stellen.

De prioriteit wordt gebruikt wanneer er meer dan een reservering bestaat voor de bedrijfsgroep. Een reservering met de prioriteit 1 wordt eerder ingericht dan een reservering met de prioriteit 2.

- 7 (Optioneel) Schakel het selectievakje **Deze reservering inschakelen** uit als u niet wilt dat deze reservering actief is.

- 8 Klik op **OK**.

Brongegevens configureren voor Azure-reservering

Wanneer u een Azure-reservering installeert, kunt u gegevens over de brongroep en opslagaccount toewijzen op basis van de gebruikte Azure-instantie. Wanneer u een reservering installeert, zal de inrichtingslogica van vRealize Automation bij de inrichting van virtual machines bronnen, zoals brongroepen en opslagaccounts, proberen toe wijzen op basis van de brongegevens van die reservering.

U kunt gegevens over brongroepen en opslagaccounts voor een Azure virtual machine in de reservering configureren, maar u kunt deze velden bij de reservering desgewenst ook leeg laten. Als u de velden niet invult, worden de standaardgegevens voor brongroepen en opslagaccounts van de opgegeven Azure-abonnements-id gebruikt voor alle betrokken blueprints. U kunt deze gegevens ook bijwerken wanneer u een blueprint maakt of een virtual machine inricht.

Voorwaarden

Haal de abonnements-id van uw Azure-instantie op.

Procedure

- 1 Voer uw abonnements-id van Azure in het tekstvak **Abonnements-id** in.

- 2 Klik op de vervolgkeuzelijst **Locatie** en selecteer de reserveringslocatie.

U kunt dit veld leeg laten om een reservering te maken zonder kennis van de locatie. Maar u moet die locatiegegevens dan alsnog opgeven wanneer u een blueprint maakt of een Azure virtual machine inricht.

- 3 Klik op **Nieuw** in de tabel met brongroepen.

- a Voer de naam van de gewenste brongroep uit de Azure-instantie in het tekstvak **Naam** in.

Opmerking Het vak **Naam** moet worden ingevuld.

- b Wijs een numerieke prioriteitswaarde toe in het tekstvak **Prioriteit**.

Wanneer een brongroep meerdere brongroepen heeft, kunt u zo een prioriteit instellen, te beginnen bij het laagste nummer.

- c Klik op **Opslaan** om de brongroep toe te voegen aan de reservering.

4 Klik op **Nieuw** in de tabel met opslagaccounts.

- a Voer de naam van het gewenste opslagaccount uit de Azure-instantie in het tekstvak **Naam** in.

Opmerking Het vak **Naam** moet worden ingevuld.

- b Wijs een numerieke prioriteitswaarde toe in het tekstvak **Prioriteit**.
- c Klik op **Opslaan** om de opslagaccount toe te voegen aan de reservering.

Wanneer een reservering meerdere opslagaccounts heeft, kunt u zo een prioriteit instellen, te beginnen bij het laagste nummer.

5 Klik op **OK** om door te gaan naar het volgende tabblad.

Azure-eigenschappen configureren

U kunt aangepaste eigenschappen toevoegen aan een Azure-reservering om opties te ondersteunen zoals VPN-tunneling ten behoeve van communicatie tussen meerdere netwerken. Deze functionaliteit maakt ook het toevoegen van softwareonderdelen aan blueprints mogelijk.

U moet aangepaste eigenschappen maken die de juiste URL's definiëren om VPN-tunneling in uw netwerk te ondersteunen. Ook moet u eigenschappen maken die het pad definiëren naar de configuratiescripts voor Azure-tunneling die u eerder hebt gedownload.

Gebruik het privé-IP-adres van uw fysieke Azure-tunnelmachine en poort 1443, die u hebt toegewezen voor *vRealize_automation_appliance_fqdn* toen u de SSH-tunnel hebt aangeroepen.

In de volgende tabel staan de namen en waarden voor de eigenschappen die zijn vereist om VPN-tunneling te ondersteunen.

Naam	Waarde
Azure.Windows.ScriptPath	Geeft het pad naar het gedownloade script aan waarmee tunneling wordt geconfigureerd voor Windows-systemen. Werk het pad bij voor uw implementatie.
Azure.Linux.ScriptPath	Geeft het pad naar het gedownloade script aan waarmee tunneling wordt geconfigureerd voor Linux-systemen. Werk het pad bij voor uw implementatie.
agent.download.url	Geeft de URL aan voor de VPN-agent in uw implementatie. De URL-indeling is <code>https://Privé_IP:1443/software-service//bronnen/noble-agent.jar</code>
software.agent.service.url	Voer de URL in voor de VPN-softwareagentservice voor uw implementatie. De URL-indeling is <code>https://Privé_IP:1443/software-service/api</code>
software.ebs.url	Voer de URL in van de event-broker-service voor uw implementatie. De URL-indeling is <code>https://Privé_IP:1443/event-broker-service/api</code>

Voorwaarden

- Download de door VMware geleverde Azure-scripts op de pagina **Installatieprogramma's voor gast- en softwareagenten** op uw vRealize Automation-toepassing

Met deze scripts installeert u Azure-extensies die vereist zijn om VPN-tunneling te ondersteunen. Er zijn twee scripts: `script.ps1` en `script.sh`. Het `.ps1`-bestand is voor Windows-systemen en het `.sh`-bestand voor Linux-systemen.

- a Voer `https://vrealize-automation-appliance-fqdn/software` uit om de VMware vRealize Automation-toepassingspagina te openen.
- b Klik op de koppeling voor **gast- en softwareagenten** onder het kopje vRealize Automation-onderdelen (IaaS, gast- en softwareagenten, hulpprogramma's) installeren.
- c Download de Azure-scriptbestanden onder het kopje Azure-machines. Sla de scriptbestanden op een geschikte locatie op. U moet naar deze locatie verwijzen wanneer u de aangepaste eigenschappen van Azure-reserveringen configureert.

Procedure

- 1 Klik op het tabblad **Eigenschappen**.
- 2 Klik op **Nieuw**.
- 3 Voer de juiste naam en waarde voor de aangepaste eigenschap in het dialoogvenster Eigenschappen in.
- 4 Klik bij het maken van elke eigenschap op **OK** in het dialoogvenster om de eigenschap toe te voegen.
- 5 Nadat u alle vereiste eigenschappen hebt toegevoegd, klikt u op **OK** om de instellingen op te slaan.

Wat nu te doen

Nadat u de aangepaste eigenschappen hebt gemaakt om VPN-tunneling te ondersteunen, kunt u softwareonderdelen maken voor uw Azure-blueprints. Raadpleeg *vRealize Automation configureren* voor meer informatie.

Wanneer u een softwareonderdeel voor Azure instelt, selecteert u **Virtuele Azure-machine** in de vervolgkeuzelijst Container op de pagina Nieuwe software.

Netwerkgegevens configureren voor een Azure-reservering

U kunt in een Azure-reservering gegevens configureren voor het virtuele netwerk en de load balancer van een virtual machine.

U kunt deze pagina ook deels of volledig leeg laten en de gegevens over het virtuele netwerk en de load balancer configureren tijdens het inrichten van een virtual machine.

Als u een netwerkprofiel opgeeft zonder een subnet te definiëren, wordt de naam van het eerste netwerkbereik van het opgegeven netwerkprofiel gebruikt als subnetnaam. Als er een netwerkprofiel is ingesteld, kunt u het tekstvak vNet desgewenst leeg laten. In dat geval wordt de naam van het eerste netwerkbereik in het opgegeven netwerkprofiel gebruikt als subnetnaam en wordt de vNet-naam omgezet naar het eerste Azure vNet dat een passend subnet bevat.

Voorwaarden

Haal de bijbehorende gegevens over het virtuele netwerk en de load balancer voor uw Azure-instantie indien nodig op.

Procedure

- 1 Klik op **Nieuw** in de netwerktabel om het gewenste virtuele Azure-netwerk voor uw virtual machine te configureren.
 - a Plak de bijbehorende vNet-naam uit de Azure-instantie in het tekstvak **vNet**.
 - b Plak de bijbehorende subnetnaam uit de Azure-instantie in het tekstvak **Subnet**.
De subnetspecificatie is optioneel. Als u dit vaak leeg laat, wordt standaard het subnet van het opgegeven vNet gebruikt.
 - c Typ of plak de bijbehorende naam in het tekstvak **Netwerkprofiel**. U kunt het netwerkprofiel in de blueprint gebruiken om een netwerkinterfacekaart te koppelen aan een netwerk.
De specificatie voor het netwerkprofiel is optioneel. Gebruik deze specificatie wanneer het netwerkprofiel van de blueprint is gedefinieerd in vRealize Automation en u geen koppeling met Azure-netwerkconstructies gebruikt.
 - d Wijs indien nodig een numerieke prioriteitswaarde toe in het tekstvak **Prioriteit**.
Wanneer een virtueel netwerk meerdere reserveringen heeft, kunt u zo een prioriteit instellen, te beginnen bij het laagste nummer.
 - e Klik op **Opslaan** om de brongroep toe te voegen aan de reservering.
- 2 Klik op **Nieuw** in de tabel met load balancers als u meerdere machines implementeert en een load balancer gebruikt.
 - a Plak de naam van de bijbehorende load balancer uit de Azure-instantie in het tekstvak **Naam**.
 - b Plak de bijbehorende naam uit de Azure-instantie in het tekstvak **Backend-adresgroep**.
 - c Wijs indien nodig een numerieke prioriteitswaarde toe in het tekstvak **Prioriteit**.
Wanneer een virtueel netwerk meerdere load balancers heeft, kunt u zo een prioriteit instellen, te beginnen bij het laagste nummer.
 - d Klik op **Opslaan** om de load balancer toe te voegen aan de reservering.

3 Klik op **Nieuw** in de tabel met beveiligingsgroepen als u meerdere machines implementeert die via een firewall communiceren.

a Plak de naam van de beveiligingsgroep uit de Azure-instantie in het tekstvak **Naam**.

b Wijs indien nodig een numerieke prioriteitswaarde toe in het tekstvak **Prioriteit**.

Wanneer een virtueel netwerk meerdere beveiligingsgroepen heeft, kunt u zo een prioriteit instellen, te beginnen bij het laagste nummer.

c Klik op **Opslaan** om de beveiligingsgroep toe te voegen aan de reservering.

4 Klik op **OK**.

Scenario: een Amazon-reservering maken voor een omgeving om concepten te testen
Omdat u een SSH-tunnel hebt gemaakt om netwerk-naar-Amazon VPC-connectiviteit voor uw 'proof of concept'-omgeving tijdelijk tot stand te brengen, moet u aangepaste eigenschappen aan uw Amazon-reserveringen toevoegen om ervoor te zorgen dat de communicatie van de Software-bootstrapagent en de gastagent via de tunnel loopt.

Netwerk-naar-Amazon VPC-connectiviteit is alleen vereist als u de gastagent wilt gebruiken om ingerichte machines aan te passen, of als u Software-onderdelen in uw blueprints wilt opnemen. Voor een productieomgeving moet u deze connectiviteit officieel configureren via Amazon Web Services, maar omdat u in een 'proof of concept'-omgeving werkt, hebt u in plaats daarvan een tijdelijke SSH-tunnel geconfigureerd.

Met behulp van uw materiaalbeheerderprivileges maakt u een reservering om uw Amazon Web Services-bronnen toe te wijzen en neemt u verschillende aangepaste eigenschappen op om SSH-tunneling te ondersteunen. U configureert ook de reservering op dezelfde regio en VPC als uw tunnelmachine.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Configureer een SSH-tunnel om netwerk-naar-Amazon VPC-connectiviteit tot stand te brengen. Noteer het subnet, de beveiligingsgroep en het privé IP-adres van uw Amazon Web Services-tunnelmachine. Zie [Netwerk-naar-Amazon VPC-connectiviteit configureren voor een 'proof of concept'-omgeving](#).
- Maak een bedrijfsgroep voor leden van uw IT-organisatie die blueprints moeten maken in uw 'proof of concept'-omgeving. Zie [Een bedrijfsgroep maken](#).
- Controleer of de tenantbeheerder ten minste één bedrijfsgroep heeft gemaakt.

Procedure

1 [Scenario: Amazon Web Services-reserveringsinformatie opgeven voor een 'proof of concept'-omgeving](#)

U wilt bronnen reserveren voor uw team van blueprintarchitecten zodat deze de functionaliteit in uw 'proof of concept'-omgeving kunnen testen. Daarom configureert u deze reservering om bronnen toe te wijzen aan uw bedrijfsgroep met architecten.

2 Scenario: Amazon Web Services-netwerkinstellingen opgeven voor een 'proof of concept'-omgeving

U configureert de reservering om dezelfde regio- en netwerkinstellingen te gebruiken die uw tunnemachine gebruikt, en u beperkt het aantal machines dat kan worden ingeschakeld voor deze reservering om het brongebruik te beheren.

3 Scenario: aangepaste eigenschappen opgeven om agentcommunicatie via uw tunnel uit te voeren

Als u netwerk-naar-Amazon VPC-connectiviteit hebt geconfigureerd, hebt u port mapping geconfigureerd zodat uw Amazon Web Services-tunnemachine toegang krijgt tot vRealize Automation-bronnen.

Scenario: Amazon Web Services-reserveringsinformatie opgeven voor een 'proof of concept'-omgeving

U wilt bronnen reserveren voor uw team van blueprintarchitecten zodat deze de functionaliteit in uw 'proof of concept'-omgeving kunnen testen. Daarom configureert u deze reservering om bronnen toe te wijzen aan uw bedrijfsgroep met architecten.

Opmerking Nadat u een reservering hebt gemaakt, kunt u de koppelingen met bedrijfsgroepen of computerbronnen niet meer wijzigen.

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Reserveringen**.
- 2 Klik op het pictogram **Nieuw** (+) en selecteer het type reservering dat u wilt maken.
Selecteer **Amazon**.
- 3 Voer **Amazon Tunnel POC** in het tekstvak **Naam** in.
- 4 Selecteer in het vervolgkeuzemenu **Bedrijfsgroep** de bedrijfsgroep die u voor uw blueprintarchitecten hebt gemaakt.
- 5 Voer **1** in het tekstvak **Prioriteit** in om deze reservering de hoogste prioriteit te geven.

Resultaten

U hebt de bedrijfsgroep en de prioriteit voor de reservering geconfigureerd, maar u moet nog bronnen toewijzen en de aangepaste eigenschappen voor de SSH-tunnel configureren.

Scenario: Amazon Web Services-netwerkinstellingen opgeven voor een 'proof of concept'-omgeving

U configureert de reservering om dezelfde regio- en netwerkinstellingen te gebruiken die uw tunnemachine gebruikt, en u beperkt het aantal machines dat kan worden ingeschakeld voor deze reservering om het brongebruik te beheren.

Procedure

- 1 Klik op het tabblad **Bronnen**.

- 2 Selecteer een computerbron waarop u machines wilt inrichten in het vervolgkeuzemenu **Computerbron**.

Selecteer de Amazon Web Services-regio waar uw tunnelmachine zich bevindt.

- 3 (Optioneel) Geef een getal op in het tekstvak **Machinequotum** om het maximum aantal machines in te stellen dat kan worden ingericht voor deze reservering.

Alleen machines die zijn ingeschakeld worden meegeteld in het quotum. Laat het tekstvak leeg om geen beperkingen te stellen aan de reservering.

- 4 Selecteer **Sleutelpaar opgeven** in het vervolgkeuzemenu **Sleutelpaar**.

Omdat dit een 'proof of concept'-omgeving is, kunt u één sleutelpaar delen voor alle machines die zijn ingericht met behulp van deze reservering.

- 5 Selecteer het sleutelpaar dat u wilt delen met uw architect-gebruikers in het vervolgkeuzemenu **Sleutelpaar**.

- 6 Schakel het selectievakje **Toewijzen aan een subnet in een VPC** in.

- 7 Selecteer hetzelfde subnet en dezelfde beveiligingsgroepen die door uw tunnelmachine worden gebruikt.

Resultaten

U hebt de reservering geconfigureerd om dezelfde regio- en netwerkinstellingen te gebruiken als uw tunnelmachine, maar u moet nog de aangepaste eigenschappen toevoegen om ervoor te zorgen dat de communicatie van de Software-bootstrapagent en de gastagent via de tunnel loopt.

Scenario: aangepaste eigenschappen opgeven om agentcommunicatie via uw tunnel uit te voeren

Als u netwerk-naar-Amazon VPC-connectiviteit hebt geconfigureerd, hebt u port mapping geconfigureerd zodat uw Amazon Web Services-tunnelmachine toegang krijgt tot vRealize Automation-bronnen.

U moet aangepaste tunneleigenschappen toevoegen op de reservering om de agenten te configureren die toegang krijgen tot deze poorten.

Opmerking Als u een PAT- of NAT-systeemnetwerk gebruikt tussen het netwerk van uw organisatie en het vRealize Automation-netwerk, kunt u deze eigenschappen gebruiken om toegang te krijgen tot uw privé IP-adres en poort.

Procedure

- 1 Klik op het tabblad **Eigenschappen**.
- 2 Klik op **Nieuw**.

3 Configureer de aangepaste eigenschappen van de tunnel.

Gebruik het privé IP-adres van uw Amazon Web Services-tunnelmachine en poort 1443, dat u hebt toegewezen voor *vRealize_automation_appliance_fqdn* toen u de SSH-tunnel hebt aangeroepen.

Optie	Waarde
<code>software.ebs.url</code>	<code>https://Private_IP:1443/event-broker-service/api</code>
<code>software.agent.service.url</code>	<code>https://Private_IP:1443/software-service/api</code>
<code>agent.download.url</code>	<code>https://Private_IP:1443/software-service/resources/nobel-agent.jar</code>

4 Klik op **Opslaan**.

Resultaten

U hebt een reservering gemaakt om Amazon Web Services-bronnen toe te wijzen aan uw architectenbedrijfsgroep. U hebt de reservering geconfigureerd om de gastagent en de Software-bootstrapagent te ondersteunen. Uw architecten kunnen blueprints maken die de gastagent gebruiken om geïmplementeerde machines aan te passen of Software-onderdelen op te nemen.

Virtuele reserveringen maken

Een virtuele reservering voorziet in toegang tot de inrichtingsservices van een virtual machine-implementatie voor een bepaalde vRealize Automation-bedrijfsgroep. Beschikbare typen virtuele reservering zijn onder meer vSphere, Hyper-V, KVM, SCVMM en XenServer.

Een reservering is een deel van de geheugen-, CPU-, netwerk- en opslagbronnen van een computerbron dat aan een specifieke vRealize Automation-bedrijfsgroep wordt toegewezen.

Een bedrijfsgroep kan meerdere reserveringen op één endpoint hebben of reserveringen op meerdere endpoints.

Om virtual machines in te richten, moet een bedrijfsgroep minimaal één reservering op een virtuele computerbron hebben. Elke reservering is slechts voor één bedrijfsgroep, maar een bedrijfsgroep kan meerdere reserveringen op één computerbron of meerdere reserveringen op verschillende computerbrontypen hebben.

Naast het definiëren van het deel van materiaalbronnen dat aan de bedrijfsgroep is toegewezen, kan een reservering beleidsregels, prioriteiten en quotas definiëren die de plaatsing van machines bepaalt.

Voor een goede inrichting moet de reservering voldoende beschikbare opslag hebben. De beschikbare opslag van de reservering is afhankelijk van:

- Hoeveel opslag in de datastore en/of het cluster beschikbaar is.
- Hoeveel van die opslag is gereserveerd voor die datastore en/of dat cluster.
- Hoeveel van die opslag al is toegewezen in vRealize Automation

Zelfs als bijvoorbeeld vCenter Server opslag beschikbaar heeft voor de datastore en/of het cluster, zal de inrichting mislukken met een fout van het type 'Geen reservering beschikbaar om toe te wijzen...' als er te weinig opslag is gereserveerd. De toegewezen opslag op een reservering is afhankelijk van het aantal VM's (ongeacht hun status) op die specifieke reservering. Zie het VMware Knowledge Base-artikel *Machine XXX: Geen reservering beschikbaar om binnen de groep XXX toe te wijzen. In totaal werd XX GB aan opslag aangevraagd (2151030)* op <http://kb.vmware.com/kb/2151030> voor meer informatie.

Informatie over de selectielogica voor reserveringen

Wanneer een lid van een bedrijfsgroep een inrichtingsaanvraag maakt voor een virtual machine, wordt door vRealize Automation een machine geselecteerd uit de reserveringen die beschikbaar zijn voor die bedrijfsgroep.

De reservering waarvoor een machine wordt ingericht, moet aan de volgende criteria voldoen:

- De reservering moet gebruikmaken van hetzelfde type platform als de blueprint waaruit de machine is aangevraagd.

Een algemene virtuele blueprint kan worden ingericht voor elk type virtuele reservering.

- De reservering moet geactiveerd zijn.
- De computerbron moet toegankelijk zijn en zich niet in de onderhoudsmodus bevinden.
- De reservering moet resterende capaciteit in het machinequotum hebben of over een onbeperkt machinequotum beschikken.

Het toegewezen machinequotum omvat uitsluitend machines die zijn ingeschakeld. Als een reservering bijvoorbeeld beschikt over een quotum van 50 en er 40 machines zijn ingericht waarvan slechts 20 zijn ingeschakeld, is 40 procent van het quotum van de reservering toegewezen en niet 80 procent.

- De reservering moet over voldoende niet-toegewezen geheugen en opslagbronnen beschikken om de machine in te richten.

Wanneer het machinequotum, het geheugen of de opslag van een virtuele reservering volledig is toegewezen, kunnen er verder geen virtual machines meer worden ingericht voor deze reservering. Er kunnen meer computerbronnen voor virtualisatie worden gereserveerd dan fysiek aanwezig, maar wanneer de fysieke capaciteit van een computerbron voor 100% is toegewezen, kunnen er geen machines meer worden ingericht voor reserveringen met die computerbron, totdat de bronnen weer terug worden gewonnen.

- Als de blueprint specifieke netwerkinstellingen bevat, moet de reservering dezelfde netwerken gebruiken.

Als voor de blueprint of de reservering een netwerkprofiel voor toewijzing van statische IP-adressen is opgegeven, moet een IP-adres beschikbaar zijn om toe te wijzen aan de nieuwe machine.

- Als in de blueprint of de aanvraag een locatie is opgegeven, moet de computerbron zijn gekoppeld aan die locatie.

Als de aangepaste eigenschap `Vrm.DataCenter.Policy` de waarde **Exact** heeft en als er geen reservering voor een computerbron is gekoppeld aan die locatie terwijl aan alle andere criteria is voldaan, mislukt de provisioning.

Als `Vrm.DataCenter.Policy` de waarde **NotExact** heeft en als er geen reservering voor een computerbron is gekoppeld aan die locatie terwijl aan alle andere criteria is voldaan, kan de provisioning doorgaan voor een andere reservering, ongeacht de locatie. Deze optie is standaard.

- Als in de blueprint of de aanvraag de aangepaste eigenschap `VirtualMachine.Host.TpmEnabled` is opgegeven, moet vertrouwde hardware worden geïnstalleerd op de computerbron voor de reservering.
- Als in de blueprint een reserveringsbeleid is opgegeven, moet de reservering onderdeel uitmaken van dat reserveringsbeleid.

Een reserveringsbeleid is een manier om te garanderen dat de geselecteerde reservering voldoet aan de extra vereisten voor de inrichting van machines op basis van een specifieke blueprint. U kunt bijvoorbeeld een reserveringsbeleid gebruiken om de inrichting te beperken tot computerbronnen met een specifieke sjabloon voor klonen.

Als er geen reservering beschikbaar is die aan alle selectiecriteria voldoet, mislukt de inrichting.

Als er meerdere reserveringen voldoen aan alle criteria, wordt op de volgende wijze bepaald welke reservering wordt gebruikt om een aangevraagde machine in te richten:

- Een reservering met een lagere prioriteit wordt geselecteerd voor een reservering met een hogere prioriteit.
- Als er meerdere reserveringen dezelfde prioriteit hebben, wordt de reservering geselecteerd waarvoor het laagste percentage machinequotum is toegewezen.
- Als er meerdere reserveringen zijn met dezelfde prioriteit en hetzelfde quotumgebruik, worden machines evenredig gedistribueerd onder de reserveringen.

Opmerking De round-robin-selectie van netwerkprofielen wordt niet ondersteund, round-robin-selectie van netwerken (indien aanwezig) wordt ondersteund, en kan worden gekoppeld aan verschillende netwerkprofielen.

Als er meerdere opslagpaden beschikbaar zijn voor een reservering met voldoende capaciteit om de machinevolumes in te richten, worden de opslagpaden geselecteerd op basis van de volgende logica.

- Als in de blueprint of aanvraag een opslagreserveringsbeleid is opgegeven, moet het opslagpad onderdeel uitmaken van dat opslagreserveringsbeleid.

Als de aangepaste eigenschap `VirtualMachine.DiskN.StorageReservationPolicyMode` de waarde **NotExact** heeft en als er geen opslagpad is met voldoende capaciteit binnen het opslagreserveringsbeleid, kan de provisioning doorgaan met een opslagpad dat buiten het opgegeven opslagreserveringsbeleid ligt. De standaardwaarde van `VirtualMachine.DiskN.StorageReservationPolicyMode` is **Exact**.

- Een opslagpad met een lagere prioriteit wordt geselecteerd voor een opslagpad met een hogere prioriteit.
- Als er meerdere opslagpaden zijn met dezelfde prioriteit, worden de machines evenredig gedistribueerd over de opslagpaden.

Een vSphere-reservering voor NSX Network en beveiliging in vRealize Automation maken
U kunt een vSphere-reservering maken die werkt met uw gekoppelde NSX-T- of NSX for vSphere-endpoint in vRealize Automation.

Algemene overwegingen voor NSX

Als u NSX hebt geconfigureerd, kunt u bij het maken of bewerken van een blueprint NSX-instellingen opgeven voor de transportzone, het netwerkreserveringsbeleid en de app-isolatie. Deze instellingen zijn beschikbaar op het tabblad **NSX-instellingen** van de pagina's **Blueprint** en **Blueprinteigenschappen**.

De instellingen voor netwerk- en beveiligingsonderdelen die u aan de blueprint toevoegt, worden afgeleid van uw configuratie van NSX for vSphere en NSX-T. Raadpleeg de *Administration Guide* in de [NSX for vSphere-productdocumentatie](#) of [NSX-T-productdocumentatie](#), afhankelijk van welke toepassing u gebruikt, voor informatie over het configureren van NSX.

Voor een succesvolle inrichting moet de transportzone van de reservering overeenkomen met die van een machineblueprint waarmee machinenetwerken worden gedefinieerd. Evenzo moet bij de inrichting van de geleide gateway van een machine de ingestelde transportzone van de reservering overeenkomen met die van de blueprint.

Zie [Informatie over de NSX-T-implementatietopologieën voor netwerken, beveiliging en load balancer-configuraties](#) voor meer informatie over NSX-T-specifieke overwegingen met betrekking tot topologie.

Overwegingen voor NSX for vSphere

Als vRealize Automation machines met NAT- of geleide netwerken inricht, wordt een geleide gateway ingericht als netwerkrouter. De Edge- of geleide gateway is een beheermachine die computerbronnen verbruikt. Deze beheert ook de netwerkcommunicatie voor de ingerichte machineonderdelen. De reservering die wordt gebruikt om de Edge-gateway of geleide gateway in te richten, bepaalt het externe netwerk dat wordt gebruikt voor NAT- en geleide netwerkprofielen. Deze bepaalt ook de Edge-gateway of geleide gateway van de reservering die wordt gebruikt om geleide netwerken te configureren. De geleide gateway van de reservering koppelt geleide netwerken aan vermeldingen in de routingstabel.

Wanneer u een Edge of geleide gateway en een netwerkprofiel selecteert voor een reservering voor geleide netwerken, selecteert u het netwerkpad dat moet worden gebruikt bij het koppelen van geleide netwerken. Wijs het netwerkpad toe aan het externe netwerkprofiel dat wordt gebruikt om het profiel voor het geleide netwerk te configureren. De lijst met netwerkprofielen die kunnen worden toegewezen aan een netwerkpad, wordt gefilterd, zodat deze overeenkomt met het subnet van het netwerkpad, dat is gebaseerd op het subnetmasker en het primaire IP-adres, dat is geselecteerd voor de netwerkinterface.

U kunt een reserveringsbeleid voor Edge-gateways of geleide gateways opgeven om te identificeren welke reserveringen moeten worden gebruikt bij het inrichten van de machines met de Edge-gateway of geleide gateway. Standaard maakt vRealize Automation gebruik van dezelfde reserveringen voor de geleide gateway en de machineonderdelen.

Als u een Edge-gateway of een geleide gateway wilt gebruiken in vRealize Automation-reserveringen, kunt u de geleide gateway extern configureren in de NSX-omgeving en vervolgens inventarisgegevens verzamelen. Voor NSX moet u over een werkende NSX Edge-instantie beschikken voordat u de standaardgateway kunt configureren voor een statische of dynamische routing via een gateway met Edge-services of een router voor logische distributie. Zie *NSX Administration Guide*.

U selecteert een of meer beveiligingsgroepen in de reservering om een baseline-beveiligingsbeleid af te dwingen voor alle onderdeelmachines die met die reservering zijn ingericht in vRealize Automation. Elke ingerichte machine wordt toegevoegd aan de opgegeven beveiligingsgroepen.

Overwegingen voor NSX-T

Wanneer u een reservering maakt voor een vSphere-endpoint dat is gekoppeld aan een NSX-T-endpoint, moet u de volgende informatie voor de reservering configureren:

- Definieer een transportzone voor de blueprint.
- Selecteer een logische router van tier 0 voor de ingerichte implementatie waarmee verbinding moet worden gemaakt.
- Wijs een extern netwerkprofiel toe aan de logische router van tier 0.

NSX-T NS-groepen worden niet ondersteund in reserveringen.

Zie [Informatie over de NSX-T-implementatietopologieën voor netwerken, beveiliging en load balancer-configuraties](#) voor meer informatie over NSX-T-specifieke overwegingen met betrekking tot implementatie en topologie.

Een reservering maken voor Hyper-V, KVM, SCVMM, vSphere of XenServer

U moet bronnen aan machines toewijzen door een reservering te maken voordat leden van een bedrijfsgroep machine-inrichting kunnen aanvragen.

Elke bedrijfsgroep moet minstens één reservering hebben zodat de leden van die groep machines van dat type kunnen inrichten. Een bedrijfsgroep met een vSphere-reservering, maar geen KVM (RHEV)-reservering, kan bijvoorbeeld geen KVM (RHEV)-virtual machine aanvragen. In dit voorbeeld moet specifiek een reservering voor KVM (RHEV)-bronnen worden toegewezen aan de bedrijfsgroep.

Procedure

1 Virtuele reserveringsinformatie opgeven

Elke reservering is geconfigureerd voor een specifieke bedrijfsgroep om gebruikers toegang te verlenen om machines aan te vragen op een opgegeven computerbron.

2 Bron- en netwerkinstellingen opgeven voor een virtuele reservering

Geef bron- en netwerkinstellingen op voor het inrichten van machines vanaf deze vRealize Automation-reservering.

3 Aangepaste eigenschappen en waarschuwingen voor virtuele reserveringen opgeven

U kunt aangepaste eigenschappen koppelen aan een vRealize Automation-reservering. U kunt ook waarschuwingen configureren om e-mailmeldingen te verzenden wanneer er weinig reserveringsbronnen zijn.

Virtuele reserveringsinformatie opgeven

Elke reservering is geconfigureerd voor een specifieke bedrijfsgroep om gebruikers toegang te verlenen om machines aan te vragen op een opgegeven computerbron.

U kunt bepalen hoe reserveringen worden weergegeven, tijdens het toevoegen, bewerken of verwijderen, door gebruik te maken van de optie **Filteren op categorie** op de pagina Reserveringen. Houd er rekening mee dat reserveringen van testagenten niet worden weergegeven in de lijst met reserveringen wanneer u filtert op categorie.

Opmerking Nadat u een reservering hebt gemaakt, kunt u de koppelingen met bedrijfsgroepen of computerbronnen niet meer wijzigen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Controleer of de tenantbeheerder ten minste één bedrijfsgroep heeft gemaakt.
- Controleer of er een computerbron bestaat.
- Configureer de netwerkinstellingen.
- (Optioneel) Configureer de informatie over een netwerkprofiel.

Procedure

1 Selecteer **Infrastructuur > Reserveringen > Reserveringen**.

2 Klik op het pictogram **Nieuw** (+) en selecteer het type reservering dat u wilt maken.

De beschikbare virtuele reserveringstypes zijn Hyper-V, KVM, SCVMM, vSphere en XenServer.

Selecteer bijvoorbeeld **vSphere**.

3 Geef een naam op in het tekstvak **Naam**.

4 Selecteer een tenant in het vervolgkeuzemenu **Tenant**.

5 Selecteer een bedrijfsgroep in het vervolgkeuzemenu **Bedrijfsgroep**.

Alleen gebruikers in deze bedrijfsgroep kunnen machines inrichten met behulp van deze reservering.

6 (Optioneel) Selecteer een reserveringsbeleid in het vervolgkeuzemenu **Reserveringsbeleid**.

Voor deze optie is vereist dat er minimaal één reserveringsbeleid bestaat. U kunt de reservering later bewerken om een reserveringsbeleid op te geven.

U kunt een reserveringsbeleid gebruiken om de inrichting te beperken tot bepaalde reserveringen.

7 Geef een getal op in het tekstvak **Prioriteit** om de prioriteit voor de reservering in te stellen.

De prioriteit wordt gebruikt wanneer er meer dan een reservering bestaat voor de bedrijfsgroep. Een reservering met de prioriteit 1 wordt eerder ingericht dan een reservering met de prioriteit 2.

8 (Optioneel) Schakel het selectievakje **Deze reservering inschakelen** uit als u niet wilt dat deze reservering actief is.**Resultaten**

Verlaat deze pagina niet. Uw reservering is niet compleet.

Bron- en netwerkinstellingen opgeven voor een virtuele reservering

Geef bron- en netwerkinstellingen op voor het inrichten van machines vanaf deze vRealize Automation-reservering.

U kunt een FlexClone-datastore selecteren in de reservering als u over een vSphere-omgeving en over opslagapparaten beschikt die gebruikmaken van Net App FlexClone-technologie. SDRS wordt niet ondersteund op FlexClone-opslagapparaten.

Voor een goede inrichting moet de reservering voldoende beschikbare opslag hebben. De beschikbare opslag van de reservering is afhankelijk van:

- Hoeveel opslag in de datastore en/of het cluster beschikbaar is.
- Hoeveel van die opslag is gereserveerd voor die datastore en/of dat cluster.
- Hoeveel van die opslag al is toegewezen in vRealize Automation

Zelfs als bijvoorbeeld vCenter Server opslag beschikbaar heeft voor de datastore en/of het cluster, zal de inrichting mislukken met een fout van het type 'Geen reservering beschikbaar om toe te wijzen...' als er te weinig opslag is gereserveerd. De toegewezen opslag op een reservering is afhankelijk van het aantal VM's (ongeacht hun status) op die specifieke reservering. Zie het VMware Knowledge Base-artikel *Machine XXX: Geen reservering beschikbaar om binnen de groep XXX toe te wijzen. In totaal werd XX GB aan opslag aangevraagd (2151030)* op <http://kb.vmware.com/kb/2151030> voor meer informatie.

Als u een vSphere (vCenter)-reservering maakt of bewerkt voor gebruik met NSX for vSphere of NSX-T, kunt u de informatie over de transportzone en logische router laag 1 opgeven met behulp van de geavanceerde opties voor het geselecteerde netwerk.

Voorwaarden

[Virtuele reserveringsinformatie opgeven.](#)

Procedure

- 1 Klik op het tabblad **Bronnen**.
- 2 Selecteer een computerbron waarop u machines wilt inrichten in het vervolgkeuzemenu **Computerbron**.

Alleen sjablonen die zich op het geselecteerde cluster bevinden, kunnen worden gekloond met deze reservering.

Tijdens het inrichten worden machines in een host geplaatst die is verbonden met de lokale opslag. Als de reservering gebruikmaakt van de lokale opslag, worden alle machines die door de reservering zijn ingericht, in de host geplaatst die deze lokale opslag bevat. Als u echter de aangepaste `VirtualMachine.Admin.ForceHost`-eigenschap gebruikt, die een machine forceert om te worden ingericht op een andere host, mislukt de inrichting. De inrichting mislukt ook als de sjabloon aan de hand waarvan de machine is gekloond zich op de lokale opslag bevindt, en is gekoppeld aan een machine in een ander cluster. In dit geval mislukt de inrichting omdat de sjabloon niet toegankelijk is.

- 3 (Optioneel) Geef een getal op in het tekstvak **Machinequotum** om het maximum aantal machines in te stellen dat kan worden ingericht voor deze reservering.

Alleen machines die zijn ingeschakeld worden meegeteld in het quotum. Laat het tekstvak leeg om geen beperkingen te stellen aan de reservering.

- 4 Geef de hoeveelheid geheugen (in GB) op die moet worden toegewezen aan deze reservering in de tabel Geheugen.

De waarde van het totale geheugen voor de reservering wordt bepaald aan de hand van de geselecteerde computerbron.

- 5 Geef de hoeveelheid geheugen (in GB) op die moet worden toegewezen aan deze reservering in de tabel Geheugen.

De waarde van het totale geheugen voor de reservering wordt bepaald aan de hand van de geselecteerde computerbron.

- 6 Selecteer één of meer opslagpaden in de lijst.

De beschikbare opties voor opslagpaden worden bepaald aan de hand van de geselecteerde computerbron.

Voor integraties die gebruikmaken van SDRS-opslag (Storage Distributed Resource Scheduler), kunt u een opslagcluster selecteren zodat SDRS automatisch de opslaglocatie en taakverdeling kan afhandelen van machines die worden ingericht vanuit deze reservering. De automatiseringsmodus voor SDRS moet worden ingesteld op Automatisch. Selecteer anders een datastore binnen het cluster om het gedrag van standalone datastores te leren kennen. SDRS wordt niet ondersteund op FlexClone-opslagapparaten.

U kunt afzonderlijke schijven in de cluster selecteren of een opslagcluster, maar niet beide. Als u een opslagcluster selecteert, handelt SDRS de opslaglocatie en taakverdeling af van machines die worden ingericht vanuit deze reservering.

- 7 Indien deze beschikbaar is voor de computerbron, selecteert u een bronpool in het vervolgkeuzemenu **Bronpool**.
- 8 Klik op het tabblad **Netwerk**.
- 9 Configureer een netwerkpad voor machines die worden ingericht met behulp van deze reservering.

- a (Optioneel) Als de optie beschikbaar is, selecteert u een opslagendpoint in het vervolgkeuzemenu **Endpoint**.

De optie FlexClone wordt weergegeven in de kolom endpoint als een NetApp ONTAP-endpoint bestaat en er een virtuele host is. Als er een NetApp ONTAP-endpoint is, wordt op de reserveringspagina het endpoint weergegeven dat is gekoppeld aan het opslagpad. Wanneer u een endpoint voor een opslagpad toevoegt, bijwerkt of verwijdt, wordt deze wijziging weergegeven in alle betreffende reserveringen.

Wanneer u een endpoint voor een opslagpad toevoegt, bijwerkt of verwijdt, wordt deze wijziging weergegeven in de reserveringspagina.

- b Selecteer een of meer **netwerkadapters** voor de machines die moeten worden ingericht voor deze reservering.
- c (Optioneel) Selecteer een beschikbaar **netwerkprofiel** voor elke geselecteerde netwerkadapter.
- d (Optioneel) Als de geavanceerde instellingen beschikbaar zijn, selecteert u een **transportzone** en een of meer **laag 0 logische routers** die moeten worden gebruikt bij het implementeren van een blueprint die load balancers bevat.

Met een transportzone wordt aangegeven welke clusters de netwerkadapters omvatten. Als u een transportzone opgeeft in een reservering en in een blueprint, moeten de waarden voor de transportzone overeenkomen.

U kunt meer dan één netwerkadapter selecteren in een reservering, maar er wordt slechts één netwerk gebruikt bij de inrichting van een machine.

Resultaten

U kunt de reservering nu opslaan door te klikken op **Opslaan**. Of u kunt aangepaste eigenschappen toevoegen om nog nauwkeuriger te bepalen hoe reserveringsspecificaties worden weergegeven. U kunt ook waarschuwingse-mails configureren, zodat u meldingen ontvangt wanneer de hoeveelheid bronnen voor de reservering beneden een bepaald peil daalt. Aangepaste eigenschappen en waarschuwingen voor virtuele reserveringen opgeven

U kunt aangepaste eigenschappen koppelen aan een vRealize Automation-reservering. U kunt ook waarschuwingen configureren om e-mailmeldingen te verzenden wanneer er weinig reserveringsbronnen zijn.

Aangepaste eigenschappen en waarschuwingse-mails zijn optionele configuraties voor de reservering. Als u geen koppelingen wilt maken voor de aangepaste eigenschappen of waarschuwingen wilt instellen, klikt u op **Opslaan** om het maken van de reservering te beëindigen.

U kunt nu zoveel aangepaste eigenschappen toevoegen als er nodig zijn.

Belangrijk Meldingen worden alleen verzonden als waarschuwingse-mails zijn geconfigureerd en meldingen zijn ingeschakeld.

Als het zo is geconfigureerd, kunnen waarschuwingen dagelijks worden gegenereerd, in plaats van bij het bereiken van de opgegeven drempelwaardes.

Voorwaarden

[Bron- en netwerkinstellingen opgeven voor een virtuele reservering.](#)

Procedure

- 1 Klik op het tabblad **Eigenschappen**.
- 2 Klik op **Nieuw**.
- 3 Geef een geldige naam op voor de aangepaste eigenschap.
- 4 Geef indien nodig een waarde op voor de eigenschap.
- 5 (Optioneel) Schakel het selectievakje **Gecodeerd** in om de waarde van de eigenschap te versleutelen.
- 6 (Optioneel) Schakel het selectievakje **Vragen aan gebruiker** in om ervoor te zorgen dat de gebruiker een waarde moet opgeven.
Deze optie kan niet worden overschreven tijdens het inrichten.
- 7 (Optioneel) Voeg extra aangepaste eigenschappen toe.
- 8 Klik op het tabblad **Waarschuwingen**.
- 9 Schakel het selectievakje **Waarschuwingen over capaciteit** in om de waarschuwingen te configureren die worden verzonden.
- 10 Gebruik de schuifregelaar om de drempelwaarde in te stellen voor de toewijzing van de beschikbare bronnen.
- 11 Voer in het tekstvak **Ontvangers** de AD-gebruikers- of groepsnamen (geen e-mailadressen) in om waarschuwingmeldingen te ontvangen.
Voer op elke regel een naam in. Druk op Enter om de verschillende vermeldingen te scheiden.
- 12 Selecteer **Waarschuwingen naar groepsbeheerder sturen** om groepsbeheerders toe te voegen aan de ontvangers van waarschuwingse-mails.
De e-mailwaarschuwingen worden verzonden naar de gebruikers in de lijst **E-mails van beheerder versturen aan** voor de bedrijfsgroep.
- 13 Geef een herinneringsfrequentie (dagen) op.
- 14 Klik op **Opslaan**.

Resultaten

De reservering wordt opgeslagen en weergegeven in de lijst Reserveringen.

Wat nu te doen

U kunt optioneel een reserveringsbeleid configureren of beginnen met de voorbereiding van de inrichting.

Gebruikers die het recht hebben om blueprints te maken, kunnen deze nu maken.

Een reservering bewerken om een netwerkprofiel toe te wijzen

U kunt een netwerkprofiel aan een reservering toewijzen, bijvoorbeeld om de toewijzing van statische IP-adressen in te schakelen voor machines die op die reservering zijn ingericht.

U kunt ook een netwerkprofiel aan een blueprint toewijzen met behulp van de aangepaste eigenschap `VirtualMachine.NetworkN.ProfileName` op het tabblad **Eigenschappen** van de pagina **Nieuwe blueprint** of **Blueprinteigenschappen**.

Als u een netwerkprofiel opgeeft in een reservering en een blueprint, krijgen de blueprintwaarden voorrang.

Opmerking Deze informatie is niet van toepassing op Amazon Web Services.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Maak een netwerkprofiel. Zie [Een netwerkprofiel maken in vRealize Automation](#).

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Reserveringen**.
- 2 Wijs een reservering aan en klik op **Bewerken**.
- 3 Klik op het tabblad **Netwerk**.
- 4 Wijs een netwerkprofiel toe aan een netwerkpad.
 - a Selecteer het netwerkpad waarop u statische IP-adressen wilt inschakelen.
De netwerkpadopties zijn afgeleid van de instellingen op het tabblad **Bronnen**.
 - b Selecteer een profiel in het vervolgkeuzemenu **Netwerkprofiel** om dit toe te wijzen aan het pad.
 - c (Optioneel) Herhaal deze stap om netwerkprofielen toe te wijzen aan aanvullende netwerkpaden op deze reservering.
- 5 Klik op **OK**.

Reserveringsbeleid

U kunt een reserveringsbeleid gebruiken om te beheren hoe reserveringsaanvragen worden verwerkt. Wanneer u machines inricht aan de hand van een blueprint, is de inrichting beperkt tot de bronnen die zijn opgegeven in het reserveringsbeleid.

Met reserveringsbeleid (optioneel) kunt u regelen hoe reserveringsaanvragen moeten worden verwerkt. U kunt een reserveringsbeleid toepassen op een blueprint om het aantal machines dat op basis van die blueprint wordt ingericht, te beperken tot een subset met beschikbare reserveringen.

U kunt een reserveringsbeleid gebruiken om bronnen in groepen voor verschillende serviceniveaus te verzamelen of om een bepaald brontype eenvoudig beschikbaar te maken voor een bepaald doel. Wanneer een gebruiker een machine aanvraagt, kan deze worden ingericht via elke reservering van het juiste type met voldoende capaciteit voor de machine. In de volgende scenario's ziet u een aantal voorbeelden van mogelijk gebruik van reserveringsbeleid:

- Om er zeker van te zijn dat ingerichte machines in reserveringen worden geplaatst met specifieke apparaten die NetApp FlexClone ondersteunen.
- De inrichting van cloudmachines beperken tot een specifieke regio die een machine-image bevat die vereist is voor een specifieke blueprint.
- Als een extra middel om Betalen-naar-gebruik te hanteren als toewijzingsmodel voor machinetypes die deze mogelijkheid ondersteunen.

U kunt meerdere reserveringen aan een reserveringsbeleid toevoegen, maar een reservering kan maar bij één beleid horen. U kunt een enkel reserveringsbeleid aan meer dan één blueprint toewijzen. Een blueprint kan maar één reserveringsbeleid hebben.

Opmerking Reserveringen die zijn gedefinieerd voor vCloud Air-endpoints en vCloud Director-endpoints bieden geen ondersteuning voor het gebruik van netwerkprofielen voor het inrichten van machines.

Opmerking Als u SDRS op uw platform hebt ingeschakeld, kunt u instellen dat de opslag via SDRS wordt verdeeld voor afzonderlijke virtual machineschijven, of dat alle opslag voor de virtual machine wordt verdeeld. Als u met SDRS-datastoreclusters werkt, kunnen er conflicten optreden als u reserveringsbeleid en opslagreserveringsbeleid gebruikt. Als bijvoorbeeld een afzonderlijke datastore of een datastore binnen een SDRS-cluster wordt geselecteerd bij een van de reserveringen in een beleid of opslagbeleid, kan de opslagruimte van uw virtual machine geblokkeerd raken in plaats van dat deze wordt aangestuurd door SDRS. Als u opnieuw inrichten aanvraagt voor een machine met een opslaglocatie op een SDRS-cluster, wordt de machine verwijderd als het SDRS-automatiseringsniveau is gedeactiveerd. Zie de aangepaste eigenschap `VirtualMachine.Admin.Datastore.Cluster.ResourceLeaseDurationSec` voor gerelateerde informatie over provisioning en SDRS.

Een reserveringsbeleid configureren

U kunt reserveringsbeleidsregels maken om bronnen in groepen voor verschillende serviceniveaus te verzamelen of om een bepaald brontype eenvoudig beschikbaar te maken

voor een bepaald doel. Nadat u het reserveringsbeleid hebt gemaakt, moet u dit vullen met reserveringen voordat tenantbeheerders en bedrijfsgroepbeheerders het beleid efficiënt kunnen gebruiken in een blueprint.

Een reserveringsbeleid kan verschillende typen reserveringen bevatten, maar alleen reserveringen die overeenkomen met het blueprinttype, zijn beschikbaar wanneer een reservering voor een bepaalde aanvraag wordt geselecteerd.

Procedure

1 Een reserveringsbeleid maken

U kunt reserveringsbeleidsregels maken om soortgelijke reserveringen te groeperen.

2 Een reserveringsbeleid toewijzen aan een reservering

U kunt een reserveringsbeleid toewijzen aan een reservering wanneer u de reservering maakt. U kunt ook een bestaande reservering bewerken om er een reserveringsbeleid aan toe te wijzen, of de toewijzing van het reserveringsbeleid wijzigen.

Een reserveringsbeleid maken

U kunt reserveringsbeleidsregels maken om soortgelijke reserveringen te groeperen.

Maak eerst het reserveringsbeleid en voeg vervolgens het beleid toe aan reserveringen om een auteur van blueprints de toestemming te geven het reserveringsbeleid in een blueprint te gebruiken.

Het beleid wordt gemaakt als een lege container.

U kunt bepalen hoe het reserveringsbeleid wordt weergegeven, tijdens het toevoegen, bewerken of verwijderen, door gebruik te maken van de optie **Filteren op type** op de pagina Reserveringsbeleid.

Voorwaarden

Meld u aan bij vRealize Automation als een **materiaalbeheerder**.

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Reserveringsbeleid**.
- 2 Klik op het pictogram **Nieuw (+)**.
- 3 Geef een naam op in het tekstvak **Naam**.
- 4 Selecteer **Reserveringsbeleid** in het vervolgkeuzemenu **Type**.
- 5 Geef een beschrijving op in het tekstvak **Beschrijving**.
- 6 Klik op **OK**.

Een reserveringsbeleid toewijzen aan een reservering

U kunt een reserveringsbeleid toewijzen aan een reservering wanneer u de reservering maakt. U kunt ook een bestaande reservering bewerken om er een reserveringsbeleid aan toe te wijzen, of de toewijzing van het reserveringsbeleid wijzigen.

Voorwaarden

[Een reserveringsbeleid maken.](#)

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Reserveringen**.
- 2 Wijs een reservering aan en klik op **Bewerken**.
- 3 Selecteer een reserveringsbeleid in het vervolgkeuzemenu **Reserveringsbeleid**.
- 4 Klik op **Opslaan**.

Opslagreserveringsbeleid

U kunt opslagreserveringsbeleid maken om blueprintarchitecten in staat te stellen volumes van virtual machines toe te wijzen aan verschillende datastores op platformen van het type vSphere, KVM (RHEV) en SCVMM of aan verschillende opslagprofielen voor andere bronnen, zoals vCloud Air- of vCloud Director-bronnen.

Als u de volumes van een virtual machine aan verschillende datastores of verschillende opslagprofielen toewijst, kunnen de architecten van blueprints de opslagruimte efficiënter beheren en gebruiken. Ze kunnen bijvoorbeeld het besturingssysteem implementeren op tragere, goedkopere datastores of opslagprofielen en het databasevolume op snellere datastores of opslagprofielen.

Bepaalde machine-endpoints bieden alleen ondersteuning voor één opslagprofiel; andere bieden ondersteuning voor schijfopslag op meerdere niveaus. Schijfopslag op meerdere niveaus is beschikbaar voor vCloud Director 5.6-endpoints en hoger en voor vCloud Air-endpoints. Schijfopslag op meerdere niveaus wordt niet ondersteund voor vCloud Director 5.5-endpoints.

Als u een blueprint maakt, kunt u één datastore toewijzen of een opslagreserveringsbeleid met meerdere datastores voor een volume. Wanneer u één datastore of opslagprofiel aan een volume toewijst, gebruikt vRealize Automation de datastore of het opslagprofiel in kwestie indien mogelijk bij de inrichting. Als u een opslagreserveringsbeleid toewijst aan een volume, gebruikt vRealize Automation bij de inrichting een van zijn datastores of opslagprofielen (indien gebruik wordt gemaakt van andere bronnen zoals vCloud Air of vCloud Director).

Een opslagreserveringsbeleid is in principe een label dat een materiaalbeheerder op een of meer datastores of opslagprofielen toepast om datastores of opslagprofielen met soortgelijke kenmerken (zoals snelheid of prijs) te groeperen. U kunt een datastore of opslagprofiel slechts aan één opslagreserveringsbeleid tegelijk toewijzen, maar een opslagreserveringsbeleid kan veel verschillende datastores of opslagprofielen bevatten.

U kunt een opslagreserveringsbeleid maken en toewijzen aan een of meer datastores of opslagprofielen. Een auteur van blueprints kan het opslagreserveringsbeleid vervolgens toewijzen aan een volume in een virtuele blueprint. Wanneer een gebruiker een machine aanvraagt op basis van de blueprint, gebruikt vRealize Automation het opslagreserveringsbeleid dat in de blueprint is opgegeven om een datastore of opslagprofiel te selecteren voor het volume van de machine.

Opmerking Als u SDRS op uw platform hebt ingeschakeld, kunt u instellen dat de opslag via SDRS wordt verdeeld voor afzonderlijke virtual machineschijven, of dat alle opslag voor de virtual machine wordt verdeeld. Als u met SDRS-datastoreclusters werkt, kunnen er conflicten optreden als u reserveringsbeleid en opslagreserveringsbeleid gebruikt. Als bijvoorbeeld een afzonderlijke datastore of een datastore binnen een SDRS-cluster wordt geselecteerd bij een van de reserveringen in een beleid of opslagbeleid, kan de opslagruimte van uw virtual machine geblokkeerd raken in plaats van dat deze wordt aangestuurd door SDRS. Als u opnieuw inrichten aanvraagt voor een machine met een opslaglocatie op een SDRS-cluster, wordt de machine verwijderd als het SDRS-automatiseringsniveau is gedeactiveerd. Zie de aangepaste eigenschap `VirtualMachine.Admin.Datastore.Cluster.ResourceLeaseDurationSec` voor gerelateerde informatie over provisioning en SDRS.

Opslagruimte en geheugen die door middel van een reservering zijn toegewezen aan een ingerichte machine, worden vrijgemaakt wanneer de machine waaraan ze zijn gekoppeld, in vRealize Automation wordt verwijderd door de actie Vernietigen. De opslagruimte en het geheugen worden niet vrijgemaakt als de machine wordt verwijderd in de vCenter Server.

Bijvoorbeeld: u kunt geen reservering verwijderen die is gekoppeld aan machines in een bestaande implementatie. Als u geïmplementeerde machines handmatig verplaatst of verwijderd in de vCenter Server, blijft vRealize Automation de geïmplementeerde machines als live herkennen en voorkomen dat u bijbehorende reserveringen verwijderd.

Een opslagreserveringsbeleid configureren

U kunt opslagreserveringsbeleidsregels maken om datastores met soortgelijke kenmerken, zoals snelheid of prijs, te groeperen. Nadat u het opslagreserveringsbeleid hebt gemaakt, moet u dit invullen met datastores voordat u het beleid in een blueprint gebruikt.

Procedure

1 Een opslagreserveringsbeleid maken

U kunt een opslagreserveringsbeleid gebruiken om datastores met soortgelijke kenmerken, zoals snelheid of prijs, te groeperen.

2 Een opslagreserveringsbeleid toewijzen aan een datastore

U kunt een opslagreserveringsbeleid koppelen aan een computerbron. Nadat het opslagreserveringsbeleid is gemaakt, vult u het met datastores. Een datastore kan maar bij één opslagreserveringsbeleid horen. Voeg meerdere datastores toe om een groep met datastores te maken voor gebruik met een blueprint.

Een opslagreserveringsbeleid maken

U kunt een opslagreserveringsbeleid gebruiken om datastores met soortgelijke kenmerken, zoals snelheid of prijs, te groeperen.

Het beleid wordt gemaakt als een lege container.

U kunt bepalen hoe het reserveringsbeleid wordt weergegeven, tijdens het toevoegen, bewerken of verwijderen, door gebruik te maken van de optie **Filteren op type** op de pagina Reserveringsbeleid.

Voorwaarden

Meld u aan bij vRealize Automation als een **materiaalbeheerder**.

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Reserveringsbeleid**.
- 2 Klik op het pictogram **Nieuw** (+).
- 3 Geef een naam op in het tekstvak **Naam**.
- 4 Selecteer **Opslagreserveringsbeleid** in het vervolgkeuzemenu **Type**.
- 5 Geef een beschrijving op in het tekstvak **Beschrijving**.
- 6 Klik op **OK**.

Een opslagreserveringsbeleid toewijzen aan een datastore

U kunt een opslagreserveringsbeleid koppelen aan een computerbron. Nadat het opslagreserveringsbeleid is gemaakt, vult u het met datastores. Een datastore kan maar bij één opslagreserveringsbeleid horen. Voeg meerdere datastores toe om een groep met datastores te maken voor gebruik met een blueprint.

Voorwaarden

[Een opslagreserveringsbeleid maken](#).

Procedure

- 1 Selecteer **Infrastructuur > Computerbronnen > Computerbronnen**.
- 2 Wijs een computerbron aan en klik op **Bewerken**.
- 3 Klik op het tabblad **Configuratie**.
- 4 Zoek naar de datastore die u aan uw opslagreserveringsbeleid wilt toevoegen in de tabel Opslag.
- 5 Klik op het pictogram **Bewerken** (✎) naast het gewenste **Opslagpad**-object.
- 6 Selecteer een opslagreserveringsbeleid in de kolom **Opslagreserveringsbeleid** van het vervolgkeuzemenu.

Na het inrichten van een machine, kunt u het opslagreserveringsbeleid ervan niet wijzigen als dit betekent dat het opslagprofiel op een schijf wordt gewijzigd.

- 7 Klik op **OK**.
- 8 (Optioneel) Wijs aanvullende datastores toe aan uw opslagreserveringsbeleid.
- 9 Klik op **OK**.

Plaatsing van werklasten

Wanneer u een blueprint implementeert, gebruikt plaatsing van werkbelasting verzamelde gegevens om aan te bevelen waar u de blueprint moet implementeren op basis van de beschikbare bronnen. vRealize Automation en vRealize Operations Manager werken samen om aanbevelingen voor plaatsing te bieden voor werkbelasting in de implementatie van nieuwe blueprints.

Terwijl vRealize Automation het organisatiebeleid beheert, zoals bedrijfsgroepen, reserveringen en quota, integreert het met de capaciteitsanalyses van vRealize Operations Manager bij het plaatsen van machines. Plaatsing van werkbelasting is alleen beschikbaar voor vSphere-endpoints.

Gebruikte termen bij plaatsing van werkbelasting

Bij de plaatsing van werkbelasting worden verschillende termen gebruikt.

- Clusters in vSphere zijn toegewezen aan computerbronnen in vRealize Automation.
- Bij reserveringen horen berekenen en opslaan, waarbij de opslag kan bestaan uit individuele datastores of datastoreclusters. Een reservering kan meerdere datastores, datastoreclusters of beide bevatten.
- Meerdere reserveringen kunnen naar dezelfde cluster verwijzen.
- Virtuele machines kunnen verplaatst worden naar meerdere clusters.
- Wanneer plaatsing van werkbelasting is ingeschakeld, maakt de inrichtingswerkstroom gebruik van het plaatsingsbeleid om aanbevelingen te doen waar de blueprint moet worden geïmplementeerd.

Blueprints inrichten met plaatsing van werkbelasting

Wanneer u plaatsing van werkbelasting gebruikt om blueprints in te richten, gebruikt de inrichtingswerkstroom de reserveringen in vRealize Automation en de plaatsingsoptimalisatie uit vRealize Operations Manager.

- 1 vRealize Automation verschaft de governanceregels om plaatsingsbestemmingen toe te staan.
- 2 vRealize Operations Manager verschaft aanbevelingen voor plaatsingsoptimalisatie in overeenstemming met analysegegevens.
- 3 vRealize Automation zet het inrichtingsproces voort in overeenstemming met de plaatsingsaanbevelingen van vRealize Operations Manager.

Als vRealize Operations Manager geen aanbeveling kan doen of als u de aanbeveling niet kunt gebruiken, valt vRealize Automation terug op de standaardlogica voor plaatsing.

Als een ontwikkelaar een catalogusitem selecteert en het formulier invult om het catalogusitem aan te vragen, houdt vRealize Automation rekening met de volgende overwegingen om de virtual machines in te richten.

Tabel 2-16. Overwegingen bij het inrichten van virtuele machines

Overweging	Effect
Beleidsregels	Het reserveringsbeleid van vRealize Automation kan meer dan één reservering aangeven.
Reserveringen	<p>vRealize Automation evalueert de aanvraag en bepaalt welke reserveringen kunnen voldoen aan de beperkingen die in de aanvraag zijn gemaakt.</p> <ul style="list-style-type: none"> ■ Als plaatsing is ingeschakeld en gebaseerd op vRealize Operations Manager-analysegegevens, geeft vRealize Automation de lijst met reserveringen door aan vRealize Operations Manager om te bepalen welke reservering het meest geschikt is voor plaatsing op basis van operationele metriecken. ■ Als plaatsing niet is gebaseerd op vRealize Operations Manager, bepaalt vRealize Automation de plaatsing op basis van prioriteiten en beschikbaarheid. <p>De reserveringen worden bijgewerkt om bij te houden dat bronnen zijn verbruikt.</p> <p>Als vRealize Operations Manager een cluster of datastore aanbeveelt die volgens vRealize Automation niet voldoende capaciteit heeft of niet van toepassing is, registreert vRealize Automation de uitzondering. vRealize Automation staat toe dat het inrichten worden verdergezet volgens de standaardplaatsingsmechanismen.</p>

Om bronnen te identificeren voor een virtuele machine, biedt vRealize Automation een lijst met kandidaatreserveringen. De kandidaten in de lijst kunnen een cluster en één of meer datastores of datastoreclusters bevatten. vRealize Operations Manager gebruikt de kandidaatreserveringen om een lijst te maken van doelkandidaten en om het beste doel vast te stellen.

Met het beleid in vRealize Operations Manager wordt het niveau van evenwicht, gebruik en bufferruimte voor de cluster ingesteld. Voor elke reservering, die een cluster of datastorecluster is, valideert vRealize Automation of de aanbeveling haalbaar is voor het plaatsingsdoel.

- Als de bestemming haalbaar is, plaatst vRealize Automation de blueprint volgens de aanbeveling.
- Als de bestemming niet haalbaar is, gebruikt vRealize Automation het standaard-plaatsingsgedrag om de virtuele machines te plaatsen.

Bij plaatsingsoverwegingen moet ook rekening worden gehouden met status- en gebruiksproblemen. Terwijl de cloudbeheerder en de beheerder van de virtuele infrastructuur de infrastructuur beheren, dragen ontwikkelaars de zorg voor de status van hun toepassingen. Om ontwikkelaars te ondersteunen moet in de plaatsingsstrategie van de werkbelasting rekening worden gehouden met status- en gebruiksproblemen.

Tabel 2-17. Overwegingen voor status- en gebruiksproblemen

Probleem met werkbelasting	Plaatsingsoplossing
Ontwikkelaar constateert een statusprobleem in de omgeving.	vRealize Automation richt blueprints in clusters in die problemen hebben of die te veel worden gebruikt vanwege een grote werkbelasting. vRealize Automation moet integreren met de capaciteitsanalyse in vRealize Operations Manager om ervoor te zorgen dat blueprints worden ingericht in clusters die voldoende capaciteit hebben.
Ontwikkelaar constateert een gebruiksprobleem.	De clusters in de omgeving worden te weinig gebruikt. vRealize Automation moet integreren met de capaciteitsanalyse die vRealize Operations Manager verschaft om ervoor te zorgen dat blueprints worden ingericht in een cluster waarin het gebruik is geoptimaliseerd.

Gebruikers die blueprints inrichten

De volgende gebruikers voeren acties uit om blueprints in te richten.

Tabel 2-18. Gebruikers en rollen bij het inrichten van blueprints

Stap	Gebruiker	Actie	Vereiste rol
1	Cloudbeheerder of VI-beheerder (Virtual Infrastructure)	Zorgt ervoor dat de initiële plaatsing van virtual machines conform het organisatorische beleid is en dat de virtual machines worden geoptimaliseerd in overeenstemming met de operationele analysegegevens.	IaaS-beheerdersrol
1	Materiaalbeheerder	Definieert reserveringen, reserveringsbeleid en plaatsingsbeleid in vRealize Automation.	Materiaalbeheerdersrol, Infrastructuurarchitect
1	IaaS-beheerder	Definieert de endpoints voor vSphere en vRealize Operations Manager, die noodzakelijk zijn voor plaatsing van werklasten.	IaaS-beheerdersrol
2	Infrastructuurarchitect	Werkt als blueprintarchitect direct met onderdeeltypen voor virtual machines en wijst reserveringsbeleid toe aan virtual machines wanneer een blueprint wordt ontworpen. Bepaalt het reserveringsbeleid als eigenschap van het machineonderdeel in de blueprint.	Infrastructuurarchitect

Tabel 2-18. Gebruikers en rollen bij het inrichten van blueprints (vervolg)

Stap	Gebruiker	Actie	Vereiste rol
3	Infrastructuurarchitect, Toepassingsarchitect, Softwarearchitect en XaaS-architect	<p>Maakt en publiceert de blueprint om de virtual machines in te richten. Alleen de Infrastructuurarchitect werkt rechtstreeks met machineonderdelen. De overige architectrollen kunnen infrastructuurblueprints hergebruiken bij nesten, maar ze kunnen de instellingen voor machineonderdelen niet bewerken.</p> <p>De blueprint kan één onderdeel bevatten of kan geneste blueprints, XaaS-onderdelen, meerdere virtuele machines in een toepassing van meerdere lagen, enzovoort bevatten.</p> <p>vRealize Automation plaatst de virtual machines volgens de configuratie van de reserveringen en voegt optioneel het reserveringsbeleid toe op het niveau van het machineonderdeel voor de blueprint. Als uw blueprint bijvoorbeeld twee machines bevat, kan op elke machine een ander beleid worden toegepast.</p> <p>vRealize Automation optimaliseert ook de virtuele machines in overeenstemming met de operationele analysegegevens die vRealize Operations Manager verschaft.</p>	Infrastructuurarchitect
4	Cloudbeheerder of VI-beheerder	<p>Selecteert het beleid op basis waarvan de initiële plaatsing wordt bepaald van de virtuele machines die vRealize Automation inricht.</p> <p>De beheerder kan:</p> <ul style="list-style-type: none"> ■ Het beleid selecteren door een API te gebruiken. ■ Het standaard-plaatsingsbeleid gebruiken waarin elke server in vRealize Automation beurtelings wordt gebruikt om de werkbelasting te verdelen. Voor deze methode is geen invoer van vRealize Operations Manager vereist. 	IaaS-beheedersrol, Infrastructuurarchitect
5	VI-beheerder	Maakt het aangepaste datacenter en de aangepaste groepen in vRealize Operations Manager. Vervolgens past de VI-beheerder het beleid toe op basis waarvan de werkbelasting van deze aangepaste datacenters wordt geconsolideerd en verdeeld.	IaaS-beheedersrol, Infrastructuurarchitect
6	Materiaalbeheerder	Selecteert het plaatsingsbeleid in vRealize Automation. Het plaatsingsbeleid voor werkbelasting gebruiken om vRealize Automation de plaats van machines te laten bepalen wanneer u nieuwe blueprints implementeert. Het plaatsingsbeleid vereist gegevens uit vRealize Operations Manager.	Materiaalbeheederrol

Tabel 2-18. Gebruikers en rollen bij het inrichten van blueprints (vervolg)

Stap	Gebruiker	Actie	Vereiste rol
7	Ontwikkelaar	Vraagt een blueprint aan om virtuele machines in te richten. De blueprint kan bestaan uit meerdere machines om een toepassing met drie lagen uit te voeren.	
8	Ontwikkelaar	Als de ontwikkelaar de blueprint implementeert, zoekt vRealize Operations Manager naar een plaatsingsbeleid dat past bij de relevante clusters voor de aanvraag.	

Zie [Plaatsingsbeleid](#) voor meer informatie over het plaatsingsbeleid.

Zie [Werklastplaatsing configureren](#) om de plaatsing van werkbelasting te configureren.

Distributed Resource Scheduler (DRS) is vereist om virtuele machines te plaatsen

vSphere DRS is de plaatsingsengine die wordt gebruikt door vRealize Automation en vRealize Operations Manager om virtuele machines in te richten en te plaatsen.

vRealize Automation kan alleen de beste plaatsing voor de virtuele machines voorstellen als u DRS op het cluster inschakelt en instelt op volledig automatisch. vRealize Automation gebruikt vervolgens de API's van vSphere DRS om de juiste plaatsing te bepalen voor de virtuele machines.

vRealize Automation integreert met de vRealize Operations Manager plaatsingsservice. vRealize Operations Manager biedt alleen aanbevelingen voor plaatsing voor clusters waarop DRS is ingeschakeld en volledig automatisch is.

Gevolgen van vRealize Automation-opslagreserveringsbeleid

De aanwezigheid van vRealize Automation-opslagreserveringsbeleid is van invloed op de verdeling van belasting met vRealize Operations Manager.

Als de verdeling van belasting met vRealize Operations Manager is ingeschakeld, geeft vRealize Automation een lijst met beschikbare reserveringen door aan vRealize Operations Manager, en evalueert vRealize Operations Manager de reserveringen voor opslagplaatsing gebaseerd op operationele analyse.

Opmerking Verdeling van belasting met vRealize Operations Manager ondersteunt alleen virtual machines met een of meer schijven, waarbij slechts één opslagreserveringsbeleid aanwezig is. Meerdere beleidscombinaties worden niet ondersteund voor schijfplaatsing, omdat de plaatsing van afzonderlijke schijven niet wordt ondersteund.

Als een blueprint een opslagreserveringsbeleid bevat, veranderen aanbevelingen voor de verdeling van belasting van vRealize Operations Manager op de volgende manieren:

Configuratie	Plaatsing
Virtual machines met een of meer schijven, waar geen enkele een opslagreserveringsbeleid specificeert	Plaatsing gebeurt zoals gewoonlijk. vRealize Operations Manager evalueert de volledige, ongefilterde lijst met kandidaatreserveringen.
Virtual machines met een of meer schijven, waar allen hetzelfde opslagreserveringsbeleid specificeren	Kandidaatreserveringen worden gefilterd op opslagniveau, zodat vRealize Operations Manager alleen de gegevensopslag evalueert die overeenkomt met dat opslagreserveringsbeleid.
Virtual machines met meerdere schijven, waarbij sommigen hetzelfde opslagbeleid specificeren, maar waar anderen geen opslagreserveringsbeleid opgeven	<ul style="list-style-type: none"> ■ Wanneer het opslagallocatietype COLLECTED is, de standaard, worden alle schijven behandeld alsof ze hetzelfde beleid delen. vRealize Operations Manager evalueert de gegevensopslag die overeenkomt met dat opslagreserveringsbeleid. ■ Wanneer het opslagallocatietype DISTRIBUTED is, kunnen virtual machines niet geplaatst worden volgens de aanbevelingen van vRealize Operations Manager omdat de plaatsing van afzonderlijke schijven niet wordt ondersteund. Standaard worden er dan in plaats daarvan vRealize Automation-plaatsingsalgoritmes gebruikt. <p>U kunt het opslagallocatietype instellen met behulp van een aangepaste eigenschap.</p>
Virtual machines met meerdere schijven, waarbij de schijven een verschillend opslagreserveringsbeleid specificeren	Omdat ze conflicterende vereisten hebben voor het opslagreserveringsbeleid, kunnen deze virtual machines niet worden geplaatst volgens vRealize Operations Manager-aanbevelingen. Standaard worden er dan in plaats daarvan vRealize Automation-plaatsingsalgoritmes gebruikt.
Virtual machines die een specifiek opslagpad vereisen	<p>Deze virtual machines worden niet via een vRealize Operations Manager-aanbeveling geplaatst, omdat u al een opslagpad heeft opgegeven. Plaatsing komt mogelijk, of mogelijk niet, overeen met wat vRealize Operations Manager zou hebben aanbevolen.</p> <p>U kunt het opslagpad instellen door gebruik te maken van een aangepaste eigenschap.</p>

Plaatsingsfouten - wanneer op vRealize Operations Manager gebaseerde plaatsing niet uitgevoerd kan worden, wordt de reden beschreven door een fout. Redenen kunnen de niet-ondersteunde situaties zijn die in de lijst hierboven zijn beschreven, of omgevingsfactoren zoals mislukte communicatie tussen vRealize Operations Manager en vRealize Automation.

Om fouten te controleren, gaat u naar **Aanvragen > Uitvoering**. Klik rechtsboven op **Plaatsingsfouten weergeven**.

Beperkingen op plaatsing van werklust

Wanneer u het plaatsingsbeleid voor plaatsing van werkbelasting gebruikt om machines te plaatsen wanneer u nieuwe blueprints implementeert, dient u rekening te houden met de beperkingen.

- In vRealize Operations Manager identificeert de vRealize Automation-oplossing de clusters en virtual machines die vRealize Automation beheert.
- Wanneer vRealize Automation de onderliggende objecten van een datacenter- of aangepaste datacentercontainer in vRealize Operations Manager beheert, is de mogelijkheid om die objecten opnieuw te verdelen niet beschikbaar. U kunt het uitsluiten van acties op door vRealize Automation beheerde objecten niet uitschakelen.

- Voor de objecten die vRealize Automation beheert, werkt de werklastplaatsing als volgt:
 - Wanneer een datacenter of een aangepast datacenter een cluster bevat dat vRealize Automation beheert, zal de werklastplaatsing u niet toestaan het cluster opnieuw te verdelen.
 - Wanneer een cluster virtual machines bevat die vRealize Automation beheert, zal de plaatsing van werkbelasting u niet toestaan deze virtual machines te verplaatsen.
- vRealize Operations Manager biedt geen ondersteuning voor plaatsing van werkbelasting op bronnenpools in vCenter Server.
- vRealize Operations Manager 7.5 en hoger ondersteunt vSAN-gegevensopslagruimten voor de plaatsing van workloads. Zie de release notes voor vRealize Operations Manager 7.5 <https://docs.vmware.com/nl/vRealize-Operations-Manager/7.5/rn/vRealize-Operations-Manager-75.html> voor gerelateerde informatie.

Rechten om de plaatsing van werklasten te configureren

U moet rechten in vRealize Automation en vRealize Operations Manager hebben om de plaatsing van werklasten en het plaatsingsbeleid te configureren.

U moet de rol Materiaalbeheerder hebben om plaatsing van werklasten te configureren in vRealize Automation. Zie Overzicht gebruikersrollen in het vRealize Automation-informatiecentrum.

In vRealize Operations Manager moet u een gebruikersrol maken voor plaatsing van werkbelasting en machtigingen aan de rol toewijzen.

- Wijs in het gebruikersaccount het recht alleen-lezen toe aan vSphere-hosts en -clusters, en vSphere-opslagruimte, in de objectenhierarchie.
- Wijs lees- en schrijfrechten toe in API's om de gebruikersrol API-oproepen te laten gebruiken in de plaatsing van werkbelasting. Selecteer **Beheer > Toegangscontrole > Rechten** en selecteer **REST API's > Alle andere lees-, schrijf-API's**.

vRealize Automation gebruikt de vRealize Operations Manager-role wanneer u de endpoint registreert, en om plaatsingsaanbevelingen tijdens inrichting aan te vragen namens gebruikers die catalogusitems aanvragen.

Zie Toegangscontrole in het vRealize Operations Manager-informatiecentrum voor meer informatie.

Plaatsingsbeleid

U kunt het plaatsingsbeleid gebruiken om vRealize Automation de plaats van machines te laten bepalen wanneer u nieuwe blueprints implementeert. Het plaatsingsbeleid maakt gebruik van de analyse van vRealize Operations Manager om werklasten op uw clusters te bepalen zodat bestemmingen voor de plaatsing kunnen worden voorgesteld.

U moet verschillende stappen uitvoeren voordat u het plaatsingsbeleid kunt gebruiken. In vRealize Automation maakt u endpoints voor de vRealize Operations Manager- en vCenter Server-instanties. Daarna maakt u een materiaalgroep en voegt u reserveringen toe aan uw vCenter Server-endpoint.

Om ervoor te zorgen dat vRealize Operations Manager aan vRealize Automation een analyse van de werklastplaatsing biedt, moet u het volgende doen:

- Installeer de vRealize Automation-oplossing in de vRealize Operations Manager-instantie die voor de werklastplaatsing wordt gebruikt.
- Configureer vRealize Operations Manager om de vCenter Server te bewaken.

Zie [Werklastplaatsing configureren](#) als u vRealize Automation en vRealize Operations Manager voor werklastplaatsing wilt configureren.

Het plaatsingsbeleid zoeken

Selecteer in uw vRealize Automation-instantie **Infrastructuur > Reserveringen > Plaatsingsbeleid**.

Als u de analyse van de werklastplaatsing wilt gebruiken die door vRealize Operations Manager wordt geboden, selecteert u **vRealize Operations Manager gebruiken voor plaatsingsaanbevelingen**.

Als u het beleid voor plaatsing van werkbelasting niet gebruikt, gebruikt vRealize Automation de standaardplaatsingsmethode.

Werklastplaatsing configureren

Als u het plaatsingsbeleid wilt gebruiken om machines te plaatsen wanneer u nieuwe blueprints implementeert, configureert u vRealize Automation voor het gebruik van de analyses die vRealize Operations Manager levert. U kunt vRealize Operations Manager ook zodanig configureren dat er beleid wordt toegepast om werklasten te consolideren en evenwichtig te verdelen onder uw clustercomputerbronnen.

In vRealize Automation kunt u endpoints configureren, een materiaalgroep maken en reserveringen toevoegen. In vRealize Operations Manager kunt u beleid configureren om een evenwichtige werklast te ondersteunen en dat beleid toepassen op een aangepaste groep waarin uw aangepaste computerbronnen zijn opgenomen.

Voorwaarden

Voordat het plaatsingsbeleid plaatsingsdoelen voor blueprints kan voorstellen, moet u enkele stappen uitvoeren.

- Begrijp het plaatsingsbeleid. Zie [Plaatsingsbeleid](#).
- Controleer of er een endpoint bestaat in vRealize Automation voor de instantie van vRealize Operations Manager die voor werklastplaatsing wordt gebruikt. Zie [Een vRealize Operations Manager-endpoint maken](#).
- Controleer of er een endpoint bestaat in vRealize Automation voor de instantie van vCenter Server. Zie [Een vSphere-endpoint in vRealize Automation maken en koppelen aan NSX](#).

- Voeg reserveringen toe aan het endpoint van vCenter Server. Zie [Reserveringen](#).
- Voeg een materiaalgroep toe en controleer of uw gebruiker een materiaalgroepbeheerder is. Zie [Een materiaalgroep maken](#).
- Controleer of vRealize Operations Manager dezelfde infrastructuur bewaakt die vRealize Automation bewaakt, om ervoor te zorgen dat het om dezelfde instanties van vCenter Server gaat. Zie [VMware vSphere Solution in vRealize Operations Manager](#) in vRealize Operations Manager Informatiecentrum.
- Zorg dat u reserveringen, opslagreservering, blueprints en gedelegeerde providers begrijpt. Zie vRealize Automation Informatiecentrum.
- Begrijp en definieer de instellingen voor invullen en evenwichtige verdeling in het vRealize Operations Manager-beleid dat voor werklastplaatsing wordt gebruikt. Zie [Workload Automation Details](#) in vRealize Operations Manager Informatiecentrum.

Procedure

1 [vRealize Automation configureren voor werklastplaatsing](#)

Als u analyses voor werklastplaatsing wilt gebruiken om machines te plaatsen wanneer u nieuwe blueprints implementeert, moet u de instantie van vRealize Automation hierop voorbereiden.

2 [vRealize Operations Manager configureren voor werklastplaatsing in vRealize Automation](#)

Als u analyses voor werklastplaatsing wilt leveren aan vRealize Automation om machines te plaatsen wanneer u nieuwe blueprints implementeert, moet u de instantie van vRealize Operations Manager hierop voorbereiden.

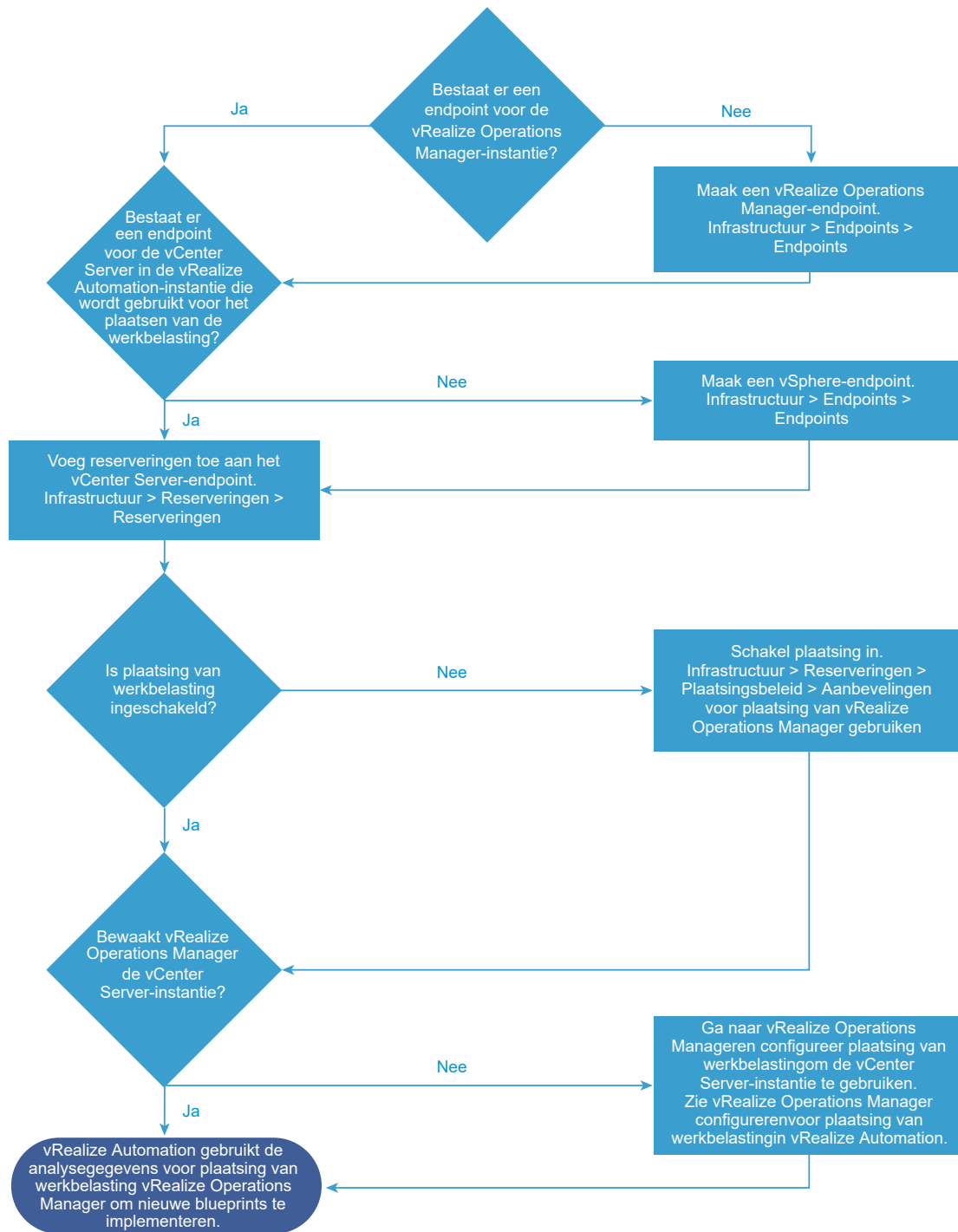
Resultaten

U hebt vRealize Automation en vRealize Operations Manager geconfigureerd om op basis van analyses van werklasten plaatsingsdoelen voor nieuwe blueprints voor te stellen.

vRealize Automation configureren voor werklastplaatsing

Als u analyses voor werklastplaatsing wilt gebruiken om machines te plaatsen wanneer u nieuwe blueprints implementeert, moet u de instantie van vRealize Automation hierop voorbereiden.

Om uw instantie van vRealize Automation voor te bereiden op het gebruik van het plaatsingsbeleid, configureert u de endpoints, maakt u een materiaalgroep en voegt u reserveringen toe.



Voorwaarden

- Zorg dat u de vereisten voor werklustplaatsing begrijpt. Zie [Werklustplaatsing configureren](#).
- Voeg in vRealize Automation een specifieke gebruikersrol en machtigingen toe zodat vRealize Operations Manager referenties kan valideren. Zie Overzicht gebruikersrollen in het vRealize Automation-informatiecentrum.

Procedure

- 1 Voeg in uw instantie van vRealize Automation een endpoint toe voor de instantie van vRealize Operations Manager en klik op **OK**.
 - a Selecteer **Infrastructuur > Endpoint > Endpoints**.
 - b Selecteer **Nieuw > Management > vRealize Operations Manager**.
 - c Voer de algemene informatie in voor het **vRealize Operations Manager**-endpoint.
U hoeft geen eigenschappen op te geven voor het endpoint.
- 2 Voeg in uw instantie van vRealize Automation een endpoint toe voor de instantie van vCenter Server en klik op **OK**.
 - a Selecteer **Infrastructuur > Endpoint > Endpoints**.
 - b Selecteer **Nieuw > Virtueel > vSphere (vCenter)**.
 - c Voer de algemene informatie, eigenschappen en associaties in voor het vCenter Server-endpoint.

Nadat u endpoints hebt toegevoegd en vRealize Automation gegevens daarvoor heeft verzameld, zijn de computerbronnen voor die endpoints beschikbaar. Vervolgens kunt u die computerbronnen toevoegen aan de materiaalgroep die u maakt.

- 3 Maak een materiaalgroep zodat andere gebruikers reserveringen kunnen maken, en schakel het plaatsingsbeleid in.
 - a Selecteer **Infrastructuur > Endpoint > Materiaalgroepen**.
 - b Klik op **Nieuw** en voer informatie over de materiaalgroep in.

Optie	Beschrijving
Naam	Voer een betekenisvolle naam voor de materiaalgroep in.
Beschrijving	Voer een uitgebreide beschrijving in.
Materiaalbeheerders	Voer het e-mailadres in voor iedereen die u als materiaalbeheerder wilt aanstellen.
Computerbronnen	Selecteer de computerbronclusters die de beheerders kunnen beheren.

Nadat u computerbronnen aan een materiaalgroep hebt toegevoegd en vRealize Automation gegevens erover heeft verzameld, kunnen materiaalbeheerders reserveringen maken voor de computerbronnen.

4 Maak reserveringen voor de computerbronnen in de instantie van vCenter Server.

- a Selecteer **Infrastructuur > Reserveringen > Reserveringen**.
- b Selecteer **Nieuw > vSphere (vCenter)**.
- c Voer op elk tabblad de informatie voor de reservering in.

Optie	Actie
Algemeen	Selecteer een reserveringsbeleid, de prioriteit voor elk beleid en klik op Deze reservering inschakelen .
Bronnen	Selecteer machinequota, geheugen en opslag. U hoeft geen bronpool op te geven.
Netwerk	Selecteer de netwerkadapter. U hoeft geen netwerkprofiel op te geven.
Propertes	Voeg indien nodig aangepaste eigenschappen aan de reservering toe.
Waarschuwing	Selecteer Waarschuwingen over capaciteit indien nodig om ontvangers te melden wanneer de capaciteit de reserveringsdrempel overstijgt.

5 Schakel het plaatsingsbeleid in.

- a Selecteer **Infrastructuur > Reserveringen > Plaatsingsbeleid**.
- b Schakel het selectievakje **vRealize Operations Manager gebruiken voor plaatsingsaanbevelingen** in.

Resultaten

U hebt vRealize Automation geconfigureerd om op basis van analyses van vRealize Operations Manager machines te plaatsen wanneer gebruikers blueprints implementeren.

Wat nu te doen

Configureer vRealize Operations Manager om de instantie van vCenter Server te bewaken en beleid voor werklustplaatsing toe te passen op uw clustercomputerbronnen. Zie [vRealize Operations Manager configureren voor werklustplaatsing in vRealize Automation](#).

vRealize Operations Manager configureren voor werklustplaatsing in vRealize Automation

Als u analyses voor werklustplaatsing wilt leveren aan vRealize Automation om machines te plaatsen wanneer u nieuwe blueprints implementeert, moet u de instantie van vRealize Operations Manager hierop voorbereiden.

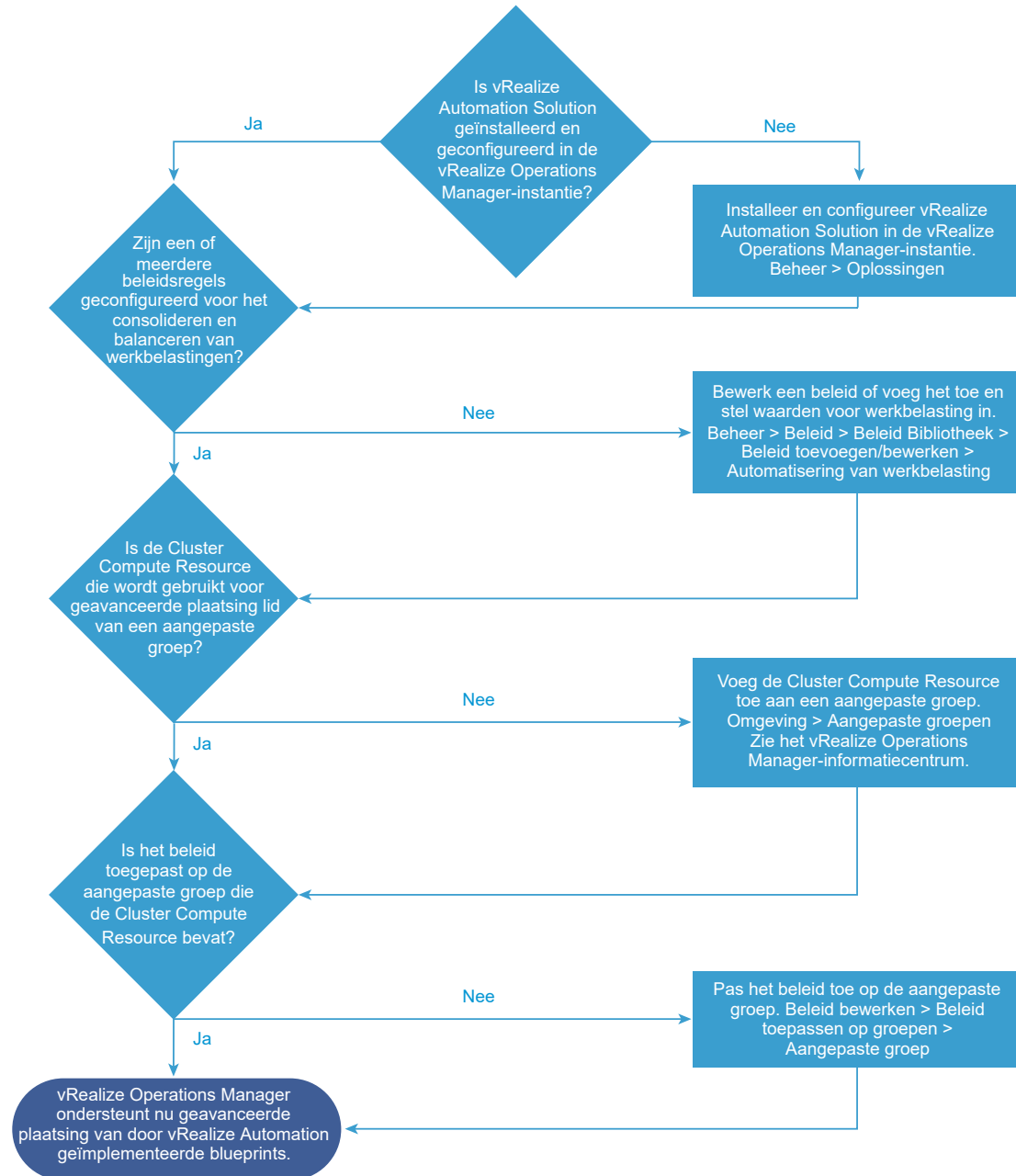
Voorzichtig Installeer de vRealize Automation-oplossing, waarin Management Pack is inbegrepen, op slechts één enkele instantie van vRealize Operations Manager.

Om uw instantie van vRealize Operations Manager voor te bereiden op het leveren van analyses aan vRealize Automation, moet u de vRealize Automation-oplossing installeren en configureren. U moet ook beleid configureren en dit toepassen op uw clustercomputerbronnen.

Nadat u de vRealize Automation-oplossing hebt geconfigureerd, kunt u virtual machines die door vRealize Automation worden beheerd niet meer verplaatsen of opnieuw verdelen.

Als de vRealize Automation-oplossing niet in de vRealize Operations Manager-instantie is geïnstalleerd, kunt u met plaatsing van werkbelasting nog steeds virtual machines verplaatsen of opnieuw verdelen die worden beheerd door vRealize Automation.

Als u de plaatsing van werkbelasting wilt toestaan om virtual machines te verplaatsen, moeten deze virtual machines zich in een datacenter of aangepast datacenter bevinden.



Voorwaarden

- Configureer vRealize Automation om analyses voor werklastplaatsing te gebruiken. Zie [vRealize Automation configureren voor werklastplaatsing](#).

- Controleer of de vRealize Automation-oplossing is geïnstalleerd en geconfigureerd in de instantie van vRealize Operations Manager die voor werklastplaatsing wordt gebruikt. Zie [Management Pack for vRealize Automation op Solution Exchange](#) voor meer informatie over deze oplossing. Voor informatie over hoe werklastplaatsing werkt in vRealize Operations Manager verwijzen wij u naar [Workload Automation Details](#) en verwante onderwerpen in de vRealize Operations Manager-documentatie.

Procedure

- 1 Installeer en configureer de vRealize Automation-oplossing in de instantie van vRealize Operations Manager die werklastplaatsing beheert.

De oplossing is mogelijk al geïnstalleerd.

- a Klik op **Beheer > Oplossingen** om de oplossingen te zien die in vRealize Operations Manager zijn geïnstalleerd.

- b Controleer of de vRealize Automation-oplossing al is geïnstalleerd.

Download en installeer de oplossing als de vRealize Automation-oplossing niet in de lijst wordt weergegeven. Zie [Management Pack for vRealize Automation op Solution Exchange](#).

- c Als de oplossing in de lijst wordt weergegeven, selecteert u de **VMware vRealize Automation-oplossing** en klikt u op **Configureren**.

- d Configureer de vRealize Automation-oplossing en sla de instellingen op.

Zie [Solutions in vRealize Operations Manager](#) in het vRealize Operations Manager-informatiecentrum voor meer informatie over het configureren van de oplossing.

- 2 Als u het vRealize Operations Manager-standaardbeleid niet gebruikt, moet u een aangepaste groep maken. Vervolgens voegt u uw clustercomputerbronnen toe aan de aangepaste groep.

Als u een ander beleid dan het standaardbeleid wilt toepassen op uw clusters, voegt u een aangepaste groep toe. Vervolgens kunt u het beleid op de aangepaste groep toepassen. Als u het standaardbeleid gebruikt, hoeft u geen aangepaste groep te maken, omdat het standaardbeleid op alle objecten wordt toegepast.

- a Klik op **Omgeving > Aangepaste groepen**.

- b Maak een aangepaste groep als er geen aangepaste groep voor uw clusters bestaat.

Zie [User Scenario: Creating Custom Object Groups](#) in het vRealize Operations Manager-informatiecentrum voor meer informatie.

- c Voeg het cluster toe aan de aangepaste groep en sla de aangepaste groep op.

- 3 Configureer beleid om werklasten op uw clusters te consolideren en in evenwicht te brengen, en pas dat beleid toe op de aangepaste groep.

U kunt beleid configureren in vRealize Operations Manager om de instellingen te bepalen voor consolidatie, evenwichtige verdeling, invulling, CPU, geheugen en schijfruimte. U kunt

bijvoorbeeld de instelling met de naam Werklasten consolideren wijzigen om op basis van de clusterstatus en capaciteit de beste plaatsing te bepalen voor nieuwe beheerde werklasten. Ook kunt u de drempelinstelling voor Werklasten evenwichtig verdelen aanpassen aan het assertiviteitsniveau dat nodig is voor het plaatsen van werklasten. U kunt een of meer verzamelingen met beleidsregels configureren en deze toepassen op uw clustercomputerbronnen.

- a Klik op **Beheer > Beleid > Beleidsbibliotheek**.
- b Klik op **Beleid toevoegen/bewerken** en klik op **Automatisering van werklast** om waarden voor werklasten in te stellen.

De instellingen met de naam Werklasten consolideren en Clusterheadroom zijn van toepassing op de initiële plaatsing van virtual machines.

- Wanneer u Werklasten consolideren instelt op **geen**, verdeelt de plaatsing van werkbelasting de werklast over alle clusters waarop het beleid wordt toegepast. Wanneer u Werklasten consolideren instelt op een andere waarde dan geen, vult de plaatsing van werkbelasting eerst de drukste cluster.
 - Clusterheadroom is de bufferruimte die in een cluster is gereserveerd als een percentage van de totale capaciteit. Als u de clusterheadroom bijvoorbeeld instelt op 20%, kan die buffer mogelijk voorkomen dat de plaatsing van werkbelasting virtual machines op die cluster plaatst. De reden waarom dit de plaatsing voorkomt, is omdat de cluster 20% minder vrije CPU-, geheugen- of schijfruimte heeft.
- c Klik op **Beleid op groepen toepassen** in de beleidwerkrumte.
 - d Selecteer de aangepaste groep.
 - e Sla het beleid op.

Resultaten

U hebt vRealize Operations Manager zodanig geconfigureerd dat vRealize Automation de analyses voor werklastplaatsingen gebruikt om plaatsingsdoelen van machines voor te stellen wanneer gebruikers blueprints implementeren.

Wat nu te doen

Wacht tot vRealize Automation en vRealize Operations Manager gegevens hebben verzameld bij de endpoints en objecten in uw omgeving. Wanneer u nieuwe blueprints implementeert, geeft vRealize Automation de aanbevelingen voor werklastplaatsingen, doelkandidaten en geselecteerde plaatsing weer die u kunt bevestigen.

Problemen met plaatsing werkbelasting oplossen

Als u problemen met de plaatsing van de werkbelasting ondervindt, gebruik dan de informatie over het oplossen van problemen om deze op te lossen.

De vRealize Automation-oplossing is vereist voor een goede werking van de plaatsing van werklasten

Plaatsing van werklasten is gebaseerd op individuele machines en de plaatsing gebeurt op machineniveau. Wanneer vRealize Automation en vRealize Operations Manager samen zijn geïnstalleerd, moet de oplossing vRealize Automation ook zijn geïnstalleerd.

De oplossing, die het management pack en de adapter bevat, identificeert de clusters waar de actie Container opnieuw verdelen of VM verplaatsen is gedeactiveerd. De actie Opnieuw verdelen is gedeactiveerd in het aangepaste datacenter waartoe het cluster behoort.

- Voor niet-beheerde vRealize Automation-clusters die behoren tot een aangepast datacenter dat geen beheerde vRealize Automation-clusters heeft, zijn de acties VM verplaatsen en Container opnieuw verdelen ingeschakeld. Voor beheerde vRealize Automation-clusters zijn deze acties gedeactiveerd.
- In vRealize Operations Manager zorgt de vRealize Automation-adapter ervoor dat VM's in clusters die reserveringen toewijzen, niet beschikbaar zijn voor verplaatsing of herverdeling.

Voorzichtig De oplossing vRealize Automation mag slechts op één exemplaar van vRealize Operations Manager worden geïnstalleerd.

Hoge beschikbaarheid is ingeschakeld, maar moet worden gedeactiveerd

Wanneer hoge beschikbaarheid is ingeschakeld en vRealize Operations Manager is uitgevallen, kan de time-out voor plaatsing van de werklasting voor het oproepen van vRealize Operations Manager mislukken.

vRealize Automation registreert werklasting de plaatsing van fouten in het logboekbestand `catalina.out`.

vSphere-endpoints in vRealize Automation worden niet gecontroleerd

vRealize Operations Manager controleert de vSphere vCenter Server-instantie met de reserveringsclusters niet.

Als vRealize Operations Manager de vRealize Automation-kandidaatreserveringen voor een cluster, datastore of datastorecluster niet herkent bij een poging om deze te plaatsen, worden ze genegeerd. Als reactie op de plaatsing communiceert vRealize Operations Manager aan vRealize Automation dat ze niet worden herkend.

In de plaatsingsgegevens voor de aanvraaguitvoering geeft vRealize Automation een waarschuwingspictogram weer bij de kandidaatreservering om aan te geven dat deze niet wordt herkend.

Wanneer versies niet overeenkomen, wordt vRealize Automation boven aan de lijst weergegeven

vRealize Automation en vRealize Operations Manager beheren verschillende weergaven van de infrastructuur. Ze moeten echter beide dezelfde instanties van vCenter Server in dezelfde infrastructuur beheren.

Verbrekingen van verbindingen en niet-overeenkomende versies moeten worden geïdentificeerd en de details moeten worden weergegeven.

Wat moet u doen als de vRealize Automation-adapter is uitgevallen

Bij de initiële plaatsing wordt altijd rekening gehouden met de lijst met bestemmingskandidaten die wordt ontvangen van vRealize Operations Manager, zoals wanneer een gebruiker direct na installatie een cluster toevoegt.

Als de oplossing vRealize Automation, die het Management Pack en de Adapter bevat, niet beschikbaar is in de vRealize Operations Manager, zijn de acties VM verplaatsen en Container opnieuw balanceren beschikbaar.

Continue optimalisatie met behulp van vRealize Operations Manager

Continue optimalisatie maakt een doorlopend autonoom beheer van vRealize Automation-werklasten door vRealize Operations Manager mogelijk.

Met continue optimalisatie beschikt u over de mogelijkheid om werklasten anders te verdelen en te verplaatsen en kunt u vRealize Automation met vRealize Operations Manager gebruiken voor meer dan alleen de initiële werklastverdeling. Wanneer virtualisatiebronnen worden verplaatst of zwaarder of lichter worden belast, kan vRealize Automation ingerichte werklasten indien nodig verplaatsen.

- De continue optimalisatie maakt automatisch een nieuw datacenter in vRealize Operations Manager.
Er is één nieuw datacenter voor elk vRealize Automation vCenter-endpoint.
- Het nieuwe datacenter bevat elk beheerd vRealize Automation-cluster dat is gekoppeld aan het endpoint.

Opmerking Maak niet handmatig een gemengd datacenter van vRealize Automation- en niet-vRealize Automation-clusters.

- U kunt de continue optimalisatie alleen uitvoeren vanaf het nieuw gemaakte vRealize Automation -datacenter.
- Optimalisatie biedt geen ondersteuning voor verschillende reserveringsvereisten tussen clusters in de vCenter, die kunnen optreden wanneer u verschillende bedrijfsgroepen hebt.
Optimalisatie vindt plaats op het op vRealize Automation gebaseerde datacenterniveau en verschillende reserveringsvereisten op meerdere clusters kunnen succes voorkomen. Wanneer dat gebeurt, verschijnt er een foutmelding dat bepaalde bestemmingsclusters of opslag niet aan de vereisten voldoen, waardoor sommige optimalisatieacties niet mogelijk waren.
- Bij optimalisatie wordt nooit een nieuwe vRealize Automation- of vRealize Operations Manager-beleids-overtreding gemaakt.
 - Als u bestaande beleidsovertredingen hebt, kan optimalisatie operationele-intentieproblemen in vRealize Operations Manager oplossen.

- Als u bestaande beleidsovertredingen hebt, kan optimalisatie geen bedrijfsintentieproblemen in vRealize Operations Manager oplossen.

Als u bijvoorbeeld een virtual machine handmatig hebt verplaatst naar een cluster dat geen deel uitmaakte van haar reserveringsbeleid, zal vRealize Operations Manager geen overtreding detecteren, noch proberen deze op te lossen. Als u problemen met de bedrijfsintentie wilt oplossen, moet u vRealize Automation gebruiken om de werklast te verplaatsen.

- Deze versie voldoet aan de operationele intentie op het niveau van het datacenter. Alle vRealize Automation-ledenclusters worden geoptimaliseerd naar dezelfde instellingen.

Als u een andere operationele intentie wilt instellen voor clusters, moet u deze configureren in afzonderlijke vRealize Automation-datacenters, gekoppeld aan afzonderlijke vCenter-endpoints. U kunt bijvoorbeeld verschillende test- en productieclusters instellen.

- vRealize Operations Manager vraagt de toegestane plaatsing op bij vRealize Automation op basis van beleidsregels en reserveringen van vRealize Automation.
- Plaatsingstags van vRealize Operations Manager kunnen niet worden toegepast op ingerichte vRealize Automation-werklasten.

Verder wordt geplande optimalisatie met meerdere machines ondersteund. Regelmatige geplande optimalisaties zijn geen alles-of-niets-processen. Als machineverplaatsingen door omstandigheden worden onderbroken, blijven met succes verplaatste machines verplaatst en probeert vRealize Operations Manager in de volgende cyclus de resterende machines te verplaatsen, zoals gebruikelijk is voor vRealize Operations Manager. Een gedeeltelijk voltooide optimalisatie heeft geen negatieve invloed op vRealize Automation.

Zoeken naar onevenwichtige werklasten in vRealize Automation

vRealize Automation kan detecteren wanneer te veel werklasten in hetzelfde cluster zijn ingericht.

Procedure

- 1 Klik op **Infrastructuur > Computerbronnen > Computerbronnen** om te zien waar werklasten zijn ingericht.

Let op een onevenwichtige plaatsing van machines.

- 2 Reserveringen kunnen tot zware belasting van één cluster leiden. Klik op **Infrastructuur > Reserveringen > Reserveringen** om de reserveringen te bekijken.

Let op de prioriteit en welke invloed dit kan hebben op de plaatsing van machines.

Continue optimalisatie inschakelen

Wanneer u de vRealize Automation-adapter toevoegt in vRealize Operations Manager, maakt vRealize Operations Manager automatisch een nieuw, apart datacenter aan voor vRealize Automation-werklasten.

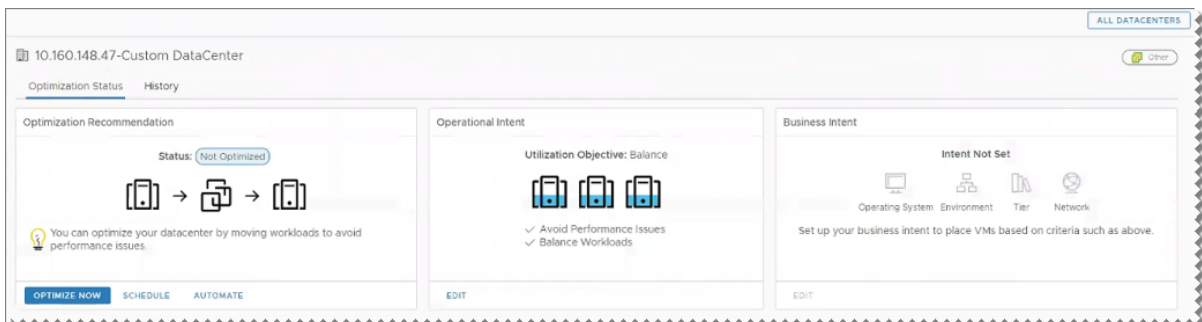
Behalve het toevoegen van de adapter zijn geen afzonderlijke installatiestappen vereist voor continue optimalisatie. U kunt beginnen met het configureren en gebruiken van vRealize Operations Manager voor het verplaatsen van werklasten in het nieuwe datacenter. Zie de [Voorbeeld van continue optimalisatie](#).

Voorbeeld van continue optimalisatie

Het volgende voorbeeld toont een herverdeling van de werkstroom voor continue optimalisatie van vRealize Automation met vRealize Operations Manager.

- 1 Klik op de startpagina van vRealize Operations Manager op **Optimalisatie van werkbelasting**.
- 2 Selecteer het automatisch gemaakte vRealize Automation-datacenter.
- 3 Klik onder **Operationele intentie** op **Bewerken** en selecteer **Verdelen**.

Het is niet mogelijk om Bedrijfsintentie te selecteren of te bewerken, die wordt gedeactiveerd bij een datacenter voor vRealize Automation-optimalisatie.

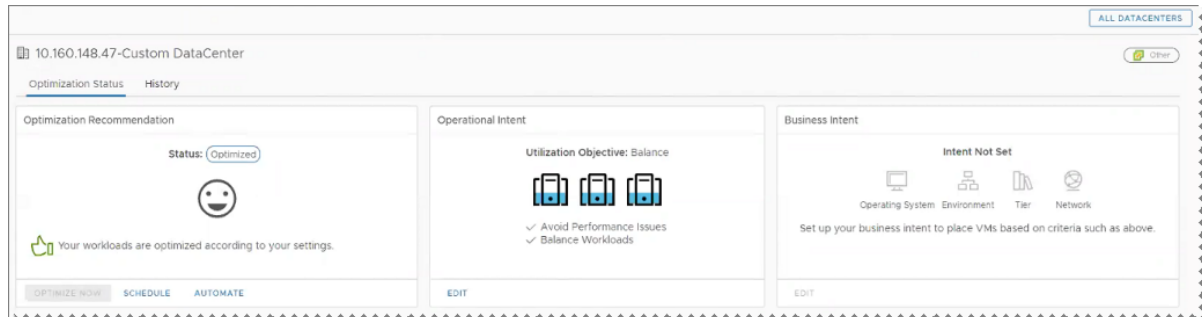


- 4 Klik onder **Aanbeveling voor optimalisatie** op **Nu optimaliseren**.
vRealize Operations Manager toont een voor-en-na-diagram van de voorgestelde bewerking.
- 5 Klik op **Volgende**.
- 6 Klik op **Actie beginnen**.
- 7 Controleer de uitgevoerde bewerking in vRealize Automation door op **Implementaties** te klikken en de gebeurtenisstatus te bekijken.

Events Request inputs			
#7 - Relocate RRD-WLP-003 In Progress Requested by: System User Requested for: Fritz Arbeiter Requested on: August 13, 2018 11:43 AM			
Tasks	Component	Status	Depends On
Submitted	Deployment	Successful	
Pre-approval	Deployment	Approved	
Relocate	Deployment	In Progress	
Post-approval	Deployment		
Completed	Deployment		

Wanneer de herverdeling is voltooid, wordt vRealize Automation vernieuwd. De pagina Computerbronnen toont dat er machines zijn verplaatst.

In vRealize Operations Manager vernieuwt de volgende gegevensverzameling de weergave om te tonen dat de optimalisatie is voltooid.



U kunt de bewerking in vRealize Operations Manager bekijken door te klikken op **Beheer > Geschiedenis > Recente taken**.

vRealize Automation-datacenters zoeken in vRealize Operations Manager

U kunt vRealize Operations Manager gebruiken om alleen de beheerde vRealize Automation-datacenters weer te geven.

Procedure

- 1 Klik op de startpagina van vRealize Operations Manager op **Optimalisatie van werkbelasting**.
- 2 Klik rechtsboven op het vervolgkeuzemenu **Weergave**.
- 3 Selecteer alleen de beheerde vRealize Automation-datacenters.



Sleutelparen beheren

Sleutelparen worden gebruikt om een cloudinstantie in te richten en ermee verbinding te maken. Een sleutelpaar wordt gebruikt om Windows-wachtwoorden te ontsleutelen of om aan te melden bij een Linux-machine.

Sleutelparen zijn vereist voor inrichting met Amazon Web Services. Voor Red Hat OpenStack zijn sleutelparen optioneel.

Bestaande sleutelparen worden geïmporteerd als deel van de gegevensverzameling wanneer u een cloudeindpunt toevoegt. Een materiaalbeheerder kan ook sleutelparen maken en beheren met behulp van de vRealize Automation-console. Als u een sleutelpaar verwijdert uit de vRealize Automation-console, wordt dit ook verwijderd uit het cloudserviceaccount.

Naast het handmatig beheren van sleutelparen kunt u vRealize Automation configureren om sleutelparen automatisch te genereren per machine of per bedrijfsgroep.

- Een materiaalbeheerder kan het automatisch genereren van sleutelparen configureren op het niveau van een reservering.
- Als een sleutelbaar zal worden beheerd op het blueprintniveau, moet de materiaalbeheerder **Niet opgegeven** inschakelen op de reservering.
- Een tenantbeheerder of bedrijfsgroepbeheerder kan het automatisch genereren van sleutelparen configureren op het niveau van een blueprint.
- Als het genereren van sleutelparen is geconfigureerd op reserverings- en blueprintniveau, dan overschrijft de reserveringsinstelling de blueprintinstelling.

Een sleutelbaar maken

U kunt vRealize Automation gebruiken om sleutelparen te maken ten behoeve van endpoints.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Maak een cloudendpoint en voeg de computerbronnen voor de cloud toe aan een materiaalgroep. Zie [Een endpointscenario kiezen](#) en [Een materiaalgroep maken](#).

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Sleutelparen**.
- 2 Klik op **Nieuw**.
- 3 Geef een naam op in het tekstvak **Naam**.
- 4 Selecteer een cloudregio in het vervolgkeuzemenu **Computerbron**.
- 5 Klik op **OK**.

Resultaten

Het sleutelbaar is klaar voor gebruik wanneer de kolom Geheime sleutel de waarde ***** bevat.

De persoonlijke sleutel uploaden voor een sleutelbaar

U kunt de persoonlijke sleutel voor een sleutelbaar uploaden in de PEM-indeling.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- U moet al over een sleutelbaar beschikken. Zie [Een sleutelbaar maken](#).

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Sleutelparen**.

- 2 Zoek het sleutelpaar waarvoor u een persoonlijke sleutel wilt uploaden.
- 3 Klik op het pictogram **Bewerken** (✎).
- 4 Gebruik een van de volgende methodes om de sleutel te uploaden.
 - Blader naar een bestand in PEM-indeling en klik op **Uploaden**.
 - Plak de tekst van de persoonlijke sleutel, beginnend met -----BEGIN RSA PRIVATE KEY----- en eindigend met -----END RSA PRIVATE KEY-----.
- 5 Klik op het pictogram **Opslaan** (✓).

De persoonlijke sleutel van een sleutelpaar exporteren

U kunt de persoonlijke sleutel van een sleutelpaar exporteren naar een PEM-gecodeerd bestand.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Er moet een sleutelpaar met een persoonlijke sleutel bestaan. Zie [De persoonlijke sleutel uploaden voor een sleutelpaar](#).

Procedure

- 1 Selecteer **Infrastructuur > Reserveringen > Sleutelparen**.
- 2 Zoek naar het sleutelpaar waarvan u de persoonlijke sleutel wilt exporteren.
- 3 Klik op het pictogram **Exporteren** (📄➔).
- 4 Ga naar de locatie waarop u het bestand wilt opslaan en klik op **Opslaan**.

Scenario: een locatie toewijzen aan een computerbron voor interregionale implementaties

Als materiaalbeheerder wilt u uw computerbronnen labelen als toebehorend aan het datacenter in Boston of in Londen, ter ondersteuning van interregionale implementaties. Wanneer uw blueprintarchitecten de locatiefunctie in hun blueprint inschakelen, kunnen gebruikers kiezen of ze machines willen inrichten in het datacenter in Boston of in Londen.



U hebt een datacenter in Londen en een datacenter in Boston en u wilt voorkomen dat gebruikers in Boston machines inrichten op de infrastructuur in Londen en omgekeerd. Om ervoor te zorgen dat uw gebruikers in Boston machines inrichten op uw infrastructuur voor Boston (en gebruikers in Londen de infrastructuur van Londen gebruiken), is het aan te raden gebruikers de juiste locatie te laten selecteren voor de inrichting wanneer ze machines aanvragen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **materiaalbeheerder**.
- Als systeembeheerder definieert u de locaties van de datacenters. Zie [Scenario: datacenterlocaties toevoegen voor interregionale implementaties](#).

Procedure

- 1 Selecteer **Infrastructuur > Computerbronnen > Computerbronnen**.
- 2 Wijs de computerbron in het datacenter in Boston aan en klik op **Bewerken**.
- 3 Selecteer Boston in het vervolgkeuzemenu **Locaties**.
- 4 Klik op **OK**.
- 5 Herhaal deze procedure zo vaak als nodig voor het koppelen van uw computerbronnen aan de locaties Boston en Londen.

Resultaten

IaaS-architecten kunnen locatiefuncties inschakelen, zodat gebruikers de optie hebben om machines in te richten in Londen of Boston bij het invullen van aanvraagformulieren voor catalogusitems. Zie [Gebruikers datacenterlocaties laten selecteren voor interregionale implementaties](#).

Een vRealize Automation-implementatie inrichten met een externe IPAM-provider

U kunt IP-adressen en -bereiken voor gebruik in een vRealize Automation-netwerkprofiel verkrijgen van de provider van een ondersteunde externe IPAM-oplossing, zoals Infoblox.

De IP-adresbereiken in het netwerkprofiel worden gebruikt in een gekoppelde reservering, die u kunt opgeven in een blueprint. Wanneer een gemachtigde gebruiker de inrichting van een machine aanvraagt via het catalogusitem van de blueprint, wordt een IP-adres verkregen uit het door de externe IPAM opgegeven bereik met IP-adressen. Nadat de machine is geïmplementeerd, kunt u de gebruikte IP-adressen vinden door een query uit te voeren op de pagina met itemdetails van vRealize Automation.

Tabel 2-19. Voorbereiding voor de inrichting van een vRealize Automation-implementatie met IPAM-checklist van Infoblox

Taak	Beschrijving	Details
De invoegtoepassing of het pakket van de provider van de externe IPAM-oplossing verkrijgen, importeren en configureren.	Verkrijg en importeer de invoegtoepassing vRealize Orchestrator, voer de configuratiewerkstromen van vRealize Orchestrator uit en registreer het endpointtype van de IPAM-provider in vRealize Orchestrator. Als de VMware Solution Exchange op https://marketplace.vmware.com/vsx niet het benodigde pakket van de IPAM-provider bevat, kunt u uw eigen pakket maken met behulp van een IPAM Solution Provider SDK en ondersteuningsdocumentatie. Zie de pagina vRealize Automation Example Third-Party IPAM Package op code.vmware.com/web/sdk .	Zie Checklist voor het bieden van ondersteuning voor externe IPAM-providers .
Een endpoint voor de provider van de externe IPAM-oplossing maken.	Maak een nieuw IPAM-endpoint in vRealize Automation.	Zie Een endpoint van een externe IPAM-provider maken .
Endpointinstellingen voor de provider van de externe IPAM-oplossing opgeven in een extern netwerkprofiel.	Maak een extern netwerkprofiel en geef het gedefinieerde IPAM-endpoint op in vRealize Automation.	Zie Een extern netwerkprofiel maken via een externe IPAM-provider .
(Optioneel) Endpointinstellingen voor de provider van de externe IPAM-oplossing opgeven in een gerouteerd netwerkprofiel.	Maak een profiel voor een netwerk op aanvraag en geef het gedefinieerde IPAM-endpoint op in vRealize Automation.	Zie Een geleid netwerkprofiel maken met een IPAM-endpoint van derden of Een NAT-netwerkprofiel maken met een extern IPAM-endpoint in vRealize Automation .
Een reservering voor het gebruik van het netwerkprofiel definiëren.	Maak een reservering die het netwerkprofiel oproept in vRealize Automation.	Zie Een reservering maken voor Hyper-V, KVM, SCVMM, vSphere of XenServer .
Een blueprint definiëren die gebruikmaakt van het netwerkprofiel.	Maak een blueprint die gebruikmaakt van de reservering in vRealize Automation.	Zie Hoofdstuk 3 Serviceblueprints aanbieden aan gebruikers .
De blueprint in de catalogus publiceren om deze beschikbaar te maken voor gebruik.	Publiceer de blueprint in de catalogus van vRealize Automation. Voeg eventueel benodigde rechten toe.	Zie Een blueprint publiceren .
De inrichting van de machine aanvragen met het catalogusitem voor de blueprint.	Gebruik het catalogusitem voor de blueprint om de inrichting van een machine in vRealize Automation aan te vragen.	Zie De servicecatalogus beheren .

XaaS-bronnen configureren

Door XaaS-endpoints te configureren, kunt u vRealize Automation verbinden met uw omgeving. Wanneer u vRealize Orchestrator-invoegtoepassingen configureert als endpoint, gebruikt u de

vRealize Automation-gebruikersinterface voor het configureren van de invoegtoepassingen in plaats van de vRealize Orchestrator-configuratie-interface.

Als u vRealize Orchestrator-mogelijkheden en de vRealize Orchestrator-invoegtoepassingen wilt gebruiken om VMware-technologie en technologie van derden beschikbaar te maken voor vRealize Automation, kunt u de vRealize Orchestrator-invoegtoepassingen configureren door de invoegtoepassingen toe te voegen als endpoint. Hierdoor kunt u verbindingen tot stand brengen met verschillende hosts en servers, zoals vCenter Server-instanties, een Microsoft Active Directory-host, enzovoort.

Wanneer u een vRealize Orchestrator-invoegtoepassing toevoegt als endpoint met behulp van de vRealize Automation-gebruikersinterface, voert u een configuratiewerkstroom uit op de vRealize Orchestrator-server. De configuratiewerkstromen bevinden zich in de werkstroommap **vRealize Automation > XaaS > Endpoint Configuration**.

Belangrijk Het configureren van één invoegtoepassing in vRealize Orchestrator en in de vRealize Automation-console wordt niet ondersteund en heeft fouten tot gevolg.

De Active Directory-invoegtoepassing configureren als endpoint

U voegt een endpoint toe en configureert de Active Directory-invoegtoepassing om een verbinding tot stand te brengen met een actieve Active Directory-instantie en om gebruikers en groepen, Active Directory-computers, organisatie-eenheden, enzovoort te beheren.

Nadat u een Active Directory-endpoint hebt toegevoegd, kunt u het op elk gewenst moment bijwerken.

Voorwaarden

- Controleer of u toegang hebt tot een Microsoft Active Directory-instantie. Zie de Microsoft Active Directory-documentatie.
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > vRO-configuratie > Endpoints**.
- 2 Klik op het pictogram **Nieuw (+)**.
- 3 Selecteer in het vervolgkeuzemenu **Invoegtoepassing** de optie **Active Directory**.
- 4 Klik op **Volgende**.
- 5 Voer een naam in en desgewenst een beschrijving.
- 6 Klik op **Volgende**.

7 Configureer de details van de Active Directory-server.

- a Voer in het tekstvak **IP/URL van Active Directory-host** het IP-adres of de DNS-naam in van de host waarop Active Directory wordt uitgevoerd.

- b Typ de opzoekpoort van de Active Directory-server in het tekstvak **Poort**.

vRealize Orchestrator ondersteunt de hiërarchische domeinstructuur van Active Directory. Als uw domeincontroller is geconfigureerd voor de globale catalogus, moet u poort 3268 gebruiken. U kunt standaardpoort 389 niet gebruiken om verbinding te maken met de globale-catalogusserver. Naast poorten 389 en 3268 kunt u 636 gebruiken voor LDAPS.

- c Typ het hoofdelement van de Active Directory-service in het tekstvak **Root**.

Als uw domeinnaam bijvoorbeeld *mycompany.com* is, is het Active Directory-hoofdelement **dc=mycompany,dc=com**.

Dit knooppunt wordt gebruikt voor het bladeren door de servicedirectory nadat u de vereiste verificatiegegevens hebt ingevoerd. Voor grote servicedirectory's wordt het zoekbereik verkleind als u een knooppunt in de structuur opgeeft. Dit verbetert ook de prestaties. In plaats van bijvoorbeeld in de volledige directory te zoeken, kunt u **ou=employees,dc=mycompany,dc=com** opgeven. Met dit hoofdelement worden alle gebruikers in de groep Employees weergegeven.

- d (Optioneel) Als u versleutelde certificering wilt activeren voor de verbinding tussen vRealize Orchestrator en Active Directory, selecteert u **Ja** in het vervolgkeuzemenu **SSL gebruiken**.

Het SSL-certificaat wordt automatisch geïmporteerd zonder dat u om bevestiging wordt gevraagd, zelfs wanneer het certificaat automatisch ondertekenend is.

- e (Optioneel) Voer het domein in het tekstvak **Standaarddomein** in.

Als uw domeinnaam *mycompany.com* is, typt u bijvoorbeeld **@mycompany.com**.

8 Configureer de instellingen voor gedeelde sessies.

De verificatiegegevens worden door vRealize Orchestrator gebruikt om alle Active Directory-werkstromen en -acties uit te voeren.

- a Geef de gebruikersnaam voor de gedeelde sessie op in het tekstvak **Gebruikersnaam voor de gedeelde sessie**.

- a Geef het wachtwoord voor de gedeelde sessie op in het tekstvak **Wachtwoord voor de gedeelde sessie**.

9 Klik op **Voltooien**.

Resultaten

U hebt een Active Directory-instantie als endpoint toegevoegd. XaaS-architecten kunnen XaaS gebruiken voor het publiceren van werkstromen voor Active Directory-invoegtoepassingen als catalogusitems en bronacties.

Wat nu te doen

- Als u vRealize Automation-blueprints wilt gebruiken om de Active Directory-gebruikers in uw omgeving te beheren, maakt u een XaaS-blueprint op basis van Active Directory. Zie [Een XaaS-blueprint en -actie maken voor het maken en wijzigen van een gebruiker](#) voor een voorbeeld.
- Als u vRealize Automation wilt gebruiken om Active Directory-records te maken wanneer een machine wordt geïmplementeerd, kunt u meer dan één Active Directory-beleid maken en een verschillend beleid toepassen op verschillende bedrijfsgroepen en blueprints. Zie [Active Directory-beleid maken en toepassen](#).

De HTTP-REST-invoegtoepassing configureren als endpoint

U kunt een endpoint toevoegen en de HTTP-REST-invoegtoepassing configureren om verbinding te maken met een REST-host.

Voorwaarden

- Meld u bij vRealize Automation aan als **tenantbeheerder**.
- Controleer of u toegang hebt tot een REST-host.

Procedure

- 1 Selecteer **Beheer > vRO-configuratie > Endpoints**.
- 2 Klik op het pictogram **Nieuw (+)**.
- 3 Selecteer **HTTP-REST** in het vervolgkeuzemenu **Invoegtoepassing**.
- 4 Klik op **Volgende**.
- 5 Voer een naam in en desgewenst een beschrijving.
- 6 Klik op **Volgende**.
- 7 Geef de informatie over de REST-host op.
 - a Geef de naam van de host op in het tekstvak **Naam**.
 - b Geef het adres van de host op in het tekstvak **URL**.

Opmerking Als u Kerberos-toegangsverificatie gebruikt, moet u het hostadres opgeven in FQDN-indeling.

- c (Optioneel) Geef het aantal seconden op voordat een time-out optreedt voor een verbinding in het tekstvak **Time-out bij verbinding (seconden)**.

De standaardwaarde is 30 seconden.

- d (Optioneel) Geef het aantal seconden op voordat een time-out optreedt voor een bewerking in het tekstvak **Time-out bij bewerking (seconden)**.

De standaardwaarde is 60 seconden.

8 (Optioneel) Configureer de proxyinstellingen.

- a Selecteer **Ja** in het vervolgkeuzemenu **Proxy gebruiken** als u een proxy wilt gebruiken.
- b Typ het IP-adres van de proxyserver in het tekstvak **Proxyadres**.
- c Voer het poortnummer in voor communicatie met de externe proxyserver in het tekstvak **Proxypoort**.

9 Klik op **Volgende**.**10** Selecteer het verificatietype.

Optie	Actie
Geen	Er is geen verificatie vereist.
OAuth 1.0	<p>Gebruikt het OAuth 1.0-protocol. U moet de vereiste verificatieparameters opgeven onder OAuth 1.0.</p> <ul style="list-style-type: none"> a Geef de sleutel op die wordt gebruikt voor het identificeren van de consument als serviceprovider in het tekstvak Consumentensleutel. b Geef het geheim op om eigendom van de consumentensleutel vast te stellen in het tekstvak Consumentengeheim. c (Optioneel) Geef het toegangstoken op dat de consument gebruikt om toegang te krijgen tot de beveiligde bronnen in het tekstvak Toegangstoken. d (Optioneel) Geef het geheim op dat de consument gebruikt om eigendom te bevestigen van een token in het tekstvak Geheim voor toegangstoken.
OAuth 2.0	<p>Gebruikt het OAuth 2.0-protocol.</p> <p>Typ het verificatietoken in het tekstvak Token.</p>
Basis	<p>Biedt basistoegangsverificatie. De communicatie met de host vindt in de gedeelde-sessiemodus plaats.</p> <ul style="list-style-type: none"> a Geef de naam voor de gedeelde sessie op in het tekstvak Gebruikersnaam voor verificatie. b Geef het wachtwoord voor de gedeelde sessie op in het tekstvak Wachtwoord voor verificatie.
Verificatiesamenvatting	<p>Biedt samengevatte toegangsverificatie die gebruikmaakt van versleuteling. De communicatie met de host vindt in de gedeelde-sessiemodus plaats.</p> <ul style="list-style-type: none"> a Geef de naam voor de gedeelde sessie op in het tekstvak Gebruikersnaam voor verificatie. b Geef het wachtwoord voor de gedeelde sessie op in het tekstvak Wachtwoord voor verificatie.

Optie	Actie
NTLM	<p>Biedt NT LAN Manager-toegangsverificatie (NTLM) binnen de Windows Security Support Provider-structuur (SSP). De communicatie met de host vindt in de gedeelde-sessiemodus plaats.</p> <ol style="list-style-type: none"> Geef de verificatiegegevens van de gebruiker op voor de gedeelde sessie. <ul style="list-style-type: none"> Geef de naam voor de gedeelde sessie op in het tekstvak Gebruikersnaam voor verificatie. Geef het wachtwoord voor de gedeelde sessie op in het tekstvak Wachtwoord voor verificatie. Configureer de NTLM-gegevens <ul style="list-style-type: none"> (Optioneel) Voer de naam van het werkstation in het tekstvak Werkstation voor NTLM-verificatie in. Voer de domeinnaam in het tekstvak Domein voor NTLM-verificatie in.
Kerberos	<p>Biedt Kerberos-toegangsverificatie. De communicatie met de host vindt in de gedeelde-sessiemodus plaats.</p> <ol style="list-style-type: none"> Geef de naam voor de gedeelde sessie op in het tekstvak Gebruikersnaam voor verificatie. Geef het wachtwoord voor de gedeelde sessie op in het tekstvak Wachtwoord voor verificatie.

11 Klik op **Voltooien**.

Resultaten

U hebt het endpoint geconfigureerd en een REST-host toegevoegd. XaaS-architecten kunnen XaaS gebruiken voor het publiceren van werkstromen voor HTTP-REST-invoegtoepassingen als catalogusitems en bronacties.

De PowerShell-invoegtoepassing configureren als endpoint

U kunt een endpoint toevoegen en de PowerShell-invoegtoepassing configureren om een verbinding te maken met een actieve PowerShell-host zodat u PowerShell-scripts en cmdlets kunt aanroepen via vRealize Orchestrator-acties en -werkstromen.

Voorwaarden

- Controleer of u toegang hebt tot een Windows PowerShell-host. Zie de Windows PowerShell-documentatie voor meer informatie over Microsoft Windows PowerShell.
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- Selecteer **Beheer > vRO-configuratie > Endpoints**.
- Klik op het pictogram **Nieuw (+)**.
- Selecteer **PowerShell** in het vervolgkeuzemenu **Invoegtoepassing**.
- Klik op **Volgende**.

- 5 Voer een naam in voor het PowerShell-endpoint.
- 6 (Optioneel) Geef een beschrijving op voor het PowerShell-endpoint.
- 7 Klik op **Volgende**.
- 8 Geef de PowerShell-hostgegevens op.
 - a Geef de naam van de host op in het tekstvak **Naam**.
 - b Voer het IP-adres of de FQDN van de host in het tekstvak **Host/IP** in.
- 9 Configureer de WinRM-instellingen voor de PowerShell-host.
 - a Voer het poortnummer voor communicatie met de host in het tekstvak **Poort** in, in het gedeelte met de PowerShell-hostgegevens.
 - b Selecteer een transportprotocol in het vervolgkeuzemenu **Transportprotocol**.

Opmerking Als u het HTTPS-transportprotocol gebruikt, wordt het certificaat van de externe PowerShell-host geïmporteerd in de vRealize Orchestrator-keystore.

 - c Selecteer het verificatietype in het vervolgkeuzemenu **Verificatie**.

Opmerking Als u Kerberos-verificatie wilt gebruiken, moet u deze voor de WinRM-service inschakelen. Zie *De PowerShell-invoegtoepassing gebruiken* voor informatie over het configureren van Kerberos-verificatie.

- 10 Voer de verificatiegegevens in voor communicatie in een gedeelde sessie met de PowerShell-host in de tekstvakken **Gebruikersnaam** en **Wachtwoord**.
- 11 Klik op **Voltooien**.

Resultaten

U hebt een Windows PowerShell-host als endpoint toegevoegd. XaaS-architecten kunnen de XaaS gebruiken voor het publiceren van werkstromen voor PowerShell-invoegtoepassingen als catalogusitems en bronacties.

De SOAP-invoegtoepassing configureren als endpoint

U kunt een endpoint toevoegen en de SOAP-invoegtoepassing configureren om een SOAP-service te definiëren als inventarisobject, zodat u SOAP-bewerkingen kunt uitvoeren voor de gedefinieerde objecten.

Voorwaarden

- Controleer of u toegang hebt tot een SOAP-host. De invoegtoepassing ondersteunt SOAP-versie 1.1 en 1.2 en WSDL 1.1 en 2.0.
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > vRO-configuratie > Endpoints**.

- 2 Klik op het pictogram **Nieuw (+)**.
- 3 Selecteer **SOAP** in het vervolgkeuzemenu **Invoegtoepassing**.
- 4 Klik op **Volgende**.
- 5 Voer een naam in en desgewenst een beschrijving.
- 6 Klik op **Volgende**.
- 7 Geef de gegevens voor de SOAP-host op.
 - a Geef de naam van de host op in het tekstvak **Naam**.
 - b Selecteer of de WSDL-inhoud als tekst moet worden opgegeven via het vervolgkeuzemenu **WSDL-inhoud opgeven**.

Optie	Actie
Ja	Voer de WSDL-tekst in het tekstvak WSDL-inhoud in.
Nee	Voer het juiste pad in het tekstvak WSDL-URL in.

- c (Optioneel) Geef het aantal seconden op voordat een time-out optreedt voor een verbinding in het tekstvak **Time-out bij verbinding (in seconden)**.
De standaardwaarde is 30 seconden.
 - d (Optioneel) Geef het aantal seconden op voordat een time-out optreedt voor een bewerking in het tekstvak **Time-out bij aanvraag (seconden)**.
De standaardwaarde is 60 seconden.
- 8 (Optioneel) Geef de proxyinstellingen op.
 - a Als u een proxy wilt gebruiken, selecteert u **Ja** in het vervolgkeuzemenu **Proxy**.
 - b Typ het IP-adres van de proxyserver in het tekstvak **Adres**.
 - c Voer het poortnummer in voor communicatie met de proxyserver in het tekstvak **Proxy**.
- 9 Klik op **Volgende**.
- 10 Selecteer het verificatietype.

Optie	Actie
Geen	Er is geen verificatie vereist.
Basis	Biedt basistoegangsverificatie. De communicatie met de host vindt in de gedeelde-sessiemodus plaats. <ol style="list-style-type: none"> a Geef de naam voor de gedeelde sessie op in het tekstvak Gebruikersnaam. b Geef het wachtwoord voor de gedeelde sessie op in het tekstvak Wachtwoord.

Optie	Actie
Verificatiesamenvatting	Biedt samengevatte toegangsverificatie die gebruikmaakt van versleuteling. De communicatie met de host vindt in de gedeelde-sessiemodus plaats. <ol style="list-style-type: none"> Geef de naam voor de gedeelde sessie op in het tekstvak Gebruikersnaam. Geef het wachtwoord voor de gedeelde sessie op in het tekstvak Wachtwoord.
NTLM	Biedt NT LAN Manager-toegangsverificatie (NTLM) in de Windows Security Support Provider-structuur (SSP). De communicatie met de host vindt in de gedeelde-sessiemodus plaats. <ol style="list-style-type: none"> Geef de gebruikersreferenties op. <ul style="list-style-type: none"> Geef de naam voor de gedeelde sessie op in het tekstvak Gebruikersnaam. Geef het wachtwoord voor de gedeelde sessie op in het tekstvak Wachtwoord. Geef de NTLM-instellingen op. <ul style="list-style-type: none"> Voer de domeinnaam in het tekstvak NTLM-domein in. (Optioneel) Voer de naam van het werkstation in het tekstvak NTLM-werkstation in.
Onderhandelen	Biedt Kerberos-toegangsverificatie. De communicatie met de host vindt in de gedeelde-sessiemodus plaats. <ol style="list-style-type: none"> Geef de gebruikersreferenties op. <ol style="list-style-type: none"> Geef de naam voor de gedeelde sessie op in het tekstvak Gebruikersnaam. Geef het wachtwoord voor de gedeelde sessie op in het tekstvak Wachtwoord. Voer de SPN van de Kerberos-service in het tekstvak SPN van Kerberos-service in.

11 Klik op **Voltooien**.

Resultaten

U hebt een SOAP-service toegevoegd. XaaS-architecten kunnen XaaS gebruiken voor het publiceren van werkstromen voor SOAP-invoegtoepassingen als catalogusitems en bronacties.

De vCenter Server-invoegtoepassing configureren als endpoint

U kunt een endpoint toevoegen en de vCenter Server-invoegtoepassing configureren om een verbinding te maken met een actieve vCenter Server-instantie, voor het maken van XaaS-blueprints die vSphere-inventarisobjecten beheren.

Voorwaarden

- Installeer en configureer vCenter Server. Zie *vSphere installeren en instellen*.
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > vRO-configuratie > Endpoints**.

- 2 Klik op het pictogram **Nieuw (+)**.
- 3 Selecteer **vCenter Server** in het vervolgkeuzemenu **Invoegtoepassing**.
- 4 Klik op **Volgende**.
- 5 Voer een naam in en desgewenst een beschrijving.
- 6 Klik op **Volgende**.
- 7 Geef de informatie over de vCenter Server-instantie op.
 - a Voer het IP-adres of de DNS-naam in van de machine in het tekstvak **IP-adres of hostnaam van de vCenter Server-instantie die u wilt toevoegen**.

Dit is het IP-adres of de DNS-naam van de machine waarop de vCenter Server-instantie is geïnstalleerd die u wilt toevoegen.
 - b Voeg de poort in voor communicatie met de vCenter Server-instantie in het tekstvak **Poort van de vCenter Server-instantie**.

De standaardpoort is 443.
 - c Voer de locatie in van de SDK die u wilt gebruiken om verbinding te maken met de vCenter Server-instantie in het tekstvak **Locatie van de SDK die u gebruikt om verbinding te maken met de vCenter Server-instantie**.

Bijvoorbeeld: `/sdk`.
- 8 Klik op **Volgende**.
- 9 Geef de verbindingsparameters op.
 - a Voer de HTTP-poort van de vCenter Server-instantie in het tekstvak **HTTP-poort van de vCenter Server-instantie - van toepassing op VC-invoegtoepassing, versie 5.5.2 of eerder** in.
 - b Voer de verificatiegegevens in voor vRealize Orchestrator die worden gebruikt om de verbinding tot stand te brengen met de vCenter Server-instantie, in het tekstvak **Gebruikersnaam van de gebruiker die Orchestrator gebruikt om verbinding te maken met de vCenter Server-instantie** en **Wachtwoord van de gebruiker dat Orchestrator gebruikt om verbinding te maken met de vCenter Server-instantie**.

De gebruiker die u selecteert, moet een geldige gebruiker zijn met privileges voor het beheren van vCenter Server-extensies en een set aangepaste privileges.
- 10 Klik op **Voltooien**.

Resultaten

U hebt een vCenter Server-instantie toegevoegd als endpoint. XaaS-architecten kunnen de XaaS gebruiken voor het publiceren van werkstromen voor vCenter Server-invoegtoepassingen als catalogusitems en bronacties.

Een Microsoft Azure-endpoint maken

U kunt een Microsoft Azure-endpoint maken om een geverifieerde verbinding tussen vRealize Automation en een Azure-implementatie te vergemakkelijken.

Een endpoint brengt een verbinding tot stand met een bron, in dit geval een Azure-instantie, die u kunt gebruiken voor het maken van blueprints voor virtual machines. U moet een Azure-endpoint hebben om te gebruiken als basis van blueprints voor het inrichten van Azure virtual machines. Als u meerdere Azure-abonnementen gebruikt, hebt u voor elke abonnements-id een endpoint nodig.

U kunt ook rechtstreeks een Azure-verbinding tot stand brengen vanuit vRealize Orchestrator door middel van de opdracht Een Azure-verbinding toevoegen onder **Bibliotheek > Azure > Configuratie** in de vRealize Orchestrator-workflowstructuur. In de meeste gevallen is de hierin beschreven verbinding door middel van de endpoint-configuratie de beste optie.

Azure-endpoints worden ondersteund door vRealize Orchestrator- en XaaS-functionaliteit. U kunt een Azure-endpoint maken, verwijderen en bewerken. Als u een bestaand endpoint wijzigt en gedurende meerdere uren geen updates uitvoert op de Azure-portal via de bijgewerkte verbinding, kunnen er problemen optreden. U moet de service vRealize Orchestrator opnieuw starten met behulp van de opdracht service vco-service restart. Als u dat niet doet, kunnen er fouten optreden.

Voorwaarden

- Configureer een Microsoft Azure-instantie en verkrijg een geldig Microsoft Azure-abonnement waarvan u de abonnements-id kunt gebruiken. Zie [Microsoft Azure-endpointconfiguratie](#) voor meer informatie over het configureren van Azure en het verkrijgen van een abonnements-id.
- Controleer of uw vRealize Automation-implementatie ten minste één tenant en één bedrijfsgroep heeft.
- Maak een Active Directory-toepassing zoals beschreven in <https://azure.microsoft.com/nl-nl/documentation/articles/resource-group-create-service-principal-portal>.
- Noteer de volgende Azure-gegevens. U hebt deze nodig tijdens de configuratie van het endpoint en de blueprint.
 - abonnements-id
 - tenant-id
 - naam opslagaccount
 - naam brongroep
 - locatie
 - naam virtual machine
 - clienttoepassings-id
 - geheime sleutel clienttoepassing

- image-URN van virtual machine
- De vRealize Automation Azure-implementatie ondersteunt een subset van de regio's die door Microsoft Azure worden ondersteund. Zie [Door Azure ondersteunde regio's](#).
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > vRO-configuratie > Endpoints**.
- 2 Klik op het pictogram **Nieuw (+)**.
- 3 Klik op het tabblad Invoegtoepassing op het vervolgkeuzemenu **Invoegtoepassing** en selecteer **Azure**.
- 4 Klik op **Volgende**.
- 5 Voer een naam in en desgewenst een beschrijving.
- 6 Klik op **Volgende**.
- 7 Vul de tekstvakken op het tabblad Details in voor het endpoint.

Parameter	Beschrijving
Verbindingsinstellingen	
Verbindingsnaam	De unieke naam voor de nieuwe endpointverbinding. Deze naam wordt weergegeven in de vRealize Orchestrator-interface om u te helpen een bepaalde verbinding te identificeren.
Azure-abonnements-id	De id voor uw Azure-abonnement. Met deze id worden de opslagaccounts, virtual machines en andere Azure-bronnen waar u toegang toe hebt gedefinieerd.
Azure-omgeving	De geografische regio voor de geïmplementeerde Azure-bron. vRealize Automation ondersteunt alle huidige Azure-regio's op basis van de abonnements-id.
Instellingen bronbeheerder	
URI voor Azure-service	Dit is de URI die u nodig hebt voor toegang tot uw Azure-instantie. De standaardwaarde van <code>https://management.azure.com/</code> is doorgaans geschikt voor veel normale implementaties. Dit vakje wordt automatisch ingevuld wanneer u een omgeving selecteert.
Tenant-id	Dit is de Azure-tenant-id die het endpoint moet gebruiken.
Client-id	Dit is de Azure-client-id die het endpoint moet gebruiken. Deze wordt toegewezen wanneer u een Active Directory-toepassing maakt.

Parameter	Beschrijving
Clientgeheim	De sleutel die wordt gebruikt voor de Azure-client-id. Deze sleutel wordt toegewezen wanneer u een Active Directory-toepassing maakt.
Opslag-URI voor Azure	De URI via welke u toegang krijgt tot de opslaginstantie van Azure. Dit vakje wordt automatisch ingevuld wanneer u een omgeving selecteert.
Proxy-instellingen	
Proxy-host	Als uw bedrijf een proxyserver gebruikt, geeft u de hostnaam van die server op.
Proxypoort	Als uw bedrijf een proxyserver gebruikt, geeft u het poortnummer van die server op.

- 8** (Optioneel) Klik op Eigenschappen en voeg opgegeven aangepaste eigenschappen, eigenschapsgroepen of uw eigen eigenschapsdefinities toe.

- 9** Klik op **Voltooien**.

Wat nu te doen

Maak de toepasselijke brongroepen, opslagaccounts en netwerkbeveiligingsgroepen in Azure. Indien uw implementatie dit vereist, moet u tevens load balancers maken.

Actie	Opties
Een relevante brongroep maken	<ul style="list-style-type: none"> ■ Maak de brongroep via het Azure-portal. Raadpleeg de Azure-documentatie voor specifieke instructies. ■ Gebruik de van toepassing zijnde vRealize Orchestrator-werkstroom in de brongroep Bibliotheek/Azure/Bron/Maken. ■ Maak en publiceer in vRealize Automation een XaaS-blueprint die de vRealize Orchestrator-werkstroom bevat. U kunt de brongroep aanvragen nadat u deze aan de service en rechten hebt gekoppeld. <p>Opmerking Het brontype Brongroep wordt niet ondersteund of beheerd door vRealize Automation.</p>
Een Azure Storage-account maken	<ul style="list-style-type: none"> ■ Gebruik Azure om een opslagaccount te maken. Raadpleeg de Azure-documentatie voor specifieke instructies. ■ Gebruik de van toepassing zijnde vRealize Orchestrator-werkstroom in het opslagaccount Bibliotheek/Azure/Opslag/Maken. ■ Maak en publiceer in vRealize Automation een XaaS-blueprint die de vRealize Orchestrator-werkstroom bevat. U kunt het opslagaccount aanvragen nadat u dit aan de service en rechten hebt gekoppeld.
Een Azure-netwerkbeveiligingsgroep maken	<ul style="list-style-type: none"> ■ Gebruik Azure om een beveiligingsgroep te maken. Raadpleeg de Azure-documentatie voor specifieke instructies. ■ Gebruik de van toepassing zijnde vRealize Orchestrator-werkstroom in de beveiligingsgroep Bibliotheek/Azure/Netwerk/Netwerk maken. ■ Maak en publiceer in vRealize Automation een XaaS-blueprint die de vRealize Orchestrator-werkstroom bevat. U kunt de beveiligingsgroep aanvragen nadat u deze aan de service en rechten hebt gekoppeld.

Door Azure ondersteunde regio's

De vRealize Automation Azure-implementatie ondersteunt een subset van de regio's die door Microsoft Azure worden ondersteund.

De volgende Azure-regio's worden door de Azure-implementatie in vRealize Automation ondersteund.

■ Oost-Azië	■ Australië - oost
■ Zuidoost-Azië	■ Australië - zuidoost
■ VS - midden	■ Zuid-India
■ VS - oost	■ Centraal-India
■ VS - oost 2	■ West-India
■ VS - west	■ Canada Centraal
■ VS - west 2	■ Canada Oost
■ Noord-centraal VS	■ West-centraal VS
■ Zuid-centraal VS	■ Korea Centraal
■ Noord-Europa	■ Korea Zuid
■ West-Europa	■ VK West
■ Japan - west	■ VK Zuid
■ Japan - oost	■ Oost-China
■ Brazilië - zuid	■ Noord-China

Containers maken en configureren

U kunt het tabblad Containers in vRealize Automation gebruiken om de geïntegreerde toepassing Containers voor vRealize Automation te openen en de containers en netwerkinstellingen van containers te maken en te configureren, zodat deze beschikbaar zijn voor architecten van vRealize Automation-blueprints.

U kunt containers definiëren door nieuwe en bestaande sjablonen en images te gebruiken in de geïntegreerde toepassing Containers. U kunt vervolgens containeronderdelen en hun bijbehorende netwerkinstellingen toevoegen aan vRealize Automation-blueprints.

Containerhosts en clusters beheren

U kunt de hosts die u toevoegt vanaf de pagina Clusters weergeven en beheren. In de context van Containers is de host een virtual machine of infrastructuur waarmee u containers kunt uitvoeren.

De pagina Clusters, op het tabblad infrastructuur, bevat de besturingselementen voor het toevoegen van nieuwe clusters en hosts. Als u een host in de omgeving Containers wilt toevoegen, moet u deze aan een cluster toevoegen. U kunt de status van provisioning-aanvragen van bestaande hosts controleren en gebeurtenislogboeken weergeven voor uw containers vanuit elke pagina in de tabbladen Bibliotheek en Implementaties. De vensters Aanvragen en Gebeurtenislogboek bevinden zich aan de rechterkant van de pagina.

Een containerhostcluster maken

U moet een host toevoegen aan een cluster om containers te implementeren.

Voorwaarden

Selecteer een bedrijfsgroep in de linkerbovenhoek van het tabblad Containers.

Procedure

- 1 Meld u aan bij de vRealize Automation-console als **containerbeheerder**.

- 2 Klik op het tabblad **Containers**.
- 3 Klik op **Infrastructuur > Containerhostclusters**.
- 4 Klik op **Cluster**.
- 5 Voer een naam en een beschrijving in voor het cluster.
- 6 Selecteer een virtuele containerhost (VCH) van Docker in het vervolgkeuzemenu **Type**.
- 7 Voer het IP-adres of de naam van de host in. Gebruik hierbij de URL-indeling **http(s)://<hostnaam>:<poort>**
- 8 Selecteer uw verificatiegegevens in de lijst.

Containers ondersteunt verificatie op basis van verificatiegegevens en openbare of persoonlijke sleutels. U kunt uw verificatiegegevens toevoegen in de pagina **Identity Management**.
- 9 Klik op **Opslaan**.

Resultaten

U hebt een containerhostcluster gemaakt.

Containerimplementatiebeleid gebruiken

U kunt implementatiebeleid koppelen aan hosts en containerdefinities. U kunt implementatiebeleid gebruiken in Containers voor vRealize Automation om een voorkeur in te stellen voor de specifieke host en quotas wanneer u een container implementeert.

Implementatiebeleid dat wordt toegepast op een container heeft een hogere prioriteit dan plaatsingen die worden toegepast op containerhosts.

Opmerking Het implementatiebeleid is verouderd en zal worden verwijderd in een toekomstige release van vRealize Automation.

Een implementatiebeleid op een host instellen

Stel een voorkeur in voor de opgegeven host en quota wanneer u een container implementeert.

Opmerking Het implementatiebeleid is verouderd en zal worden verwijderd in een toekomstige release van vRealize Automation.

Voorwaarden

Voeg een host toe aan een cluster.

Procedure

- 1 Meld u aan bij de vRealize Automation-console als **containerbeheerder**.
- 2 Klik op het tabblad **Containers**.
- 3 Selecteer **Infrastructuur > Containerhostclusters**.

- 4 Klik op het cluster met de host die u wilt bewerken.
- 5 Klik op **Bronnen**.
- 6 Klik op het pictogram van de opties op de host die u wilt configureren en klik op **Bewerken**.
- 7 Selecteer het implementatiebeleid en klik op **Bijwerken**.

Een implementatiebeleid voor een containerdefinitie instellen

Stel een implementatiebeleid voor een containerdefinitie in.

Opmerking Het implementatiebeleid is verouderd en zal worden verwijderd in een toekomstige release van vRealize Automation.

Procedure

- 1 Klik op het tabblad **Containers**.
- 2 Klik op **Container Hot Clusters** om te beginnen met het inrichten van de container.
- 3 Selecteer een bestaande container in de lijst.
- 4 Klik op **Beleid** in de provisioning-opties.
- 5 Selecteer in de vervolgkeuzelijst **Implementatiebeleid** een bestaand beleid.
- 6 Voer provisioning uit op de container of sla deze op als sjabloon.

Containerinstellingen configureren

U kunt een toepassing met één of meer containers definiëren op basis van nieuwe en bestaande eigenschappen en instellingen voor containerconfiguraties.

Naast de hoofdinstanties van Containers voor vRealize Automation kunt u de volgende vRealize Automation-instellingen gebruiken voor implementaties die werken met containeronderdelen:

- Statusconfiguratie
- Koppelingen
- Vrijgegeven services
- Parameters voor cluster grootte en in- en uitschalen

Statuscontroles configureren in Containers

U kunt een methode voor statuscontroles instellen waarmee de status van een container wordt bijgewerkt op basis van aangepaste criteria.

U kunt HTTP- of TCP-protocollen gebruiken om opdrachten voor de container uit te voeren. U kunt tevens een methode voor statuscontroles opgeven.

Voorwaarden

- Controleer of Containers voor vRealize Automation is ingeschakeld voor uw ondersteunde vRealize Automation-implementatie.

- Controleer of u rechten hebt voor de rol van **containerbeheerder** of **containerarchitect**.

Procedure

- 1 Meld u aan bij vRealize Automation.
- 2 Klik op het tabblad **Containers**.
- 3 Selecteer **Bibliotheek > Sjablonen** in het linkervenster.
- 4 Bewerk de sjabloon of de image.

Optie	Beschrijving
Een sjabloon bewerken	<ol style="list-style-type: none"> a Klik op Bewerken rechtsboven in de sjabloon die u wilt openen. b Klik op Bewerken rechtsboven in de container die u wilt openen.
Een image bewerken	Klik op de pijl naast de knop Inrichten van de image en klik op Aanvullende gegevens invoeren .

- 5 Klik op het tabblad **Statusconfig**.
- 6 Selecteer een statusmodus.

Tabel 2-20. Modi voor statusconfiguratie

Modus	Beschrijving
Geen	Standaard. Er worden geen statuscontroles geconfigureerd.
HTTP	<p>Als u HTTP selecteert, moet u opgeven welke API en HTTP-methode en -versie worden gebruikt. De API is relatief en u hoeft het adres van de container niet op te geven. U kunt ook een time-outperiode voor de bewerking opgeven en statusdrempels instellen.</p> <p>Een statusdrempel van 2 betekent bijvoorbeeld dat er twee opeenvolgende aanroepen moeten lukken voordat de container in orde wordt bevonden en de status RUNNING krijgt. Evenzo moeten er bij een statusdrempel van 2 twee opeenvolgende aanroepen mislukken voordat de container niet in orde wordt bevonden en de status ERROR krijgt. Bij elke tussenliggende drempel tussen de status in orde en niet in orde krijgt de container de status DEGRADED.</p>
TCP-verbinding	Als u TCP-verbinding selecteert, moet u een poort opgeven voor de container. De statuscontrole probeert via de opgegeven poort een TCP-verbinding te maken met de container. U kunt ook een time-out voor de bewerking opgeven en drempels voor de status in orde en niet in orde instellen.
Opdracht	Als u Opdracht selecteert, moet u een opdracht opgeven die u wilt uitvoeren voor de container. Het resultaat van de statuscontrole wordt bepaald door de status waarmee de opdracht wordt afgesloten.

Tabel 2-20. Modi voor statusconfiguratie (vervolg)

Modus	Beschrijving
Statuscontrole bij inrichten negeren	Schakel dit selectievakje uit om de statuscontrole bij het inrichten af te dwingen. Hierdoor wordt een container pas beschouwd als ingericht nadat een statuscontrole met succes is voltooid.
Automatisch implementeren	Automatische herimplementatie van containers wanneer deze de status FOUT hebben.

7 Klik op **Opslaan**.

Koppelingen configureren in Containers

Koppelingen en vrijgegeven services faciliteren de communicatie tussen containerservices en de taakverdeling op hosts. U kunt de koppelingsinstellingen voor uw containers configureren in Containers.

U kunt koppelingen gebruiken om communicatie tussen meerdere services in uw toepassing mogelijk te maken. De koppelingen in Containers zijn een soort Docker-koppelingen, maar dan bedoeld om containers op verschillende hosts met elkaar te verbinden. Een koppeling bestaat uit twee onderdelen: een servicenaam en een alias. De servicenaam is de naam van de aangeroepen service of sjabloon. De alias is de naam van de host die u wilt gebruiken voor de communicatie met die service.

Stel u hebt een toepassing met een web- en databaseservice en u maakt vanuit de webservice een koppeling naar de databaseservice met behulp van een alias van **my-db**. De webservicetoepassing opent dan een TCP-verbinding met `my-db:{PORT_OF_DB}`. Deze `PORT_OF_DB` is de poort waar de database naar luistert, ongeacht welke openbare poort via de containerinstellingen is toegewezen aan de host. Als MySQL naar updates zoekt op de standaardpoort 3306, terwijl poort 32799 als gepubliceerde poort voor de containerhost wordt gebruikt, zal de webtoepassing de database benaderen op `my-db:3306`.

Opmerking Het wordt aanbevolen om netwerken te gebruiken in plaats van koppelingen. Koppelingen worden inmiddels als een verouderde Docker-functie beschouwd met aanzienlijke beperkingen bij het koppelen van containerclusters, zoals:

- Docker ondersteunt het gebruik van meerdere koppelingen met dezelfde alias niet. Het wordt aanbevolen om de koppelingsaliassen door Containers voor vRealize Automation te laten genereren.
- U kunt voor een container-runtime geen koppelingen bijwerken. Wanneer u een gekoppelde cluster opschaaft of neerschaalt, worden de koppelingen van de afhankelijke container niet bijgewerkt.

Voorwaarden

- Controleer of Containers voor vRealize Automation is ingeschakeld voor uw ondersteunde vRealize Automation-implementatie.

- Controleer of u rechten hebt voor de rol van **containerbeheerder** of **containerarchitect**.
- Zorg dat er een netwerkbridge beschikbaar is voor het koppelen van services.
- Zorg dat de interne poort van de doelservice is gepubliceerd. U kunt de service voor een kruislingse communicatie toewijzen aan een willekeurige andere poort, mits deze buiten de host om toegankelijk is.
- Controleer of er verbinding is tussen de servicehosts.

Procedure

- 1 Meld u aan bij vRealize Automation.
- 2 Klik op het tabblad Containers.
- 3 Selecteer **Bibliotheek > Sjablonen** in het linkervenster.
- 4 Bewerk de sjabloon of de image.

Optie	Beschrijving
Een sjabloon bewerken	a Klik op Bewerken rechtsboven in de sjabloon die u wilt openen. b Klik op Bewerken rechtsboven in de container die u wilt openen.
Een image bewerken	Klik op de pijl naast de knop Inrichten van de image en klik op Aanvullende gegevens invoeren .

- 5 Klik op het tabblad **Basis**.
- 6 Typ in het tekstvak **Services** een door komma's gescheiden lijst van services waarvan de container afhankelijk is.
- 7 Typ in het tekstvak **Alias** een beschrijvende naam van de service of een door komma's gescheiden lijst met services.
- 8 Klik op **Opslaan**.

Vrijgegeven services configureren in Containers

U kunt een unieke hostnaam voor een load balancer instellen door een adres met een tijdelijke aanduiding op te geven in de containerinstellingen.

De tijdelijke aanduiding verwijst naar de locatie van een deel van de URL dat automatisch wordt gegenereerd. Deze waarde is uniek voor elke hostnaam. U kunt het teken %s in het adres gebruiken om de locatie van de tijdelijke aanduiding aan te geven.

Opmerking Als u geen tijdelijke aanduiding gebruikt, wordt deze, afhankelijk van de systeemconfiguratie, als voor- of achtervoegsel in de hostnaam opgenomen.

Wanneer u een toepassing bouwt waarbij een service wordt gebruikt die algemeen wordt vrijgegeven en die tevens moet kunnen in- en uitschalen, wordt het aanbevolen om een load balancer te gebruiken die aanvragen voor elk knooppunt kan afhandelen. Als u de toepassing hebt ingericht, wordt de configuratie van de load balancer dan automatisch bijgewerkt zodra de service wordt in- of uitgeschaald met vRealize Automation.

Voorwaarden

- Controleer of Containers voor vRealize Automation is ingeschakeld voor uw ondersteunde vRealize Automation-implementatie.
- Controleer of u rechten hebt voor de rol van **containerbeheerder** of **containerarchitect**.

Procedure

- 1 Meld u aan bij vRealize Automation.
- 2 Klik op het tabblad **Containers**.
- 3 Selecteer **Bibliotheek > Sjablonen** in het linkervenster.
- 4 Bewerk de sjabloon of de image.

Optie	Beschrijving
Een sjabloon bewerken	<ol style="list-style-type: none"> a Klik op Bewerken rechtsboven in de sjabloon die u wilt openen. b Klik op Bewerken rechtsboven in de container die u wilt openen.
Een image bewerken	Klik op de pijl naast de knop Inrichten van de image en klik op Aanvullende gegevens invoeren .

- 5 Klik op het tabblad **Netwerk**.
- 6 Voer in het tekstvak **Adres** de locatie van de tijdelijke aanduiding in.
 De adreshost werkt als een virtuele host. Om toegang tot de adreshost te krijgen, kunt u toewijzingsinformatie toevoegen aan het bestand `etc/hosts` of een DNS gebruiken die het containeradres toewijst aan de hostnaam.
- 7 Geef in het tekstvak **Containerpoort** het nummer op van de poort waarmee de service wordt vrijgegeven.
 Gebruik de voorbeeldindeling uit het formulier. Als de containertoepassing meerdere poorten tegelijk beschikbaar stelt, geeft u aan via welke interne poort of poorten de service wordt vrijgegeven.
- 8 Klik op **Opslaan**.

Clustergrootte en schaal configureren in Containers

U kunt containerclusters maken door een clustergrootte op te geven via de plaatsingsinstellingen van Containers.

Wanneer u een cluster configureert, richt Containers het aantal opgegeven containers in. Alle aanvragen worden via taakverdeling over alle containers in de cluster verdeeld.

U kunt de clustergrootte van een ingerichte container of toepassing aanpassen door de omvang met één cluster te vergroten of verkleinen. Wanneer u de clustergrootte tijdens runtime wijzigt, worden alle affiniteitsfilters en plaatsingsregels meegewogen.

Voorwaarden

- Controleer of Containers voor vRealize Automation is ingeschakeld voor uw ondersteunde vRealize Automation-implementatie.
- Controleer of u rechten hebt voor de rol van **containerbeheerder** of **containerarchitect**.

Procedure

- 1 Meld u aan bij vRealize Automation.
- 2 Klik op het tabblad **Containers**.
- 3 Selecteer **Bibliotheek > Sjablonen** in het linkervenster.
- 4 Bewerk de sjabloon of de image.

Optie	Beschrijving
Een sjabloon bewerken	<ol style="list-style-type: none"> a Klik op Bewerken rechtsboven in de sjabloon die u wilt openen. b Klik op Bewerken rechtsboven in de container die u wilt openen.
Een image bewerken	Klik op de pijl naast de knop Inrichten van de image en klik op Aanvullende gegevens invoeren .

- 5 Klik op het tabblad **Beleid**.
- 6 Stel de clustergrootte van de container in.
- 7 Klik op **Opslaan**.

Sjablonen en images gebruiken in Containers

Containers gebruikt sjablonen om containers in te richten.

Een sjabloon is een herbruikbare configuratie voor het inrichten van een container of een suite containers. In een sjabloon kunt u een toepassing met meerdere lagen definiëren die uit gekoppelde services bestaat.

Een service wordt gedefinieerd als een of meerdere containers van hetzelfde type of dezelfde image.

U kunt een aangepaste containersjabloon maken op basis van een bestaande sjabloon op de pagina **Sjablonen** of u kunt een correct opgemaakt YAML-bestand importeren. U kunt ook een containersjabloon of -image inrichten.

Een aangepaste containersjabloon maken

U kunt een aangepaste sjabloon maken en deze gebruiken om een container te definiëren.

Een sjabloon is een herbruikbare configuratie waarmee u een container of een verzameling containers kunt inrichten.

Op de pagina Sjablonen ziet u welke sjabloonimages beschikbaar zijn op basis van de registers die u hebt gedefinieerd. U kunt een aangepaste sjabloon maken op basis van een bestaande sjabloonimage, of een sjabloon of Docker Compose-bestand importeren. Zie [Een sjabloon voor een container of een Docker Compose-bestand importeren](#).

U kunt ook een aangepaste sjabloon of image maken via **Inrichten > Aanvullende gegevens invoeren**. Deze optie wordt beschreven in [Een container inrichten op basis van een sjabloon of een image](#).

Voorwaarden

- Controleer of u rechten hebt voor de rol van **containerbeheerder**.

Procedure

- 1 Meld u aan bij de vRealize Automation-console als **containerbeheerder**.
- 2 Klik op het tabblad **Containers**.
- 3 Selecteer **Bibliotheek > Sjablonen** in het linkervenster.

Er verschijnt een lijst met sjablonen en images die beschikbaar zijn om in te richten.

- Geconfigureerde sjablonen in de weergave Images.
- Bestaande of aangepaste sjablonen in de weergave **Sjablonen**.
- Alle beschikbare sjablonen en images op basis van uw opgegeven registers in de weergave **Alles**.

Ook zijn de opties **Importeren** en **Exporteren** beschikbaar om sjablonen en images te importeren of exporteren.

- 4 Klik op de pijl naast de knop **Inrichting** voor een image die u wilt opnemen in de sjabloon.
- 5 Klik op **Extra informatie invoeren**.
- 6 Klik op **Opslaan als sjabloon** als u uw wijzigingen als een nieuwe containersjabloon wilt opslaan in Containers voor vRealize Automation.

Wat nu te doen

U kunt een sjabloon bewerken voor inrichtingen die u in de toekomst wilt uitvoeren. Deze wijzigingen achteraf hebben geen gevolgen voor de bestaande toepassingen die u met deze sjabloon hebt ingericht.

Een sjabloon voor een container of een Docker Compose-bestand importeren

U kunt een geïmporteerde Docker Container-sjabloon of een Docker Compose YAML-bestand als een aangepaste sjabloon gebruiken in Containers voor vRealize Automation.

Als u een YAML-bestand gebruikt, geeft u de inhoud van het YAML-bestand als tekst op of bladert u naar het YAML-bestand en uploadt u dit. Het YAML-bestand bevat de sjabloon, de configuratie van de verschillende containers en de verbindingen ertussen. De ondersteunde typen indelingen zijn Docker Compose YAML en Containers voor vRealize Automation YAML.

Containers voor vRealize Automation YAML is vergelijkbaar met Docker Compose, maar het gebruikt de YAML-indeling voor vRealize Automation-blueprint die zichtbaar is in vRealize Automation REST API of in vRealize CloudClient. Met Containers voor vRealize Automation YAML kunt u importeren in bestaande Docker Compose-toepassingen en deze wijzigen, inrichten en beheren met behulp van Containers.

Voorwaarden

- Controleer of Containers voor vRealize Automation is ingeschakeld voor uw ondersteunde vRealize Automation-implementatie.
- Meld u bij vRealize Automation aan als **containerbeheerder**.

Ga voor informatie over de YAML-indeling die wordt gebruikt door REST API's van de vRealize Automation-service naar *Naslaggids voor vRealize Automation API*.

Procedure

- 1 Klik op het tabblad **Containers**.

- 2 Selecteer **Bibliotheek > Sjablonen** in het linkervenster.

Er verschijnt een lijst met sjablonen en images die beschikbaar zijn om in te richten.

- Geconfigureerde sjablonen in de weergave **Images**.
- Bestaande of aangepaste sjablonen in de weergave **Sjablonen**.
- Alle beschikbare sjablonen en images op basis van uw opgegeven registers in de weergave **Alles**.

Ook zijn de opties **Importeren** en **Exporteren** beschikbaar om sjablonen en images te importeren of exporteren.

- 3 Klik op het pictogram **Import van sjabloon of Docker Compose**.

De pagina Sjabloon importeren verschijnt.

- 4 Lever de inhoud van het YAML-bestand aan.

Optie	Beschrijving
Laden uit bestand	Klik op Laden uit bestand en zoek het YAML-bestand op in de bijbehorende map.
Invoer van sjabloon of Docker Compose	Plak de inhoud van een YAML-bestand met de juiste indeling in het tekstvak Invoer van sjabloon of Docker Compose .

- 5 Klik op **Importeren**.

De nieuwe sjabloon verschijnt in de weergave **Sjablonen**.

Een container inrichten op basis van een sjabloon of een image

U kunt een container inrichten op basis van een sjabloon of een image in de weergave Sjablonen.

Tijdens het inrichtingsproces wordt een container gemaakt op basis van de configuratie-instellingen die voorkomen in de sjabloon of het image waarmee de inrichting wordt uitgevoerd.

U kunt een container inrichten op basis van een sjabloon of image door ofwel bestaande configuratie-instellingen te gebruiken ofwel door de configuratie-instellingen te bewerken en vervolgens de inrichting uit te voeren.

U kunt ook de configuratie-instellingen bewerken en deze opslaan in een nieuwe, aangepaste sjabloon of image van de container.

Voorwaarden

- Controleer of Containers voor vRealize Automation is ingeschakeld voor uw ondersteunde vRealize Automation-implementatie.
- Meld u bij vRealize Automation aan als **containerbeheerder**.

Procedure

1 Klik op het tabblad **Containers**.

2 Selecteer **Bibliotheek > Sjablonen** in het linkervenster.

Er verschijnt een lijst met sjablonen en images die beschikbaar zijn om in te richten.

- Geconfigureerde sjablonen in de weergave **Images**.
- Bestaande of aangepaste sjablonen in de weergave **Sjablonen**.
- Alle beschikbare sjablonen en images op basis van uw opgegeven registers in de weergave **Alles**.

Ook zijn de opties **Importeren** en **Exporteren** beschikbaar om sjablonen en images te importeren of exporteren.

3 Gebruik de weergaveopties **Alle**, **Images** of **Sjablonen** om de sjabloon of het image voor de inrichting weer te geven.

4 Richt de sjabloon of het image in.

Optie	Beschrijving
Inrichten met bestaande instellingen.	<p>a Klik op Provision.</p> <p>In de weergave Inrichtingsaanvragen wordt informatie over de voortgang van de inrichting weergegeven.</p>
Inrichten door instellingen te bewerken.	<p>a Klik op de pijl naast de knop Provision.</p> <p>b Klik op Extra informatie invoeren.</p> <p>c Voer de extra informatie in voor de container in het formulier Een container inrichten.</p> <p>d Wanneer u klaar bent met het bijwerken van het formulier, klikt u op Provision om de gewijzigde instellingen in te richten.</p> <p>e Klik op Opslaan als sjabloon wanneer u uw wijziging als een nieuwe sjabloon voor containers wilt opslaan in Containers voor vRealize Automation.</p> <p>In de weergave Inrichtingsaanvragen wordt informatie over de voortgang van de inrichting weergegeven.</p>

Een sjabloon voor een container of een Docker Compose-bestand exporteren

U kunt een sjabloon voor een container exporteren als een Docker Compose YAML-bestand of een Containers voor vRealize Automation YAML-bestand.

U kunt een sjabloon importeren, dit programmatisch wijzigen met behulp van de vRealize Automation REST API of van vRealize CloudClient of het grafisch wijzigen in Containers. U kunt vervolgens het aangepaste bestand weer exporteren. Zo kunt u bijvoorbeeld een bestand importeren in de Docker Compose-indeling en de blueprint exporteren in de YAML-indeling die wordt gebruikt in de API van de vRealize Automation-compositieservice. Echter, bepaalde configuraties die specifiek zijn voor Containers, zoals de statusconfiguratie en de affiniteitsbeperkingen, worden niet opgenomen als u de sjabloon exporteert in de Docker Compose-indeling.

Voorwaarden

- Controleer of Containers voor vRealize Automation is ingeschakeld voor uw ondersteunde vRealize Automation-implementatie.
- Meld u bij vRealize Automation aan als **containerbeheerder**.

Ga voor informatie over de YAML-indeling die wordt gebruikt door REST API's van de vRealize Automation-service naar *Naslaggids voor vRealize Automation API*.

Procedure

1 Klik op het tabblad **Containers**.

2 Selecteer **Bibliotheek > Sjablonen** in het linkervenster.

Er verschijnt een lijst met sjablonen en images die beschikbaar zijn om in te richten.

- Geconfigureerde sjablonen in de weergave Images.

- Bestaande of aangepaste sjablonen in de weergave **Sjablonen**.
- Alle beschikbare sjablonen en images op basis van uw opgegeven registers in de weergave **Alles**.

Ook zijn de opties **Importeren** en **Exporteren** beschikbaar om sjablonen en images te importeren of exporteren.

3 Wijs een sjabloon aan en klik op het pictogram **Exporteren**.

4 Selecteer een type indeling voor de uitvoer, wanneer dit wordt gevraagd.

- **YAML-blueprint**

Deze indeling stemt overeen met de YAML-indeling voor blueprints die wordt gebruikt in de API voor de vRealize Automation-compositieservice.

- **Docker Compose**

Deze indeling stemt overeen met de YAML-indeling die wordt gebruikt in de Docker Compose-toepassing.

5 Klik op **Exporteren**.

6 Sla het bestand op of open dit met de juiste toepassing wanneer dat wordt gevraagd.

Containerregisters gebruiken

Een Docker-register is een staatloze servertoepassing. U kunt registers gebruiken in Containers voor vRealize Automation om Docker-images op te slaan en te verdelen.

Als u een register wilt configureren, moet u het adres, een aangepaste registernaam en optionele verificatiegegevens opgeven. Het adres moet beginnen met HTTP of HTTPS om op te geven of het register beveiligd of niet-beveiligd is. Als het verbindingstype niet wordt opgegeven, wordt standaard HTTPS gebruikt.

Opmerking Voor HTTP moet u poort 80 declareren en voor HTTPS poort 443. Als er geen poort is opgegeven, verwacht de Docker-engine poort 5000, wat kan leiden tot verbroken verbindingen.

Opmerking Wij raden u aan geen HTTP-registers te gebruiken, omdat HTTP als onveilig wordt beschouwd. Als u HTTP wilt gebruiken, moet u de `DOCKER_OPTS`-eigenschap op elke host als volgt wijzigen:

```
DOCKER_OPTS="--insecure-registry myregistrydomain.com:5000".
```

Raadpleeg de documentatie voor Docker op <https://docs.docker.com/registry/insecure/>.

Containers kan op de volgende manier communiceren met Docker-register HTTP API V1 en V2:

V1 via HTTP (niet-beveiligd, standaard HTTP-register)

U kunt vrij zoeken naar dit type register, maar u moet elke Docker-host handmatig configureren met de `--insecure-registry`-markering om containers in te richten op basis

van images van onbeveiligde registers. U moet de Docker-daemon opnieuw opstarten nadat u de eigenschap hebt ingesteld.

V1 via HTTPS

Gebruik dit achter een reverse proxy, zoals NGINX. De standaardimplementatie is beschikbaar als een open source op <https://github.com/docker/docker-registry>.

V2 via HTTPS

De standaardimplementatie is beschikbaar als een open source op <https://github.com/docker/distribution>.

V2 via HTTPS met basisverificatie

De standaardimplementatie is beschikbaar als een open source op <https://github.com/docker/distribution>.

V2 via HTTPS met verificatie via een centrale service

U kunt een Docker-register uitvoeren in standalone modus, waarbij geen autorisatiecontroles worden uitgevoerd. Ondersteunde externe registers zijn JFrog Artifactory en Harbor. Docker Hub wordt standaard ingeschakeld voor alle tenants en is niet aanwezig in de lijst met registers, maar kan worden gedeactiveerd met een systeemeigenschap.

Opmerking Docker communiceert normaal niet met beveiligde registers die zijn geconfigureerd met certificaten die door een onbekende certificeringsinstantie zijn ondertekend. De containerservice behandelt dit geval door niet-vertrouwde certificaten automatisch te uploaden naar alle Docker-hosts en de hosts toegang tot deze registers te verschaffen. Als een certificaat niet kan worden geüpload naar een bepaalde host, wordt de host automatisch gedeactiveerd.

Containerregisters maken en beheren

U kunt meerdere registers configureren om toegang te krijgen tot zowel openbare als particuliere images.

Registers zijn openbare of particuliere opslagruimten waar u images kunt uploaden en downloaden. U kunt de gemaakte registers deactiveren, bewerken of verwijderen. De images op het tabblad **Sjablonen** zijn gebaseerd op de registers die u definieert.

Wanneer u registers maakt of beheert, kunt u op de knoppen **Verificatiegegevens** of **Certificaat** klikken om verificatiegegevens en certificaten toe te voegen of te beheren.

Voorwaarden

- Meld u bij vRealize Automation aan als **containerbeheerder**.
- Controleer of er ten minste één host is geconfigureerd die u kunt gebruiken voor de configuratie van het containernetwerk.

Procedure

- 1 Klik op het tabblad **Containers**.

- 2 Selecteer **Bibliotheek > Algemene registers**.
- 3 Klik op **Register** om een nieuw register te maken.
- 4 Voer het registeradres in.
- 5 Voer de naam van het register in.
- 6 Selecteer uw verificatiegegevens in de vervolgkeuzelijst.
- 7 (Optioneel) Klik op **Verifiëren** om de geldigheid van de geconfigureerde parameters te bevestigen.
- 8 Klik op **Opslaan** om het register toe te voegen.

Image toevoegen aan favorieten

U kunt images toevoegen als favorieten om snel toegang te krijgen tot uw meest gebruikte of favoriete images.

Wanneer een image als favoriet is toegevoegd, wordt deze weergegeven op de startpagina van Opslagplaatsen zonder dat u hoeft te zoeken. Alleen containerbeheerders kunnen images toevoegen aan of verwijderen uit de favorieten, terwijl alle gebruikers de favoriete images per opslagplaats kunnen bekijken. Images die als favoriet zijn gemarkeerd, worden weergegeven met een sterretje.

Procedure

- 1 Open de pagina Opslagplaatsen, selecteer het register in het vervolgkeuzemenu en zoek de gewenste image.
- 2 Klik op de pijl naast de **Inrichting** en selecteer **Image toevoegen aan favorieten**.

Er wordt een melding weergegeven om aan te geven dat de image is toegevoegd aan de favorieten en er verschijnt een sterretje naast de naam van de image.

Resultaten

De image wordt weergegeven op de pagina Opslagplaatsen zonder dat u hoeft te zoeken. Als u de image uit de favorieten wilt verwijderen op de pagina Opslagplaatsen, klikt u op de pijl naast de **Inrichting** en selecteert u **Image verwijderen uit favorieten**.

Netwerkbronnen voor containers configureren

U kunt netwerkconfiguraties maken, wijzigen en toevoegen aan containers en containersjablonen in de Containers voor vRealize Automation-toepassing.

Wanneer u een container inricht, is de netwerkconfiguratie ingesloten en beschikbaar. U kunt de netwerkinstellingen aanpassen voor containeronderdelen die u aan een vRealize Automation-blueprint hebt toegevoegd.

Een nieuw netwerk maken voor containers

Als er geen geschikte netwerkconfiguratie beschikbaar is, kunt u een nieuw netwerk maken in vRealize Automation.

Voorwaarden

- Controleer of u rechten hebt voor de rol van **containerbeheerder**, **containerarchitect** of **IaaS-beheerder**.
- Controleer of er ten minste één host is geconfigureerd die u kunt gebruiken voor de configuratie van het containernetwerk.

Procedure

- 1 Meld u aan bij vRealize Automation.
- 2 Klik op het tabblad **Containers**.
- 3 Selecteer **Implementaties > Netwerken** in het linkervenster.

In het hoofdvenster ziet u de bestaande netwerkconfiguraties die u kunt gebruiken als onderdeel van de containerimplementatie. De weergegeven verzameling netwerkconfiguraties bestaat uit die van toegevoegde Docker-hosts en configuraties die zijn gemaakt in vRealize Automation. De pictogrammen voor de netwerkconfiguraties tonen informatie over netwerk- en IPAM-stuurprogramma's, het subnet, de gateway en het IP-bereik, alsmede het aantal containers dat gebruikmaakt van de netwerkconfiguratie, plus het aantal hosts.

- 4 Klik op **+Netwerk**.
- 5 Voer een naam voor het netwerk in.

Wanneer u de nieuwe configuratie hebt voltooid, wordt de naamwaarde toegevoegd met een unieke id.

- 6 (Optioneel) Als u meer gedetailleerde configuratie-instellingen wilt toevoegen, schakelt u het selectievakje **Geavanceerd** in.

Er verschijnen aanvullende instellingen voor de netwerkconfiguratie in het scherm Netwerk toevoegen.

7 Configureer de geavanceerde netwerkconfiguratie-instellingen.

Optie	Beschrijving
IPAM-configuratie	<p>Subnet</p> <p>Geef de unieke subnet- en gateway-adressen voor deze netwerkconfiguratie op. Deze waarden mogen niet overlappen met andere netwerken op dezelfde containerhost.</p>
Aangepaste eigenschappen	<p>Geef eventueel aangepaste eigenschappen voor de nieuwe netwerkconfiguratie op.</p> <p>containers.ipam.driver</p> <p>Uitsluitend voor gebruik met containers Hiermee wordt het IPAM-stuurprogramma opgegeven dat wordt gebruikt wanneer een netwerkonderdeel Containers wordt toegevoegd aan een blueprint. De ondersteunde waarden zijn afhankelijk van de stuurprogramma's die zijn geïnstalleerd in de hostomgeving van de container waar ze worden gebruikt. Een ondersteunde waarde kan bijvoorbeeld <code>infoblox</code> of <code>calico</code> zijn, afhankelijk van de IPAM-invoegtoepassingen die zijn geïnstalleerd op de host van de container.</p> <p>Deze eigenschapsnaam en -waarde zijn hoofdlettergevoelig. De waarde van de eigenschap wordt niet gevalideerd wanneer u deze toevoegt. Als het opgegeven stuurprogramma niet bestaat op de host van de container tijdens de inrichting, wordt een foutmelding geretourneerd en mislukt de inrichting.</p> <p>containers.network.driver</p> <p>Uitsluitend voor gebruik met containers Hiermee wordt het netwerkstuurprogramma opgegeven dat wordt gebruikt wanneer een netwerkonderdeel Containers wordt toegevoegd aan een blueprint. De ondersteunde waarden zijn afhankelijk van de stuurprogramma's die zijn geïnstalleerd in de hostomgeving van de container waar ze worden gebruikt. De door Docker geleverde netwerkstuurprogramma's omvatten de stuurprogramma's <code>bridge</code>, <code>overlay</code> en <code>macvlan</code>, terwijl in de door Virtual Container Host (VCH) geleverde stuurprogramma's het stuurprogramma <code>bridge</code> is opgenomen. Netwerkstuurprogramma's van derden, zoals <code>weave</code> en <code>calico</code>, zijn mogelijk ook beschikbaar, afhankelijk van de netwerkinvoegtoepassingen die zijn geïnstalleerd op de host van de container.</p> <p>Deze eigenschapsnaam en -waarde zijn hoofdlettergevoelig. De waarde van de eigenschap wordt niet gevalideerd wanneer u deze toevoegt. Als het opgegeven stuurprogramma niet bestaat op de host van de container tijdens de inrichting, wordt een foutmelding geretourneerd en mislukt de inrichting.</p>

Opmerking Als u een netwerk hebt gemaakt zonder geavanceerde instellingen, worden de instellingen door vRealize Automation automatisch ingevuld.

8 Selecteer in het vervolgkeuzemenu de host waarmee u wilt dat uw netwerk verbinding maakt.

9 Klik op **Maken**.

Een netwerk toevoegen aan een containersjabloon

U kunt een netwerkconfiguratie toevoegen aan een containersjabloon om de containers met elkaar te verbinden. Deze netwerkconfiguratie wordt automatisch geïmplementeerd voor alle toepassingen die gebruikmaken van de sjabloon. U kunt een bestaand netwerk toevoegen of zo nodig een nieuw netwerk configureren en toevoegen.

Voorwaarden

- Zorg dat u een sjabloon beschikbaar hebt. Maak anders eerst een nieuwe sjabloon.
- Controleer of u rechten hebt voor de rol van **containerbeheerder**, **containerarchitect** of **IaaS-beheerder**.
- Controleer of er ten minste één host is geconfigureerd die u kunt gebruiken voor de configuratie van het containernetwerk.

Procedure

- 1 Meld u aan bij vRealize Automation.
- 2 Klik op het tabblad **Containers**.
- 3 Selecteer **Bibliotheek > Sjablonen** in het linkervenster.
Er verschijnt een reeks pictogrammen voor de sjablonen en images die beschikbaar zijn om in te richten.
- 4 (Optioneel) Wijzig de weergave zodat alleen sjablonen worden weergegeven. Hiertoe klikt u op **Weergave: Sjablonen** in de header rechtsboven de pictogrammen.
- 5 Klik op **Bewerken** rechtsboven in de sjabloon die u wilt aanpassen.
Op de geopende pagina Sjabloon bewerken worden de containerpictogrammen en een leeg pictogram met een plusteken weergegeven.
- 6 Wijs het lege pictogram aan.
Het pictogram **Netwerk toevoegen** wordt weergegeven.
- 7 Klik op het pictogram **Netwerk toevoegen**.
Het venster Netwerk toevoegen verschijnt.

8 Voeg een bestaand netwerk toe of maak een nieuw netwerk en voeg dit toe.

Optie	Beschrijving
Voeg een bestaand netwerk toe.	<ul style="list-style-type: none"> a Klik op het selectievakje Bestaand. b Klik in het veld Naam om een lijst met bestaande netwerken weer te geven. c Selecteer het netwerk dat u wilt gebruiken en klik op Opslaan.
Configureer een nieuw netwerk en voeg dit toe.	<ul style="list-style-type: none"> a Voer een naam voor het netwerk in. b Als u meer gedetailleerde configuratie-instellingen wilt toevoegen, schakelt u het selectievakje Geavanceerd in. c Klik op Opslaan.

9 Verbind het netwerk met een container door het netwerkverbindingspictogram te slepen van de container naar een punt op het horizontale pictogram dat het netwerk vertegenwoordigt.

Volumes configureren voor containers

U kunt volumes maken, wijzigen en toevoegen aan containers en containersjablonen in de Containers voor vRealize Automation-toepassing.

Containers voor vRealize Automation gebruikt Docker-volumes voor persistent gegevensbeheer. Met volumes kunt u de volgende taken uitvoeren:

- Volumes delen tussen verschillende containers in dezelfde host.
- Gegevens onmiddellijk bijwerken.
- De volumegegevens opslaan nadat de container is verwijderd.

Een nieuw volume maken voor containers

Om uw containeropslagruimte uit te breiden, moet u eerst een gegevensvolume maken.

Voorwaarden

- Controleer of u rechten hebt voor de rol van **containerbeheerder**, **containerarchitect** of **laaS-beheerder**.
- Controleer of er ten minste één host is geconfigureerd die u kunt gebruiken voor de configuratie van het containervolume.

Procedure

- 1 Meld u aan bij vRealize Automation.
- 2 Klik op het tabblad **Containers**.

3 Selecteer **Implementaties > Volumes** in het linkervenster.

In het hoofdvenster ziet u de bestaande volumeconfiguraties die kunnen worden verbonden met de geïmplementeerde containers. De weergegeven verzameling volumeconfiguraties bestaat uit die van toegevoegde Docker-hosts en configuraties die zijn gemaakt in vRealize Automation. De volume-instanties geven het stuurprogramma, het bereik en de stuurprogrammaopties weer.

4 Klik op **+Volume**.

5 Voer een naam voor het volume in.

Wanneer u de configuratie hebt voltooid, wordt de naamwaarde toegevoegd met een unieke id.

6 Voer in het tekstvak **Stuurprogramma** het stuurprogramma in van de volume-invoegtoepassing die u wilt gebruiken. Als u niets invoert, wordt local gebruikt als de standaardwaarde.

7 (Optioneel) Als u meer gedetailleerde configuratie-instellingen wilt toevoegen, schakelt u het selectievakje **Geavanceerd** in.

Er worden aanvullende configuratie-instellingen weergegeven.

8 (Optioneel) Configureer de geavanceerde volume-instellingen.

Optie	Beschrijving
Opties van stuurprogramma	Geef de stuurprogrammaopties op die u wilt gebruiken. De opties zijn afhankelijk van de volume-invoegtoepassing die u gebruikt.
Aangepaste eigenschappen	Geef aangepaste eigenschappen voor de nieuwe configuratie op.

9 Selecteer in het vervolgkeuzemenu de host waarmee u wilt dat uw volume verbinding maakt.

10 Klik op **Maken**.

Het venster Volume maken verdwijnt en het toegevoegde volume wordt weergegeven op het tabblad Volumes.

Wat nu te doen

[Een volume toevoegen aan een containersjabloon](#)

Een volume toevoegen aan een containersjabloon

Verbind een volume met een container door dit aan een sjabloon toe te voegen.

Voorwaarden

- Zorg dat u een sjabloon beschikbaar hebt. Maak anders eerst een nieuwe sjabloon.
- Controleer of u rechten hebt voor de rol van **containerbeheerder**, **containerarchitect** of **laaS-beheerder**.

- Controleer of er ten minste één host is geconfigureerd die u kunt gebruiken voor de configuratie van het containervolume.

Procedure

1 Meld u aan bij vRealize Automation.

2 Klik op het tabblad **Containers**.

3 Selecteer **Bibliotheek > Sjablonen** in het linkervenster.

Er verschijnt een reeks pictogrammen voor de sjablonen en images die beschikbaar zijn om in te richten.

4 (Optioneel) Wijzig de weergave zodat alleen sjablonen worden weergegeven. Hiertoe klikt u op **Weergave: Sjablonen** in de header rechtsboven de pictogrammen.

5 Klik op **Bewerken** rechtsboven in de sjabloon die u wilt aanpassen.

De pagina Sjabloon bewerken verschijnt met daarop de containerpictogrammen en een leeg pictogram met een plusteken.

6 Plaats de cursor op het lege pictogram met het plusteken om het pictogram **Volume toevoegen** weer te geven.

7 Klik op het pictogram **Volume toevoegen**.

8 Voeg een bestaand volume toe of maak een nieuw volume en voeg dit toe.

Optie	Beschrijving
Voeg een bestaand volume toe.	<ul style="list-style-type: none"> a Klik op het selectievakje Bestaand. b Klik in het veld Naam om een lijst met bestaande volumes weer te geven. c Selecteer het volume dat u wilt gebruiken en klik op Opslaan.
Configureer een nieuw volume en voeg dit toe.	<ul style="list-style-type: none"> a Voer een naam voor het volume in. b Voer in het tekstvak Stuurprogramma het stuurprogramma in van de volume-invoegtoepassing die u wilt gebruiken. Als u geen extern opslagsysteem gebruikt, voert u local in. c Als u meer gedetailleerde configuratie-instellingen wilt toevoegen, schakelt u het selectievakje Geavanceerd in. d Klik op Opslaan.

Het venster Volume toevoegen wordt gesloten en het toegevoegde volume wordt als een horizontaal pictogram weergegeven onder de containerpictogrammen op de pagina Sjabloon bewerken. Er wordt tevens een volumepictogram weergegeven aan de onderkant van de containerpictogrammen.

9 Verbind het volume met een container door het volumeverbindingspictogram te slepen van de container naar een punt op het horizontale pictogram dat het volume vertegenwoordigt.

10 (Optioneel) Klik op het containerpad om de locatie waar u het volume wilt koppelen, te wijzigen.

Wat nu te doen

[Een container inrichten op basis van een sjabloon of een image](#)

PKS-containers maken en configureren

Met Pivotal Container Service (PKS) kunnen bedrijven en serviceproviders de implementatie en bewerkingen van op Kubernetes gebaseerde containerservices vereenvoudigen.

PKS-containers bieden de volgende belangrijke functies:

- Hoge beschikbaarheid
 - PKS heeft een ingebouwde fouttolerantie met routine-gezondheidscontroles en zelfcorrectiemogelijkheden voor Kubernetes-clusters.
- Geavanceerde netwerk- en beveiligingsonderdelen
 - PKS is nauw geïntegreerd met NSX-T voor geavanceerde containernetwerken, inclusief microsegmentatie, taakverdeling en beveiligingsbeleid.
- Gestroomlijnde bewerkingen
 - PKS maakt clusterimplementatie en levenscyclusbeheer van Kubernetes mogelijk.
- Multitenancy
 - PKS ondersteunt multitenancy voor taaklastisolatie en privacy in zakelijke en cloudservices.

Een PKS-endpoint toevoegen

Voordat u een PKS-container maakt, moet u een PKS-endpoint toevoegen.

De eerste stap om een PKS-container te maken is het toevoegen van een PKS-endpoint. PKS-endpoints stellen u in staat om plannen, bestaande Kubernetes-clusters en bedrijfsgroepen te koppelen.

Voorwaarden

- Bevoegdheid van containerbeheerder
- PKS-verificatiegegevens
- UAA-adres
- PKS-endpointadres

Procedure

- 1 Ga naar de verificatiegegevens met behulp van het pad **Identiteitsbeheer > Verificatiegegevens** om uw PKS-verificatiegegevens op te slaan.
- 2 Selecteer **PKS-endpoints > Endpoint maken**.

- 3 Voer de gegevens van uw PKS-endpoint in en test de verbinding voordat u het opslaat.

Als de test mislukt, controleert u of de PKS-verificatiegegevens, het UAA-adres en het PKS-endpointadres correct zijn. Mogelijk moet u de adressen pingen om te controleren of ze actief zijn. Probeer opnieuw verbinding te maken.

- 4 Klik op **Maken** om uw PKS-endpoint op te slaan.

Opmerking Als er een venster voor certificaatcontrole wordt weergegeven, kunt u **Certificaat weergeven** selecteren om de details van het certificaat te bekijken. Klik op **Ja** om door te gaan en sla uw endpoint op.

Resultaten

Uw PKS-endpoint is opgeslagen. Na het opslaan van uw PKS-endpoint kunt u op het endpoint klikken om de beschikbare eraan gekoppelde Kubernetes-clusters weer te geven. Als het cluster niet is geregistreerd in vRealize Automation, wordt de waarde **Nee** weergegeven in de kolom Aangevraagd. U moet [een cluster toevoegen](#) om het te registeren. Als u uw endpoint wilt bewerken, klikt u op de naam van het PKS-endpoint en wijzigt u de gegevens. U kunt het endpoint verwijderen door het te selecteren en op **Verwijderen** te klikken.

PKS-endpoints toewijzen aan bedrijfsgroepen

Na het maken van een PKS-endpoint kunt u dit toewijzen aan specifieke bedrijfsgroepen om toegang te verlenen.

Na het maken van een PKS-endpoint kunt u specifieke bedrijfsgroepen toegang geven tot het endpoint door er plannen aan toe te wijzen. Deze functie wordt gebruikt om de toegang van bepaalde groepen tot bepaalde functionaliteit te beperken.

Opmerking U kunt plannen afzonderlijk maken in PKS. Plannen kunnen niet worden toegevoegd of aangepast in vRealize Automation.

Voorwaarden

- Bevoegdheid van containerbeheerder
- Bestaand PKS-endpoint

Procedure

- 1 Open uw PKS-endpoint en klik op **Plantoewijzingen**.
- 2 Selecteer de gewenste groep in de lijst met groepen en het plan in de lijst met plannen.

Opmerking Met de knoppen + en - kunt u meerdere plannen toewijzen aan elke bedrijfsgroep en hetzelfde plan toewijzen aan meerdere bedrijfsgroepen.

- 3 Klik op **Opslaan** om uw plantoewijzingen op te slaan.

Een nieuw PKS-cluster aanvragen

Als uw gewenste clusterconfiguratie niet bestaat, kunt u een nieuw cluster voor een bestaand PKS-endpoint aanvragen.

Als containerontwikkelaar of containerbeheerder kunt u een nieuw cluster voor uw PKS-endpoint aanvragen. Elk PKS-endpoint kan meerdere clusters bevatten. Na het maken van een nieuw cluster kunt u dit aan uw omgeving toevoegen met **Cluster toevoegen** en het naar wens inrichten.

Voorwaarden

- Een bestaand PKS-endpoint
- Bevoegdheid van containerontwikkelaar of containerbeheerder

Procedure

- 1 Selecteer **PKS-clusters > Nieuw cluster**.

- 2 Selecteer het PKS-endpoint.

Na het selecteren van een PKS-endpoint wordt het plan automatisch ingevuld op basis van de plannen die beschikbaar zijn voor uw bedrijfsgroep.

- 3 Voer de details van het cluster in.

Opmerking Hoewel het aantal werkerknooppunten wordt gedefinieerd door het plan, kunt u dit aantal aanpassen al naargelang uw behoeften.

- 4 Selecteer hoe verbinding moet worden gemaakt met dit cluster:

- Hostnaam van master - er wordt verbinding gemaakt met behulp van de hostnaam van het cluster, ervan uitgaande dat een DNS-record bestaat.
- IP van hoofdknooppunt - er wordt verbinding gemaakt met behulp van het IP-adres van het cluster.

- 5 Klik op **Maken**.

Resultaten

Het nieuwe cluster is gemaakt en wordt weergegeven op de startpagina van de PKS-clusters.

Een PKS-cluster toevoegen

Nadat een PKS-endpoint is gemaakt, kunt u de beschikbare gekoppelde clusters registreren in vRealize Automation.

Nadat een PKS-endpoint is gemaakt, kunt u de gekoppelde clusters registreren door een cluster toe te voegen in vRealize Automation. Zodra de clusters zijn geregistreerd, kunt u deze inrichten met enkelvoudige images.

Voorwaarden

- Bevoegdheid van containerbeheerder

■ PKS-endpoint met beschikbare clusters

Procedure

- 1 Zorg dat u een cluster toevoegt aan de juiste bedrijfsgroep. De naam van de bedrijfsgroep wordt vermeld in het bovenste venster links. Klik op **Groep** als u tussen bedrijfsgroepen wilt wisselen.
- 2 Selecteer **PKS-cluster > Cluster toevoegen**.
- 3 Selecteer het PKS-endpoint om de beschikbare clusters in te vullen.
- 4 Selecteer hoe verbinding moet worden gemaakt met dit cluster:
 - Hostnaam van master - er wordt verbinding gemaakt via de hostnaam van het cluster, ervan uitgaande dat een DNS-record bestaat.
 - IP van hoofdknooppunt - er wordt verbinding gemaakt via het IP-adres van het cluster.
- 5 Klik op **Toevoegen**.

Resultaten

Het cluster wordt weergegeven op de pagina met PKS-clusters.

PKS-clusterdetails

De details van een cluster bieden informatie en tools om het cluster te bewerken en met het cluster te communiceren.

U kunt bestaande PKS-clusters bekijken en wijzigen door op de naam van het cluster te klikken in de pagina **PKS-clusters**. Bovendien bevatten de details van het cluster interactieve tools die u kunt gebruiken om met het cluster te communiceren voor complexere configuraties.

Opmerking U kunt alleen het aantal werkerknooppunten van een cluster bewerken.

Dashboard

De dashboardveldstatus geeft aan dat het Kubernetes-dashboard is geïnstalleerd. Indien geïnstalleerd krijgt u toegang tot het dashboard door op **Geïnstalleerd** te klikken en u aan te melden.

Opmerking Het dashboard moet in het cluster zijn geconfigureerd voor basisverificatie. Zonder basisverificatie kunt u zich niet aanmelden.

Kubeconfig

De kubeconfig-koppeling is een downloadbaar configuratiebestand voor het cluster. U kunt dit configuratiebestand, als containerontwikkelaar, gebruiken om verbinding te maken met en de configuratie uit te voeren van het Kubernetes-cluster in het promptvenster van de opdrachtregel. Bijvoorbeeld met behulp van het commando **kubect1**.

Een enkele image inrichten in een Kubernetes-cluster

Met de containerfunctionaliteit in vRealize Automation kunt u een enkele image inrichten in een PKS-cluster.

Na het toevoegen van een PKS-cluster kunt u een enkele image inrichten in dit cluster als combinatie van een Kubernetes-pod en -implementatie.

Voorwaarden

- Bevoegdheid van containerontwikkelaar
- PKS-cluster

Procedure

- 1 Ga naar **Bibliotheek > Opslagplaatsen**.
- 2 Selecteer het gewenste register in het vervolgkeuzemenu.
- 3 Zoek naar een bestaande image binnen dat register met behulp van het tekstvak Opslagplaatsen.
- 4 Klik op **Inrichten** op de gewenste imagetegel.
- 5 Geef de inrichtingsgegevens op en klik op **Inrichten**.

Resultaten

De geselecteerde image wordt ingericht in het Kubernetes-cluster en weergegeven in het venster **Aanvragen** in de zijbalk. Hij wordt ook weergegeven onder **Kubernetes > Implementaties** en **Kubernetes > Pods** voor verificatiedoeleinden.

Opmerking U kunt het cluster ook inrichten door het bestand kubeconfig te downloaden en het commando **kubect1** te gebruiken. Zie [PKS-clusterdetails](#) voor meer informatie.

Aanvullende invoegtoepassingen installeren op de vRealize Orchestrator-standaardserver

U kunt aanvullende pakketten en invoegtoepassingen op de vRealize Orchestrator-standaardserver installeren via de vRealize Orchestrator configuratie-interface.

U kunt aanvullende invoegtoepassingen op de vRealize Orchestrator-standaardserver installeren en de werkstromen gebruiken met XaaS.

U kunt ook aanvullende pakketten importeren op de vRealize Orchestrator-standaardserver voor configuratie als endpointtypen van de externe IPAM-provider vRealize Automation. Zie [Checklist voor het bieden van ondersteuning voor externe IPAM-providers](#) voor bijvoorbeeld informatie over het verkrijgen, importeren en configureren van het IPAM-pakket Infoblox.

Pakketbestanden (.package) en installatiebestanden van invoegtoepassingen (.vmoapp of .dar) zijn verkrijgbaar bij de VMware Solution Exchange op https://solutionexchange.vmware.com/store/category_groups/cloud-management. Zie vRealize Orchestrator Documentatie over invoegtoepassingen op https://www.vmware.com/support/pubs/vco_plugins_pubs.html voor meer informatie over invoegtoepassingbestanden.

Voor meer informatie over het installeren van nieuwe invoegtoepassingen raadpleegt u *VMware vCenter Orchestrator installeren en configureren*.

Werken met een Active Directory-beleid

Een Active Directory-beleid bepaalt de eigenschappen van een machinerecord, bijvoorbeeld een domein, alsook de organisatie-eenheid waarin de record wordt gemaakt met behulp van een vRealize Automation-blueprint.

Als u een beleid toepast op een bedrijfsgroep, worden alle machineaanvragen van de leden van die bedrijfsgroep toegevoegd aan een opgegeven organisatie-eenheid. U kunt meer dan één beleid maken voor verschillende organisatie-eenheden en vervolgens een verschillend beleid toepassen op verschillende bedrijfsgroepen.

Aangepaste eigenschappen gebruiken om een Active Directory-beleid te overschrijven

Met de meegeleverde aangepaste eigenschappen van Active Directory kunt u het Active Directory-beleid, het domein, de organisatie-eenheid en andere waarden in een bepaalde blueprint overschrijven wanneer deze wordt geïmplementeerd.

De lijst met meegeleverde aangepaste eigenschappen van Active Directory is opgenomen in de *Naslaggids voor aangepaste eigenschappen*. Het voorvoegsel van de aangepaste eigenschappen is `ext.policy.activedirectory`.

Naast de bijgeleverde eigenschappen kunt u uw eigen aangepaste eigenschappen maken. Uw aangepaste eigenschappen moeten het voorvoegsel `ext.policy.activedirectory` hebben. Bijvoorbeeld, `ext.policy.activedirectory.domain.extension` of `ext.policy.activedirectory.yourproperty`. De eigenschappen worden doorgegeven aan uw aangepaste vRealize Orchestrator Active Directory-werkstromen.

Zie *Naslaggids voor aangepaste eigenschappen* voor meer informatie over aangepaste eigenschappen. Afhankelijk van de waarden die u overschrijft, moet u mogelijk een eigenschapsdefinitie maken. U kunt bijvoorbeeld een eigenschapsdefinitie maken die het beschikbare Active Directory-beleid ophaalt van vRealize Automation. Of u kunt een definitie maken die de aanvrager toestaat twee of meer alternatieve organisatie-eenheden te selecteren. Zie *Naslaggids voor aangepaste eigenschappen*.

Active Directory-beleid maken en toepassen

U maakt één of meer dan één Active Directory-beleid zodat u een verschillend beleid kunt toewijzen aan verschillende bedrijfsgroepen. Een verschillend beleid maakt het mogelijk

machinerecords toe te voegen aan verschillende organisatie-eenheden op basis van lidmaatschap van een bedrijfsgroep.

Indien nodig kunt u het toegewezen Active Directory-beleid overschrijven.

Procedure

1 Een Active Directory-beleid maken

U maakt een Active Directory-beleid om te bepalen waar records worden toegevoegd in een Active Directory-instantie wanneer uw gebruikers machines implementeren. U kunt een beleid toewijzen aan een bedrijfsgroep zodat alle machine-implementaties door leden van de bedrijfsgroep tot gevolg hebben dat een record wordt aangemaakt in de opgegeven organisatie-eenheid.

2 Scenario: een aangepaste eigenschap toevoegen aan blueprints om een Active Directory-beleid te overschrijven

Als blueprintarchitect voor de bedrijfsgroep ontwikkeling hebt u een blueprint die een toepassingsmachine en een databasemachine omvat. U wilt dat de databasemachinerecord aan een andere organisatie-eenheid wordt toegevoegd dan is opgegeven in het toegepaste Active Directory-beleid.

Een Active Directory-beleid maken

U maakt een Active Directory-beleid om te bepalen waar records worden toegevoegd in een Active Directory-instantie wanneer uw gebruikers machines implementeren. U kunt een beleid toewijzen aan een bedrijfsgroep zodat alle machine-implementaties door leden van de bedrijfsgroep tot gevolg hebben dat een record wordt aangemaakt in de opgegeven organisatie-eenheid.

U maakt meer dan één Active Directory-beleid als u wilt dat machines die door verschillende bedrijfsgroepen zijn geïmplementeerd, verschillende domeinen hebben of worden toegevoegd aan verschillende Active Directory-instanties.

Voorwaarden

- Controleer of u een Active Directory-endpoint hebt gemaakt. Zie [De Active Directory-invoegtoepassing configureren als endpoint](#).
- Als u een externe vRealize Orchestrator-server gebruikt, controleert u of deze correct is ingesteld. Zie [Een externe vRealize Orchestrator-server configureren](#).
- Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > Active Directory-beleid**.
- 2 Klik op het pictogram **Nieuw** (+).

3 Configureer de details van het Active Directory-beleid.

Optie	Beschrijving
Id	Voer de permanente waarde in. De waarde mag geen spaties of speciale tekens bevatten. U kunt deze waarde later niet wijzigen. U kunt het beleid alleen opnieuw maken met een andere id.
Beschrijving	Beschrijf het beleid.
Active Directory-endpoint	Selecteer het Active Directory-endpoint waarvoor dit beleid wordt gemaakt.
Domein	Voer het hoofddomein in. De notatie is <i>mycompany.com</i> .
Organisatie-eenheid	Voer de Distinguished Name van de organisatie-eenheid in voor dit beleid. De hiërarchie moet worden ingevoerd als een door komma's gescheiden lijst. Bijvoorbeeld, <i>ou=development,dc=corp,dc=domain,dc=com</i> .

4 Klik op **OK**.

Resultaten

Het vRealize Orchestrator Active Directory-endpoint wordt toegevoegd aan de lijst. U kunt het beleid toepassen in bedrijfsgroepen of gebruiken in blueprints of bedrijfsgroepen.

Wat nu te doen

- Maak meer dan één beleid als u meerdere beleidsopties wilt bieden.
- Als u wilt dat records worden toegevoegd aan Active Directory op basis van het lidmaatschap van een bedrijfsgroep wanneer een blueprint wordt geïmplementeerd, voegt u het juiste Active Directory-beleid toe aan een bedrijfsgroep. Zie [Een bedrijfsgroep maken](#). U kunt het beleid toepassen wanneer u de bedrijfsgroep maakt of later toevoegen.
- Als u het Active Directory-beleid van de bedrijfsgroep wilt overschrijven voor een bepaalde blueprint, voegt u aangepaste eigenschappen van Active Directory toe aan de blueprint. Zie [Scenario: een aangepaste eigenschap toevoegen aan blueprints om een Active Directory-beleid te overschrijven](#).

Scenario: een aangepaste eigenschap toevoegen aan blueprints om een Active Directory-beleid te overschrijven

Als blueprintarchitect voor de bedrijfsgroep ontwikkeling hebt u een blueprint die een toepassingsmachine en een databasemachine omvat. U wilt dat de databasemachinerecord aan een andere organisatie-eenheid wordt toegevoegd dan is opgegeven in het toegepaste Active Directory-beleid.

U hebt een bestaand beleid dat wordt toegepast op de bedrijfsgroep ontwikkeling. Het beleid voegt machinerecords toe aan *ou=development,dc=corp,dc=domain,dc=com*. U wilt dat alle databasemachines worden toegevoegd aan *ou=databases,dc=corp,dc=domain,dc=com*. In een blueprint die een databaseserver bevat, overschrijft u de organisatie-eenheid van Active Directory om de databasemachinerecord toe te voegen aan *ou=databases,dc=corp,dc=domain,dc=com*.

Dit scenario gaat uit van de volgende veronderstellingen:

- Uw Active Directory omvat organisatie-eenheden voor ontwikkeling en databases.
- U hebt een testblueprint die is opgenomen in een service en rechten voor deze service zijn verleend.

Dit was een eenvoudig voorbeeld van hoe u het beleid kunt overschrijven. Daarnaast kunt u samen met het Active Directory-beleid aangepaste eigenschappen gebruiken om andere wijzigingen aan Active Directory aan te brengen bij het implementeren van blueprints. Zie [Werken met een Active Directory-beleid](#).

Voorwaarden

- Controleer of u ten minste één Active Directory-beleid hebt. Zie [Een Active Directory-beleid maken](#). U maakt bijvoorbeeld een ontwikkelingsbeleid dat records toevoegt aan `ou=development,dc=corp,dc=domain,dc=com`.
- Controleer of u een bedrijfsgroep hebt waarop u een Active Directory-beleid hebt toegepast. Zie [Een bedrijfsgroep maken](#). Uw bedrijfsgroep ontwikkeling gebruikt bijvoorbeeld het ontwikkelingsbeleid.

Procedure

- 1 Selecteer de databasemachine in het ontwerpcanvas van uw testblueprint.
- 2 Klik op het tabblad **Eigenschappen**.
- 3 Klik op het tabblad **Aangepaste eigenschappen**.
- 4 Klik op het pictogram **Nieuw (+)**.
- 5 Voeg de aangepaste eigenschap toe om de standaard ingestelde organisatie-eenheid te wijzigen.
 - a Voer in het tekstvak **Naam** de tekst `ext.policy.activedirectory.orgunit` in.
 - b Voer in het tekstvak **Waarde** de tekst `ou=databases,dc=corp,dc=domain,dc=com` in.
 - c Schakel **Overschrijfbaar** uit.
 - d Klik op **OK**.
- 6 Klik op **Voltooien**.

Resultaten

De testblueprint bevat de aangepaste eigenschap, maar uw gebruikers zien de aangepaste eigenschap niet in het aanvraagformulier.

Wat nu te doen

Vraag uw testblueprint aan. Controleer of de record voor de databasemachine is toegevoegd aan de organisatie-eenheid voor databases en dat de record voor de toepassingsmachine is toegevoegd aan de organisatie-eenheid voor ontwikkeling. Bent u tevreden met de resultaten, dan kunt u de aangepaste eigenschap toevoegen aan uw productieblueprints.

Gebruikersvoorkeuren voor meldingen en afgevaardigden

U gebruikt de gebruikersvoorkeuren om de standaardconfiguraties van uw systeemgoedkeurdersmeldingen en meldingstaalvoorkeuren te overschrijven.

U kunt de gebruikersvoorkeuren openen door te klikken op uw gebruikersnaam in de koptekst van vRealize Automation en **Voorkeuren** te selecteren.

De volgende opties zijn specifiek voor u als de aangemelde gebruiker.

Tabel 2-21. Gebruikersvoorkeursopties

Optie	Beschrijving
Afgevaardigden toewijzen	Hiermee kunt u uw goedkeuringsaanvragen aan andere gebruikers toewijzen. Bijvoorbeeld: u bent de goedkeurder voor catalogusaanvragen, maar u gaat op vakantie. U delegeert al uw goedkeuringsmeldingen naar een of meer goedkeurders. Deze toewijzing stuurt de verzoeken onmiddellijk door naar uw afgevaardigde. De delegaties zijn actief totdat u ze uit de lijst verwijdt.
Meldingen	Hiermee kunt u uw meldingstaal wijzigen zodat de e-mailberichten in uw voorkeurstaal naar u worden verzonden, in plaats van in de standaardtaal. Selecteer de taal en voeg het meldingsabonnement toe dat overeenkomt met uw taalvoorkeur.

Serviceblueprints aanbieden aan gebruikers

3

U levert services op aanvraag aan gebruikers door catalogusitems en acties te maken en vervolgens rechten en goedkeuringen te verlenen om zorgvuldig te bepalen wie deze services mag aanvragen.

Dit hoofdstuk omvat de volgende onderwerpen:

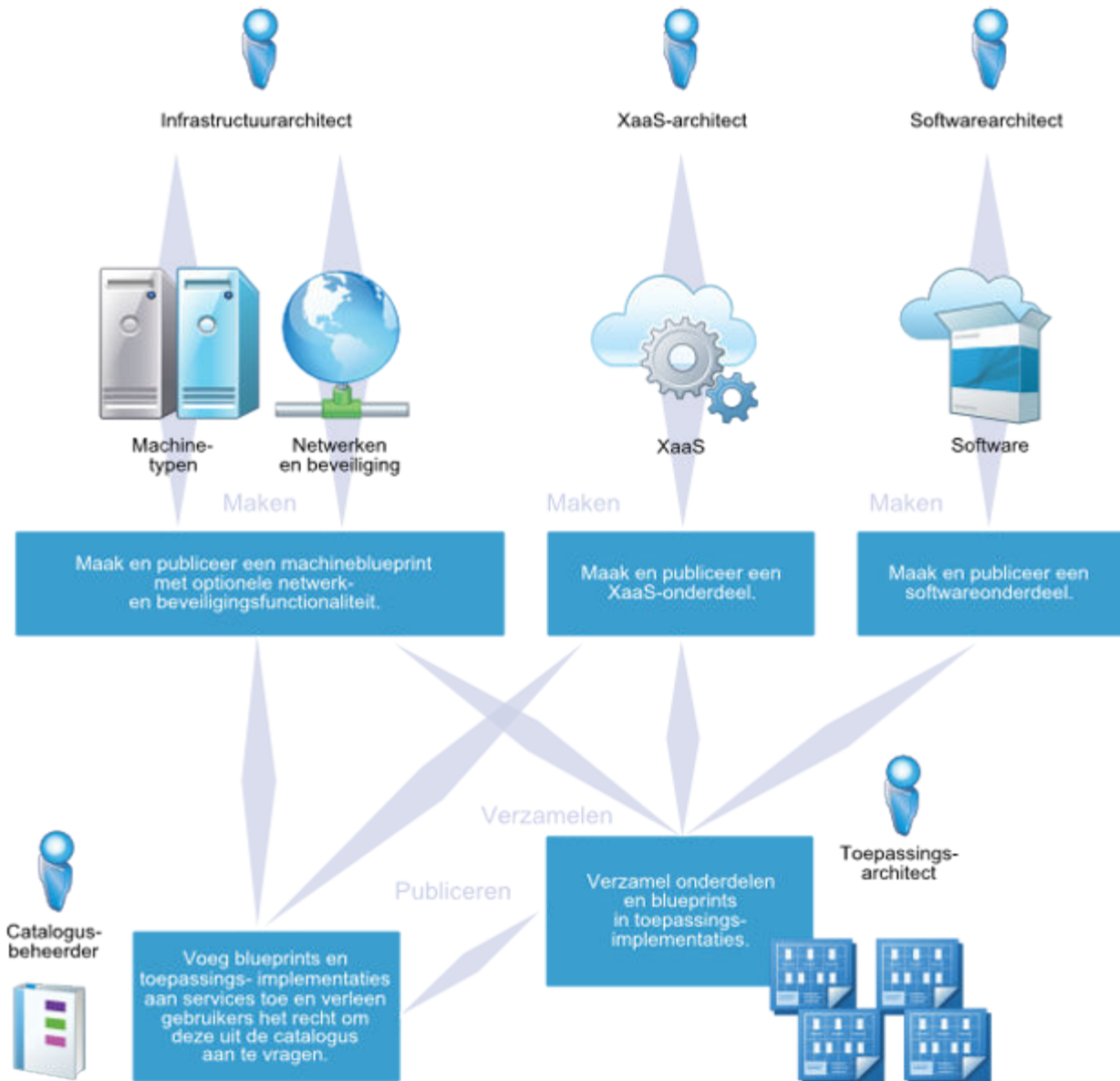
- [Blueprints ontwerpen](#)
- [Uw ontwerpbibliotheek opbouwen](#)
- [Werken met door ontwikkelaar gestuurde blueprints](#)
- [Samengestelde blueprints samenstellen](#)
- [Aanpassen van blueprint-aanvraagformulieren](#)
- [Mislukte provisioning-aanvragen testen en problemen oplossen](#)
- [De servicecatalogus beheren](#)

Blueprints ontwerpen

Blueprintarchitecten bouwen Software-onderdelen, machineblueprints en aangepaste XaaS-blueprints en gebruiken deze onderdelen om blueprints samen te stellen die bepalen welke items gebruikers kunnen aanvragen uit de catalogus. Een standaardaanvraagformulier kan worden weergegeven in de catalogus, of u kunt een aangepast formulier voor elke gepubliceerde blueprint maken.

U kunt blueprints voor afzonderlijke machines of afzonderlijke aangepaste XaaS-blueprints maken en publiceren, maar ook machineonderdelen en XaaS-blueprints combineren met andere bouwstenen om blueprints te maken voor meer complexe catalogusitems zoals diverse machines, Networking and Security, software met complete levenscyclusondersteuning, en aangepaste XaaS-functionaliteit.

Afhankelijk van het catalogusitem dat u wilt definiëren, kan het een simpel proces zijn waarbij één infrastructuurarchitect één machineonderdeel publiceert als een blueprint. Maar het kan ook een proces zijn waarbij meerdere architecten zijn betrokken en allerlei typen onderdelen worden gemaakt zodat gebruikers een complete toepassingsstack kunnen aanvragen.



Onderdelen van Software

U kunt softwareonderdelen maken en publiceren ten behoeve van de software-installatie door gebruikers tijdens de machine-inrichting en ter ondersteuning van de levenscyclus van de software. U kunt bijvoorbeeld een blueprint voor ontwikkelaars maken waarmee ze een machine kunnen aanvragen waarbij hun ontwikkelomgeving al is geïnstalleerd en geconfigureerd. Softwareonderdelen kunnen op zichzelf geen catalogusitem zijn. U moet ze combineren met een machineonderdeel om een blueprint als catalogusitem te maken. Zie [Software-onderdelen ontwerpen](#).

Machineblueprints

U kunt eenvoudige blueprints voor het inrichten van afzonderlijke machines maken en publiceren of u kunt complexere blueprints maken die extra machineonderdelen bevatten en eventueel een combinatie van de volgende onderdeelstypen:

- Onderdelen van Software
- Bestaande blueprints
- NSX-netwerkonderdelen en -beveiligingsonderdelen
- Onderdelen van XaaS
- Onderdelen van Containers
- Aangepaste onderdelen of andere onderdelen

Zie [Machineblueprints ontwerpen](#).

XaaS-blueprints

U kunt uw vRealize Orchestrator-werkstromen publiceren als XaaS-blueprints. U kunt bijvoorbeeld een aangepaste bron voor Active Directory-gebruikers maken en een XaaS-blueprint ontwerpen waarmee u beheerders nieuwe gebruikers laat inrichten in hun Active Directory-groep. U maakt en beheert de XaaS-onderdelen buiten het ontwerptabblad om. U kunt gepubliceerde XaaS-blueprints opnieuw gebruiken om een toepassingsblueprint te maken. Dit kan echter alleen in combinatie met minimaal één machineonderdeel. Zie [XaaS-blueprints en bronacties ontwerpen](#).

Toepassingsblueprints met meerdere machines, XaaS- en Software-onderdelen

U kunt een willekeurig aantal machineonderdelen, Software-onderdelen en XaaS-blueprints toevoegen aan machineblueprint om gebruikers een doorwrochte functionaliteit te bieden.

U kunt bijvoorbeeld een blueprint voor beheerders maken om een personeelsaanstelling in te richten. Voor de inrichting van nieuwe Active Directory-gebruikers kunt u een combinatie maken van meerdere machineonderdelen, softwareonderdelen en een XaaS-blueprint. De QE-beheerder kan dan uw catalogusitem Nieuw personeel aanvragen voor de inrichting van de nieuwe kwaliteitsmedewerker in Active Directory om hem met twee virtuele machines te laten werken, een voor Windows en een voor Linux, elk voorzien van alle vereiste software om testcases in deze omgevingen uit te voeren.

Uw ontwerpbibliotheek opbouwen

U kunt een bibliotheek met herbruikbare blueprintonderdelen maken die uw architecten kunnen samenstellen tot toepassingsblueprints voor het leveren van uitgebreide services op aanvraag aan gebruikers.

Bouw een bibliotheek op met de kleinste ontwerponderdelen voor blueprints: eenvoudige machineblueprints, Software-onderdelen en XaaS-blueprints en combineer deze basisbouwstenen op allerlei nieuwe manieren om uitgebreide catalogusitems te maken die steeds meer functionaliteit bieden aan uw gebruikers.

Voorbeeldblueprints zijn beschikbaar in de VMware Solution Exchange op <https://solutionexchange.vmware.com> en op <https://code.vmware.com>.

Tabel 3-1. Uw ontwerpbibliotheek opbouwen

Catalogusitem	Rol	Onderdelen	Beschrijving	Details
Machines	Infrastructuurarchitect	Maak machineblueprints op het tabblad Blueprints .	U kunt machineblueprints maken om uw gebruikers snel te voorzien van machines voor virtuele, particuliere, openbare of hybride clouds. Catalogusbeheerders kunnen gepubliceerde machineblueprints als zodanig in de catalogus opnemen. U kunt machineblueprints echter ook met andere onderdelen combineren om meer uitgebreide catalogusitems samen te stellen met machineblueprints, Software- of XaaS-blueprints.	Een machineblueprint configureren
NSX-netwerk en -beveiliging voor machines	Infrastructuurarchitect	U kunt NSX-onderdelen voor netwerken en beveiliging toevoegen aan vSphere-machineblueprints op het tabblad Blueprints .	U kunt netwerk- en beveiligingsonderdelen, zoals netwerkprofielen en beveiligingsgroepen, configureren zodat virtual machines in fysieke en virtuele netwerken veilig en efficiënt met elkaar kunnen communiceren. U moet de netwerk- en beveiligingsonderdelen met minimaal één vSphere-machineonderdeel combineren voordat een catalogusbeheerder ze in de catalogus kan opnemen. U kunt uitsluitend NSX-onderdelen voor netwerken en beveiliging aan vSphere-machineblueprints toevoegen.	Blueprints met NSX-instellingen ontwerpen

Tabel 3-1. Uw ontwerpbibliotheek opbouwen (vervolg)

Catalogusitem	Rol	Onderdelen	Beschrijving	Details
Software op machines	Softwarearchitect Om softwareonderdelen met succes aan het ontwerpcanvas toe te voegen, moet u ook toegang als bedrijfsgroeps lid, bedrijfsgroepbeheerder of tenantbeheerder tot de doelcatalogus hebben.	Maak en publiceer Software-onderdelen op het tabblad Software en combineer deze met machineblueprints op het tabblad Blueprints .	Voeg Software-onderdelen toe aan uw machineblueprints om complexe toepassingen in een cloudomgeving te standaardiseren, implementeren, configureren, updaten en schalen. Dit kunnen toepassingen zijn van eenvoudige webtoepassingen tot uitgebreide aangepaste toepassingen en gebundelde toepassingen. Software-onderdelen kunnen niet zelfstandig in de catalogus worden opgenomen. U moet uw Software-onderdelen eerst maken en publiceren en vervolgens een toepassingsblueprint als catalogusitem samenstellen met ten minste één machine.	Een Softwareonderdeel maken
Aangepaste IT-services	XaaS-architecten	Maak en publiceer XaaS-blueprints op het tabblad XaaS .	U kunt XaaS-catalogusitems maken met een vRealize Automation-functionaliteit die verder reikt dan de inrichting van machines, netwerken, beveiligingen en software. U kunt de levering van IT-services automatiseren met behulp van bestaande vRealize Orchestrator-werkstromen en invoegtoepassingen of aangepaste scripts die u ontwikkelt in vRealize Orchestrator. Catalogusbeheerders kunnen gepubliceerde XaaS-blueprints als zodanig in de catalogus opnemen. U kunt ze echter ook met andere onderdelen samenvoegen op het tabblad Blueprints om meer uitgebreide catalogusitems samen te stellen.	XaaS-blueprints en bronacties ontwerpen
Gepubliceerde blueprint-bouwstenen samenstellen tot nieuwe catalogusitems	<ul style="list-style-type: none"> ■ Toepassingsarchitect ■ Infrastructuurarchitect ■ Softwarearchitect 	Combineer aanvullende machineblueprints, XaaS-blueprints en Software-onderdelen met ten minste een machineonderdeel of een machineblueprint op het tabblad Blueprints .	U kunt gepubliceerde onderdelen en blueprints gebruiken en deze op nieuwe manieren combineren voor het maken van IT-servicepakketten die uitgebreide functionaliteit bieden aan gebruikers.	Samengestelde blueprints samenstellen

Machineblueprints ontwerpen

Machineblueprints zijn de volledige specificatie voor een machine. Ze bepalen de kenmerken van een machine, de manier waarop deze wordt ingericht en de beleids- en beheerinstellingen van de machine. Afhankelijk van de complexiteit van het catalogusitem dat u bouwt, kunt u een of meer machineonderdelen in de blueprint combineren met andere onderdelen in het ontwerpcanvas om meer complexe catalogusitems te maken die netwerk en beveiliging, Software-onderdelen, XaaS-onderdelen en andere blueprintonderdelen bevatten.

Ruimtebesparende opslag voor virtuele inrichting

Een ruimtebesparende opslagtechnologie heft tekortkomingen van traditionele opslagmethoden op door de opslag te beperken tot de ruimte die werkelijk vereist is voor de machinebewerkingen. Doorgaans is dit maar een fractie van de werkelijk toegewezen opslagruimte voor de machines. vRealize Automation ondersteunt twee inrichtingsmethoden met een ruimtebesparende technologie: thin provisioning en FlexClone-inrichting.

Bij standaardopslag is de toegewezen opslagruimte voor een ingerichte machine in zijn geheel bestemd voor die machine, ook wanneer deze uitgeschakeld is. Dit kan tot een aanzienlijke verspilling van opslagbronnen leiden. Er zijn immers maar weinig virtual machines die alle toegewezen ruimte ook daadwerkelijk gebruiken, net zoals als er maar weinig fysieke machines in bedrijf zijn met een volledig volle schijf. Wanneer u een ruimtebesparende technologie gebruikt, worden de toegewezen opslag en gebruikte opslag afzonderlijk bijgehouden en wordt alleen de gebruikte opslagruimte daadwerkelijk ingezet voor de ingerichte machine.

Thin provisioning

Thin provisioning wordt ondersteund voor alle virtuele inrichtingsmethoden. Afhankelijk van uw virtualisatieplatform, opslagtype en ingestelde standaardopslag, kan thin provisioning altijd als mogelijkheid worden overwogen bij de machine-inrichting. Thin provisioning wordt bijvoorbeeld altijd ingezet bij vSphere ESX Server-integraties die gebruikmaken van NFS-opslag. Bij vSphere ESX Server-integraties die gebruikmaken van lokale of iSCSI-opslag, wordt thin provisioning echter alleen gebruikt voor de machine-inrichting als de aangepaste eigenschap `VirtualMachine.Admin.ThinProvision` is opgegeven op de blueprint. Zie de documentatie van uw virtualisatieplatform voor meer informatie over thin provisioning.

Net App FlexClone-inrichting

U kunt een blueprint voor Net App FlexClone-inrichting maken als u in een vSphere-omgeving werkt waarin NFS-opslag (Network File System) en FlexClone-technologie worden gebruikt.

U kunt alleen NFS-opslag gebruiken. Anders mislukt de inrichting. U kunt een FlexClone-opslagpad voor andere soorten machine-inrichting opgeven, maar het FlexClone-opslagpad functioneert als standaardopslag.

Hier volgt een algemeen overzicht van de vereiste stappen voor het inrichten van machines die gebruikmaken van de FlexClone-technologie:

- 1 Een IaaS-beheerder maakt een NetApp ONTAP-endpoint. Zie [Naslaginformatie endpointinstellingen](#).

- 2 Een IaaS-beheerder voert een gegevensverzameling uit op het endpoint, zodat het endpoint wordt weergegeven op de computerbron en reserveringspagina's.

De FlexClone-optie wordt in de endpointkolom van de reserveringspagina weergegeven als een NetApp ONTAP-endpoint bestaat en er een virtuele host is. Als er een NetApp ONTAP-endpoint is, wordt op de reserveringspagina het endpoint weergegeven dat is gekoppeld aan het opslagpad.

- 3 Een materiaalbeheerder maakt een vSphere-reservering, schakelt de FlexClone-opslag in en geeft het NFS-opslagpad voor de FlexClone-technologie op. Zie [Een reservering maken voor Hyper-V, KVM, SCVMM, vSphere of XenServer](#).
- 4 Een infrastructuurarchitect of andere bevoegde gebruiker maakt een blueprint voor FlexClone-inrichting.

Het toewijzen van parameters aan blueprints begrijpen en gebruiken

U kunt parameters aan blueprints toewijzen via onderdeelprofielen. U hoeft dan geen afzonderlijke kleine, normale en grote blueprint voor een specifiek type implementatie te maken, maar kunt één blueprint maken met een keuze van een kleine, normale of grote virtual machine. Gebruikers kunnen een van deze formaten selecteren wanneer ze het catalogusitem implementeren.

Onderdeelprofielen beperken het uitdijen van blueprints en vereenvoudigen uw catalogusaanbiedingen. Met onderdeelprofielen kunt u vSphere-machineonderdelen in een blueprint definiëren. De beschikbare onderdeelprofieltypen zijn *Size* en *Image*. Wanneer u onderdeelprofielen aan een machineonderdeel toevoegt, overschrijven de instellingen van het onderdeelprofiel andere instellingen van het machineonderdeel, zoals aantal CPU's of hoeveelheid opslagruimte.

Onderdeelprofielen zijn alleen beschikbaar voor vSphere-machineonderdelen.

Zie in *Naslaggids voor aangepaste eigenschappen* voor informatie over het definiëren van waardesets voor de onderdeelprofielen *Size* en *Image*.

Zie [Instellingen voor vSphere-machineonderdelen in vRealize Automation](#) voor informatie over het toevoegen van onderdeelprofielen en geselecteerde waardesets voor een vSphere-machineonderdeel in een blueprint.

Voor informatie over het toevoegen van onderdeelprofielgegevens met behulp van instellingen die zijn geïmporteerd vanaf een OVF, raadpleegt u [Een blueprint configureren om in te richten vanaf een OVF](#).

Zie [Machine-inrichting aanvragen met behulp van een blueprint met parameters](#) voor informatie over het gebruik van onderdeelprofielen wanneer u machine-inrichting aanvraagt.

U kunt goedkeuringsbeleid maken om voorafgaande goedkeuring te vereisen wanneer u machine-inrichting aanvraagt van blueprints met betrekking tot waardesetvoorwaarden voor het onderdeelprofiel Size en Image. Zie [Voorbeelden van goedkeuringsbeleid op basis van beleidstypen voor virtual machines](#) voor meer informatie.

Opmerking

Zie [Machine-inrichting aanvragen met behulp van een blueprint met parameters](#) voor informatie over het gebruik van parameters in blueprints wanneer u machine-inrichting aanvraagt uit de catalogus.

Een machineblueprint configureren

Configureer en publiceer een machineonderdeel als een stand-aloneblueprint die andere architecten opnieuw kunnen gebruiken als een onderdeel in toepassingsblueprints, en die catalogusbeheerders kunnen opnemen in catalogusservices.

Deze procedure biedt een eenvoudig overzicht van het proces voor het maken van blueprints. Voor meer informatie raadpleegt u het volgende:

- [Blueprints met NSX-instellingen ontwerpen](#)
- [Het toewijzen van parameters aan blueprints begrijpen en gebruiken](#)
- [Instellingen voor blueprunteigenschappen](#)
- [Een blueprint configureren om in te richten vanaf een OVF](#)
- [Blueprints en inhoud exporteren en importeren](#)
- [Microsoft Azure-blueprints maken en bronacties hierin opnemen](#)
- [Configuratiebeheermogelijkheden toevoegen aan vSphere-blueprints](#)

Voorwaarden

- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Voltooi externe voorbereidingen voor inrichting, zoals het maken van sjablonen, WinPE's en ISO's, of verzamel de informatie over externe voorbereidingen van uw beheerders.
- Configureer uw tenant. Zie [Tenantinstellingen configureren](#).
- Configureer uw IaaS-bronnen. Zie [Checklist voor het configureren van IaaS-bronnen](#).
- Zie *vRealize Automation configureren*.

Procedure

- 1 Selecteer **Ontwerpen > Blueprints**.
- 2 Klik op het pictogram **Nieuw** (+).
- 3 Volg de instructies in het dialoogvenster **Nieuwe blueprint** om de algemene instellingen te configureren.

- 4 Klik op **OK**.
- 5 Klik op **Machinetypen** in het gebied Categorieën om een lijst met beschikbare machinetypen weer te geven.
- 6 Sleep het machinetype dat u wilt inrichten naar het ontwerpcanvas.
- 7 Voer informatie in op elk van de tabbladen om de details van de machine-inrichting te configureren, zoals beschreven in [Instellingen voor blueprinteigenschappen](#).
- 8 Klik op **Voltooien**.
- 9 Selecteer de blueprint en klik op **Publiceren**.

Resultaten

U hebt een machineonderdeel geconfigureerd en gepubliceerd als een stand-aloneblueprint. Catalogusbeheerders kunnen deze machineblueprint in catalogusservices opnemen en aan gebruikers rechten verlenen om deze blueprint aan te vragen. Andere architecten kunnen deze machineblueprint opnieuw gebruiken om meer complexe toepassingsblueprints te maken die Software-onderdelen, XaaS-blueprints of aanvullende machineblueprints bevatten.

Wat nu te doen

U kunt een machineblueprint combineren met Software-onderdelen, XaaS-blueprints of aanvullende machineblueprints om meer complexe toepassingsblueprints te maken. Zie [Samengestelde blueprints samenstellen](#) en [Informatie over genest blueprintgedrag](#).

Instellingen voor machineblueprints

U kunt configuratie-instellingen en aangepaste eigenschappen opgeven voor de algehele blueprint.

Instellingen voor blueprinteigenschappen

U kunt instellingen opgeven die gelden voor de hele blueprint, door de pagina **Blueprinteigenschappen** te gebruiken wanneer u de blueprint maakt. Als u de blueprint hebt gemaakt, kunt u deze instellingen bewerken op de pagina Blueprinteigenschappen.

Tabblad Algemeen

Instellingen op het tabblad Algemeen zijn van toepassing op de gehele vRealize Automation-blueprint.

Tabel 3-2. Instellingen tabblad **Algemeen**

Instelling	Beschrijving
Naam	Voer een naam in voor uw blueprint.
Id	Het id-veld wordt automatisch ingevuld op basis van de door u ingevoerde naam. U kunt dit veld nu bewerken, maar u kunt het niet meer wijzigen nadat u de blueprint hebt opgeslagen. Identificatie is permanent en uniek binnen de tenant. U kunt deze gebruiken om via programmering met blueprints te werken en om eigenschapsbindingen te maken.
Beschrijving	Vat uw blueprint samen ten behoeve van andere architecten. Deze beschrijving wordt ook voor gebruikers op het aanvraagformulier weergegeven.
Implementatielimiet	Geef aan hoeveel implementaties er maximaal kunnen worden gemaakt wanneer u deze blueprint gebruikt voor het inrichten van machines.
Aantal leasedagen: Minimum en Maximum	<p>Voer een minimum- en een maximumwaarde in om gebruikers de keuze te geven in een bereik van leaseduren. Wanneer de lease eindigt, wordt de implementatie vernietigd dan wel gearchiveerd. Als u geen minimum- of maximumwaarde opgeeft, komt de lease nooit te vervallen.</p> <p>Voer de lease-informatie voor uw machines in uw vRealize Automation-blueprint in en niet in de toepassing van het oorspronkelijke endpoint. Als u de lease-informatie in een externe toepassing opgeeft, wordt deze niet herkend in vRealize Automation.</p>
Archiefdagen	U kunt een archiveringsperiode opgeven om implementaties tijdelijk te behouden in plaats van implementaties te vernietigen zodra hun lease verloopt. Geef 0 op om de implementatie te vernietigen zodra de bijbehorende lease verloopt. De archiefperiode begint op de dag dat de lease verloopt. Wanneer de archiefperiode eindigt, wordt de implementatie vernietigd. De standaardwaarde is 0.
Updates voor bestaande implementaties doorvoeren	Ruimere minimum-maximumbereiken voor CPU, geheugen of opslag worden gepusht naar actieve implementaties die zijn ingericht vanaf de blueprint. Het nieuwe bereik moet het oude bereik volledig insluiten. Bijvoorbeeld: als het minimum oorspronkelijk 32 is en het maximum 128 (32, 128), kan een wijziging zoals (16, 128) of (32, 256) of (2, 1000) worden toegepast bij herconfiguratie of uitschaling, maar een wijziging zoals (33, 512) of (4, 64) niet.

Tabblad **NSX-instellingen**

Als u NSX hebt geconfigureerd, kunt u bij het maken of bewerken van een blueprint NSX-instellingen opgeven voor de transportzone, het netwerkreserveringsbeleid en de app-isolatie. Deze instellingen zijn beschikbaar op het tabblad **NSX-instellingen** van de pagina's **Blueprint** en **Blueprinteigenschappen**.

Voor meer informatie over NSX-instellingen raadpleegt u [Instellingen op de pagina's Nieuwe blueprint en Blueprinteigenschappen voor NSX in vRealize Automation](#).

Tabblad Eigenschappen

Aangepaste eigenschappen die u op blueprintniveau toevoegt, zijn van toepassing op de gehele blueprint, inclusief alle onderdelen. Zie *Naslaggids voor aangepaste eigenschappen* voor informatie over de voorrangsvolgorde.

Tabel 3-3. Instellingen tabblad Eigenschappen

Tabblad	Instelling	Beschrijving
Eigenschapsgroepen	Eigenschapsgroepen zijn herbruikbare groepen met eigenschappen om het toevoegen van aangepaste eigenschappen aan blueprints te vereenvoudigen.	
	Toevoegen	Voeg hiermee een of meer bestaande eigenschapsgroepen toe en pas deze toe op de algehele blueprint. De volgende aan Containers gerelateerde eigenschapsgroepen zijn beschikbaar: <ul style="list-style-type: none"> ■ Eigenschappen voor containerhosts met certificaatverificatie ■ Eigenschappen voor containerhosts met verificatie op basis van gebruikers/wachtwoorden
	Naar boven /Naar beneden	Beheer de voorrangsvolgorde die u aan alle eigenschapsgroepen ten opzichte van elkaar hebt gegeven door prioriteiten in te stellen voor groepen. De eerste groep in de lijst heeft de hoogste prioriteit en de aangepaste eigenschappen ervan hebben als eerste voorrang. U kunt ook schuiven om de volgorde te wijzigen.
	Eigenschappen weergeven	Geef de aangepaste eigenschappen in de geselecteerde eigenschapsgroep weer.
	Samengevoegde eigenschappen weergeven	Als een aangepaste eigenschap in meer dan één eigenschapsgroep is opgenomen, krijgt de waarde die in de eigenschapsgroep met de hoogste prioriteit is opgenomen voorrang.
Aangepaste eigenschappen	U kunt individuele aangepaste eigenschappen toevoegen in plaats van eigenschapsgroepen.	
	Nieuw	Voeg hiermee een individuele aangepaste eigenschap toe en pas deze toe op de algehele blueprint.
	Naam	Voer de eigenschapsnaam in. Zie <i>Naslaggids voor aangepaste eigenschappen</i> voor een lijst met aangepaste eigenschappen en hun definities.
	Waarde	Voer de waarde in voor de aangepaste eigenschap.

Tabel 3-3. Instellingen tabblad **Eigenschappen** (vervolg)

Tabblad	Instelling	Beschrijving
	Versleuteld	Versleutel de eigenschapswaarde, bijvoorbeeld als de waarde een wachtwoord is.
	Overschrijfbaar	De blueprintgebruiker kan de eigenschapswaarde overschrijven. Als u Weergeven in aanvraag selecteert, kunnen gebruikers eigenschapswaarden zien en bewerken wanneer ze catalogusitems aanvragen.
	Weergeven in aanvraag	De eigenschapsnaam en -waarde zijn zichtbaar voor gebruikers op het inrichtingsaanvraagformulier. Selecteer Overschrijfbaar als u gebruikers wilt toestaan om een waarde op te geven.

Instellingen voor vSphere-machineonderdelen in vRealize Automation

Krijg inzicht in de instellingen en opties die u voor een vSphere-machineonderdeel in het ontwerpcanvas van de vRealize Automation-blueprint kunt configureren.

Tabblad **Algemeen**

Hier configureert u algemene instellingen voor een vSphere-machineonderdeel.

Tabel 3-4. Instellingen tabblad **Algemeen**

Instelling	Beschrijving
Id	Voer een naam in voor uw machineonderdeel of accepteer de standaardwaarde.
Beschrijving	Vat uw machineonderdeel samen ten behoeve van andere architecten.
Locatie op verzoek weergeven	In een cloudomgeving, zoals vCloud Air, kunnen gebruikers een regio selecteren voor hun ingerichte machines. Voor een virtuele omgeving kunt u gebruikers een datacentrumlocatie laten selecteren voor het inrichten van een aangevraagde machine. Een systeembeheerder moet informatie over het datacentrum toevoegen aan een locatiebestand. Een materiaalbeheerder moet een computerbron bewerken om deze aan een locatie te koppelen.
Reserveringsbeleid	Pas een reserveringsbeleid toe op een blueprint om het aantal machines dat op basis van die blueprint wordt ingericht, te beperken tot een subset met beschikbare reserveringen. Alleen het reserveringsbeleid dat van toepassing is op de huidige tenant, is beschikbaar.

Tabel 3-4. Instellingen tabblad **Algemeen** (vervolg)

Instelling	Beschrijving
Machinevoorvoegsel	<p>Machinevoorvoegsels worden gebruikt om ingerichte machines een naam te geven. Als u Standaardinstelling van groep gebruiken selecteert, krijgen machines een naam die is gebaseerd op het standaardvoorvoegsel van de machine voor uw bedrijfsgroep. Als u geen voorvoegsel opgeeft, wordt er een gegenereerd op basis van de naam van uw bedrijfsgroep. Alleen de machinevoorvoegsels die van toepassing zijn op de huidige tenant, zijn beschikbaar.</p> <p>Als uw materiaalbeheerder andere machinevoorvoegsels configureert die u kunt selecteren, dan kunt u één voorvoegsel toepassen op alle machines die vanaf uw blueprint zijn ingericht, ongeacht wie de aanvrager is.</p>
Instanties: Minimum en Maximum	<p>Configureer het maximale en het minimale aantal instanties dat gebruikers kunnen aanvragen voor een implementatie of een op- of neerschaalbewerking. Door dezelfde waarde in te voeren in de velden Minimum en Maximum, configureert u het exacte aantal instanties geconfigureerd dat moet worden ingericht.</p> <p>XaaS-onderdelen zijn niet schaalbaar en kunnen niet worden bijgewerkt tijdens een schalingsbewerking. Als u XaaS-onderdelen in uw blueprint gebruikt, kunt u een bronactie voor gebruikers maken die kan worden uitgevoerd na een schalingsbewerking, waarmee uw XaaS-onderdelen naar wens kunnen worden geschaald of bijgewerkt. U kunt schalen deactiveren door het aantal instanties te configureren dat is toegestaan bij elk machineonderdeel.</p>

Tabblad **Versie-informatie**

Hier configureert u versie-informatie-instellingen voor een vSphere-machineonderdeel.

Tabel 3-5. Tabblad **Versie-informatie**

Instelling	Beschrijving
Blueprinttype	<p>Voor administratieve doeleinden en licentiedoeleinden selecteert u of machines die vanaf deze blueprint zijn ingericht, worden geclassificeerd als Desktop of als Server.</p>
Actie	<p>Welke opties u in het vervolgkeuzemenu voor acties ziet, is afhankelijk van het door u geselecteerde machinetype. De volgende acties zijn beschikbaar:</p> <ul style="list-style-type: none"> ■ Maken <p>Maak de specificatie voor het machineonderdeel zonder gebruik te maken van een kloonoptie.</p> ■ Klonen <p>Maak kopieën van een virtual machine vanaf een sjabloon en een aanpassingsobject.</p> ■ Gekoppelde kloon <p>Een ruimtebesparende kopie inrichten van een virtual machine, een gekoppelde kloon genoemd. Gekoppelde klonen zijn gebaseerd op een momentopname van een VM en maken gebruik van een keten van deltaschijven om de verschillen met de oorspronkelijke machine vast te leggen.</p> <p>Voordat u VM's van de gekoppelde kloon inricht, schakelt u VM-momentopname uit.</p> ■ NetApp FlexClone <p>Als uw reserveringen NetApp FlexClone-opslag gebruiken, kunt u ruimtebesparende kopieën van machines klonen.</p>

Tabel 3-5. Tabblad **Versie-informatie** (vervolg)

Instelling	Beschrijving
Inrichtingswerkstroom	<p data-bbox="810 279 1310 365">Welke opties u in het vervolgkeuzemenu voor inrichtingswerkstroom ziet, is afhankelijk van het machinetype en de actie die u selecteert.</p> <ul style="list-style-type: none"> <li data-bbox="810 380 1043 407">■ BasicVmWorkflow <p data-bbox="847 426 1390 453">Richt een machine zonder gastbesturingssysteem in.</p> <li data-bbox="810 468 1171 495">■ ExternalProvisioningWorkflow <p data-bbox="847 514 1378 600">Maak een machine door te starten vanaf een virtual machine-instantie of een op de cloud gebaseerde installatiekopie.</p> <li data-bbox="810 615 1059 642">■ ImportOvfWorkflow <p data-bbox="847 661 1406 873">Hiermee kunt u een vSphere virtual machine implementeren via een OVF-sjabloon, net als u met een CloneWorkflow een vSphere virtual machine implementeert via een sjabloon voor virtual machines. U kunt het importproces richten op een vSphere-onderdeel van een machineblueprint of op een Image-onderdeelprofiel van een blueprint met parameters.</p> <li data-bbox="810 888 1107 915">■ LinuxKickstartWorkflow <p data-bbox="847 934 1390 1083">Richt een machine in door op te starten vanuit een ISO-image en vervolgens een Kickstart- of autoYaSt-configuratiebestand en een distributie-image voor Linux te gebruiken om het besturingssysteem op de machine te installeren.</p> <li data-bbox="810 1098 1211 1125">■ VirtualSccmProvisioningWorkflow <p data-bbox="847 1144 1406 1293">Richt een machine in en geef vervolgens de besturing over aan een SCCM-takenreeks voor het opstarten op basis van een ISO-image, implementeer een Windows-besturingssysteem en installeer de vRealize Automation-gastagent.</p> <li data-bbox="810 1308 1067 1335">■ WIMImageWorkflow <p data-bbox="847 1354 1406 1503">Richt een machine in door op te starten in een WinPE-omgeving en een besturingssysteem te installeren met behulp van een WIM-image (Windows Imaging File Format) van een bestaande Windows-referentiemachine.</p> <p data-bbox="810 1522 1414 1734">Voor blueprints met een WIM-inrichtingswerkstroom moet de opgegeven opslagwaarde rekening houden met de grootte van elke schijf die op de machine wordt gebruikt. Gebruik de totale waarde van alle schijven als minimumopslagwaarde voor het machineonderdeel. Zorg er tevens voor dat elke schijf groot genoeg is om het besturingssysteem te kunnen huisvesten.</p>

Tabel 3-5. Tabblad **Versie-informatie** (vervolg)

Instelling	Beschrijving
Klonen van	<p>Selecteer een machinesjabloon om te klonen. U kunt de lijst met beschikbare sjablonen verfijnen met behulp van de optie Filters in het vervolgkeuzemenu van elke kolom. Voor gekoppelde klonen worden alleen machines weergegeven die over beschikbare momentopnamen beschikken waaruit u kunt klonen, en die u als tenantbeheerder of bedrijfsgroepbeheerder kunt beheren.</p> <p>U kunt alleen klonen op basis van sjablonen die aanwezig zijn op de machines die u als bedrijfsgroepbeheerder of tenantbeheerder in beheer heeft.</p>
Klonen van momentopname	<p>Selecteer voor de gekoppelde kloon een bestaande momentopname die u wilt gebruiken voor een kloonbewerking op basis van de geselecteerde machinesjabloon. Machines worden alleen in de lijst weergegeven als ze al over een momentopname beschikken en als u de machine beheert als tenantbeheerder of bedrijfsgroepbeheerder.</p> <p>Als u Huidige momentopname gebruiken selecteert, wordt de kloon gedefinieerd met dezelfde eigenschappen als de recentste status van de virtual machine. Als u in plaats daarvan een kloon wilt maken die verwant is aan een werkelijke momentopname, klikt u op de optie in het vervolgkeuzemenu en selecteert u de specifieke momentopname in de lijst.</p> <p>Opmerking Het gebruik van de term momentopname kan tot verwarring leiden. Als u een bestaande momentopname selecteert, maakt u met de optie een nieuwe schijf met de momentopname als bovenliggend element. Bij de optie Huidige momentopname gebruiken kan geen basisschijf als bovenliggend element worden gebruikt en wordt stilzwijgend een volledige kloonactie uitgevoerd. U kunt dit omzeilen door de momentopnamen op de basisschijf te maken of een vRealize Orchestrator-werkstroom te gebruiken waarmee u een momentopname maakt die u gebruikt om een directe kloon te maken.</p> <p>Deze optie is alleen beschikbaar voor de actie Gekoppelde kloon.</p>
Specificatie aanpassing	<p>Geef een beschikbare aanpassingsspecificatie op. Een aanpassingsspecificatie is alleen vereist wanneer u kloont met statische IP-adressen.</p> <p>Zonder aanpassingsspecificatie kunt u geen aanpassingen van Windows-machines uitvoeren. Voor Linux-kloonmachines kunt u een aanpassingsspecificatie, een extern script of beide gebruiken om aanpassingen uit te voeren.</p>

Tabblad **Machinebronnen**

Hier geeft u CPU-, geheugen- en opslaginstellingen voor een vSphere-machineonderdeel op.

Tabel 3-6. Tabblad **Machinebronnen**

Instelling	Beschrijving
CPU's: Minimum en Maximum	Geef aan hoeveel CPU's er minimaal en maximaal kunnen worden gebruikt door ingerichte machines.
Geheugen (MB): Minimum en Maximum	Voer de minimale en maximale hoeveelheid geheugen in die kan worden gebruikt door ingerichte machines.
Opslag (GB): Minimum en Maximum	Voer een minimale en maximale hoeveelheid opslagruimte in die kan worden gebruikt door ingerichte machines. Voor blueprints met een WIM-inrichtingswerkstroom moet de opgegeven opslagwaarde rekening houden met de grootte van elke schijf die op de machine wordt gebruikt. Gebruik de totale waarde van alle schijven als minimumopslagwaarde voor het machineonderdeel. Zorg er tevens voor dat elke schijf groot genoeg is om het besturingssysteem te kunnen huisvesten.

Tabblad **Opslag**

U kunt de opslagruimte beheren door instellingen voor opslagvolumes, inclusief opslagreserveringsbeleidsregels, toe te wijzen aan het machineonderdeel.

Tabel 3-7. Instellingen tabblad **Opslag**

Instelling	Beschrijving
Id	Voer een id of naam voor het opslagvolume in.
Capaciteit (GB)	Voer de opslagcapaciteit voor het opslagvolume in.
Stationsletter/koppelingspad	Geef een stationsletter of koppelingspad voor het opslagvolume op. Deze optie wordt gebruikt tijdens de inrichting in combinatie met een gastagent. Ze kan niet worden gewijzigd na de inrichting van de machine. Als u geen gastagent gebruikt, wordt deze optie genegeerd.
Label	Geef een label voor de stationsletter en het koppelingspad van het opslagvolume op. Deze optie wordt gebruikt tijdens de inrichting in combinatie met een gastagent. Ze kan niet worden gewijzigd na de inrichting van de machine. Als u geen gastagent gebruikt, wordt deze optie genegeerd.
Opslagreserveringsbeleid	Geef op welk bestaand opslagreserveringsbeleid u wilt gebruiken voor dit opslagvolume. Alleen het opslagreserveringsbeleid dat van toepassing is op de huidige tenant, is beschikbaar.
Aangepaste eigenschappen	Geef op welke aangepaste eigenschappen u wilt gebruiken voor dit opslagvolume.

Tabel 3-7. Instellingen tabblad **Opslag** (vervolg)

Instelling	Beschrijving
Maximumaantal volumes	Geef op hoeveel opslagvolumes er maximaal mogen worden gebruikt bij de inrichting vanaf het machineonderdeel. Voer 0 in als u wilt voorkomen dat andere gebruikers opslagvolumes kunnen toevoegen. De standaardwaarde is 60.
Gebruikers toestaan opslagreserveringsbeleid te zien en te wijzigen	Schakel het selectievakje in om gebruikers in staat te stellen een toegewezen reserveringsbeleid te verwijderen of een ander reserveringsbeleid op te geven bij de inrichting.

Tabblad **Netwerk**

U kunt netwerkinstellingen voor een vSphere-machineonderdeel configureren op basis van de instellingen van NSX-netwerken en -load balancers die buiten vRealize Automation zijn geconfigureerd. U kunt instellingen gebruiken van een of meer onderdelen voor bestaande en op aanvraag geleverde NSX-netwerkonderdelen in het ontwerpcanvas.

Zie [Instellingen van netwerk- en beveiligingsonderdelen configureren in vRealize Automation](#) en [Instellingen op de pagina's Nieuwe blueprint en Blueprinteigenschappen voor NSX in vRealize Automation](#) voor gerelateerde informatie.

Tabel 3-8. Instellingen tabblad **Netwerk**

Instelling	Beschrijving
Netwerk	Selecteer een netwerkonderdeel in het vervolgkeuzemenu. De lijst bevat uitsluitend bestaande netwerkonderdelen in het ontwerpcanvas. Alleen de netwerkprofielen die van toepassing zijn op de huidige tenant, zijn beschikbaar. Het netwerk dat u selecteert, bepaalt het netwerktype en ook of het cluster dat wordt geïmplementeerd op het netwerk, wordt beheerd door NSX for vSphere of NSX-T.
Toewijzingstype	Accepteer de standaardtoewijzing die is overgenomen van het netwerkonderdeel of selecteer een toewijzingstype uit het vervolgkeuzemenu. De waarden voor de opties DHCP en Statisch worden overgenomen van de instellingen voor het netwerkonderdeel.
Adres	Geef het IP-adres van het netwerk op. De optie is alleen beschikbaar voor statische adressen.
Taakverdeling	Geef de service op die voor taakverdeling moet worden gebruikt.
Aangepaste eigenschappen	Toon de aangepaste eigenschappen die zijn ingesteld voor het geselecteerde netwerkonderdeel of netwerkprofiel.
Maximumaantal netwerkadapters	Geef op hoeveel netwerkadapters of NIC's er maximaal mogen worden gebruikt voor dit machineonderdeel. De standaardwaarde is onbeperkt. Stel deze optie in op 0 als u de mogelijkheid om NIC's aan de machineonderdelen toe te voegen, wilt deactiveren.

Tabblad **Beveiliging**

U kunt beveiligingsinstellingen voor een vSphere-machineonderdeel configureren op basis van NSX-instellingen die buiten vRealize Automation zijn geconfigureerd. U kunt desgewenst ook instellingen gebruiken van bestaande en op aanvraag geleverde NSX-beveiligingsonderdelen in het ontwerpcanvas.

De instellingen van de onderdelen voor bestaande en op aanvraag geleverde beveiligingsgroepen en beveiligingstags in het ontwerpcanvas zijn automatisch beschikbaar.

Voor informatie over het toevoegen en configureren van NSX-netwerkonderdelen en -beveiligingsonderdelen voordat u instellingen op het tabblad **Beveiliging** voor een vSphere-machineonderdeel gebruikt, raadpleegt u [Instellingen van netwerk- en beveiligingsonderdelen configureren in vRealize Automation](#).

Zie [Instellingen op de pagina's Nieuwe blueprint en Blueprinteigenschappen voor NSX in vRealize Automation](#) voor informatie over het opgeven van de NSX-informatie die van toepassing is op alle vSphere-machineonderdelen in de blueprint.

Tabel 3-9. Instellingen tabblad **Beveiliging**

Instelling	Beschrijving
Naam	Toon de naam van een NSX-beveiligingsgroep of -tag. Deze namen worden overgenomen van de beveiligingsonderdelen in het ontwerpcanvas. Schakel het selectievakje naast een weergegeven beveiligingsgroep of -tag in om aan te geven dat u die groep of tag wilt gebruiken voor de inrichting vanaf dit machineonderdeel.
Type	Geef aan of het beveiligingselement een beveiligingsgroep op aanvraag, een bestaande beveiligingsgroep of een beveiligingstag is.
Beschrijving	Toon de geregistreerde beschrijving van een beveiligingsgroep of -tag.
Endpoint	Toon het endpoint dat wordt gebruikt door de NSX-beveiligingsgroep of -tag.

Tabblad **Eigenschappen**

Geef aangepaste eigenschaps- en eigenschapsgroepsinformatie op voor het vSphere-machineonderdeel.

Via het tabblad **Eigenschappen** kunt u aangepaste eigenschappen afzonderlijk of groepsgewijs toevoegen aan het machineonderdeel. U kunt het tabblad **Eigenschappen** ook gebruiken om aangepaste eigenschappen en eigenschapsgroepen toe te voegen aan de algemene blueprint die u maakt of bewerkt met behulp van de pagina **Blueprinteigenschappen**.

Via het tabblad **Aangepaste eigenschappen** kunt u opties voor bestaande aangepaste eigenschappen toevoegen en instellen. Aangepaste eigenschappen worden bij vRealize Automation geleverd, maar u kunt ook nieuwe eigenschapsdefinities toevoegen.

Tabel 3-10. Instellingen tabblad **Eigenschappen** > **Aangepaste eigenschappen**

Instelling	Beschrijving
Naam	Voer de naam van de aangepaste eigenschap in of selecteer een beschikbare aangepaste eigenschap in het vervolgkeuzemenu. Eigenschappen worden alleen weergegeven in het vervolgkeuzemenu als uw tenantbeheerder of materiaalbeheerder eigenschapsdefinities heeft gemaakt.
Waarde	Typ of bewerk de waarde die u wilt koppelen aan de naam van de aangepaste eigenschap. Stel de waarde bijvoorbeeld in op <code>true</code> , zodat gebruikers aan wie rechten zijn verleend, via SSH verbinding kunnen maken met VM's.
Versleuteld	U kunt ervoor kiezen om de eigenschapswaarde te coderen, bijvoorbeeld als de waarde een wachtwoord is.
Overschrijfbaar	U kunt opgeven dat de eigenschapswaarde kan worden overschreven door de volgende persoon of hierop volgende persoon die de eigenschap gebruikt. Als u Weergeven in aanvraag selecteert, kunnen gebruikers eigenschapswaarden bewerken wanneer ze catalogusitems aanvragen.
Weergeven in aanvraag	U kunt de eigenschapsnaam en -waarde weergeven voor gebruikers wanneer deze de inrichting van een machine aanvragen. Selecteer de optie Overschrijfbaar als u wilt dat gebruikers een waarde opgeven.

Via het tabblad **Eigenschapsgroepen** kunt u instellingen voor bestaande aangepaste eigenschapsgroepen toevoegen en instellen. U kunt zelf eigenschapsgroepen maken of eigenschapsgroepen gebruiken die voor u zijn gemaakt.

Tabel 3-11. Instellingen tabblad **Eigenschappen** > **Eigenschapsgroepen**

Instelling	Beschrijving
Naam	Selecteer een beschikbare eigenschapsgroep in het vervolgkeuzemenu.
Naar boven en Naar beneden	Maak een hiërarchische sortering van de eigenschapsgroepen in aflopende volgorde. De eerste eigenschapsgroep in de lijst krijgt dan voorrang boven de tweede eigenschapsgroep in de lijst, enzovoort.
Eigenschappen weergeven	Geef de aangepaste eigenschappen in de geselecteerde eigenschapsgroep weer.
Samengevoegde eigenschappen weergeven	Geef de aangepaste eigenschappen weer in de volgorde waarin ze worden weergegeven in de lijst met eigenschapsgroepen. Als dezelfde eigenschap in meerdere groepen tegelijk voorkomt, wordt de eigenschap één keer in de lijst opgenomen, en wel op de positie waarin deze voor de eerste keer werd aangetroffen.

Tabblad Profielen

Onderdeelprofielen zijn een manier om parameters in te stellen voor blueprints. In plaats van afzonderlijke blueprints te maken, kunt u bijvoorbeeld een kleine, middelgrote en grote mogelijkheid maken in één blueprint. U kunt een grootte voor de blueprint selecteren tijdens de implementatie. Onderdeelprofielen zijn ontworpen om uw catalogus te vereenvoudigen.

Als u waardesets hebt gemaakt voor de geleverde vRealize Automation-onderdeelprofielen **Size** en **Image**, kunt u die instellingen voor het machineonderdeel configureren in de blueprint. U kunt ook een andere waardeset selecteren wanneer u het catalogusitem implementeert.

Onderdeelprofielen zijn alleen beschikbaar voor vSphere-machineonderdelen.

Een onderdeelprofiel overschrijft de instellingen voor het machineonderdeel, zoals het aantal CPU's en de opslag.

De waardeset van het onderdeelprofiel wordt toegepast op alle vSphere-machines in een cluster.

U kunt machines niet opnieuw configureren met behulp van onderdeelprofielen van **Size** of **Image**. Het bereik van de CPU, het geheugen en de opslag wordt berekend op basis van het profiel en blijft beschikbaar voor het opnieuw configureren van acties. Gebruik bijvoorbeeld een kleine waardeset (1 CPU, 1024 MB geheugen en 10 GB opslag), een middelgrote waardeset (3 CPU's, 2048 MB geheugen, 12 GB opslag) en een grote waardeset (5 CPU's, 3072 MB geheugen, 15 GB opslag) voor **Size**. De beschikbare bereiken tijdens de herconfiguratie van de machine zijn 1-5 CPU's, 1024-3072 MB geheugen en 1-15 GB opslag.

Zie *Naslaggids voor aangepaste eigenschappen* voor meer informatie.

Tabel 3-12. Instellingen tabblad Profielen

Instelling	Beschrijving
Toevoegen	Voeg hiermee het onderdeelprofiel Size of Image toe.
Waardesets bewerken	Wijs hiermee een of meer waardesets voor het geselecteerde onderdeelprofiel toe door een selectie te maken uit een lijst met gedefinieerde waardesets. U kunt een van de waardesets als standaardset selecteren.
Verwijderen	Verwijder hiermee het onderdeelprofiel Size of Image .

Instellingen voor vCloud Air-machineonderdelen

Krijg inzicht in de instellingen en opties die u voor een vCloud Air-machineonderdeel in het ontwerpcanvas van de vRealize Automation-blueprint kunt configureren.

Tabblad Algemeen

Hier configureert u algemene instellingen voor een vCloud Air-machineonderdeel.

Tabel 3-13. Instellingen tabblad **Algemeen**

Instelling	Beschrijving
Id	Voer een naam in voor uw machineonderdeel of accepteer de standaardwaarde.
Beschrijving	Vat uw machineonderdeel samen ten behoeve van andere architecten.
Locatie op verzoek weergeven	<p>In een cloudomgeving, zoals vCloud Air, kunnen gebruikers een regio selecteren voor hun ingerichte machines.</p> <p>Voor een virtuele omgeving kunt u gebruikers een datacentrumlocatie laten selecteren voor het inrichten van een aangevraagde machine. Een systeembeheerder moet informatie over het datacentrum toevoegen aan een locatiebestand. Een materiaalbeheerder moet een computerbron bewerken om deze aan een locatie te koppelen.</p>
Reserveringsbeleid	Pas een reserveringsbeleid toe op een blueprint om het aantal machines dat op basis van die blueprint wordt ingericht, te beperken tot een subset met beschikbare reserveringen. Alleen het reserveringsbeleid dat van toepassing is op de huidige tenant, is beschikbaar.
Machinevoorvoegsel	<p>Machinevoorvoegsels worden gebruikt om ingerichte machines een naam te geven. Als u Standaardinstelling van groep gebruiken selecteert, krijgen machines een naam die is gebaseerd op het standaardvoorvoegsel van de machine voor uw bedrijfsgroep. Als u geen voorvoegsel opgeeft, wordt er een gegenereerd op basis van de naam van uw bedrijfsgroep. Alleen de machinevoorvoegsels die van toepassing zijn op de huidige tenant, zijn beschikbaar.</p> <p>Als uw materiaalbeheerder andere machinevoorvoegsels configureert die u kunt selecteren, dan kunt u één voorvoegsel toepassen op alle machines die vanaf uw blueprint zijn ingericht, ongeacht wie de aanvrager is.</p>
Instanties: Minimum en Maximum	<p>Configureer het maximale en het minimale aantal instanties dat gebruikers kunnen aanvragen voor een implementatie of een op- of neerschaalbewerking. Door dezelfde waarde in te voeren in de velden Minimum en Maximum, configureert u het exacte aantal instanties geconfigureerd dat moet worden ingericht.</p> <p>XaaS-onderdelen zijn niet schaalbaar en kunnen niet worden bijgewerkt tijdens een schalingsbewerking. Als u XaaS-onderdelen in uw blueprint gebruikt, kunt u een bronactie voor gebruikers maken die kan worden uitgevoerd na een schalingsbewerking, waarmee uw XaaS-onderdelen naar wens kunnen worden geschaald of bijgewerkt. U kunt schalen deactiveren door het aantal instanties te configureren dat is toegestaan bij elk machineonderdeel.</p>

Tabblad **Versie-informatie**

Hier configureert u versie-informatie-instellingen voor een vCloud Air-machineonderdeel.

Tabel 3-14. Tabblad **Versie-informatie**

Instelling	Beschrijving
Blueprinttype	Voor administratieve doeleinden en licentiedoeleinden selecteert u of machines die vanaf deze blueprint zijn ingericht, worden geclassificeerd als Desktop of als Server.
Actie	<p>Welke opties u in het vervolgkeuzemenu voor acties ziet, is afhankelijk van het door u geselecteerde machinetype. De enige inrichtingsactie die beschikbaar is voor een vCloud Air-machineonderdeel is Clone.</p> <p>■ Klonen</p> <p>Maak kopieën van een virtual machine vanaf een sjabloon en een aanpassingsobject.</p>
Inrichtingswerkstroom	<p>Welke opties u in het vervolgkeuzemenu voor inrichtingswerkstroom ziet, is afhankelijk van het machinetype en de actie die u selecteert. De enige inrichtingsactie die beschikbaar is voor een vCloud Air-machineonderdeel is CloneWorkflow.</p> <p>■ CloneWorkflow</p> <p>Maak kopieën van een virtual machine via een kloon, een gekoppelde kloon of een NetApp FlexClone.</p>
Klonen van	<p>Selecteer een machinesjabloon om te klonen. U kunt de lijst met beschikbare sjablonen verfijnen met behulp van de optie Filters in het vervolgkeuzemenu van elke kolom. Voor gekoppelde klonen worden alleen machines weergegeven die over beschikbare momentopnamen beschikken waaruit u kunt klonen, en die u als tenantbeheerder of bedrijfsgroepbeheerder kunt beheren.</p> <p>U kunt alleen klonen op basis van sjablonen die aanwezig zijn op de machines die u als bedrijfsgroepbeheerder of tenantbeheerder in beheer heeft.</p>

Tabblad **Machinebronnen**

Hier geeft u CPU-, geheugen- en opslaginstellingen voor het vCloud Air-machineonderdeel op.

Tabel 3-15. Tabblad **Machinebronnen**

Instelling	Beschrijving
CPU's: Minimum en Maximum	Geef aan hoeveel CPU's er minimaal en maximaal kunnen worden gebruikt door ingerichte machines.
Geheugen (MB): Minimum en Maximum	Voer de minimale en maximale hoeveelheid geheugen in die kan worden gebruikt door ingerichte machines.
Opslag (GB): Minimum en Maximum	Voer een minimale en maximale hoeveelheid opslagruimte in die kan worden gebruikt door ingerichte machines.

Tabblad Opslag

U kunt de opslagruimte beheren door instellingen voor opslagvolumes, inclusief opslagreserveringsbeleidsregels, toe te wijzen aan het machineonderdeel.

Tabel 3-16. Instellingen tabblad **Opslag**

Instelling	Beschrijving
Id	Voer een id of naam voor het opslagvolume in.
Capaciteit (GB)	Voer de opslagcapaciteit voor het opslagvolume in.
Stationsletter/koppelingspad	Geef een stationsletter of koppelingspad voor het opslagvolume op. Deze optie wordt gebruikt tijdens de inrichting in combinatie met een gastagent. Ze kan niet worden gewijzigd na de inrichting van de machine. Als u geen gastagent gebruikt, wordt deze optie genegeerd.
Label	Geef een label voor de stationsletter en het koppelingspad van het opslagvolume op. Deze optie wordt gebruikt tijdens de inrichting in combinatie met een gastagent. Ze kan niet worden gewijzigd na de inrichting van de machine. Als u geen gastagent gebruikt, wordt deze optie genegeerd.
Opslagreserveringsbeleid	Geef op welk bestaand opslagreserveringsbeleid u wilt gebruiken voor dit opslagvolume. Alleen het opslagreserveringsbeleid dat van toepassing is op de huidige tenant, is beschikbaar.
Aangepaste eigenschappen	Geef op welke aangepaste eigenschappen u wilt gebruiken voor dit opslagvolume.
Maximumaantal volumes	Geef op hoeveel opslagvolumes er maximaal mogen worden gebruikt bij de inrichting vanaf het machineonderdeel. Voer 0 in als u wilt voorkomen dat andere gebruikers opslagvolumes kunnen toevoegen. De standaardwaarde is 60.
Gebruikers toestaan opslagreserveringsbeleid te zien en te wijzigen	Schakel het selectievakje in om gebruikers in staat te stellen een toegewezen reserveringsbeleid te verwijderen of een ander reserveringsbeleid op te geven bij de inrichting.

Tabblad Eigenschappen

U kunt ook aangepaste eigenschaps- en eigenschapsgroepsinformatie voor het vCloud Air-machineonderdeel opgeven.

Via het tabblad **Eigenschappen** kunt u aangepaste eigenschappen afzonderlijk of groepsgewijs toevoegen aan het machineonderdeel. U kunt het tabblad **Eigenschappen** ook gebruiken om aangepaste eigenschappen en eigenschapsgroepen toe te voegen aan de algemene blueprint die u maakt of bewerkt met behulp van de pagina **Blueprinteigenschappen**.

Via het tabblad **Aangepaste eigenschappen** kunt u opties voor bestaande aangepaste eigenschappen toevoegen en instellen. Aangepaste eigenschappen worden bij vRealize Automation geleverd, maar u kunt ook nieuwe eigenschapsdefinities toevoegen.

Tabel 3-17. Instellingen tabblad **Eigenschappen > Aangepaste eigenschappen**

Instelling	Beschrijving
Naam	Voer de naam van de aangepaste eigenschap in of selecteer een beschikbare aangepaste eigenschap in het vervolgkeuzemenu. Eigenschappen worden alleen weergegeven in het vervolgkeuzemenu als uw tenantbeheerder of materiaalbeheerder eigenschapsdefinities heeft gemaakt.
Waarde	Typ of bewerk de waarde die u wilt koppelen aan de naam van de aangepaste eigenschap. Stel de waarde bijvoorbeeld in op <code>true</code> , zodat gebruikers aan wie rechten zijn verleend, via SSH verbinding kunnen maken met VM's.
Versleuteld	U kunt ervoor kiezen om de eigenschapswaarde te coderen, bijvoorbeeld als de waarde een wachtwoord is.
Overschrijfbaar	U kunt opgeven dat de eigenschapswaarde kan worden overschreven door de volgende persoon of hierop volgende persoon die de eigenschap gebruikt. Als u Weergeven in aanvraag selecteert, kunnen gebruikers eigenschapswaarden bewerken wanneer ze catalogusitems aanvragen.
Weergeven in aanvraag	U kunt de eigenschapsnaam en -waarde weergeven voor gebruikers wanneer deze de inrichting van een machine aanvragen. Selecteer de optie Overschrijfbaar als u wilt dat gebruikers een waarde opgeven.

Via het tabblad **Eigenschapsgroepen** kunt u instellingen voor bestaande aangepaste eigenschapsgroepen toevoegen en instellen. U kunt zelf eigenschapsgroepen maken of eigenschapsgroepen gebruiken die voor u zijn gemaakt.

Tabel 3-18. Instellingen tabblad **Eigenschappen > Eigenschapsgroepen**

Instelling	Beschrijving
Naam	Selecteer een beschikbare eigenschapsgroep in het vervolgkeuzemenu.
Naar boven en Naar beneden	Maak een hiërarchische sortering van de eigenschapsgroepen in aflopende volgorde. De eerste eigenschapsgroep in de lijst krijgt dan voorrang boven de tweede eigenschapsgroep in de lijst, enzovoort.
Eigenschappen weergeven	Geef de aangepaste eigenschappen in de geselecteerde eigenschapsgroep weer.
Samengevoegde eigenschappen weergeven	Geef de aangepaste eigenschappen weer in de volgorde waarin ze worden weergegeven in de lijst met eigenschapsgroepen. Als dezelfde eigenschap in meerdere groepen tegelijk voorkomt, wordt de eigenschap één keer in de lijst opgenomen, en wel op de positie waarin deze voor de eerste keer werd aangetroffen.

Instellingen voor Amazon-machineonderdelen

Hier volgt een overzicht van de instellingen en opties die u kunt configureren voor Amazon-machineonderdelen in het ontwerpcanvas van vRealize Automation-blueprints.

Tabblad **Algemeen**

Hier configureert u algemene instellingen voor het Amazon-machineonderdeel.

Tabel 3-19. Instellingen tabblad **Algemeen**

Instelling	Beschrijving
Id	Voer een naam in voor uw machineonderdeel of accepteer de standaardwaarde.
Beschrijving	Vat uw machineonderdeel samen ten behoeve van andere architecten.
Locatie op verzoek weergeven	<p>In een cloudomgeving, zoals vCloud Air, kunnen gebruikers een regio selecteren voor hun ingerichte machines.</p> <p>Voor een virtuele omgeving kunt u gebruikers een datacentrumlocatie laten selecteren voor het inrichten van een aangevraagde machine. Een systeembeheerder moet informatie over het datacentrum toevoegen aan een locatiebestand. Een materiaalbeheerder moet een computerbron bewerken om deze aan een locatie te koppelen.</p>
Reserveringsbeleid	Pas een reserveringsbeleid toe op een blueprint om het aantal machines dat op basis van die blueprint wordt ingericht, te beperken tot een subset met beschikbare reserveringen. Alleen het reserveringsbeleid dat van toepassing is op de huidige tenant, is beschikbaar.
Machinevoorvoegsel	<p>Machinevoorvoegsels worden gebruikt om ingerichte machines een naam te geven. Als u Standaardinstelling van groep gebruiken selecteert, krijgen machines een naam die is gebaseerd op het standaardvoorvoegsel van de machine voor uw bedrijfsgroep. Als u geen voorvoegsel opgeeft, wordt er een gegenereerd op basis van de naam van uw bedrijfsgroep. Alleen de machinevoorvoegsels die van toepassing zijn op de huidige tenant, zijn beschikbaar.</p> <p>Als uw materiaalbeheerder andere machinevoorvoegsels configureert die u kunt selecteren, dan kunt u één voorvoegsel toepassen op alle machines die vanaf uw blueprint zijn ingericht, ongeacht wie de aanvrager is.</p>
Instanties: Minimum en Maximum	<p>Configureer het maximale en het minimale aantal instanties dat gebruikers kunnen aanvragen voor een implementatie of een op- of neerschaalbewerking. Door dezelfde waarde in te voeren in de velden Minimum en Maximum, configureert u het exacte aantal instanties geconfigureerd dat moet worden ingericht.</p> <p>XaaS-onderdelen zijn niet schaalbaar en kunnen niet worden bijgewerkt tijdens een schalingsbewerking. Als u XaaS-onderdelen in uw blueprint gebruikt, kunt u een bronactie voor gebruikers maken die kan worden uitgevoerd na een schalingsbewerking, waarmee uw XaaS-onderdelen naar wens kunnen worden geschaald of bijgewerkt. U kunt schalen deactiveren door het aantal instanties te configureren dat is toegestaan bij elk machineonderdeel.</p>

Tabblad **Versie-informatie**

Hier configureert u instellingen voor de versie-informatie van het Amazon-machineonderdeel.

Tabel 3-20. Tabblad Versie-informatie

Instelling	Beschrijving
Blueprinttype	Voor administratieve doeleinden en licentiedoeleinden selecteert u of machines die vanaf deze blueprint zijn ingericht, worden geclassificeerd als Desktop of als Server.
Inrichtingswerkstroom	<p>Voor een Amazon-machineonderdeel hebt u alleen de beschikking over de inrichtingswerkstroom CloudProvisioningWorkflow.</p> <p>■ CloudProvisioningWorkflow</p> <p>Maak een machine door te starten vanaf een virtual machine-instantie of een op de cloud gebaseerde installatiekopie.</p>
Image van een Amazon-machine-image	Selecteer een beschikbare image van een Amazon-machine-image. Een image van een Amazon-machine is een sjabloon die de softwareconfiguratie bevat, inclusief een besturingssysteem. Machine-images worden beheerd door Amazon Web Services-accounts. U kunt de lijst met weergegeven namen van Amazon-machine-images specifieker maken door de optie Filters in het vervolgkeuzemenu van de kolom AMI-ID te gebruiken.

Tabel 3-20. Tabblad Versie-informatie (vervolg)

Instelling	Beschrijving
Sleutelpaar	<p>Sleutelparen zijn vereist voor inrichting met Amazon Web Services.</p> <p>Sleutelparen worden gebruikt om een cloudinstantie in te richten en ermee verbinding te maken. Daarnaast worden ze gebruikt voor de ontsleuteling van Windows-wachtwoorden en de aanmelding bij Linux-machines.</p> <p>Voor sleutelparen zijn de volgende opties beschikbaar:</p> <ul style="list-style-type: none"> ■ Niet opgegeven <p>Hiermee wordt het gedrag bepaald van het sleutelpaar op het niveau van de blueprint in plaats van het niveau van de reservering.</p> ■ Automatisch gegenereerd per bedrijfsgroep <p>Hiermee bepaalt u dat elke machine die in dezelfde bedrijfsgroep wordt ingericht, hetzelfde sleutelpaar heeft, inclusief machines die in andere reserveringen worden ingericht wanneer de machines dezelfde computingbron en bedrijfsgroep hebben. Omdat de sleutelparen zijn gekoppeld aan een bedrijfsgroep, worden de sleutelparen verwijderd, wanneer de bedrijfsgroep wordt verwijderd.</p> ■ Automatisch gegenereerd per machine <p>Hiermee bepaalt u dat elke machine een uniek sleutelpaar heeft. De optie voor automatisch genereren per machine is de veiligste methode omdat er geen sleutelparen worden gedeeld tussen machines onderling.</p>
Amazon-netwerkopties op machine inschakelen	<p>Hier kunt u gebruikers die een aanvraag indienen, laten kiezen of ze een machine willen inrichten in een Virtual Private Cloud (VPC) of op een niet-VPC-locatie.</p>
Instantietypen	<p>Selecteer één of meer Amazon-instantietypen. Een Amazon-instantie is een virtuele server waarop toepassingen kunnen worden uitgevoerd in Amazon Web Services. Instanties worden gemaakt aan de hand van een image van een Amazon-machine en door de juiste instantietypes te kiezen. vRealize Automation beheert de instantietypen van installatiekopieën van machines die beschikbaar zijn voor inrichting.</p> <p>Zie Informatie over Amazon-instantietypes en Een Amazon-instantietype toevoegen voor meer informatie over het gebruik van Amazon-instantietypen in vRealize Automation.</p>

Tabblad Machinebronnen

Hier geeft u instellingen op voor de gebruikte CPU's, geheugenbronnen, opslagbronnen en EBS-volumes van het Amazon-machineonderdeel.

U kunt ook alle Amazon-machineopslagvolumes in de implementatie met uitzondering van het rootvolume opnieuw configureren.

Tabel 3-21. Tabblad **Machinebronnen**

Instelling	Beschrijving
CPU's: Minimum en Maximum	Geef aan hoeveel CPU's er minimaal en maximaal kunnen worden gebruikt door ingerichte machines.
Geheugen (MB): Minimum en Maximum	Voer de minimale en maximale hoeveelheid geheugen in die kan worden gebruikt door ingerichte machines.
Opslag (GB): Minimum en Maximum	Voer een minimale en maximale hoeveelheid opslagruimte in die kan worden gebruikt door ingerichte machines.
EBS-opslag (GB): Minimum en Maximum	<p>Voer een minimale en maximale hoeveelheid Amazon Elastic Block Store (EBS)-opslagvolume in die kan worden gebruikt door ingerichte machines.</p> <p>Wanneer u een implementatie vernietigt die een Amazon-machineonderdeel bevat, worden alle EBS-volumes die tijdens de levenscyclus aan de machine werden toegevoegd niet vernietigd maar verwijderd. vRealize Automation biedt geen optie voor het vernietigen van de EBS-volumes.</p>
Volumes verwijderen	<p>Geeft aan of u EC2-volumes individueel of bulkgewijs kunt verwijderen bij het vernietigen van Amazon-implementaties.</p> <p>Zowel Ja als Nee maken een bulkvernietigingsactie van alle volumes in de implementatie mogelijk. De standaardwaarde is null of leeg.</p> <ul style="list-style-type: none"> ■ Ja - de Amazon-implementatie vernietigen en volumes verwijderen. ■ Nee - de Amazon-implementatie te vernietigen en volumes behouden. ■ null of leeg - vereist dat de gebruiker de waarde Ja of Nee opgeeft bij het vernietigen van Amazon-implementaties.

Tabblad **Eigenschappen**

Hier kunt u optioneel gegevens opgeven voor de aangepaste eigenschappen en eigenschapsgroepen van het Amazon-machineonderdeel.

Via het tabblad **Eigenschappen** kunt u aangepaste eigenschappen afzonderlijk of groepsgewijs toevoegen aan het machineonderdeel. U kunt het tabblad **Eigenschappen** ook gebruiken om aangepaste eigenschappen en eigenschapsgroepen toe te voegen aan de algemene blueprint die u maakt of bewerkt met behulp van de pagina **Blueprinteigenschappen**.

Via het tabblad **Aangepaste eigenschappen** kunt u opties voor bestaande aangepaste eigenschappen toevoegen en instellen. Aangepaste eigenschappen worden bij vRealize Automation geleverd, maar u kunt ook nieuwe eigenschapsdefinities toevoegen.

Tabel 3-22. Instellingen tabblad **Eigenschappen > Aangepaste eigenschappen**

Instelling	Beschrijving
Naam	Voer de naam van de aangepaste eigenschap in of selecteer een beschikbare aangepaste eigenschap in het vervolgkeuzemenu. Eigenschappen worden alleen weergegeven in het vervolgkeuzemenu als uw tenantbeheerder of materiaalbeheerder eigenschapsdefinities heeft gemaakt.
Waarde	Typ of bewerk de waarde die u wilt koppelen aan de naam van de aangepaste eigenschap. Stel de waarde bijvoorbeeld in op <code>true</code> , zodat gebruikers aan wie rechten zijn verleend, via SSH verbinding kunnen maken met VM's.
Versleuteld	U kunt ervoor kiezen om de eigenschapswaarde te coderen, bijvoorbeeld als de waarde een wachtwoord is.
Overschrijfbaar	U kunt opgeven dat de eigenschapswaarde kan worden overschreven door de volgende persoon of hierop volgende persoon die de eigenschap gebruikt. Als u Weergeven in aanvraag selecteert, kunnen gebruikers eigenschapswaarden bewerken wanneer ze catalogusitems aanvragen.
Weergeven in aanvraag	U kunt de eigenschapsnaam en -waarde weergeven voor gebruikers wanneer deze de inrichting van een machine aanvragen. Selecteer de optie Overschrijfbaar als u wilt dat gebruikers een waarde opgeven.

Via het tabblad **Eigenschapsgroepen** kunt u instellingen voor bestaande aangepaste eigenschapsgroepen toevoegen en instellen. U kunt zelf eigenschapsgroepen maken of eigenschapsgroepen gebruiken die voor u zijn gemaakt.

Tabel 3-23. Instellingen tabblad **Eigenschappen > Eigenschapsgroepen**

Instelling	Beschrijving
Naam	Selecteer een beschikbare eigenschapsgroep in het vervolgkeuzemenu.
Naar boven en Naar beneden	Maak een hiërarchische sortering van de eigenschapsgroepen in aflopende volgorde. De eerste eigenschapsgroep in de lijst krijgt dan voorrang boven de tweede eigenschapsgroep in de lijst, enzovoort.
Eigenschappen weergeven	Geef de aangepaste eigenschappen in de geselecteerde eigenschapsgroep weer.
Samengevoegde eigenschappen weergeven	Geef de aangepaste eigenschappen weer in de volgorde waarin ze worden weergegeven in de lijst met eigenschapsgroepen. Als dezelfde eigenschap in meerdere groepen tegelijk voorkomt, wordt de eigenschap één keer in de lijst opgenomen, en wel op de positie waarin deze voor de eerste keer werd aangetroffen.

Instellingen voor OpenStack-machineonderdelen

Hier volgt een overzicht van de instellingen en opties die u kunt configureren voor OpenStack-machineonderdelen in het ontwerpcanvas van vRealize Automation-blueprints.

Tabblad **Algemeen**

Hier configureert u algemene instellingen voor een OpenStack-machineonderdeel.

Tabel 3-24. Instellingen tabblad **Algemeen**

Instelling	Beschrijving
Id	Voer een naam in voor uw machineonderdeel of accepteer de standaardwaarde.
Beschrijving	Vat uw machineonderdeel samen ten behoeve van andere architecten.
Locatie op verzoek weergeven	<p>In een cloudomgeving, zoals vCloud Air, kunnen gebruikers een regio selecteren voor hun ingerichte machines.</p> <p>Voor een virtuele omgeving kunt u gebruikers een datacentrumlocatie laten selecteren voor het inrichten van een aangevraagde machine. Een systeembeheerder moet informatie over het datacentrum toevoegen aan een locatiebestand. Een materiaalbeheerder moet een computerbron bewerken om deze aan een locatie te koppelen.</p>
Reserveringsbeleid	Pas een reserveringsbeleid toe op een blueprint om het aantal machines dat op basis van die blueprint wordt ingericht, te beperken tot een subset met beschikbare reserveringen. Alleen het reserveringsbeleid dat van toepassing is op de huidige tenant, is beschikbaar.
Machinevoorvoegsel	<p>Machinevoorvoegsels worden gebruikt om ingerichte machines een naam te geven. Als u Standaardinstelling van groep gebruiken selecteert, krijgen machines een naam die is gebaseerd op het standaardvoorvoegsel van de machine voor uw bedrijfsgroep. Als u geen voorvoegsel opgeeft, wordt er een gegenereerd op basis van de naam van uw bedrijfsgroep. Alleen de machinevoorvoegsels die van toepassing zijn op de huidige tenant, zijn beschikbaar.</p> <p>Als uw materiaalbeheerder andere machinevoorvoegsels configureert die u kunt selecteren, dan kunt u één voorvoegsel toepassen op alle machines die vanaf uw blueprint zijn ingericht, ongeacht wie de aanvrager is.</p>
Instanties: Minimum en Maximum	<p>Configureer het maximale en het minimale aantal instanties dat gebruikers kunnen aanvragen voor een implementatie of een op- of neerschaalbewerking. Door dezelfde waarde in te voeren in de velden Minimum en Maximum, configureert u het exacte aantal instanties geconfigureerd dat moet worden ingericht.</p> <p>XaaS-onderdelen zijn niet schaalbaar en kunnen niet worden bijgewerkt tijdens een schalingsbewerking. Als u XaaS-onderdelen in uw blueprint gebruikt, kunt u een bronactie voor gebruikers maken die kan worden uitgevoerd na een schalingsbewerking, waarmee uw XaaS-onderdelen naar wens kunnen worden geschaald of bijgewerkt. U kunt schalen deactiveren door het aantal instanties te configureren dat is toegestaan bij elk machineonderdeel.</p>

Tabblad **Versie-informatie**

Hier configureert u instellingen voor de versie-informatie van een OpenStack-machineonderdeel.

Tabel 3-25. Tabblad **Versie-informatie**

Instelling	Beschrijving
Blueprinttype	Voor administratieve doeleinden en licentiedoeleinden selecteert u of machines die vanaf deze blueprint zijn ingericht, worden geclassificeerd als Desktop of als Server.
Inrichtingswerkstroom	<p>De volgende inrichtingswerkstromen zijn beschikbaar voor een OpenStack-machineonderdeel:</p> <ul style="list-style-type: none"> ■ CloudLinuxKickstartWorkflow <p>Richt een machine in door op te starten vanuit een ISO-image en vervolgens een Kickstart- of autoYaSt-configuratiebestand en een distributie-image voor Linux te gebruiken om het besturingssysteem op de machine te installeren.</p> ■ CloudProvisioningWorkflow <p>Maak een machine door te starten vanaf een virtual machine-instantie of een op de cloud gebaseerde installatiekopie.</p> ■ CloudWIMImageWorkflow <p>Richt een machine in door op te starten in een WinPE-omgeving en een besturingssysteem te installeren met behulp van een WIM-image (Windows Imaging File Format) van een bestaande Windows-referentiemachine.</p> <p>Voor blueprints met een WIM-inrichtingswerkstroom moet de opgegeven opslagwaarde rekening houden met de grootte van elke schijf die op de machine wordt gebruikt. Gebruik de totale waarde van alle schijven als minimumopslagwaarde voor het machineonderdeel. Zorg er tevens voor dat elke schijf groot genoeg is om het besturingssysteem te kunnen huisvesten.</p>
OpenStack-image	Selecteer een beschikbare OpenStack-image. Een OpenStack-image is een sjabloon die een softwareconfiguratie bevat, inclusief een besturingssysteem. De images worden beheerd door OpenStack-accounts. U kunt de lijst met weergegeven namen van OpenStack-images specifieker maken door de optie Filters in het vervolgkeuzemenu van de kolom Namen te gebruiken.

Tabel 3-25. Tabblad **Versie-informatie** (vervolg)

Instelling	Beschrijving
Sleutelpaar	<p>Sleutelparen zijn optioneel voor inrichting met OpenStack. Sleutelparen worden gebruikt om een clouddinstantie in te richten en ermee verbinding te maken. Daarnaast worden ze gebruikt voor de ontsleuteling van Windows-wachtwoorden en de aanmelding bij Linux-machines. Voor sleutelparen zijn de volgende opties beschikbaar:</p> <ul style="list-style-type: none"> ■ Niet opgegeven Hiermee wordt het gedrag bepaald van het sleutelpaar op het niveau van de blueprint in plaats van het niveau van de reservering. ■ Automatisch gegenereerd per bedrijfsgroep Hiermee bepaalt u dat elke machine die in dezelfde bedrijfsgroep wordt ingericht, hetzelfde sleutelpaar heeft, inclusief machines die in andere reserveringen worden ingericht wanneer de machines dezelfde computingbron en bedrijfsgroep hebben. Omdat de sleutelparen zijn gekoppeld aan een bedrijfsgroep, worden de sleutelparen verwijderd, wanneer de bedrijfsgroep wordt verwijderd. ■ Automatisch gegenereerd per machine Hiermee bepaalt u dat elke machine een uniek sleutelpaar heeft. De optie voor automatisch genereren per machine is de veiligste methode omdat er geen sleutelparen worden gedeeld tussen machines onderling.
Soorten	<p>Selecteer een of meer OpenStack-soorten. Een OpenStack-soort is een virtuele hardwaresjabloon waarmee de specificaties van machinebronnen worden gedefinieerd voor instanties die in OpenStack zijn ingericht. Soorten worden beheerd door de OpenStack-provider en worden geïmporteerd tijdens het verzamelen van gegevens.</p>

Tabblad **Machinebronnen**

Hier geeft u instellingen op voor de gebruikte CPU's, geheugenbronnen en opslagbronnen van het OpenStack-machineonderdeel.

Tabel 3-26. Tabblad **Machinebronnen**

Instelling	Beschrijving
CPU's: Minimum en Maximum	Geef aan hoeveel CPU's er minimaal en maximaal kunnen worden gebruikt door ingerichte machines.
Geheugen (MB): Minimum en Maximum	Voer de minimale en maximale hoeveelheid geheugen in die kan worden gebruikt door ingerichte machines.
Opslag (GB): Minimum en Maximum	Voer een minimale en maximale hoeveelheid opslagruimte in die kan worden gebruikt door ingerichte machines. Voor blueprints met een WIM-inrichtingswerkstroom moet de opgegeven opslagwaarde rekening houden met de grootte van elke schijf die op de machine wordt gebruikt. Gebruik de totale waarde van alle schijven als minimumopslagwaarde voor het machineonderdeel. Zorg er tevens voor dat elke schijf groot genoeg is om het besturingssysteem te kunnen huisvesten.

Tabblad **Eigenschappen**

Hier kunt u desgewenst aangepaste gegevens opgeven voor eigenschappen en eigenschapsgroepen van het OpenStack-machineonderdeel.

Via het tabblad **Eigenschappen** kunt u aangepaste eigenschappen afzonderlijk of groepsgewijs toevoegen aan het machineonderdeel. U kunt het tabblad **Eigenschappen** ook gebruiken om aangepaste eigenschappen en eigenschapsgroepen toe te voegen aan de algemene blueprint die u maakt of bewerkt met behulp van de pagina **Blueprinteigenschappen**.

Via het tabblad **Aangepaste eigenschappen** kunt u opties voor bestaande aangepaste eigenschappen toevoegen en instellen. Aangepaste eigenschappen worden bij vRealize Automation geleverd, maar u kunt ook nieuwe eigenschapsdefinities toevoegen.

Tabel 3-27. Instellingen tabblad **Eigenschappen > Aangepaste eigenschappen**

Instelling	Beschrijving
Naam	Voer de naam van de aangepaste eigenschap in of selecteer een beschikbare aangepaste eigenschap in het vervolgkeuzemenu. Eigenschappen worden alleen weergegeven in het vervolgkeuzemenu als uw tenantbeheerder of materiaalbeheerder eigenschapsdefinities heeft gemaakt.
Waarde	Typ of bewerk de waarde die u wilt koppelen aan de naam van de aangepaste eigenschap. Stel de waarde bijvoorbeeld in op true, zodat gebruikers aan wie rechten zijn verleend, via SSH verbinding kunnen maken met VM's.
Versleuteld	U kunt ervoor kiezen om de eigenschapswaarde te coderen, bijvoorbeeld als de waarde een wachtwoord is.

Tabel 3-27. Instellingen tabblad **Eigenschappen** > **Aangepaste eigenschappen** (vervolg)

Instelling	Beschrijving
Overschrijfbaar	U kunt opgeven dat de eigenschapswaarde kan worden overschreven door de volgende persoon of hierop volgende persoon die de eigenschap gebruikt. Als u Weergeven in aanvraag selecteert, kunnen gebruikers eigenschapswaarden bewerken wanneer ze catalogusitems aanvragen.
Weergeven in aanvraag	U kunt de eigenschapsnaam en -waarde weergeven voor gebruikers wanneer deze de inrichting van een machine aanvragen. Selecteer de optie Overschrijfbaar als u wilt dat gebruikers een waarde opgeven.

Via het tabblad **Eigenschapsgroepen** kunt u instellingen voor bestaande aangepaste eigenschapsgroepen toevoegen en instellen. U kunt zelf eigenschapsgroepen maken of eigenschapsgroepen gebruiken die voor u zijn gemaakt.

Tabel 3-28. Instellingen tabblad **Eigenschappen** > **Eigenschapsgroepen**

Instelling	Beschrijving
Naam	Selecteer een beschikbare eigenschapsgroep in het vervolgkeuzemenu.
Naar boven en Naar beneden	Maak een hiërarchische sortering van de eigenschapsgroepen in aflopende volgorde. De eerste eigenschapsgroep in de lijst krijgt dan voorrang boven de tweede eigenschapsgroep in de lijst, enzovoort.
Eigenschappen weergeven	Geef de aangepaste eigenschappen in de geselecteerde eigenschapsgroep weer.
Samengevoegde eigenschappen weergeven	Geef de aangepaste eigenschappen weer in de volgorde waarin ze worden weergegeven in de lijst met eigenschapsgroepen. Als dezelfde eigenschap in meerdere groepen tegelijk voorkomt, wordt de eigenschap één keer in de lijst opgenomen, en wel op de positie waarin deze voor de eerste keer werd aangetroffen.

Aangepaste eigenschappen voor netwerken gebruiken

U kunt netwerk- en beveiligingsinformatie opgeven voor andere machineonderdelen dan vSphere en voor blueprints die NSX niet bevatten door aangepaste eigenschappen voor netwerken te gebruiken op het niveau van de blueprint of het machineonderdeel.

De onderdelen van **Netwerk en beveiliging** zijn alleen beschikbaar voor gebruik in combinatie met vSphere-machineonderdelen. Er is geen tabblad **Netwerk** of **Beveiliging** voor andere machineonderdelen dan vSphere.

Voor vSphere-machineonderdelen met gekoppelde NSX gebruikt u de netwerk-, beveiligings- en load balancing-instellingen in de gebruikersinterface. Voor machineonderdelen zonder tabblad **Netwerk** of **Beveiliging** kunt u netwerk- en beveiligingseigenschappen, zoals `VirtualMachine.Network0.Name`, toevoegen aan het tabblad **Eigenschappen** in het ontwerpcanvas. Netwerk-, beveiligings- en load balancer-eigenschappen voor NSX zijn uitsluitend van toepassing op vSphere-machines.

U kunt aangepaste eigenschappen individueel definiëren of als deel van een bestaande eigenschapsgroep met behulp van het tabblad **Eigenschappen** bij het configureren van een machineonderdeel in het ontwerpcanvas. De aangepaste eigenschappen die u definieert voor een machineonderdeel zijn van toepassing op machines van dat type die vanaf de blueprint worden ingericht.

Voor informatie over de beschikbare aangepaste eigenschappen, gaat u naar *Naslaggids voor aangepaste eigenschappen*.

Problemen oplossen bij blueprints voor kloon en gekoppelde kloon

Er ontbreken machines of sjablonen wanneer u een blueprint maakt van een gekoppelde kloon of kloon. Het lukt niet om machines in te richten bij een machine-aanvraag met behulp van een gedeelde blueprint van een kloon.

Probleem

Wanneer u werkt met blueprints van een kloon of gekoppelde kloon, kunnen de volgende problemen optreden:

- Wanneer u een blueprint maakt van een gekoppelde kloon, worden er geen machines weergegeven in de kloonlijst of wordt de machine die u wilt klonen, niet weergegeven.
- Wanneer u een blueprint van een kloon maakt, worden er geen sjablonen weergegeven in de lijst met sjablonen die u wilt klonen of wordt de gewenste sjabloon niet weergegeven.
- Wanneer machines worden aangevraagd door gebruik te maken van uw gedeelde blueprint van een kloon, mislukt de inrichting.
- Omdat gegevensverzamelingen steeds op een specifiek tijdstip worden uitgevoerd, is het mogelijk dat gebruikers een verwijderde sjabloon nog steeds te zien krijgen wanneer ze blueprints van gekoppelde klonen maken of bewerken.

Houd er rekening mee dat gekoppelde klonen niet worden ondersteund bij de inrichting op SDRS. Gekoppelde klonen zouden in dezelfde datastore gemaakt worden als de bovenliggende datastore, maar niet geherbalanceerd worden in de clusterdatastores. In dergelijke gevallen kan de bovenliggende datastore uiteindelijk vol raken.

Oorzaak

Er zijn meerdere oorzaken mogelijk voor deze algemene problemen met blueprints van klonen en gekoppelde klonen.

Voor gerelateerde informatie over de opties **Klonen van** en **Klonen van momentopname** met **Huidige momentopname gebruiken** die beschikbaar zijn wanneer u blueprints maakt, raadpleegt u [Instellingen voor vSphere-machineonderdelen in vRealize Automation](#).

Tabel 3-29. Oorzaken voor algemene problemen met blueprints van klonen en gekoppelde klonen

Probleem	Oorzaak	Oplossing
Ontbrekende machines	U kunt alleen blueprints van gekoppelde klonen maken door machines te gebruiken die u beheert als een tenantbeheerder of bedrijfsgroepbeheerder.	<p>Een gebruiker in de tenant of bedrijfsgroep moet een vSphere-machine aanvragen. Als u over de juiste rollen beschikt, kunt u dit zelf doen.</p> <p>Mogelijk krijgt u in dit dialoogvenster ook onbeheerde machines te zien.</p> <p>Mogelijk zijn er beheerde machines geïmporteerd. Het is niet vereist dat machines die vanaf vRealize Automation worden ingericht, in dit dialoogvenster te zien zijn.</p>
Ontbrekende sjablonen	Het verzamelen van gegevens is mislukt op een bepaald endpoint of er zijn geen endpoints beschikbaar op het platform van het onderdeel.	<ul style="list-style-type: none"> ■ Als de endpoints in een cluster staan en meerder computerbronnen bevatten, controleert u of uw IaaS-beheerder het cluster met de sjablonen heeft toegevoegd aan uw materiaalgroep. ■ Voor nieuwe sjablonen controleert u of IT de sjablonen op hetzelfde cluster heeft geplaatst als de materiaalgroep.
Inrichtingsprobleem met gedeelde blueprint	Er is voor blueprints geen verificatie beschikbaar om te controleren of de geselecteerde sjabloon bestaat in de reservering waarmee een machine wordt ingericht op basis van uw gedeelde blueprint van een kloon.	Overweeg om rechten te gebruiken om de toegang tot de blueprint te beperken tot gebruikers die een reservering voor de computerbron hebben waarop de sjabloon zich bevindt.

Tabel 3-29. Oorzaken voor algemene problemen met blueprints van klonen en gekoppelde klonen (vervolg)

Probleem	Oorzaak	Oplossing
Inrichtingsprobleem met een gastagent	Mogelijk wordt de virtual machine onmiddellijk opgestart nadat de aanpassing van het gastbesturingssysteem is voltooid terwijl de werkitens van de gastagent nog niet zijn voltooid. Hierdoor mislukt de inrichting. U kunt de aangepaste eigenschap <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> gebruiken om de vertraging te verlengen.	Controleer of u de aangepaste eigenschap <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> hebt toegevoegd. De waarde moet de indeling UU:MM:SS hebben. Als de waarde niet is ingesteld, is de standaardwaarde één minuut (00:01:00).
De inrichting met blueprints van een kloon of gekoppelde kloon mislukt, omdat de sjabloon waarop de kloon is gebaseerd niet wordt gevonden	Het is niet mogelijk om machines in te richten vanaf een blueprint die is gekloond op basis van een sjabloon die niet meer bestaat. vRealize Automation voert een regelmatige gegevensverzameling uit. Standaard gebeurt dit elke 24 uur. Als een sjabloon wordt verwijderd, wordt de wijziging pas bij de volgende gegevensverzameling doorgevoerd. Daardoor kan het voorkomen dat een blueprint wordt gemaakt op basis van een sjabloon die niet meer bestaat.	Voer de definitie van de blueprint opnieuw uit op basis van een bestaande sjabloon en vraag de inrichting vervolgens opnieuw aan. U kunt uit voorzorg een gegevensverzameling uitvoeren voordat u de blueprint van een kloon of gekoppelde kloon definieert.

Blueprints met NSX-instellingen ontwerpen

Als u vRealize Automation-integratie met NSX for vSphere of NSX-T hebt geconfigureerd, kunt u netwerk-, beveiligings- en load balancer-onderdelen gebruiken om uw blueprints te configureren voor het inrichten van machines.

U kunt ook de volgende NSX-instellingen voor netwerk en beveiliging toevoegen aan de algehele blueprint:

- **Transportzone**
Bevat de netwerken die worden gebruikt voor de ingerichte machine-implementatie.
- **Netwerkreserveringsbeleid**
Beheert de netwerkcommunicatie voor de ingerichte machine-implementatie.
- **App-isolatie**
Staat alleen intern verkeer toe tussen de machines die worden gebruikt in de ingerichte machine-implementatie.

Voor meer informatie over integratie van vRealize Automation en NSX raadpleegt u het blogartikel [vRA en NSX - Inleiding tot netwerk- en beveiligingsautomatisering](#) en de voorbeeldinhoud voor de reeks cursussen over [Netwerken en beveiliging met vRealize Automation en NSX](#).

NSX-instellingen zijn alleen van toepassing op vSphere-machineonderdeeltypen.

Instellingen op de pagina's Nieuwe blueprint en Blueprinteigenschappen voor NSX in vRealize Automation

U kunt instellingen opgeven die gelden voor de volledige vRealize Automation-blueprint, inclusief enkele NSX-instellingen, door de pagina **Nieuwe blueprint** te gebruiken wanneer u de blueprint maakt. Als u de blueprint hebt gemaakt, kunt u deze instellingen bewerken op de pagina **Blueprinteigenschappen**.

Tabblad Algemeen

Instellingen op het tabblad Algemeen zijn van toepassing op de gehele vRealize Automation-blueprint.

Tabel 3-30. Instellingen tabblad **Algemeen**

Instelling	Beschrijving
Naam	Voer een naam in voor uw blueprint.
Id	Het id-veld wordt automatisch ingevuld op basis van de door u ingevoerde naam. U kunt dit veld nu bewerken, maar u kunt het niet meer wijzigen nadat u de blueprint hebt opgeslagen. Identificatie is permanent en uniek binnen de tenant. U kunt deze gebruiken om via programmering met blueprints te werken en om eigenschapsbindingen te maken.
Beschrijving	Vat uw blueprint samen ten behoeve van andere architecten. Deze beschrijving wordt ook voor gebruikers op het aanvraagformulier weergegeven.
Implementatielimiet	Geef aan hoeveel implementaties er maximaal kunnen worden gemaakt wanneer u deze blueprint gebruikt voor het inrichten van machines.
Aantal leasedagen: Minimum en Maximum	<p>Voer een minimum- en een maximumwaarde in om gebruikers de keuze te geven in een bereik van leasheduren. Wanneer de lease eindigt, wordt de implementatie vernietigd dan wel gearchiveerd. Als u geen minimum- of maximumwaarde opgeeft, komt de lease nooit te vervallen.</p> <p>Voer de lease-informatie voor uw machines in uw vRealize Automation-blueprint in en niet in de toepassing van het oorspronkelijke endpoint. Als u de lease-informatie in een externe toepassing opgeeft, wordt deze niet herkend in vRealize Automation.</p>
Archiefdagen	U kunt een archiveringsperiode opgeven om implementaties tijdelijk te behouden in plaats van implementaties te vernietigen zodra hun lease verloopt. Geef 0 op om de implementatie te vernietigen zodra de bijbehorende lease verloopt. De archiefperiode begint op de dag dat de lease verloopt. Wanneer de archiefperiode eindigt, wordt de implementatie vernietigd. De standaardwaarde is 0.
Updates voor bestaande implementaties doorvoeren	Ruimere minimum-maximumbereiken voor CPU, geheugen of opslag worden gepusht naar actieve implementaties die zijn ingericht vanaf de blueprint. Het nieuwe bereik moet het oude bereik volledig insluiten. Bijvoorbeeld: als het minimum oorspronkelijk 32 is en het maximum 128 (32, 128), kan een wijziging zoals (16, 128) of (32, 256) of (2, 1000) worden toegepast bij herconfiguratie of uitschaling, maar een wijziging zoals (33, 512) of (4, 64) niet.

Tabblad **NSX-instellingen**

Als u NSX hebt geconfigureerd, kunt u bij het maken of bewerken van een blueprint NSX-instellingen opgeven voor de transportzone, het netwerkreserveringsbeleid en de app-isolatie. Deze instellingen zijn beschikbaar op het tabblad **NSX-instellingen** van de pagina's **Blueprint** en **Blueprinteigenschappen**.

Voor informatie over uw NSX-toepassing raadpleegt u de [documentatie voor VMware NSX Data Center for vSphere](#) of de [documentatie voor VMware NSX-T Data Center](#).

Tabel 3-31. Instellingen tabblad **NSX-instellingen**

Instelling	Beschrijving
Transportzone	<p>Selecteer een bestaande NSX-transportzone met een of meer netwerken die door de ingerichte machine-implementatie kunnen worden gebruikt.</p> <p>Met een transportzone wordt aangegeven welke clusters de netwerken kunnen omvatten. Als er bij de inrichting van machines een transportzone is opgegeven in een reservering en in een blueprint, moeten de waarden voor de transportzone overeenstemmen. Alleen de transportzones die van toepassing zijn op de huidige tenant, zijn beschikbaar.</p> <p>Een transportzone is vereist voor blueprints die netwerk- en beveiligingsobjecten op aanvraag voor NSX for vSphere of NSX-T bevatten.</p> <p>Zie Een NSX-transportzone toepassen op een blueprint voor meer informatie.</p> <p>Geef een transportzone op die geschikt is voor een implementatie van NSX for vSphere of NSX-T.</p>
Netwerkreserveringsbeleid	<p>Selecteer een netwerkreserveringsbeleid voor NSX for vSphere om te helpen bepalen waar u de edge of DLR wilt plaatsen in de implementatie.</p> <p>Als vRealize Automation een machine met NAT- of geleide netwerken inricht, wordt een geleide gateway ingericht als netwerkrouter. De Edge- of geleide gateway is een beheermachine die computerbronnen verbruikt. Deze beheert ook de netwerkcommunicatie voor alle machines in die implementatie. De reservering die wordt gebruikt om de Edge of geleide gateway in te richten, bepaalt welk extern netwerk wordt gebruikt voor de virtuele IP-adressen van NAT en load balancers. We raden u aan om afzonderlijke beheerclusters te gebruiken voor beheermachines, zoals NSX Edges.</p> <p>Selecteer een netwerkreserveringsbeleid voor NSX-T om te helpen bepalen waar u de logische router van tier 0 wilt plaatsen in de blueprintimplementatie.</p> <p>Zie Een NSX-netwerkreserveringsbeleid toepassen op een blueprint voor meer informatie.</p> <p>Geef een reserveringsbeleid op dat geschikt is voor een implementatie van NSX for vSphere of NSX-T. Clusters die door de blueprint worden geïmplementeerd, kunnen worden beheerd door NSX for vSphere of NSX-T.</p>
Isolatie van app	<p>Schakel het selectievakje Isolatie van app in als u gebruik wilt maken van het beveiligingsbeleid voor app-isolatie dat is geconfigureerd in NSX for vSphere. Het app-isolatiebeleid wordt toegepast op alle vSphere-machineonderdelen in de blueprint. U kunt beveiligingsgroepen en -tags toevoegen, zodat vRealize Orchestrator het geïsoleerde netwerk kan openen en de app-isolatie kan voorzien van aanvullende paden voor inkomend en uitgaand verkeer.</p> <p>Zie NSX-appisolatie toepassen op een blueprint voor meer informatie.</p>

Tabblad Eigenschappen

Aangepaste eigenschappen die u op blueprintniveau toevoegt, zijn van toepassing op de gehele blueprint, inclusief alle onderdelen. Zie *Naslaggids voor aangepaste eigenschappen* voor informatie over de voorrangsvolgorde.

Tabel 3-32. Instellingen tabblad **Eigenschappen**

Tabblad	Instelling	Beschrijving
Eigenschapsgroepen	Eigenschapsgroepen zijn herbruikbare groepen met eigenschappen om het toevoegen van aangepaste eigenschappen aan blueprints te vereenvoudigen.	
	Toevoegen	Voeg hiermee een of meer bestaande eigenschapsgroepen toe en pas deze toe op de algehele blueprint. De volgende aan Containers gerelateerde eigenschapsgroepen zijn beschikbaar: <ul style="list-style-type: none"> ■ Eigenschappen voor containerhosts met certificaatverificatie ■ Eigenschappen voor containerhosts met verificatie op basis van gebruikers/wachtwoorden
	Naar boven /Naar beneden	Beheer de voorrangsvolgorde die u aan alle eigenschapsgroepen ten opzichte van elkaar hebt gegeven door prioriteiten in te stellen voor groepen. De eerste groep in de lijst heeft de hoogste prioriteit en de aangepaste eigenschappen ervan hebben als eerste voorrang. U kunt ook schuiven om de volgorde te wijzigen.
	Eigenschappen weergeven	Geef de aangepaste eigenschappen in de geselecteerde eigenschapsgroep weer.
	Samengevoegde eigenschappen weergeven	Als een aangepaste eigenschap in meer dan één eigenschapsgroep is opgenomen, krijgt de waarde die in de eigenschapsgroep met de hoogste prioriteit is opgenomen voorrang.
Aangepaste eigenschappen	U kunt individuele aangepaste eigenschappen toevoegen in plaats van eigenschapsgroepen.	
	Nieuw	Voeg hiermee een individuele aangepaste eigenschap toe en pas deze toe op de algehele blueprint.
	Naam	Voer de eigenschapsnaam in. Zie <i>Naslaggids voor aangepaste eigenschappen</i> voor een lijst met aangepaste eigenschappen en hun definities.
	Waarde	Voer de waarde in voor de aangepaste eigenschap.

Tabel 3-32. Instellingen tabblad **Eigenschappen** (vervolg)

Tabblad	Instelling	Beschrijving
	Versleuteld	Versleutel de eigenschapswaarde, bijvoorbeeld als de waarde een wachtwoord is.
	Overschrijfbaar	De blueprintgebruiker kan de eigenschapswaarde overschrijven. Als u Weergeven in aanvraag selecteert, kunnen gebruikers eigenschapswaarden zien en bewerken wanneer ze catalogusitems aanvragen.
	Weergeven in aanvraag	De eigenschapsnaam en -waarde zijn zichtbaar voor gebruikers op het inrichtingsaanvraagformulier. Selecteer Overschrijfbaar als u gebruikers wilt toestaan om een waarde op te geven.

Een NSX-transportzone toepassen op een blueprint

Een NSX-beheerder kan transportzones maken om clustergebruik van netwerken te beheren.

Een transportzone controleert welke hosts een logische schakeloptie kan bereiken. De zone kan een of meer hostclusters bevatten, inclusief hosts in meerdere vCenters.

Voor blueprints die een NAT op aanvraag of een geleid netwerk op aanvraag bevatten, geeft u een transportzone op die de netwerken bevat die moeten worden gebruikt door de ingerichte machine-implementatie.

U moet een transportzone opgeven voor blueprints die een NSX-T-endpoint bevatten.

De transportzone die u opgeeft voor de blueprint, moet overeenkomen met de transportzone die u opgeeft voor de reservering die door de blueprint wordt gebruikt. Zie [Een NSX-netwerkreserveringsbeleid toepassen op een blueprint](#).

- Als uw blueprint geen NSX-T-onderdelen op aanvraag gebruikt, wordt de waarde voor de transportzone genegeerd.
- NSX-T ondersteunt meerdere overlay-transportzones en meerdere VLAN-transportzones.
- Een transportzone is vereist om een logische schakeloptie te maken. Logische schakelopties worden gemaakt binnen transportzones.
- Alleen de transportzones voor de huidige tenant worden beschikbaar gesteld bij het ontwerpen van een blueprint. Transportzones worden beschikbaar gemaakt als ze worden gebruikt door een reservering in de huidige tenant.

Een NSX-netwerkreserveringsbeleid toepassen op een blueprint

Wanneer u de blueprint inricht, wordt het reserveringsbeleid gebruikt om de reserveringen te groeperen die voor de implementatie in aanmerking kunnen komen. Elke reservering bevat netwerkinformatie.

Als er een transportzone in dit reserveringsbeleid aanwezig is, moet deze overeenkomen met de transportzone die in de blueprint is opgegeven. Zie [Een NSX-transportzone toepassen op een blueprint](#).

U kunt een netwerkreserveringsbeleid op blueprintniveau toepassen met behulp van de pagina **Nieuwe blueprint** of **Blueprinteigenschappen**.

Overwegingen voor NSX for vSphere

Voor NSX for vSphere helpt dit reserveringsbeleid bij het bepalen van de plaatsing van de NSX-edge of selectie van de DLR (logische gedistribueerde router) die gekoppeld is met de netwerken op aanvraag. Dit wordt ook wel een reserveringsbeleid voor geleide gateways of een edge-reserveringsbeleid genoemd.

Voor NSX for vSphere bijvoorbeeld kan met een NAT-netwerkprofiel en een load balancer vRealize Automation worden ingeschakeld om een NSX-edge-servicesgateway te implementeren. Een geleid netwerkprofiel maakt gebruik van een NSX for vSphere logische gedistribueerde router (DLR). De DLR moet worden gemaakt in NSX voordat deze kan worden verbruikt door vRealize Automation. vRealize Automation kan geen DLR's maken. Nadat de gegevens zijn verzameld, kan vRealize Automation de DLR gebruiken voor het inrichten van virtual machines.

Een NSX-edge biedt routingsservices en connectiviteit met netwerken die extern zijn voor de NSX-implementatie. De NSX-Edge-gateway verbindt geïsoleerde subnetten met gedeelde (uplink-)netwerken door veelgebruikte gateway-services zoals NAT en dynamische routing te bieden. Veelgebruikte implementaties van NSX-edges omvatten omgevingen met meerdere tenants waarbij de NSX-edge virtuele grenzen voor elke tenant maakt.

vRealize Automation richt een geleide gateway in, bijvoorbeeld een edge services-gateway voor NAT-netwerken en voor load balancers. Voor geleide netwerken maakt vRealize Automation gebruik van gedistribueerde routers.

De reservering die wordt gebruikt om de Edge of geleide gateway in te richten, bepaalt de beschikbare profielen voor NAT-, private of geleide netwerken en de virtuele IP-adressen van de load balancer.

Overwegingen voor NSX-T

Voor NSX-T helpt dit reserveringsbeleid bij het selecteren van een logische router van tier 0 die voor de implementatie wordt gebruikt.

Logische routers van tier 0 hebben downlinkpoorten om verbinding te maken met logische routers van tier 1 en uplinkpoorten om verbinding te maken met externe netwerken. vRA verbindt een logische router van tier 1 met een logische router van tier 0 voor toegang tot een noordelijke fysieke router en wijst een edge-cluster toe aan een logische router voor het uitvoeren van NAT- en load balancer-services.

NSX-appisolatie toepassen op een blueprint

U kunt appisolatie inschakelen zodat alleen intern verkeer tussen de door de blueprint ingerichte onderdelen wordt toegestaan.

Een NSX-appisolatiebeleid fungeert als een firewall om al het binnenkomende en het uitgaande verkeer naar en van de ingerichte machines in de implementatie te blokkeren. Wanneer u een gedefinieerd NSX-appisolatiebeleid opgeeft, kunnen de machines die zijn ingericht door de blueprint met elkaar communiceren maar geen verbindingen maken buiten de firewall.

Wanneer een regel voor appisolatie wordt opgegeven, en beveiligingsregels ook zijn opgegeven door het gebruik van beveiligingsgroepen in de blueprint, is de appisolatie-instelling de laatste regel die wordt verwerkt tijdens de blueprintimplementatie.

U kunt appisolatie op blueprintniveau toepassen met behulp van de pagina **Nieuwe blueprint of Blueprinteigenschappen**.

Overwegingen voor NSX for vSphere

De ingerichte onderdelen worden in een beveiligingsgroep geplaatst die wordt geïsoleerd met behulp van firewallregels. Voor de activering moet het vSphere-endpoint zijn geconfigureerd om NSX-appisolatie te ondersteunen.

Bij gebruik van een NSX for vSphere-appisolatiebeleid is alleen intern verkeer toegestaan tussen de machines die door de blueprint zijn ingericht. Wanneer u een inrichting aanvraagt, wordt er een beveiligingsgroep gemaakt voor de machines die worden ingericht. Een beleid voor appisolatie wordt gemaakt in NSX for vSphere en toegepast op de beveiligingsgroep. Firewallregels worden gedefinieerd in het beveiligingsbeleid om alleen intern verkeer toe te staan tussen de onderdelen in de implementatie.

Bij inrichting met een blueprint die zowel een NSX for vSphere Edge-load balancer als een NSX for vSphere-appisolatiebeveiligingsbeleid gebruikt, wordt de dynamisch ingerichte load balancer niet toegevoegd aan de beveiligingsgroep. Dit voorkomt dat de load balancer communiceert met de machines waarvoor het verbindingen moet afhandelen. Omdat Edges worden uitgesloten uit de met NSX for vSphere gedistribueerde firewall, kunnen deze niet worden toegevoegd aan beveiligingsgroepen. Om ervoor te zorgen dat de taakverdeling correct werkt, gebruikt u een andere beveiligingsgroep of een ander beveiligingsbeleid dat het verkeer naar de onderdeel-VM's toestaat voor de taakverdeling.

Het appisolatiebeleid heeft een lagere prioriteit in vergelijking met andere beveiligingsgroepen in NSX for vSphere. Als de ingerichte implementatie bijvoorbeeld een webonderdeelmachine en een apponderdeelmachine bevat en de webonderdeelmachine een webservice host, moet de service binnenkomend verkeer toestaan op poorten 80 en 443. In dit geval moeten gebruikers een webbeveiligingsbeleid in NSX for vSphere maken met firewallregels die zijn gedefinieerd om binnenkomend verkeer naar deze poorten toe te staan. In vRealize Automation moeten gebruikers het webbeveiligingsbeleid toepassen op het webonderdeel van de ingerichte machine-implementatie.

Opmerking Als een blueprint een load balancer bevat en app-isolatie is ingeschakeld, worden de load balancer-VIP's aan de app-isolatiebeveiligingsgroep toegevoegd als IPSet. Als een blueprint een beveiligingsgroep op aanvraag bevat die is gekoppeld aan een machinelaag die ook is gekoppeld aan een load balancer, bevat de beveiligingsgroep op aanvraag de machinelaag IPSet en VIP's.

Als de webonderdeelmachine toegang vereist tot de apponderdeelmachine met behulp van een load balancer op de poorten 8080 en 8443, moet het webbeveiligingsbeleid naast de bestaande firewallregels die het binnenkomend verkeer op de poorten 80 en 443 toestaan, tevens firewallregels bevatten die uitgaand verkeer via de poorten 8080 en 8443 mogelijk maken.

Overwegingen voor NSX-T

De ingerichte onderdelen worden in een NSGroup geplaatst die wordt geïsoleerd met behulp van firewallregels. Voor de activering moet het vSphere-endpoint zijn geconfigureerd om NSX-appisolatie te ondersteunen.

NSX-T ondersteunt het maken van een logische-routertopologie met twee tiers: de logische router op de bovenste tier is tier 0 en de logische router op de onderste tier is tier 1. Deze structuur biedt zowel de beheerder van de provider als de tenantbeheerders volledige controle over hun services en beleidsregels. In NSX-T beheren en configureren beheerders routing en services van tier 0 en beheren en controleren tenantbeheerders tier 1.

Instellingen van netwerk- en beveiligingsonderdelen configureren in vRealize Automation

vRealize Automation ondersteunt gevirtualiseerde netwerken op basis van het NSX-platform. Ook geïntegreerde Containers voor vRealize Automation-netwerken worden ondersteund.

Om netwerk en beveiliging van NSX te integreren met vRealize Automation, moet een IaaS-beheerder endpoints van vSphere en NSX configureren. vRealize Automation ondersteunt NSX for vSphere en NSX-T.

Voor informatie over externe voorbereidingen raadpleegt u *vRealize Automation configureren*.

U kunt netwerkprofielen maken die netwerkinstellingen opgeven in reserveringen en in de blueprint. Externe netwerkprofielen definiëren bestaande fysieke netwerken. NAT op aanvraag en geleide netwerkprofielen kunnen logische NSX-switches en geschikte routeringsinstellingen voor een nieuw netwerkpad opbouwen.

De instellingen voor netwerk- en beveiligingsonderdelen die u aan de blueprint toevoegt, worden afgeleid van uw configuratie van NSX for vSphere en NSX-T. Raadpleeg de *Administration Guide* in de [NSX for vSphere-productdocumentatie](#) of [NSX-T-productdocumentatie](#), afhankelijk van welke toepassing u gebruikt, voor informatie over het configureren van NSX.

Voor vSphere-machineonderdelen met gekoppelde NSX gebruikt u de netwerk-, beveiligings- en load balancing-instellingen in de gebruikersinterface. Voor machineonderdelen zonder tabblad **Netwerk** of **Beveiliging** kunt u netwerk- en beveiligingseigenschappen, zoals `VirtualMachine.Network0.Name`, toevoegen aan het tabblad **Eigenschappen** in het ontwerpcanvas. Netwerk-, beveiligings- en load balancer-eigenschappen voor NSX zijn uitsluitend van toepassing op vSphere-machines.

Als u een netwerkprofiel opgeeft in een reservering en een blueprint, krijgen de blueprintwaarden voorrang.

Afhankelijk van de computerbron kunt u een transportzone selecteren die een vSphere-endpoint identificeert. Een transportzone geeft de hosts en clusters op die kunnen worden gekoppeld met logische switches die in de zone zijn gemaakt. Een transportzone kan meerdere vSphere-clusters bevatten. De blueprint en de reserveringen die in de inrichting zijn gebruikt, moeten dezelfde transportzone-instellingen hebben. Transportzones worden gedefinieerd in de NSX-omgevingen.

U kunt beveiligingsinstellingen configureren door informatie op te geven in een reservering, blueprint of script van een gastagent. Als machines een gastagent vereisen, voegt u een beveiligingsregel toe aan de reservering of de blueprint.

Ook kunt u een Containers-netwerkonderdeel toevoegen aan een blueprint.

Voor gerelateerde informatie over het configureren van netwerk en beveiliging voor NSX-T in vRealize Automation raadpleegt u het VMware-blogartikel [Application Networking and Security with vRealize Automation and NSX-T](#).

Tenanttoegang voor beveiligingsobjecten beheren in vRealize Automation

U kunt de beschikbaarheid van NSX-beveiligingsobjecten voor meerdere tenants in vRealize Automation beheren.

Wanneer u een NSX-beveiligingsobject maakt, kan de standaardbeschikbaarheid algemeen zijn, wat betekent dat deze beschikbaar is in alle tenants waarvoor het gekoppelde endpoint een reservering heeft, of verborgen voor alle gebruikers behalve de beheerder.

De beschikbaarheid van beveiligingsobjecten voor verschillende tenants is afhankelijk van de vraag of het gekoppelde endpoint een reservering of een reserveringsbeleid in de tenant heeft.

NSX heeft geen beveiligingsgroepen voor de tenant. U kunt echter de beschikbaarheid van de beveiligingsgroep in vRealize Automation beheren met behulp van de aangepaste eigenschap `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects`.

Standaard zijn nieuwe beveiligingsobjecten beschikbaar voor alle tenants voor de gekoppelde NSX-endpoints waarin u een reservering hebt. Als het endpoint geen reservering in de actieve tenant heeft, zijn de beveiligingsobjecten niet beschikbaar in de actieve tenant.

Als u de aangepaste eigenschap `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` op NSX-endpoints nog niet hebt ingesteld, worden nieuwe beveiligingsobjecten standaard ingesteld op algemeen. Beveiligingsobjecten die bestonden voorafgaand aan de upgrade naar deze release van vRealize Automation zijn ingesteld op algemeen ongeacht de aangepaste eigenschap.

Opmerking Wanneer u een upgrade uitvoert naar deze release van vRealize Automation, worden beveiligingsgroepen van de vorige release standaard ingesteld op algemeen. Bestaande beveiligingsgroepen en beveiligingstags zijn beschikbaar in alle tenants waarin het gekoppelde endpoint een reservering heeft.

Door de aangepaste eigenschap `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` toe te voegen aan het bijbehorende NSX-endpoint kunt u nieuwe beveiligingsgroepen standaard verbergen. Deze instelling wordt van kracht de volgende keer dat het NSX-endpoint gegevens verzamelt en wordt alleen toegepast op nieuwe beveiligingsobjecten.

U kunt ook de instelling voor tenants van een bestaand beveiligingsobject programmatisch wijzigen. Bijvoorbeeld: als een beveiligingsgroep is ingesteld op algemeen, kunt u de beschikbaarheid van de tenant van een beveiligingsobject met behulp van de instelling van de gekoppelde tenant-id van het NSX-endpoint wijzigen in de vRealize Automation REST API of in vRealize CloudClient. De beschikbare instellingen van de tenant-id voor het NSX-endpoint zijn als volgt:

- "<global>" - het beveiligingsobject is beschikbaar voor alle tenants. Dit is de standaardinstelling voor bestaande beveiligingsobjecten na de upgrade naar deze release en voor alle nieuwe beveiligingsobjecten die u maakt.
- "<unscoped>" - het beveiligingsobject is niet beschikbaar voor alle tenants. Alleen de systeembeheerder heeft toegang tot het beveiligingsobject. Dit is een ideale instelling voor het definiëren van beveiligingsobjecten die uiteindelijk aan een specifieke tenant worden toegewezen.
- "*tenant_id_name*" - het beveiligingsobject is alleen beschikbaar voor een enkele, benoemde tenant.

U kunt de vRealize Automation REST API of vRealize CloudClient tools gebruiken om de parameter tenant-id (*tenantId*) van beveiligingsobjecten toe te wijzen die zijn gekoppeld aan een specifieke endpoint en aan een benoemde tenant.

Voor informatie over vRealize Automation REST API-opdrachten zie de *Naslaggids voor vRealize Automation API* in de sectie [Documentatie voor vRealize Automation API](#) voor uw vRealize Automation 7.x-release. Voor meer informatie zie de *vRealize Automation-programmeerhandleiding* in de sectie [Documentatie voor vRealize Automation API](#) voor uw vRealize Automation 7.x-release.

Zie <https://code.vmware.com/web/dp/tool/cloudclient> voor informatie over vRealize CloudClient.

Informatie over de NSX-T-implementatietopologieën voor netwerken, beveiliging en load balancer-configuraties

U kunt verschillende implementatietopologieën instellen en gebruiken op basis van hoe u uw NSX-T-netwerk en -beveiliging en uw load balancer-onderdelen configureert in de vRealize Automation-blueprint.

Netwerk en beveiliging

■ Geleide netwerken

Als u een onderdeel van een geleid NSX-T-netwerk koppelt aan een vSphere-machineonderdeel in de blueprint, wordt de volgende topologie ingericht in NSX-T:

- Er wordt een tier 1-router gemaakt.
- Er wordt een logische schakeloptie gemaakt.
- De tier 1-router wordt gedownlinkt naar de logische schakeloptie.
- Specifieke geleide routes worden geadverteerd op de tier 1-router.

■ NAT-netwerken (statisch IP)

Als u een NSX-T NAT-netwerk koppelt aan een vSphere-machineonderdeel in de blueprint, wordt de volgende topologie ingericht in NSX-T:

- Er wordt een tier 1-router gemaakt.
- Er wordt een logische schakeloptie gemaakt.
- De tier 1-router wordt verbonden met het randcluster.
- De tier 1-router wordt geüplinkt naar een tier 0-router; de tier 0-router wordt geselecteerd op basis van de reservering.
- De tier 1-router wordt gedownlinkt naar de logische schakeloptie.
- Alle NAT-routes worden geadverteerd op de tier 1-router.
- Er wordt één extern IP-adres toegewezen voor elk NAT-netwerk op basis van het externe netwerkprofiel dat het NAT-netwerkprofiel op aanvraag ondersteunt. Dit IP-adres wordt gebruikt voor SNAT- en DNAT-regels.
- NAT-netwerken (DHCP)

Als u een NSX-T NAT-netwerk met DHCP koppelt aan een vSphere-machineonderdeel in de blueprint, wordt de volgende topologie ingericht in NSX-T:

- Er wordt een tier 1-router gemaakt.
- Er wordt een logische schakeloptie gemaakt.
- De tier 1-router wordt verbonden met het randcluster.
- De tier 1-router wordt geüplinkt naar een tier 0-router; de tier 0-router wordt geselecteerd op basis van de reservering.
- De tier 1-router wordt gedownlinkt naar de logische schakeloptie.
- Er wordt een DHCP-server met een IP-pool ingericht.
- Alle NAT-routes worden geadverteerd op de tier 1-router.
- App-isolatie

Als app-isolatie is vereist voor een blueprint met NSX-T-onderdelen, wordt de volgende topologie ingericht in NSX-T:

Opmerking U configureert de app-isolatie voor de blueprint op de pagina Blueprint-eigenschappen wanneer u de blueprint maakt of bewerkt.

- Er wordt een NS Group gemaakt.
- Er wordt een firewallsectie, met firewall-isolatieregels, gemaakt.
- De machines in de blueprint worden aan de NS Group voor app-isolatie toegevoegd met behulp van tags.
- Het VIP- en externe IP-adres van de load balancer voor NAT-netwerken op de IPset worden toegevoegd aan de NS Group voor app-isolatie.

Om NS Groups voor app-isolatie te ondersteunen, moet u de machines verbinden met ondoorzichtige netwerken.

- **Bestaande NS Groups**

Als u een onderdeel van een bestaande NS Group koppelt aan een vSphere-machineonderdeel in de blueprint, wordt de volgende topologie ingericht in NSX-T:

- De machines die zijn gekoppeld aan de NS Group worden toegevoegd aan de NS Group in NSX-T met tags als lidmaatschaps criterium.

Om bestaande NS Groups te ondersteunen, moet u de machines verbinden met ondoorzichtige netwerken.

Load balancers

De volgende topologieën worden ondersteund voor load balancers in een NSX-T-blueprintimplementatie:

- One-armed in een NAT-netwerk op aanvraag.
- One-armed in een geleid netwerk op aanvraag.
- One-armed in een extern (bestaand) netwerk.
- Two-armed, één in een NAT- en één in een extern netwerk.
- Two-armed, één in een geleid en één in een extern netwerk.

Als een NSX-T load balancer wordt toegevoegd aan de blueprint, wordt, naast de netwerktopologieën, de volgende topologie ingericht in de implementatie:

- Voor alle topologieën behalve die waarbij de load balancer one-armed is in een extern netwerk:
 - Er wordt één load balancer-service gemaakt, zelfs als de blueprint meerdere load balancer-onderdelen bevat.
 - De load balancer-service wordt gekoppeld aan de tier 1-router, voor de implementatie. De tier 1-router wordt op aanvraag gemaakt.
- Voor topologieën waarbij de load balancer one-armed is in een extern netwerk:
 - Het externe netwerk dat is opgegeven in de reservering moet een VC-ondoorzichtig netwerk zijn (logische NSX-T-schakeloptie).
 - Er moet een tier 1-router bestaan en deze moet gekoppeld zijn aan het externe netwerk (logische NSX-T-schakeloptie).
 - Als er nog geen tier 1-router bestaat, wordt de load balancer-server op aanvraag gemaakt en gekoppeld aan de tier 1-router; anders wordt een reeds bestaande load balancer gebruikt.
- De VIP-route wordt geadverteerd, tenzij het VIP zich in een particulier NAT-netwerk bevindt.
- Er worden een of meer virtuele servers gemaakt in de load balancer-service.

Er gelden beperkingen op het aantal virtuele servers per load balancer-service op basis van de grootte van de load balancer.

- Er wordt een virtuele server-applicatieprofiel gemaakt voor elke virtuele server.
- Er wordt een virtuele server-persistentieprofiel gemaakt voor elke virtuele server waarvoor persistentieopties zijn geconfigureerd.
- Er wordt een lidmaatschapspool geconfigureerd dat het statische IP-adres van elke machine in de lidmaatschapspool bevat.
- Er wordt één load balancer-service gemaakt, ongeacht het aantal load balancer-onderdelen in de blueprint.
- Er wordt een statusmonitor gemaakt en geconfigureerd voor elke ledenpool.

Voor virtuele servers met HTTP-ondersteuning is er, in tegenstelling tot load balancers in NSX for vSphere, geen ondersteuning voor SSL-passthrough in NSX-T load balancers. vRealize Automation configureert de virtuele server van de load balancer zodanig dat SSL wordt beëindigd op de load balancer en dat gewone HTTP van de load balancer wordt gebruikt voor de poolleden. De naam van het certificaat en de naam van het SSL-clientprofiel, die beide moeten bestaan in NSX-T, moeten worden opgegeven bij het configureren van de virtuele server met HTTPS. U kunt certificaten importeren in de NSX-T-trustmanager.

Wanneer de blueprint meer dan één NSX-T-onderdeel bevat, wordt de logische tier 1-router gedeeld door alle onderdelen en dienovereenkomstig geconfigureerd. De externe id van de logische tier 1-router wordt weergegeven in de detailweergave van elk onderdeel op de pagina vRealize Automation-implementaties.

NSX for vSphere-netwerkonderdelen gebruiken in een vRealize Automation-blueprint

U kunt een of meer NSX for vSphere-netwerkonderdelen aan het ontwerpcanvas toevoegen en de bijbehorende instellingen voor vSphere-machineonderdelen in een vRealize Automation-blueprint configureren.

De instellingen voor netwerk- en beveiligingsonderdelen die u aan de blueprint toevoegt, worden afgeleid van uw NSX for vSphere-configuratie. Raadpleeg de *NSX Administration Guide* in de [NSX for vSphere-productdocumentatie](#) voor informatie over het configureren van NSX for vSphere.

Een bestaand netwerkonderdeel toevoegen voor NSX for vSphere

U kunt een bestaand NSX for vSphere-netwerkonderdeel toevoegen aan het ontwerpcanvas om de instellingen hiervan te koppelen aan een of meer vSphere-machineonderdelen van de blueprint.

U kunt een bestaand netwerk als onderdeel gebruiken om een NSX for vSphere-netwerk toe te voegen aan het ontwerpcanvas en de instellingen ervan te configureren voor gebruik met vSphere-machineonderdelen en Software- of XaaS-onderdelen die van toepassing zijn op vSphere.

Wanneer u een onderdeel van een bestaand netwerk of een netwerk op aanvraag koppelt aan een machineonderdeel, wordt de NIC-informatie opgeslagen bij het machineonderdeel. De opgegeven netwerkprofielgegevens worden opgeslagen in het netwerkonderdeel.

U kunt meerdere netwerk- en beveiligingsonderdelen toevoegen aan het ontwerpcanvas.

Voor vSphere-machineonderdelen met gekoppelde NSX gebruikt u de netwerk-, beveiligings- en load balancing-instellingen in de gebruikersinterface. Voor machineonderdelen zonder tabblad **Netwerk** of **Beveiliging** kunt u netwerk- en beveiligingseigenschappen, zoals `VirtualMachine.Network0.Name`, toevoegen aan het tabblad **Eigenschappen** in het ontwerpcanvas. Netwerk-, beveiligings- en load balancer-eigenschappen voor NSX zijn uitsluitend van toepassing op vSphere-machines.

Alleen de netwerkprofielen die van toepassing zijn op de huidige tenant worden beschikbaar gesteld bij het ontwerpen van een blueprint. Met name worden netwerkprofielen beschikbaar gesteld als er ten minste één reservering in de huidige tenant is waarbij ten minste één netwerk is toegewezen aan het profiel.

Voorwaarden

- Netwerkinstellingen maken en configureren voor NSX. Raadpleeg de NSX configuratiechecklist in *vRealize Automation configureren* en de *NSX for vSphere Administration Guide* in de [productdocumentatie voor NSX for vSphere](#).
- Controleer of de NSX-inventaris met succes is uitgevoerd voor uw cluster.
Als u NSX-configuraties in vRealize Automation wilt gebruiken, moet u gegevensverzameling uitvoeren.
- Maak een netwerkprofiel.
- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Open een nieuwe of bestaande blueprint in het ontwerpcanvas met behulp van het tabblad **Ontwerpen**.

Procedure

- 1 Als u de lijst met beschikbare netwerk- en beveiligingsonderdelen wilt weergeven, klikt u op **Netwerk en beveiliging** in de sectie Categorieën.
- 2 Sleep een **Bestaand netwerk**-onderdeel naar het ontwerpcanvas.
- 3 Klik in het tekstvak **Bestaand netwerk** en selecteer een bestaand netwerkprofiel.
De waarden voor de beschrijving, het subnetmasker en de gateway worden ingevuld op basis van het geselecteerde netwerkprofiel.
- 4 (Optioneel) Klik op het tabblad **DNS/WINS**.
- 5 (Optioneel) Geef de DNS- en WINS-instellingen voor het netwerkprofiel op.
 - Primaire DNS
 - Secundaire DNS
 - DNS-achtervoegsel
 - Gewenste WINS

- Alternatieve WINS

Voor een bestaand netwerk kunt u de DNS- of WINS-instellingen niet wijzigen.

6 (Optioneel) Klik op het tabblad **IP-bereiken**.

U ziet het IP-bereik of de IP-bereiken voor het netwerkprofiel. U kunt de sorteervolgorde of kolomweergave wijzigen. Voor NAT-netwerken kunt u ook de waarden van het IP-bereik wijzigen.

7 Als u de blueprint wilt opslaan als concept of verder wilt gaan met het configureren van de blueprint, klikt u op **Opslaan** of **Voltooien**.

Wat nu te doen

U kunt netwerkinstellingen toevoegen op het tabblad **Netwerk** van een vSphere-machineonderdeel.

Het onderdeel Privaat netwerk toevoegen voor NSX for vSphere in vRealize Automation

U kunt het NSX for vSphere-onderdeel Privaat netwerk toevoegen aan het ontwerpcanvas om de instellingen hiervan te koppelen aan een of meer vSphere-machineonderdelen van de vRealize Automation-blueprint.

Alleen de netwerkprofielen die van toepassing zijn op de huidige tenant worden beschikbaar gesteld wanneer u een blueprint ontwerpt.

Deze optie voor privaat netwerk is alleen beschikbaar voor NSX for vSphere. Deze optie is niet beschikbaar voor NSX-T.

Voorwaarden

- Netwerkinstellingen maken en configureren voor NSX. Raadpleeg de NSX configuratiechecklist in *vRealize Automation configureren* en de *NSX for vSphere Administration Guide* in de [productdocumentatie voor NSX for vSphere](#).
- Controleer of de NSX-inventaris met succes is uitgevoerd voor uw cluster.
Als u NSX-configuraties in vRealize Automation wilt gebruiken, moet u gegevensverzameling uitvoeren.
- Maak een netwerkprofiel.
- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Open een nieuwe of bestaande blueprint in het ontwerpcanvas met behulp van het tabblad **Ontwerpen**.

Procedure

- 1 Als u de lijst met beschikbare netwerk- en beveiligingsonderdelen wilt weergeven, klikt u op **Netwerk en beveiliging** in de sectie Categorieën.
- 2 Sleep het onderdeel Privaat netwerk op aanvraag naar het ontwerpcanvas.

- 3 Als u het onderdeel een uniek label wilt geven in het ontwerpcanvas, voert u in het tekstvak **ID** een onderdeelnaam in.
- 4 Selecteer een relevant, bestaand netwerkprofiel in het vervolgkeuzemenu **Profiel bovenliggend netwerk**.
- 5 (Optioneel) Typ een beschrijving van het onderdeel in het tekstvak **Beschrijving**.
- 6 (Optioneel) Klik op het tabblad **DNS/WINS**.
- 7 (Optioneel) Geef de DNS- en WINS-instellingen voor het netwerkprofiel op.
 - Primaire DNS
 - Secundaire DNS
 - DNS-achtervoegsel
 - Gewenste WINS
 - Alternatieve WINS

Voor een bestaand netwerk kunt u de DNS- of WINS-instellingen niet wijzigen.

- 8 Klik op het tabblad **IP-bereiken**.
 - a Geef de beginwaarde van het IP-adresbereik op in het tekstvak **Begin IP-bereik**.
 - b Geef de eindwaarde van het IP-adresbereik op in het tekstvak **Eind IP-bereik**.
- 9 Als u de blueprint wilt opslaan als concept of verder wilt gaan met het configureren van de blueprint, klikt u op **Opslaan** of **Voltooien**.

NAT-regels maken en gebruiken voor NSX for vSphere

U kunt NAT-regels aan een een-op-veel NAT-netwerkonderdeel in een blueprint toevoegen wanneer het NAT-netwerkonderdeel is gekoppeld aan een niet-geclusterd vSphere-machineonderdeel of een NSX for vSphere-load balanceronderdeel op aanvraag.

U kunt NAT-regels definiëren voor elk door NSX for vSphere ondersteund protocol. U kunt een poort of een bereik van poorten van het externe IP-adres van een Edge toewijzen aan een privé IP-adres in het NAT-netwerkonderdeel.

■ vSphere-machineonderdeel

U kunt NAT-regels maken voor een NAT een-op-veel netwerkonderdeel dat aan een niet-geclusterd vSphere-machineonderdeel is gekoppeld.

Als bijvoorbeeld twee machines aan een NAT een-op-veel netwerkonderdeel op de blueprint zijn gekoppeld, kunt u een NAT-regel definiëren waarop poort 443 op het externe IP-adres verbinding kan maken met de machines via poort 80 in het NAT-netwerk en het TCP-protocol.

■ NSX for vSphere-load balanceronderdeel

U kunt NAT-regels maken voor een NAT een-op-veel netwerkonderdeel dat aan het VIP-netwerk van een NSX for vSphere-load balanceronderdeel is gekoppeld.

Als het NAT-netwerkonderdeel bijvoorbeeld is gekoppeld aan een load balanceronderdeel dat als load balancer voor drie machines fungeert, kunt u een NAT-regel definiëren waarop poort 90 op het externe IP-adres verbinding kan maken met de load balancer-VIP via poort 80 in het NAT-netwerk en het UDP-protocol.

U kunt een willekeurig aantal NAT-regels maken en de volgorde bepalen waarin de regels worden verwerkt.

De volgende elementen worden niet ondersteund voor NAT-regels:

- NIC's die zich niet in het huidige netwerk bevinden
- NIC's die worden geconfigureerd om IP-adressen op te halen via DHCP
- Machineclusters

Als u NAT-regels wilt toevoegen aan een NAT-netwerkonderdeel in een blueprint, zie [Het onderdeel NAT-netwerk op aanvraag of Geleid netwerk op aanvraag toevoegen in vRealize Automation](#).

Zie openbare artikelen zoals deze [blogpost van het vmwarelab](#) voor gerelateerde informatie over het gebruik van NAT-regels.

Het onderdeel NAT-netwerk op aanvraag of Geleid netwerk op aanvraag toevoegen in vRealize Automation

U kunt het onderdeel NSX for vSphere NAT-netwerk op aanvraag of het onderdeel NSX for vSphere geleid netwerk op aanvraag aan het ontwerpcanvas toevoegen als voorbereiding op het koppelen van de bijbehorende instellingen aan een of meer vSphere-machineonderdelen in de vRealize Automation-blueprint.

Wanneer u een onderdeel van een bestaand netwerk of een netwerk op aanvraag koppelt aan een machineonderdeel, wordt de NIC-informatie opgeslagen bij het machineonderdeel. De opgegeven netwerkprofielgegevens worden opgeslagen in het netwerkonderdeel.

U kunt meerdere netwerk- en beveiligingsonderdelen toevoegen aan het ontwerpcanvas.

U kunt meer dan één netwerkonderdeel op aanvraag hebben in één blueprint. Alle netwerkprofielen op aanvraag echter die worden gebruikt in de blueprint, moeten verwijzen naar hetzelfde externe netwerkprofiel.

Voor vSphere-machineonderdelen met gekoppelde NSX gebruikt u de netwerk-, beveiligings- en load balancing-instellingen in de gebruikersinterface. Voor machineonderdelen zonder tabblad **Netwerk** of **Beveiliging** kunt u netwerk- en beveiligingseigenschappen, zoals `VirtualMachine.Network0.Name`, toevoegen aan het tabblad **Eigenschappen** in het ontwerpcanvas. Netwerk-, beveiligings- en load balancer-eigenschappen voor NSX zijn uitsluitend van toepassing op vSphere-machines.

Alleen de netwerkprofielen die van toepassing zijn op de huidige tenant worden beschikbaar gesteld bij het ontwerpen van een blueprint. Met name worden netwerkprofielen beschikbaar gesteld als er ten minste één reservering in de huidige tenant is waarbij ten minste één netwerk is toegewezen aan het profiel.

Voorwaarden

- Netwerkinstellingen maken en configureren voor NSX for vSphere. Raadpleeg *vRealize Automation configureren* en *NSX Administration Guide* in de productdocumentatie van [NSX for vSphere](#).
- Controleer of de NSX-inventaris met succes is uitgevoerd voor uw cluster.
Als u NSX-configuraties in vRealize Automation wilt gebruiken, moet u gegevensverzameling uitvoeren.
- Maak een extern netwerkprofiel op aanvraag. Zie [Een netwerkprofiel maken in vRealize Automation](#).
Een voorbeeld: als u een NAT-netwerkonderdeel op aanvraag toevoegt, verwijzen wij u naar [Een NAT-netwerkprofiel maken voor een netwerk op aanvraag](#).
- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Open een nieuwe of bestaande blueprint in het ontwerpcanvas met behulp van het tabblad **Ontwerpen**.
- Als u NAT-regels wilt opgeven voor een NAT-netwerkonderdeel, moet u een één-op-veel NAT-netwerkprofiel gebruiken. Zie [Een NAT-netwerkprofiel maken met het meegeleverde IPAM-endpoint](#) of [Een NAT-netwerkprofiel maken met een extern IPAM-endpoint in vRealize Automation](#). Voor informatie over NAT-regels verwijzen wij u naar [NAT-regels maken en gebruiken voor NSX for vSphere](#).

Procedure

- 1 Als u de lijst met beschikbare netwerk- en beveiligingsonderdelen wilt weergeven, klikt u op **Netwerk en beveiliging** in de sectie Categorieën.
- 2 Sleep een NAT-netwerk op aanvraag-onderdeel of een geleid netwerkonderdeel op aanvraag naar het ontwerpcanvas.
- 3 Als u het onderdeel een uniek label wilt geven in het ontwerpcanvas, voert u in het tekstvak **ID** een onderdeelnaam in.
- 4 Selecteer het gewenste netwerkprofiel in het vervolgkeuzemenu **Bovenliggend netwerkprofiel**. Een voorbeeld: als u een NAT-netwerkonderdeel wilt toevoegen, selecteert u een NAT-netwerkprofiel dat is geconfigureerd om ondersteuning te bieden voor uw beoogde netwerkinstellingen.

Als u NAT-regels wilt opgeven in een NAT-netwerkonderdeel, moet u een profiel voor een bovenliggend netwerk gebruiken dat is geconfigureerd voor een één-op-veel NAT-netwerkprofiel.

Afhankelijk van het profieltype dat u selecteert, zijn op basis van uw netwerkprofielselectie de volgende netwerkinstellingen ingevuld. U kunt deze waarden wijzigen in het betreffende netwerkprofiel:

- Naam extern netwerkprofiel

- NAT-type (NAT op aanvraag)
- Subnetmasker
- Bereik subnetmasker (Geleid op aanvraag)
- Bereik subnetmasker (Geleid op aanvraag)
- Basis IP-adres (Geleid op aanvraag)

5 (Optioneel) Typ een beschrijving van het onderdeel in het tekstvak **Beschrijving**.

6 (Optioneel) Klik op het tabblad **DNS/WINS**.

7 (Optioneel) Geef de DNS- en WINS-instellingen voor het netwerkprofiel op.

- Primaire DNS
- Secundaire DNS
- DNS-achtervoegsel
- Gewenste WINS
- Alternatieve WINS

Voor een bestaand netwerk kunt u de DNS- of WINS-instellingen niet wijzigen.

8 Klik op het tabblad **IP-bereiken**.

U ziet het IP-bereik of de IP-bereiken voor het netwerkprofiel. U kunt de sorteervolgorde of kolomweergave wijzigen. Voor NAT-netwerken kunt u ook de waarden van het IP-bereik wijzigen.

- a Geef de beginwaarde van het IP-adresbereik op in het tekstvak **Begin IP-bereik**.
- b Geef de beginwaarde van het IP-adresbereik op in het tekstvak **Begin IP-bereik**.

9 Als u een NAT-netwerk gebruikt dat is gebaseerd op een één-op-veel NAT-netwerkprofiel dat gebruikmaakt van statische IP-bereiken, kunt u op het tabblad **NAT-regels** regels toevoegen waarmee een extern IP-adres toegang kan krijgen tot onderdelen in het interne NAT-netwerk.

Voor een NAT een-op-veel-netwerk kunt u NAT-regels definiëren die kunnen worden geconfigureerd wanneer u een NAT-netwerkonderdeel aan de blueprint toevoegt. U kunt een NAT-regel wijzigen wanneer u het NAT-netwerk in een implementatie bewerkt.

De opties die beschikbaar zijn om te selecteren zijn gebaseerd op de vSphere-machine of onderdelen van de load balancer van NSX for vSphere die u met het NAT-netwerkonderdeel hebt geassocieerd.

- **Naam:** voer een unieke regelnaam in.
- **Onderdeel:** maak een selectie in een lijst met geassocieerde onderdelen voor de vSphere-machine of de load balancer waaraan het NAT-netwerk is gekoppeld.

NAT-regels worden alleen ondersteund voor niet-geclusterde machines. Als u een clustergrootte van meer dan 1 hebt opgegeven, worden geen onderdelen weergegeven omdat de configuratie niet wordt ondersteund.

- **Bronpoort:** selecteer de optie Willekeurig, voer een geldige poort of een geldig poortbereik in, of geef een geldige eigenschapbinding op.
- **Doelpoort:** selecteer de optie Willekeurig, voer een geldige poort of een geldig poortbereik in, of geef een geldige eigenschapbinding op.
- **Protocol:** voer een geldig door NSX for vSphere ondersteund protocol in of selecteer de optie TCP, UDP of Willekeurig.
- **Beschrijving:** voer een korte beschrijving van de NAT-regel in.

10 Als u de blueprint wilt opslaan als concept of verder wilt gaan met het configureren van de blueprint, klikt u op **Opslaan** of **Voltooien**.

Wat nu te doen

U kunt netwerkinstellingen toevoegen op het tabblad **Netwerk** van een vSphere-machineonderdeel.

NSX-T-netwerkonderdelen gebruiken in een blueprint

U kunt een of meer NSX-T-netwerkonderdelen aan het ontwerpcanvas toevoegen en de bijbehorende instellingen voor vSphere-machineonderdelen in de blueprint configureren.

De instellingen voor netwerk- en beveiligingsonderdelen die u aan de blueprint toevoegt, worden afgeleid van uw NSX-T-configuratie. Raadpleeg de *NSX-T Administration Guide* in de [NSX-T-productdocumentatie](#) voor informatie over het configureren van NSX-T.

Wanneer u een blueprint implementeert die een NSX-T-endpoint bevat, wijst de implementatie een tag toe aan NSX-T-onderdelen in de implementatie. De naam van de tag en de naam van de implementatie komen overeen.

Zie [Informatie over de NSX-T-implementatietopologieën voor netwerken, beveiliging en load balancer-configuraties](#) voor meer informatie over NSX-T-specifieke overwegingen met betrekking tot implementatie en topologie.

Een bestaand netwerkonderdeel toevoegen voor NSX-T

U kunt een bestaand NSX-T-netwerkonderdeel toevoegen aan het ontwerpcanvas om de instellingen hiervan te koppelen aan een of meer vSphere-machineonderdelen van de blueprint.

U kunt een bestaand netwerk als onderdeel gebruiken om een NSX-T-netwerk toe te voegen aan het ontwerpcanvas en de instellingen ervan te configureren voor gebruik met vSphere-machineonderdelen en Software- of XaaS-onderdelen die van toepassing zijn op vSphere.

Wanneer u een onderdeel van een bestaand netwerk of een netwerk op aanvraag koppelt aan een machineonderdeel, wordt de NIC-informatie opgeslagen bij het machineonderdeel. De opgegeven netwerkprofielgegevens worden opgeslagen in het netwerkonderdeel.

U kunt meerdere netwerk- en beveiligingsonderdelen toevoegen aan het ontwerpcanvas.

Voor vSphere-machineonderdelen met gekoppelde NSX gebruikt u de netwerk-, beveiligings- en load balancing-instellingen in de gebruikersinterface. Voor machineonderdelen zonder tabblad **Netwerk** of **Beveiliging** kunt u netwerk- en beveiligingseigenschappen, zoals `VirtualMachine.Network0.Name`, toevoegen aan het tabblad **Eigenschappen** in het ontwerpcanvas. Netwerk-, beveiligings- en load balancer-eigenschappen voor NSX zijn uitsluitend van toepassing op vSphere-machines.

Alleen de netwerkprofielen die van toepassing zijn op de huidige tenant worden beschikbaar gesteld bij het ontwerpen van een blueprint. Met name worden netwerkprofielen beschikbaar gesteld als er ten minste één reservering in de huidige tenant is waarbij ten minste één netwerk is toegewezen aan het profiel.

Voorwaarden

- Netwerkinstellingen maken en configureren voor NSX-T. Raadpleeg *vRealize Automation configureren* en *NSX-T Administration Guide* in de [NSX-T-productdocumentatie](#).
- Controleer of de NSX-inventaris met succes is uitgevoerd voor uw cluster.
Als u NSX-configuraties in vRealize Automation wilt gebruiken, moet u gegevensverzameling uitvoeren.
- Maak een netwerkprofiel.
- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Open een nieuwe of bestaande blueprint in het ontwerpcanvas met behulp van het tabblad **Ontwerpen**.

Procedure

- 1 Als u de lijst met beschikbare netwerk- en beveiligingsonderdelen wilt weergeven, klikt u op **Netwerk en beveiliging** in de sectie Categorieën.
- 2 Sleep een **Bestaand netwerk**-onderdeel naar het ontwerpcanvas.
- 3 Klik in het tekstvak **Bestaand netwerk** en selecteer een bestaand netwerkprofiel.
De waarden voor de beschrijving, het subnetmasker en de gateway worden ingevuld op basis van het geselecteerde netwerkprofiel.
- 4 (Optioneel) Klik op het tabblad **DNS/WINS**.
- 5 (Optioneel) Geef de DNS- en WINS-instellingen voor het netwerkprofiel op.
 - Primaire DNS
 - Secundaire DNS
 - DNS-achtervoegsel
 - Gewenste WINS
 - Alternatieve WINS

Voor een bestaand netwerk kunt u de DNS- of WINS-instellingen niet wijzigen.

6 (Optioneel) Klik op het tabblad **IP-bereiken**.

U ziet het IP-bereik of de IP-bereiken voor het netwerkprofiel. U kunt de sorteervolgorde of kolomweergave wijzigen. Voor NAT-netwerken kunt u ook de waarden van het IP-bereik wijzigen.

7 Als u de blueprint wilt opslaan als concept of verder wilt gaan met het configureren van de blueprint, klikt u op **Opslaan** of **Voltooien**.

Wat nu te doen

U kunt netwerkinstellingen toevoegen op het tabblad **Netwerk** van een vSphere-machineonderdeel.

NAT-regels maken en gebruiken voor NSX-T

U kunt NAT-regels aan een een-op-veel NAT-netwerkonderdeel in een blueprint toevoegen wanneer het NAT-netwerkonderdeel is gekoppeld aan een niet-geclusterd vSphere-machineonderdeel.

U kunt NAT-regels definiëren voor elk door NSX-T ondersteund protocol. U kunt een poort of een bereik van poorten van het externe IP-adres van een Edge toewijzen aan een privé IP-adres in het NAT-netwerkonderdeel.

U kunt NAT-regels maken voor een NAT een-op-veel netwerkonderdeel dat aan een niet-geclusterd vSphere-machineonderdeel is gekoppeld. Als bijvoorbeeld twee machines aan een NAT een-op-veel netwerkonderdeel op de blueprint zijn gekoppeld, kunt u een NAT-regel definiëren waarop poort 443 op het externe IP-adres verbinding kan maken met de machines via poort 80 in het NAT-netwerk en het TCP-protocol.

NAT-regels worden niet ondersteund voor NSX-T load balancers of voor NSX-T versie 2.2.

U kunt een willekeurig aantal NAT-regels maken en de volgorde bepalen waarin de regels worden verwerkt.

De volgende elementen worden niet ondersteund voor NAT-regels:

- NIC's die zich niet in het huidige netwerk bevinden
- NIC's die worden geconfigureerd om IP-adressen op te halen via DHCP
- Machineclusters

Als u NAT-regels wilt toevoegen aan een NAT-netwerkonderdeel in een blueprint, zie [Een NSX-T NAT-netwerk op aanvraag-onderdeel of NSX-T geleid netwerkonderdeel op aanvraag toevoegen](#).

Een NSX-T NAT-netwerk op aanvraag-onderdeel of NSX-T geleid netwerkonderdeel op aanvraag toevoegen

U kunt een NSX-T NAT-netwerkonderdeel of NSX-Tgeleid netwerk op aanvraag als onderdeel toevoegen aan het ontwerpcanvas als u de bijbehorende instellingen wilt koppelen aan een of meer vSphere-machineonderdelen op de blueprint.

Wanneer u een onderdeel van een bestaand netwerk of een netwerk op aanvraag koppelt aan een machineonderdeel, wordt de NIC-informatie opgeslagen bij het machineonderdeel. De opgegeven netwerkprofielgegevens worden opgeslagen in het netwerkonderdeel.

U kunt meerdere netwerk- en beveiligingsonderdelen toevoegen aan het ontwerpcanvas.

U kunt meer dan één netwerkonderdeel op aanvraag hebben in één blueprint. Alle netwerkprofielen op aanvraag echter die worden gebruikt in de blueprint, moeten verwijzen naar hetzelfde externe netwerkprofiel.

Voor NSX-T mogen de netwerkbereiken die door de verschillende netwerken in uw blueprint worden gebruikt elkaar niet overlappen. Deze beperking treedt op wanneer u NSX-T Tier-1-routernetwerken configureert.

Voor vSphere-machineonderdelen met gekoppelde NSX gebruikt u de netwerk-, beveiligings- en load balancing-instellingen in de gebruikersinterface. Voor machineonderdelen zonder tabblad **Netwerk** of **Beveiliging** kunt u netwerk- en beveiligingseigenschappen, zoals `VirtualMachine.Network0.Name`, toevoegen aan het tabblad **Eigenschappen** in het ontwerpcanvas. Netwerk-, beveiligings- en load balancer-eigenschappen voor NSX zijn uitsluitend van toepassing op vSphere-machines.

Alleen de netwerkprofielen die van toepassing zijn op de huidige tenant worden beschikbaar gesteld bij het ontwerpen van een blueprint. Met name worden netwerkprofielen beschikbaar gesteld als er ten minste één reservering in de huidige tenant is waarbij ten minste één netwerk is toegewezen aan het profiel.

Voorwaarden

- Netwerkinstellingen maken en configureren voor NSX for vSphere. Raadpleeg *vRealize Automation configureren* en *NSX for vSphere Administration Guide* in de [NSX-T-productdocumentatie](#).

- Controleer of de NSX-inventaris met succes is uitgevoerd voor uw cluster.

Als u NSX-configuraties in vRealize Automation wilt gebruiken, moet u gegevensverzameling uitvoeren.

- Maak een extern netwerkprofiel op aanvraag. Zie [Een netwerkprofiel maken in vRealize Automation](#).

Een voorbeeld: als u een NAT-netwerkonderdeel op aanvraag toevoegt, verwijzen wij u naar [Een NAT-netwerkprofiel maken voor een netwerk op aanvraag](#).

- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Open een nieuwe of bestaande blueprint in het ontwerpcanvas met behulp van het tabblad **Ontwerpen**.

- Als u NAT-regels wilt opgeven voor een NAT-netwerkonderdeel, moet u een één-op-veel NAT-netwerkprofiel gebruiken. Zie [Een NAT-netwerkprofiel maken met het meegeleverde IPAM-endpoint](#) of [Een NAT-netwerkprofiel maken met een extern IPAM-endpoint in vRealize Automation](#). Voor informatie over NAT-regels verwijzen wij u naar [NAT-regels maken en gebruiken voor NSX for vSphere](#).

Procedure

- 1 Als u de lijst met beschikbare netwerk- en beveiligingsonderdelen wilt weergeven, klikt u op **Netwerk en beveiliging** in de sectie Categorieën.
- 2 Sleep een NSX-T NAT-netwerk op aanvraag-onderdeel of NSX-T geleid netwerkonderdeel op aanvraag naar het ontwerpcanvas.
- 3 Als u het onderdeel een uniek label wilt geven in het ontwerpcanvas, voert u in het tekstvak **ID** een onderdeelnaam in.
- 4 Selecteer het gewenste netwerkprofiel in het vervolgkeuzemenu **Bovenliggend netwerkprofiel**. Een voorbeeld: als u een NAT-netwerkonderdeel wilt toevoegen, selecteert u een NAT-netwerkprofiel dat is geconfigureerd om ondersteuning te bieden voor uw beoogde netwerkinstellingen.

Als u NAT-regels wilt opgeven in een NAT-netwerkonderdeel, moet u een profiel voor een bovenliggend netwerk gebruiken dat is geconfigureerd voor een één-op-veel NAT-netwerkprofiel.

Afhankelijk van het profieltype dat u selecteert, zijn op basis van uw netwerkprofielselectie de volgende netwerkinstellingen ingevuld. U kunt deze waarden wijzigen in het betreffende netwerkprofiel:

- Naam extern netwerkprofiel
 - NAT-type (NSX-T NAT op aanvraag)
 - Subnetmasker
 - Bereik subnetmasker (NSX-T geleid op aanvraag)
 - Bereik subnetmasker (NSX-T geleid op aanvraag)
 - Basis IP-adres (NSX-T geleid op aanvraag)
- 5 (Optioneel) Typ een beschrijving van het onderdeel in het tekstvak **Beschrijving**.
 - 6 (Optioneel) Klik op het tabblad **DNS/WINS**.
 - 7 (Optioneel) Geef de DNS- en WINS-instellingen voor het netwerkprofiel op.
 - Primaire DNS
 - Secundaire DNS
 - DNS-achtervoegsel
 - Gewenste WINS

- Alternatieve WINS

Voor een bestaand netwerk kunt u de DNS- of WINS-instellingen niet wijzigen.

8 Klik op het tabblad **IP-bereiken**.

U ziet het IP-bereik of de IP-bereiken voor het netwerkprofiel. U kunt de sorteervolgorde of kolomweergave wijzigen. Voor NAT-netwerken kunt u ook de waarden van het IP-bereik wijzigen.

- a Geef de beginwaarde van het IP-adresbereik op in het tekstvak **Begin IP-bereik**.
- b Geef de beginwaarde van het IP-adresbereik op in het tekstvak **Begin IP-bereik**.

9 Als u een NAT-netwerk gebruikt dat is gebaseerd op een één-op-veel NAT-netwerkprofiel dat gebruikmaakt van statische IP-bereiken, kunt u op het tabblad **NAT-regels** regels toevoegen waarmee een extern IP-adres toegang kan krijgen tot onderdelen in het interne NAT-netwerk.

Voor een NAT een-op-veel-netwerk kunt u NAT-regels definiëren die kunnen worden geconfigureerd wanneer u een NAT-netwerkonderdeel aan de blueprint toevoegt. U kunt een NAT-regel wijzigen wanneer u het NAT-netwerk in een implementatie bewerkt.

De opties die beschikbaar zijn om te selecteren zijn gebaseerd op de vSphere-machineonderdelen die u met het NAT-netwerkonderdeel hebt geassocieerd.

- **Naam:** voer een unieke regelnaam in.
- **Onderdeel:** maak een selectie in een lijst met geassocieerde onderdelen voor de vSphere-machine of de load balancer waaraan het NAT-netwerk is gekoppeld.

NAT-regels worden alleen ondersteund voor niet-geclusterde machines. Als u de grootte van een cluster van meer dan 1 hebt opgegeven, worden geen componenten weergegeven als de configuratie niet wordt ondersteund.
- **Bronpoort:** selecteer de optie Willekeurig, voer een geldige poort of een geldig poortbereik in, of geef een geldige eigenschapbinding op.
- **Doelpoort:** selecteer de optie Willekeurig, voer een geldige poort of een geldig poortbereik in, of geef een geldige eigenschapbinding op.
- **Protocol:** voer een geldig door NSX-T ondersteund protocol in of selecteer de optie TCP, UDP of Willekeurig.
- **Beschrijving:** voer een korte beschrijving in van datgene waarvoor de NAT-regel is ontworpen.

10 Als u de blueprint wilt opslaan als concept of verder wilt gaan met het configureren van de blueprint, klikt u op **Opslaan** of **Voltooien**.

Wat nu te doen

U kunt netwerkinstellingen toevoegen op het tabblad **Netwerk** van een vSphere-machineonderdeel.

NSX for vSphere load balancer-onderdelen gebruiken in een blueprint

U kunt een of meer NSX for vSphere load balancer-onderdelen op aanvraag aan het ontwerpcanvas toevoegen om instellingen van vSphere-machineonderdelen in de blueprint te configureren.

De instellingen voor netwerk- en beveiligingsonderdelen die u aan de blueprint toevoegt, worden afgeleid van uw configuratie van NSX for vSphere en NSX-T. Raadpleeg de *Administration Guide* in de [NSX for vSphere-productdocumentatie](#) of [NSX-T-productdocumentatie](#), afhankelijk van welke toepassing u gebruikt, voor informatie over het configureren van NSX.

De volgende regels zijn van toepassing op load balancer-pools en VIP-netwerkinstellingen in de blueprint.

- Als het netwerkprofiel van de pool NAT is, kan het VIP-netwerkprofiel deel uitmaken van het NAT-netwerkprofiel.
- Als het netwerkprofiel van de pool geleid is, kan het VIP-netwerkprofiel zich alleen op hetzelfde geleide netwerk bevinden.
- Als het netwerkprofiel van de pool extern is, kan het VIP-netwerkprofiel alleen hetzelfde externe netwerkprofiel zijn.

Elke component van de load balancer kan meerdere virtuele servers hebben, die tevens kunnen worden aangeduid als load balancer services. Elke virtuele server in het load balancer-onderdeel heeft één poort en één protocol. U kunt bijvoorbeeld load balancing uitvoeren voor een HTTP-service of HTTPS-service. Een load balancer kan load balancing uitvoeren voor meerdere services.

De NSX Edge is het netwerkkapparaat dat de virtuele servers van de load balancer bevat. Hoewel u meer dan één load balancer-onderdeel in een blueprint kunt hebben, bevinden de virtuele servers die in elk load balancer-onderdeel zijn gedefinieerd, zich in één NSX Edge wanneer u de implementatie inricht.

Als een blueprint een load balancer bevat en app-isolatie is ingeschakeld, worden de load balancer-VIP's aan de app-isolatiebeveiligingsgroep toegevoegd als IPSet. Als een blueprint een beveiligingsgroep op aanvraag bevat die is gekoppeld aan een machinelaag die ook is gekoppeld aan een load balancer, bevat de beveiligingsgroep op aanvraag de machinelaag IPSet en VIP's.

U kunt de instellingen van de load balancer opnieuw configureren in een bestaande implementatie om virtuele servers toe te voegen, te bewerken of te verwijderen.

Overwegingen bij het werken met geüpgradede of gemigreerde load balancer-onderdelen
De volgende overwegingen zijn belangrijk om te begrijpen en naar te handelen met betrekking tot NSX-load balancer-onderdelen in de doelversie van vRealize Automation.

Deze informatie geldt voor NSX for vSphere-load balancer-onderdelen die zijn geüpgradede of gemigreerd naar deze versie van vRealize Automation.

- U moet de verzameling inventarisgegevens van NSX-netwerk en -beveiliging uitvoeren voor en na het upgraden of migreren naar deze versie om problemen te voorkomen wanneer u de actie Load balancer opnieuw configureren uitvoert. Dit heeft geen invloed op de actie Load balancer opnieuw configureren voor nieuwe implementaties.

Voor meer informatie raadpleegt u *Upgraden van vRealize Automation 7.1 en hoger en vRealize Automation migreren*.

- U kunt een load balancer opnieuw configureren. Het vereiste catalogusrecht is Opnieuw configureren (load balancer).
- Voor implementaties die zijn geüpgraded of gemigreerd van vRealize Automation 7.x naar deze versie van vRealize Automation is het opnieuw configureren van de load balancer beperkt tot implementaties die één load balancer bevatten.
- De optie Load balancer opnieuw configureren wordt niet ondersteund voor implementaties die zijn geüpgraded of gemigreerd van vRealize Automation 6.2.x naar deze versie van vRealize Automation.

Het onderdeel load balancer op aanvraag toevoegen

U kunt een NSX-load balancer-onderdeel op aanvraag naar het ontwerpcanvas slepen en de bijbehorende instellingen configureren voor gebruik met vSphere-machineonderdelen en containeronderdelen in de blueprint.

Raadpleeg de *NSX-beheerhandleiding* in de [NSX for vSphere-productdocumentatie](#) voor gerelateerde informatie over het maken van NSX for vSphere-toepassingsprofielen om het gedrag van een specifiek type netwerkverkeer te definiëren.

Procedure

1 [Instellingen voor leden van load balancers definiëren](#)

U kunt een NSX-load balancer-onderdeel op aanvraag definiëren om de taakverwerking te verdelen over ingerichte vSphere-lidmachines of containermachines in een netwerk.

2 [Algemene instellingen voor virtuele server definiëren](#)

U kunt een protocol en poort voor één virtuele server definiëren voor uw load balancer of u kunt extra virtuele servers toevoegen om extra opties voor NSX load balancers aan te passen.

3 [Distributie-instellingen voor virtuele server definiëren](#)

Door de optie **Aanpassen** op het tabblad **Algemeen** te selecteren, kunt u informatie opgeven over de poolleden, zoals de poort waarop de leden verkeer ontvangen, het protocoltype dat de load balancer van NSX kan gebruiken om toegang te krijgen tot die poort, het algoritme dat wordt gebruikt voor load balancing en de persistentie-instellingen.

4 [Instellingen voor de statuscontrole van de virtuele server definiëren](#)

Door de optie **Aanpassen** te selecteren op het tabblad **Algemeen**, geeft u op hoe en of de load balancer van NSX statuscontroles moet uitvoeren op poolleden binnen de virtuele server.

5 Geavanceerde instellingen voor virtuele server definiëren

Door de optie **Aanpassen** te selecteren op het tabblad **Algemeen** kunt u het load balancer-onderdeel van NSX aanpassen om instellingen op te geven, zoals het aantal gelijktijdige verbindingen dat één poolid kan herkennen en het maximum aantal gelijktijdige verbindingen dat de virtuele server kan verwerken.

6 Logboekopties voor load balancers definiëren

U kunt de typen logboekacties voor load balancers definiëren die worden vastgelegd en geregistreerd in de logboeken voor load balancers.

Instellingen voor leden van load balancers definiëren

U kunt een NSX-load balancer-onderdeel op aanvraag definiëren om de taakverwerking te verdelen over ingerichte vSphere-lidmachines of containermachines in een netwerk.

Wanneer u een load balancer-onderdeel toevoegt aan een blueprint in het ontwerpcanvas, kunt u een standaard- of aangepaste optie kiezen wanneer u de definities voor uw virtuele server maakt of bewerkt in het load balancer-onderdeel. Met de standaardoptie kunt u het protocol, de poort en een beschrijving opgeven voor de virtuele server en standaardwaarden gebruiken voor alle andere instellingen. Met de aangepaste optie kunt u extra detailniveaus definiëren.

Als de load balancer is ingericht met een extern netwerk, moeten het VIP (VIP-netwerk) en de ledenpool (het ledennetwerk) zich op hetzelfde bestaande netwerk bevinden. De inrichting zal mislukken als het VIP en de ledenpool zich niet in hetzelfde externe netwerk bevinden.

Voorwaarden

- Load balancer-instellingen maken en configureren voor NSX. Zie *vRealize Automation configureren* en *NSX Administration Guide*.
- Controleer of de NSX-inventaris met succes is uitgevoerd voor uw cluster.
Als u NSX-configuraties in vRealize Automation wilt gebruiken, moet u gegevensverzameling uitvoeren.
- Maak een netwerkprofiel.
- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Open een nieuwe of bestaande blueprint in het ontwerpcanvas met behulp van het tabblad **Ontwerpen**.
- Controleer dat ten minste één vSphere-machineonderdeel of -containeronderdeel bestaat in de blueprint.

Procedure

- 1 Als u de lijst met beschikbare netwerk- en beveiligingsonderdelen wilt weergeven, klikt u op **Netwerk en beveiliging** in de sectie Categorieën.
- 2 Sleep een **Load Balancer op aanvraag**-onderdeel naar het ontwerpcanvas.

- 3 Als u het onderdeel een uniek label wilt geven in het ontwerpcanvas, voert u in het tekstvak **ID** een onderdeelnaam in.

- 4 Selecteer de naam van een vSphere-machineonderdeel of -containeronderdeel in het vervolgkeuzemenu **Lid**.

De lijst bevat alleen de vSphere-machineonderdelen en -containeronderdelen in de actieve blueprint.

- 5 Selecteer de NIC voor de load balancing in de vervolgkeuzelijst **Ledennetwerk**.

De lijst bevat NIC's die zijn gedefinieerd voor het geselecteerde vSphere-machinelid.

- 6 Selecteer een beschikbaar virtueel IP-adresnetwerk in de vervolgkeuzelijst **VIP-netwerk**. Selecteer bijvoorbeeld een beschikbaar extern of NAT-netwerk.

U kunt meerdere NSX load balancers en NSX-netwerkonderdelen op aanvraag in een blueprint hebben, maar ze moeten allemaal zijn gekoppeld aan hetzelfde VIP-netwerk.

- 7 (Optioneel) Typ een geldig IP-adres voor de NIC in het tekstvak **IP-adres**.

De standaardinstelling is het statische IP-adres dat is gekoppeld aan het VIP-netwerk. U kunt een ander IP-adres of een IP-adresbereik opgeven. Standaard wordt het eerstvolgende beschikbare IP-adres uit het geassocieerde VIP-netwerk toegewezen.

Laat het veld IP-adres leeg als u tijdens de inrichting het IP-adres wilt laten toewijzen vanuit het gekoppelde VIP-netwerk.

Als u een IP-adres van een ander type netwerk opgeeft, kan slechts één implementatie worden ingericht. Bij volgende implementaties zal de IP-toewijzing mislukken omdat het IP-adres al door de eerste implementatie wordt gebruikt.

- 8 Als u een definitie voor een virtuele server wilt maken, klikt u op **Nieuw** en raadpleegt u [Algemene instellingen voor virtuele server definiëren](#).

Elk load balancer-onderdeel vereist ten minste één virtuele server.

Zie [Logboekopties voor load balancers definiëren](#) als u logboekopties wilt opgeven.

Algemene instellingen voor virtuele server definiëren

U kunt een protocol en poort voor één virtuele server definiëren voor uw load balancer of u kunt extra virtuele servers toevoegen om extra opties voor NSX load balancers aan te passen.

Bijvoorbeeld: u kunt het load balancer-onderdeel aanpassen om instellingen als statuscontroleprotocol en -poort, algoritme, persistentie en transparantie te definiëren.

Voorwaarden

[Instellingen voor leden van load balancers definiëren](#).

Procedure

- 1 Klik op het tabblad **Algemeen** op de pagina **Nieuwe virtuele server**.

- 2 Selecteer het netwerkverkeerprotocol in het vervolgkeuzemenu **Protocol** voor het verdelen van taken op de virtuele server.

De protocolopties zijn HTTP, HTTPS, TCP, en UDP.

- 3 Voer een poortwaarde in in het tekstvak **Poort**.

Het geselecteerde protocol bepaalt de standaardpoortinstelling.

Protocol	Standaardpoort
HTTP	80
HTTPS	443
TCP	8080
UDP	geen standaard

De HTTP-, HTTPS- en TCP-protocollen kunnen een poort delen met UDP. Bijvoorbeeld: als service 1 TCP, HTTP of HTTPS gebruikt op poort 80, kan service 2 UDP gebruiken op poort 80. Maar als service 1 UDP gebruikt op poort 80, kan service 2 niet UDP gebruiken op poort 80.

- 4 (Optioneel) Voer een beschrijving voor het virtuele-serveronderdeel in.
- 5 Selecteer een van de opties voor **Instellingen**.

- **Standaardinstellingen gebruiken voor alle overige waarden**

Accepteer alle overige standaardinstellingen. Klik op **OK** om de definitie van het load balancer-onderdeel te voltooien en door te gaan met uw werk in de blueprint.

U kunt de standaardinstellingen weergeven door te klikken op **Aanpassen** en de aanvullende opties op het tabblad te bekijken. Als de standaardinstellingen in orde zijn, klikt u op **Standaardwaarde gebruiken voor alle andere instellingen** op het tabblad **Algemeen**.

- **Aanpassen**

Configureer het load balancer-onderdeel met extra instellingen, bijvoorbeeld om een ander protocol te definiëren voor statuscontrole of een andere poort om het verkeer van een lid te controleren.

Er worden extra tabbladen weergegeven waarop u aangepaste instellingen kunt toevoegen.

Als u **Standaardinstellingen gebruiken voor alle overige waarden** hebt geselecteerd en op **OK** hebt geklikt, bent u klaar en kunt u doorgaan met het definiëren of bewerken van uw blueprint in het ontwerpcanvas. Als u **Aanpassen** hebt geselecteerd, gaat u door met de stap.

- 6 Klik op het tabblad **Distributie** en ga naar het onderwerp [Distributie-instellingen voor virtuele server definiëren](#) om door te gaan met het definiëren van de virtuele server in het load balancer-onderdeel van NSX.

Distributie-instellingen voor virtuele server definiëren

Door de optie **Aanpassen** op het tabblad **Algemeen** te selecteren, kunt u informatie opgeven over de poolleden, zoals de poort waarop de leden verkeer ontvangen, het protocoltype dat de load balancer van NSX kan gebruiken om toegang te krijgen tot die poort, het algoritme dat wordt gebruikt voor load balancing en de persistentie-instellingen.

Een pool vertegenwoordigt een cluster met machines waarover de taken worden verdeeld. Een poolid vertegenwoordigt één machine in dat cluster.

De standaardinstellingen voor het lidprotocol en de lidpoort komen overeen met de instellingen voor het protocol en de poort op de pagina **Algemeen**.

De pool met machines die lid zijn, wordt weergegeven in de waarde voor de optie **Lid** in de gebruikersinterface van het load balancer-onderdeel in de blueprint. De vermelding bij **Lid** wordt ingesteld op de pool of het cluster met machines.

Voorwaarden

[Algemene instellingen voor virtuele server definiëren.](#)

Procedure

- 1 (Optioneel) De instelling **Lidprotocol** komt overeen met het protocol dat u hebt opgegeven op het tabblad **Algemeen**. Deze instelling definieert hoe het poolid netwerkverkeer ontvangt.
- 2 (Optioneel) Voer een poortnummer in in het tekstvak **Lidpoort** om de poort te bepalen waarop het poolid netwerkverkeer ontvangt.

Als de aanvraag voor het virtuele IP-adres (VIP) van de load balancer binnenkomt op poort 80, moet u de aanvraag mogelijk doorverwijzen naar een andere poort, bijvoorbeeld poort 8080, op de poolleden.

- 3 (Optioneel) Selecteer de verdelingsmethode op basis van een algoritme voor deze pool.

De algoritmeopties en de algoritmeparameters voor de opties die ze vereisen, worden beschreven in de volgende tabel.

Optie	Beschrijving en algoritmeparameters
ROUND_ROBIN	<p>Elke server wordt beurtelings gebruikt op basis van het gewicht dat eraan is toegewezen.</p> <p>Als de load balancer is gemaakt in vRealize Automation, is het gewicht voor alle leden hetzelfde.</p> <p>Dit is het vloeiendste en meest evenredige algoritme wanneer de verwerkingstijd van de server gelijk verdeeld blijft.</p> <p>Algoritmeparameters zijn gedeactiveerd voor deze optie.</p>
IP-HASH	<p>Selecteert een server op basis van een hash van het oorspronkelijke IP-adres en het totale gewicht van alle actieve servers.</p> <p>Algoritmeparameters zijn gedeactiveerd voor deze optie.</p>

Optie	Beschrijving en algoritmeparameters
LEASTCONN	<p>Distribueert clientaanvragen over meerdere servers op basis van het aantal verbindingen dat al aanwezig is op de server.</p> <p>Nieuwe verbindingen worden verzonden naar de server die de minste verbindingen heeft.</p> <p>Algoritmeparameters zijn gedeactiveerd voor deze optie.</p>
URI	<p>Het linkergedeelte van de URI (voor het vraagteken) wordt gehasht en gedeeld door het totale gewicht van de actieve servers.</p> <p>Het resultaat bepaalt welke server de aanvraag ontvangt. Dit zorgt ervoor dat een URI altijd wordt doorverwezen naar dezelfde server zolang er geen servers actief of inactief worden.</p> <p>De URI-algoritmeparameter heeft twee opties: <code>uriLength=<len></code> en <code>uriDepth=<dep></code>. Voer de lengte- en diepteparameters op afzonderlijke regels in in het tekstvak Algoritmeparameters.</p> <p>Lengte- en diepteparameters worden gevolgd door een positief geheel getal. Deze opties kunnen taken alleen over servers verdelen op basis van het begin van de URI.</p> <p>De lengteparameter geeft aan dat het algoritme alleen rekening moet houden met de gedefinieerde tekens aan het begin van de URI om de hash te berekenen. Het bereik voor de lengteparameter moet $1 \leq \text{len} < 256$ zijn.</p> <p>De diepteparameter geeft de maximumdirectorydiepte aan die moet worden gebruikt om de hash te berekenen. Voor elke slash in de aanvraag wordt één niveau geteld. Het bereik voor de diepteparameter moet $1 \leq \text{dep} < 10$ zijn.</p> <p>Als beide parameters zijn opgegeven, stopt de evaluatie wanneer een van de parameters is bereikt.</p>
HTTPHEADER	<p>De naam van de HTTP-header wordt opgezocht in elke HTTP-aanvraag.</p> <p>De naam van de header tussen haakjes is niet hoofdlettergevoelig, vergelijkbaar met de ACL-functie <code>'hdr()'</code>.</p> <p>De algoritmeparameter HTTPHEADER heeft één optie <code>headerName=<name></code>. Zo kunt u bijvoorbeeld host gebruiken als de algoritmeparameter HTTPHEADER.</p> <p>Als de header afwezig is of geen waarde bevat, wordt het roundrobin algoritme toegepast.</p>
URL	<p>De URL-parameter die is opgegeven in het argument, wordt opgezocht in de querytekenreeks van elke HTTP GET-aanvraag.</p> <p>De algoritmeparameter URL heeft één optie <code>urlParam=<url></code>.</p> <p>Als de parameter wordt gevolgd door een gelijkteken = en een waarde, wordt de waarde gehasht en gedeeld door het totale gewicht van de actieve servers. Het resultaat bepaalt welke server de aanvraag ontvangt. Dit proces wordt gebruikt om gebruikers-id's in aanvragen te volgen en om ervoor te zorgen dat eenzelfde gebruikers-id altijd naar dezelfde server wordt verzonden zolang er geen servers actief of inactief worden.</p> <p>Als geen waarde of parameter wordt gevonden, wordt het roundrobin algoritme toegepast.</p>

4 (Optioneel) Selecteer de persistentiemethode voor deze pool.

Persistentie volgt en bewaart sessiegegevens, zoals het specifieke poolid dat een clientaanvraag heeft behandeld. Met persistentie worden clientaanvragen doorverwezen naar hetzelfde poolid voor de levensduur van een sessie of tijdens opeenvolgende sessies.

Protocol	Persistentiemethode ondersteund
HTTP	Geen, Cookie, Bron-IP
HTTPS	Geen, Bron-IP en SSL-sessie-id
TCP	Geen, Bron-IP, MSRDP
UDP	Geen, Bron-IP

- Selecteer **Cookie** om een unieke cookie in te voegen om de sessie te identificeren de eerste keer dat een client toegang krijgt tot de site. Bij elke volgende aanvraag wordt de cookie gelezen om ervoor te zorgen dat verbinding wordt gemaakt met de geschikte server.
- Selecteer **Bron-IP** om sessies te volgen op basis van het oorspronkelijke IP-adres. Als een client een verbinding aanvraagt voor een virtuele server die affiniteitspersistentie van het bronadres ondersteunt, controleert de load balancer of die client eerder is verbonden. Als dat zo is, wordt de client naar hetzelfde groepsid geleid.
- Selecteer **SSL-sessie-id** en selecteer het HTTPS-verkeerspatroon SSL Passthrough.
 - SSL-passthrough - client -> HTTPS -> LB (SSL beëindigen) -> HTTPS -> server
 - Client: HTTP-> LB -> HTTP -> servers

Opmerking vRealize Automation ondersteunt momenteel alleen SSL Passthrough. De methode SSL Passthrough wordt altijd gebruikt, ongeacht de optie die u selecteert.

- Selecteer **MSRDP** om persistente sessies te handhaven tussen de Windows-clients en -servers waarop de service Microsoft Remote Desktop Protocol (RDP) wordt uitgevoerd. In het aanbevolen scenario voor het inschakelen van MSRDP-persistentie maakt u een load balancer-pool die bestaat uit leden waarop de ondersteunde Windows-server wordt uitgevoerd, waarbij alle leden behoren tot een Windows-cluster en deelnemen aan een Windows-sessiedirectory.
- Selecteer **Geen** om op te geven dat sessieacties niet worden opgeslagen voor latere intrekking.

5 Als u een persistentie-instelling voor cookies gebruikt, voert u de naam van de cookie in.

- 6 (Optioneel) Selecteer de modus waarmee de cookie wordt ingevoegd, in het vervolgkeuzemenu **Modus**.

Optie	Beschrijving
Invoegen	NSX Edge verzendt een cookie. Als de server een of meer cookies verzendt, ontvangt de client een extra cookie (servercookie(s) + NSX Edge-cookie). Als de server geen cookie verzendt, ontvangt de client geen NSX Edge-cookie.
Voorvoegsel	De server verzendt een cookie. Gebruik deze optie als uw client niet meer dan één cookie ondersteunt. Als u uw eigen toepassing gebruikt met uw eigen client die slechts één cookie ondersteunt, verzendt de webserver een cookie, maar plaatst de NSX Edge de cookie-informatie (als voorvoegsel) in de servercookiewaarde.
App-sessie	De server verzendt geen cookie, maar verzendt de informatie over de gebruikerssessie als URL. Bijvoorbeeld: <code>http://mysite.com/admin/UpdateUserServlet;jsessionid=X000X0XXX0XXXX</code> , waarbij <code>jsessionid</code> de informatie over de gebruikerssessie is die wordt gebruikt voor persistentie.

- 7 (Optioneel) Voer de vervaltijd voor persistentie in seconden in voor de cookie.

Bijvoorbeeld: voor L7 load balancing met een TCP-bron-IP, treedt er een time-out op voor de persistentievermelding als geen nieuwe TCP-verbindingen tot stand worden gebracht gedurende de specifieke vervaltijd, zelfs als de bestaande verbindingen nog steeds actief zijn.

- 8 (Optioneel) Klik op het tabblad **Statuscontrole** en ga naar het onderwerp [Instellingen voor de statuscontrole van de virtuele server definiëren](#) om door te gaan met het definiëren van de virtuele server in het load balancer-onderdeel van NSX.

Instellingen voor de statuscontrole van de virtuele server definiëren

Door de optie **Aanpassen** te selecteren op het tabblad **Algemeen**, geeft u op hoe en of de load balancer van NSX statuscontroles moet uitvoeren op poolleden binnen de virtuele server.

De standaardinstellingen voor het statuscontroleprotocol en de statuscontrolepoort komen overeen met de instellingen voor het protocol en de poort op het tabblad **Algemeen**.

Zie *Een servicemonitor maken* in de productdocumentatie van NSX op https://www.vmware.com/support/pubs/nsx_pubs.html. Merk op dat de NSX-documentatie als een poolid naar het virtuele-serverlid verwijst.

Voorwaarden

[Algemene instellingen voor virtuele server definiëren](#).

Procedure

- 1 (Optioneel) Selecteer een statuscontroleprotocol in het vervolgkeuzemenu **Statuscontroleprotocol** om op te geven hoe het poolid wordt benaderd wanneer de load balancer luistert om de status van het poolid te bepalen.

De protocolopties zijn **HTTP**, **HTTPS**, **TCP**, **ICMP**, **UDP** en **Geen**.

U kunt ook het standaardprotocol accepteren dat is opgegeven op het tabblad Algemeen.

- 2 (Optioneel) Geef een waarde op in het vak **Statuscontrolepoort** om aan te geven naar welke poort de load balancer luistert om de status van het virtuele-serverlid of -poolid te bewaken.

Merk op dat de NSX-documentatie als een poolid naar een virtuele-serverlid verwijst.

De HTTP-, HTTPS- en TCP-protocollen kunnen een poort delen met UDP. Bijvoorbeeld: als service 1 TCP, HTTP of HTTPS gebruikt op poort 80, kan service 2 UDP gebruiken op poort 80. Maar als service 1 UDP gebruikt op poort 80, kan service 2 niet UDP gebruiken op poort 80.

- 3 Voer een **Interval** in seconden in waarna een server moet worden gepingd.
- 4 Voer de maximumtijd in seconden in (**Time-out**) waarbinnen een antwoord van de server moet worden ontvangen.
- 5 Geef bij **Max. aantal nieuwe pogingen** het aantal keer op dat de server moet worden gepingd voordat deze als buiten bedrijf wordt beschouwd.
- 6 Geef aanvullende statuscontrole-instellingen op, gebaseerd op het door u geselecteerde **Statuscontroleprotocol**.

- a Voer de **Methode** in die moet worden gebruikt om de serverstatus te detecteren. De opties zijn GET, OPTIONS en POST.

- b Voer de **URL** in die in de aanvraag moet worden gebruikt om de serverstatus te detecteren. Dit is de URL die wordt gebruikt voor de methodeopties GET en POST (standaard is dit "/").

- c Voer in het tekstvak **Verzenden** de tekenreeks in die naar de server moet worden verzonden nadat er een verbinding tot stand is gebracht.

Voer in het tekstvak **Verzenden** de tekenreeks in die naar de server moet worden verzonden nadat er een verbinding tot stand is gebracht.

- d Voer in het tekstvak **Ontvangen** de tekenreeks op die van de server wordt verwacht.

Alleen als de tekenreeks die wordt ontvangen overeenkomt met deze definitie wordt de server als in bedrijf beschouwd.

De tekenreeks kan een koptekst zijn of in het hoofdonderdeel van de reactie staan.

- 7 Klik op het tabblad **Geavanceerd** en ga naar het onderwerp [Geavanceerde instellingen voor virtuele server definiëren](#) om door te gaan met het definiëren van de virtuele server in het load balancer-onderdeel van NSX.

Zie [Logboekopties voor load balancers definiëren](#) als u logboekopties wilt opgeven.

Geavanceerde instellingen voor virtuele server definiëren

Door de optie **Aanpassen** te selecteren op het tabblad **Algemeen** kunt u het load balancer-onderdeel van NSX aanpassen om instellingen op te geven, zoals het aantal gelijktijdige verbindingen dat één poolid kan herkennen en het maximum aantal gelijktijdige verbindingen dat de virtuele server kan verwerken.

Voorwaarden

Algemene instellingen voor virtuele server definiëren.

Procedure

- 1 Voer een waarde in in het tekstvak **Verbindingslimiet** om het maximum aantal gelijktijdige verbindingen in NSX op te geven dat de virtuele server kan verwerken.
Deze instelling houdt rekening met het aantal verbindingen van alle leden.
Voer de waarde 0 in om geen limiet op te geven.
- 2 Voer een waarde in het tekstvak **Verbindingssnelheidslimiet** in om het maximum aantal inkomende verbindingsaanvragen in NSX op te geven dat kan worden verwerkt per seconde.
Deze instelling houdt rekening met het aantal verbindingen van alle leden.
Voer de waarde 0 in om geen limiet op te geven.
- 3 (Optioneel) Schakel het selectievakje **Versnelling inschakelen** in om te bepalen dat elk virtueel IP (VIP) de snellere L4 load balancer gebruikt in plaats van de L7 load balancer.
- 4 (Optioneel) Schakel het selectievakje **Transparant** in om toe te staan dat de leden van de load balancer-pool het IP-adres zien van de machines die de load balancer aanroepen.
Als het selectievakje is uitgeschakeld, zien de leden van de load balancer-pool het IP-adres van de verkeersbron als het interne IP-adres van een load balancer.
- 5 Voer een waarde in in het tekstvak **Max. aantal verbindingen** om het maximum aantal gelijktijdige verbindingen op te geven dat één poolid kan herkennen.
Als het aantal inkomende aanvragen hoger is dan deze waarde, worden aanvragen in de wachtrij geplaatst en vervolgens verwerkt in de volgorde waarin ze worden ontvangen wanneer verbindingen worden vrijgegeven.
Voer de waarde 0 in als u geen maximumwaarde wilt instellen.
- 6 Voer een waarde in het tekstvak **Min. aantal verbindingen** in om het minimum aantal gelijktijdige verbindingen op te geven dat één poolid altijd moet accepteren.
Voer de waarde 0 in als u geen minimumwaarde wilt instellen.
- 7 Klik op **OK** om het definiëren van de virtuele server te voltooien.
- 8 Zie [Logboekopties voor load balancers definiëren](#) of klik op **Opslaan** of **Voltooien** om logboekopties op te geven.

Logboekopties voor load balancers definiëren

U kunt de typen logboekacties voor load balancers definiëren die worden vastgelegd en geregistreerd in de logboeken voor load balancers.

Nadat u een load balancer-onderdeel hebt gedefinieerd, of wanneer u een load balancer-onderdeel definieert, kunt u een logboekniveau opgeven om logboekinformatie over het verkeer van de load balancers te verzamelen. De logboekniveaus die u definieert voor een load balancer-onderdeel in de blueprint, zijn van toepassing op alle load balancers die worden gedefinieerd in de blueprint.

De logboekniveaus zijn Fouten opsporen, Informatie, Waarschuwing, Fout en Kritiek. Met de opties Fouten opsporen en Informatie worden gebruikersaanvragen geregistreerd, terwijl met de opties Waarschuwing, Fout en Kritiek geen gebruikersaanvragen worden geregistreerd.

Zie de *NSX Administration Guide* voor meer informatie over logboekopties voor NSX load balancers.

Voorwaarden

[Instellingen voor leden van load balancers definiëren.](#)

Procedure

- 1 Selecteer het tabblad **Algemeen** in het load balancer-onderdeel in het ontwerpcanvas.
- 2 Selecteer een of meer logboekopties in het vervolgkeuzemenu **Logboekniveau**.

Selecteer een logboekniveau voor het verzamelen van logboekinformatie over verkeer van load balancers. De instelling is van toepassing op alle load balancer-onderdelen van NSX in de blueprint.

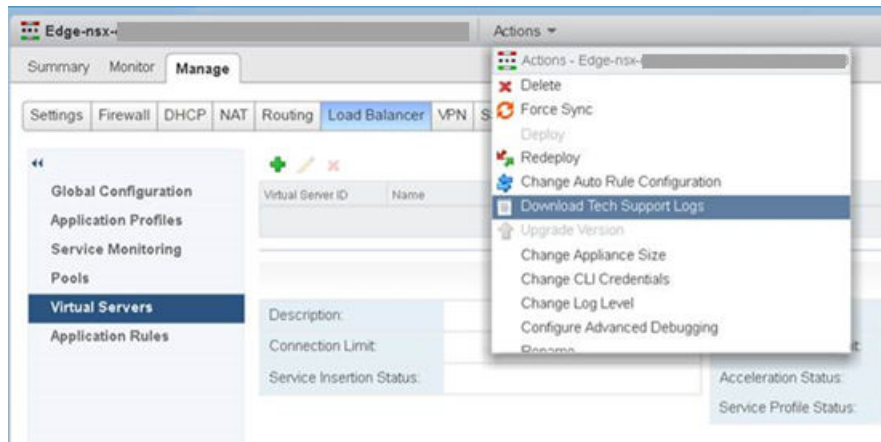
De logboekinstellingen worden gedefinieerd in de vSphere-webclient.

- Geen
- Informatie
- Noodgeval
- Waarschuwing
- Kritiek
- Error
- Waarschuwing
- Melding
- Fouten opsporen

- 3 Klik op **Opslaan**.

Resultaten

U kunt de logboeken in de vSphere-webclient bekijken en downloaden via het menu **Acties** voor de NSX Edge, zoals beschreven in *Download Tech Support Logs for NSX Edge* in de NSX-productdocumentatie op https://www.vmware.com/support/pubs/nsx_pubs.html.



NSX-T load balancer-onderdelen gebruiken in een blueprint

U kunt een of meer NSX-T load balancer-onderdelen op aanvraag aan het ontwerpcanvas toevoegen om instellingen van vSphere-machineonderdelen in de blueprint te configureren.

De instellingen voor netwerk- en beveiligingsonderdelen die u aan de blueprint toevoegt, worden afgeleid van uw configuratie van NSX for vSphere en NSX-T. Raadpleeg de *Administration Guide* in de [NSX for vSphere-productdocumentatie](#) of [NSX-T-productdocumentatie](#), afhankelijk van welke toepassing u gebruikt, voor informatie over het configureren van NSX.

De instellingen voor netwerk- en beveiligingsonderdelen die u aan de blueprint toevoegt, worden afgeleid van uw NSX-T-configuratie. Raadpleeg de *NSX-T Administration Guide* in de [NSX-T-productdocumentatie](#) voor informatie over het configureren van NSX-T.

De volgende regels zijn van toepassing op load balancer-pools en VIP-netwerkinstellingen in de blueprint.

- Als het netwerkprofiel van de pool NAT is, kan het VIP-netwerkprofiel deel uitmaken van het NAT-netwerkprofiel.
- Als het netwerkprofiel van de pool geleid is, kan het VIP-netwerkprofiel zich alleen op hetzelfde geleide netwerk of hetzelfde externe netwerk bevinden.
- Als het netwerkprofiel van de pool extern is, kan het VIP-netwerkprofiel alleen hetzelfde externe netwerkprofiel zijn.

Elke component van de load balancer kan meerdere virtuele servers hebben, die tevens kunnen worden aangeduid als load balancer services. Elke virtuele server in het load balancer-onderdeel heeft één poort en één protocol. U kunt bijvoorbeeld load balancing uitvoeren voor een HTTP-service of HTTPS-service. Een load balancer kan load balancing uitvoeren voor meerdere services.

De NSX load balancer is de service die de virtuele servers van de load balancer bevat.

Als een blueprint een load balancer bevat en app-isolatie is ingeschakeld, worden de load balancer-VIP's aan de app-isolatiebeveiligingsgroep toegevoegd als IPSet. Als een blueprint een beveiligingsgroep op aanvraag bevat die is gekoppeld aan een machinelaag die ook is gekoppeld aan een load balancer, bevat de beveiligingsgroep op aanvraag de machinelaag IPSet en VIP's.

Zie [Informatie over de NSX-T-implementatietopologieën voor netwerken, beveiliging en load balancer-configuraties](#) voor meer informatie over NSX-T-specifieke overwegingen met betrekking tot implementatie en topologie.

Een NSX-T load balancer op aanvraag toevoegen

U kunt een NSX-T-load balancer-onderdeel op aanvraag naar het ontwerpcanvas slepen en de bijbehorende instellingen configureren voor gebruik met vSphere-machineonderdelen en containeronderdelen in de blueprint.

De NSX-T-load balancer distribueert inkomende serviceaanvragen gelijkmatig over meerdere servers zodanig dat de load distributie transparant is voor gebruikers. Load balancing (het verdelen van taken) zorgt ervoor dat bronnen optimaal worden gebruikt, dat de doorvoer wordt gemaximaliseerd, dat de responstijd wordt geminimaliseerd en dat overload wordt vermeden.

U kunt een virtueel IP-adres toewijzen aan een set met poolservers voor load balancing. De load balancer aanvaardt TCP-, UDP-, HTTP- of HTTPS-aanvragen op het virtuele IP-adres en bepaalt welk poolid wordt gebruikt. Een load balancer wordt toegevoegd aan een logische router van Tier-1.

Afhankelijk van de noden voor uw omgeving kunt u de prestaties van de load balancer schalen door het aantal bestaande virtuele servers en poolleden te verhogen om zwaarder netwerkverkeer aan te kunnen.

Voor meer informatie over het maken van NSX-T-load balancers om het gedrag van netwerkverkeer te definiëren, raadpleegt u *Logische load balancer* en *Load balancer-onderdelen configureren* in de *NSX-T Administration Guide* in de [productdocumentatie voor NSX-T](#).

Procedure

1 [Instellingen voor leden van NSX-T load balancers definiëren](#)

U kunt een NSX-T-load balancer-onderdeel op aanvraag definiëren om de taakverwerking te verdelen over ingerichte vSphere-lidmachines of containermachines in een netwerk.

2 [Algemene instellingen voor virtuele server definiëren voor NSX-T](#)

U kunt een protocol en poort voor één virtuele server definiëren voor uw load balancer of u kunt extra virtuele servers toevoegen om extra opties voor NSX-T load balancers aan te passen.

3 [Distributie-instellingen voor virtuele server definiëren voor NSX-T](#)

Door de optie **Aanpassen** te selecteren wanneer u een virtuele server definieert, kunt u informatie opgeven over de poolleden, zoals de poort waarop de leden verkeer ontvangen, het protocoltype dat de NSX-T load balancer kan gebruiken om toegang te krijgen tot die poort, het algoritme dat wordt gebruikt voor load balancing en de persistentie-instellingen.

4 [Instellingen voor de statuscontrole van de virtuele server definiëren voor NSX-T](#)

Door de optie **Aanpassen** te selecteren op het tabblad **Algemeen**, geeft u op hoe en of de load balancer van NSX-T statuscontroles moet uitvoeren op poolleden binnen de virtuele server.

5 Geavanceerde instellingen voor virtuele server definiëren voor NSX-T

Door de optie **Aanpassen** te selecteren op het tabblad **Algemeen** kunt u het load balancer-onderdeel van NSX-T aanpassen om instellingen op te geven, zoals het aantal gelijktijdige verbindingen dat één poolid kan herkennen en het maximum aantal gelijktijdige verbindingen dat de virtuele server kan verwerken.

6 Logboekopties voor NSX-T load balancers definiëren

U kunt de typen logboekacties voor load balancers definiëren die worden vastgelegd en geregistreerd in de logboeken voor load balancers.

Instellingen voor leden van NSX-T load balancers definiëren

U kunt een NSX-T-load balancer-onderdeel op aanvraag definiëren om de taakverwerking te verdelen over ingerichte vSphere-lidmachines of containermachines in een netwerk.

Wanneer u een load balancer-onderdeel toevoegt aan een blueprint in het ontwerpcanvas, kunt u een standaard- of aangepaste optie kiezen wanneer u de definities voor uw virtuele server maakt of bewerkt in het load balancer-onderdeel. Met de standaardoptie kunt u het protocol, de poort en een beschrijving opgeven voor de virtuele server en standaardwaarden gebruiken voor alle andere instellingen. Met de aangepaste optie kunt u extra detailniveaus definiëren.

Als de load balancer is ingericht met een extern netwerk, moeten het VIP (VIP-netwerk) en de ledenpool (het ledennetwerk) zich op hetzelfde bestaande netwerk bevinden. De inrichting zal mislukken als het VIP en de ledenpool zich niet in hetzelfde externe netwerk bevinden.

Voorwaarden

- Load balancer-instellingen maken en configureren voor NSX. Zie [Checklist voor de voorbereiding van de netwerk- en beveiligingsconfiguratie van NSX](#).
- Controleer of de NSX-inventaris met succes is uitgevoerd voor uw cluster.
Als u NSX-configuraties in vRealize Automation wilt gebruiken, moet u gegevensverzameling uitvoeren.
- Maak een netwerkprofiel. Zie [Een netwerkprofiel maken in vRealize Automation](#).
- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Open een nieuwe of bestaande blueprint in het ontwerpcanvas met behulp van het tabblad **Ontwerpen**.
- Controleer dat ten minste één vSphere-machineonderdeel of -containeronderdeel bestaat in de blueprint.

Procedure

- 1 Als u de lijst met beschikbare netwerk- en beveiligingsonderdelen wilt weergeven, klikt u op **Netwerk en beveiliging** in de sectie Categorieën.
- 2 Sleep een **NSX-T load balancer op aanvraag**-onderdeel naar het ontwerpcanvas.

- 3 Als u het onderdeel een uniek label wilt geven in het ontwerpcanvas, voert u in het tekstvak **ID** een onderdeelnaam in.

- 4 Selecteer de naam van een vSphere-machineonderdeel of -containeronderdeel in het vervolgkeuzemenu **Lid**.

De lijst bevat alleen de vSphere-machineonderdelen en -containeronderdelen in de actieve blueprint.

- 5 Selecteer de NIC voor de load balancing in de vervolgkeuzelijst **Ledennetwerk**.

De lijst bevat NIC's die zijn gedefinieerd voor het geselecteerde vSphere-machinelid.

- 6 Selecteer een beschikbaar virtueel IP-adresnetwerk in de vervolgkeuzelijst **VIP-netwerk**. Selecteer bijvoorbeeld een beschikbaar extern of NAT-netwerk.

U kunt meerdere NSX load balancers en NSX-netwerkonderdelen op aanvraag in een blueprint hebben, maar ze moeten allemaal zijn gekoppeld aan hetzelfde VIP-netwerk.

- 7 (Optioneel) Typ een geldig IP-adres voor de NIC in het tekstvak **IP-adres**.

De standaardinstelling is het statische IP-adres dat is gekoppeld aan het VIP-netwerk. U kunt een ander IP-adres of een IP-adresbereik opgeven. Standaard wordt het eerstvolgende beschikbare IP-adres uit het geassocieerde VIP-netwerk toegewezen.

Laat het veld IP-adres leeg als u tijdens de inrichting het IP-adres wilt laten toewijzen vanuit het gekoppelde VIP-netwerk.

Als u een IP-adres van een ander type netwerk opgeeft, kan slechts één implementatie worden ingericht. Bij volgende implementaties zal de IP-toewijzing mislukken omdat het IP-adres al door de eerste implementatie wordt gebruikt.

- 8 Als u een definitie voor een virtuele server wilt maken, klikt u op **Nieuw** en raadpleegt u [Algemene instellingen voor virtuele server definiëren voor NSX-T](#).

Elk load balancer-onderdeel vereist ten minste één virtuele server.

Zie [Logboekopties voor NSX-T load balancers definiëren](#) als u logboekopties wilt opgeven.

Algemene instellingen voor virtuele server definiëren voor NSX-T

U kunt een protocol en poort voor één virtuele server definiëren voor uw load balancer of u kunt extra virtuele servers toevoegen om extra opties voor NSX-T load balancers aan te passen.

Bijvoorbeeld: u kunt het load balancer-onderdeel aanpassen om instellingen als statuscontroleprotocol en -poort, algoritme, persistentie en transparantie te definiëren.

Voorwaarden

[Instellingen voor leden van NSX-T load balancers definiëren](#).

Procedure

- 1 Klik op het tabblad **Algemeen** op de pagina **Virtuele server**.

- 2 Selecteer het netwerkverkeerprotocol in het vervolgkeuzemenu **Protocol** voor het verdelen van taken op de virtuele server.

De protocolopties zijn HTTP, HTTPS, TCP, en UDP.

NSX-T load balancers bieden geen ondersteuning voor de SSL passthrough-modus, maar in plaats daarvan kan de SSL-beëindigingsmodus worden gebruikt. Als u HTTPS kiest, moet u de volgende aanvullende informatie opgeven, die al moet bestaan in de NSX-T-manager:

- Naam van het certificaat in de NSX-T-certificaatinventaris. De load balancer biedt dit certificaat voor clients.
- Naam van het SSL-clientprofiel.

- 3 Voer een poortwaarde in in het tekstvak **Poort**.

Het geselecteerde protocol bepaalt de standaardpoortinstelling.

Protocol	Standaardpoort
HTTP	80
HTTPS	443
TCP	8080
UDP	geen standaard

De HTTP-, HTTPS- en TCP-protocollen kunnen een poort delen met UDP. Bijvoorbeeld: als service 1 TCP, HTTP of HTTPS gebruikt op poort 80, kan service 2 UDP gebruiken op poort 80. Maar als service 1 UDP gebruikt op poort 80, kan service 2 niet UDP gebruiken op poort 80.

- 4 (Optioneel) Voer een beschrijving voor het virtuele-serveronderdeel in.
- 5 Klik op het tabblad **Distributie** en ga naar het onderwerp [Distributie-instellingen voor virtuele server definiëren voor NSX-T](#) om door te gaan met het definiëren van de virtuele server in het load balancer-onderdeel van NSX-T.

Distributie-instellingen voor virtuele server definiëren voor NSX-T

Door de optie **Aanpassen** te selecteren wanneer u een virtuele server definieert, kunt u informatie opgeven over de poolleden, zoals de poort waarop de leden verkeer ontvangen, het protocoltype dat de NSX-T load balancer kan gebruiken om toegang te krijgen tot die poort, het algoritme dat wordt gebruikt voor load balancing en de persistentie-instellingen.

Een pool vertegenwoordigt een cluster met machines waarover de taken worden verdeeld. Een poolid vertegenwoordigt één machine in dat cluster.

De standaardinstellingen voor het lidprotocol en de lidpoort komen overeen met de instellingen voor het protocol en de poort op de pagina **Algemeen**.

De pool met machines die lid zijn, wordt weergegeven in de waarde voor de optie **Lid** in de gebruikersinterface van het load balancer-onderdeel in de blueprint. De vermelding bij **Lid** wordt ingesteld op de pool of het cluster met machines.

Voorwaarden

Instellingen voor leden van NSX-T load balancers definiëren.

Procedure

- 1 (Optioneel) De instelling **Lidprotocol** komt overeen met het protocol dat u hebt opgegeven op het tabblad **Algemeen**. Deze instelling definieert hoe het poolid netwerkverkeer ontvangt.
- 2 (Optioneel) Voer een poortnummer in in het tekstvak **Lidpoort** om de poort te bepalen waarop het poolid netwerkverkeer ontvangt.

Als de aanvraag voor het virtuele IP-adres (VIP) van de load balancer binnenkomt op poort 80, moet u de aanvraag mogelijk doorverwijzen naar een andere poort, bijvoorbeeld poort 8080, op de poolleden.

- 3 (Optioneel) Selecteer de verdelingsmethode op basis van een algoritme voor deze pool.

De algoritmeopties en de algoritmeparameters voor de opties die ze vereisen, worden beschreven in de volgende tabel.

Raadpleeg *Een serverpool toevoegen voor taakverdeling* in de [NSX-T-productdocumentatie](#) voor gerelateerde informatie.

Optie	Beschrijving en algoritmeparameters
ROUND_ROBIN	Inkomende clientaanvragen doorlopen een lijst met beschikbare servers die de aanvraag kunnen afhandelen. Negeert het gewicht van serverpoolleden zelfs als dit geconfigureerd is.
WEIGHTED ROUND ROBIN	Aan elke server wordt een gewichtswaarde toegewezen die opgeeft hoe die server presteert ten opzichte van andere servers in de pool. De waarde bepaalt hoeveel clientverzoeken naar een server worden verzonden in vergelijking met andere servers in de pool. Dit algoritme voor load balancing focust op een gelijke verdeling van de taken tussen de beschikbare serverbronnen.
IP-HASH	Selecteert een server op basis van een hash van het oorspronkelijke IP-adres en het totale gewicht van alle actieve servers.
LEASTCONN	Hiermee worden clientaanvragen naar meerdere servers gedistribueerd op basis van het bestaande aantal verbindingen op de server. Nieuwe verbindingen worden verzonden naar de server met het minste aantal verbindingen. Negeert het gewicht van serverpoolleden zelfs als dit geconfigureerd is.
WEIGHTED LEASTCONN	Aan elke server wordt een gewichtswaarde toegewezen die opgeeft hoe die server presteert ten opzichte van andere servers in de pool. De waarde bepaalt hoeveel clientverzoeken naar een server worden verzonden in vergelijking met andere servers in de pool. Dit algoritme voor load balancing focust op het gebruik van de gewichtswaarde voor een gelijke verdeling van de taken tussen de beschikbare serverbronnen. De gewichtswaarde is standaard 1 als de waarde niet is geconfigureerd en langzame start is ingeschakeld.

4 (Optioneel) Selecteer de persistentiemethode voor deze pool.

Persistentie volgt en bewaart sessiegegevens, zoals het specifieke poolid dat een clientaanvraag heeft behandeld. Met persistentie worden clientaanvragen doorverwezen naar hetzelfde poolid voor de levensduur van een sessie of tijdens opeenvolgende sessies. Zie *Persistente profielen configureren* in de [NSX-T-productdocumentatie](#) voor meer informatie over de persistentiemethoden.

- Selecteer **Geen** om op te geven dat sessieacties niet worden opgeslagen voor latere intrekking.
- Selecteer **Cookie** om een unieke cookie in te voegen om de sessie te identificeren de eerste keer dat een client toegang krijgt tot de site. Bij elke volgende aanvraag wordt de cookie gelezen om ervoor te zorgen dat verbinding wordt gemaakt met de geschikte server.
- Selecteer **Bron-IP** om sessies te volgen op basis van het oorspronkelijke IP-adres. Als een client een verbinding aanvraagt voor een virtuele server die affiniteitspersistentie van het bronadres ondersteunt, controleert de load balancer of die client eerder is verbonden. Als dat zo is, wordt de client naar hetzelfde groepslid geleid.

5 Als u persistente cookies gebruikt, voert u de naam van de cookie in.

6 (Optioneel) Selecteer deodus waarmee de cookie wordt ingevoegd, in het vervolgkeuzemenu **Modus**.

Optie	Beschrijving
Invoegen	Maak een uniek cookie om de sessie te identificeren.
Voorvoegsel	Wordt toegevoegd aan de bestaande cookie.
Herschrijven	Overschrijft de bestaande cookie.

7 (Optioneel) Voer de vervaltijd voor persistentie in seconden in voor de cookie.

Bijvoorbeeld: voor L7 load balancing met een TCP-bron-IP, treedt er een time-out op voor de persistentievermelding als geen nieuwe TCP-verbindingen tot stand worden gebracht gedurende de specifieke vervaltijd, zelfs als de bestaande verbindingen nog steeds actief zijn.

8 (Optioneel) Klik op het tabblad **Statuscontrole** en ga naar het onderwerp [Instellingen voor de statuscontrole van de virtuele server definiëren voor NSX-T](#) om door te gaan met het definiëren van de virtuele server in het load balancer-onderdeel van NSX-T.

Instellingen voor de statuscontrole van de virtuele server definiëren voor NSX-T

Door de optie **Aanpassen** te selecteren op het tabblad **Algemeen**, geeft u op hoe en of de load balancer van NSX-T statuscontroles moet uitvoeren op poolleden binnen de virtuele server.

De standaardinstellingen voor het statuscontroleprotocol en de statuscontrolepoort komen overeen met de instellingen voor het protocol en de poort op het tabblad **Algemeen**.

Raadpleeg de [NSX-T-productdocumentatie](#) voor gerelateerde informatie. Merk op dat de NSX-T-documentatie als een poolid naar het virtuele-serverlid verwijst.

Voorwaarden

Distributie-instellingen voor virtuele server definiëren voor NSX-T.

Procedure

- 1 (Optioneel) Selecteer een statuscontroleprotocol in het vervolgkeuzemenu **Statuscontroleprotocol** om op te geven hoe het poolid wordt benaderd wanneer de load balancer luistert om de status van het poolid te bepalen.
De protocolopties zijn **Geen**, **HTTP**, **HTTPS**, **TCP**, **ICMP** en **UDP**.
U kunt ook het standaardprotocol accepteren dat is opgegeven op het tabblad Algemeen.
- 2 (Optioneel) Geef een waarde op in het vak **Statuscontrolepoort** om aan te geven naar welke poort de load balancer luistert om de status van het virtuele-serverlid of -poolid te bewaken.
Merk op dat de NSX-documentatie als een poolid naar een virtuele-serverlid verwijst.
De HTTP-, HTTPS- en TCP-protocollen kunnen een poort delen met UDP. Bijvoorbeeld: als service 1 TCP, HTTP of HTTPS gebruikt op poort 80, kan service 2 UDP gebruiken op poort 80. Maar als service 1 UDP gebruikt op poort 80, kan service 2 niet UDP gebruiken op poort 80.
- 3 Voer een **Interval** in seconden in waarna een server moet worden gepingd.
- 4 Voer de maximumtijd in seconden in (**Time-out**) waarbinnen een antwoord van de server moet worden ontvangen.
- 5 Geef bij **Max. aantal nieuwe pogingen** het aantal keer op dat de server moet worden gepingd voordat deze als buiten bedrijf wordt beschouwd.
- 6 Als u een HTTP- of HTTPS-protocol hebt opgegeven, voert u de **Methode** in die moet worden gebruikt om de serverstatus te detecteren.
- 7 Voer, indien beschikbaar, de **URL** in die in de aanvraag moet worden gebruikt om de serverstatus te detecteren. Dit is de URL die wordt gebruikt voor de methodeopties GET en POST (standaard is dit "/").
- 8 Voer, indien beschikbaar, de tekenreeksen in die moeten worden verzonden en ontvangen in de tekstvakken **Verzenden** en **Ontvangen**.
Voer in het tekstvak **Verzenden** de tekenreeks in die naar de server moet worden verzonden nadat er een verbinding tot stand is gebracht.
Voer in het tekstvak **Ontvangen** de tekenreeks op die van de server wordt verwacht. Alleen als de tekenreeks die wordt ontvangen overeenkomt met deze definitie wordt de server als in bedrijf beschouwd.
- 9 Klik op het tabblad **Geavanceerd** en ga naar het onderwerp [Geavanceerde instellingen voor virtuele server definiëren voor NSX-T](#) om door te gaan met het definiëren van de virtuele server in het load balancer-onderdeel van NSX-T.
Zie [Logboekopties voor NSX-T load balancers definiëren](#) als u logboekopties wilt opgeven.

Geavanceerde instellingen voor virtuele server definiëren voor NSX-T

Door de optie **Aanpassen** te selecteren op het tabblad **Algemeen** kunt u het load balancer-onderdeel van NSX-T aanpassen om instellingen op te geven, zoals het aantal gelijktijdige verbindingen dat één poollid kan herkennen en het maximum aantal gelijktijdige verbindingen dat de virtuele server kan verwerken.

Voorwaarden

[Algemene instellingen voor virtuele server definiëren voor NSX-T.](#)

Procedure

- 1 Voer een waarde in in het tekstvak **Verbindingslimiet** om het maximum aantal gelijktijdige verbindingen in NSX-T op te geven dat de virtuele server kan verwerken.

Deze instelling houdt rekening met het aantal verbindingen van alle leden.

Voer de waarde 0 in om geen limiet op te geven.
- 2 Voer een waarde in het tekstvak **Verbindingssnelheidslimiet** in om het maximum aantal inkomende verbindingsaanvragen in NSX-T op te geven dat kan worden verwerkt per seconde.

Deze instelling houdt rekening met het aantal verbindingen van alle leden.

Voer de waarde 0 in om geen limiet op te geven.
- 3 (Optioneel) Schakel het selectievakje **Transparant** in om toe te staan dat de leden van de load balancer-pool het IP-adres zien van de machines die de load balancer aanroepen.

Als het selectievakje is uitgeschakeld, zien de leden van de load balancer-pool het IP-adres van de verkeersbron als het interne IP-adres van een load balancer.
- 4 Voer een waarde in in het tekstvak **Max. aantal verbindingen** om het maximum aantal gelijktijdige verbindingen op te geven dat één poollid kan herkennen.

Als het aantal inkomende aanvragen hoger is dan deze waarde, worden aanvragen in de wachtrij geplaatst en vervolgens verwerkt in de volgorde waarin ze worden ontvangen wanneer verbindingen worden vrijgegeven.

Voer de waarde 0 in als u geen maximumwaarde wilt instellen.
- 5 Klik op **OK** om het definiëren van de virtuele server te voltooien.
- 6 Zie [Logboekopties voor NSX-T load balancers definiëren](#) of klik op **Opslaan** of **Voltooien** om logboekopties op te geven.

Logboekopties voor NSX-T load balancers definiëren

U kunt de typen logboekacties voor load balancers definiëren die worden vastgelegd en geregistreerd in de logboeken voor load balancers.

U kunt een logboekniveau opgeven voor het verzamelen van logboekinformatie over verkeer van load balancers. De logboekniveaus die u definieert voor een NSX-T load balancer-onderdeel in de blueprint, zijn van toepassing op alle load balancers in de blueprint.

De logboekniveaus zijn Fouten opsporen, Informatie, Waarschuwing, Fout en Kritiek. Met de opties Fouten opsporen en Informatie worden gebruikersaanvragen geregistreerd, terwijl met de opties Waarschuwing, Fout en Kritiek geen gebruikersaanvragen worden geregistreerd.

Raadpleeg de *NSX-T Administration Guide* in de [NSX-T-productdocumentatie](#) voor meer informatie over de logboekregistratie van NSX-T load balancers.

Voorwaarden

Instellingen voor leden van NSX-T load balancers definiëren

Procedure

- 1 Selecteer het tabblad **Algemeen** in het load balancer-onderdeel in het ontwerpcanvas.
- 2 Selecteer een of meer logboekopties in het vervolgkeuzemenu **Logboekniveau**.
De logboekinstellingen worden gedefinieerd in de vSphere-webclient.
 - Geen
 - Noodgeval
 - Waarschuwing
 - Kritiek
 - Error
 - Waarschuwing
 - Informatie
 - Fouten opsporen
- 3 Selecteer een kleine, normale of grote load balancer.
- 4 Klik op **Opslaan** en klik vervolgens op **Voltooien**.

NSX for vSphere-beveiligingsonderdelen gebruiken in een blueprint

U kunt NSX for vSphere-beveiligingsonderdelen aan het ontwerpcanvas toevoegen om de bijbehorende geconfigureerde instellingen beschikbaar te maken voor een of meer vSphere-machineonderdelen in de blueprint.

Beveiligingsgroepen, tags en beleidsregels worden buiten vRealize Automation in de toepassing NSX geconfigureerd.

De instellingen voor netwerk- en beveiligingsonderdelen die u aan de blueprint toevoegt, worden afgeleid van uw configuratie van NSX for vSphere en NSX-T. Raadpleeg de *Administration Guide* in de [NSX for vSphere-productdocumentatie](#) of [NSX-T-productdocumentatie](#), afhankelijk van welke toepassing u gebruikt, voor informatie over het configureren van NSX.

U kunt beveiligingsfuncties aan blueprints toevoegen door beveiligingsgroepen, tags en beleidsregels voor de vSphere-computerbron in NSX te configureren. Nadat u gegevensverzameling hebt uitgevoerd, zijn de beveiligingsconfiguraties beschikbaar in vRealize Automation.

Voor een voorbeeld van een NSX for vSphere-beveiligingsstrategie raadpleegt u deze blogpost over [vRealize en NSX](#).

Bestaande beveiligingsgroepen en beveiligingsgroepen op aanvraag voor NSX for vSphere

Een beveiligingsgroep bestaat uit verschillende activa of groeperingsobjecten uit de vSphere-inventaris die aan een verzameling beveiligingsregels worden gekoppeld, bijvoorbeeld gedistribueerde firewallregels en integraties van beveiligingsservices van derden, zoals antivirus- en inbraakcontrole. De groeperingsfunctie stelt u in staat om aangepaste containers te maken, waaraan u bronnen kunt toewijzen, zoals virtual machines en netwerkadapters, voor gedistribueerde beveiliging van de firewall. Nadat een groep is gedefinieerd, kunt u deze groep als bron of bestemming ter beveiliging toevoegen aan de regel van de firewall.

In aanvulling op de beveiligingsgroepen voor de reservering, kunt u vSphere bestaande of on-demand beveiligingsgroepen toevoegen aan een blueprint.

U kunt een of meer on-demand beveiligingsgroepen maken. U kunt een of meer beveiligingsbeleidsdocumenten selecteren voor configuratie in een beveiligingsgroep.

Een beveiligingsbeleid is een set services voor endpoints, firewalls en netwerkintrospecties die kunnen worden toegepast op een beveiligingsgroep. U kunt beveiligingsbeleid toevoegen aan een vSphere virtual machine door een beveiligingsgroep op aanvraag op te nemen in een blueprint. U kunt het beveiligingsbeleid niet direct toevoegen aan een reservering. Nadat de gegevensverzameling is uitgevoerd, zijn beveiligingsbeleidsregels die zijn gedefinieerd in NSX for vSphere voor een computerbron beschikbaar voor selectie in een blueprint.

Beveiligingsgroepen worden beheerd in de basis van de bron. Voor informatie over het beheren van beveiligingsgroepen voor verschillende brontypen, raadpleegt u de documentatie van NSX for vSphere.

Opmerking Wanneer app-isolatie is uitgeschakeld, wordt een afzonderlijk beveiligingsbeleid gemaakt. App-isolatie maakt gebruik van een logische firewall om alle inkomend en uitgaand verkeer naar en van de toepassingen in de blueprint, te blokkeren. Onderdeelmachines die zijn ingericht door een blueprint met een beveiligingsbeleid dat gebruik maakt van app-isolatie, kunnen met elkaar communiceren maar geen verbinding maken buiten de firewall, tenzij de blueprint beschikt over andere beveiligingsgroepen met een beleid dat die toegang wel biedt.

Als een blueprint een load balancer bevat en app-isolatie is ingeschakeld, worden de load balancer-VIP's aan de app-isolatiebeveiligingsgroep toegevoegd als IPSet. Als een blueprint een beveiligingsgroep op aanvraag bevat die is gekoppeld aan een machinelaag die ook is gekoppeld aan een load balancer, bevat de beveiligingsgroep op aanvraag de machinelaag IPSet en VIP's.

Bestaande beveiligingstags voor NSX for vSphere

U kunt bestaande beveiligingstagonderdelen voor NSX for vSphere toevoegen. Een beveiligingstag is een kwalificatieobject of categorisering die u als groeperingsmechanisme kunt gebruiken. U definieert de criteria waaraan een object moet voldoen om te worden toegevoegd aan de beveiligingsgroep die u maakt. Hierdoor hebt u de mogelijkheid om machines op te nemen door een filtercriterium te definiëren met een aantal ondersteunde parameters die zijn gericht op het voldoen aan de zoekcriteria. U kunt bijvoorbeeld alle machines die over een specifieke beveiligingstag beschikken toevoegen aan een beveiligingsgroep.

Een bestaand beveiligingsgroepsonderdeel toevoegen voor NSX for vSphere

U kunt een bestaand NSX for vSphere-beveiligingsgroepsonderdeel toevoegen aan het ontwerpcanvas als u de bijbehorende instellingen wilt koppelen aan een of meer vSphere-machineonderdelen van de blueprint.

U kunt een onderdeel van een bestaande beveiligingsgroep gebruiken om een NSX-beveiligingsgroep toe te voegen aan het ontwerpcanvas en de instellingen ervan te configureren voor gebruik met vSphere-machineonderdelen en Software- of XaaS-onderdelen die van toepassing zijn op vSphere.

Standaard worden de beveiligingsgroepen die van toepassing zijn op de huidige tenant beschikbaar gesteld bij het ontwerpen van een blueprint. Met name worden beveiligingsgroepen beschikbaar gesteld als het gekoppelde endpoint een reservering in de huidige tenant heeft. Zie [Tenanttoegang voor beveiligingsobjecten beheren in vRealize Automation](#) voor meer informatie over het beheren van toegang tot de tenancy.

Voorwaarden

- Beveiligingsgroepen maken en configureren voor NSX. Raadpleeg de NSX configuratiechecklist in *vRealize Automation configureren* en de *NSX for vSphere Administration Guide* in de [productdocumentatie voor NSX for vSphere](#).
- Controleer of de NSX-inventaris met succes is uitgevoerd voor uw cluster.
Als u NSX-configuraties in vRealize Automation wilt gebruiken, moet u gegevensverzameling uitvoeren.
- Controleer de concepten voor het beveiligingsonderdeel. Zie [NSX for vSphere-beveiligingsonderdelen gebruiken in een blueprint](#).
- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Open een nieuwe of bestaande blueprint in het ontwerpcanvas met behulp van het tabblad **Ontwerpen**.

Procedure

- 1 Als u de lijst met beschikbare netwerk- en beveiligingsonderdelen wilt weergeven, klikt u op **Netwerk en beveiliging** in de sectie Categorieën.
- 2 Sleep een **Bestaande beveiligingsgroep**-onderdeel naar het ontwerpcanvas.
- 3 Selecteer een bestaande beveiligingsgroep in het vervolgkeuzemenu **Beveiligingsgroep**.
- 4 Klik op **OK**.

- 5 Als u de blueprint wilt opslaan als concept of verder wilt gaan met het configureren van de blueprint, klikt u op **Opslaan** of **Voltooien**.

Resultaten

U kunt beveiligingsinstellingen toevoegen op het tabblad **Beveiliging** van een vSphere-machineonderdeel.

Een bestaand beveiligingstagonderdeel toevoegen voor NSX for vSphere

U kunt een bestaand NSX for vSphere-beveiligingstagonderdeel aan het ontwerpcanvas van een blueprint toevoegen als u de bijbehorende instellingen wilt koppelen aan een of meer vSphere-onderdelen in de blueprint.

U kunt een beveiligingstagonderdeel gebruiken om een bestaande vSphere-beveiligingstag toe te voegen aan het ontwerpcanvas en de instellingen ervan te configureren voor gebruik met vSphere-machineonderdelen en Software-onderdelen die van toepassing zijn op vSphere.

Standaard worden de beveiligingstags die van toepassing zijn op de huidige tenant beschikbaar gesteld bij het ontwerpen van een blueprint. Beveiligingstags worden met name beschikbaar gemaakt als het gekoppelde endpoint een reservering in de huidige tenant heeft. Zie [Tenanttoegang voor beveiligingsobjecten beheren in vRealize Automation](#) voor meer informatie over het beheer van toegang tot de tenancy.

U kunt meerdere netwerk- en beveiligingsonderdelen toevoegen aan het ontwerpcanvas.

Zie [NSX for vSphere-beveiligingsonderdelen gebruiken in een blueprint](#) voor meer informatie.

Voorwaarden

- Beveiligingstags maken en configureren voor NSX. Raadpleeg de NSX configuratiechecklist in *vRealize Automation configureren* en de *NSX for vSphere Administration Guide* in de [productdocumentatie voor NSX for vSphere](#).
- Controleer of de NSX-inventaris met succes is uitgevoerd voor uw cluster.
Als u NSX-configuraties in vRealize Automation wilt gebruiken, moet u gegevensverzameling uitvoeren.
- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Open een nieuwe of bestaande blueprint in het ontwerpcanvas met behulp van het tabblad **Ontwerpen**.

Procedure

- 1 Als u de lijst met beschikbare netwerk- en beveiligingsonderdelen wilt weergeven, klikt u op **Netwerk en beveiliging** in de sectie Categorieën.
- 2 Sleep een **Bestaande beveiligingstag**-onderdeel naar het ontwerpcanvas.
- 3 Klik in het tekstvak **Beveiligingstag** en selecteer een bestaande beveiligingstag.
- 4 Klik op **OK**.

- 5 Als u de blueprint wilt opslaan als concept of verder wilt gaan met het configureren van de blueprint, klikt u op **Opslaan** of **Voltooien**.

Resultaten

U kunt beveiligingsinstellingen toevoegen op het tabblad **Beveiliging** van een vSphere-machineonderdeel.

Het onderdeel beveiligingsgroep op aanvraag toevoegen

U kunt een NSX-beveiligingsgroeponderdeel op aanvraag aan het ontwerpcanvas van een blueprint toevoegen als u de bijbehorende instellingen wilt koppelen aan een of meer vSphere-machineonderdelen of andere beschikbare typen onderdelen van de blueprint.

Wanneer u een beveiligingsgroep op aanvraag wilt maken, moet u een beveiligingsbeleid toevoegen om de groep te maken. Het beveiligingsbeleid kan standaard worden weergegeven of verborgen. Beleidsregels worden alleen weergegeven in tenants waarvoor de gekoppelde NSX endpoint een reservering in die tenant heeft.

Standaard worden de beveiligingsgroepen die van toepassing zijn op de huidige tenant beschikbaar gesteld bij het ontwerpen van een blueprint. Met name worden beveiligingsgroepen beschikbaar gesteld als het gekoppelde endpoint een reservering in de huidige tenant heeft. Zie [Tenanttoegang voor beveiligingsobjecten beheren in vRealize Automation](#) voor meer informatie over het beheer van toegang tot de tenancy.

Voorwaarden

- Maak en configureer een beveiligingsbeleid in NSX. Zie *NSX Administration Guide*.
- Controleer of de NSX-inventaris met succes is uitgevoerd voor uw cluster.
Als u NSX-configuraties in vRealize Automation wilt gebruiken, moet u gegevensverzameling uitvoeren.
- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Controleer de concepten voor het beveiligingsonderdeel. Zie [NSX for vSphere-beveiligingsonderdelen gebruiken in een blueprint](#).
- Open een nieuwe of bestaande blueprint in het ontwerpcanvas met behulp van het tabblad **Ontwerpen**.

Procedure

- 1 Als u de lijst met beschikbare netwerk- en beveiligingsonderdelen wilt weergeven, klikt u op **Netwerk en beveiliging** in de sectie Categorieën.
- 2 Sleep een **Beveiligingsgroep op aanvraag**-onderdeel naar het ontwerpcanvas.
- 3 Voer een naam in en desgewenst een beschrijving.
- 4 Voeg beveiligingsbeleid toe door op het pictogram **Toevoegen** te klikken in het gedeelte **Beveiligingsbeleid** en het beschikbare beveiligingsbeleid te selecteren.
- 5 Klik op **OK**.

- 6 Als u de blueprint wilt opslaan als concept of verder wilt gaan met het configureren van de blueprint, klikt u op **Opslaan** of **Voltooien**.

Resultaten

U kunt beveiligingsinstellingen toevoegen op het tabblad **Beveiliging** van een vSphere-machineonderdeel.

NSX-T-beveiligingsonderdelen gebruiken in een blueprint

U kunt een NSX-T-netwerkbeveiligingsonderdeel aan het ontwerpcanvas toevoegen om de bijbehorende geconfigureerde instellingen beschikbaar te maken voor een of meer gekoppelde vSphere-machineonderdelen in de blueprint.

Met een bestaande NSX-T NS-groep kunt u resources toewijzen, zoals virtuele machines en netwerkadapters, voor gedistribueerde firewallbescherming.

U kunt beveiligingselementen aan blueprints toevoegen door NS-groepen te configureren voor de vSphere-computerresource in NSX-T. Nadat u gegevensverzameling hebt uitgevoerd, zijn de beveiligingsconfiguraties beschikbaar in vRealize Automation. U kunt een bestaand NSX-T NS-groepsonderdeel aan de blueprint toevoegen als bron of doel van een firewallregel.

NSX-T NS-beveiligingsgroepen worden buiten vRealize Automation beheerd in de toepassing NSX-T. Zie de productdocumentatie van NSX-T voor informatie over het beheren van NS-groepen.

De instellingen voor netwerk- en beveiligingsonderdelen die u aan de blueprint toevoegt, worden afgeleid van uw configuratie van NSX for vSphere en NSX-T. Raadpleeg de *Administration Guide* in de [NSX for vSphere-productdocumentatie](#) of [NSX-T-productdocumentatie](#), afhankelijk van welke toepassing u gebruikt, voor informatie over het configureren van NSX.

Wanneer u een blueprint implementeert die een NSX-T-endpoint bevat, wijst de implementatie een tag toe aan NSX-T-onderdelen in de implementatie. De naam van de tag en de naam van de implementatie komen overeen.

Als app-isolatie is ingeschakeld, wordt een nieuwe firewallsectie met regels gemaakt voor een implementatie. App-isolatie maakt gebruik van een logische firewall om alle inkomend en uitgaand verkeer naar en van de toepassingen in de blueprint, te blokkeren. Componentmachines die zijn voorzien van een blueprint die een app-isolatiebeleid bevat, kunnen met elkaar communiceren, maar kunnen geen verbinding maken buiten de firewall tenzij andere NS-groepen zijn toegevoegd aan de blueprint met beveiligingsregels die toegang toestaan.

Als een blueprint een load balancer bevat en app-isolatie is ingeschakeld, worden de load balancer-VIP's aan de app-isolatiebeveiligingsgroep toegevoegd als IPSet. Als een blueprint een beveiligingsgroep op aanvraag bevat die is gekoppeld aan een machinelaag die ook is gekoppeld aan een load balancer, bevat de beveiligingsgroep op aanvraag de machinelaag IPSet en VIP's.

Voor NSX-T is app-isolatie de enige aangemaakte NS-groep op aanvraag. Het bevat een IP-set die load balancer VIP's en externe IP-adressen van één-op-veel NAT-netwerken bevat.

Zie [Informatie over de NSX-T-implementatietopologieën voor netwerken, beveiliging en load balancer-configuraties](#) voor meer informatie over NSX-T-specifieke overwegingen met betrekking tot implementatie en topologie.

Een NSX-T NSGroup-onderdeel toevoegen

U kunt een bestaand NSX-T NSGroup-onderdeel toevoegen aan het ontwerpcanvas en de instellingen ervan configureren voor gebruik met vSphere-machineonderdelen en hun overige gekoppelde onderdelen, zoals software- en netwerkonderdelen.

Een NSX-T NSGroup kan een combinatie van IP-sets, MAC-sets, logische poorten, logische schakelopties en andere NSGroups bevatten. U kunt NSGroups opgeven als bronnen en bestemmingen in firewallregels. Voor meer informatie over eigenschappen van NSGroups raadpleegt u *Een NSGroup maken* in de *NSX-T Administration Guide* in de [productdocumentatie van NSX-T](#).

Opmerking De NSGroup-beveiliging wordt toegepast op VM's die verbonden zijn met ondoorzichtige netwerken die worden beheerd door NSX-T. Als een VM verbonden is met een vSphere dvPortGroup, is microsegmentatie niet beschikbaar voor dat netwerk.

Standaard worden NSGroups die van toepassing zijn op de huidige tenant beschikbaar gesteld wanneer u een blueprint maakt of bewerkt. Beveiligingsgroepen worden beschikbaar gesteld als het gekoppelde endpoint een reservering in de huidige tenant heeft. Zie [Tenanttoegang voor beveiligingsobjecten beheren in vRealize Automation](#) voor meer informatie over het beheer van toegang tot de tenancy.

Voorwaarden

- Maak en configureer een NSGroup in NSX-T. Zie [Checklist voor de voorbereiding van de netwerk- en beveiligingsconfiguratie van NSX](#).
- Controleer of de NSX-inventaris met succes is uitgevoerd voor uw cluster.
Als u NSX-configuraties in vRealize Automation wilt gebruiken, moet u gegevensverzameling uitvoeren.
- Controleer de concepten voor het beveiligingsonderdeel. Zie [NSX-T-beveiligingsonderdelen gebruiken in een blueprint](#).
- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Open een nieuwe of bestaande blueprint in het ontwerpcanvas met behulp van het tabblad **Ontwerpen**.

Procedure

- 1 Als u de lijst met beschikbare netwerk- en beveiligingsonderdelen wilt weergeven, klikt u op **Netwerk en beveiliging** in de sectie Categorieën.
- 2 Sleep een **NSX-T NSGroup**-onderdeel naar het ontwerpcanvas.
- 3 Selecteer een NSGroup in het vervolgkeuzemenu.

- 4 Voer desgevraagd een gekoppeld endpoint in.
- 5 Als u de blueprint wilt opslaan als concept of verder wilt gaan met het configureren van de blueprint, klikt u op **Opslaan** of **Voltooien**.

Resultaten

U kunt beveiligingsinstellingen toevoegen op het tabblad **Beveiliging** van een vSphere-machineonderdeel.

Netwerk- en beveiligingsonderdelen koppelen

U kunt netwerk- en beveiligingsonderdelen naar het ontwerpcanvas slepen om hun instellingen beschikbaar te maken voor de configuratie van machineonderdelen in de blueprint. Nadat u netwerk- en beveiligingsinstellingen voor de machine hebt opgegeven, kunt u optioneel instellingen van een load balancer-onderdeel koppelen.

Nadat u een NSX-netwerk- of -beveiligingsonderdeel aan het ontwerpcanvas hebt toegevoegd en de beschikbare instellingen ervan hebt gedefinieerd, kunt u de netwerk- en beveiligingstabbladen van een vSphere-machineonderdeel in het canvas openen en de instellingen ervan configureren.

U kunt een NAT-netwerkonderdeel op aanvraag naar het ontwerpcanvas slepen en aan het onderdeel vSphere-machine of het onderdeel NSX-load balancer in de blueprint koppelen.

De instellingen voor netwerk- en beveiligingsonderdelen die u aan de blueprint toevoegt, worden afgeleid van uw configuratie van NSX for vSphere en NSX-T. Raadpleeg de *Administration Guide* in de [NSX for vSphere-productdocumentatie](#) of [NSX-T-productdocumentatie](#), afhankelijk van welke toepassing u gebruikt, voor informatie over het configureren van NSX.

Opmerking Als een blueprint een load balancer bevat en app-isolatie is ingeschakeld, worden de load balancer-VIP's aan de app-isolatiebeveiligingsgroep toegevoegd als IPSet. Als een blueprint een beveiligingsgroep op aanvraag bevat die is gekoppeld aan een machinelaag die ook is gekoppeld aan een load balancer, bevat de beveiligingsgroep op aanvraag de machinelaag IPSet en VIP's.

Zie [NAT-regels maken en gebruiken voor NSX for vSphere](#) of [NAT-regels maken en gebruiken voor NSX-T](#) voor informatie over het gebruik van NAT-regels om te zorgen dat een TCP- of UDP-poort kan worden toegewezen vanaf het externe IP-adres van een Edge (bronpoort) aan een particulier IP-adres in het NAT-netwerkonderdeel (de doelpoort).

Zie [Informatie over de NSX-T-implementatietopologieën voor netwerken, beveiliging en load balancer-configuraties](#) voor meer informatie over NSX-T-specifieke overwegingen met betrekking tot implementatie en topologie.

Een blueprint configureren om in te richten vanaf een OVF

U kunt een OVF gebruiken voor het definiëren van de eigenschappen en hardware-instellingen van vSphere-machines die normaal gesproken op de blueprintconfiguratiepagina's in vRealize Automation worden gedefinieerd of via een programmering met behulp van vRealize Automation REST API's of vRealize CloudClient.

U kunt ook instellingen importeren vanuit een OVF om een waardeset voor een onderdeelprofiel van een image te definiëren. Blueprints met parameters gebruiken de onderdeelprofielen voor image en grootte.

OVF is een open source standaard voor het inpakken en distribueren van softwaretoepassingen voor virtual machines.

OVF-inrichting is vergelijkbaar met klonen, behalve dat de machinebron een OVF-sjabloon is die wordt gehost op een server of een website en geen sjabloon voor virtual machines die wordt gehost in vCenter.

Een OVF-bestand wordt doorgaans gebruikt om een afzonderlijke virtual machine of virtual appliance te beschrijven. Het kan informatie bevatten over de indeling van het imagebestand van een virtuele schijf en een beschrijving van de virtuele hardware die moet worden geëmuleerd voor het uitvoeren van het besturingssysteem of de applicatie op de image. Een OVA-bestand is een virtual appliance-pakket met bestanden die een virtual machine beschrijven, zoals een OVF-descriptorbestand, optionele manifest- en certificaatbestanden, en andere bijbehorende bestanden.

De optionele `ImportOvfWorkflow`-inrichting is beschikbaar voor een vSphere-machineonderdeel wanneer u een blueprint definieert. De optie is ook beschikbaar als u een waardeset voor een onderdeelprofiel van een image definieert in het eigenschappenwoordenboek.

U kunt blueprintconfiguratie-instellingen toevoegen aan een OVF ter beschrijving van de volgende typen informatie:

- Minimale CPU, geheugen en opslagtoewijzingen.
- Door de gebruiker configureerbare aangepaste eigenschappen.
- Onderdeelprofielinstellingen voor parameterisering van blueprints.

OVF en OVA met meerdere machines wordt niet ondersteund.

Belangrijke overwegingen zijn onder andere de volgende bepalingen:

- OVF-bestanden en OVA-pakketten worden ondersteund.
- Basisverificatie met gebruikersnaam en wachtwoord voor de HTTP-server waarop zich het gehoste OVF- of OVA-bestand bevindt, wordt ondersteund. De opgegeven URL wordt gevalideerd in de blueprint.
- Gegevens van OVF's en OVA's worden niet verzameld van de vCenter Server.
- EBS-abonnementen worden ondersteund.
- U kunt aangepaste eigenschappen definiëren wanneer u door de gebruiker instelbare OVF-instellingen in de blueprint importeert.
- U kunt de instellingen die zijn opgehaald uit een OVF-import toevoegen, wijzigen of verwijderen wanneer u de vSphere machine-inrichting aanvraagt.
- U kunt instellingen toevoegen, wijzigen of verwijderen bij een herconfiguratie van een machine.

Blueprintinstellingen definiëren voor een vSphere-onderdeel met behulp van een OVF-bestand

U kunt instellingen importeren van een OVF om het proces voor het configureren van instellingen voor vSphere-machineonderdelen in een vRealize Automation-blueprint te vereenvoudigen.

Bij deze procedure wordt ervan uitgegaan dat u een elementaire kennis hebt van het proces voor het maken van vRealize Automation-blueprints.

Voorwaarden

- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Voldoen aan de resterende vereisten die worden opgegeven in [Een machineblueprint configureren](#).

Procedure

- 1 Selecteer **Ontwerpen > Blueprints**.
- 2 Klik op het pictogram **Nieuw (+)**.
- 3 Voer een naam en beschrijving voor de blueprint in en klik op **OK**.
- 4 Klik op **Machinetypen** in het gebied Categorieën en sleep een **vSphere (vCenter)-machine**onderdeel naar het ontwerpcanvas.
- 5 Klik op het tabblad **Versie-informatie** en geef de volgende opties op:
 - **Blueprinttype:** Server
 - **Actie:** Maken
 - **Inrichtingswerkstroom:** ImportOvfWorkflow

Met de ImportOvfWorkflow-instelling wordt de **URL**-optie beschikbaar.

The screenshot shows the 'Design Canvas' interface. A 'vSphere (vCenter)' machine component is being added to the canvas. The configuration panel for this component is open, displaying the 'Build Information' tab. The 'Blueprint type' is set to 'Server', the 'Action' is 'Create', and the 'Provisioning workflow' is 'ImportOvfWorkflow'. The 'URL' field is highlighted with an orange box, and the 'CONF...' button is visible next to it. Other options like 'Authentication needed' and 'Use proxy' are also present.

- 6 Geef de locatie van het OVF-bestand op.
 - Gebruik de indeling `https://server/mapnaam.ovf` of de `naam.ova` om het pad naar de OVF-URL in te voeren.

Als u verificatie inschakelt voor de server die als OVF-host fungeert, voert u de verificatiegegevens in waarmee de gebruiker wordt geverifieerd.

- Als een OVF wordt gehost op een website en u een proxyendpoint hebt gemaakt om de website te openen, selecteert u **Proxy gebruiken** en selecteert u het beschikbare proxyendpoint.

7 Klik op **Configureren**.

Opmerking Als u een verificatiefoutbericht ontvangt, zijn verificatiegegevens vereist voor de server waarop het OVF wordt gehost. Als dit gebeurt, schakelt u het selectievakje **Verificatie vereist** in, voert u de verificatiegegevens voor **Gebruikersnaam** en **Wachtwoord** in die vereist zijn voor verificatie met de HTTP-server waarop het OVF zich bevindt en klikt u opnieuw op **Configureren**.

Met de optie Configureren opent u een wizard waarin alle door de gebruiker instelbare eigenschappen en waarden voor het importeren van een OVF beschikbaar zijn als aangepaste eigenschappen. Als er geen configureerbare eigenschappen zijn om te importeren, is het deelvenster leeg.

- a Gebruik de wizard om ofwel de standaardwaarden die moeten worden geïmporteerd, te accepteren of deze waarden te wijzigen voor de blueprint voordat u het importeren start.
- b Klik op **OK** om de eigenschappen en waarden te importeren.

Alle door gebruikers instelbare eigenschappen in de OVF-sjabloon worden in de blueprint geïmporteerd als bewerkbare aangepaste eigenschappen voor vRealize Automation, voorafgegaan door VMware.Ovf, terwijl andere worden geïmporteerd als verborgen eigenschappen die niet moeten worden bewerkt na het importeren.

- 8 Klik op het tabblad **Machinebronnen** om de resultaten van de OVF-import weer te geven die worden opgenomen in de minimumwaardevermeldingen voor de opties **CPU's**, **Geheugen (MB)** en **Opslag (GB)**.

U kunt deze waarden wijzigen na het importeren.

- 9 Klik op het tabblad **Opslag** om de resultaten van de OVF-import weer te geven.
- 10 Klik op de tabbladreeks **Eigenschappen > Aangepaste eigenschappen** om de resultaten van de OVF-import weer te geven.
- 11 Klik op **Opslaan**.

Wat nu te doen

Ga verder met het definiëren van blueprintinstellingen of klik op **Voltooien**.

Een imagewaardeset voor een onderdeelprofiel definiëren met behulp van een OVF

U kunt instellingen uit een OVF importeren om een of meer waardesets te maken voor een imageonderdeelprofiel dat u wilt gebruiken in een vRealize Automation-blueprint met parameters.

Nadat u waardesetdefinities voor het Image-onderdeelprofiel hebt geïmporteerd, kunt u een of meer waardesets aan het onderdeelprofiel toevoegen voor een vSphere-machineonderdeel in een blueprint. Wanneer een gebruiker een catalogusitem aanvraagt, kan deze een beschikbare Image selecteren en implementeren met behulp van de parameters die zijn gedefinieerd in de waardeset van de image.

Wanneer u een OVF importeert, worden de door gebruikers instelbare eigenschappen en waarden van het OVF-bestand niet als aangepaste eigenschappen in de waardeset geïmporteerd. Als u nieuwe aangepaste eigenschappen van het geïmporteerde OVF voor de imagewaardeset wilt gebruiken, moet u de nieuwe aangepaste eigenschappen handmatig definiëren in het vSphere-machineonderdeel of de algemene blueprint. De aangepaste eigenschappen in de blueprint met parameters zijn dan van toepassing op de waardeset van elke onderdeelprofielimage.

Opmerking De aangepaste OVF-eigenschappen voor vRealize Automation zijn niet van toepassing op aangepaste OVF-eigenschappen voor vSphere. U kunt eventueel ook een imagewaardeset maken voor vRealize Automation en een voor vSphere.

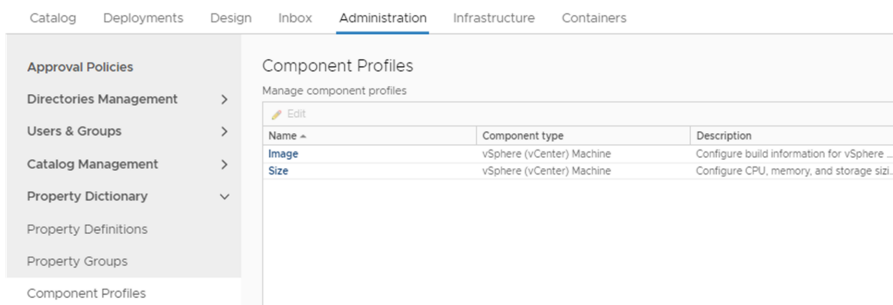
Zie [Het toewijzen van parameters aan blueprints begrijpen en gebruiken](#) voor meer informatie over het gebruik van onderdeelprofielen voor parameterisering van blueprints.

Voorwaarden

- Meld u aan bij vRealize Automation als een beheerder met de toegangsrechten voor **tenantbeheerder** en **laaS-beheerder**.

Procedure

- 1 Selecteer **Beheer > Woordenboek voor eigenschappen > Onderdeelprofielen**.



- 2 Klik op **Image** in de kolom Naam.

Er wordt informatie over de geboden eigenschap van het image-onderdeel weergegeven.

- 3 Klik op het tabblad **Waardesets**.

- 4 Als u een nieuwe waardeset wilt definiëren, klikt u op **Nieuw** en configureert u de Image-instellingen.
 - a Voer in het veld **Weergavenaam** een waarde in om aan het scheidingsteken ValueSet toe te voegen, bijvoorbeeld **ProdOVF**.
 - b Accepteer de standaardwaarde die wordt weergegeven in het tekstvak **Naam** of voer een aangepaste naam in.
 - c Voer in het tekstvak **Beschrijving** een beschrijving in zoals **Versie-instellingen voor kloonscenario A**.
 - d Selecteer **Actief** of **Inactief** in het vervolgkeuzemenu **Status**.
 Selecteer **Actief** om de waardeset zichtbaar te maken in het aanvraagformulier voor catalogusinrichting.
 - e Selecteer de versie-actie **Maken**.
 - f Selecteer **Server** of **Desktop** als blueprinttype.
 - g Selecteer de inrichtingswerkstroom **ImportOvfWorkflow**.
 - h Gebruik de indeling `https://server/mapnaam.ovf` of de `naam.ova` om het pad naar de OVF-URL in te voeren.
 - i Als u verificatie inschakelt voor de server die als OVF-host fungeert, voert u de verificatiegegevens in waarmee de gebruiker wordt geverifieerd.
 - j Als een OVF wordt gehost op een website en u een proxyendpoint hebt gemaakt om de website te openen, selecteert u **Proxy gebruiken** en selecteert u het beschikbare proxyendpoint.
- 5 Klik op **Opslaan**.
- 6 Klik op **Voltooien** wanneer u tevreden bent met uw instellingen.

Wat nu te doen

Nadat u de image hebt gemaakt en het OVF-bestand waarmee de imagewaardeset wordt gedefinieerd, hebt geïmporteerd, kunt u de image toevoegen aan een vSphere-machineonderdeel in een blueprint.

Containeronderdelen gebruiken in blueprints

U kunt containeronderdelen configureren en gebruiken in een blueprint.

Wanneer de containerbeheerder containers heeft gedefinieerd in Containers voor vRealize Automation, kan een containerarchitect containeronderdelen voor vRealize Automation-blueprints toevoegen en configureren in het ontwerpcanvas.

Instellingen voor containeronderdelen

U kunt blueprintinstellingen en -opties configureren voor een Containers voor vRealize Automation-containeronderdeel in het ontwerpcanvas van vRealize Automation.

Tabblad **Algemeen**

Configureer op het ontwerpcanvas algemene instellingen voor het containeronderdeel van de blueprint.

Tabel 3-33. Instellingen tabblad **Algemeen**

Instelling	Beschrijving
Naam	Voer een naam in voor het containeronderdeel op de blueprint.
Beschrijving	Vat uw containeronderdeel samen ten behoeve van andere architecten.
Image	Voer de volledige naam in van een image in een beheerd register, zoals een particulier register of Docker Hub-register. Bijvoorbeeld <code>registry.hub.docker.com/library/python</code> .
Opdrachten	Voer een opdracht in voor de opgegeven image, zoals <code>python app.py</code> . De opdracht wordt uitgevoerd wanneer het inrichtingsproces voor de container wordt gestart.
Koppelingen	U kunt ook koppelingen gebruiken om containers op een of meerdere hosts met elkaar te verbinden. Geef op met welke service(s), zoals redis of datadog, u deze container wilt koppelen.

Tabblad **Netwerk**

Configureer op het ontwerpcanvas netwerkinstellingen voor het containeronderdeel van de blueprint.

U kunt een container aan een netwerk koppelen. Het netwerk wordt als een containernetwerkonderdeel weergegeven op het ontwerpcanvas. De informatie over de beschikbare netwerken wordt opgegeven op de netwerkpagina van het containeronderdeelformulier.

Tabel 3-34. Instellingen tabblad **Netwerk**

Instelling	Beschrijving
Netwerken	Geef de bestaande netwerken op die zijn gedefinieerd voor de geselecteerde image. U kunt ook een nieuw netwerk maken. Als u een netwerkcontaineronderdeel toevoegt aan het ontwerpformulier, worden de opgegeven netwerken hier als beschikbaar weergegeven.
Poortbindingen	Geef de poortbindingen van het geselecteerde netwerk op. Poortbindingen bestaan uit een protocolhost, hostpoort en containerpoort.
Alle poorten publiceren	Schakel het selectievakje in om de poorten die in de containerimage worden gebruikt, beschikbaar te stellen voor alle gebruikers.

Tabel 3-34. Instellingen tabblad **Netwerk** (vervolg)

Instelling	Beschrijving
Hostnaam	Geef de hostnaam van de container op. Als u geen naam opgeeft, wordt standaard de naam ingesteld van het containeronderdeel in de blueprint.
Netwerkmodus	Geef de netwerkstack van de container op. Als u geen waarde opgeeft, wordt bridging als netwerkmodus voor de container ingesteld.

Tabblad **Opslag**

Configureer de opslaginstellingen voor het containeronderdeel in de blueprint op het ontwerpcanvas.

Tabel 3-35. Instellingen tabblad **Opslag**

Instellingen	Beschrijving
Volumes	Bepaal welke opslagvolumes die worden toegewezen door de host, mogen worden gebruikt door de container.
Volumes van	Bepaal welke opslagvolumes worden overgenomen van een andere container.
Werkdirectory	Geef op vanuit welke directory de opdrachten worden uitgevoerd.

Tabblad **Beleid**

Configureer beleidsinstellingen zoals implementatiebeleid en affiniteitsbeperkingen voor het containeronderdeel op het ontwerpcanvas.

Tabel 3-36. Instellingen tabblad **Beleid**

Instellingen	Beschrijving
Implementatiebeleid	Kies een implementatiebeleid om te bepalen welke specifieke hosts bij voorkeur worden gebruikt bij de implementatie van deze container. U kunt implementatiebeleidsregels aan specifieke hosts koppelen en andere beleidsregels en containerdefinities maken om een voorkeur voor bepaalde hosts, beleidsregels en quota in te stellen wanneer u een container implementeert. U kunt een implementatiebeleid toevoegen met behulp van het tabblad Containers in vRealize Automation.
Clustergrootte	Bepaal hoeveel instanties van deze container als een cluster worden gegenereerd.
Beleid opnieuw starten	Geef een beleid voor opnieuw starten op voor de manier waarop een container opnieuw moet worden opgestart na het afsluiten.
Max opnieuw starten	Als u indien mislukt hebt geselecteerd als beleid voor opnieuw starten, kunt u het maximum aantal pogingen voor opnieuw starten opgeven.

Tabel 3-36. Instellingen tabblad **Beleid** (vervolg)

Instellingen	Beschrijving
CPU-delingen	Geef op hoeveel CPU-delingen worden toegewezen voor de ingerichte bron.
Geheugenlimiet	Geef een getal op tussen 0 en het beschikbare geheugen van de plaatsingszone. Dit is het totale beschikbare geheugen voor de bronnen in deze plaatsing. 0 betekent geen limiet.
Geheugen wisselen	Totale geheugenlimiet.
Affiniteitsbeperkingen	<p>Definieert regels voor de inrichting van containers op dezelfde of verschillende hosts.</p> <ul style="list-style-type: none"> ■ Affiniteitstype <p>Bij een anti-affiniteit worden de containers op verschillende hosts geplaatst. Anders worden ze op dezelfde host geplaatst.</p> ■ Service <p>De naam van de service in het vervolgkeuzemenu komt overeen met de naam van het containeronderdeel dat u hebt opgegeven in het veld Naam op het tabblad Algemeen.</p> ■ Beperking <p>Een harde beperking betekent dat de inrichting mislukt wanneer niet aan de beperking wordt voldaan. Een zachte beperking betekent dat de inrichting doorgaat wanneer niet aan de beperking wordt voldaan.</p>

Tabblad **Omgeving**

Configureer omgevingsinstellingen zoals eigenschapsbindingen voor het containeronderdeel in de blueprint op het ontwerpcanvas.

Tabel 3-37. Instellingen tabblad **Omgeving**

Instelling	Beschrijving
Naam	De naam van de variabele.
Binding	Bind de variabele aan een andere eigenschap die deel uitmaakt van de sjabloon. Wanneer u binding selecteert, moet u een waarde invoeren in de syntaxis <i>_resource~TemplateComponent~TemplateComponentProperty</i> .
Waarde	De waarde van de omgevingsvariabele of als u binding hebt geselecteerd, de waarde van de eigenschap die u wilt binden.

Tabblad **Eigenschappen**

Configureer omgevingsinstellingen zoals eigenschapsbindingen voor het containeronderdeel op het ontwerpcanvas.

Als u het tabblad **Eigenschapsgroepen** selecteert en op **Toevoegen** klikt, zijn de volgende opties beschikbaar:

- Eigenschappen voor containerhosts met certificaatverificatie
- Eigenschappen voor containerhosts met verificatie op basis van gebruikers/wachtwoorden

Overige eigenschapsgroepen die eventueel zijn gedefinieerd, worden ook weergegeven.

Als u het tabblad **Aangepaste eigenschappen** selecteert en op **Toevoegen** klikt, kunt u afzonderlijke aangepaste eigenschappen toevoegen aan het containeronderdeel.

Tabel 3-38. Instellingen voor aangepaste eigenschappen op het tabblad Eigenschappen

Instelling	Beschrijving
Naam	Voer de naam van de aangepaste eigenschap in of selecteer een beschikbare aangepaste eigenschap in het vervolgkeuzemenu.
Waarde	Typ of bewerk de waarde die u wilt koppelen aan de naam van de aangepaste eigenschap.
Versleuteld	U kunt ervoor kiezen om de eigenschapswaarde te coderen, bijvoorbeeld als de waarde een wachtwoord is.
Overschrijfbaar	U kunt opgeven dat de eigenschapswaarde kan worden overschreven door de volgende persoon of hierop volgende persoon die de eigenschap gebruikt. Dit is normaal gesproken een andere architect, maar als u Weergeven in aanvraag selecteert, kunnen uw zakelijke gebruikers eigenschapswaarden weergeven en bewerken wanneer ze catalogusitems aanvragen.
Weergeven in aanvraag	Als u de eigenschapsnaam en -waarde aan uw eindgebruikers wilt tonen, kunt u ervoor kiezen om de eigenschap op het aanvraagformulier weer te geven bij aanvragen voor het inrichten van machines. U moet ook Overschrijfbaar selecteren als u wilt dat gebruikers een waarde opgeven.

Tabblad Statusconfig

Configureer een statusconfiguratiemodus voor het containeronderdeel van de blueprint op het ontwerpcanvas.

Tabel 3-39. Instellingen op tabblad **Statusconfig**

Modusinstelling	Beschrijving
Geen	Standaard. Er worden geen statuscontroles geconfigureerd.
HTTP	<p>Als u HTTP selecteert, moet u opgeven welke API en HTTP-methode en -versie worden gebruikt. De API is relatief en u hoeft het adres van de container niet op te geven. U kunt ook een time-outperiode voor de bewerking opgeven en statusdrempels instellen.</p> <p>Een statusdrempel van 2 betekent bijvoorbeeld dat er twee opeenvolgende aanroepen moeten lukken voordat de container in orde wordt bevonden en de status RUNNING krijgt. Evenzo moeten er bij een statusdrempel van 2 twee opeenvolgende aanroepen mislukken voordat de container niet in orde wordt bevonden en de status ERROR krijgt. Bij elke tussenliggende drempel tussen de status in orde en niet in orde krijgt de container de status DEGRADED.</p>
TCP-verbinding	Als u TCP-verbinding selecteert, moet u een poort opgeven voor de container. De statuscontrole probeert via de opgegeven poort een TCP-verbinding te maken met de container. U kunt ook een time-out voor de bewerking opgeven en drempels voor de status in orde en niet in orde instellen.
Opdracht	Als u Opdracht selecteert, moet u een opdracht opgeven die u wilt uitvoeren voor de container. Het resultaat van de statuscontrole wordt bepaald door de status waarmee de opdracht wordt afgesloten.
Statuscontrole bij inrichten negeren	Schakel dit selectievakje uit om de statuscontrole bij het inrichten af te dwingen. Hierdoor wordt een container pas beschouwd als ingericht nadat een statuscontrole met succes is voltooid.
Automatisch implementeren	Automatische herimplementatie van containers wanneer deze de status FOUT hebben.

Tabblad **Logconfig**

Configureer een logmodus en andere logboekopties voor het containeronderdeel op het ontwerpcanvas.

Tabel 3-40. Instellingen op tabblad **Logconfig**

Instelling	Beschrijving
Stuurprogramma	Selecteer een logboekindeling in het vervolgkeuzemenu.
Opties	Voer opties voor het stuurprogramma in op basis van dezelfde naam- en waarde-indeling als de logboekindeling.

Containereigenschappen en eigenschapsgroepen in een blueprint gebruiken

U kunt vooraf gedefinieerde eigenschapsgroepen toevoegen aan een onderdeel met containers in een vRealize Automation-blueprint. Wanneer machines worden ingericht met behulp van een blueprint die deze eigenschappen bevat, wordt de ingerichte machine geregistreerd als een Docker-containerhostmachine.

Containers voor vRealize Automation heeft de volgende twee eigenschapsgroepen van containerspecifieke, aangepaste eigenschappen geleverd. Wanneer u een containeronderdeel toevoegt aan een blueprint, kunt u deze eigenschapsgroepen toevoegen aan de container om ingerichte machines te registreren als containerhosts.

- Eigenschappen voor containerhosts met certificaatverificatie
- Eigenschappen voor containerhosts met verificatie op basis van gebruikers/wachtwoorden

Deze eigenschapsgroepen zijn zichtbaar in vRealize Automation wanneer u **Beheer > Woordenboek voor eigenschappen > Eigenschapsgroepen** selecteert.

Omdat eigenschapsgroepen worden gedeeld door alle tenants, kunt u, als u in een omgeving met meerdere tenants werkt, overwegen om uw eigenschappen te klonen en aan te passen. Door eigenschapsgroepen en eigenschappen in groepen een unieke naam te geven, kunt u deze bewerken om aangepaste waarden te definiëren voor gebruik in een specifieke tenant.

De meest gebruikte eigenschappen zijn `Container.Auth.PublicKey` en `Container.Auth.PrivateKey` waarbij de containerbeheerder het clientcertificaat opgeeft voor verificatie met de containerhost.

Tabel 3-41. Containers Aangepaste eigenschappen

Eigenschap	Beschrijving
<code>containers.ipam.driver</code>	Uitsluitend voor gebruik met containers Hiermee wordt het IPAM-stuurprogramma opgegeven dat wordt gebruikt wanneer een netwerkonderdeel Containers wordt toegevoegd aan een blueprint. De ondersteunde waarden zijn afhankelijk van de stuurprogramma's die zijn geïnstalleerd in de hostomgeving van de container waar ze worden gebruikt. Een ondersteunde waarde kan bijvoorbeeld <code>infoblox</code> of <code>calico</code> zijn, afhankelijk van de IPAM-invoegtoepassingen die zijn geïnstalleerd op de host van de container.
<code>containers.network.driver</code>	Uitsluitend voor gebruik met containers Hiermee wordt het netwerkstuurprogramma opgegeven dat wordt gebruikt wanneer een netwerkonderdeel Containers wordt toegevoegd aan een blueprint. De ondersteunde waarden zijn afhankelijk van de stuurprogramma's die zijn geïnstalleerd in de hostomgeving van de container waar ze worden gebruikt. De door Docker geleverde netwerkstuurprogramma's omvatten de stuurprogramma's <code>bridge</code> , <code>overlay</code> en <code>macvlan</code> , terwijl in de door Virtual Container Host (VCH) geleverde stuurprogramma's het stuurprogramma <code>bridge</code> is opgenomen. Netwerkstuurprogramma's van derden, zoals <code>weave</code> en <code>calico</code> , zijn mogelijk ook beschikbaar, afhankelijk van de netwerkinvoegtoepassingen die zijn geïnstalleerd op de host van de container.
<code>Container</code>	Uitsluitend voor gebruik met containers De standaardwaarde is <code>App.Docker</code> en dit is een vereiste waarde. Wijzig deze eigenschap niet.
<code>Container.Auth.User</code>	Uitsluitend voor gebruik met containers Hiermee wordt de gebruikersnaam opgegeven om verbinding te maken met de host van Containers.
<code>Container.Auth.Password</code>	Uitsluitend voor gebruik met containers Hiermee wordt het wachtwoord voor de gebruikersnaam opgegeven of het wachtwoord van de openbare of persoonlijke sleutel dat moet worden gebruikt. Versleuteling van de eigenschapswaarde wordt ondersteund.
<code>Container.Auth.PublicKey</code>	Uitsluitend voor gebruik met containers Hiermee wordt de openbare sleutel opgegeven om verbinding te maken met de host van Containers.
<code>Container.Auth.PrivateKey</code>	Uitsluitend voor gebruik met containers Hiermee wordt de persoonlijke sleutel opgegeven om verbinding te maken met de host van Containers. Versleuteling van de eigenschapswaarde wordt ondersteund.
<code>Container.Connection.Protocol</code>	Uitsluitend voor gebruik met containers Hiermee wordt het communicatieprotocol opgegeven. De standaardwaarde is <code>API</code> en dit is een vereiste waarde. Wijzig deze eigenschap niet.

Tabel 3-41. Containers Aangepaste eigenschappen (vervolg)

Eigenschap	Beschrijving
Container.Connection.Scheme	Uitsluitend voor gebruik met containers Hiermee wordt het communicatieschema opgegeven. De standaardwaarde is https.
Container.Connection.Port	Uitsluitend voor gebruik met containers Hiermee wordt de verbindingspoort voor Containers opgegeven. De standaardwaarde is 2376.
Extensibility.Lifecycle.Properties.VMPSMasterWorkf low32.MachineActivated	Uitsluitend voor gebruik met containers Hiermee wordt opgegeven dat de eigenschap gebeurtenisbroker alle eigenschappen van Containers beschikbaar moet maken en dat deze wordt gebruikt voor het registreren van een ingerichte host. De standaardwaarde is Container* en dit is een vereiste waarde. Wijzig deze eigenschap niet.
Extensibility.Lifecycle.Properties.VMPSMasterWorkf low32.Disposing	Uitsluitend voor gebruik met containers Hiermee wordt opgegeven dat de eigenschap gebeurtenisbroker alle bovenstaande eigenschappen van Containers beschikbaar moet maken en dat deze wordt gebruikt voor het ongedaan maken van de registratie van een ingerichte host. De standaardwaarde is Container* en dit is een vereiste waarde. Wijzig deze eigenschap niet.

Containers Netwerkonderdelen gebruiken in het ontwerpcanvas

U kunt een of meer Containers-netwerkonderdelen aan het ontwerpcanvas toevoegen en de bijbehorende instellingen voor vSphere-machineonderdelen in de blueprint configureren.

U kunt de `containers.ipam.driver` en `containers.network.driver` toevoegen aan het onderdeel wanneer u deze aan de blueprint toevoegt.

Het onderdeel Containernetwerk toevoegen

U kunt gegevens voor containernetwerken toevoegen aan een vRealize Automation-blueprint die containeronderdelen bevat.

U kunt containers in Containers voor vRealize Automation configureren met behulp van het tabblad vRealize Automation **Containers**. U kunt die containers en hun netwerkinstellingen als onderdelen van een blueprint toevoegen met behulp van opties op het tabblad vRealize Automation **Ontwerpen**.

Voorwaarden

- Meld u aan bij vRealize Automation als een **containerarchitect**.
- Open een nieuwe of bestaande blueprint in het ontwerpcanvas met behulp van het tabblad **Ontwerpen**.

Procedure

- 1 Als u de lijst met beschikbare netwerk- en beveiligingsonderdelen wilt weergeven, klikt u op **Netwerk en beveiliging** in de sectie Categorieën.

- 2 Sleep een **Containernetwerk**-onderdeel naar het ontwerpcanvas.
- 3 Als u het onderdeel een uniek label wilt geven in het ontwerpcanvas, voert u in het tekstvak **Naam** een naam in.
- 4 (Optioneel) Typ een beschrijving van het onderdeel in het tekstvak **Beschrijving**.
- 5 (Optioneel) Schakel het selectievakje **Extern** in als u geen externe IPAM-instellingen wilt opgeven.

Als u het selectievakje **Extern** inschakelt, wordt het tabblad **IPAM-configuratie** verwijderd.

- 6 Klik op het tabblad **IPAM-configuratie** om een subnet, IP-bereik en gateway in te stellen of te bewerken voor het netwerk dat is opgegeven in een containeronderdeel op de blueprint.

De IPAM-configuratie heeft betrekking op nieuwe netwerken die met vRealize Automation worden gemaakt, niet voor oudere netwerken die zijn gemaakt in Docker of andere ondersteunde containertoepassingen. Deze instellingen worden niet gevalideerd en de inrichting mislukt als er overlappende instellingen met andere netwerken zijn. Het subnet en de gateway van de containerhost moeten bijvoorbeeld uniek zijn.

- 7 Klik op het tabblad **Eigenschappen** om aangepaste eigenschappen voor het onderdeel op te geven.

Als u het tabblad **Eigenschapsgroepen** selecteert en op **Toevoegen** klikt, zijn de volgende opties beschikbaar:

- Eigenschappen voor containerhosts met certificaatverificatie
- Eigenschappen voor containerhosts met verificatie op basis van gebruikers/wachtwoorden

Overige eigenschapsgroepen die eventueel zijn gedefinieerd, worden ook weergegeven.

Als u het tabblad **Aangepaste eigenschappen** selecteert en op **Toevoegen** klikt, kunt u afzonderlijke aangepaste eigenschappen toevoegen aan het containeronderdeel.

Tabel 3-42. Instellingen voor aangepaste eigenschappen op het tabblad **Eigenschappen**

Instelling	Beschrijving
Naam	Voer de naam van de aangepaste eigenschap in of selecteer een beschikbare aangepaste eigenschap in het vervolgkeuzemenu.
Waarde	Typ of bewerk de waarde die u wilt koppelen aan de naam van de aangepaste eigenschap.
Versleuteld	U kunt ervoor kiezen om de eigenschapswaarde te coderen, bijvoorbeeld als de waarde een wachtwoord is.

Tabel 3-42. Instellingen voor aangepaste eigenschappen op het tabblad **Eigenschappen** (vervolg)

Instelling	Beschrijving
Overschrijfbaar	U kunt opgeven dat de eigenschapswaarde kan worden overschreven door de volgende persoon of hierop volgende persoon die de eigenschap gebruikt. Dit is normaal gesproken een andere architect, maar als u Weergeven in aanvraag selecteert, kunnen uw zakelijke gebruikers eigenschapswaarden weergeven en bewerken wanneer ze catalogusitems aanvragen.
Weergeven in aanvraag	Als u de eigenschapsnaam en -waarde aan uw eindgebruikers wilt tonen, kunt u ervoor kiezen om de eigenschap op het aanvraagformulier weer te geven bij aanvragen voor het inrichten van machines. U moet ook Overschrijfbaar selecteren als u wilt dat gebruikers een waarde opgeven.

- 8 Als u de blueprint wilt opslaan als concept of verder wilt gaan met het configureren van de blueprint, klikt u op **Opslaan** of **Voltooien**.

Wat nu te doen

U kunt containernetwerkinstellingen toevoegen op het tabblad **Network** van een containeronderdeel.

Sjablonen voor containers pushen voor gebruik in blueprints

U kunt een sjabloon voor een container beschikbaar maken voor gebruik in een vRealize Automation-blueprint.

Een sjabloon voor een container kan meerdere containers bevatten. Wanneer u een sjabloon met meerdere containers pusht naar vRealize Automation, wordt het sjabloon gemaakt als een blueprint met meerdere containers in vRealize Automation.

De containerspecifieke eigenschappen die u toevoegt aan het sjabloon voor containers, worden als zodanig herkend in de vRealize Automation-blueprint. Zie [Containereigenschappen en eigenschapsgroepen in een blueprint gebruiken](#).

Wanneer u de inrichting aanvraagt van een blueprint die is gepubliceerd in de vRealize Automation-catalogus, richt u de broncontainertoepassing voor die blueprint in.

U kunt andere onderdelen toevoegen aan de vRealize Automation-blueprint, inclusief de volgende onderdeeltypen:

- Machinetypen
- Softwareonderdelen
- Andere blueprints
- NSX-netwerkonderdelen en -beveiligingsonderdelen
- Onderdelen van XaaS

■ Aangepaste onderdelen

U kunt een sjabloon van Containers naar vRealize Automation pushen. Wijzigingen die u aanbrengt in de vRealize Automation-blueprint, hebben geen effect op de sjabloon voor Containers.

U kunt vervolgens wijzigingen aanbrengen in de sjabloon voor Containers en deze opnieuw pushen om de blueprint in vRealize Automation te overschrijven. Door de sjabloon naar vRealize Automation te pushen, wordt de blueprint overschreven en gaan alle wijzigingen verloren die in de blueprint in vRealize Automation zijn aangebracht tussen de twee pushbewerkingen. Als u wilt vermijden dat de wijzigingen in de blueprint verloren gaan, gebruikt u vRealize CloudClient om de blueprint te klonen of exporteert u de blueprint.

Een Docker-container of -host inrichten op basis van een blueprint

U kunt vRealize Automation-blueprints maken en gebruiken om machines in te richten als geregistreerde Docker Container-hosts.

Voordat een ingerichte machine kan worden geregistreerd als een host van een container, moet deze aan de volgende vereisten voldoen:

- De machine wordt ingericht met behulp van een blueprint die Containers-specifieke aangepaste eigenschappen bevat.

De vereiste containerspecifieke aangepaste eigenschappen worden geleverd door twee eigenschapsgroepen. Zie [Containereigenschappen en eigenschapsgroepen in een blueprint gebruiken](#).

Raadpleeg voor meer informatie over het gebruik van aangepaste eigenschappen en eigenschapsgroepen in vRealize Automation, *Naslaggids voor aangepaste eigenschappen*.

- De machine is toegankelijk via het netwerk.

De machine moet dan beschikken over een geldig IP-adres en zijn ingeschakeld.

U kunt in de definitie van een vRealize Automation-blueprint opnemen dat de machine specifieke aangepaste eigenschappen bevat waardoor deze als een host voor containers wordt aangemerkt wanneer u de machine inricht met behulp van de blueprint.

Wanneer een machine met de vereiste blueprinteigenschappen met succes is ingericht, wordt deze geregistreerd in de Containers ontvangt deze gebeurtenissen en acties van vRealize Automation.

Microsoft Azure-blueprints maken en bronacties hierin opnemen

Als cloud- of materiaalbeheerder kunt u Microsoft Azure-blueprints voor virtual machines maken die door bedrijfsgroepbeheerders worden gebruikt als bouwstenen om aangepaste, ingerichte machines te maken voor consumenten. DevOps-beheerders kunnen ook blueprints voor Azure-machines maken of ze kunnen bestaande blueprints voor Azure-machines gebruiken wanneer ze samengestelde blueprints maken.

- **Een blueprint maken voor Microsoft Azure**

U kunt blueprints maken voor Microsoft Azure virtual machines die toegang verlenen aan de Azure-bronnen van virtual machines.

- **Aangepaste Azure-bronacties maken**

U kunt aangepaste bronacties maken en gebruiken om Azure virtual machines te beheren.

Een blueprint maken voor Microsoft Azure

U kunt blueprints maken voor Microsoft Azure virtual machines die toegang verlenen aan de Azure-bronnen van virtual machines.

Een standaard Azure-machinesjabloon wordt weergegeven in de categorie **Machinetypen (Machine Types)** op de pagina vRealize Automation-blueprint bewerken. U kunt deze sjabloon voor virtual machines gebruiken als de basis voor een Azure-blueprint zoals beschreven in de volgende procedure. Nadat u een Azure-blueprint hebt gemaakt, kunt u deze publiceren en implementeren zoals ontworpen of kunt u deze samen met aangepaste Azure-bronnen gebruiken of met andere blueprints om een samengestelde blueprint te maken.

Na het maken en publiceren van de blueprint kunnen gebruikers met de juiste bevoegdheden een Azure-instantie aanvragen en inrichten via de vRealize Automation-servicecatalogus.

Azure-blueprints definiëren vereisten voor virtual machines. vRealize Automation gebruikt deze vereisten om de meest geschikte reservering te selecteren voor de implementatie.

Raadpleeg *vRealize Automation configureren* voor informatie over de tabbladen NSX-instellingen en Eigenschappen in het dialoogvenster Nieuwe blueprint.

Als u twee virtual machines tegelijk wilt maken via één implementatie, moet u twee netwerkinterfacenamen en twee namen voor virtual machines maken.

Opmerking Voorkom de provisioning van een implementatie aan zowel Azure als vSphere met behulp van hetzelfde voorvoegsel, omdat dit kan resulteren in dubbele namen in Azure en vSphere die kunnen leiden tot problemen voor sommige gebruikers.

Voorwaarden

- Verkrijg een geldige Azure-abonnements-id en gerelateerde informatiebron, inclusief brongroep, opslagaccount en virtuele netwerkinformatie, die u misschien nodig hebt om een blueprint te maken.
- Configureer een Azure-endpoint om een verbinding te maken met Azure voor gebruik met uw vRealize Automation-installatie.
- Configureer de geschikte Azure-reserveringen voor uw bedrijfsgroepen.

Procedure

- 1 Selecteer **Ontwerpen > Blueprints**.
- 2 Klik op het pictogram **Nieuw** (+).

- 3 Geef een naam voor de blueprint op in het tekstvak **Naam**.

De naam die u opgeeft wordt ook ingevuld in het tekstvak **Id**. Meestal kunt u de tabbladen **NSX-instellingen** en **Eigenschappen** negeren.

- 4 Klik op **OK**.

- 5 Klik op **Machinetypen (Machine Types)** in het menu Categorieën (Categories).

- 6 Sleep de sjabloon voor de virtual machine **Azure-machine** naar het ontwerpcanvas.

Als u een aangepaste Azure-bron hebt gemaakt voor gebruik als basis voor een blueprint, kunt u die bron selecteren uit de toegewezen categorie in de lijst Categorieën.

- 7 Voer de vereiste informatie voor de Azure virtual machine in de tekstvelden in op de pagina's met tabbladen die zich onderaan het ontwerpcanvas bevinden die worden weergegeven wanneer u de Azure-machinesjabloon naar het ontwerpcanvas sleept.

De beschikbare opties voor tekstvakken en andere parameters op al deze tabbladen worden voornamelijk bepaald door het Azure-endpoint dat als basis voor blueprints is geconfigureerd.

Voor de meeste parameters geldt dat, wanneer u kunt klikken op het tekstveld naast de parameter naam, een nieuw venster wordt geopend op de rechterzijde van de pagina. In dit venster kunt u parameterwaarden invoeren in het tekstveld **Waarde (Value)** en aangeven of deze al dan niet **Vereist (Required)** is. Houd er rekening mee dat u in sommige gevallen ook een **Minimumwaarde (Minimum Value)** en een **Maximumwaarde (Maximum Value)** kunt invoeren. Klik op **Toepassen (Apply)** in het rechterdeelvenster om het initiële tekstveld in te vullen.

Figuur 3-1. Menu rechterzijde Azure-blueprint

The screenshot shows the 'Azure_Machine_1' configuration window with the 'Machine Resources' tab selected. It features two main sections: 'Resource Group' and 'Availability Set'. Each section has radio buttons for 'Create New' and 'Use Existing'. The 'Resource Group Name' field contains 'RG1-vAficionado'. The 'Value' field for the 'Resource Group' is highlighted with an orange box, and an arrow points to it from the 'Use Existing' radio button. The 'Required' dropdown is set to 'No'.

De meeste parameters hebben ook een knop **Geavanceerde opties**. Met deze opties kunt u parameterlengten opgeven en zelfs parameters verbergen voor eindgebruikers.

Opmerking U moet de vereiste parameters op elk tabblad invullen om verder te gaan met de configuratie van de blueprint. Als u een veld leeg wilt laten, kunt u teruggaan en de invoer verwijderen voordat u deze opslaat.

Tabblad	Beschrijving	Belangrijke parameters
Algemeen	Selecteer basisverbindingsgegevens voor de Azure virtual machine zoals het endpoint dat moet worden gebruikt.	<p>Id (ID) - Identificeert de Azure virtual machine die u maakt. Als u deze naam wijzigt, wordt ook de image van de Azure virtual machine op het ontwerpcanvas automatisch bijgewerkt.</p> <p>Beschrijving (Description) - Identificeert de virtual machine die u maakt en of dit al dan niet vereist is.</p> <p>Instanties - Met deze selectie kunt u een schaalbare virtual machine creëren. Gebruik de velden Minimum en Maximum om het aantal Azure-instanties aan te geven die vanaf deze machine kunnen worden gemaakt.</p> <p>Wachtwoordverificatie gebruiken (Use password authentication): selecteer Ja om wachtwoordverificatie te gebruiken of Nee om SSH te gebruiken.</p> <p>Gebruikersnaam beheerder (Admin username) - Laat dit leeg zodat de gebruiker die de machine inricht de naam kan toewijzen.</p> <p>Beheerderswachtwoord (Admin password) - Laat dit veld leeg zodat de persoon die de machine inricht het juiste wachtwoord kan opgeven,</p>
Versie-informatie	Hiermee kunt u de informatie configureren van de virtual machine die wordt gemaakt.	<p>Locatie (Location) - Selecteer de geografische locatie waar deze virtual machine wordt geïmplementeerd.</p> <p>Machinevoorvoegsel (Machine Prefix) - Selecteer het gewenste keuzerondje om aan te geven of dat u het machinevoorvoegsel wilt gebruiken van de gekoppelde bedrijfsgroep of dat u een aangepast voorvoegsel wilt maken. Als u een aangepast voorvoegsel wilt gebruiken, voert u dit in het tekstveld Aangepast machinevoorvoegsel in.</p> <p>Type image van virtual machine (Virtual machine image type) - Kies het gewenste keuzerondje voor een Aangepast (Custom) of Stereotiep (Stock) image van de virtual machine. Een aangepaste virtual machine wordt gemaakt op basis van een klassieke Azure-implementatie en biedt meer configuratiemogelijkheden met betrekking tot cloudservices, accounts voor opslagruimtes en beschikbaarheidssets.</p> <p>Image van virtual machine (Virtual Machine Image) - Identificeert de image van de Azure virtual machine waarop de blueprint wordt gebaseerd.</p> <ul style="list-style-type: none"> ■ Voor een stereotiepe image van een virtual machine, moet de URN van de machine-image de volgende indeling hebben: (publisher):(offer):(sku): (version). ■ Voor een beheerde schijf moet de URN van de machine-image de volgende indeling hebben: (ResourceGroupName):(CustomImageName) ■ Voor een aangepaste image van een virtual machine, moet de URN van de machine-image de volgende indeling hebben: <p><code>https://storageaccount.blob.core.windows.net/container/image.vhd</code></p> <p>U moet ook het tekstveld Besturingssysteem voor type image invullen (Windows of Linux) voor aangepaste images.</p>

Tabblad	Beschrijving	Belangrijke parameters
		<p>Admingebruiker (Admin User) - Typ de naam van de aangewezen admingebruiker die is geconfigureerd voor virtual machines die op deze blueprint zijn gebaseerd. Eventueel kan het hier leeg gelaten worden en worden ingevuld op het aanvraagformulier.</p> <p>Verificatie (Authentication) - Selecteer het gewenste keuzerondje om aan te geven of voor virtual machines die zijn gebaseerd op deze blueprint, wachtwoord- of SSH-verificatie is vereist.</p> <p>Adminwachtwoord (Admin Password) - Het beheerderswachtwoord voor de instantie van de virtual machine.</p> <p>Serie (Series) - Definieert de algemene grootte van de instantie van een virtual machine. Raadpleeg de documentatie van Azure bij https://azure.microsoft.com/nl-nl/documentation/articles/virtual-machines-windows-sizes/ voor meer informatie over series.</p> <p>Grootte (Size) - Definieert de specifieke grootte van de instantie van een virtual machine binnen een serie. Grootte is gerelateerd aan de geselecteerde serie. Als u een geldige verbinding hebt met een Azure-instantie, dan worden de beschikbare groottes automatisch dynamisch ingevuld op basis van het abonnement en de selecteerde locatie en serie. Raadpleeg de documentatie van Azure voor meer informatie over de grootte.</p> <p>Groottedetails van instantie (Instance Size Details) - Optionele informatie over de serie en grootte van de instantie van een virtual machine.</p>

Tabblad	Beschrijving	Belangrijke parameters
Machinebronnen	<p>Organiseer de bronnen van de virtual machine in buckets. Een brongroep is een organisatiestructuur die bronnen van een virtual machine zoals websites, accounts, databases en netwerken groepeer. Een beschikbaarheidsset is een mechanisme voor het beheren van twee of meer virtual machines om redundantie te ondersteunen. Raadpleeg https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-manage-availability/ voor meer informatie over beschikbaarheidssets van Azure.</p> <hr/> <p>Opmerking Als u een blueprint configureert waarvan het maximaal aantal Azure-instanties is ingesteld op een waarde die groter is dan 1, kunt u het beste de bestaande brongroep en beschikbaarheidsset gebruiken in plaats van nieuwe te maken. Het gebruik van nieuwe brongroepen of nieuwe beschikbaarheidssets voor meer dan één instantie in dezelfde implementatie, leidt tot fouten en andere problemen bij koppeling aan load balancers.</p>	<p>Brongroep maken of opnieuw gebruiken (Create or reuse Resource group) - Selecteer het gewenste keuzerondje om aan te geven of u de bestaande Azure-brongroep wilt gebruiken of een nieuwe wilt maken. U kunt de naam van de bestaande brongroep vinden op de pagina Brongroepen (Resource Groups) in het Azure-portal. Als u ervoor kiest een nieuwe brongroep te maken, wordt een geschikte naam voor de nieuwe groep automatisch weergegeven in het tekstveld Brongroep (Resource Group).</p> <p>Beschikbaarheidsset maken of opnieuw gebruiken (Create or reuse Availability set) - Selecteer het gewenste keuzerondje. Als u Nieuw maken (Create New) selecteert, wordt de bijbehorende informatie voor de nieuwe beschikbaarheidsset weergegeven in het tekstveld.</p>

Tabblad	Beschrijving	Belangrijke parameters
Opslag	Hiermee kunt u een beheerde Azure-schijf of een opslagaccount kiezen voor deze blueprint. Met een beheerde schijf handelt Azure de meeste opslaggerelateerde configuratie- en onderhoudstaken af. Een opslagaccount geeft toegang tot de verschillende opslagtypen van Azure, zoals Azure Blob, Wachtrijtabel en Bestandsopslag. Voor de meeste blueprints kunt u de standaardwaarden accepteren.	<p>Opslagtype - Kies of u een beheerde schijf of een handmatig beheerde opslagaccount wilt opgeven.</p> <ul style="list-style-type: none"> ■ Als u Beheerde schijf hebt geselecteerd, kiest u of u een premium-schijf of een standaardschijf wilt gebruiken in het vak VM-schijftype. De andere selectievakken kunt u negeren. ■ Als u Opslagaccount hebt geselecteerd, geeft u de naam van het opslagaccount voor de virtual machine op in het vak OS-schijfopslagaccount. De besturingssysteemschijf voor de Azure virtual machine wordt geïmplementeerd voor deze opslagaccount. U vindt informatie over opslaggroepen in het Azure-portal. U beschikt mogelijk over meer opslagaccounts. <hr/> <p>Opmerking Opslagaccountnamen met onderstrepingstekens of andere speciale tekens kunnen fouten veroorzaken.</p> <hr/> <p>Opstartdiagnose inschakelen - Schakel dit selectievakje in als u diagnostische gegevens wilt gebruiken voor uw Azure-instantie.</p> <p>Aantal opslagschijven - Selecteer het gewenste aantal schijven voor gegevensopslag, zoals gebruikt door uw virtual machine. U kunt maximaal vier schijven opgeven. Deze schijven worden opgeteld bij de schijf voor het besturingssysteem zoals opgegeven in het tekstveld Opslagaccount (Storage Account).</p> <p>Opslagschijfnummer (Storage Disk #)</p> <ul style="list-style-type: none"> ■ Schijfnaam (Disk Name) - Identificerende naam die is toegewezen aan de schijf. ■ Schijftype (Disk Type) - Type opslagapparaat. ■ Schijfgrootte (Disk Size) - Opslaggrootte. ■ Replicatie (Replication) - Redundantiemethode die wordt gebruikt voor back-ups van de schijf. ■ Cache van host (Host Caching) - Geeft aan of lees-/schrijfbewerkingen in cache worden opgeslagen om de prestaties te verbeteren.

Tabblad	Beschrijving	Belangrijke parameters
Netwerk	<p>Hier kunt u de netwerkinstellingen selecteren voor de blueprint van de virtual machine. Voor de meeste blueprints kunt u de standaardwaarden accepteren, zodat de consument de gewenste netwerkinformatie kan invoeren tijdens de implementatie.</p> <hr/> <p>Opmerking U kunt slechts één virtual machine per interface maken, maar elke virtual machine kan maximaal vier interfaces hebben.</p> <hr/>	<p>Klik op de tabel om rechts een dialoogvenster te openen dat een andere bewerkbare tabel met de volgende velden bevat.</p> <ul style="list-style-type: none"> ■ Naam van load balancer (Load Balancer Name) - De load balancer die wordt gebruikt bij de Azure-instantie. ■ Aantal netwerkinterfaces (Number of Network Interfaces) - Selecteer het aantal netwerkinterfaces dat wordt gebruikt met de Azure-instantie. Het aantal netwerkinterfaces moet worden ondersteund door de grootte van de virtual machine die is geselecteerd op het tabblad Opslag (Storage). ■ Netwerkinterface (Network interface) - Selecteer de juiste netwerkinterface voor de blueprint van de virtual machine. Als u een bestaand netwerk opgeeft, kunt u alle andere netwerktabbladen negeren. Als u een naam voor de netwerkinterface opgeeft die niet bestaat, wordt een nieuw interface met die naam gemaakt en kunt u de andere netwerktabbladen gebruiken om de interface te configureren. ■ Voorvoegsel NIC-naam (NIC Name Prefix) - Het voorvoegsel voor de netwerkinterfacekaart. ■ Type IP-adres (IP Address Type) - Geef aan of de virtual machine een statisch of dynamisch IP-adres gebruikt. ■ Netwerkconfiguratie (Networking Configuration) - Voer de gewenste netwerkconfiguratie in. Netwerkprofielen worden ondersteund. Er zijn twee opties, Azure-netwerken opgeven (Specify Azure Networks) en Netwerkprofielen gebruiken (Use Network Profile), en de daarop volgende velden wijzigen afhankelijk van de gekozen optie. <ul style="list-style-type: none"> ■ De volgende opties zijn beschikbaar als u Azure-netwerken opgeven (Specify Azure Networks) selecteert. Als u deze tekstvelden leeg laat, worden de standaard netwerkstructuren gebruikt op basis van de informatie die wordt opgegeven in de betreffende reservering. <ul style="list-style-type: none"> ■ vNet-naam (vNet Name) - Naam van het virtuele netwerk. ■ subNet-naam (subNet Name) - De domeinnaam van het Azure-subnet. <hr/> <p>Opmerking U kunt het openbaar IP-adres voor Azure tijdens Day 2 Operations instellen.</p> <hr/>

Tabblad	Beschrijving	Belangrijke parameters
		<ul style="list-style-type: none"> ■ Als u Netwerkprofiel gebruiken (Use Network Profile) selecteert, wordt de netwerkconfiguratie losgekoppeld van de onderliggende Azure-structuren en wordt deze in plaats daarvan gekoppeld aan het vRealize Automation-netwerkprofiel. ■ Als u het tekstveld Netwerkprofiel (Network Profile) leeg laat, wordt het standaardpaar van Azure-vNet en subnet opgelost op basis van de betreffende reserveringen met het opgegeven netwerkprofiel. ■ Als u een netwerkprofiel invoert, worden het Azure-vNet en het subnet opgelost op basis van de overeenstemmende reservering.
Properties	<p>Hiermee kunt u aangepaste eigenschappen toevoegen aan uw blueprint.</p> <p>Aangepaste eigenschappen die hier zijn toegepast, kunnen worden overschreven door de eigenschappen die later in de voorrangsketen worden toegewezen. Voor meer informatie over de voorrangsvolgorde voor aangepaste eigenschappen, gaat u naar <i>Naslaggids voor aangepaste eigenschappen</i>.</p>	<p>Er zijn twee opties voor het toevoegen van aangepaste eigenschappen, zoals weergegeven door twee tabbladen in het dialoogvenster Eigenschappen.</p> <ul style="list-style-type: none"> ■ Eigenschapsgroepen: Dit zijn herbruikbare groepen die het proces waarmee aangepaste eigenschappen kunnen worden toegevoegd vereenvoudigen. Er zijn vier opties voor het selecteren van eigenschapsgroepen: <ul style="list-style-type: none"> ■ Toevoegen - stelt u in staat een beschikbare eigenschapsgroep toe te voegen aan de blueprint. ■ Omhoog/omlaag verplaatsen - Hiermee kunt u de prioriteit van eigenschapsgroepen beheren. De eerste groep heeft de hoogste prioriteit en de aangepaste eigenschappen ervan hebben als eerste voorrang. ■ Eigenschappen weergeven - stelt u in staat de aangepaste eigenschappen te bekijken binnen de geselecteerde groep. ■ Gecombineerde eigenschappen weergeven - Als een aangepaste eigenschap in meer dan één eigenschapsgroep is opgenomen, krijgt de waarde in de eigenschapsgroep met de hoogste prioriteit voorrang. Het weergeven van deze samengevoegde eigenschappen, kan u helpen de juiste prioriteit te bepalen van eigenschapsgroepen. ■ Aangepaste eigenschappen: Gebruik dit tabblad om afzonderlijke aangepaste eigenschappen toevoegen. <ul style="list-style-type: none"> ■ Nieuw - stelt u in staat een individuele aangepaste eigenschap toevoegen aan de blueprint. ■ Naam - Voer een unieke naam voor de eigenschap in ter identificatie. Zie <i>Naslaggids voor aangepaste eigenschappen</i> voor een lijst met aangepaste eigenschappen en hun definities. ■ Waarde - Voer een waarde voor de aangepaste eigenschap in. ■ Versleuteld - u kunt de eigenschap versleutelen. ■ Overschrijfbaar - u kunt opgeven dat de eigenschapswaarde kan worden overschreven door de volgende of daaropvolgende gebruiker. Dit is normaal

Tabblad	Beschrijving	Belangrijke parameters
		<p>gesproken een andere architect, maar als u Weergeven in aanvraag selecteert, kunnen uw zakelijke gebruikers eigenschapswaarden weergeven en bewerken wanneer ze catalogusitems aanvragen.</p> <ul style="list-style-type: none"> ■ Weergeven in aanvraag - Als u de eigenschapsnaam en -waarde aan eindgebruikers wilt tonen, kunt u ervoor kiezen om de eigenschap op het aanvraagformulier weer te geven bij aanvragen voor het inrichten van machines. U moet ook Overschrijfbaar selecteren als u wilt dat gebruikers een waarde opgeven.

- 8 Klik op **Beëindigen (Finish)** om de blueprintconfiguratie op te slaan en terug te keren naar de hoofdpagina voor blueprints.

Wat nu te doen

Als u aangepaste eigenschappen hebt geconfigureerd in uw Azure-reservering om een VPN-tunnel te ondersteunen, kunt u softwareonderdelen aan Azure-blueprints toevoegen.

- 1 Selecteer **Softwareonderdelen** in het menu Categorieën. Softwareonderdelen waarvoor u Azure-blueprints hebt geconfigureerd, worden in het deelvenster eronder weergegeven.
- 2 Select Azure virtual machine in de waarden in het vervolgkeuzemenu voor de container.
- 3 Selecteer het gewenste softwareonderdeel en sleep het naar de Azure virtual machine op het ontwerpcanvas.
- 4 Als er eigenschappen vereist zijn voor het softwareonderdeel, voert u deze in de relevante parametertekstvakken onder het ontwerpcanvas in.
- 5 Klik op **Opslaan**.

Als u de blueprint wilt publiceren, selecteert u deze op de hoofdpagina voor blueprints en klikt u op **Publiceren (Publish)**. Een gepubliceerde blueprint is beschikbaar via de pagina Catalogusitems. Een bedrijfsgroepbeheerder of equivalente persoon kan deze gepubliceerde blueprint gebruiken als de basis van een samengestelde blueprint.

Aangepaste Azure-bronacties maken

U kunt aangepaste bronacties maken en gebruiken om Azure virtual machines te beheren.

De vRealize Automation Azure-implementatie wordt geleverd met twee gebruiksklare aangepaste bronacties:

- Virtual machine starten
- Virtual machine stoppen

Daarnaast kunt u aangepaste bronacties maken met werkstromen die toegankelijk zijn via de vRealize Orchestrator-bibliotheek, die beschikbaar is in de vRealize Automation-interface.

U kunt Azure-bronacties op dezelfde manier gebruiken als alle andere XaaS-bronacties in vRealize Automation. Zie *XaaS-blueprints en -bronacties maken* en *Integratie van vRealize Orchestrator in vRealize Automation* in *vRealize Automation configureren* voor meer informatie over XaaS-bronacties.

Voorwaarden

Configureer een geldig Azure-endpoint voor uw vRealize Automation-implementatie.

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Bronacties**
- 2 Klik op **Nieuw**.
- 3 Blader naar **Orchestrator > Bibliotheek > Azure** in devRealize Orchestrator werkstroombibliotheek.
- 4 Selecteer de gewenste map en werkstroom.
- 5 Configureer de actie naar wens zoals elke andere XaaS-bronactie.

Configuratiebeheermogelijkheden toevoegen aan vSphere-blueprints

U kunt configuratiebeheeronderdelen toevoegen aan vSphere-blueprints om het configuratiebeheer van virtuele vSphere-machines te ondersteunen.

vRealize Automation ondersteunt het toevoegen van Puppet- en Ansible-configuratiebeheerfuncties in vSphere-blueprints.

Op Puppet gebaseerd configuratiebeheer gebruikt doorgaans rollen en omgevingen om softwareconfiguratie te definiëren en te beheren op basis van de Puppet Enterprise-toepassing. Wees u ervan bewust dat de betekenis van rol en omgeving in Puppet afwijkt van de algemene betekenis die deze woorden in een IT-context hebben.

Op Ansible gebaseerd configuratiebeheer werkt met taaksjablonen die zijn gedefinieerd in een Ansible Tower-implementatie. U kunt meerdere sjablonen kiezen en opnieuw ordenen. U kunt deze sjablonen uitvoeren nadat een machine is geïmplementeerd en voordat deze wordt vernietigd in vRealize Automation.

Een endpoint brengt een verbinding tot stand met een bestaande zakelijke Puppet- of Ansible-omgeving. Wanneer het endpoint wordt gemaakt, haalt vRealize Automation de juiste informatie van de opgegeven implementaties op. U kunt vroege bindings- of late bindingsscenario's opgeven bij het configureren van een blueprint voor een virtuele Puppet- of Ansible-machine.

Opmerking Ansible- en Puppet-onderdelen worden momenteel alleen ondersteund op vSphere-blueprints en virtuele vSphere-machines.

Een Puppet-onderdeel toevoegen aan een vSphere-blueprint

U kunt een Puppet-configuratiebeheeronderdeel aan een vSphere-blueprint toevoegen om beheer te forceren van virtuele vSphere-machines die een Puppet Master gebruiken.

Als u een Puppet-onderdeel toevoegt aan een vSphere-blueprint, wordt er een Puppet-agent toegevoegd aan virtuele machines die van die blueprint zijn gemaakt.

Wanneer u voor Puppet geschikte vSphere-blueprints maakt, moet u kiezen of u een configuratie met een vroege binding of een late binding wilt maken.

Bij een vroege binding definiëren gebruikers de Puppet-rol en omgevingsinstellingen voor alle virtuele machines op basis van een bepaalde blueprint wanneer het Puppet-onderdeel aan de blueprint wordt toegevoegd. Deze instellingen blijven onveranderd gedurende de levensduur van de blueprint. Voor late binding beschikt u over verschillende opties.

- Laat de tekstvakken **Puppet-omgeving** en **Puppet-rol** leeg in de blueprint, zodat gebruikers deze instellingen kunnen opgeven op het moment van de aanvraag.
- Geef een **Puppet-omgeving** op en laat het tekstvak **Puppet-rol** leeg. Gebruikers moeten de rol opgeven op het moment van de aanvraag.

Voorwaarden

Maak een geschikte vSphere-blueprint. Raadpleeg [Instellingen voor vSphere-machineonderdelen in vRealize Automation](#) voor meer informatie.

Procedure

- 1 Selecteer **Ontwerpen > Blueprints**.
- 2 Selecteer **Configuratiebeheer** in het menu Categorieën op de pagina Ontwerpen voor blueprints.
- 3 Selecteer het Puppet-onderdeel en sleep het naar het vSphere-onderdeel op het ontwerpcanvas.
- 4 Geef een **Id** en **Beschrijving** op voor het Puppet-onderdeel op het tabblad Algemeen onder aan de pagina.

De id en beschrijving zijn niet verplicht.

- 5 Klik op het tabblad Server.
- 6 Klik op het vervolgkeuzemenu en selecteer de juiste Puppet Master voor de blueprint.
- 7 Selecteer de juiste **Puppet-omgeving** en **Puppet-rol** als u vroege binding voor dit onderdeel wilt gebruiken.

Als u vroege binding wilt configureren, selecteert u een Puppet-omgeving en -rol. Als u een onderdeel met late binding wilt maken, selecteert u een **Puppet-omgeving** of laat u de tekstvakken **Puppet-omgeving** en **Puppet-rol** leeg en schakelt u de selectievakjes **Instellen in aanvraagformulier** in.

Opmerking De selectievakjes bij **Instellen in aanvraagformulier** zijn onderling verbonden. Als u er een inschakelt, worden ze automatisch allemaal ingeschakeld.

- 8 Klik op **Voltooien** om de Puppet-onderdeelconfiguratie op te slaan en terug te keren naar de hoofdpagina voor het ontwerpen van blueprints.

Een Ansible-onderdeel toevoegen aan een vSphere-blueprint

U kunt een Ansible-configuratiebeheeronderdeel aan een vSphere-blueprint toevoegen om beheer te forceren van virtuele vSphere-machines die een Ansible Tower gebruiken.

Door een Ansible-onderdeel toe te voegen aan een vSphere-blueprint, kan de Ansible Tower communiceren met de geïmplementeerde bronnen voor het uitvoeren van commando's.

Voorwaarden

Maak een geschikte vSphere-blueprint. Raadpleeg [Instellingen voor vSphere-machineonderdelen in vRealize Automation](#) voor meer informatie.

Procedure

- 1 Selecteer **Ontwerpen > Blueprints**.
- 2 Selecteer **Configuratiebeheer** in het menu Categorieën op de pagina Ontwerpen voor blueprints.
- 3 Selecteer het Ansible-onderdeel en sleep het naar het vSphere-onderdeel op het ontwerpcanvas.
- 4 Geef een **Id** en **Beschrijving** op voor het Ansible-onderdeel op het tabblad Algemeen onder aan de pagina.

De id en beschrijving zijn niet verplicht.
- 5 Klik op het tabblad Details en voer de juiste informatie over de Ansible Tower, het project en de sjabloon in.
 - a Selecteer een geschikte **Ansible Tower** en **Organisatie** die dit onderdeel zullen gebruiken.
 - b Configureer vroege of late binding voor het Ansible-onderdeel.
 - Als u vroege binding wilt gebruiken voor dit onderdeel, selecteert u het juiste **Project** en de juiste **Taaksjabloon**. Selecteer een geschikte sjabloon om uit te voeren wanneer de machine wordt vernietigd in het tekstvak **Taaksjabloon inrichting opheffen**. Laat de selectievakjes bij **Instellen in aanvraagformulier** leeg. Selecteer ook een geschikte Ansible-omgeving en rol.
 - Als u een onderdeel met late binding wilt maken, kunt u de selectievakjes **Instellen in aanvraagformulier** kiezen in plaats van individuele instellingswaarden voor de vakjes **Project**, **Taaksjabloon** en **Taaksjabloon inrichting opheffen**.

Opmerking De selectievakjes bij **Instellen in aanvraagformulier** zijn onderling verbonden. Als u er één selecteert, worden de vakjes eronder automatisch ook geselecteerd. Deze functionaliteit is het gevolg van het feit dat het veld **Project** als filter voor de Taaksjablonen fungeert. Als u een project opgeeft, wordt de lijst met taaksjablonen automatisch gefilterd op project. Daarom worden de volgende twee velden automatisch geselecteerd als u **Instellen in aanvraagformulier** kiest voor een project.

- 6 Klik op **Voltooien** om de Ansible-onderdeelconfiguratie op te slaan en terug te keren naar de hoofdpagina voor het ontwerpen van blueprints.

Ondersteuning voor RDP-verbinding toevoegen aan Windows-machineblueprints

Voeg aangepaste RDP-eigenschappen aan de blueprint toe en verwijst naar het RDP-bestand dat de systeembeheerder heeft voorbereid, als u catalogusbeheerders in staat wilt stellen gebruikers toe te staan om met een RDP-actie voor Windows-blueprints verbinding te maken.

Opmerking Als uw materiaalbeheerder een eigenschapsgroep maakt die de vereiste aangepaste eigenschappen bevat en u neemt deze op in uw blueprint, dan hoeft u de aangepaste eigenschappen niet individueel aan de blueprint toe te voegen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **bedrijfsgroepbeheerder**.
- Haal de naam op van het aangepaste RDP-bestand dat de systeembeheerder voor u heeft gemaakt. Zie [Een aangepast RDP-bestand maken ter ondersteuning van RDP-verbindingen voor ingerichte machines](#).
- Maak ten minste één Windows-machineblueprint.

Procedure

- 1 Selecteer **Ontwerpen > Blueprints**.
- 2 Wijs de blueprint die u wilt bijwerken aan en klik op **Bewerken**.
- 3 Selecteer het machineonderdeel op uw canvas om de details te bewerken.
- 4 Klik op het tabblad **Eigenschappen**.
- 5 Klik op het tabblad **Aangepaste eigenschappen**.

6 Configureer de RDP-instellingen.

- Klik op **Nieuwe eigenschap**.
- Typ de naam van de aangepaste RDP-eigenschappen in het tekstvak **Naam** en de bijbehorende waarde in het tekstvak **Waarde**.

Optie	Beschrijving en waarde
VirtualMachine.Rdp.File	Geeft een RDP-bestand op waarvan instellingen worden verkregen, bijvoorbeeld <code>My_RDP_Settings.rdp</code> . Het bestand moet zich in de <code>Website\Rdp</code> -submap van de vRealize Automation-installatiemap bevinden.
VirtualMachine.Rdp.SettingN	Geeft de RDP-instellingen op die moeten worden gebruikt bij het openen van een RDP-koppeling naar de machine. <i>N</i> is een uniek nummer dat wordt gebruikt om de ene RDP-instelling te onderscheiden van de andere. Bijvoorbeeld: als u een RDP-verificatieniveau wilt opgeven zodat er geen verificatievereiste wordt opgegeven, definieert u de aangepaste eigenschap <code>VirtualMachine.Rdp.Setting1</code> en stelt u de waarde in op verificatieniveau:i:3. Zie Microsoft Windows RDP-documentatie zoals RDP Settings for Remote Desktop Services in Windows Server voor informatie over beschikbare RDP-instellingen en de bijbehorende juiste syntaxis.
VirtualMachine.Admin.NameCompletion	Geeft de domeinnaam op om deze op te nemen in de volledig gekwalificeerde domeinnaam van de machine die de RDP- of SSH-bestanden genereert voor de gebruikersinterfaceopties Verbinding maken met RDP of Verbinding maken met SSH . Stel de waarde bijvoorbeeld in op <code>myCompany.com</code> om de volledig gekwalificeerde domeinnaam <code>my-machine-name.myCompany.com</code> in het RDP- of SSH-bestand te genereren.

- Klik op **Opslaan**.

7 Selecteer de blueprintrijs en klik op **Publiceren**.

Resultaten

De catalogusbeheerders kunnen gebruikers het recht geven om de actie **Verbinding maken via RDP** te gebruiken voor de machines die worden ingericht met uw blueprint. Gebruikers die niet gerechtigd zijn voor deze actie, kunnen geen verbinding maken via RDP.

Active Directory-opschoning toevoegen aan uw CentOS-blueprint

U bent IaaS-architect en wilt vRealize Automation configureren om uw Active Directory-omgeving op te schonen zodra er ingerichte machines van uw hypervisors worden verwijderd. U bewerkt daarom uw blueprint zodat u de opschoningsmodule voor Active Directory kunt configureren.

Met de opschoningsmodule voor Active Directory kunt u de volgende acties voor het Active Directory-account laten uitvoeren wanneer een machine wordt verwijderd van een hypervisor:

- Het AD-account verwijderen
- Het AD-account deactiveren
- De naam van het AD-account wijzigen

- Het AD-account verplaatsen naar een andere AD-organisatie-eenheid

Voorwaarden

Opmerking Deze informatie is niet van toepassing op Amazon Web Services.

- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Verzamel de volgende informatie over uw Active Directory-omgeving:
 - De gebruikersnaam en het wachtwoord voor een Active Directory-account met voldoende rechten om AD-accounts te verwijderen, te deactiveren, een nieuwe naam te geven of te verplaatsen. Voor de gebruikersnaam moet de indeling domein \gebruikersnaam worden gebruikt.
 - (Optioneel) De naam van de OU waar vernietigde machines naar moeten worden verplaatst.
 - (Optioneel) Het voorvoegsel dat aan vernietigde machines moet worden toegevoegd.
- Maak een machineblueprint. Zie [Een machineblueprint configureren](#).

Procedure

- 1 Selecteer **Ontwerpen > Blueprints**.
- 2 Wijs uw blueprint aan en klik op **Bewerken**.
- 3 Selecteer het machineonderdeel op uw canvas om het tabblad Details weer te geven.
- 4 Klik op het tabblad **Eigenschappen**.
- 5 Klik op het tabblad **Aangepaste eigenschappen** om de Active Directory-opschoningsmodule te configureren.
 - a Klik op **Nieuwe eigenschap**.
 - b Typ `Plugin.AdMachineCleanup.Execute` in het tekstvak **Naam**.
 - c Typ **true** in het tekstvak **Waarde**.
 - d Klik op het pictogram **Opslaan** (✓).
- 6 Configureer de Active Directory-opschoningsmodule door aangepaste eigenschappen toe te voegen.

Optie	Beschrijving en waarde
<code>Plugin.AdMachineCleanup.UserName</code>	Geef de gebruikersnaam van het Active Directory-account op in het tekstvak Waarde . Deze gebruiker moet voldoende rechten hebben om Active Directory-accounts te verwijderen, te deactiveren, te verplaatsen of van naam te veranderen. De gebruikersnaam moet in de indeling domein \gebruikersnaam worden ingevoerd.
<code>Plugin.AdMachineCleanup.Password</code>	Geef het wachtwoord van het Active Directory-account op in het tekstvak Waarde .

Optie	Beschrijving en waarde
<code>Plugin.AdMachineCleanup.Delete</code>	Stel dit in op True om de accounts van vernietigde machines te verwijderen, in plaats van deze uit te schakelen.
<code>Plugin.AdMachineCleanup.MoveToOu</code>	Verplaatst het account van vernietigde machines naar een nieuwe Active Directory-organisatie-eenheid. De waarde is de organisatie-eenheid waarnaar u het account verplaatst. Deze waarde moet de indeling <code>ou=OU, dc=dc</code> hebben, bijvoorbeeld <code>ou=trash,cn=computers,dc=lab,dc=local</code> .
<code>Plugin.AdMachineCleanup.RenamePrefix</code>	Wijzigt de naam van de accounts van vernietigde machines door een voorvoegsel toe te voegen. De waarde is de voorvoegseltekenreeks die voorafgaat, bijvoorbeeld <code>destroyed_</code> .

7 Klik op **OK**.

Resultaten

De Active Directory-omgeving wordt nu bijgewerkt telkens wanneer er machines die zijn ingericht via uw blueprint, worden verwijderd van de hypervisor.

Aanvragers een hostnaam voor machines laten opgeven

U wilt als blueprintarchitect uw gebruikers toestaan een eigen machinenaam te kiezen bij de aanvraag voor uw blueprints. Dus bewerkt u uw blueprint om de aangepaste eigenschap Hostnaam toe te voegen en configureert u deze zodat gebruikers een waarde moeten opgeven wanneer ze een aanvraag willen verzenden.

Opmerking Als uw materiaalbeheerder een eigenschapsgroep maakt die de vereiste aangepaste eigenschappen bevat en u neemt deze op in uw blueprint, dan hoeft u de aangepaste eigenschappen niet individueel aan de blueprint toe te voegen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Maak een machineblueprint. Zie [Een machineblueprint configureren](#).

Procedure

- 1 Selecteer **Ontwerpen > Blueprints**.
- 2 Wijs uw blueprint aan en klik op **Bewerken**.
- 3 Selecteer het machineonderdeel op uw canvas om het tabblad met details weer te geven.
- 4 Klik op het tabblad **Eigenschappen**.
- 5 Klik op **Nieuwe eigenschap**.
- 6 Geef **Hostnaam** op in het tekstvak **Naam**.
- 7 Laat het tekstvak **Waarde** leeg.

- 8 Configureer vRealize Automation zodat gebruikers bij hun aanvraag wordt gevraagd een waarde voor de hostnaam op te geven.

- a Schakel **Overschrijfbaar** in.
- b Selecteer **Weergeven in aanvraag**.

Omdat hostnamen uniek moeten zijn, kunnen gebruikers slechts één machine tegelijk aanvragen voor deze blueprint.

- 9 Klik op het pictogram **Opslaan** (✓).

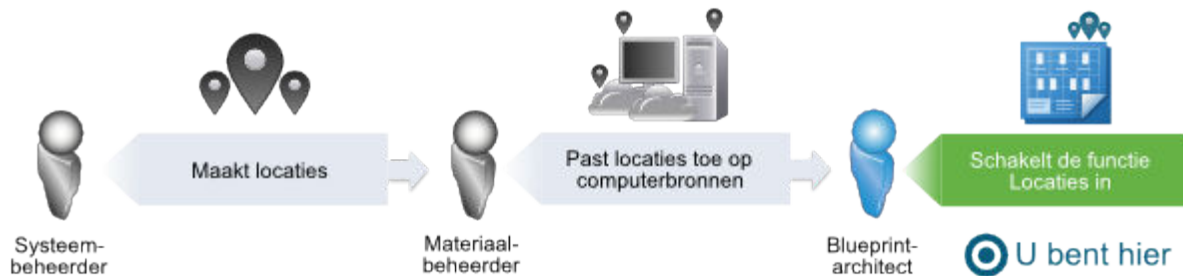
- 10 Klik op **OK**.

Resultaten

Gebruikers die een machine aanvragen via uw blueprint, moeten een hostnaam opgeven voor hun machine. vRealize Automation controleert of de opgegeven hostnaam uniek is.

Gebruikers datacenterlocaties laten selecteren voor interregionale implementaties

Als blueprintarchitect wilt u gebruikers laten kiezen of ze hun machines willen inrichten via de infrastructuur in Londen of Boston, dus bewerkt u uw blueprint om de locatiefunctie in te schakelen.



U hebt een datacenter in Londen en een datacenter in Boston en u wilt voorkomen dat gebruikers in Boston machines inrichten op de infrastructuur in Londen en omgekeerd. Om ervoor te zorgen dat uw gebruikers in Boston machines inrichten op uw infrastructuur voor Boston (en gebruikers in Londen de infrastructuur van Londen gebruiken), is het aan te raden gebruikers de juiste locatie te laten selecteren voor de inrichting wanneer ze machines aanvragen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Als systeembeheerder definieert u de locaties van de datacenters. Zie [Scenario: datacenterlocaties toevoegen voor interregionale implementaties](#).
- Als materiaalbeheerder past u de juiste locaties toe op uw computerbronnen. Zie [Scenario: een locatie toewijzen aan een computerbron voor interregionale implementaties](#).
- Maak een machineblueprint. Zie [Een machineblueprint configureren](#).

Procedure

- 1 Selecteer **Ontwerpen > Blueprints**.
- 2 Wijs uw blueprint aan en klik op **Bewerken**.
- 3 Selecteer het machineonderdeel op uw canvas om het tabblad **Algemene details** te selecteren.
- 4 Schakel het selectievakje **Locatie op verzoek weergeven** in.
- 5 Klik op **Voltooien**.
- 6 Wijs uw blueprint aan en klik op **Publiceren**.

Resultaten

Bedrijfsgroepgebruikers wordt nu gevraagd een datacenterlocatie te selecteren wanneer ze een machine aanvragen die moet worden ingericht met uw blueprint.

Software-onderdelen ontwerpen

Als softwarearchitect kunt u herbruikbare softwareonderdelen maken, configuratie-eigenschappen standaardiseren en actiescripts gebruiken om exact op te geven hoe onderdelen worden geïnstalleerd, geconfigureerd, verwijderd of bijgewerkt tijdens bewerkingen op implementatieschaal. U kunt deze actiescripts op elk gewenst moment herschrijven en deze live publiceren om wijzigingen door te voeren in ingerichte softwareonderdelen.

U kunt uw actiescripts op een algemene en herbruikbare manier ontwerpen door naam- en waardeparen die software-eigenschappen worden genoemd, te definiëren en te verbruiken en ze als parameters door te geven aan uw actiescripts. Als uw software-eigenschappen over onbekende waarden beschikken of als de waarden in de toekomst moeten worden gedefinieerd, kunt u andere blueprintarchitecten of eindgebruikers de waarden laten opgeven. Als u een waarde van een ander onderdeel in een blueprint nodig hebt, bijvoorbeeld het IP-adres van een machine, kunt u uw software-eigenschap aan de IP-adreseigenschap van die machine binden. Met behulp van software-eigenschappen kunt u uw actiescripts parameteriseren om ze algemeen en herbruikbaar te maken, zodat u softwareonderdelen kunt implementeren in verschillende omgevingen zonder uw scripts te hoeven wijzigen.

Tabel 3-43. Levenscyclusacties

Levenscyclusacties	Beschrijving
Installeren	Installeer uw software. U kunt bijvoorbeeld de installatiefragmenten van Tomcat-server downloaden en een Tomcat-service installeren. Scripts die u voor de actie Levenscyclus installeren schrijft, worden uitgevoerd wanneer de software voor de eerste keer wordt ingericht, tijdens een eerste implementatieaanvraag of als onderdeel van een opschaling.
Configureren	Configureer uw software. Voor het voorbeeld van Tomcat kunt u de JAVA_OPTS en CATALINA_OPTS instellen. Configuratiescripts worden uitgevoerd nadat de installatie-actie is voltooid.

Tabel 3-43. Levenscyclusacties (vervolg)

Levenscyclusacties	Beschrijving
Start	Start uw software. U kunt bijvoorbeeld proberen de Tomcat-service te starten met behulp van de startopdracht in de Tomcat-server. Startscripts worden uitgevoerd nadat de configuratie-actie is voltooid.
Bijwerken	Als u uw softwareonderdeel zodanig ontwerpt dat deze schaalbare blueprints kan ondersteunen, dient u alle updates uit te voeren die vereist zijn na een opschaal- of neerschaalbewerking. U kunt bijvoorbeeld de clustergrootte van een geschaalde implementatie wijzigen en de geclusterde knooppunten beheren met behulp van een load balancer. Ontwerp uw updatescripts zodanig dat ze meerdere keren kunnen worden uitgevoerd (idempotent) en dat ze zowel opschaal- als neerschaalbewerkingen kunnen uitvoeren. Wanneer een schalingsbewerking is uitgevoerd, kunnen er updatescripts worden uitgevoerd op alle afhankelijke softwareonderdelen.
Installatie ongedaan maken	Verwijder uw software. U kunt bijvoorbeeld specifieke acties uitvoeren in de toepassing voordat een implementatie wordt vernietigd. Verwijderingsscripts worden uitgevoerd wanneer softwareonderdelen worden vernietigd.

U kunt vooraf gedefinieerde Software-onderdelen downloaden voor een reeks middleware-services en -toepassingen van de VMware Solution Exchange. Als u de vRealize CloudClient of de vRealize Automation-REST-API gebruikt, kunt u vooraf gedefinieerde Software-onderdelen programmatisch importeren in uw vRealize Automation-instantie.

- Ga naar https://solutionexchange.vmware.com/store/category_groups/cloud-management om de VMware Solution Exchange te bezoeken.
- Voor informatie over de vRealize Automation REST API raadpleegt u *Programmeergids* en [vRealize Automation-inhoudsservice-API](https://code.vmware.com) op <https://code.vmware.com>.
- Voor meer informatie over vRealize CloudClient, raadpleegt u <https://developercenter.vmware.com/tool/cloudclient>.

Opties voor eigenschapstypen en -instellingen

U kunt uw actiescripts op een algemene en herbruikbare manier ontwerpen door naam- en waardeparen die software-eigenschappen worden genoemd, te definiëren en te verbruiken en ze als parameters door te geven aan uw actiescripts. U kunt software-eigenschappen maken die string-, array-, inhouds-, boolean- of integerwaarden verwachten. U kunt de waarde zelf opgeven, iemand anders kan worden verplicht de waarde op te geven of de waarde kan worden opgehaald bij een ander blueprintonderdeel door een binding te maken.

Eigenschapsopties

U kunt de waarde van elke stringeigenschap berekenen door het selectievakje 'berekend' in te schakelen en u kunt elke eigenschap gecodeerd, overschrijfbaar of vereist maken door de overeenkomstige selectievakjes te selecteren wanneer u Software-eigenschappen configureert. Combineer deze opties met uw waarden om verschillende doelen te bereiken. U wilt bijvoorbeeld blueprintarchitecten verplichten een waarde voor een wachtwoord op te geven en die waarde te versleutelen wanneer ze uw softwareonderdeel gebruiken in een blueprint. Maak de

wachtwoordeigenschap, maar laat het waardetekstvak leeg. Selecteer Overschrijfbaar, Vereist, en Versleuteld. Als het verwachte wachtwoord bij uw eindgebruiker hoort, kan de blueprintarchitect **Weergeven in aanvraag** selecteren om uw gebruikers te verplichten het wachtwoord in te voeren wanneer ze het aanvraagformulier invullen.

Optie	Beschrijving
Gecodeerd	Geeft aan dat de eigenschap gecodeerd is en dat de waarde in vRealize Automation gemaskeerd wordt weergegeven met sterretjes. Als u de eigenschap terugzet op ongecodeerd, wordt de eigenschapswaarde opnieuw ingesteld door vRealize Automation. U moet om veiligheidsredenen een nieuwe waarde voor de eigenschap instellen.
Overschrijfbaar	U kunt architecten bij het samenstellen van een toepassingsblueprint toestaan de waarde van deze eigenschap te overschrijven. De waarde die u invoert, wordt als standaardwaarde weergegeven.
Vereist	U kunt vereisen dat architecten een waarde voor deze eigenschap opgeven of anders uw standaardwaarde moeten accepteren.
Berekend	Waarden voor berekende bronnen worden toegewezen door de levenscyclusscripts INSTALL, CONFIGURE, START en UPDATE. De toegewezen waarde wordt doorgegeven naar de daaropvolgende beschikbare levenscyclusfasen en naar onderdelen die gebonden zijn aan deze eigenschappen in een blueprint. Als u Berekend selecteert voor een eigenschap die geen stringeigenschap is, wordt het eigenschapstype gewijzigd in string.

Als u de berekende eigenschapsoptie selecteert, laat u de waarde voor uw aangepaste eigenschap leeg. Ontwerp uw scripts voor de berekende waarden.

Tabel 3-44. Scriptvoorbeelden voor de berekende eigenschapswaarde

Voorbeeldstringeigenschap	Scriptsyntaxis	Voorbeeldgebruik
my_unique_id = ""	Bash - \$my_unique_id	export my_unique_id="0123456789"
	Windows CMD - %my_unique_id%	set my_unique_id=0123456789
	Windows PowerShell - \$my_unique_id	\$my_unique_id = "0123456789"

Stringeigenschap

Stringeigenschappen verwachten stringwaarden. U kunt de waarde zelf opgeven, iemand anders kan worden verplicht de waarde op te geven of de waarde kan worden opgehaald bij een ander blueprintonderdeel door een binding te maken met een andere stringeigenschap. Stringwaarden kunnen alle ASCII-tekenen bevatten. Als u een eigenschapsbinding wilt maken, gebruikt u het tabblad **Eigenschappen** op het ontwerpcanvas om de juiste eigenschap voor een binding te selecteren. De eigenschapswaarde wordt vervolgens aan de actiescripts doorgegeven als onbewerkte stringdata. Wanneer u een binding maakt met een stringeigenschap van een blueprint, zorgt u dat het blueprintonderdeel waarmee u de binding maakt, niet kan worden geclusterd. Als het onderdeel is geclusterd, wordt de stringwaarde een array en ontvangt u niet de waarde die u verwacht.

Voorbeeldstringeigenschap	Scriptsyntaxis	Voorbeeldgebruik
admin_email = "admin@email987.com"	Bash - \$admin_email	echo \$admin_email
	Windows CMD - %admin_email%	echo %admin_email%
	Windows PowerShell - \$admin_email	write-output \$admin_email

Arrayeigenschap

Arrayeigenschappen verwachten een array met stringwaarden, integerwaarden, decimale waarden of boolean-waarden die worden gedefinieerd als ["waarde1", "waarde2", "waarde3"...]. U kunt de waarde zelf opgeven, iemand anders kan worden verplicht de waarde op te geven of de waarde kan worden opgehaald bij een ander blueprintonderdeel door een binding te maken met een eigenschap.

Wanneer u een software-eigenschap van het type Array maakt, waarbij het gegevenstype integer of decimaal is, moet u een puntkomma gebruiken als scheidingsteken voor arrayelementen, ongeacht de landinstellingen. Gebruik geen komma (,) of punt (.). Voor sommige landinstellingen kunt u een komma (,) gebruiken als decimaal scheidingsteken. Bijvoorbeeld:

- Een geldige array voor het Frans is bijvoorbeeld als volgt: [1,11;2,22;3,33]
- Een geldige array voor het Engels is bijvoorbeeld als volgt: [1.11,2.22,3.33]

Wanneer u grote getallen in een array doorgeeft, gebruik dan de groeperingsindeling niet. Gebruik bijvoorbeeld niet **4444 444.000** (Frans), **4.444.444,000** (Italiaans) of **4,444,444.000** (Engels), omdat gegevensbestanden die landinstellingsspecifieke indelingen bevatten mogelijk verkeerd geïnterpreteerd kunnen worden wanneer ze worden doorgegeven aan een machine met een andere landinstelling. De groeperingsindeling is niet toegestaan omdat een getal zoals **4,444,444.000** als drie afzonderlijke getallen zou worden beschouwd. Voer in plaats daarvan gewoon **4444444.000** in.

Wanneer u waarden opgeeft voor een array-eigenschap, moet u de array insluiten in vierkante haakjes. Voor een array van strings kan de waarde in de arrayelementen alleen ASCII-tekens bevatten. Om een backslash correct te coderen in een waarde van een arrayeigenschap, moet u een extra backslash toevoegen, bijvoorbeeld ["c:\\test1\\test2"]. Voor een gebonden eigenschap gebruikt u het tabblad **Eigenschappen** in het ontwerpcanvas om de juiste eigenschap voor het binden te selecteren. Als u een binding maakt met een array, moet u echter wel uw eigen softwareonderdelen ontwerpen zodat ze geen array met waarden in een bepaalde volgorde verwachten.

Overweeg bijvoorbeeld om een virtual machine als load balancer te gebruiken om de belasting voor een cluster met virtual machines voor toepassingsservers te verdelen. In een dergelijk geval wordt een arrayeigenschap voor de load balancer-service gedefinieerd en ingesteld op de array IP-adressen van de virtual machines van de toepassingsserver.

Deze configuratiescripts van de load balancer-service gebruiken de arrayeigenschap om de juiste belastingverdeling in te stellen op de besturingssystemen Red Hat, Windows en Ubuntu.

Voorbeeld van de arrayeigenschap	Scriptsyntaxis	Voorbeeldgebruik
operating_systems = ["Red Hat","Windows","Ubuntu"]	Bash - \${operating_systems[@]} voor de gehele array van strings \${operating_systems[N]} voor het individuele arrayelement	for ((i = 0 ; i < \${#operating_systems[@]} ; i++)) ; do echo \${operating_systems[i]} done
	Windows CMD - %operating_systems_% waarbij <i>N</i> de positie van het element in de array vertegenwoordigt	for /F "delims== tokens=2" %%A in ('set operating_systems_') do (echo %%A)
	Windows PowerShell - \$operating_systems voor de gehele array van strings \$operating_systems[N] voor het individuele arrayelement	foreach (\$os in \$operating_systems){ write-output \$os }

Inhoudseigenschap

De waarde van de inhoudseigenschap is een URL naar een bestand voor het downloaden van inhoud. De Software-agent downloadt de inhoud van de URL naar de virtual machine en geeft de locatie van het lokale bestand in de virtual machine aan het script door.

Inhoudseigenschappen moeten als een geldige URL met het HTTP- of HTTPS-protocol worden gedefinieerd. Het Software-onderdeel van de JBOSS-toepassingsserver in de Dukes Bank-voorbeeldtoepassing geeft bijvoorbeeld een inhoudseigenschap `cheetah_tgz_url` op. De artefacten worden gehost in de Software-toepassing en de URL verwijst naar die locatie in de toepassing. De Software-agent downloadt de artefacten vanaf de opgegeven locatie naar de geïmplementeerde virtual machine.

Ga voor meer informatie over `software.http.proxy`-instellingen die kunnen worden gebruikt met inhoudseigenschappen naar *Naslaggids voor aangepaste eigenschappen*.

Voorbeeldstringeigenschap	Scriptsyntaxis	Voorbeeldgebruik
<code>cheetah_tgz_url = "http:// app_content_server_ip:port/artifacts/ software/jboss/cheetah-2.4.4.tar.gz"</code>	Bash - <code>\$cheetah_tgz_url</code>	<code>tar -zxvf \$cheetah_tgz_url</code>
	Windows CMD - <code>%cheetah_tgz_url%</code>	<code>start /wait c:\unzip.exe %cheetah_tgz_url%</code>
	Windows PowerShell - <code>\$cheetah_tgz_url</code>	<code>& c:\unzip.exe \$cheetah_tgz_url</code>

Eigenschap booleaans

Gebruik het eigenschapstype boolean om keuzes voor Waar en Onwaar op te geven in het vervolgkeuzemenu Waarde.

Eigenschap geheel getal

Gebruik het eigenschapstype integer voor nullen, en positieve of negatieve integers.

Decimale eigenschap

Gebruik het eigenschapstype decimaal voor waarden die niet-herhaalde decimale fracties voorstellen.

Wanneer uw Software-onderdeel informatie van een ander onderdeel nodig heeft

In diverse implementatiescenario's heeft een onderdeel de eigenschapswaarde van een ander onderdeel nodig om te kunnen worden aangepast. Dit kunt u met vRealize Automation doen door eigenschapsbindingen te maken. U kunt uw Software-actiescripts voor eigenschapsbindingen ontwerpen, maar de werkelijke bindingen worden geconfigureerd door de architect die de blueprint samenstelt.

Naast het instellen van een eigenschap voor een hardgecodeerde waarde, kan een softwarearchitect, IaaS-architect of toepassingsarchitect Software-onderdeeleigenschappen aan andere eigenschappen in de blueprint binden, zoals een IP-adres of een installatielocatie. Wanneer u een Software-eigenschap bindt aan een andere eigenschap, kunt u een script aanpassen op basis van de waarde van een andere onderdeeleigenschap of eigenschap van een virtual machine. Een WAR-onderdeel heeft bijvoorbeeld mogelijk de installatielocatie van de Apache Tomcat-server nodig. In uw scripts kunt u het WAR-onderdeel configureren voor het instellen van de eigenschapswaarde `server_home` op de eigenschapswaarde `install_path` voor de Apache Tomcat-server in uw script. Zolang de architect die de blueprint samenstelt de `server_home`-eigenschap aan de `install_path`-eigenschap van de Apache Tomcat-server bindt, is de eigenschapswaarde `server_home` op de juiste manier ingesteld.

Uw actiescripts kunnen alleen eigenschappen gebruiken die u in deze scripts opgeeft, en u kunt alleen eigenschapsbindingen maken met string- en arraywaarden. Eigenschapsarrays van blueprints worden niet in een specifieke volgorde geretourneerd, dus een binding met clusterbare of schaalbare onderdelen levert wellicht niet de verwachte waarden. Als voor uw softwareonderdeel bijvoorbeeld de machine-ID's van elke machine in een reeks zijn vereist, en u uw gebruikers toestemming geeft om een reeks van 1 t/m 10 op te vragen, en de implementatie op te schalen van 1 tot 10 machines. Als u uw software-eigenschap als stringtype configureert, ontvangt u een willekeurig geselecteerde machine-ID van het cluster. Als u uw software-eigenschap als arraytype configureert, ontvangt u een array van alle machine-ID's in het cluster, maar niet in een bepaalde volgorde. Als uw gebruikers de implementatie opschalen, kan de volgorde van waarden per bewerking verschillen. Als u zeker wilt weten dat u nooit waarden van geclusterde onderdelen verliest, kunt u het arraytype voor alle software-eigenschappen gebruiken. U moet echter wel uw eigen softwareonderdelen ontwerpen zodat ze geen array met waarden in een bepaalde volgorde verwachten.

Raadpleeg de tabel Voorbeelden van stringeigenschapsbindingen voor voorbeelden van een stringeigenschapswaarde bij het binden met verschillende soorten eigenschappen.

Tabel 3-45. Voorbeelden van stringeigenschapsbindingen

Voorbeeld van eigenschapstype	Eigenschapstype om te binden	Uitkomst van binden (A bindt zich aan B)
String (eigenschap A)	String (eigenschap B="Hi")	A="Hi"
String (eigenschap A)	Inhoud (eigenschap B="http://my.com/content")	A="http://my.com/content"
String (eigenschap A)	Array (eigenschap B=["1","2"])	A=["1","2"]
String (eigenschap A)	Berekend (eigenschap B="Hallo")	A="Hallo"

Raadpleeg de tabel Voorbeelden van array-eigenschapsbindingen voor voorbeelden van een array-eigenschapswaarde bij het binden met verschillende soorten eigenschappen.

Tabel 3-46. Voorbeelden van array-eigenschapsbindingen

Voorbeeld van eigenschapstype	Eigenschapstype om te binden	Uitkomst van binden (A bindt zich aan B)
Array (eigenschap A)	String (eigenschap B="Hi")	A="Hi"
Array (eigenschap A)	Inhoud (eigenschap B="http://my.com/content")	A="http://my.com/content"
Array (eigenschap A)	Berekend (eigenschap B="Hallo")	A="Hallo"

Zie [Opties voor eigenschapstypen en -instellingen](#) voor een uitgebreide beschrijving van de ondersteunde eigenschapstypen.

Eigenschapswaarden tussen levenscyclusfasen verplaatsen

U kunt actiescripts gebruiken om eigenschapswaarden van de ene levenscyclusfase naar de andere te verplaatsen en door te geven.

Voor een berekende eigenschap kunt u de waarde aanpassen en de waarde naar de volgende levenscyclusfase van het actiescript verplaatsen. Als voor onderdeel A bijvoorbeeld de waarde `progress_status` als gefaseerd is gedefinieerd, wijzigt u deze waarde in `progress_status=installed` in de desbetreffende actiescripts van de levenscyclusfasen **INSTALLEREN** en **CONFIGUREREN**. Als onderdeel B aan onderdeel A is gebonden, zijn de eigenschapswaarden van `progress_status` in de levenscyclusfasen van het actiescript dezelfde als bij onderdeel A.

Definieer in het softwareonderdeel dat onderdeel B afhankelijk is van A. Deze afhankelijkheid bepaalt de verplaatsing van de juiste eigenschapswaarden tussen onderdelen, of ze zich nu in hetzelfde knooppunt of in verschillende knooppunten bevinden.

U kunt bijvoorbeeld een eigenschapswaarde in een actiescript bijwerken met behulp van de ondersteunde scripts.

- Bash `progress_status="completed"`
- Windows CMD `set progress_status=completed`
- Windows PowerShell `$progress_status="completed"`

Opmerking Array- en inhoudeigenschappen ondersteunen de verplaatsing van aangepaste eigenschapswaarden tussen actiescripts van levenscyclusfasen niet.

Beste praktijken voor het ontwikkelen van onderdelen

U kunt de beste praktijken voor het definiëren van eigenschappen en actiescripts uitproberen door Software-onderdelen en toepassingsblueprints te downloaden en importeren van de VMware Solution Exchange.

Volg deze beste praktijken bij het ontwikkelen van Software-onderdelen.

- Om een script zonder onderbrekingen uit te voeren, moet de returnwaarde op nul (0) worden ingesteld. Deze instelling geeft de agent de mogelijkheid om alle eigenschappen vast te leggen en deze naar de Software-server te versturen.
- Sommige installatieprogramma's hebben toegang tot de tty-console nodig. Leid de in invoer om van `/dev/console`. Het RabbitMQ Software-onderdeel gebruikt bijvoorbeeld mogelijk de opdracht `./rabbitmq_rhel.py --setup-rabbitmq < /dev/console` in het installatiescript.
- Wanneer een onderdeel een levenscyclus met meerdere fasen heeft, kan de eigenschapswaarde veranderd worden in de **INSTALLATIE**-fase. De nieuwe waarde wordt naar de volgende fase in de levenscyclus verzonden. Actiescripts kunnen de waarde van een eigenschap berekenen gedurende de implementatie om de waarde aan andere afhankelijke scripts te leveren. In bijvoorbeeld de voorbeeldtoepassing **Clustered Dukes Bank** berekent de service `JBossAppServer` de eigenschap `JVM_ROUTE` gedurende de installatiefase in de levenscyclus. Deze eigenschap wordt door de service `JBossAppServer` gebruikt voor het

configureren van de levenscyclus. De service Apache load balancer verbindt vervolgens de eigenschap JVM_ROUTE aan de eigenschap all(appserver:JbossAppServer:JVM_ROUTE) om de uiteindelijke berekende waarde voor knooppunt0 en knooppunt1 te verkrijgen. Indien een onderdeel een eigenschapswaarde van een ander onderdeel vereist voor het succesvol voltooien van een toepassingsimplementatie, moet u afhankelijkheden uitdrukkelijk in de toepassingsblueprint vermelden.

Opmerking Het is niet mogelijk om de eigenschapswaarde van de inhoud van een onderdeel te wijzigen wanneer dit een levenscyclus van meerdere fasen heeft.

Een Softwareonderdeel maken

Configureer en publiceer een Softwareonderdeel dat andere softwarearchitecten, IaaS-architecten en toepassingsarchitecten kunnen gebruiken om toepassingsblueprints samen te stellen.

Voorwaarden

Meld u aan bij vRealize Automation als een **softwarearchitect**.

Procedure

1 Selecteer **Ontwerpen > Softwareonderdelen**.

2 Klik op het pictogram **Toevoegen (+)**.

3 Voer een naam in en desgewenst een beschrijving.

Op basis van de opgegeven naam voor het Software-onderdeel genereert vRealize Automation voor het Software-onderdeel een unieke id voor de tenant. U kunt dit veld nu bewerken, maar u kunt het niet meer wijzigen nadat u de blueprint hebt opgeslagen. Omdat id's permanent en uniek zijn in uw tenant, kunt u deze gebruiken om via een programma met blueprints te communiceren en eigenschapsbindingen te maken.

4 (Optioneel) Als u wilt beheren hoe uw Softwareonderdeel wordt toegevoegd aan blueprints, selecteert u een type container in het vervolgkeuzemenu **Container**.

Optie	Beschrijving
Machines	Uw Softwareonderdeel moet direct op een machine worden geplaatst.
Een van uw gepubliceerde Softwareonderdelen	Als u een Softwareonderdeel ontwerpt dat specifiek moet worden geïnstalleerd op een ander Softwareonderdeel dat u hebt gemaakt, selecteert u het betreffende Softwareonderdeel in de lijst. Als u bijvoorbeeld een EAR-onderdeel ontwerpt dat moet worden geïnstalleerd op een eerder gemaakt JBOSS-onderdeel, selecteert u het JBOSS-onderdeel in de lijst.
Softwareonderdelen	Als u een Softwareonderdeel ontwerpt dat niet rechtstreeks op een machine moet worden geïnstalleerd, maar dat in verschillende Softwareonderdelen kan worden geïnstalleerd, selecteert u de optie Softwareonderdelen. Als u bijvoorbeeld een WAR-onderdeel ontwerpt en dit wilt installeren in uw Tomcat Server Software-onderdeel en uw Tcserver Software-onderdeel, selecteert u het containertype Softwareonderdelen.

5 Klik op **Volgende**.

6 Geef de eigenschappen op die u van plan bent te gebruiken in uw actiescripts.

- Klik op het pictogram **Toevoegen (+)**.
- Voer een naam in voor de eigenschap.
- Voer een beschrijving in voor de eigenschap.

Deze beschrijving wordt weergegeven voor architecten die uw Softwareonderdeel in blueprints gebruiken.

- Selecteer het verwachte type voor de waarde van uw eigenschap.
- Geef de waarde voor uw eigenschap op.

Optie	Beschrijving
De waarde gebruiken die u nu opgeeft	<ul style="list-style-type: none"> Voer een waarde in. Schakel Overschrijfbaar uit. Selecteer Vereist.
Vereisen dat architecten een waarde opgeven	<ul style="list-style-type: none"> Voer een waarde in als u een standaardwaarde wilt leveren. Schakel Overschrijfbaar in. Selecteer Vereist.
Architecten toestaan om een waarde op te geven als ze dit willen	<ul style="list-style-type: none"> Voer een waarde in als u een standaardwaarde wilt leveren. Schakel Overschrijfbaar in. Schakel Vereist uit.

Architecten kunnen de Softwareeigenschappen zo configureren dat deze in het aanvraagformulier aan gebruikers worden getoond. Architecten kunnen de optie Weergeven in aanvraag gebruiken om te vereisen of aan te vragen dat gebruikers waarden invullen voor eigenschappen die u als overschrijfbaar aanduidt.

7 Volg de prompts en geef een script op voor ten minste een van de acties voor de levenscyclus van de software.

Tabel 3-47. Levenscyclusacties

Levenscyclusacties	Beschrijving
Installeren	Installeer uw software. U kunt bijvoorbeeld de installatiefragmenten van Tomcat-server downloaden en een Tomcat-service installeren. Scripts die u voor de actie Levenscyclus installeren schrijft, worden uitgevoerd wanneer de software voor de eerste keer wordt ingericht, tijdens een eerste implementatieaanvraag of als onderdeel van een opschaling.
Configureren	Configureer uw software. Voor het voorbeeld van Tomcat kunt u de JAVA_OPTS en CATALINA_OPTS instellen. Configuratiescripts worden uitgevoerd nadat de installatie-actie is voltooid.
Start	Start uw software. U kunt bijvoorbeeld proberen de Tomcat-service te starten met behulp van de startopdracht in de Tomcat-server. Startscripts worden uitgevoerd nadat de configuratie-actie is voltooid.

Tabel 3-47. Levenscyclusacties (vervolg)

Levenscyclusacties	Beschrijving
Bijwerken	Als u uw softwareonderdeel zodanig ontwerpt dat deze schaalbare blueprints kan ondersteunen, dient u alle updates uit te voeren die vereist zijn na een opschaal- of neerschaalbewerking. U kunt bijvoorbeeld de cluster grootte van een geschaalde implementatie wijzigen en de geclusterde knooppunten beheren met behulp van een load balancer. Ontwerp uw updatescripts zodanig dat ze meerdere keren kunnen worden uitgevoerd (idempotent) en dat ze zowel opschaal- als neerschaalbewerkingen kunnen uitvoeren. Wanneer een schalingsbewerking is uitgevoerd, kunnen er updatescripts worden uitgevoerd op alle afhankelijke softwareonderdelen.
Installatie ongedaan maken	Verwijder uw software. U kunt bijvoorbeeld specifieke acties uitvoeren in de toepassing voordat een implementatie wordt vernietigd. Verwijderingsscripts worden uitgevoerd wanneer softwareonderdelen worden vernietigd.

Gebruik afsluit- en statuscodes in uw actiescripts. Elk ondersteunde scripttype heeft unieke vereisten voor afsluit- en statuscodes.

Scripttype	Geslaagde status	Foutstatus	Niet-ondersteunde opdrachten
Bash	■ return 0 ■ exit 0	■ return non-zero ■ exit non-zero	Geen
Windows CMD	exit /b 0	exit /b non-zero	Geen exit 0- of exit non-zero-codes gebruiken.
PowerShell	exit 0	exit non-zero;	Geen warning-, verbose-, debug- of host-aanroepen gebruiken.

- 8 Schakel het selectievakje **Opnieuw opstarten** in voor scripts waarvoor het vereist is dat de machine opnieuw wordt opgestart.

Nadat het script is uitgevoerd, wordt de machine opgestart voordat het volgende levenscyclusscript wordt gestart.

- 9 Klik op **Voltooien**.

- 10 Selecteer het Software-onderdeel en klik op **Publiceren**.

Resultaten

U hebt een Softwareonderdeel geconfigureerd en gepubliceerd. Andere softwarearchitecten, IaaS-architecten en toepassingsarchitecten kunnen dit Softwareonderdeel gebruiken om software toe te voegen aan toepassingsblueprints.

Wat nu te doen

Voeg uw gepubliceerde Softwareonderdeel toe aan een toepassingsblueprint. Zie [Samengestelde blueprints samenstellen](#).

Instellingen voor Software-onderdelen

Configureer algemene instellingen, maak eigenschappen en schrijf aangepaste actiescripts om een Software-onderdeel op ingerichte machines te installeren, te configureren, bij te werken of te verwijderen.

Als softwarearchitect klikt u op **Ontwerpen > Softwareonderdelen** en vervolgens op het pictogram **Toevoegen** om een nieuw Software-onderdeel te maken.

Algemene instellingen voor nieuwe Software

Pas algemene instellingen toe op uw Software-onderdeel.

Tabel 3-48. Algemene instellingen voor nieuwe Software

Instelling	Beschrijving
Naam	Voer een naam in voor het Software-onderdeel.
Id	Op basis van de opgegeven naam voor het Software-onderdeel genereert vRealize Automation voor het Software-onderdeel een unieke id voor de tenant. U kunt dit veld nu bewerken, maar u kunt het niet meer wijzigen nadat u de blueprint hebt opgeslagen. Omdat id's permanent en uniek zijn in uw tenant, kunt u deze gebruiken om via een programma met blueprints te communiceren en eigenschapsbindingen te maken.
Beschrijving	Vat uw Software-onderdeel samen ten behoeve van andere architecten.
Container	<p>Op het ontwerpcanvas kunnen blueprintarchitecten alleen uw Software-onderdeel in het containertype plaatsen dat u selecteert.</p> <ul style="list-style-type: none"> ■ Selecteer Machines om architecten te verplichten uw Software-onderdeel rechtstreeks in een machineonderdeel op het ontwerpcanvas te plaatsen. ■ Selecteer Softwareonderdelen als u een Software-onderdeel ontwerpt dat nooit rechtstreeks in een machineonderdeel mag worden geplaatst, maar wel in een of verschillende Software-onderdelen kan worden genest. ■ Selecteer een specifiek gepubliceerd Software-onderdeel als u een Software-onderdeel ontwerpt dat specifiek in een ander Software-onderdeel dat u hebt gemaakt, kan worden genest. ■ Selecteer Azure virtual machine als u een Software-onderdeel specifiek voor een Azure-blueprint ontwerpt.

Eigenschappen voor nieuwe Software

Software-onderdeeleigenschappen worden gebruikt om parameters aan scripts toe te voegen om de gedefinieerde eigenschappen als omgevingsvariabelen door te geven aan scripts die op een machine worden uitgevoerd. Voordat de scripts worden uitgevoerd, vraagt de Software-agent van de ingerichte machine de gewenste eigenschappen op bij vRealize Automation. De agent maakt met deze eigenschappen vervolgens scriptspecifieke variabelen en geeft deze door aan de scripts.

Tabel 3-49. Eigenschappen voor nieuwe Software

Instelling	Beschrijving
Naam	Voer een naam in voor de Software-eigenschap. De namen van eigenschappen zijn hoofdlettergevoelig en kunnen alleen letters, cijfers, streepjes (-) en lage streepjes (_) bevatten.
Beschrijving	U kunt ten behoeve van andere gebruikers een samenvatting geven van de eigenschap en de vereisten voor de bijbehorende waarde.
Type	Software ondersteunt de typen string, array, inhoud, boolean en integer. Voor een uitgebreide uitleg van ondersteunde eigenschapstypen, raadpleegt u Opties voor eigenschapstypen en -instellingen . Voor meer informatie over eigenschapsbindingen, raadpleegt u Wanneer uw Software-onderdeel informatie van een ander onderdeel nodig heeft en Eigenschapsbindingen maken tussen blueprintonderdelen .
Waarde	<ul style="list-style-type: none"> ■ Als u de waarde die u opgeeft, wilt laten gebruiken, gaat u als volgt te werk: <ul style="list-style-type: none"> ■ Geef een Waarde op. ■ Selecteer Vereist. ■ Schakel Overschrijfbaar uit. ■ Als u architecten wilt verplichten een waarde op te geven, gaat u als volgt te werk: <ul style="list-style-type: none"> ■ (Optioneel) Geef een Waarde op als standaardwaarde. ■ Schakel Overschrijfbaar in. ■ Selecteer Vereist. ■ Als u architecten de mogelijkheid wilt bieden een waarde op te geven of de waarde leeg te laten, gaat u als volgt te werk: <ul style="list-style-type: none"> ■ (Optioneel) Geef een Waarde op als standaardwaarde. ■ Schakel Overschrijfbaar in. ■ Schakel Vereist uit.
Gecodeerd	<p>Geeft aan dat de eigenschap gecodeerd is en dat de waarde in vRealize Automation gemaskeerd wordt weergegeven met sterretjes. Als u de eigenschap terugzet op ongecodeerd, wordt de eigenschapswaarde opnieuw ingesteld door vRealize Automation. U moet om veiligheidsredenen een nieuwe waarde voor de eigenschap instellen.</p> <p>Belangrijk Als beveiligde eigenschappen worden afgedrukt in het script met behulp van de opdracht echo of andere vergelijkbare opdrachten, worden deze waarden als platte tekst in de logbestanden weergegeven. De waarden in de logbestanden zijn wel zichtbaar.</p>

Tabel 3-49. Eigenschappen voor nieuwe Software (vervolg)

Instelling	Beschrijving
Overschrijfbaar	U kunt architecten bij het samenstellen van een toepassingsblueprint toestaan de waarde van deze eigenschap te overschrijven. De waarde die u invoert, wordt als standaardwaarde weergegeven.
Vereist	U kunt vereisen dat architecten een waarde voor deze eigenschap opgeven of anders uw standaardwaarde moeten accepteren.
Berekend	Waarden voor berekende bronnen worden toegewezen door de levenscyclusscripts INSTALL, CONFIGURE, START en UPDATE. De toegewezen waarde wordt doorgegeven naar de daaropvolgende beschikbare levenscyclusfasen en naar onderdelen die gebonden zijn aan deze eigenschappen in een blueprint. Als u Berekend selecteert voor een eigenschap die geen stringeigenschap is, wordt het eigenschapstype gewijzigd in string.

Acties voor nieuwe Software

U maakt Bash-, Windows CMD-, of PowerShell-actiescripts om exact op te geven hoe onderdelen worden geïnstalleerd, geconfigureerd, verwijderd of bijgewerkt tijdens schalingsbewerkingen van de implementatie.

Tabel 3-50. Levenscyclusacties

Levenscyclusacties	Beschrijving
Installeren	Installeer uw software. U kunt bijvoorbeeld de installatiefragmenten van Tomcat-server downloaden en een Tomcat-service installeren. Scripts die u voor de actie Levenscyclus installeren schrijft, worden uitgevoerd wanneer de software voor de eerste keer wordt ingericht, tijdens een eerste implementatieaanvraag of als onderdeel van een opschaling.
Configureren	Configureer uw software. Voor het voorbeeld van Tomcat kunt u de JAVA_OPTS en CATALINA_OPTS instellen. Configuratiescripts worden uitgevoerd nadat de installatie-actie is voltooid.
Start	Start uw software. U kunt bijvoorbeeld proberen de Tomcat-service te starten met behulp van de startopdracht in de Tomcat-server. Startscripts worden uitgevoerd nadat de configuratie-actie is voltooid.
Bijwerken	Als u uw softwareonderdeel zodanig ontwerpt dat deze schaalbare blueprints kan ondersteunen, dient u alle updates uit te voeren die vereist zijn na een opschaal- of neerschaalbewerking. U kunt bijvoorbeeld de clustergrootte van een geschaalde implementatie wijzigen en de geclusterde knooppunten beheren met behulp van een load balancer. Ontwerp uw updatescripts zodanig dat ze meerdere keren kunnen worden uitgevoerd (idempotent) en dat ze zowel opschaal- als neerschaalbewerkingen kunnen uitvoeren. Wanneer een schalingsbewerking is uitgevoerd, kunnen er updatescripts worden uitgevoerd op alle afhankelijke softwareonderdelen.
Installatie ongedaan maken	Verwijder uw software. U kunt bijvoorbeeld specifieke acties uitvoeren in de toepassing voordat een implementatie wordt vernietigd. Verwijderingsscripts worden uitgevoerd wanneer softwareonderdelen worden vernietigd.

Schakel het selectievakje **Opnieuw opstarten** in voor scripts waarvoor het vereist is dat de machine opnieuw wordt opgestart. Nadat het script is uitgevoerd, wordt de machine opgestart voordat het volgende levenscyclusscript wordt gestart. Controleer of er geen processen zijn die prompts geven voor gebruikersinteractie wanneer het actiescript wordt uitgevoerd. Scripts worden stopgezet door onderbrekingen, waardoor ze oneindig in ruststand blijven, en daardoor uiteindelijk mislukken. Bovendien moeten uw scripts de juiste afsluitcodes bevatten die kunnen worden toegepast op de toepassingsimplementatie. Als het script geen afsluit- en retourcodes bevat, wordt de opdracht in het script die als laatste is uitgevoerd de afsluitstatus. Afsluit- en retourcodes verschillen per ondersteund scripttype, Bash, Windows CMD, PowerShell.

Scripttype	Geslaagde status	Foutstatus	Niet-ondersteunde opdrachten
Bash	<ul style="list-style-type: none"> ■ return 0 ■ exit 0 	<ul style="list-style-type: none"> ■ return non-zero ■ exit non-zero 	Geen
Windows CMD	exit /b 0	exit /b non-zero	Geen exit 0- of exit non-zero-codes gebruiken.
PowerShell	exit 0	exit non-zero;	Geen warning-, verbose-, debug- of host-aanroepen gebruiken.

XaaS-blueprints en bronacties ontwerpen

De XaaS-blueprints kunnen worden gepubliceerd als catalogusitem of kunnen worden gebruikt in het blueprintontwerpprogramma. De bronacties zijn acties die u uitvoert op geïmplementeerde items.

XaaS gebruikt vRealize Orchestrator voor het uitvoeren van werkstromen waarmee items worden ingericht of acties worden uitgevoerd. U kunt bijvoorbeeld de werkstromen configureren om vSphere virtual machines, Active Directory-gebruikers in groepen te maken of om PowerShell-scripts uit te voeren. Als u een aangepaste vRealize Orchestrator-werkstroom maakt, kunt u die werkstroom als item beschikbaar maken in de servicecatalogus, zodat gebruikers aan wie rechten zijn verleend de werkstroom kunnen uitvoeren.

U kunt een XaaS-blueprint gebruiken als een onderdeel in een blueprint die u maakt in het ontwerpcanvas of u kunt de blueprint direct publiceren in de servicecatalogus.

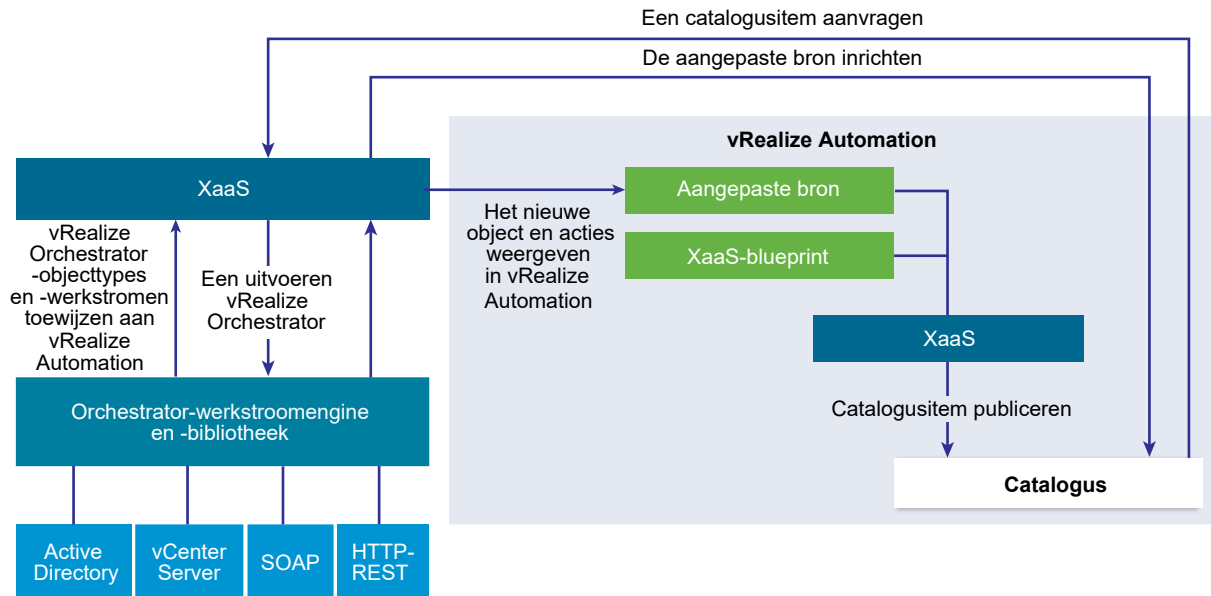
Als u een blueprint gebruikt als een onderdeel in een andere blueprint, kunt u deze zo configureren dat de schaal ervan wordt aangepast wanneer de blueprint wordt opgeschaald of neergeschaald.

vRealize Orchestrator-integratie in vRealize Automation

vRealize Orchestrator is de werkstroomengine die is geïntegreerd in vRealize Automation.

De vRealize Orchestrator-server die wordt gedistribueerd met vRealize Automation is vooraf geconfigureerd. Als uw systeembeheerder de vRealize Automation-toepassing implementeert, is als gevolg daarvan de vRealize Orchestrator-server actief.

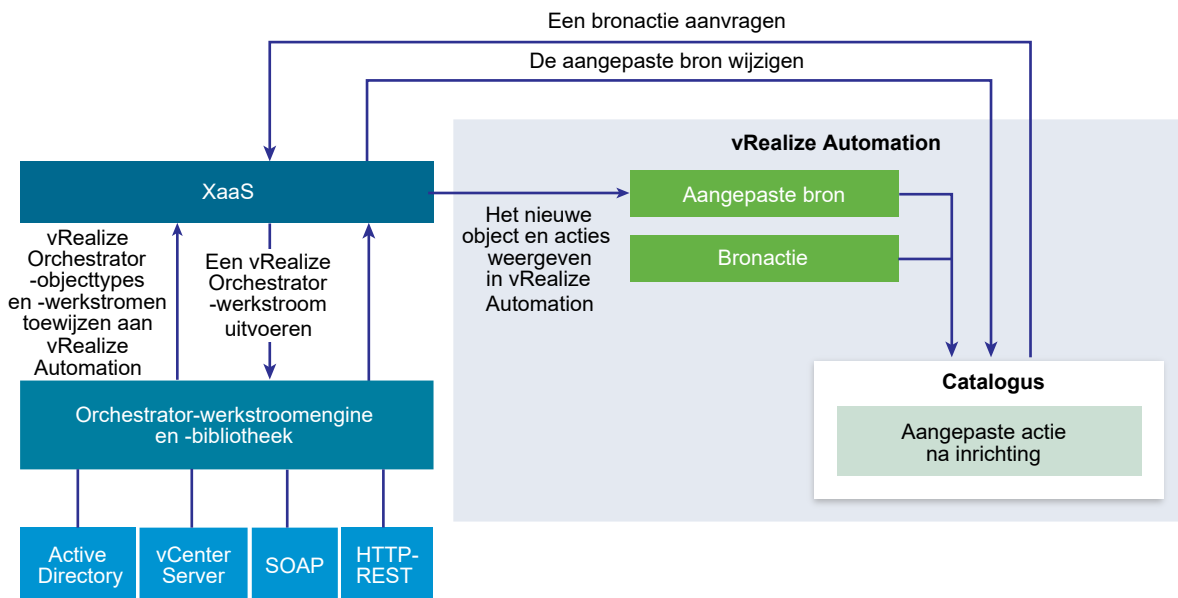
Figuur 3-2. Catalogusitems die zijn opgenomen in een XaaS maken en aanvragen om een aangepaste bron in te richten



XaaS-architecten voegen aangepaste bronnen toe die verbonden zijn aan de ondersteunde endpoints en opgegeven werkstromen, en vervolgens maken ze XaaS-blueprints en -acties op basis van deze bronnen. Tenantbeheerders en bedrijfsgroepbeheerders kunnen de XaaS-blueprints en -acties toevoegen aan de servicecatalogus. De XaaS-blueprint kan ook in het blueprintontwerpprogramma worden gebruikt.

Wanneer de gebruiker van de servicecatalogus een item aanvraagt, voert vRealize Automation een vRealize Orchestrator-werkstroom uit om de aangepaste bron in te richten.

Figuur 3-3. Aangepaste bronacties maken en aanvragen om een aangepaste bron te wijzigen



XaaS-architecten kunnen ook vRealize Orchestrator-werkstromen toevoegen als bronacties om de vRealize Automation-mogelijkheden uit te breiden. Nadat de gebruikers van de servicecatalogus een aangepaste bron hebben ingericht, kunnen ze de actie na inrichting uitvoeren. Op die manier voeren de consumenten een vRealize Orchestrator-werkstroom uit en wijzigen ze de ingerichte aangepaste bron.

Wanneer een gebruiker van de servicecatalogus een XaaS-blueprint of -bronactie aanvraagt als een catalogusitem, voert de XaaS-service de overeenkomstige vRealize Orchestrator-werkstroom uit zodat de volgende gegevens als algemene parameters naar de werkstroom worden doorgegeven:

Tabel 3-51. Algemene parameters voor XaaS

Parameter	Beschrijving
__asd_tenantRef	De tenant van de gebruiker die de werkstroom aanvraagt.
__asd_subtenantRef	De bedrijfsgroep van de gebruiker die de werkstroom aanvraagt.
__asd_catalogRequestId	De aanvraag-id van de catalogus voor deze werkstroomuitvoering.
__asd_requestedFor	De doelgebruiker van de aanvraag. Als de aanvraag namens een gebruiker wordt gedaan, dan is dit de gebruiker namens wie de werkstroom wordt aangevraagd. Als dit niet het geval is, is dit de gebruiker die de werkstroom aanvraagt.
__asd_requestedBy	De gebruiker die de werkstroom aanvraagt.

Als een XaaS-blueprint of -bronactie een vRealize Orchestrator-werkstroom gebruikt die een schema-element voor gebruikersinteractie bevat en een consument vraagt de service aan, dan onderbreekt de werkstroom de uitvoering ervan en wacht deze totdat de gebruiker de vereiste gegevens opgeeft. Om een gebruikersinteractie die in de wacht staat, te beantwoorden, moet de gebruiker naar **Postvak IN > Handmatige gebruikersactie** gaan.

De standaardvRealize Orchestrator-serverinventaris wordt gedeeld door alle tenants en kan niet per tenant worden gebruikt. Als een servicearchitect bijvoorbeeld een serviceblueprint maakt voor het maken van een geclusterde computerbron, dan moeten de consumenten van verschillende tenants door de inventarisitems van alle vCenter Server-instanties bladeren hoewel deze mogelijk bij een andere tenant horen.

Systeembeheerders kunnen vRealize Orchestrator installeren of de vRealize Orchestrator Appliance afzonderlijk implementeren om een externe vRealize Orchestrator-instantie in te stellen en vRealize Automation configureren om te werken met deze externe vRealize Orchestrator-instantie.

Systeembeheerders kunnen ook vRealize Orchestrator-werkstroomcategorieën configureren per tenant en bepalen welke werkstromen beschikbaar zijn voor elke tenant.

Bovendien kunnen tenantbeheerders ook een externe vRealize Orchestrator-instantie configureren, maar alleen voor hun eigen tenants.

Voor informatie over het configureren van een externe vRealize Orchestrator-instantie en vRealize Orchestrator-werkstroomcategorieën raadpleegt u *vCenter Orchestrator en invoegtoepassingen configureren*.

Lijst met vRealize Orchestrator-invoegtoepassingen

Met invoegtoepassingen kunt u vRealize Orchestrator gebruiken om toegang te krijgen tot externe technologieën en toepassingen en deze te beheren. Doordat een externe technologie beschikbaar wordt gemaakt in een vRealize Orchestrator-invoegtoepassing, kunt u objecten en functies opnemen in werkstromen die toegang krijgen tot de objecten en functies van de externe technologie.

De externe technologieën waartoe u toegang hebt via invoegtoepassingen kunnen beheertools voor virtualisatie, e-mailsystemen, databases, directoryservices, interfaces voor beheer op afstand, enzovoort omvatten.

U kunt de standaardset vRealize Orchestrator-invoegtoepassingen gebruiken om externe technologieën, zoals de vCenter Server API en e-mailfuncties, op te nemen in werkstromen. U kunt bovendien de open vRealize Orchestrator-architectuur voor invoegtoepassingen gebruiken om invoegtoepassingen te maken die toegang kunnen verkrijgen tot andere toepassingen.

Tabel 3-52. Invoegtoepassingen die standaard deel uitmaken van vRealize Orchestrator

Plug-In	Doel
vCenter Server	Biedt toegang tot de vCenter Server API, zodat u alle vCenter Server-objecten en -functies kunt opnemen in de beheerprocessen die u automatiseert met vRealize Orchestrator.
Configuration	Biedt werkstromen voor het configureren van de verificatie, databaseverbinding, SSL-certificaten, enzovoort van vRealize Orchestrator.
vCO Library	Biedt werkstromen die fungeren als bouwstenen voor aanpassing en automatisering van clientprocessen. De werkstroombibliotheek bevat sjablonen voor levenscyclusbeheer, inrichting, noodherstel, back-ups zonder opnieuw opstarten en andere standaardprocessen. U kunt de sjablonen kopiëren en bewerken en aan uw behoeften aanpassen.
SQL	Levert de Java Database Connectivity API (JDBC), de industriestandaard voor database-onafhankelijke connectiviteit tussen de Java-programmeertaal en een groot aantal databases. De databases omvatten de SQL-databases en andere gegevensbronnen in tabelvorm, zoals spreadsheets of platte bestanden. De JDBC API biedt een API op oproepniveau voor databasetoegang via SQL vanuit werkstromen.
SSH	Levert een implementatie van het Secure Shell v2-protocol (SSH-2). Maakt externe opdracht- en bestandsoverdrachtsessies in werkstromen mogelijk met verificatie op basis van wachtwoorden en openbare sleutels. Ondersteunt interactieve verificatie via toetsenborden. Optioneel kan de SSH-invoegtoepassing direct bladeren in het externe bestandssysteem van de vRealize Orchestrator-clientinventaris bieden.

Tabel 3-52. Invoegtoepassingen die standaard deel uitmaken van vRealize Orchestrator (vervolg)

Plug-In	Doel
XML	Een volledige Document Object Model XML-parser (DOM) die u in werkstromen kunt implementeren. U kunt ook de ECMAScript for XML-implementatie (E4X) in de vRealize Orchestrator JavaScript API gebruiken.
Mail	Maakt gebruik van Simple Mail Transfer Protocol (SMTP) voor het verzenden van e-mail vanuit werkstromen.
Net	Verpakt de Jakarta Apache Commons Net Library. Biedt implementaties van Telnet, FTP, POP3 en IMAP. Het POP3- en IMAP-gedeelte wordt gebruikt voor het lezen van e-mail. In combinatie met de Mail-invoegtoepassing biedt de Net-invoegtoepassing volledige verzend- en ontvangstmogelijkheden voor e-mail in werkstromen.
Enumeration	Levert veelgebruikte opgesomde typen die kunnen worden gebruikt door andere werkstromen.
Workflow documentation	Biedt werkstromen waarmee u informatie in PDF-indeling kunt genereren over een werkstroom of een werkstroomcategorie.
HTTP-REST	Hiermee kunt u REST-webservices beheren dankzij interactie tussen vCenter Orchestrator en REST-hosts.
SOAP	Hiermee kunt u SOAP-webservices beheren dankzij interactie tussen vCenter Orchestrator en SOAP-hosts.
AMQP	Hiermee kunt u interacties aangaan met Advanced Message Queuing Protocol-servers (AMQP), die ook brokers worden genoemd.
SNMP	Hiermee kan vCenter Orchestrator een verbinding maken met en informatie ontvangen van systemen waarop SNMP ingeschakeld is.
Active Directory	Levert interactie tussen vCenter Orchestrator en Microsoft Active Directory.
vCO WebOperator	Een webweergave die toegang biedt tot de werkstromen in de vRealize Orchestrator-bibliotheek en hiermee interacties kan aangaan via een netwerk met behulp van een webbrowser.
Dynamic Types	Hiermee kunt u dynamische typen definiëren en objecten van deze dynamische typen maken en gebruiken.
PowerShell	Hiermee kunt u PowerShell-hosts beheren en aangepaste PowerShell-bewerkingen uitvoeren.
Multi-Node	Bevat werkstromen voor hiërarchische orkestratie, beheer van Orchestrator-instanties en uitschalen van Orchestrator-activiteiten.
vRealize Automation	Hiermee kunt u werkstromen maken en uitvoeren voor interactie tussen vRealize Orchestrator en vRealize Automation.

Zie de landingspagina van de VMware vRealize™ Orchestrator™-documentatie voor meer informatie over de vRealize Orchestrator-invoegtoepassingen die VMware ontwikkelt en distribueert.

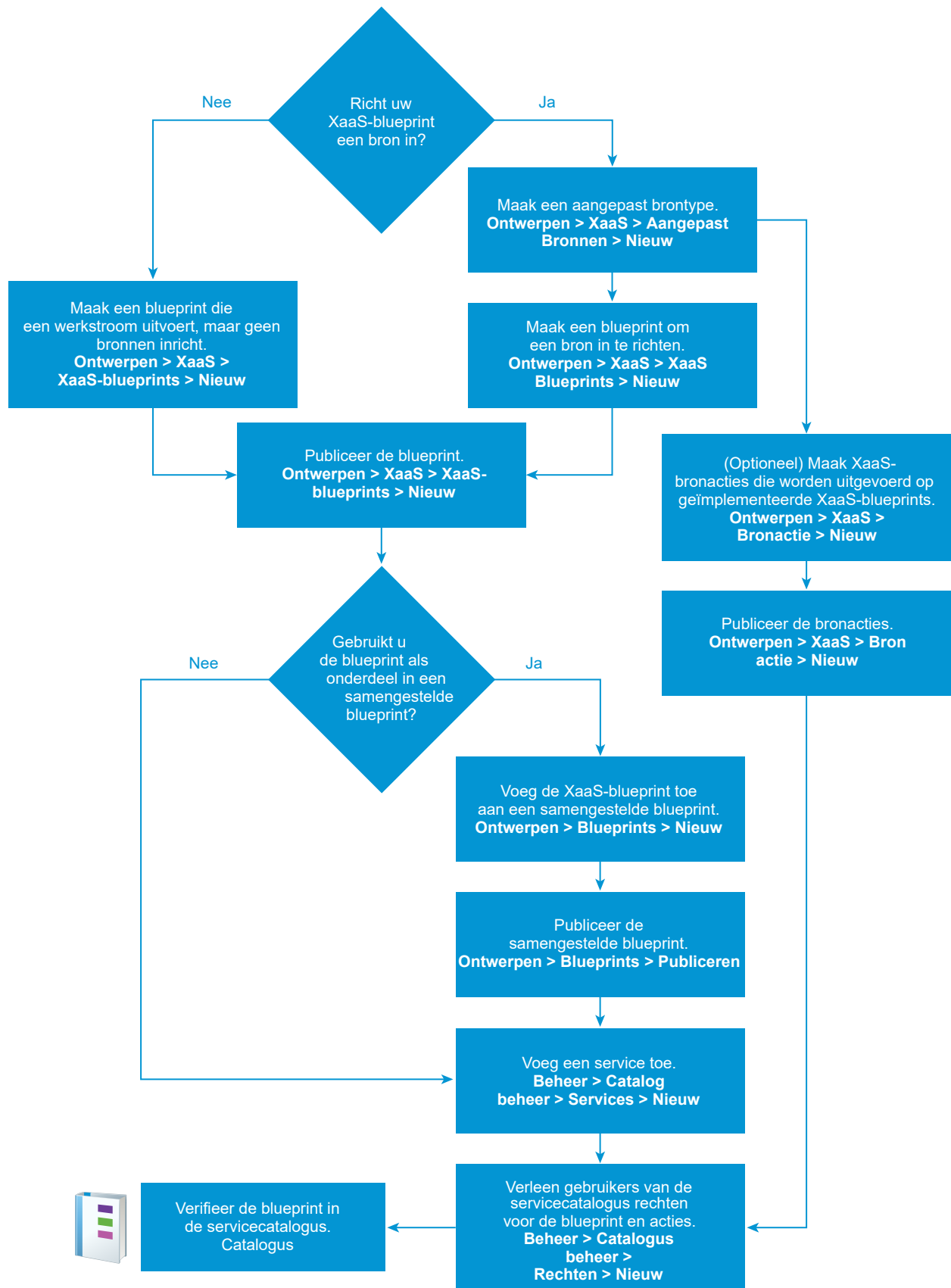
XaaS-blueprints en -bronacties maken

Voor de XaaS-blueprints kunnen rechten aan gebruikers worden verleend als catalogusitem. Ze kunnen ook worden verzameld in een samengestelde blueprint met het ontwerpcanvas. De bronacties worden uitgevoerd voor de ingerichte items om de items te beheren nadat deze zijn ingericht.

U kunt bijvoorbeeld een XaaS-blueprint gebruiken om Active Directory-gebruikers in een groep te maken. U kunt een bronactie gebruiken om te vereisen dat de gebruiker het wachtwoord verandert.

Werkstroom voor XaaS-blueprint

De werkstroom die u volgt om een XaaS -blueprint te maken en alle optionele bronacties variëren afhankelijk van de manier waarop u de blueprint wilt gebruiken. In de volgende werkstroom wordt het basisproces weergegeven.



XaaS-blueprintterminologie

XaaS-blueprints zijn vRealize Orchestrator-werkstromen die bronnen kunnen inrichten, wijzigingen in ingerichte bronnen kunnen maken of zich kunnen gedragen als een service die een taak in uw omgeving uitvoert. De blueprints en de bronacties hebben verschillende nuances die u moet begrijpen wanneer u blueprints voor uw servicecatalogusgebruikers ontwerpt.

De volgende definities helpen u de termen begrijpen die worden gebruikt bij het werken met XaaS-blueprints.

Aangepaste bron

Een vRealize Orchestrator-objecttype dat beschikbaar wordt gemaakt als een bron via de API van een vRealize Orchestrator-invoegtoepassing. U maakt een aangepaste bron voor het definiëren van de uitvoerparameter van een XaaS-inrichtingsblueprint en voor het definiëren van een invoerparameter van een bronactie.

XaaS-blueprintonderdeel

Een inrichtings- of niet-inrichtingsblueprint die u kunt gebruiken in het ontwerpcanvas van de blueprint. Deze blueprint kan ook een standalone XaaS-blueprint zijn.

Standalone XaaS-blueprint

Een inrichtings- of niet-inrichtingsblueprint die direct op de servicecatalogus wordt gepubliceerd en waaraan direct rechten voor de servicecatalogus worden verleend.

Inrichtingsblueprint

Een inrichtingsblueprint die een vRealize Orchestrator-werkstroom uitvoert om bronnen op het doelendpoint in te richten met behulp van de vRealize Orchestrator-invoegtoepassings-API voor de endpoint. Voeg bijvoorbeeld virtual NIC's toe aan een netwerkkapparaat in vSphere. Om een inrichtingsblueprint te maken, moet u een aangepaste bron hebben die het vRealize Orchestrator-brontype definieert.

Wanneer een servicecatalogusgebruiker dit type catalogusitem opvraagt, zorgt de workflow voor de provisioning van het item en wordt het geïmplementeerde item opgeslagen op het tabblad **Implementaties**. U kunt bewerking na inrichting definiëren voor dit type ingerichte bronnen. U kunt de blueprints ook schaalbaar maken door een instantie indien nodig toe te voegen of te verwijderen.

Niet-inrichtingsblueprint

Een niet-inrichtingsblueprint voert een vRealize Orchestrator-werkstroom uit om een taak uit te voeren die de API niet nodig heeft om wijzigingen in een endpoint te maken. Bijvoorbeeld de werkstroom die een rapport maakt en dit vervolgens e-mailt naar of post op een doelcommunicatiesysteem.

Wanneer een servicecatalogusgebruiker dit type catalogusitem opvraagt, voert de workflow de scriptopdracht uit, maar wordt het item niet toegevoegd aan het tabblad **Implementaties**. U kunt geen bewerking na inrichting uitvoeren voor dit type blueprint. U kunt niet-inrichtingsblueprints gebruiken als ondersteunde werkstromen in schaalbare blueprints. U

kunt bijvoorbeeld een blueprint maken om een load balancer met hoge beschikbaarheid te maken.

Samengestelde blueprint

Een blueprint die is gemaakt met behulp van het ontwerpcanvas. De samengestelde blueprint gebruikt een of meer onderdelen. Bijvoorbeeld een machineonderdeel, een softwareonderdeel of een XaaS-onderdeel. Wanneer u deze aan een service toevoegt, wordt deze weergegeven als een Implementatie. Wanneer u deze toevoegt aan een recht om deze beschikbaar te maken voor servicecatalogusgebruikers, wordt deze weergegeven als een samengestelde blueprint. Een samengestelde blueprint kan één blueprintonderdeel hebben, of deze kan een volledige toepassing bevatten met meerdere machines, software en netwerken.

Bronactie

Een werkstroom die u kunt uitvoeren op een geïmplementeerde inrichtingsblueprint. De geïmplementeerde blueprint kan een XaaS-blueprint of blueprintonderdeel zijn, of het kan een machinetype zijn dat u hebt toegewezen aan een vRealize Orchestrator-brontype.

Overwegingen voor het ontwerpen van XaaS-blueprints

Voordat u een XaaS-blueprint maakt, moet u de bedoeling van uw blueprint begrijpen zodat u een blueprint kunt maken die uw bronnen correct inricht.

U kunt XaaS-blueprints maken en gebruiken als een blueprintonderdeel in het ontwerpcanvas of als een standalone blueprint. De blueprint kan een inrichtingsblueprint of een niet-inrichtingsblueprint zijn.

Tabel 3-53. XaaS-blueprinttypen en resultaten

XaaS-blueprinttype	Is een aangepaste bron vereist?	Is de blueprint schaalbaar in een implementatie?	Kan ik een bronactie uitvoeren op de geïmplementeerde blueprint?
Blueprintonderdeel dat bronnen inricht	Ja	Ja. Het is geconfigureerd om te schalen en het zal schalen wanneer de implementatie wordt geschaald.	Ja. Het wordt geschaald wanneer de implementatie wordt geschaald, en u kunt andere bronacties op het geïmplementeerde onderdeel uitvoeren. De blueprintcomponent wordt weergegeven op het tabblad Implementaties.
Blueprintonderdelen die een werkstroom uitvoeren maar geen bronnen inrichten	Nee. De blueprint gebruikt de vRealize Orchestrator-serverconfiguratie, maar vereist geen aangepaste XaaS-bron.	Nee. Deze richt geen bronnen in, maar kan worden uitgevoerd als deel van een schalingsbewerking. Werk bijvoorbeeld een load balancer bij met de nieuwe configuratie op basis van de schalingsbewerking.	Nee. U kunt geen bronactie uitvoeren op een niet-inrichtingsonderdeel.
Standalone blueprint die bronnen inricht	Ja	Nee. U moet bronacties maken om instanties toe te voegen of te vernietigen.	Ja. U kunt bronacties uitvoeren op de geïmplementeerde bron, inclusief alle bronnen die u hebt gemaakt om schaling te ondersteunen. De blueprint wordt weergegeven op het tabblad Implementaties.
Standalone blueprint die een werkstroom uitvoert maar geen bronnen inricht	Nee. De blueprint gebruikt de vRealize Orchestrator-serverconfiguratie, maar vereist geen aangepaste XaaS-bron.	Nee. Deze richt geen bronnen in, maar kan worden uitgevoerd als deel van een bronactie.	Nee. U kunt geen bronactie uitvoeren op een niet-inrichtingsonderdeel.

Een aangepaste bron voor XaaS toevoegen

U maakt een aangepaste bron voor het definiëren van het XaaS-item dat moet worden ingericht. Voordat u een blueprint of actie voor XaaS kunt maken, moet u beschikken over een aangepaste bron die compatibel is met het objecttype van de blueprint of de actiewerkstroom.

Door een aangepaste bron te maken, wijst u een objecttype dat beschikbaar is gemaakt via de API van een vRealize Orchestrator-invoegtoepassing als bron toe. In de aangepaste bron wordt de uitvoerparameter gedefinieerd van een XaaS-blueprint voor de inrichting en wordt een invoerparameter gedefinieerd van een bronactie.

Als de werkstroom van een blueprint of van een bronactie geen bron inricht of een geïmplementeerde blueprint uitvoert, hoeft u geen aangepaste bron te maken. Zo hebt u bijvoorbeeld geen aangepaste bron nodig als uw werkstroom een databasewaarde bijwerkt of een e-mailbericht stuurt na een inrichtingsbewerking.

Als u een aangepaste bron maakt, kunt u in de velden van het alleen-lezen-formulier de details opgeven van een ingericht item. Zie [Een formulier voor aangepaste bronnen ontwerpen](#).

Voorwaarden

- Meld u aan bij vRealize Automation als een **XaaS-architect**.
- Gebruik de gedetailleerde informatie over opties om de aangepaste bron te configureren. Zie [Opties voor wizard voor aangepaste XaaS-bronnen](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Aangepaste bronnen**.
- 2 Klik op het pictogram **Nieuw (+)**.
- 3 Configureer de waarden op het tabblad **Brontype**.
 - a Selecteer het objecttype voor vRealize Orchestrator of voer dit in het tekstvak **Orchestrator-type** in.
Voer bijvoorbeeld de letter **v** in om de typen te bekijken die de letter 'v' bevatten. Als u alle typen wilt weergeven, voert u een spatie in.
 - b Voer een naam in en desgewenst een beschrijving.
 - c Voer een versienummer in.
De ondersteunde indeling kan hoofd.bij.micro-revisie omvatten.
 - d Klik op **Volgende**.
- 4 Bewerk indien nodig het tabblad **Detailsformulier**.
U kunt het formulier van de aangepaste bron wijzigen door elementen te verwijderen, te bewerken en opnieuw te rangschikken. U kunt ook een formulier en formulierpagina's toevoegen en de elementen naar het nieuwe formulier en de nieuwe formulierpagina slepen.
- 5 Klik op **Voltooien**.

Resultaten

U hebt een aangepaste bron gemaakt en u kunt deze zien op de pagina Aangepaste bronnen. U kunt XaaS-blueprints of -acties maken op basis van deze aangepaste bron.

Wat nu te doen

- Maak een XaaS-blueprint. Zie [Een XaaS-blueprint toevoegen](#).
- Maak een actie voor een XaaS-bron. Zie [Een XaaS-bronactie maken](#).

Opties voor wizard voor aangepaste XaaS-bronnen

U gebruikt deze opties voor aangepaste bronnen om een aangepaste bron te maken of te wijzigen zodat u werkstromen voor XaaS-blueprints en -bronacties kunt uitvoeren die bronnen inrichten of ingerichte bronnen wijzigen.

U kunt slechts één aangepaste bron voor een objecttype maken. U kunt de aangepaste bron gebruiken voor meerdere blueprints en bronacties.

Om een aangepaste bronactie te maken, selecteert u **Ontwerpen > XaaS > Aangepaste bronnen**

Brontype

De lijst met mogelijke objecttypen die wordt weergegeven op het tabblad **Brontype** gebaseerd op de geïnstalleerde invoegtoepassingen in de geconfigureerde vRealize Orchestrator-instantie. vRealize Automation verzamelt de waarden van de geconfigureerde vRealize Orchestrator-instantie.

Tabel 3-54. Brontypeopties

Optie	Beschrijving
Orchestrator-type	Voer het type in of selecteer het type dat de werkstroom ondersteunt die u gebruikt voor het inrichten. Het type is samengesteld uit de naam van de invoegtoepassing zoals deze wordt weergegeven in de script-API, bijvoorbeeld VC voor vCenter, en het objecttype, bijvoorbeeld VirtualMachine. In dit voorbeeld gebruikt de API de waarde VC:VirtualMachine. Dit type kan de uitvoerparameter van de blueprintwerkstroom of de invoerparameter van de bronactiewerkstroom zijn.
Naam	Voer een informatieve naam in voor de aangepaste bron zodat u deze kunt identificeren wanneer u XaaS-blueprints of bronacties maakt.
Beschrijving	Geef een uitgebreide beschrijving op.
Versie	Het ondersteunde formulier kan major.minor.micro-revision omvatten.

Detailsformulier

Deze formulervelden worden weergegeven als alleen-lezen waarden wanneer uw servicecatalogusgebruikers een item inrichten dat deze aangepaste bron gebruikt. U kunt de bestaande velden wijzigen en nieuwe extern gedefinieerde velden toevoegen.

Zie [Een formulier voor aangepaste bronnen ontwerpen](#) voor meer informatie over het configureren van de formulieren.

Waar gebruikt

Omdat u slechts één aangepaste bron per objecttype kunt maken, kunt u deze pagina van de wizard gebruiken om te begrijpen hoe de aangepaste bron wordt gebruikt.

Dit tabblad is beschikbaar voor opgeslagen aangepaste bronnen, niet wanneer u de bron maakt.

Tabel 3-55. Opties voor Waar gebruikt

Optie	Beschrijving
XaaS-blueprints	<p>Een lijst met de blueprints die zijn geconfigureerd om deze aangepaste bron te gebruiken.</p> <p>Vanaf deze pagina kunt u de volgende acties uitvoeren:</p> <ul style="list-style-type: none"> ■ Bewerken. Opent de blueprint zodat u kunt zien hoe deze is geconfigureerd of om deze te wijzigen. ■ Publiceren/publicatie ongedaan maken. Wijzigt de status van de blueprint door deze beschikbaar te maken voor gebruik in een samengestelde blueprint of om deze aan een service toe te voegen. Als u de publicatie van een blueprint ongedaan maakt, maakt u deze mogelijk onbeschikbaar voor gebruik in samengestelde blueprints of toevoeging aan een service of maakt u deze onbeschikbaar in de servicecatalogus. ■ Verwijderen. Verwijder deze blueprint uit het systeem.
Bronacties	<p>Een lijst met de bronacties die zijn geconfigureerd om deze aangepaste bron te gebruiken.</p> <p>Vanaf deze pagina kunt u de volgende acties uitvoeren:</p> <ul style="list-style-type: none"> ■ Bewerken. Opent de bronactie zodat u kunt zien hoe deze is geconfigureerd of om deze te wijzigen. ■ Publiceren/publicatie ongedaan maken. Wijzig de status van de bronactie door deze beschikbaar te maken in een recht. Als u de publicatie van een bronactie ongedaan maakt, maakt u deze mogelijk onbeschikbaar voor toevoeging aan een service of maakt u deze onbeschikbaar voor uitvoering op geïmplementeerde blueprints. ■ Verwijderen. Verwijder deze bronactie uit het systeem.

Een XaaS-blueprint maken

Een XaaS-blueprint is geschikt voor zowel inrichtingen als niet-inrichtingen. Voorbeelden van meegeleverde vRealize Orchestrator-werkstromen voor inrichting zijn het maken van virtual machines, het toevoegen van gebruikers aan Active Directory of het maken van momentopnamen van virtual machines. Maar u kunt ook werkstromen voor niet-inrichting maken om bijvoorbeeld uw load balancer bij te werken of een rapport samen te stellen en naar de ontvangers te verzenden.

U kunt XaaS-blueprints maken op basis van de meegeleverde werkstromen van vRealize Orchestrator, maar u kunt ook zelf werkstromen voor specifieke taken in uw omgeving maken en uitvoeren.

Procedure

1 Een XaaS-blueprint toevoegen

Een XaaS-blueprint is een specificatie voor de uitvoering van een vRealize Orchestrator-werkstroom waarmee u een doelsysteem in uw omgeving wijzigt. De blueprint met de werkstroom bevat onder meer de invoerparameters, de formulieren voor indiening en informatie, de reeks acties en de (niet-)inrichtingsbewerking.

2 Een XaaS-blueprint toevoegen aan een samengestelde blueprint

U kunt een XaaS-blueprint toevoegen als onderdeel van een samengestelde blueprint. De procedure is vergelijkbaar met die van het toevoegen van andere blueprintonderdelen op het ontwerpcanvas.

Een XaaS-blueprint toevoegen

Een XaaS-blueprint is een specificatie voor de uitvoering van een vRealize Orchestrator-werkstroom waarmee u een doelsysteem in uw omgeving wijzigt. De blueprint met de werkstroom bevat onder meer de invoerparameters, de formulieren voor indiening en informatie, de reeks acties en de (niet-)inrichtingsbewerking.

U kunt een XaaS-blueprint op de volgende manieren maken en gebruiken:

- Maak een XaaS-blueprintonderdeel. Een onderdeelblueprint is een blueprint voor (niet-)inrichting die u op het ontwerpcanvas voor blueprints kunt opnemen als onderdeel van een samengestelde blueprint. Als u deze blueprint als onderdeel gebruikt, moet u levenscyclustopties voor het onderdeel configureren om in- en uitschaalbewerkingen mogelijk te maken voor de samengestelde blueprint die u implementeert.

Dit blueprinttype kan ook als standalone blueprint worden gepubliceerd.

- Maak een standalone XaaS-blueprint. Een standalone blueprint is een blueprint voor (niet-)inrichtingen die rechtstreeks, inclusief rechten in de servicecatalogus wordt gepubliceerd.

Ga voor een voorbeeld van het maken van Active Directory-gebruikers met een XaaS-blueprint naar [Een XaaS-blueprint en -actie maken voor het maken en wijzigen van een gebruiker](#).

Voorwaarden

- Meld u aan bij vRealize Automation als een **XaaS-architect**.
- Als er bronnen moeten worden ingericht met de blueprint, maakt u een aangepaste bron die overeenkomt met de invoerparameter van de serviceblueprint. Zie [Een aangepaste bron voor XaaS toevoegen](#). Als de blueprint geen vRealize Orchestrator-toepassing met API gebruikt, hoeft u geen aangepaste bron te configureren.

- Wanneer u een XaaS-blueprint maakt, publiceert u een vRealize Orchestrator-werkstroom die als onderdeelblueprint of catalogusitem kan worden gebruikt. De blueprint bevat een formulier dat u desgewenst kunt bewerken. Zie [Een XaaS-blueprintformulier maken](#).
- Gebruik de gedetailleerde informatie over de opties om de blueprint te configureren. Zie [Opties voor wizard voor nieuwe XaaS-blueprints of bewerken van blueprints](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > XaaS-blueprints**.
- 2 Klik op het pictogram **Nieuw** (+).
- 3 Selecteer op het tabblad **Werkstroom** de werkstroom die wordt uitgevoerd wanneer de blueprint wordt gebruikt om de bron in te richten.
Dit tabblad is niet beschikbaar als u een blueprint bewerkt.
 - a Blader door de werkstroombibliotheek van vRealize Orchestrator en selecteer een werkstroom die betrekking heeft op uw aangepaste bron.
 - b Controleer de invoer- en uitvoerparameters zodat u later de juiste waarden kunt invoeren.
 - c Klik op **Volgende**.
- 4 Configureer de opties op het tabblad **Algemeen** en klik op **Volgende**.
 - a Typ in het tekstvak **Naam** een unieke naam voor deze blueprint.
 - b Als u deze blueprint niet wilt gebruiken als onderdeel van een samengestelde blueprint, schakelt u het selectievakje **Beschikbaar stellen als onderdeel in het ontwerpcanvas** uit.
- 5 Wijzig het formulier desgewenst via het tabblad **Blueprintformulier** en klik op **Volgende**.
- 6 Selecteer een waarde op de pagina **Ingerichte bron** en klik op **Volgende**.

Optie	Beschrijving
Geen inrichting	Als u met deze werkstroom geen bronnen inricht, kunt u deze optie selecteren of het veld leeg laten.
<Een aangepaste bron die u eerder hebt gemaakt>	Selecteer de aangepaste bron waarvoor deze inrichtingswerkstroom kan worden gebruikt.

- 7 Definieer op het tabblad **Levenscyclus onderdeel** hoe deze blueprint zich gedraagt tijdens het inschalen, uitschalen en vernietigen.
Deze werkstromen worden uitgevoerd vanuit een geïmplementeerde, samengestelde blueprint waaraan deze blueprint als onderdeel is toegevoegd. Welke opties beschikbaar zijn, is afhankelijk van de blueprint. Niet alle blueprintwerkstromen ondersteunen of vereisen alle opties.
- 8 Klik op **Voltooien**.
- 9 Selecteer de rij met uw blueprint en klik op **Publiceren**.

Resultaten

U hebt een XaaS-blueprint gemaakt en gepubliceerd.

Wat nu te doen

- Als u deze blueprint rechtstreeks als standalone blueprint wilt toevoegen aan de servicecatalogus, voegt u een service toe waaraan u vervolgens de blueprint toevoegt. Zie [Een service toevoegen](#).
- Zie [Een XaaS-blueprint toevoegen aan een samengestelde blueprint](#) als u deze blueprint wilt gebruiken als onderdeel van een samengestelde blueprint.

Opties voor wizard voor nieuwe XaaS-blueprints of bewerken van blueprints

U kunt deze opties gebruiken om een XaaS-blueprint te maken die een vRealize Orchestrator-werkstroom uitvoert wanneer de blueprint wordt geïmplementeerd. De werkstroom wijzigt een doelsysteem in uw omgeving.

Raadpleeg [Een XaaS-blueprint toevoegen](#) voor de stappen die u moet volgen om de blueprint te maken.

Om deze wizard te gebruiken, selecteert u **Ontwerpen > XaaS > XaaS-blueprints**.

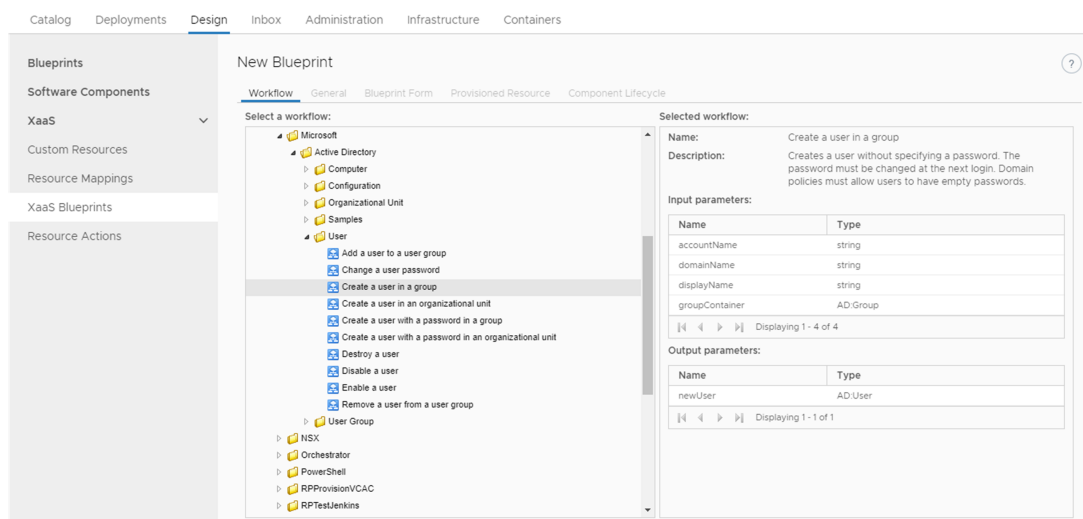
Tabblad Werkstroom

Selecteer de werkstroom die wordt uitgevoerd wanneer de blueprint de bron inricht.

Dit tabblad is niet beschikbaar als u een blueprint bewerkt.

In de volgende figuur bevindt de werkstroomstructuur zich aan de linkerkant en staan de parameters aan de rechterkant.

Figuur 3-4. Tabblad Werkstroom in de XaaS-blueprintwizard



Controleer de in- en uitvoerparameters om ervoor te zorgen dat u en uw servicecatalogusgebruikers de correcte waarden kunnen opgeven in de volgende omstandigheden:

- Als u het blueprintformulier aanpast in deze wizard of in het blueprintontwerpcanvas.
- Als u alle invoerparameters leeg laat, kunnen de servicecatalogusgebruikers de waarden instellen.

Tabblad Algemeen

Configureer de metagegevens over en het gedrag van de blueprint.

Tabel 3-56. Opties tabblad Algemeen

Optie	Beschrijving
Naam	<p>De naam van de blueprint zoals u deze wilt weergeven op de volgende locaties:</p> <ul style="list-style-type: none"> ■ Ontwerpcanvas. Als u Beschikbaar stellen als onderdeel in het ontwerpcanvas selecteert, is deze waarde de naam die wordt weergegeven in de lijst met categorieën. ■ Services. Als u deze blueprint gebruikt als een standalone blueprint, is deze waarde de naam die u ziet wanneer u catalogusitems aan de service toevoegt. ■ Rechten. Als u rechten aan de blueprint verleent als een individueel item, is deze waarde de naam die u in de lijst Items toevoegen ziet.
Beschrijving	Geef een uitgebreide beschrijving op die u helpt een onderscheid te maken tussen gelijkaardige items.
Pagina met informatie over catalogusaanvraag verbergen	Schakel het selectievakje in als u servicecatalogusconsumenten niet wilt verplichten om een beschrijving en een reden op te geven wanneer ze het item aanvragen. Dit selectievakje is standaard ingeschakeld.
Versie	De ondersteunde indeling kan hoofd.bij.micro-revisie omvatten.
Beschikbaar stellen als onderdeel in het ontwerpcanvas	<p>Als u de blueprint wilt gebruiken als een onderdeel in een ontwerpcanvasblueprint, schakelt u deze optie in.</p> <p>Als de blueprint is gepubliceerd, is deze beschikbaar in de categorie die u hebt geselecteerd bij het configureren van de aangepaste bron.</p> <p>Als u deze optie niet inschakelt, wordt de blueprint niet weergegeven in het ontwerpcanvas. U kunt deze echter nog altijd toevoegen aan een service en gebruikers rechten voor deze blueprint verlenen om deze te implementeren als een standalone blueprint.</p>

Tabblad Blueprintformulier

De velden die worden weergegeven op deze pagina van de wizard, zijn de invoerparameters van de werkstroom. U kunt een of meer van de volgende wijzigingen maken:

- Velden aan het formulier toevoegen.
- Bestaande velden wijzigen door de velden te verwijderen of opnieuw te rangschikken.
- Standaardwaarden opgeven als de invoerparameters.

Eventuele wijzigingen hebben invloed op het formulier dat wordt getoond aan:

- De toepassingsarchitect die werkt in het ontwerpcanvas wanneer deze XaaS-blueprint wordt gebruikt als een blueprintonderdeel.
- De servicecatalogusgebruiker als deze blueprint wordt gepubliceerd als een standalone blueprint.

Zie [Een XaaS-blueprintformulier maken](#) voor meer informatie over het configureren van de formulieren.

Ingerichte bron

De ingerichte bron koppelt de blueprint aan een relevante aangepaste XaaS-bron die u hebt geconfigureerd op de pagina Aangepaste bron op **Ontwerpen > XaaS > Aangepaste bron**.

Tabel 3-57. Opties Aangepaste bron

Optie	Beschrijving
Een aangepaste bron die u eerder hebt gemaakt	<p>Selecteer de aangepaste bron die het vRealize Orchestrator-brontype definieert dat vereist is om de inrichtingsblueprint uit te voeren.</p> <p>Een inrichtingsblueprint voert een vRealize Orchestrator-werkstroom uit om bronnen op het doelendpoint in te richten met behulp van de vRealize Orchestrator-invoegtoepassings-API voor de endpoint. Voeg bijvoorbeeld virtual NIC's toe aan een netwerkkapparaat in vSphere.</p> <p>U kunt bewerking na inrichting definiëren voor dit type ingerichte bronnen. U kunt de blueprint ook schaalbaar maken door instanties indien nodig toe te voegen of te verwijderen.</p> <p>Resultaten</p> <ul style="list-style-type: none"> ■ De blueprint komt in aanmerking voor schaling. ■ De blueprint wordt weergegeven in het ontwerpcanvas in de categorie die is opgegeven voor de geselecteerde aangepaste bron. ■ De blueprint wordt weergegeven op het tabblad Implementaties wanneer u een blueprint implementeert die het bevat en u kunt acties uitvoeren op het item na de implementatie.
Geen inrichting	<p>Een niet-inrichtingsblueprint voert een vRealize Orchestrator-werkstroom uit om een taak uit te voeren die de API niet nodig heeft om wijzigingen in een endpoint te maken. Maak bijvoorbeeld een rapport en e-mail het naar of post het op een doelcommunicatiesysteem.</p> <p>Resultaten</p> <ul style="list-style-type: none"> ■ De blueprint komt niet in aanmerking voor schaling. U kunt niet-inrichtingsblueprints gebruiken als ondersteunde werkstromen in schaalbare blueprints. U kunt bijvoorbeeld een blueprint maken om een load balancer met hoge beschikbaarheid te maken. ■ De blueprint wordt weergegeven in de XaaS-categorie in het ontwerpcanvas. ■ De blueprint wordt niet weergegeven op het tabblad Implementaties wanneer u een blueprint implementeert die het bevat en u kunt geen acties uitvoeren op het item na de implementatie.

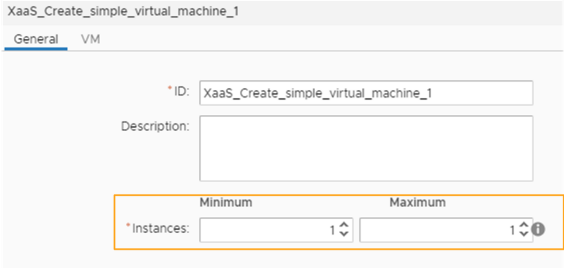
Tabblad Onderdeellevenscyclus

Het tabblad Onderdeellevenscyclus is beschikbaar als u **Beschikbaar stellen als onderdeel in het ontwerpcanvas** op het tabblad **Algemeen** hebt geselecteerd.

U gebruikt deze opties om te definiëren hoe deze blueprint zich na de implementatie gedraagt tijdens inschaal- en uitschaalbewerkingen wanneer deze wordt gebruikt als een onderdeel in een samengestelde blueprint.

De beschikbaarheid van de verschillende opties is afhankelijk van de blueprint. Niet alle blueprintwerkstromen ondersteunen of vereisen alle opties. Omdat uw XaaS mogelijk wordt gebruikt in een samengestelde blueprint, moet u de opties voor bijwerken en vernietigen en voor toewijzen en toewijzing ongedaan maken, configureren als deze beschikbaar zijn voor de blueprint zodat de blueprint correct schaal.

Tabel 3-58. Opties Onderdeellevenscyclus

Optie	Beschrijving
Schaalbaar	<p>Schakel de optie in om toe te staan dat de servicecatalogusgebruiker het aantal instanties van dit blueprintonderdeel na de implementatie ervan kan wijzigen als onderdeel van een inschaal- of uitschaalbewerking.</p> <p>Deze optie is beschikbaar als u een aangepaste bron hebt geselecteerd op het tabblad Aangepaste bron. Deze optie is niet beschikbaar als u de optie Geen inrichting hebt geselecteerd.</p> <p>Als u deze blueprint schaalbaar maakt, wordt de optie Instanties toegevoegd aan het tabblad Algemeen in het ontwerpcanvas. Zie het onderstaande voorbeeld. Als u Schaalbaar niet selecteert, is de optie Instanties niet beschikbaar in het ontwerpcanvas.</p> 
Inrichtingswerkstroom	<p>De werkstroom die wordt uitgevoerd tijdens een inrichtings- of uitschaalbewerking. Deze werkstroom werd geselecteerd toen u deze blueprint hebt gemaakt en u kunt de waarde ervan niet bewerken.</p>

Tabel 3-58. Opties Onderdeellevenscyclus (vervolg)

Optie	Beschrijving
Toewijzingswerkstroom	<p>Selecteer de werkstroom die wordt uitgevoerd voordat enige aanvankelijke inrichtings- of uitschaalbewerking wordt uitgevoerd.</p> <p>Dit levenscycluswerkstroomtype is beschikbaar voor Azure-toewijzingen. Als u een toewijzingswerkstroom maakt voor een schalingsbewerking, moet deze de volgende waarden bevatten:</p> <ul style="list-style-type: none"> ■ Invoerparameters <ul style="list-style-type: none"> ■ De parameternaam is <code>requestData</code> en het parametertype is <code>Properties</code>. ■ De parameternaam is <code>subtenant</code> en het parametertype is <code>Properties</code>. ■ <code>reservations</code> en het parametertype is <code>Arrays/Properties</code>. ■ Uitvoerparameter <ul style="list-style-type: none"> ■ Moet een parameter bevatten waarbij het parametertype <code>Properties</code> is.
Updatewerkstroom	<p>Selecteer de werkstroom die wordt uitgevoerd tijdens updatebewerkingen, inclusief inschalen of uitschalen, waarbij een onderdeel niet schaalbaar is, maar wel kan worden bijgewerkt.</p> <p>Een load balancer wordt bijvoorbeeld bijgewerkt met de nieuwe configuratie die wordt gemaakt met de inschaal- of uitschaalbewerking voor alle onderdelen in de samengestelde blueprint.</p> <p>De updatewerkstroom is mogelijk van toepassing op een onderdeel dat is gebonden aan het geschaalde onderdeel, maar dat zelf niet schaalbaar is. Deze updatewerkstroom kan het niet-schaalbare onderdeel op basis van een updatebewerking wijzigen.</p> <p>Als u een updatewerkstroom maakt voor een schalingsbewerking, moet deze de volgende waarden bevatten:</p> <ul style="list-style-type: none"> ■ Invoerparameters. <ul style="list-style-type: none"> ■ Moet een parameter bevatten, ongeacht de parameternaam, die overeenkomt met het uitvoerparametertype van de inrichtingswerkstroom. ■ De parameternaam is <code>data</code> en het parametertype is <code>Properties</code>.

Tabel 3-58. Opties Onderdeellevenscyclus (vervolg)

Optie	Beschrijving
Vernietigingswerkstroom	<p>Selecteer de werkstroom die wordt uitgevoerd tijdens een inschaal- of vernietigingsbewerking.</p> <p>Als u een vernietigingswerkstroom maakt voor een schalingsbewerking, moet deze de volgende waarde bevatten:</p> <ul style="list-style-type: none"> ■ Invoerparameter. <ul style="list-style-type: none"> ■ Moet een parameter bevatten, ongeacht de parameter naam, die overeenkomt met het uitvoerparametertype van de inrichtingswerkstroom. <p>Als bijvoorbeeld de werkstroom voor het maken van een eenvoudige inrichting van een virtual machine de uitvoerparameter VC:VirtualMachine bevat, moet de vernietigingswerkstroom een invoerparameter bevatten waarvan het type VC:VirtualMachine is.</p>
Werkstroom voor ongedaan maken van toewijzing	<p>Selecteer de werkstroom die wordt uitgevoerd na een vernietigings- of inschaalbewerking. Als het ongedaan maken van de toewijzing mislukt tijdens de bewerking, wordt de vernietigingswerkstroom nog altijd zoals verwacht uitgevoerd.</p> <p>Het ongedaan maken van de toewijzing is de laatste fase bij het inschalen of vernietigen van een samengestelde blueprint. Dit wordt uitgevoerd na de vernietigingswerkstroom en geeft bronnen vrij.</p> <p>Dit levenscycluswerkstroomtype is beschikbaar voor Azure-toewijzingen. Als u een werkstroom voor het ongedaan maken van de toewijzing maakt voor een schalingsbewerking, moet deze de volgende waarde bevatten:</p> <ul style="list-style-type: none"> ■ Invoerparameter. <ul style="list-style-type: none"> ■ De parameter naam is data en het parametertype is Properties.
Categorie	<p>Om op te geven waar de XaaS-blueprint wordt weergegeven in het ontwerpcanvas, selecteert u een waarde in het vervolgkeuzemenu Ontwerpcanvascategorie.</p> <p>Als u geen categorie selecteert, wordt de blueprint toegevoegd aan de XaaS-categorie wanneer deze wordt gepubliceerd.</p>

Een XaaS-blueprint toevoegen aan een samengestelde blueprint

U kunt een XaaS-blueprint toevoegen als onderdeel van een samengestelde blueprint. De procedure is vergelijkbaar met die van het toevoegen van andere blueprintonderdelen op het ontwerpcanvas.

Gebruik deze methode om een XaaS toe te voegen aan de samengestelde blueprint. Deze blueprint kan het enige blueprintonderdeel zijn of een uit een reeks onderdelen waaruit een toepassingsblueprint bestaat.

Als u alleen de XaaS-blueprint op zich beschikbaar wilt stellen aan uw gebruikers, kunt u deze toevoegen aan een service en gebruikers rechten geven zonder de blueprint aan een samengestelde blueprint toe te voegen.

Als u een in- of uitschaalbewerking uitvoert voor een geïmplementeerde toepassingsblueprint, wordt de XaaS-blueprint geschaald op basis van de levenscyclustopties die u hebt ingesteld voor de blueprint.

Voorwaarden

- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Maak en publiceer een XaaS-blueprint. Zie [Een XaaS-blueprint maken](#). Als u de blueprint hebt gemaakt, hebt u opgegeven tot welke categorie de blueprint op het ontwerpcanvas behoort.
- Bekijk hoe u de XaaS-blueprintformulieren in de samengestelde blueprint kunt aanpassen. Zie [Formulieren ontwerpen voor XaaS-blueprints en -acties](#).

Procedure

- 1 Selecteer **Ontwerpen > Blueprints**.
- 2 Selecteer de naam van de blueprint waaraan u de XaaS toevoegt.
Het ontwerpcanvas wordt weergegeven. Dit bevat de blueprints van de huidige toepassingsonderdelen en andere onderdelen.
- 3 Zoek de blueprint in de lijst Categorieën.
- 4 Sleep uw blueprint naar het canvas.
- 5 Configureer de standaardinstellingen op de tabbladen Algemeen en Maken.
Deze standaardwaarden worden weergegeven in het servicecatalogusformulier wanneer een gebruiker het item opvraagt.
- 6 Klik op **Voltooien**.
- 7 Selecteer de blueprint en klik op **Publiceren**.

Resultaten

De XaaS-blueprint maakt nu deel uit van de samengestelde blueprint.

Wat nu te doen

Voeg de samengestelde blueprint toe aan een service. Zie [De servicecatalogus beheren](#).

Een XaaS-bronactie maken

U maakt een bronactie zodat u ingerichte items kunt beheren met vRealize Orchestrator-werkstromen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **XaaS-architect**.
- Controleer of u een aangepaste bron hebt die de actie ondersteunt. Zie [Een aangepaste bron voor XaaS toevoegen](#).
- Als u acties maakt die moeten worden uitgevoerd voor items die niet als XaaS-catalogusitem zijn ingericht, moet u controleren of u de doelbronnen hebt toegewezen. Zie [Overige bronnen toewijzen voor gebruik met XaaS-bronacties](#).

Procedure

1 Een bronactie maken

Een bronactie is een XaaS-werkstroom die servicecatalogusgebruikers kunnen uitvoeren voor ingerichte catalogusitems. Als XaaS-architect kunt u bronacties maken om de bewerkingen te definiëren die consumenten voor de ingerichte items kunnen uitvoeren.

2 Een bronactie publiceren

De zo juist gemaakte bronactie heeft nog de status Concept. U moet de bronactie nog publiceren.

3 Een pictogram toewijzen aan een XaaS-bronactie

Nadat u een bronactie hebt gemaakt en gepubliceerd, kunt u deze bewerken en een pictogram aan de actie toewijzen.

Een bronactie maken

Een bronactie is een XaaS-werkstroom die servicecatalogusgebruikers kunnen uitvoeren voor ingerichte catalogusitems. Als XaaS-architect kunt u bronacties maken om de bewerkingen te definiëren die consumenten voor de ingerichte items kunnen uitvoeren.

Door een bronactie te maken, koppelt u een vRealize Orchestrator-werkstroom als een bewerking na inrichting. Tijdens dit proces kunt u de standaard indienformulieren en alleen-lezen formulieren bewerken. Zie [Een bronactieformulier ontwerpen](#).

Voorwaarden

- Meld u aan bij vRealize Automation als een **XaaS-architect**.
- Maak een aangepaste bron die overeenkomt met de invoerparameter van de bronactie.

Procedure

1 Selecteer **Ontwerpen > XaaS > Bronacties**.

2 Klik op het pictogram **Nieuw** (+).

3 Blader door de werkstroombibliotheek van vRealize Orchestrator en selecteer een werkstroom die betrekking heeft op uw aangepaste bron.

U kunt de naam en de beschrijving van de geselecteerde werkstroom zien en de invoer- en uitvoerparameters zoals deze zijn gedefinieerd in vRealize Orchestrator.

- 4 Klik op **Volgende**.
- 5 Selecteer de aanpaste bron die u eerder hebt gemaakt in het vervolgkeuzemenu **Brontype**.
- 6 Selecteer de invoerparameter voor de bronactie in het vervolgkeuzemenu **Invoerparameter**.
- 7 Klik op **Volgende**.
- 8 Voer een naam in en desgewenst een beschrijving.

De tekstvakken **Naam** en **Beschrijving** worden vooraf ingevuld met de naam en de beschrijving van de werkstroom zoals deze zijn gedefinieerd in vRealize Orchestrator.
- 9 (Optioneel) Als u consumenten niet wilt vragen om een beschrijving en een reden voor het aanvragen van deze bronactie in te voeren, schakelt u het selectievakje **Pagina met informatie over catalogusaanvraag verbergen** in.
- 10 Voer een versienummer in.

De ondersteunde indeling kan hoofd.bij.micro-revisie omvatten.
- 11 (Optioneel) Selecteer het type actie.

Optie	Beschrijving
Verwijdering	De invoerparameter van de resource-actiewerkflow wordt verwijderd en het item wordt verwijderd uit het tabblad Implementaties . De bronactie wordt bijvoorbeeld gebruikt voor het verwijderen van een ingerichte machine.
Inrichting	De bronactie wordt gebruikt voor het inrichten. De bronactie wordt bijvoorbeeld gebruikt voor het kopiëren van een catalogusitem. Selecteer een uitvoerparameter in het vervolgkeuzemenu. U kunt een aangepaste resource selecteren die u eerder hebt gemaakt, zodat de ingerichte items worden toegevoegd aan het tabblad Implementaties wanneer de consumenten deze resource-actie aanvragen. Als u alleen de optie Geen inrichting hebt, wordt de bronactie niet gebruikt voor inrichting, of hebt u geen eigen aangepaste bron voor de uitvoerparameter gemaakt, en kunt u niet verder gaan.
Inrichten als onderliggend	U kunt een resource inrichten als onderliggend element van de bovenliggende resource. Wanneer u een bovenliggende resource verwijdert of in- en uitschalt, moet u eerst voor de onderliggende resources zorgen.

Afhankelijk van de actiewerkstroom kunt u één, beide of geen van de opties selecteren.

- 12 Selecteer de voorwaarden waaronder de bronactie beschikbaar is voor gebruikers en klik op **Volgende**.

13 (Optioneel) Bewerk het formulier van de bronactie op het tabblad **Formulier**.

Het formulier van de bronactie wijst de vRealize Orchestrator-werkstroompresentatie toe. U kunt het formulier wijzigen door de elementen te verwijderen, te bewerken en opnieuw te rangschikken. U kunt ook een nieuw formulier en nieuwe formulierpagina's toevoegen en de nodige elementen naar het nieuwe formulier en de nieuwe formulierpagina slepen.

Optie	Actie
Een formulier toevoegen	Klik op het pictogram Nieuw formulier (+) naast de naam van het formulier, geef de vereiste informatie op en klik op Indienen .
Een formulier bewerken	Klik op het pictogram Bewerken (pencil) naast de naam van het formulier, voer de nodige wijzigingen uit en klik op Indienen .
De werkstroompresentatie opnieuw genereren	Klik op het pictogram Opnieuw bouwen (circular arrow) naast de naam van het formulier en klik op OK .
Een formulier verwijderen	Klik op het pictogram Verwijderen (X) naast de naam van het formulier en klik in het bevestigingsdialoogvenster op OK .
Een formulierpagina toevoegen	Klik op het pictogram Nieuwe pagina (+) naast de naam van de formulierpagina, geef de vereiste informatie op en klik op Indienen .
Een formulierpagina bewerken	Klik op het pictogram Bewerken (pencil) naast de naam van de formulierpagina, voer de nodige wijzigingen uit en klik op Indienen .
Een formulierpagina verwijderen	Klik op het pictogram Verwijderen (X) naast de naam van het formulier en klik in het bevestigingsdialoogvenster op OK .
Een element aan de formulierpagina toevoegen	Sleep een element van het deelvenster Nieuwe velden aan de linkerkant naar het deelvenster aan de rechterkant. Vervolgens geeft u de vereiste informatie op en klikt u op Indienen .
Een element bewerken	Klik op het pictogram Bewerken (pencil) naast het te bewerken element, voer de nodige wijzigingen uit en klik op Indienen .
Een element verwijderen	Klik op het pictogram Verwijderen (X) naast het te verwijderen element en klik in het bevestigingsdialoogvenster op OK .

14 Klik op **Voltooien**.

Resultaten

U hebt een bronactie gemaakt en u kunt deze zien in de pagina met Bronacties.

Wat nu te doen

Publiceer de bronactie. Zie [Een bronactie publiceren](#).

Een bronactie publiceren

De zo juist gemaakte bronactie heeft nog de status Concept. U moet de bronactie nog publiceren.

Voorwaarden

Meld u aan bij vRealize Automation als een **XaaS-architect**.

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Bronacties**.
- 2 Selecteer de rij van de bronactie die u wilt publiceren en klik op **Publiceren**.

Resultaten

De status van de bronactie wordt gewijzigd in Gepubliceerd.

Wat nu te doen

Wijst een pictogram toe aan de bronactie. Zie [Een pictogram toewijzen aan een XaaS-bronactie](#). Bedrijfsgroepbeheerders en tenantbeheerders kunnen vervolgens de actie gebruiken wanneer ze rechten maken.

Een pictogram toewijzen aan een XaaS-bronactie

Nadat u een bronactie hebt gemaakt en gepubliceerd, kunt u deze bewerken en een pictogram aan de actie toewijzen.

Voorwaarden

Meld u aan bij vRealize Automation als een **XaaS-architect**.

Procedure

- 1 Selecteer **Beheer > Catalogusbeheer > Acties**.
- 2 Selecteer de bronactie die u hebt gemaakt.
- 3 Klik op **Configureren**.
- 4 Klik op **Bladeren** en selecteer het pictogram dat u wilt toevoegen.
- 5 Klik op **Openen**.
- 6 Klik op **Bijwerken**.

Resultaten

U hebt een pictogram toegewezen aan de bronactie. Bedrijfsgroepbeheerders en tenantbeheerders kunnen de bronactie gebruiken in een recht.

Overige bronnen toewijzen voor gebruik met XaaS-bronacties

U wijst items toe die niet zijn ingericht met XaaS, zodat u bronacties kunt uitvoeren voor de betreffende items.

Scriptacties en werkstromen voor brontoewijzingen

U kunt de meegeleverde brontoewijzingen voor vSphere, vCloud Director of vCloud Air virtual machines gebruiken of u kunt aangepaste vRealize Orchestrator-scriptacties of -werkstromen

maken voor het toewijzen van andere vRealize Automation-catalogusbrontypen aan vRealize Orchestrator-inventaristypen.

Meegeleverde brontoewijzingen van vRealize Automation

vRealize Automation wordt geleverd met brontoewijzingen voor IaaS vSphere virtual machines, IaaS vCloud Director en implementaties.

vRealize Automation wordt geleverd met vRealize Orchestrator-scriptacties voor brontoewijzing voor elke meegeleverde XaaS-brontoewijzing. Scriptacties voor de geleverde brontoewijzingen vindt u in het `com.vmware.vcac.asd.mappings`-pakket van de ingesloten vRealize Orchestrator-server.

Wanneer u een bronactie maakt die wordt uitgevoerd op een geïmplementeerde samengestelde blueprint die een vRealize Orchestrator-werkstroom gebruikt met `vCACAFE:CatalogResource` als invoerparameter, wordt de implementatietoewijzing toegepast als ingangsbrontype. De implementatietoewijzing wordt alleen toegepast als de geselecteerde werkstroom `vCACAFE:CatalogResource` als invoerparameter bevat. Als u bijvoorbeeld een actie maakt om een bronactie aan te vragen namens een gebruiker, wordt Implementatie aangegeven als brontype op het tabblad Ingangsbron omdat deze werkstroom `vCACAFE:CatalogResource` gebruikt.

De brontoewijzingen IaaS vCD VM en IaaS VC VirtualMachine worden door een actie gebruikt om de virtual machines die overeenkomen met de IaaS-bron toe te wijzen aan de vRealize Orchestrator, vSphere of vCloud Director virtual machine.

Brontoewijzingen ontwikkelen

Afhankelijk van uw versie van vRealize Orchestrator kunt u een vRealize Orchestrator-werkstroom of -scriptactie maken voor het toewijzen van bronnen tussen vRealize Orchestrator en vRealize Automation.

Voor het ontwikkelen van de brontoewijzing kunt u een invoerparameter van het type `Properties` gebruiken, die een sleutel-waardepaar bevat dat de ingerichte bron definieert, en een uitvoerparameter van een vRealize Orchestrator-inventaristype die wordt verwacht door de vRealize Orchestrator-invoegtoepassing. De voor de toewijzing beschikbare eigenschappen zijn afhankelijk van het type bron. De eigenschap `EXTERNAL_REFERENCE_ID` is bijvoorbeeld een veelgebruikte sleutelparameter die de afzonderlijke virtual machines definieert. U kunt deze eigenschap gebruiken om een catalogusbron op te vragen. Als u een toewijzing maakt voor een bron die geen `EXTERNAL_REFERENCE_ID` gebruikt, kunt u een van de andere eigenschappen gebruiken die voor afzonderlijke virtual machines worden doorgegeven. Bijvoorbeeld naam, beschrijving enzovoort.

Zie *Ontwikkelen met VMware vCenter Orchestrator* voor meer informatie over het ontwikkelen van werkstromen en scriptacties.

Een brontoewijzing maken

vRealize Automation biedt brontoewijzingen voor vSphere-, vCloud Director- en vCloud Air-machines. U kunt aanvullende brontoewijzingen maken voor andere typen catalogusbronnen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **XaaS-architect**.
- Controleer of het script of de werkstroom voor de toewijzing beschikbaar is in vRealize Orchestrator. Zie [Scriptacties en werkstromen voor brontoewijzingen](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Brontoewijzingen**.

- 2 Klik op het pictogram **Nieuw (+)**.

- 3 Voer een naam in en desgewenst een beschrijving.

- 4 Voer een versienummer in.

De ondersteunde indeling kan hoofd.bij.micro-revisie omvatten.

- 5 Geef het type van de catalogusbron op in het tekstvak **Type catalogusbron** en druk op Enter.

Het type catalogusbron wordt weergegeven in de detailweergave van het ingerichte item.

- 6 Voer het vRealize Orchestrator-objecttype in het tekstvak **Orchestrator-type** in en druk op Enter.

Dit is de uitvoerparameter van de werkstroom voor de brontoewijzing.

- 7 (Optioneel) Voeg doelcriteria toe voor het beperken van de beschikbaarheid van bronacties die worden gemaakt met deze brontoewijzing.

Op bronacties zijn ook beperkingen van toepassing op basis van goedkeuringen en rechten.

- a Selecteer **Voorwaardelijk beschikbaar**.
- b Selecteer het type voorwaarde.

Optie	Beschrijving
Alle volgende	Als aan alle door u opgegeven componenten wordt voldaan, zijn bronacties die zijn gemaakt met deze brontoewijzing beschikbaar voor de gebruiker.
Eender welke van de volgende	Als aan een van de door u opgegeven componenten wordt voldaan, zijn bronacties die zijn gemaakt met deze brontoewijzing beschikbaar voor de gebruiker.
Niet de volgende	Als de component die u opgeeft bestaat, zijn bronacties die worden gemaakt met deze brontoewijzing niet beschikbaar.

- c Volg de prompts om uw componenten samen te stellen en voltooi de voorwaarden.

- 8 Selecteer uw brontoewijzingsscriptactie of -werkstroom in de vRealize Orchestrator-bibliotheek.

- 9 Klik op **OK**.

Formulieren ontwerpen voor XaaS-blueprints en -acties

De XaaS bevat een formulierontwerpprogramma dat u kunt gebruiken om aanvraag- en detailformulieren voor blueprints en bronacties te ontwerpen. Op basis van de presentatie van de werkstromen genereert het formulierontwerpprogramma dynamisch standaardformulieren en velden waarmee u deze standaardformulieren kunt aanpassen.

U kunt interactieve formulieren maken die gebruikers kunnen invullen als zij catalogusitems of bronacties willen aanvragen. Ook kunt u formulieren maken die alleen-lezen zijn en waarop wordt gedefinieerd welke gegevens gebruikers kunnen zien in de detailweergave van een catalogusitem of een ingerichte bron.

Bij het maken van aangepaste XaaS-bronnen, XaaS-blueprints en bronacties, worden formulieren gegenereerd voor veelvoorkomende use cases.

Tabel 3-59. XaaS-objecttypen en verwante formulieren

Objecttype	Standaardformulier	Overige formulieren
Aangepaste bron	Formulier voor de brondetails op basis van de kenmerken van het inventaristype van de vRealize Orchestrator-invoegtoepassing (alleen-lezen).	■ Geen
XaaS-blueprint	Formulier voor het indienen van aanvragen op basis van de presentatie van de geselecteerde werkstroom.	■ Details catalogusitem (alleen-lezen) ■ Details ingediende aanvraag (alleen-lezen)
Bronactie	Formulier voor het indienen van acties op basis van de presentatie van de geselecteerde werkstroom.	■ Details ingediende actie (alleen-lezen)

U kunt de standaardformulieren aanpassen en nieuwe formulieren ontwerpen. U kunt velden verslepen om ze aan het formulier toe te voegen of de volgorde ervan te wijzigen. U kunt de waarden van bepaalde velden beperken, standaardwaarden opgeven of instructies opgeven voor de eindgebruiker die het formulier invult.

In vergelijking met de ontwerpmogelijkheden voor aanvraagformulieren is het aantal bewerkingen dat u kunt uitvoeren bij het ontwerpen van alleen-lezen formulieren, beperkt. Dit houdt verband met de verschillende doeleinden van beide typen formulieren.

Velden in het formulierontwerpprogramma

U kunt de werkstroompresentatie en -functionaliteit uitbreiden door nieuwe vooraf gedefinieerde velden toe te voegen aan de standaard gegenereerde formulieren van bronacties en XaaS-blueprints.

Als een invoerparameter wordt gedefinieerd in de vRealize Orchestrator-werkstroom, verschijnt deze in vRealize Automation op het standaard gegenereerde formulier. Als u de standaard gegenereerde velden in het formulier niet wilt gebruiken, kunt u deze verwijderen en kunt u nieuwe velden van het palet slepen en neerzetten. U kunt standaard gegenereerde velden vervangen zonder de werkstroomtoewijzingen af te breken als u dezelfde id gebruikt als het veld dat u vervangt.

U kunt ook nieuwe velden toevoegen. Dit zijn andere velden dan de velden die zijn gegenereerd op basis van de vRealize Orchestrator-werkstroominvoer, zodat u de werkstroompresentatie en -functionaliteit in de volgende gevallen kunt uitbreiden:

- Beperkingen toevoegen aan de bestaande velden

U kunt bijvoorbeeld een nieuw vervolgkeuzemenu maken en het de naam **dd** geven. U kunt ook vooraf gedefinieerde opties van Goud, Zilver, Brons en Aangepast maken. Als er een vooraf gedefinieerd veld is, zoals CPU, kunt u de volgende beperkingen aan dit veld toevoegen:

- Als dd gelijk is aan Goud, dan is de CPU 2000 MHz
- Als dd gelijk is aan Zilver, dan is de CPU 1000 MHz
- Als dd gelijk is aan Brons, dan is de CPU 500 MHz
- Als dd gelijk is aan Aangepast, dan is het CPU-veld bewerkbaar en kan de consument een aangepaste waarde opgeven

- Externe waardedefinities toevoegen aan velden

U kunt een externe waardedefinitie toevoegen aan een veld zodat u vRealize Orchestrator-scriptacties kunt uitvoeren en aanvullende informatie aan consumenten kunt leveren op de formulieren die u ontwerpt. Zo kunt u bijvoorbeeld een werkstroom maken om de firewallinstellingen van een virtual machine te wijzigen. Bied op de aanvraagpagina voor de bronactie de gebruiker de mogelijkheid om de open-poortinstellingen te wijzigen, maar beperk ook de opties voor poorten die open zijn. U kunt een externe waardedefinitie toevoegen aan een veld met dubbele lijst en een aangepaste vRealize Orchestrator-scriptactie selecteren die query's uitvoert voor open poorten. Wanneer het aanvraagformulier wordt geladen, wordt de scriptactie uitgevoerd en worden de open poorten als opties aan de gebruiker voorgesteld.

- Nieuwe velden toevoegen die in de vRealize Orchestrator-werkstroom worden afgehandeld als algemene parameters

Zo kan een werkstroomontwikkelaar voor een werkstroom die bijvoorbeeld een integratie met een systeem van derden mogelijk maakt, invoerparameters definiëren die in algemene zin moeten worden afgehandeld, maar ook een manier bieden om aangepaste velden door te geven. In een scriptvak worden bijvoorbeeld alle algemene parameters die beginnen met **my3rdparty** afgehandeld. Als de XaaS-architect vervolgens bepaalde waarden wil doorgeven zodat consumenten deze kunnen bieden, kan de XaaS-architect een nieuw veld toevoegen met de naam **my3rdparty_CPU**.

Tabel 3-60. Nieuwe velden in het bronactie- of XaaS-blueprintformulier

Veld	Beschrijving
Tekstveld	Tekstvak met één regel
Tekstgebied	Tekstvak met meerdere regels

Tabel 3-60. Nieuwe velden in het bronactie- of XaaS-blueprintformulier (vervolg)

Veld	Beschrijving
Koppeling	Veld waarin consumenten een URL invoeren. U kunt http, https, ftp, mailto, of / gebruiken. Gebruik niet bestand://.
E-mail	Veld waarin consumenten een e-mailadres typen
Wachtwoordveld	Veld waarin consumenten een wachtwoord typen
Veld voor geheel getal	Tekstvak waarin consumenten een geheel getal typen U kunt van dit veld een schuifregelaar met een minimum- en maximumwaarde en een toename maken.
Decimaal veld	Tekstvak waarin consumenten een decimaal typen U kunt van dit veld een schuifregelaar met een minimum- en maximumwaarde en een toename maken.
Datum en tijd	Tekstvakken waarin consumenten een datum opgeven (door een datum te selecteren in een agendamenu) en ook de tijd kunnen selecteren (met behulp van de pijlen omhoog en omlaag)
Dubbele lijst	Een lijstbouwer waarin consumenten een vooraf gedefinieerde set met waarden tussen twee lijsten verplaatsen. De eerste lijst bevat alle niet-geselecteerde opties en de tweede lijst bevat de keuzes van de gebruiker.
Selectievakje	Selectievakje
Ja/Nee	Vervolgkeuzemenu voor de selectie van Ja of Nee
Vervolgkeuze	Vervolgkeuzemenu
Lijst	Lijst
Lijst met selectievakjes	Lijst met selectievakjes
Keuzerondjesgroep	Groep met keuzerondjes
Zoeken	Zoekvak dat de query automatisch voltooit en waarmee consumenten een object kunnen selecteren
Structuur	Structuur die consumenten gebruiken om door beschikbare objecten te bladeren en deze te selecteren
Map	Toewijzingstabel die consumenten gebruiken om sleutel-waardeparen te definiëren voor eigenschappen

U kunt ook het formulierveld **Sectietitel** gebruiken om formulierpagina's te splitsen in secties met afzonderlijke titels en het formulierveld **Tekst** om informatieve alleen-lezen teksten toe te voegen.

Beperkingen en waarden in het formulierontwerpprogramma

Wanneer u een element van het blueprint- of bronactieformulier bewerkt, kunt u verschillende beperkingen en waarden toepassen op het element.

Beperkingen

De beperkingen die u op een element kunt toepassen, verschillen naargelang het type element dat u bewerkt of aan het formulier toevoegt. Mogelijk zijn in de vRealize Orchestrator-werkstroom enkele beperkende waarden geconfigureerd. Dergelijke waarden worden niet op het tabblad Beperkingen weergegeven, omdat ze vaak afhankelijk zijn van omstandigheden die worden geëvalueerd wanneer de werkstroom wordt uitgevoerd. Elke beperkende waarde die u configureert voor het blueprintformulier overschrijft beperkingen die in de vRealize Orchestrator-werkstroom zijn opgegeven.

Nadat ze zijn berekend voor een veld worden de minimum- en maximumbindingen alleen herberekend wanneer een blueprint wordt aangevraagd.

Voor elke beperking die u op een element toepast, kunt u een van de volgende opties selecteren om de beperking te definiëren:

Niet ingesteld

Haalt de eigenschap op uit de vRealize Orchestrator-werkstroompresentatie.

Constante

Stelt het element dat u bewerkt in op vereist of optioneel.

Veld

Bindt het element aan een ander element uit het formulier. U kunt bijvoorbeeld instellen dat het element alleen vereist is wanneer een ander element, zoals een selectievakje, is ingeschakeld.

Voorwaardelijk

Past een voorwaarde toe. Gebruik de voorwaarden om verschillende componenten en expressies te maken en deze toe te passen op de status of beperkingen van het element.

Extern

Selecteer een vRealize Orchestrator-scriptactie die de waarde definieert.

Tabel 3-61. Beperkingen in het formulierontwerpprogramma

Beperking	Beschrijving
Vereist	Geeft op of het element vereist is.
Alleen-lezen	Geeft op of het veld alleen-lezen is.
Waarde	Stelt een waarde voor het element in.

Tabel 3-61. Beperkingen in het formulierontwerpprogramma (vervolg)

Beperking	Beschrijving
Zichtbaar	<p>Geeft op of de consument het element kan zien.</p> <p>Als u een zichtbaarheidsbeperking toepast op een weergavegroep in de vRealize Orchestrator-werkstroom, wordt de beperking genegeerd in het formulier Details ingediende aanvraag van XaaS en worden de velden die u wilt verbergen op het formulier weergegeven.</p> <p>Om velden te verbergen die u niet in het formulier Details ingediende aanvraag wilt zien en die niet vereist zijn voor de aanvrager, moet u de velden verwijderen uit het formulier Details ingediende aanvraag op het tabblad Blueprintformulier in het XaaS-blueprintontwerpprogramma. Zie Een nieuw XaaS-blueprintformulier toevoegen om dit tabblad te vinden.</p>
Minimumlengte	Stelt een minimumaantal tekens van het element tekenreeksinvoer in.
Maximumlengte	Stelt een maximaal aantal toegestane tekens van het element tekenreeksinvoer in.
Minimumwaarde	Stelt een minimumwaarde van het element getalinvoer in.
Maximumwaarde	Stelt een maximumwaarde van het element getalinvoer in.
Toename	Stelt een toename in voor een element zoals een veld Decimaal of Geheel getal . Als u bijvoorbeeld een veld voor Geheel getal wilt renderen als een Schuifregelaar , kunt u de waarde van de stap gebruiken.
Minimumaantal	<p>Stelt een minimumaantal selecteerbare items van het element in.</p> <p>Als u bijvoorbeeld een Lijst met selectievakjes toevoegt of bewerkt, kunt u het minimumaantal selectievakjes instellen dat de consument moet inschakelen om door te kunnen gaan.</p>
Maximumaantal	<p>Stelt een maximaal aantal selecteerbare items van het element in.</p> <p>Als u bijvoorbeeld een Lijst met selectievakjes toevoegt of bewerkt, kunt u het maximaal aantal selectievakjes instellen dat de consument moet inschakelen om door te kunnen gaan.</p>

Waarden

U kunt waarden toepassen op sommige elementen en definiëren wat de consumenten zien voor sommige velden. De beschikbare opties zijn afhankelijk van het type element dat u bewerkt of aan het formulier toevoegt.

Tabel 3-62. Waarden in het formulierontwerpprogramma

Waarde	Beschrijving
Niet ingesteld	Haal de waarde van het element dat u bewerkt, op uit de vRealize Orchestrator-werkstroompresentatie.
Vooraf gedefinieerde waarden	Selecteer waarden uit een lijst met gerelateerde objecten uit de vRealize Orchestrator-inventaris.

Tabel 3-62. Waarden in het formulierontwerpprogramma (vervolg)

Waarde	Beschrijving
Waarde	Definieer een statische aangepaste waarde met labels.
Externe waarden	Selecteer een vRealize Orchestrator-scriptactie die uw waarde definieert met gegevens die niet direct door de werkstroom worden weergegeven.

Externe waardedefinities in het formulierontwerpprogramma

Wanneer u sommige elementen in het formulierontwerpprogramma bewerkt, kunt u externe waardedefinities toewijzen die aangepaste vRealize Orchestrator-scriptacties gebruiken om informatie te bieden die niet direct door de werkstroom wordt weergegeven.

U wilt bijvoorbeeld een bronactie publiceren om software te installeren op een ingerichte machine. In plaats van de consument een statische lijst te bieden met alle software die kan worden gedownload, kunt u deze lijst dynamisch vullen met software die relevant is voor het besturingssysteem van de machine, software die de gebruiker niet eerder op de machine heeft geïnstalleerd of software die verouderd is op de machine en moet worden bijgewerkt.

Om dynamische inhoud aan uw consument te kunnen leveren, maakt u een vRealize Orchestrator-scriptactie die de informatie ophaalt die u aan uw consumenten wilt tonen. U wijst uw scriptactie toe aan een veld in het formulierontwerpprogramma als een externe waardedefinitie. Wanneer de bron of het serviceblueprintformulier aan uw consumenten wordt voorgesteld, haalt de scriptactie uw aangepaste informatie op en wordt deze aan uw consument getoond.

U kunt externe waardedefinities gebruiken om standaard- of alleen-lezen waarden te leveren, om booleaanse expressies te bouwen, om beperkingen te definiëren of om consumenten opties te bieden die ze kunnen selecteren uit lijsten, selectievakjes enzovoort.

Als u een blueprint aanmaakt met een workflow die een verplicht veld bevat, is het in het aanvraagformulier verplicht, zelfs als u dit op niet-verplicht instelt.

Werken met het formulierontwerpprogramma

Wanneer u XaaS-blueprints, aangepaste bronacties en aangepaste bronnen maakt, kunt u de formulieren van de blueprints, acties en bronnen bewerken met behulp van het formulierontwerpprogramma. U kunt de weergave bewerken en definiëren wat de consumenten van het item of de actie zien wanneer ze het catalogusitem aanvragen of de bewerking na inrichting uitvoeren.

Standaard wordt elk formulier voor een XaaS-blueprint, bronactie of aangepaste bron gegenereerd op de werkstroompresentatie in vRealize Orchestrator.

De stappen in de vRealize Orchestrator-presentatie worden weergegeven als pagina's in een formulier en de vRealize Orchestrator-presentatiegroepen worden weergegeven als aparte secties. De invoertypes van de geselecteerde werkstroom worden weergegeven als verschillende velden in het formulier. Het vRealize Orchestrator-type string wordt bijvoorbeeld weergegeven door een tekstvak. Een complex type, zoals VC:VirtualMachine wordt weergegeven door een zoekvak of een boomstructuur, zodat de consumenten een alfanumerieke waarde kunnen typen om te zoeken naar een virtual machine of kunnen bladeren om een virtual machine te selecteren.

U kunt de wijze waarop een object wordt weergegeven in het formulierontwerpprogramma, bewerken. U kunt bijvoorbeeld de standaard VC:VirtualMachine-weergave bewerken, zodat een boomstructuur wordt weergegeven in plaats van een zoekvak. U kunt ook nieuwe velden toevoegen, zodat selectievakjes, vervolgkeuzemenu's, enzovoort en diverse beperkingen toepassen. Als de door u toegevoegde nieuwe velden niet geldig zijn of als de velden niet op de juiste wijze zijn toegewezen aan de vRealize Orchestrator-werkstroominvoer, worden door vRealize Orchestrator de ongeldige of niet-toegewezen velden overgeslagen als de consument de werkstroom uitvoert.

Een formulier voor aangepaste bronnen ontwerpen

Alle velden op het formulier met brondetails worden als alleen-lezen aan de consument getoond op de pagina met itemdetails wanneer uw aangepaste bron wordt ingericht. U kunt basisbewerkingen op het formulier uitvoeren, zoals het verwijderen, wijzigen of opnieuw rangschikken van velden, of u kunt nieuw gedefinieerde velden toevoegen die gebruikmaken van vRealize Orchestrator-scriptacties om aanvullende alleen-lezen informatie aan consumenten te bieden.

- [Een aangepast bronelement bewerken](#)

U kunt sommige van de kenmerken van een element op de formulierpagina met aangepaste brondetails bewerken. Elk standaardveld op de pagina vertegenwoordigt een eigenschap van de aangepaste bron. U kunt het type van een eigenschap of de standaardwaarden ervan niet wijzigen, maar u kunt wel de naam, grootte en beschrijving bewerken.

- [Een nieuwe formulierpagina voor aangepaste bronnen toevoegen](#)

U kunt een nieuwe pagina toevoegen om het formulier opnieuw te rangschikken in meerdere tabbladen.

- [Een sectietitel in een aangepaste-bronformulier invoegen](#)

U kunt een sectietitel invoegen om het formulier in secties te splitsen.

- [Een tekstelement toevoegen aan een formulier voor aangepaste bronnen](#)

U kunt een tekstvak invoegen om beschrijvende tekst aan het formulier toe te voegen.

- [Een extern gedefinieerd veld in een aangepaste-bronformulier invoegen](#)

U kunt een nieuw veld invoegen en er een externe waardedefinitie aan toevoegen om op dynamische wijze alleen-lezen informatie te leveren die consumenten kunnen zien op de pagina met itemdetails wanneer ze een aangepaste bron inrichten.

Een aangepast bronelement bewerken

U kunt sommige van de kenmerken van een element op de formulierpagina met aangepaste brondetails bewerken. Elk standaardveld op de pagina vertegenwoordigt een eigenschap van de aangepaste bron. U kunt het type van een eigenschap of de standaardwaarden ervan niet wijzigen, maar u kunt wel de naam, grootte en beschrijving bewerken.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **XaaS-architect**.
- [Een aangepaste bron voor XaaS toevoegen](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Aangepaste bronnen**.
- 2 Klik op de aangepaste bron die u wilt bewerken.
- 3 Klik op het tabblad **Detailsformulier**.
- 4 Wijs het element aan dat u wilt bewerken en klik op het pictogram **Bewerken**.
- 5 Voer een nieuwe naam in voor het veld in het tekstvak **Label** om het label te wijzigen.
- 6 Bewerk de beschrijving in het tekstvak **Beschrijving**.
- 7 Selecteer een optie in het vervolgkeuzemenu **Grootte** om de grootte van het element te wijzigen.
- 8 Selecteer een optie in het vervolgkeuzemenu **Labelgrootte** om de grootte van het label te wijzigen.
- 9 Klik op **Indienen**.
- 10 Klik op **Voltooien**.

Een nieuwe formulierpagina voor aangepaste bronnen toevoegen

U kunt een nieuwe pagina toevoegen om het formulier opnieuw te rangschikken in meerdere tabbladen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **XaaS-architect**.
- [Een aangepaste bron voor XaaS toevoegen](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Aangepaste bronnen**.
- 2 Klik op de aangepaste bron die u wilt bewerken.
- 3 Klik op het tabblad **Detailsformulier**.
- 4 Klik op het pictogram **Nieuwe pagina (+)** naast de naam van de **formulierpagina**.
- 5 Selecteer het ongebruikte schermtype en klik op **Indienen**.
Als u al over een brondetail- of bronlijstweergave beschikt, kunt u geen weergave van hetzelfde type toevoegen.
- 6 Klik op **Indienen**.
- 7 Configureer het formulier.
- 8 Klik op **Voltooien**.

Resultaten

U kunt bepaalde elementen van de oorspronkelijke formulierpagina verwijderen en deze in de nieuwe formulierpagina invoegen, of u kunt nieuwe velden toevoegen die gebruikmaken van externe waardedefinities om consumenten informatie te bieden die niet direct wordt weergegeven door de vRealize Orchestrator-werkstroom.

Een sectietitel in een aangepaste-bronformulier invoegen

U kunt een sectietitel invoegen om het formulier in secties te splitsen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **XaaS-architect**.
- [Een aangepaste bron voor XaaS toevoegen](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Aangepaste bronnen**.
- 2 Klik op de aangepaste bron die u wilt bewerken.
- 3 Klik op het tabblad **Detailsformulier**.
- 4 Sleep het element **Sectietitel** van het deelvenster Formulier naar het deelvenster Formulierpagina.
- 5 Typ een naam voor het gedeelte.
- 6 Klik op een plaats buiten het element om de wijzigingen op te slaan.
- 7 Klik op **Voltooien**.

Een tekstelement toevoegen aan een formulier voor aangepaste bronnen

U kunt een tekstvak invoegen om beschrijvende tekst aan het formulier toe te voegen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **XaaS-architect**.
- [Een aangepaste bron voor XaaS toevoegen](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Aangepaste bronnen**.
- 2 Klik op de aangepaste bron die u wilt bewerken.
- 3 Klik op het tabblad **Detailsformulier**.
- 4 Sleep het element **Tekst** van het deelvenster Formulier naar het deelvenster Formulierpagina.
- 5 Voer de tekst in die u wilt toevoegen.
- 6 Klik op een plaats buiten het element om de wijzigingen op te slaan.
- 7 Klik op **Voltooien**.

Een extern gedefinieerd veld in een aangepaste-bronformulier invoegen

U kunt een nieuw veld invoegen en er een externe waardedefinitie aan toevoegen om op dynamische wijze alleen-lezen informatie te leveren die consumenten kunnen zien op de pagina met itemdetails wanneer ze een aangepaste bron inrichten.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **XaaS-architect**.
- [Een aangepaste bron voor XaaS toevoegen](#).
- Ontwikkel of importeer een vRealize Orchestrator-scriptactie om informatie die u aan consumenten wilt leveren, op te halen.

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Aangepaste bronnen**.
- 2 Klik op de aangepaste bron die u wilt bewerken.
- 3 Klik op het tabblad **Detailsformulier**.
- 4 Sleep een element van het deelvenster Nieuwe velden en zet het neer op het deelvenster Formulierpagina.
- 5 Typ een id voor het element in het tekstvak **Id**.
- 6 Voer een label in in het tekstvak **Label**.
Labels worden op de formulieren weergegeven voor consumenten.
- 7 (Optioneel) Selecteer een type voor het veld in het vervolgkeuzemenu **Type**.
- 8 Voer het resultaattype van uw vRealize Orchestrator-scriptactie in het zoekvak **Entiteitstype** in en druk op Enter.
Als u bijvoorbeeld een scriptactie wilt gebruiken om de huidige gebruiker weer te geven, en het script retourneert een vRealize Orchestrator-resultaattype van `LdapUser`, dan voert u **LdapUser** in het zoekvak **Entiteitstype** in en drukt u op Enter.
- 9 Klik op **Externe waarde toevoegen**.
- 10 Selecteer uw aangepaste vRealize Orchestrator-scriptactie.
- 11 Klik op **Indienen**.
- 12 Klik opnieuw op **Indienen**.
- 13 Klik op **Voltooien**.

Resultaten

Wanneer het formulier aan uw consumenten wordt voorgesteld, haalt de scriptactie uw aangepaste informatie op en wordt deze aan uw consument getoond.

Een XaaS-blueprintformulier maken

Wanneer u een XaaS-blueprint maakt, kunt u het formulier van de blueprint bewerken door nieuwe velden aan het formulier toe te voegen of de bestaande velden te wijzigen, te

verwijderen of opnieuw te rangschikken. U kunt ook nieuwe formulieren en formulierpagina's maken en hier nieuwe velden naartoe slepen en neerzetten.

- [Een nieuw XaaS-blueprintformulier toevoegen](#)

Wanneer u het standaard gegenereerde formulier bewerkt van een werkstroom die u als een XaaS-blueprint wilt publiceren, kunt u een nieuw XaaS-blueprintformulier toevoegen.

- [Een XaaS-blueprintelement bewerken](#)

U kunt sommige kenmerken van een element op de pagina Blueprintformulier van een XaaS-blueprint bewerken. U kunt het type van een element en de standaardwaarden ervan wijzigen en verschillende beperkingen en waarden toepassen.

- [Een nieuw element toevoegen](#)

Wanneer u het standaard gegenereerde formulier van een XaaS-blueprint bewerkt, kunt u een vooraf gedefinieerd, nieuw element toevoegen aan het formulier. Als u een standaard gegenereerd veld bijvoorbeeld niet wilt gebruiken, kunt u het verwijderen en vervangen door een nieuw veld.

- [Een sectietitel in een XaaSblueprintformulier invoegen](#)

U kunt een sectietitel invoegen om het formulier in secties te splitsen.

- [Een tekstelement toevoegen aan een XaaS-blueprintformulier](#)

U kunt een tekstvak invoegen om beschrijvende tekst aan het formulier toe te voegen.

Een nieuw XaaS-blueprintformulier toevoegen

Wanneer u het standaard gegenereerde formulier bewerkt van een werkstroom die u als een XaaS-blueprint wilt publiceren, kunt u een nieuw XaaS-blueprintformulier toevoegen.

Door een nieuw XaaS-blueprintformulier toe te voegen, bepaalt u het uiterlijk van de catalogusitemdetails en de pagina's met details van de ingediende aanvraag. Als u geen catalogusitemdetails en formulieren met details van de ingediende aanvraag toevoegt, ziet de consument wat er in het aanvraagformulier is bepaald.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **XaaS-architect**.
- [Een XaaS-blueprint toevoegen](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > XaaS-blueprints**.
- 2 Klik op de XaaS-blueprint die u wilt bewerken.
- 3 Klik op het tabblad **Blueprintformulier**.
- 4 Klik op het pictogram **Nieuw formulier (+)**.
- 5 Voer een naam in en desgewenst een beschrijving.

6 Selecteer het schermtype in het menu **Schermttype**.

Optie	Beschrijving
Details catalogusitem	Een pagina met catalogusitemdetails die consumenten zien wanneer ze op een catalogusitem klikken.
Aanvraagformulier	Het standaardformulier voor XaaS-blueprints. De consumenten zien het aanvraagformulier wanneer ze het catalogusitem aanvragen.
Details ingediende aanvraag	Een pagina met aanvraagdetails die consumenten zien wanneer ze het item aanvragen en besluiten om de details van de aanvraag te bekijken op het tabblad Implementaties .

7 Klik op **Indienen**.

Wat nu te doen

Voeg de gewenste velden toe door deze van het deelvenster Nieuwe velden naar het deelvenster Formulierpagina te slepen.

Een XaaS-blueprintelement bewerken

U kunt sommige kenmerken van een element op de pagina Blueprintformulier van een XaaS-blueprint bewerken. U kunt het type van een element en de standaardwaarden ervan wijzigen en verschillende beperkingen en waarden toepassen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **XaaS-architect**.
- [Een XaaS-blueprint toevoegen](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > XaaS-blueprints**.
- 2 Klik op de XaaS-blueprint die u wilt bewerken.
- 3 Klik op het tabblad **Blueprintformulier**.
- 4 Zoek naar het element dat u wilt bewerken.
- 5 Klik op het pictogram **Bewerken** (✎).
- 6 Voer een nieuwe naam in voor het veld in het tekstvak **Label** om het label dat consumenten zien, te wijzigen.
- 7 Bewerk de beschrijving in het tekstvak **Beschrijving**.
- 8 Selecteer een optie in het vervolgkeuzemenu **Type** om het weergavetype van het element te wijzigen.

De opties kunnen verschillen afhankelijk van het type element dat u bewerkt.
- 9 Selecteer een optie in het vervolgkeuzemenu **Grootte** om de grootte van het element te wijzigen.

- 10 Selecteer een optie in het vervolgkeuzemenu **Labelgrootte** om de grootte van het label te wijzigen.
- 11 Bewerk de standaardwaarde van het element.

Optie	Beschrijving
Niet ingesteld	Haalt de waarde van het element dat u bewerkt, op uit de vRealize Orchestrator-werkstroompresentatie.
Constante	Stelt de standaardwaarde van het element dat u bewerkt, in op een constante waarde die u opgeeft.
Veld	Bindt de standaardwaarde van het element aan een parameter van een ander element uit de weergave.
Voorwaardelijk	Past een voorwaarde toe. Door gebruik te maken van voorwaarden, kunt u verschillende componenten en expressies maken en deze op een element toepassen.
Extern	Selecteer een vRealize Orchestrator-scriptactie om de waarde te definiëren.

- 12 Pas beperkingen toe op het element op het tabblad **Beperkingen**.

Optie	Beschrijving
Niet ingesteld	Haalt de waarde van het element dat u bewerkt, op uit de vRealize Orchestrator-werkstroompresentatie.
Constante	Stelt de standaardwaarde van het element dat u bewerkt, in op een constante waarde die u opgeeft.
Veld	Bindt de standaardwaarde van het element aan een parameter van een ander element uit de weergave.
Voorwaardelijk	Past een voorwaarde toe. Door gebruik te maken van voorwaarden, kunt u verschillende componenten en expressies maken en deze op een element toepassen.
Extern	Selecteer een vRealize Orchestrator-scriptactie om de waarde te definiëren.

- 13 Voeg een of meer waarden toe voor het element op het tabblad **Waarden**.

De beschikbare opties zijn afhankelijk van het type element dat u bewerkt.

Optie	Beschrijving
Niet ingesteld	Haalt de waarde van het element dat u bewerkt, op uit de vRealize Orchestrator-werkstroompresentatie.
Vooraf gedefinieerde waarden	<p>Selecteer waarden uit een lijst met gerelateerde objecten uit de vRealize Orchestrator-inventaris.</p> <ul style="list-style-type: none"> a Voer een waarde in in het zoekvak Vooraf gedefinieerde waarden om de vRealize Orchestrator-inventaris te doorzoeken. b Selecteer een waarde uit de zoekresultaten en druk op Enter.

Optie	Beschrijving
Waarde	<p>Definieer aangepaste waarden met labels.</p> <ol style="list-style-type: none"> Voer een waarde in in het tekstvak Waarde. Voer een label voor de waarde in in het tekstvak Label. Klik op het pictogram Toevoegen (+).
Externe waarden	<p>Selecteer een vRealize Orchestrator-scriptactie om uw waarde te definiëren met gegevens die niet direct door de werkstroom worden weergegeven.</p> <ul style="list-style-type: none"> Selecteer Externe waarde toevoegen. Selecteer uw vRealize Orchestrator-scriptactie. Klik op Indienen.

14 Klik op **Indienen**.

15 Klik op **Voltooien**.

Een nieuw element toevoegen

Wanneer u het standaard gegenereerde formulier van een XaaS-blueprint bewerkt, kunt u een vooraf gedefinieerd, nieuw element toevoegen aan het formulier. Als u een standaard gegenereerd veld bijvoorbeeld niet wilt gebruiken, kunt u het verwijderen en vervangen door een nieuw veld.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **XaaS-architect**.
- [Een XaaS-blueprint toevoegen](#).

Procedure

- Selecteer **Ontwerpen > XaaS > XaaS-blueprints**.
- Klik op de XaaS-blueprint die u wilt bewerken.
- Klik op het tabblad **Blueprintformulier**.
- Sleep een element van het deelvenster Nieuwe velden en zet het neer op het deelvenster Formulierpagina.
- Voer de id van een werkstroom invoerparameter in in het tekstvak **Id**.
- Voer een label in in het tekstvak **Label**.
Labels worden op de formulieren weergegeven voor consumenten.
- (Optioneel) Selecteer een type voor het veld in het vervolgkeuzemenu **Type**.

- 8 Voer een vRealize Orchestrator-object in in het tekstvak **Entiteittype** en druk op Enter.

Deze stap is niet vereist voor alle veldtypen.

Optie	Beschrijving
Resultaattype	Als u een scriptactie gebruikt om een externe waarde te definiëren voor het veld, voert u het resultaattype van uw vRealize Orchestrator-scriptactie in.
Invoerparameter	Als u het veld gebruikt om invoer van consumenten te accepteren en parameters terug door te geven aan vRealize Orchestrator, voert u het type voor de invoerparameter in dat is geaccepteerd door de vRealize Orchestrator-werkstroom.
Uitvoerparameter	Als u het veld gebruikt om informatie aan consumenten te tonen, voert u het typen voor de uitvoerparameter van de vRealize Orchestrator-werkstroom in.

- 9 (Optioneel) Selecteer het selectievakje **Meerdere waarden** om consumenten toe te staan meer dan één object te selecteren.

Deze optie is niet beschikbaar voor alle veldtypen.

- 10 Klik op **Indienen**.

- 11 Klik op **Bijwerken**.

Wat nu te doen

U kunt het element bewerken door de standaardinstellingen te wijzigen en verschillende beperkingen of waarden toe te passen.

Een sectietitel in een XaaSblueprintformulier invoegen

U kunt een sectietitel invoegen om het formulier in secties te splitsen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **XaaS-architect**.
- [Een XaaS-blueprint toevoegen](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > XaaS-blueprints**.
- 2 Klik op de XaaS-blueprint die u wilt bewerken.
- 3 Klik op het tabblad **Blueprintformulier**.
- 4 Sleep het element **Sectietitel** van het deelvenster Formulier naar het deelvenster Formulierpagina.
- 5 Typ een naam voor het gedeelte.
- 6 Klik op een plaats buiten het element om de wijzigingen op te slaan.
- 7 Klik op **Bijwerken**.

Een tekstelement toevoegen aan een XaaS-blueprintformulier

U kunt een tekstvak invoegen om beschrijvende tekst aan het formulier toe te voegen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **XaaS-architect**.
- [Een XaaS-blueprint toevoegen](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > XaaS-blueprints**.
- 2 Klik op de XaaS-blueprint die u wilt bewerken.
- 3 Klik op het tabblad **Blueprintformulier**.
- 4 Sleep het element **Tekst** van het deelvenster Nieuwe velden naar het deelvenster Formulierpagina.
- 5 Voer de tekst in die u wilt toevoegen.
- 6 Klik op een plaats buiten het element om de wijzigingen op te slaan.
- 7 Klik op **Bijwerken**.

Een bronactieformulier ontwerpen

Wanneer u een bronactie maakt, kunt u het formulier van de actie bewerken door nieuwe velden aan het formulier toe te voegen of de bestaande velden te wijzigen, te verwijderen of opnieuw te rangschikken. U kunt ook nieuwe formulieren en formulierpagina's maken en hier nieuwe velden naartoe slepen en neerzetten.

Een nieuw bronactieformulier toevoegen

Wanneer u het standaard gegenereerde formulier bewerkt van een werkstroom die u als een bronactie wilt publiceren, kunt u een nieuw bronactieformulier toevoegen.

Door een nieuw bronactieformulier toe te voegen, bepaalt u hoe de pagina met details van de ingediende actie eruitziet. Als u geen formulier met details van de ingediende actie toevoegt, ziet de consument wat er in het actieformulier is gedefinieerd.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **XaaS-architect**.
- [Een bronactie maken](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Bronacties**.
- 2 Klik op de bronactie die u wilt bewerken.
- 3 Klik op het tabblad **Formulier**.
- 4 Klik op het pictogram **Nieuw formulier** (+).
- 5 Voer een naam in en desgewenst een beschrijving.

6 Selecteer het schermtype in het menu **Schermttype**.

Optie	Beschrijving
Actieformulier	Het standaardformulier voor bronacties dat consumenten zien wanneer u ervoor kiest de actie na inrichting uit te voeren.
Details ingediende actie	Een pagina met aanvraagdetails die consumenten zien wanneer ze de actie aanvragen en besluiten om de details van de aanvraag te bekijken op het tabblad Implementaties .

7 Klik op **Indienen**.

Wat nu te doen

Voeg de gewenste velden toe door deze van het deelvenster Nieuwe velden naar het deelvenster Formulierpagina te slepen.

Een nieuw element toevoegen aan een bronactiefomulier

Wanneer u het standaard gegenereerde formulier van een bronactie bewerkt, kunt u een vooraf gedefinieerd, nieuw element toevoegen aan het formulier. Als u een standaard gegenereerd veld bijvoorbeeld niet wilt gebruiken, kunt u het verwijderen en vervangen door een nieuw veld.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **XaaS-architect**.
- [Een bronactie maken](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Bronacties**.
- 2 Klik op de bronactie die u wilt bewerken.
- 3 Klik op het tabblad **Formulier**.
- 4 Sleep een element van het deelvenster Nieuwe velden en zet het neer op het deelvenster Formulierpagina.
- 5 Voer de id van een werkstroom invoerparameter in in het tekstvak **Id**.
- 6 Voer een label in in het tekstvak **Label**.
Labels worden op de formulieren weergegeven voor consumenten.
- 7 (Optioneel) Selecteer een type voor het veld in het vervolgkeuzemenu **Type**.

- 8 Voer een vRealize Orchestrator-object in in het tekstvak **Entiteittype** en druk op Enter.

Deze stap is niet vereist voor alle veldtypen.

Optie	Beschrijving
Resultaattype	Als u een scriptactie gebruikt om een externe waarde te definiëren voor het veld, voert u het resultaattype van uw vRealize Orchestrator-scriptactie in.
Invoerparameter	Als u het veld gebruikt om invoer van consumenten te accepteren en parameters terug door te geven aan vRealize Orchestrator, voert u het type voor de invoerparameter in dat is geaccepteerd door de vRealize Orchestrator-werkstroom.
Uitvoerparameter	Als u het veld gebruikt om informatie aan consumenten te tonen, voert u het typen voor de uitvoerparameter van de vRealize Orchestrator-werkstroom in.

- 9 (Optioneel) Selecteer het selectievakje **Meerdere waarden** om consumenten toe te staan meer dan één object te selecteren.

Deze optie is niet beschikbaar voor alle veldtypen.

- 10 Klik op **Indienen**.

- 11 Klik op **Voltooien**.

Wat nu te doen

U kunt het element bewerken door de standaardinstellingen te wijzigen en verschillende beperkingen of waarden toe te passen.

Een bronactie-element bewerken

U kunt sommige van de kenmerken van een element op de bronactieformulierpagina bewerken.

U kunt het type van een element en de standaardwaarden ervan wijzigen en verschillende beperkingen en waarden toepassen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **XaaS-architect**.
- [Een bronactie maken](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Bronacties**.
- 2 Klik op de bronactie die u wilt bewerken.
- 3 Klik op het tabblad **Formulier**.
- 4 Zoek naar het element dat u wilt bewerken.
- 5 Klik op het pictogram **Bewerken** (✎).
- 6 Voer een nieuwe naam in voor het veld in het tekstvak **Label** om het label dat consumenten zien, te wijzigen.

- 7 Bewerk de beschrijving in het tekstvak **Beschrijving**.
- 8 Selecteer een optie in het vervolgkeuzemenu **Type** om het weergavetype van het element te wijzigen.
De opties kunnen verschillen afhankelijk van het type element dat u bewerkt.
- 9 Selecteer een optie in het vervolgkeuzemenu **Grootte** om de grootte van het element te wijzigen.
- 10 Selecteer een optie in het vervolgkeuzemenu **Labelgrootte** om de grootte van het label te wijzigen.
- 11 Bewerk de standaardwaarde van het element.

Optie	Beschrijving
Niet ingesteld	Haalt de waarde van het element dat u bewerkt, op uit de vRealize Orchestrator-werkstroompresentatie.
Constante	Stelt de standaardwaarde van het element dat u bewerkt, in op een constante waarde die u opgeeft.
Veld	Bindt de standaardwaarde van het element aan een parameter van een ander element uit de weergave.
Voorwaardelijk	Past een voorwaarde toe. Door gebruik te maken van voorwaarden, kunt u verschillende componenten en expressies maken en deze op een element toepassen.
Extern	Selecteer een vRealize Orchestrator-scriptactie om de waarde te definiëren.

- 12 Pas beperkingen toe op het element op het tabblad **Beperkingen**.

Optie	Beschrijving
Niet ingesteld	Haalt de waarde van het element dat u bewerkt, op uit de vRealize Orchestrator-werkstroompresentatie.
Constante	Stelt de standaardwaarde van het element dat u bewerkt, in op een constante waarde die u opgeeft.
Veld	Bindt de standaardwaarde van het element aan een parameter van een ander element uit de weergave.
Voorwaardelijk	Past een voorwaarde toe. Door gebruik te maken van voorwaarden, kunt u verschillende componenten en expressies maken en deze op een element toepassen.
Extern	Selecteer een vRealize Orchestrator-scriptactie om de waarde te definiëren.

13 Voeg een of meer waarden toe voor het element op het tabblad **Waarden**.

De beschikbare opties zijn afhankelijk van het type element dat u bewerkt.

Optie	Beschrijving
Niet ingesteld	Haalt de waarde van het element dat u bewerkt, op uit de vRealize Orchestrator-werkstroompresentatie.
Vooraf gedefinieerde waarden	<p>Selecteer waarden uit een lijst met gerelateerde objecten uit de vRealize Orchestrator-inventaris.</p> <ol style="list-style-type: none"> Voer een waarde in in het zoekvak Vooraf gedefinieerde waarden om de vRealize Orchestrator-inventaris te doorzoeken. Selecteer een waarde uit de zoekresultaten en druk op Enter.
Waarde	<p>Definieer aangepaste waarden met labels.</p> <ol style="list-style-type: none"> Voer een waarde in in het tekstvak Waarde. Voer een label voor de waarde in in het tekstvak Label. Klik op het pictogram Toevoegen (+).
Externe waarden	<p>Selecteer een vRealize Orchestrator-scriptactie om uw waarde te definiëren met gegevens die niet direct door de werkstroom worden weergegeven.</p> <ul style="list-style-type: none"> ■ Selecteer Externe waarde toevoegen. ■ Selecteer uw vRealize Orchestrator-scriptactie. ■ Klik op Indienen.

14 Klik op **Indienen**.**15** Klik op **Bijwerken**.

Een sectietitel in een bronactiefomulier invoegen

U kunt een sectietitel invoegen om het formulier in secties te splitsen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **XaaS-architect**.
- [Een bronactie maken](#).

Procedure

- 1** Selecteer **Ontwerpen > XaaS > Bronacties**.
- 2** Klik op de bronactie die u wilt bewerken.
- 3** Klik op het tabblad **Formulier**.
- 4** Sleep het element **Sectietitel** van het deelvenster Formulier naar het deelvenster Formulierpagina.
- 5** Typ een naam voor het gedeelte.
- 6** Klik op een plaats buiten het element om de wijzigingen op te slaan.
- 7** Klik op **Voltooien**.

Een tekstelement toevoegen aan een bronactiefomulier

U kunt een tekstvak invoegen om beschrijvende tekst aan het formulier toe te voegen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **XaaS-architect**.
- [Een bronactie maken](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Bronacties**.
- 2 Klik op de bronactie die u wilt bewerken.
- 3 Klik op het tabblad **Formulier**.
- 4 Sleep het element **Tekst** van het deelvenster Nieuwe velden naar het deelvenster Formulierpagina.
- 5 Voer de tekst in die u wilt toevoegen.
- 6 Klik op een plaats buiten het element om de wijzigingen op te slaan.
- 7 Klik op **Voltooien**.

Voorbeelden en scenario's voor XaaS

De voorbeelden en scenario's reiken manieren aan waarop u vRealize Automation kunt gebruiken om algemene taken uit te voeren met behulp van XaaS-blueprints en bronacties.

Een XaaS-blueprint en -actie maken voor het maken en wijzigen van een gebruiker

Met behulp van XaaS kunt u een catalogusitem maken en publiceren voor het inrichten van een gebruiker in een groep. U kunt ook een nieuwe bewerking na inrichting koppelen aan de ingerichte gebruiker. Met zo'n bewerking kunt u gebruikers van de servicecatalogus bijvoorbeeld de mogelijkheid geven om hun wachtwoord te wijzigen.

Als XaaS-architect maakt u een aangepaste bron, een XaaS-blueprint en publiceert u een catalogusitem voor het maken van een gebruiker. U maakt ook een bronactie voor het wijzigen van het wachtwoord van de gebruiker.

Als catalogusbeheerder kunt u een service maken en het blueprintcatalogusitem aan de service toevoegen. Daarnaast bewerkt u de werkstroompresentatie van het catalogusitem met behulp van het formulierontwerpprogramma en wijzigt u de manier waarop consumenten het aanvraagformulier te zien krijgen.

Als bedrijfsgroepbeheerder of tenantbeheerder verleent u consumenten rechten voor de zojuist gemaakte items: de service, het catalogusitem en de bronactie.

Voorwaarden

Controleer of de Active Directory-invoegtoepassing goed is geconfigureerd en u de rechten hebt om gebruikers te maken in Active Directory.

Procedure

1 Een testgebruiker maken als een aangepaste bron

U kunt een aangepaste bron maken en deze toewijzen aan het vRealize Orchestrator -objecttype AD:User.

2 Een XaaS-blueprint maken voor het maken van een gebruiker

U maakt de XaaS-blueprint Een gebruiker in een groep maken zodat u een werkstroom kunt uitvoeren waarmee een Active Directory-gebruiker wordt toegevoegd en de gebruiker wordt toegewezen aan een Active Directory-groep. U kunt de blueprint maken als standalone XaaS-blueprint of als blueprintonderdeel. In dit scenario maakt u een standalone blueprint.

3 Een bronactie maken om een gebruikerswachtwoord te wijzigen

U kunt een bronactie maken om consumenten van de XaaS toestemming te geven het wachtwoord van de gebruiker te wijzigen nadat ze de gebruiker hebben ingericht.

4 Een service maken en de blueprint Een testgebruiker maken toevoegen aan de service

U kunt een service maken waarmee het catalogusitem Een gebruiker maken wordt weergegeven in de servicecatalogus.

5 Rechten voor de service en de bronactie verlenen aan een consument

Bedrijfsgroepbeheerders en tenantbeheerders kunnen rechten voor de service en de bronactie verlenen aan een gebruiker of een groep gebruikers. Nadat er rechten aan hen zijn verleend, kunnen ze de service in hun catalogus weergeven en het catalogusitem Een testgebruiker maken aanvragen dat is opgenomen in de service. Nadat de consumenten het item hebben ingericht, kunnen ze een aanvraag indienen om het gebruikerswachtwoord te wijzigen.

Een testgebruiker maken als een aangepaste bron

U kunt een aangepaste bron maken en deze toewijzen aan het vRealize Orchestrator -objecttype AD:User.

Voorwaarden

Meld u aan bij vRealize Automation als een **XaaS-architect**.

Procedure

1 Selecteer **Ontwerpen > XaaS > Aangepaste bronnen**.

2 Klik op het pictogram **Nieuw (+)**.

3 Voer in het tekstvak **Orchestrator-type** de tekst **AD:User** in en druk op Enter.

4 Selecteer **AD:User** in de lijst.

- 5 Typ een naam voor de bron.

Bijvoorbeeld **Testgebruiker**.

- 6 Voer een beschrijving in voor de bron.

Bijvoorbeeld

Dit is een test voor een aangepaste bron die ik zal gebruiken voor mijn catalogusitem om een gebruiker in een groep te maken.

- 7 Klik op **Volgende**.

- 8 Neem de standaardwaarden van het formulier over.

- 9 Klik op **Voltooien**.

Resultaten

U hebt een aangepaste bron Testgebruiker gemaakt en u kunt dit zien op de pagina Aangepaste bronnen.

Wat nu te doen

Maak een XaaS-blueprint.

Een XaaS-blueprint maken voor het maken van een gebruiker

U maakt de XaaS-blueprint Een gebruiker in een groep maken zodat u een werkstroom kunt uitvoeren waarmee een Active Directory-gebruiker wordt toegevoegd en de gebruiker wordt toegewezen aan een Active Directory-groep. U kunt de blueprint maken als standalone XaaS-blueprint of als blueprintonderdeel. In dit scenario maakt u een standalone blueprint.

Voorwaarden

- Controleer of de aangepaste bronactie die u maakt, de inrichting van Active Directory-gebruikers ondersteunt. Zie [Een testgebruiker maken als een aangepaste bron](#).
- Meld u aan bij vRealize Automation als een **XaaS-architect**.

Procedure

- 1 Selecteer **Ontwerpen > XaaS > XaaS-blueprints**.
- 2 Klik op het pictogram **Nieuw (+)**.
- 3 Navigeer vanuit het venster Selecteer een werkstroom naar **Orchestrator > Bibliotheek > Microsoft > Active Directory > Gebruiker** en selecteer de werkstroom **Een gebruiker in een groep maken**.
- 4 Klik op **Volgende**.

5 Configureer de opties op het tabblad **Algemeen**.

- a Wijzig de naam van de blueprint naar **Een testgebruiker maken** en behoud de beschrijving zoals deze is.
- b Schakel het selectievakje **Beschikbaar stellen als onderdeel in het ontwerpcanvas** uit.
U publiceert deze blueprint direct in de servicecatalogus en gebruikt deze dus niet als blueprintonderdeel op het ontwerpcanvas. U hoeft geen werkstromen voor in- of uitschalen te configureren.

Het tabblad **Levenscyclus onderdeel** is verwijderd uit de gebruikersinterface.

6 Klik op **Volgende**.**7** Bewerk het blueprintformulier.

- a Klik op **De domeinnaam in Win2000-formaat (The domain name in Win2000 form)**.
- b Klik op het tabblad **Beperkingen**.
- c Klik op de vervolgkeuzepijl **Waarde**, selecteer **Constante** in het vervolgkeuzemenu en voer **test.domain** in.
- d Klik op de vervolgkeuzepijl **Zichtbaar**, selecteer **Constante** in het vervolgkeuzemenu en selecteer **Nee** in het vervolgkeuzemenu.

U hebt de domeinnaam onzichtbaar gemaakt voor de consument van het catalogusitem.

- e Klik op **Toepassen** om de wijzigingen op te slaan.

8 Klik op **Volgende**.**9** Selecteer **nieuweGebruiker [Testgebruiker]** als een uitvoerparameter die moet worden ingericht.**10** Klik op **Volgende**.**11** Klik op **Voltooien**.**12** Selecteer op de pagina **XaaS-blueprints** de rij **Een testgebruiker maken** en klik op **Publiceren**.**Resultaten**

U hebt een blueprint gemaakt om een testgebruiker te maken en u hebt ervoor gezorgd dat de blueprint aan een service kan worden toegevoegd.

Wat nu te doen

Maak een actie die wordt uitgevoerd op de ingerichte gebruikersaccount. Zie [Een bronactie maken om een gebruikerswachtwoord te wijzigen](#).

Een bronactie maken om een gebruikerswachtwoord te wijzigen

U kunt een bronactie maken om consumenten van de XaaS toestemming te geven het wachtwoord van de gebruiker te wijzigen nadat ze de gebruiker hebben ingericht.

Voorwaarden

- Meld u aan bij vRealize Automation als een **XaaS-architect**.
- Controleer of de aangepaste bronactie die u maakt, de inrichting van Active Directory-gebruikers ondersteunt. Zie [Een testgebruiker maken als een aangepaste bron](#).

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Bronacties**.
- 2 Klik op het pictogram **Nieuw (+)**.
- 3 Ga naar **Orchestrator > Bibliotheek > Microsoft > Active Directory > Gebruiker** in de vRealize Orchestrator-werkstroombibliotheek en selecteer de werkstroom **Een gebruikerswachtwoord wijzigen**.
- 4 Klik op **Volgende**.
- 5 Selecteer **Testgebruiker** in het vervolgkeuzemenu **Brontype**.
Deze selectie is de aangepaste bron die u eerder hebt gemaakt.
- 6 Selecteer **gebruiker** in het vervolgkeuzemenu **Invoerparameter**.
- 7 Klik op **Volgende**.
- 8 Wijzig de naam van de bronactie in **Het wachtwoord van de testgebruiker wijzigen** en behoud de beschrijving zoals deze verschijnt op het tabblad **Details**.
- 9 Klik op **Volgende**.
- 10 (Optioneel) Behoud het formulier zoals het is.
- 11 Klik op **Voltooien**.
- 12 Selecteer op de pagina Bronacties de rij **Het wachtwoord van de testgebruiker wijzigen** en klik op **Publiceren**.

Resultaten

U hebt een bronactie gemaakt waarmee het wachtwoord van een gebruiker wordt gewijzigd en hebt de actie beschikbaar gesteld om als recht te verlenen.

Wat nu te doen

Voeg de blueprint Een testgebruiker maken toe aan een service. Zie [Een service maken en de blueprint Een testgebruiker maken toevoegen aan de service](#).

Een service maken en de blueprint Een testgebruiker maken toevoegen aan de service

U kunt een service maken waarmee het catalogusitem Een gebruiker maken wordt weergegeven in de servicecatalogus.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **catalogusbeheerder**.

- Zorg ervoor dat u een XaaS-blueprint hebt gemaakt. Zie [Een XaaS-blueprint maken voor het maken van een gebruiker](#).

Meld u aan bij vRealize Automation als een **tenantbeheerder** of **catalogusbeheerder**.

Procedure

- 1 Selecteer **Beheer > Catalogusbeheer > Services**.
- 2 Klik op het pictogram **Nieuw (+)**.
- 3 Voer **Active Directory-testgebruiker** in als naam van de service.
- 4 Selecteer **Actief** in het vervolgkeuzemenu **Status**.
- 5 Laat de andere tekstvakjes leeg.
- 6 Klik op **OK**.
- 7 Selecteer in de lijst met services de rij **Active Directory-testgebruiker** en klik op **Catalogusitems beheren**.
- 8 Klik op het pictogram **Nieuw (+)**.
- 9 Selecteer **Een testgebruiker maken** en klik op **OK**.
De XaaS-blueprint Een testgebruiker maken wordt toegevoegd aan de lijst van catalogusitems.
- 10 Klik op **Sluiten**.

Resultaten

De service Active Directory-testgebruiker bevat nu de blueprint Een testgebruiker maken. U hoeft geen acties aan de service toe te voegen.

Wat nu te doen

U kunt gebruikers het recht geven om de blueprint aan te vragen en de actie uit te voeren. Zie [Rechten voor de service en de bronactie verlenen aan een consument](#).

Rechten voor de service en de bronactie verlenen aan een consument

Bedrijfsgroepbeheerders en tenantbeheerders kunnen rechten voor de service en de bronactie verlenen aan een gebruiker of een groep gebruikers. Nadat er rechten aan hen zijn verleend, kunnen ze de service in hun catalogus weergeven en het catalogusitem Een testgebruiker maken aanvragen dat is opgenomen in de service. Nadat de consumenten het item hebben ingericht, kunnen ze een aanvraag indienen om het gebruikerswachtwoord te wijzigen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **bedrijfsgroepbeheerder**.
- Controleer of de blueprint Een gebruiker maken is toegevoegd aan de service. Zie [Een service maken en de blueprint Een testgebruiker maken toevoegen aan de service](#).

- Controleer of de bronactie Een gebruikerswachtwoord wijzigen bestaat. Zie [Een bronactie maken om een gebruikerswachtwoord te wijzigen](#).

Procedure

- 1 Selecteer **Beheer > Catalogusbeheer > Rechten**.
- 2 Klik op het pictogram **Nieuw (+)**.
- 3 Voer **Een Active Directory-gebruiker maken** in het tekstvak **Naam** in.
- 4 Laat de tekstvakken **Beschrijving** en **Vervaldatum** leeg.
- 5 Selecteer **Actief** in het vervolgkeuzemenu **Status**.
- 6 Selecteer de doelbedrijfsgroep in het vervolgkeuzemenu **Bedrijfsgroep**.
Bijvoorbeeld: IT-accountbeheerders.
- 7 Selecteer **Alle gebruikers en groepen** om aan alle leden van de bedrijfsgroep, zoals bijvoorbeeld aan alle IT-accountbeheerders, het recht te verlenen om een gebruikersaccount te maken.

De gebruikers die u selecteert, kunnen de service en de catalogusitems die in de service zijn opgenomen, in de catalogus zien. Ze kunnen ook de actie uitvoeren om een wachtwoord te wijzigen voor de gebruiker nadat deze is gemaakt.
- 8 Klik op **Volgende**.
- 9 Voer in het tekstvak **Services waarvoor rechten zijn verleend** de tekst **Active Directory-testgebruiker** in en druk op Enter.
- 10 Voer in het tekstvak **Acties waarvoor rechten zijn verleend** de tekst **Het wachtwoord van de testgebruiker wijzigen** in en druk op Enter.
- 11 Klik op **Voltooien**.

Resultaten

U hebt een actief recht gemaakt, zodat gebruikers die lid zijn van de bedrijfsgroep IT-accountbeheerders gebruikers kunnen maken. Nadat de gebruiker verder is ingericht, kan deze de bronactie uitvoeren om het wachtwoord te wijzigen van het ingerichte gebruikersaccount.

Wat nu te doen

Meld u aan als een gebruiker die het recht heeft om een Active Directory-gebruiker te maken. Controleer op het tabblad **Catalogus** of door de XaaS-blueprint een gebruiker is gemaakt, zoals verwacht. Nadat de gebruiker is aangemaakt, voert u de actie uit om het wachtwoord te wijzigen vanuit het tabblad **Implementaties**.

Een XaaS-actie voor de migratie van een virtual machine maken en publiceren

U kunt een XaaS-bronactie maken en publiceren voor het uitbreiden van de bewerkingen die consumenten kunnen uitvoeren op met IaaS ingerichte vSphere virtual machines.

In dit scenario maakt u een bronactie voor snelle migratie van een vSphere virtual machine.

Voorwaarden

Meld u aan bij vRealize Automation als een **XaaS-architect**.

Procedure

1 Een bronactie maken voor de migratie van een vSphere Virtual Machine

U maakt een aangepaste bronactie om consumenten de toestemming te geven om vSphere virtual machines te migreren nadat deze de vSphere virtual machines met IaaS hebben ingericht.

2 De actie Een vSphere virtual machine migreren publiceren

Als u de bronactie Snelle migratie van virtual machine wilt gebruiken als een bewerking na de inrichting, moet u deze actie eerst publiceren.

Een bronactie maken voor de migratie van een vSphere Virtual Machine

U maakt een aangepaste bronactie om consumenten de toestemming te geven om vSphere virtual machines te migreren nadat deze de vSphere virtual machines met IaaS hebben ingericht.

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Bronacties**.
- 2 Klik op **Toevoegen** (+).
- 3 Ga naar **Orchestrator > Bibliotheek > vCenter > Virtual Machine-beheer > Verplaatsen en migreren** in de vRealize Orchestrator-werkstroombibliotheek en selecteer de werkstroom **Snelle migratie van virtual machine**.
- 4 Klik op **Volgende**.
- 5 Selecteer **IaaS VC VirtualMachine** in het vervolgkeuzemenu **Brontype**.
- 6 Selecteer **vm** in het vervolgkeuzemenu **Invoerparameter**.
- 7 Klik op **Volgende**.
- 8 Behoud de naam van de bronactie en de beschrijving zoals deze worden weergegeven op het tabblad **Details**.
- 9 Klik op **Volgende**.
- 10 Behoud het formulier zoals het is.
- 11 Klik op **Voltooien**.

Resultaten

U hebt een bronactie gemaakt om een virtual machine te migreren en u kunt deze zien in de pagina met Bronacties.

Wat nu te doen

[De actie Een vSphere virtual machine migreren publiceren](#)

De actie Een vSphere virtual machine migreren publiceren

Als u de bronactie Snelle migratie van virtual machine wilt gebruiken als een bewerking na de inrichting, moet u deze actie eerst publiceren.

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Bronacties**.
- 2 Selecteer de rij van de bronactie Snelle migratie van virtual machine en klik op de knop **Publiceren**.

Resultaten

U hebt een vRealize Orchestrator-werkstroom gemaakt en gepubliceerd als een bronactie. U kunt naar **Beheer > Catalogusbeheer > Acties** gaan en de bronactie voor de snelle migratie van een virtual machine in de lijst met acties zien. U kunt een pictogram toewijzen aan de bronactie. Zie [Een pictogram toewijzen aan een XaaS-bronactie](#).

Wat nu te doen

Voeg de actie toe aan de rechten die de met IaaS ingerichte vSphere virtual machines bevatten. Zie [Gebruikers rechten verlenen voor services, catalogusitems en acties](#).

Een XaaS-actie maken om een virtual machine met vMotion te migreren

Met XaaS kunt u een bronactie maken en publiceren voor het migreren van een met IaaS ingerichte virtual machine met vMotion.

In dit scenario maakt u een bronactie voor het migreren van een vSphere virtual machine met vMotion. Daarnaast bewerkt u de werkstroompresentatie met behulp van het formulierontwerpprogramma en wijzigt u de manier waarop consumenten de actie te zien krijgen wanneer ze deze aanvragen.

Voorwaarden

Meld u aan bij vRealize Automation als een **XaaS-architect**.

Procedure

1 [Een actie maken om een vSphere Virtual Machine met vMotion te migreren](#)

U kunt een aangepaste bronactie maken om servicecatalogusgebruikers de toestemming te geven een vSphere virtual machine met vMotion te migreren nadat deze de machine hebben ingericht met IaaS.

2 [Het bronactieformulier bewerken](#)

Het bronactieformulier wijst de vRealize Orchestrator-werkstroompresentatie toe. U kunt het formulier bewerken en definiëren wat de consumenten van de bronactie zien wanneer ze ervoor kiezen om de bewerking na inrichting uit te voeren.

3 Een formulier met details van ingediende actie toevoegen en de actie opslaan

U kunt een nieuw formulier toevoegen aan de bronactie voor het migreren van een virtual machine met vMotion om te bepalen wat de consumenten zien, nadat ze een aanvraag hebben ingediend om de bewerking na inrichting uit te voeren.

4 De actie Een virtual machine migreren met vMotion publiceren

Als u de bronactie Een virtual machine migreren met vMotion wilt gebruiken als een bewerking na de inrichting, moet u deze actie eerst publiceren.

Een actie maken om een vSphere Virtual Machine met vMotion te migreren

U kunt een aangepaste bronactie maken om servicecatalogusgebruikers de toestemming te geven een vSphere virtual machine met vMotion te migreren nadat deze de machine hebben ingericht met IaaS.

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Bronacties**.
- 2 Klik op **Toevoegen** (+).
- 3 Ga naar **Orchestrator > Bibliotheek > vCenter > Virtual Machine-beheer > Verplaatsen en migreren** in de vRealize Orchestrator-werkstroombibliotheek en selecteer de werkstroom **Virtual machine migreren met vMotion**.
- 4 Klik op **Volgende**.
- 5 Selecteer **IaaS VC VirtualMachine** in het vervolgkeuzemenu **Brontype**.
- 6 Selecteer **vm** in het vervolgkeuzemenu **Invoerparameter**.
- 7 Klik op **Volgende**.
- 8 Behoud de naam van de bronactie en de beschrijving zoals deze worden weergegeven op het tabblad **Details**.
- 9 Klik op **Volgende**.

Wat nu te doen

[Het bronactieformulier bewerken.](#)


Het bronactieformulier bewerken

Het bronactieformulier wijst de vRealize Orchestrator-werkstroompresentatie toe. U kunt het formulier bewerken en definiëren wat de consumenten van de bronactie zien wanneer ze ervoor kiezen om de bewerking na inrichting uit te voeren.

Procedure

- 1 Klik op het pictogram **Verwijderen** (X) om het **pool**-element te verwijderen.

2 Bewerk het **host**-element.

- a Klik op het pictogram **Bewerken** () naast het **host**-veld.
- b Typ **Doelhost** in het tekstvak **Label**.
- c Selecteer **Zoeken** in het vervolgkeuzemenu **Type**.
- d Klik op het tabblad **Beperkingen**.
- e Selecteer **Constante** in het vervolgkeuzemenu **Vereist** en selecteer **Ja**.
U hebt het hostveld gemaakt dat altijd vereist is.
- f Klik op **Indienen**.

3 Bewerk het **priority**-element.

- a Klik op het pictogram **Bewerken** () naast het **priority**-veld.
- b Typ **Prioriteit van de taak** in het tekstvak **Label**.
- c Selecteer **Keuzerondjesgroep** in het vervolgkeuzemenu **Type**.
- d Klik op het tabblad **Waarden** en schakel het selectievakje **Niet ingesteld** uit.
- e Typ **lagePrioriteit** in het zoekvak **Vooraf gedefinieerde waarden** en druk op Enter.
- f Typ **standaardPrioriteit** in het zoekvak **Vooraf gedefinieerde waarden** en druk op Enter.
- g Typ **hogePrioriteit** in het zoekvak **Vooraf gedefinieerde waarden** en druk op Enter.
- h Klik op **Indienen**.

Wanneer de consumenten de bronactie aanvragen, zien ze een keuzerondjesgroep met drie keuzerondjes: **lagePrioriteit**, **standaardPrioriteit** en **hogePrioriteit**.

4 Bewerk het **state**-element.

- a Klik op het pictogram **Bewerken** () naast het **state**-veld.
- b Typ **Virtual machinestatus** in het tekstvak **Label**.
- c Selecteer **Vervolgkeuze** in het vervolgkeuzemenu **Type**.
- d Klik op het tabblad **Waarden** en schakel het selectievakje **Niet ingesteld** uit.
- e Typ **uitgeschakeld** in het zoekvak **Vooraf gedefinieerde waarden** en druk op Enter.
- f Typ **ingeschakeld** in het zoekvak **Vooraf gedefinieerde waarden** en druk op Enter.
- g Typ **onderbroken** in het zoekvak **Vooraf gedefinieerde waarden** en druk op Enter.
- h Klik op **Indienen**.

Wanneer de consumenten de bronactie aanvragen, zien ze een vervolgkeuzemenu met drie opties: **uitgeschakeld**, **ingeschakeld** en **onderbroken**.

Resultaten

U hebt de werkstroompresentatie van de werkstroom Een virtual machine migreren met vMotion bewerkt.

Wat nu te doen

[Een formulier met details van ingediende actie toevoegen en de actie opslaan.](#)

Een formulier met details van ingediende actie toevoegen en de actie opslaan

U kunt een nieuw formulier toevoegen aan de bronactie voor het migreren van een virtual machine met vMotion om te bepalen wat de consumenten zien, nadat ze een aanvraag hebben ingediend om de bewerking na inrichting uit te voeren.

Procedure

- 1 Klik op het pictogram **Nieuw formulier** (+) naast het vervolgkeuzemenu **Formulier**.
- 2 Typ **Ingediende actie** in het tekstvak **Naam**.
- 3 Laat het veld **Beschrijving** leeg.
- 4 Selecteer **Details ingediende actie** in het menu **Schermtyp**.
- 5 Klik op **Indienen**.
- 6 Klik op het pictogram **Bewerken** (pencil) naast het vervolgkeuzemenu **Formulierpagina**.
- 7 Typ **Details** in het tekstvak **Titel**.
- 8 Klik op **Indienen**.
- 9 Sleep het element **Tekst** van het deelvenster **Formulier** naar de pagina **Formulier**.
- 10 Typ
U hebt een aanvraag ingediend om uw machine te migreren met vMotion. Wacht totdat het proces is voltooid.
- 11 Klik op een plaats buiten het tekstvak om de wijzigingen op te slaan.
- 12 Klik op **Indienen**.
- 13 Klik op **Toevoegen**.

Resultaten

U hebt een bronactie gemaakt om een virtual machine te migreren met vMotion en u kunt deze zien in de pagina met Bronacties.

Wat nu te doen

[De actie Een virtual machine migreren met vMotion publiceren.](#)

De actie Een virtual machine migreren met vMotion publiceren

Als u de bronactie Een virtual machine migreren met vMotion wilt gebruiken als een bewerking na de inrichting, moet u deze actie eerst publiceren.

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Bronacties**.
- 2 Selecteer de rij van de bronactie Een virtual machine migreren met vMotion en klik op de knop **Publiceren**.

Resultaten

U hebt een vRealize Orchestrator-werkstroom gemaakt en gepubliceerd als een bronactie. U kunt naar **Beheer > Catalogusbeheer > Acties** gaan en de bronactie voor het migreren van een virtual machine met vMotion in de lijst met acties zien. U kunt een pictogram toewijzen aan de bronactie. Zie [Een pictogram toewijzen aan een XaaS-bronactie](#).

U hebt ook de presentatie van de werkstroom bewerkt en de vormgeving van de actie gedefinieerd.

Wat nu te doen

Bedrijfsgroepbeheerders en tenantbeheerders kunnen de bronactie voor het migreren van een virtual machine met vMotion opnemen in een recht. Zie [Machineblueprints ontwerpen](#) voor meer informatie over het maken en publiceren van IaaS-blueprints voor virtuele platforms.

Een XaaS-actie voor het maken van een momentopname maken en publiceren

Met XaaS kunt u een bronactie maken en publiceren voor het maken van een momentopnamen van een vSphere virtual machine die is ingericht met IaaS.

In dit scenario maakt u een bronactie voor het maken van een momentopname van een vSphere virtual machine die is ingericht met IaaS. Daarnaast bewerkt u de werkstroompresentatie met behulp van het formulierontwerpprogramma en wijzigt u de manier waarop consumenten de actie te zien krijgen wanneer ze deze aanvragen.

Voorwaarden

Meld u aan bij vRealize Automation als een **XaaS-architect**.

Procedure

- 1 [De actie voor het maken van een momentopname van een vSphere Virtual Machine maken](#)

U kunt een aangepaste bronactie maken om consumenten de toestemming te geven een momentopname te maken van een vSphere virtual machine nadat deze de machine hebben ingericht met IaaS.

- 2 [De actie Momentopname maken publiceren](#)

Als u de bronactie Momentopname maken wilt gebruiken als een bewerking na de inrichting, moet u deze actie eerst publiceren.

De actie voor het maken van een momentopname van een vSphere Virtual Machine maken

U kunt een aangepaste bronactie maken om consumenten de toestemming te geven een momentopname te maken van een vSphere virtual machine nadat deze de machine hebben ingericht met IaaS.

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Bronacties**.
- 2 Klik op **Toevoegen** (+).
- 3 Ga naar **Orchestrator > Bibliotheek > vCenter > Virtual Machine-beheer > Momentopname** in de vRealize Orchestrator-werkstroombibliotheek en selecteer de werkstroom **Een momentopname maken**.
- 4 Klik op **Volgende**.
- 5 Selecteer **IaaS VC VirtualMachine** in het vervolgkeuzemenu **Brontype**.
- 6 Selecteer **vm** in het vervolgkeuzemenu **Invoerparameter**.
- 7 Klik op **Volgende**.
- 8 Behoud de naam van de bronactie en de beschrijving zoals deze worden weergegeven op het tabblad **Details**.
- 9 Klik op **Volgende**.
- 10 Behoud het formulier zoals het is.
- 11 Klik op **Toevoegen**.

Resultaten

U hebt een bronactie gemaakt om momentopname van een virtual machine te maken en u kunt deze zien op de pagina met Bronacties.

Wat nu te doen

[De actie Momentopname maken publiceren](#).

De actie Momentopname maken publiceren

Als u de bronactie Momentopname maken wilt gebruiken als een bewerking na de inrichting, moet u deze actie eerst publiceren.

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Bronacties**.
- 2 Selecteer de rij van de bronactie Momentopname maken en klik op de knop **Publiceren**.

Resultaten

U hebt een vRealize Orchestrator-werkstroom gemaakt en gepubliceerd als een bronactie. U kunt naar **Beheer > Catalogusbeheer > Acties** gaan en de bronactie voor het maken van een momentopname in de lijst met acties zien. U kunt een pictogram toewijzen aan de bronactie. Zie [Een pictogram toewijzen aan een XaaS-bronactie](#).

Wat nu te doen

Bedrijfsgroepbeheerders en tenantbeheerders kunnen de bronactie voor het maken van een momentopname opnemen in een recht. Zie [Machineblueprints ontwerpen](#) voor meer informatie over het maken en publiceren van IaaS-blueprints voor virtuele platforms.

Een XaaS-actie voor het starten van een Amazon Virtual Machine maken en publiceren

Met XaaS kunt u acties maken en publiceren voor het uitbreiden van de bewerkingen die consumenten kunnen uitvoeren op bronnen die zijn ingericht door derden.

In dit scenario maakt en publiceert u een bronactie voor het snel opstarten van Amazon virtual machines.

Voorwaarden

- Installeer de vRealize Orchestrator-invoegtoepassing voor Amazon Web Services op uw standaard vRealize Orchestrator-server.
- Maak of importeer een vRealize Orchestrator-werkstroom voor brontoewijzing van Amazon-instanties.

Procedure

1 [Een brontoewijzing maken voor Amazon-instanties](#)

U kunt een brontoewijzing maken om Amazon-instanties die zijn ingericht met IaaS te koppelen aan het vRealize Orchestrator-type AWS:EC2Instance dat wordt weergegeven door de Amazon Web Services-invoegtoepassing.

2 [Een bronactie maken om Amazon Virtual Machine te starten](#)

U kunt een bronactie maken zodat de consumenten ingerichte Amazon-virtual machines kunnen starten.

3 [De actie Amazon-instanties starten publiceren](#)

Als u de zo juist gemaakte bronactie Instanties starten wilt gebruiken als bewerkingen na inrichting voor Amazon virtual machines, moet u deze actie eerst publiceren.

Een brontoewijzing maken voor Amazon-instanties

U kunt een brontoewijzing maken om Amazon-instanties die zijn ingericht met IaaS te koppelen aan het vRealize Orchestrator-type AWS:EC2Instance dat wordt weergegeven door de Amazon Web Services-invoegtoepassing.

Voorwaarden

- Meld u aan bij vRealize Automation als een **XaaS-architect**.
- Maak of importeer een vRealize Orchestrator-brontoewijzingswerkstroom of -scriptactie.

Procedure

1 Selecteer **Ontwerpen > XaaS > Brontoewijzingen**.

- 2 Klik op **Toevoegen** (+).
- 3 Typ **EC2 Instance** in het tekstvak **Naam**.
- 4 Typ **Cloud Machine** in het tekstvak **Catalogusbrontype**.
- 5 Typ **AWS:EC2Instance** in het tekstvak **Orchestrator-type**.
- 6 Selecteer **Altijd beschikbaar**.
- 7 Selecteer het type brontoewijzing dat u wilt gebruiken.
- 8 Selecteer uw aangepaste brontoewijzingsscriptactie of -werkstroom in de vRealize Orchestrator-bibliotheek.
- 9 Klik op **Toevoegen**.

Resultaten

U kunt uw Amazon-brontoewijzing gebruiken om bronacties te maken voor Amazon-machines die zijn ingericht met behulp van IaaS.

Wat nu te doen

[Een bronactie maken om Amazon Virtual Machine te starten.](#)

Een bronactie maken om Amazon Virtual Machine te starten

U kunt een bronactie maken zodat de consumenten ingerichte Amazon-virtual machines kunnen starten.

Voorwaarden

Meld u aan bij vRealize Automation als een **XaaS-architect**.

Procedure

- 1 Selecteer **Ontwerpen > XaaS > Bronacties**.
- 2 Klik op **Toevoegen** (+).
- 3 Selecteer **Orchestrator > Bibliotheek > Amazon Web Services > Elastische cloud > Instanties** en selecteer de werkstroom **Instanties starten** in de map met werkstromen.
- 4 Klik op **Volgende**.
- 5 Selecteer **EC2-instantie** in het vervolgkeuzemenu **Brontype**.
Dit is de naam van de brontoewijzing die u eerder hebt gemaakt.
- 6 Selecteer **instantie** in het vervolgkeuzemenu **Invoerparameter**.
Dit is de invoerparameter van de bronactiewerkstroom die overeenkomt met de brontoewijzing.
- 7 Klik op **Volgende**.

8 Laat de naam en de beschrijving zoals ze zijn.

De standaardnaam van de bronactie is Instanties starten.

9 Klik op **Volgende**.

10 Laat de velden zoals ze zijn op het tabblad **Formulier**.

11 Klik op **Toevoegen**.

Resultaten

U hebt een bronactie gemaakt om Amazon-virtual machines te starten en u kunt deze zien in de pagina met Bronacties.

Wat nu te doen

[De actie Amazon-instanties starten publiceren](#).

De actie Amazon-instanties starten publiceren

Als u de zo juist gemaakte bronactie Instanties starten wilt gebruiken als bewerkingen na inrichting voor Amazon virtual machines, moet u deze actie eerst publiceren.

Voorwaarden

Meld u aan bij vRealize Automation als een **XaaS-architect**.

Procedure

1 Selecteer **Ontwerpen > XaaS > Bronacties**.

2 Selecteer de rij van de bronactie Instanties starten en klik op **Publiceren**.

Resultaten

De status van de bronactie Instanties starten wordt gewijzigd in Gepubliceerd.

Wat nu te doen

Voeg de actie Instanties starten toe aan het recht dat het Amazon-catalogusitem bevat. Zie [Gebruikers rechten verlenen voor services, catalogusitems en acties](#).

Problemen met onjuiste accenttekens en speciale tekens in XaaS-blueprints oplossen

Wanneer u XaaS-blueprints maakt voor talen die niet-ASCII-tekenreeksen gebruiken, worden de accenttekens en speciale tekens weergegeven als onbruikbare tekenreeksen.

Oorzaak

Een vRealize Orchestrator-configuratie-eigenschap die niet standaard is ingesteld, is mogelijk ingeschakeld.

Oplossing

1 Ga op het Orchestrator-serversysteem naar `/etc/vco/app-server/`.

- 2 Open het configuratiebestand `vmo.properties` in een teksteditor.
- 3 Controleer of de volgende eigenschap is gedeactiveerd.

```
com.vmware.o11n.webview.htmlescaping.disabled
```

- 4 Sla het bestand `vmo.properties` op.
- 5 Start de vRealize Orchestrator-server opnieuw op.

Een blueprint publiceren

Blueprints worden opgeslagen met de status Concept en moeten handmatig worden gepubliceerd, voordat u ze kunt configureren als catalogusitems of ze kunt gebruiken als componenten van blueprints in het ontwerpcanvas.

Nadat u de blueprint hebt gepubliceerd, kunt u er rechten aan toekennen en de blueprint beschikbaar maken voor inrichtingsaanvragen in de servicecatalogus.

U hoeft een blueprint maar eenmaal te publiceren. Alle veranderingen die u aanbrengt in een gepubliceerde blueprint worden automatisch weergegeven in de catalogus en in geneste blueprint-onderdelen.

Een blueprint publiceren

U kunt een blueprint publiceren voor gebruik bij het inrichten van een machine en optioneel voor hergebruik in een andere blueprint. Als u de blueprint wilt gebruiken om het inrichten van een machine aan te vragen, moet u rechten toekennen aan de blueprint na publicatie. Blueprints die als componenten worden opgenomen in andere blueprints hoeven geen rechten te krijgen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **infrastructuurarchitect**.
- Maak een blueprint. Zie *Checklist voor het maken van vRealize Automation-blueprints*.

Procedure

- 1 Klik op het tabblad **Ontwerpen**.
- 2 Klik op **Blueprints**.
- 3 Wijs de blueprint die u wilt publiceren aan en klik op **Publiceren**.
- 4 Klik op **OK**.

Resultaten

De blueprint wordt gepubliceerd als een catalogusitem maar u moet er eerst rechten aan toekennen om het beschikbaar te maken voor gebruikers in de servicecatalogus.

Wat nu te doen

Voeg de blueprint toe aan de servicecatalogus en ken rechten toe aan gebruikers, zodat ze het catalogusitem kunnen aanvragen om de machine in te richten, zoals gedefinieerd in de blueprint.

Werken met door ontwikkelaar gestuurde blueprints

Naast de methode voor het maken van vRealize Automation-blueprints met een gebruikersinterface, kunt u ook programmerend werken met tools zoals vRealize CloudClient, met zelfstandig opgegeven blueprints, of blueprints van een andere bron, en in samenwerking met andere ontwikkelaars door gebruik te maken van werkstromen, met inbegrip van vRealize Suite-werkstromen en hulpprogramma's van derden.

Raadpleeg de volgende onderwerpen voor informatie over deze methoden:

- [Blueprints en inhoud exporteren en importeren](#)
- [De opgegeven standalone blueprint downloaden en configureren](#)
- [Blueprints en andere IaaS-inhoud maken in een omgeving met meerdere ontwikkelaars](#)

Blueprints en inhoud exporteren en importeren

Met de REST API van vRealize Automation of met de vRealize CloudClient kunt u blueprints en inhoud van de ene vRealize Automation-omgeving programmatisch exporteren naar een andere omgeving.

U kunt bijvoorbeeld blueprints maken en testen in een ontwikkelingsomgeving en ze vervolgens in uw productieomgeving importeren. Of u kunt een eigenschapsdefinitie uit een communityforum importeren in uw actieve vRealize Automation-tenantinstantie.

U kunt de volgende inhouditems van vRealize Automation programmatisch importeren en exporteren:

- Toepassingsblueprints en al hun onderdelen
- IaaS-machineblueprints
- Onderdelen van Software
- XaaS-blueprints
- Onderdeelprofielen
- Eigenschapsgroepen

Informatie over eigenschapsgroepen is specifiek voor een tenant en wordt alleen geïmporteerd met de blueprint als de eigenschapsgroep al bestaat in de vRealize Automation-doelinstantie.

Wanneer u een blueprint van de ene vRealize Automation-instantietenant naar een andere exporteert, wordt de informatie over de eigenschapsgroep die voor die blueprint is gedefinieerd niet herkend voor de geïmporteerde blueprint, tenzij de eigenschapsgroep al in de doeltentantinstantie bestaat. Als u bijvoorbeeld een blueprint importeert die een

eigenschapsgroep met de naam `mica1` bevat, is de eigenschapsgroep `mica1` niet aanwezig in de geïmporteerde blueprint, tenzij de eigenschapsgroep `mica1` al bestaat in de vRealize Automation-instantie waarin u de blueprint importeert. Om te voorkomen dat u informatie over eigenschapsgroepen verliest wanneer u een blueprint van de ene naar de andere vRealize Automation-instantie exporteert, gebruikt u vRealize CloudClient om een zip-bestand van het exportpakket te maken dat de eigenschapsgroep bevat. Vervolgens importeert u dat zip-bestand in de doeltenant voordat u de blueprint importeert. Voor meer informatie over het gebruik van vRealize CloudClient voor het opnoemen, verpakken, exporteren en importeren van eigenschapsgroepen, alsmede andere vRealize Automation-items, raadpleegt u het VMware Developer Center op <https://developercenter.vmware.com/tool/cloudclient>.

Tabel 3-63. Het import- en exporttool kiezen

Tool	Meer informatie
vRealize CloudClient	Zie de pagina vRealize CloudClient op de website VMware code.vmware.com op https://developercenter.vmware.com/tool/cloudclient .
vRealize Automation REST API	Zie de API-documentatie in de VMware API Explorer voor vRealize Automation op https://code.vmware.com/apis/vrealize-automation .

Opmerking Wanneer u blueprints binnen vRealize Automation-implementaties programmatisch importeert en exporteert om ze bijvoorbeeld van een testomgeving naar een productieomgeving over te brengen of van de ene organisatie naar de andere, moet u er rekening mee houden dat gegevens voor kloonsjablonen deel uitmaken van het pakket. Als u een blueprintpakket importeert, worden de standaardinstellingen namelijk automatisch ingevuld op basis van de gegevens in het pakket. Stel u hebt een blueprint gemaakt via een werkstroom met kloonbewerkingen. Wanneer u deze blueprint vervolgens exporteert en daarna importeert naar een vRealize Automation-implementatie met een endpoint waarop de sjabloon met de vereiste kloongegevens niet wordt gevonden, dan zullen bepaalde geïmporteerde blueprintinstellingen niet beschikbaar zijn voor die implementatie.

Scenario: de Dukes Bank voor vSphere-voorbeeldtoepassing importeren en configureren voor uw omgeving

U bent IT-professional en wilt in het kader van een evaluatie of training voor vRealize Automation een robuuste voorbeeldtoepassing in uw vRealize Automation-instantie importeren, zodat u snel kunt zien welke functionaliteit beschikbaar is en hoe u vRealize Automation-blueprints kunt maken die passen bij de behoeften van uw organisatie.

Voorwaarden

- Bereid een CentOS 6.x Linux-referentiemachine voor, converteer deze naar een sjabloon en maak een aanpassingsspecificatie. Zie [Scenario: import van de blueprint van de vSphere-voorbeeldtoepassing voor Dukes Bank voorbereiden](#).

- Maak een extern netwerkprofiel ten behoeve van een gateway met een IP-adresbereik. Zie [Een extern netwerkprofiel maken via een externe IPAM-provider](#).
- Koppel uw externe netwerkprofiel aan uw vSphere-reservering. Zie [Een reservering maken voor Hyper-V, KVM, SCVMM, vSphere of XenServer](#). Zonder extern netwerkprofiel kan de voorbeeldtoepassing niet juist worden ingericht.
- Controleer of u over privileges voor zowel **infrastructuurarchitect** als **softwarearchitect** beschikt. Voor beide rollen moet de Dukes Bank-voorbeeldtoepassing worden geïmporteerd en moet worden gecommuniceerd met de Dukes Bank-blueprints en de softwareonderdelen.

Procedure

1 [Scenario: de voorbeeldtoepassing Dukes Bank voor vSphere importeren](#)

U downloadt de toepassing Dukes Bank voor vSphere van uw vRealize Automation-toepassing. U importeert de voorbeeldtoepassing in uw vRealize Automation-tenant om een werkend voorbeeld te bekijken van een multi-tiered vRealize Automation-blueprint die meerdere machineonderdelen met netwerk- en softwareonderdelen bevat.

2 [Scenario: de vSphere-voorbeeldonderdelen voor Dukes Bank configureren voor uw omgeving](#)

Configureer, gebruikmakend van uw privileges als infrastructuurarchitect, de afzonderlijke machineonderdelen van de Dukes Bank zodat ze gebruikmaken van de aanpassingsspecificatie, sjabloon en machinevoorvoegsels die u voor uw omgeving hebt gemaakt.

Resultaten

U hebt de Dukes Bank voor vSphere-voorbeeldtoepassing voor uw omgeving ingesteld zodat deze kan worden gebruikt als startpunt voor de ontwikkeling van uw eigen blueprints, als hulpmiddel bij de evaluatie van vRealize Automation of bij trainingen zodat u vRealize Automation-functionaliteit en -onderdelen beter leert kennen.

Scenario: de voorbeeldtoepassing Dukes Bank voor vSphere importeren

U downloadt de toepassing Dukes Bank voor vSphere van uw vRealize Automation-toepassing. U importeert de voorbeeldtoepassing in uw vRealize Automation-tenant om een werkend voorbeeld te bekijken van een multi-tiered vRealize Automation-blueprint die meerdere machineonderdelen met netwerk- en softwareonderdelen bevat.

Procedure

- 1 Meld u aan bij uw vRealize Automation-toepassing als rootgebruiker met behulp van SSH.
- 2 Download de voorbeeldtoepassing Dukes Bank voor vSphere van uw vRealize Automation-toepassing naar /tmp.

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn:5480/blueprints/
DukesBankAppForvSphere.zip
```

Pak het pakket niet uit.

- 3 Download vRealize CloudClient van <http://developercenter.vmware.com/tool/cloudclient> naar /tmp.
- 4 Pak het pakket cloudclient-4x-dist.zip uit.
- 5 Voer vRealize CloudClient uit onder de directory /bin.

```
$>./bin/cloudclient.sh
```

- 6 Accepteer de licentieovereenkomst als u daarom wordt gevraagd.
- 7 Meld u met behulp van vRealize CloudClient aan bij de vRealize Automation-toepassing als een gebruiker met rechten voor **softwarearchitect** en **infrastructuurarchitect**.

```
CloudClient>vra login userpass --server https://vRealize_VA_Hostname_fqdn --user  
<gebruiker@domein.com> --tenant <Tenantnaam>
```

- 8 Voer uw aanmeldingswachtwoord in als u daarom wordt gevraagd.
- 9 Controleer of de inhoud van DukesBankAppForvSphere.zip beschikbaar is.

```
vra content import --path /<Path>/DukesBankAppForvSphere.zip --dry-run true --resolution OVERWRITE
```

De invoer OVERSCHRIJVEN is hoofdlettergevoelig en vereist hoofdletters.

Door de resolutie te configureren voor overschrijven in plaats van *skip* (overslaan), zorgt u dat vRealize Automation conflicten indien mogelijk corrigeert.

- 10 Importeer de Dukes Bank-voorbeeldtoepassing.

```
vra content import --path /<Path>/DukesBankAppForvSphere.zip --dry-run false --resolution  
OVERWRITE
```

De invoer OVERSCHRIJVEN is hoofdlettergevoelig en vereist hoofdletters.

Resultaten

Wanneer u zich bij de vRealize Automation-console aanmeldt als gebruiker met de rechten van een softwarearchitect en infrastructuurarchitect, ziet u blueprints en softwareonderdelen van Dukes Bank op het tabblad **Ontwerp > Blueprints** en het tabblad **Ontwerp > Softwareonderdelen**.

Scenario: de vSphere-voorbeeldonderdelen voor Dukes Bank configureren voor uw omgeving

Configureer, gebruikmakend van uw privileges als infrastructuurarchitect, de afzonderlijke machineonderdelen van de Dukes Bank zodat ze gebruikmaken van de aanpassingsspecificatie, sjabloon en machinevoorvoegsels die u voor uw omgeving hebt gemaakt.

In dit scenario worden de machineonderdelen geconfigureerd voor het klonen van machines op basis van de sjabloon die u hebt gemaakt in de vSphere Web Client. Als u ruimtebesparende kopieën van een virtual machine wilt maken op basis van een momentopname, moet de voorbeeldtoepassing ook gekoppelde klonen ondersteunen. Gekoppelde klonen maken gebruik van een keten van deltaschijven om de verschillen met de oorspronkelijke machine vast te leggen. Ze maken een snelle inrichting met lagere opslagkosten mogelijk en zijn bij uitstek geschikt voor situaties waarin prestaties niet vooropstaan.

Procedure

- 1 Meld u aan bij de vRealize Automation-console als **infrastructuurarchitect**.

U kunt de voorbeeldtoepassing Dukes Bank zo configureren dat deze in uw omgeving alleen werkt op basis van de rol **infrastructuurarchitect**, maar als u de voorbeeldsoftwareonderdelen wilt weergeven of bewerken hebt u ook de rol **softwarearchitect** nodig.

- 2 Selecteer **Ontwerpen > Blueprints**.

- 3 Selecteer de blueprint **DukesBankApplication** en klik op het pictogram **Bewerken**.

- 4 Bewerk het appserver-knooppunt zodat vRealize Automation dit machineonderdeel in uw omgeving kan inrichten.

U configureert de blueprint voor het inrichten van meerdere instanties van dit machineonderdeel, zodat u de functionaliteit van het load balancer-knooppunt kunt verifiëren.

- a Klik op het onderdeel **appserver-node** op het ontwerpcanvas.

De configuratiedetails verschijnen in het onderste venster.

- b Selecteer uw machinevoorvoegsel in het vervolgkeuzemenu **Machinevoorvoegsel**.

- c Configureer uw blueprint voor het inrichten van ten minste twee en maximaal tien instanties van dit knooppunt door minimaal 2 en maximaal 10 instanties te selecteren.

Op het aanvraagformulier kunnen gebruikers minimaal twee en maximaal tien appserver-knooppunten opgeven. Als gebruikers rechten hebben voor de acties Opschalen en Neerschalen, kunnen ze hun implementatie aanpassen aan de veranderende behoeften.

- d Klik op het tabblad **Versie-informatie**.

- e Selecteer **CloneWorkflow** in het vervolgkeuzemenu **Inrichtingswerkstroom**.

- f Selecteer uw **dukes_bank_template** in het dialoogvenster **Klonen van**.

- g Geef uw **Voorbeeld_aanpassingsspecificatie** op in het tekstvak **Specificatie aanpassing**.

Dit veld is hoofdlettergevoelig.

- h Klik op het tabblad **Machinebronnen**.

- i Controleer of bij de geheugeninstellingen ten minste 2048 MB is vermeld.

- 5 Bewerk het machineonderdeel load balancerknooppunt zodat vRealize Automation dit in uw omgeving kan inrichten.
 - a Klik op het onderdeel **load balancerknooppunt** op het ontwerpcanvas.
 - b Selecteer uw machinevoorvoegsel in het vervolgkeuzemenu **Machinevoorvoegsel**.
 - c Klik op het tabblad **Versie-informatie**.
 - d Selecteer **CloneWorkflow** in het vervolgkeuzemenu **Inrichtingswerkstroom**.
 - e Selecteer uw **dukes_bank_template** in het dialoogvenster **Klonen van**.
 - f Geef uw **Voorbeeld_aanpassingsspecificatie** op in het tekstvak **Specificatie aanpassing**.
Dit veld is hoofdlettergevoelig.
 - g Klik op het tabblad **Machinebronnen**.
 - h Controleer of bij de geheugeninstellingen ten minste 2048 MB is vermeld.
- 6 Herhaal voor het machineonderdeel **database-node**.
- 7 Klik op **Opslaan en voltooiën**.
Uw wijzigingen worden opgeslagen en u keert terug naar het tabblad **Blueprints**.
- 8 Selecteer de blueprint **DukesBankApplication** en klik op **Publiceren**.

Resultaten

U hebt de blueprint voor de Dukes Bank-voorbeeldtoepassing nu ingesteld voor uw omgeving en de definitieve blueprint gepubliceerd.

Wat nu te doen

Gepubliceerde blueprints zijn voor gebruikers pas zichtbaar in de catalogus als u een catalogusservice hebt ingesteld, de blueprint aan een service hebt toegevoegd en gebruikers rechten hebt verleend om uw blueprint aan te vragen. Zie [Checklist voor het configureren van de servicecatalogus](#).

Nadat u de weergave van de Dukes Bank-blueprint in de catalogus hebt ingesteld, is het mogelijk een aanvraag in te dienen voor inrichting van de voorbeeldtoepassing. Zie [Scenario: de Dukes Bank-voorbeeldtoepassing testen](#).

Scenario: de Dukes Bank-voorbeeldtoepassing testen

U vraagt het catalogusitem Dukes Bank aan en meldt u aan bij de voorbeeldtoepassing om controleren of de vRealize Automation-blueprint goed werkt.

Voorwaarden

- Importeer de voorbeeldtoepassing Dukes Bank configureer de blueprintonderdelen voor uw omgeving. Zie [Scenario: de Dukes Bank voor vSphere-voorbeeldtoepassing importeren en configureren voor uw omgeving](#).

- Configureer de servicecatalogus en stel uw gepubliceerde Dukes Bank-blueprint beschikbaar voor aanvraag door gebruikers. Zie [Checklist voor het configureren van de servicecatalogus](#).
- Controleer of de ingerichte virtual machines toegang hebben tot Yum-opslagplaats.

Procedure

- 1 Meld u aan bij de vRealize Automation-console als gebruiker met rechten voor het catalogusitem Dukes Bank.
- 2 Klik op het tabblad **Catalogus**.
- 3 Zoek het catalogusitem voor de Dukes Bank-voorbeeldtoepassing en klik op **Aanvragen**.
- 4 Vul de vereiste aanvraaggegevens voor elk onderdeel in (te herkennen aan het rode sterretje).
 - a Ga naar het onderdeel JBossAppServer en vul de vereiste aanvraaggegevens in.
 - b Typ de volledig gekwalificeerde domeinnaam van uw vRealize Automation-toepassing in het tekstvak **app_content_server_ip**.
 - c Ga naar de Dukes_Bank_App-softwareonderdelen en vul de vereiste aanvraaggegevens in.
 - d Typ de volledig gekwalificeerde domeinnaam van uw vRealize Automation-toepassing in de tekstvakken **app_content_server_ip**.
- 5 Klik op **Indienen**.

Afhankelijk van het netwerk en de vCenter Server-instantie, kan het ongeveer 15 à 20 minuten duren voordat de Dukes Bank-voorbeeldtoepassing volledig is ingericht. U kunt de status op het tabblad **Implementatie** volgen. Na de provisioning van de applicatie kunt u de catalogusitemgegevens bekijken op het tabblad **Implementaties**.
- 6 Als u de toepassing hebt ingericht, zoekt u het IP-adres van de load balancer-server zodat u de Dukes Bank-voorbeeldtoepassing kunt openen.
 - a Klik op **Implementaties**.
 - b Zoek uw Dukes Bank-voorbeeld van een applicatieimplementatie en klik op de implementatiennaam.
 - c Selecteer de Apache load balancer-server op het tabblad **Componenten**.
 - d Selecteer het tabblad **Netwerk**.
 - e Noteer het IP-adres.

7 Meld u aan bij de Dukes Bank-voorbeeldtoepassing.

- a Ga naar uw load balancer-server op `http://IP_Apache_Load_Balancer:8081/bank/main.faces`.

Als u de toepassingsservers rechtstreeks wilt openen, kunt u naar `http://IP_AppServer:8080/bank/main.faces` gaan.

- b Typ **200** in het tekstvak **Gebruikersnaam**.
- c Typ **foobar** in het tekstvak **Wachtwoord**.

Resultaten

U hebt de Dukes Bank-voorbeeldtoepassing ingesteld zodat deze kan worden gebruikt als startpunt voor de ontwikkeling van uw eigen blueprints, als hulpmiddel bij de evaluatie van vRealize Automation of voor trainingen waarmee u leert werken met de functionaliteit en onderdelen van vRealize Automation.

De opgegeven standalone blueprint downloaden en configureren

U kunt een opgegeven standalone blueprint en de bijbehorende softwareonderdelen downloaden van de vRealize Automation-appliance.

Het document [Standalone vRealize Automation-blueprint downloaden en configureren](#) begeleidt u door het proces voor het downloaden van een standalone vRealize Automation-blueprint van de vRealize Automation-toepassing en vervolgens voor het importeren, configureren en gebruiken van die blueprint in vRealize Automation in combinatie met verschillende vRealize Orchestrator-werkstromen.

Blueprints en andere IaaS-inhoud maken in een omgeving met meerdere ontwikkelaars

Meerdere ontwikkelaars kunnen vRealize Orchestrator-werkstromen gebruiken in combinatie met vRealize Suite en externe ontwikkelhulpprogramma's om gelijktijdig te werken aan verschillende vRealize Automation-blueprintartefacten voor dezelfde of voor verschillende vRealize Automation-blueprints.

U kunt tools zoals vRealize Suite Lifecycle Manager gebruiken om een omgeving te faciliteren met meerdere ontwikkelaars voor vRealize Automation- en andere vRealize Suite-tools en u kunt OVA's of externe tools gebruiken, zoals GitLab/GitHub, Houdini en andere toepassingsartefacten van de [VMware Solutions Exchange](#).

Raadpleeg de volgende bronnen voor meer informatie over het maken van vRealize Automation-blueprints en andere IaaS-inhoud, zoals eigenschappen, gebeurtenisbrokerabonnementsen, softwareonderdelen en vRealize Orchestrator-werkstromen in een omgeving met meerdere ontwikkelaars:

- [Video: What's New in Lifecycle Manager](#)

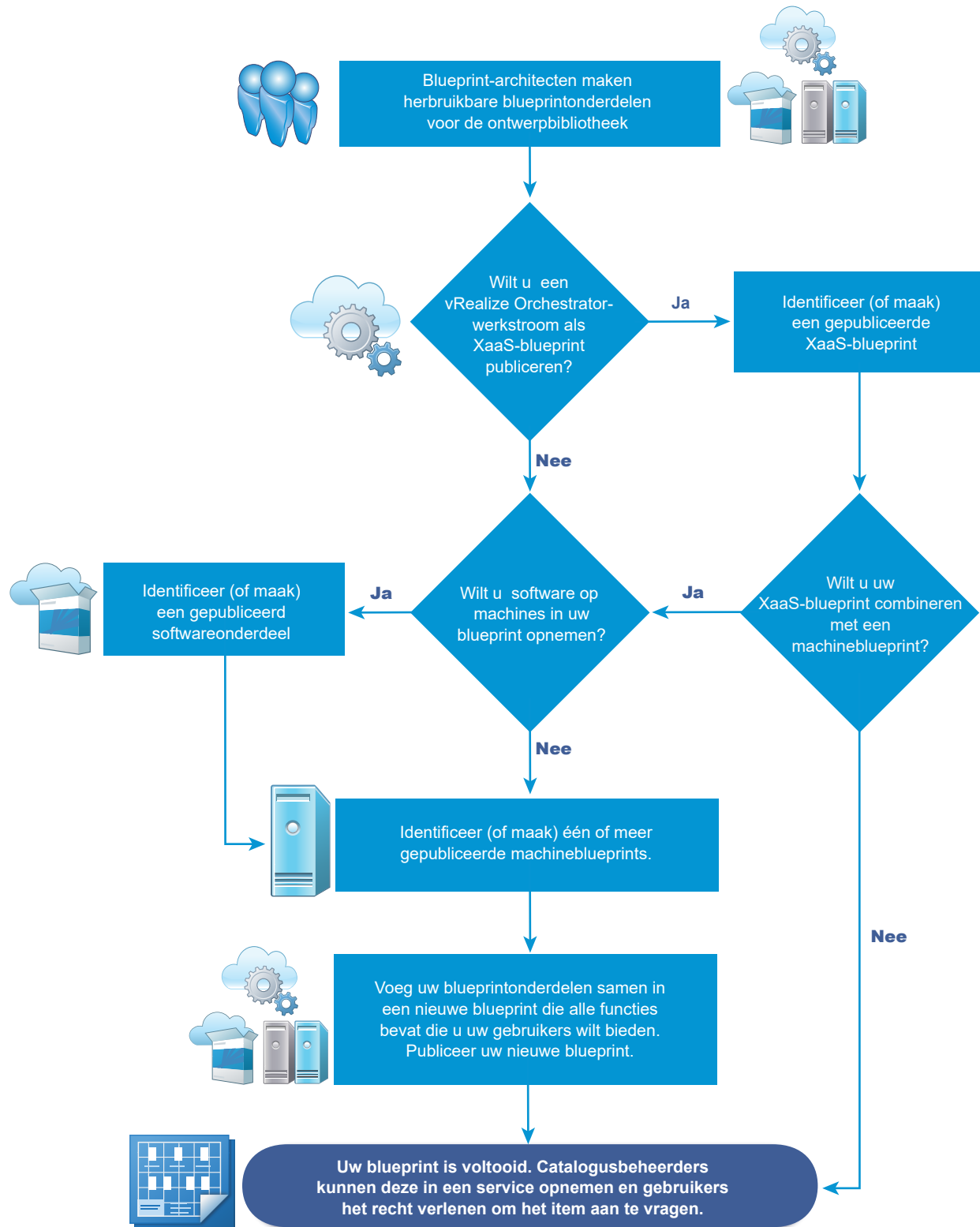
- [Blogbericht: vRealize Automation with Infrastructure Blueprint - Configuring Multi-developer Environment](#)
- Documentatie: [De opgegeven standalone blueprint downloaden en configureren](#)
- [Blogbericht: Lifecycle Manager with GitLab Integration](#)
- [Blogbericht: LifeCycle Manager overview](#)

Samengestelde blueprints samenstellen

U kunt gepubliceerde blueprints en onderdelen van blueprints gebruiken en deze op nieuwe manieren combineren voor het maken van IT-servicepakketten die uitgebreide functionaliteit bieden aan gebruikers.

Als de onderdeelblueprints aangepaste formulieren hebben, worden de aangepaste aanvraagformulieren niet toegepast op de nieuwe blueprint. U moet nieuwe formulieren voor de nieuwe blueprint maken. Zie [Aanpassen van blueprint-aanvraagformulieren](#) voor meer informatie over aangepaste aanvraagformulieren.

Figuur 3-5. Werkstroom voor het samenstellen van samengestelde blueprints



■ Informatie over genest blueprintgedrag

U kunt blueprints hergebruiken door ze als onderdeel te nesten in een andere blueprint. U kunt blueprints nesten voor hergebruik en de regeling van modulariteit bij het inrichten van machines, maar er zijn specifieke regels en overwegingen wanneer u met geneste blueprints werkt.

- **Machine- en Software-componenten gebruiken bij het samenstellen van een blueprint.**

U levert Software-onderdelen door ze boven op ondersteunde machineonderdelen te plaatsen wanneer u blueprints verzamelt.

- **Eigenschapsbindingen maken tussen blueprintonderdelen**

In diverse implementatiescenario's heeft een onderdeel de eigenschapswaarde van een ander onderdeel nodig om te kunnen worden aangepast. U kunt eigenschappen van XaaS, machines, Software en aangepaste eigenschappen binden aan andere eigenschappen in een blueprint.

- **Afhankelijkheden maken en de inrichtingsvolgorde regelen**

Als u meer informatie wilt over een van uw blueprintonderdelen zodat u de inrichting van andere onderdelen kunt voltooien, kunt u een expliciete afhankelijkheid op het ontwerpcanvas tekenen om de inrichting te verdelen zodat het afhankelijke onderdeel niet voortijdig wordt ingericht. Expliciete afhankelijkheden regelen de buildvolgorde van een implementatie en activeren afhankelijke updates tijdens een opschaal- of neerschaalbewerking. Softwareonderdelen moeten in een blueprint worden geordend.

Informatie over genest blueprintgedrag

U kunt blueprints hergebruiken door ze als onderdeel te nesten in een andere blueprint. U kunt blueprints nesten voor hergebruik en de regeling van modulariteit bij het inrichten van machines, maar er zijn specifieke regels en overwegingen wanneer u met geneste blueprints werkt.

Een blueprint die een of meer geneste blueprints bevat, wordt een buitenste blueprint genoemd. Als u een blueprintonderdeel toevoegt aan het ontwerpcanvas terwijl u een andere blueprint maakt of bewerkt, wordt het blueprintonderdeel een geneste blueprint genoemd en wordt de containerblueprint waaraan deze is toegevoegd de buitenste blueprint genoemd.

Als u geneste blueprints gebruikt, moet u rekening houden met voorschriften die niet altijd duidelijk zijn. Het is belangrijk om op de hoogte te zijn van de regels en overwegingen om uw mogelijkheden voor het inrichten van machines zo goed mogelijk te benutten.

Algemene regels en overwegingen voor het nesten van blueprints

- Als een best practice om de complexiteit van blueprints te verminderen, beperkt u blueprints tot maximaal drie diepteniveaus waarbij de blueprint op het bovenste niveau als een van de drie niveaus geldt.
- Als een gebruiker over rechten voor de buitenste blueprint beschikt, beschikt deze gebruiker ook over rechten voor de geneste blueprints.

- U kunt een goedkeuringsbeleid toepassen op een blueprint. Indien goedgekeurd, worden het blueprintcatalogusitem en alle onderdelen ervan, inclusief geneste blueprints, ingericht. U kunt ook verschillende goedkeuringsbeleidsregels toepassen op verschillende onderdelen. Alle goedkeuringsbeleidsregels moeten worden goedgekeurd voordat de aangevraagde blueprint wordt ingericht.
- Wanneer u een gepubliceerde blueprint bewerkt, wijzigt u geen implementaties die al zijn ingericht met behulp van die blueprint. Op het moment van de inrichting bevat de resulterende implementatie de huidige waarden van de blueprint, inclusief de waarden van de geneste blueprints. De enige wijzigingen die u kunt doorgeven aan ingerichte implementaties zijn aanpassingen aan softwareonderdelen, bijvoorbeeld aanpassingen aan update- of verwijderingsscripts.
- De instellingen die u opgeeft in de buitenste blueprint overschrijven de instellingen die worden geconfigureerd in geneste blueprints met de volgende uitzonderingen:
 - U kunt de naam van een geneste blueprint wijzigen, maar u kunt niet de naam van een machineonderdeel of van andere onderdelen in een geneste blueprint wijzigen.
 - U kunt geen aangepaste eigenschappen van een machineonderdeel in een geneste blueprint toevoegen of verwijderen. U kunt deze aangepaste eigenschappen echter wel bewerken. U kunt geen eigenschapsgroepen voor een machineonderdeel in een geneste blueprint toevoegen, bewerken of verwijderen.
- Wijzigingen die u of een andere architect aanbrengt in de instellingen voor geneste blueprints, worden weergegeven in de buitenste blueprints, tenzij u deze instellingen hebt genegeerd in de buitenste blueprint.
- Beperk de maximale leasetijd op de buitenste blueprint tot de laagste maximale leasewaarde van een onderdeelblueprint.

Hoewel de leasetijd die op een geneste blueprint en op de buitenste blueprint wordt opgegeven op elke waarde kan worden ingesteld, moet de maximale leasetijd op de buitenste blueprint worden beperkt tot de laagste maximale leasewaarde van een geneste blueprint. Op die manier kan de toepassingsarchitect een samengestelde blueprint ontwerpen die uniforme en variabele leasewaarden heeft, maar valt binnen de beperkingen zoals geïdentificeerd door de infrastructuurarchitect. Als de maximum leasewaarde die op een geneste blueprint is gedefinieerd, lager is dan de waarde op de buitenste blueprint, mislukt het inrichtingsverzoek.

- Wanneer u in een buitenste blueprint werkt, kunt u de machinebroninstellingen overschrijven die zijn geconfigureerd voor een machineonderdeel in een geneste blueprint.
- Wanneer u in een buitenste blueprint werkt, kunt u een softwareonderdeel naar een machineonderdeel in een geneste blueprint slepen.
- Als u een blueprint opent waarin een machineonderdeel in een geneste blueprint is verwijderd of waarvan de id is gewijzigd, en het machineonderdeel was gekoppeld aan onderdelen in de huidige blueprint, worden de gekoppelde onderdelen verwijderd en verschijnt het volgende of een gelijkaardig bericht:

Een machineonderdeel in een geneste blueprint waarnaar wordt verwezen door onderdelen in de huidige blueprint, is verwijderd of de machineonderdeel-id ervan is gewijzigd. Alle onderdelen in de huidige blueprint die gekoppeld waren aan de ontbrekende of gewijzigde machineonderdeel-id, zijn verwijderd. Klik op Annuleren om de koppelingsgeschiedenis tussen de ontbrekende of gewijzigde machineonderdeel-id in de geneste blueprint en onderdelen in de huidige blueprint te behouden en het probleem in de geneste blueprint op te lossen. Open de geneste blueprint en voeg het ontbrekende machineonderdeel met de originele id opnieuw toe of wijzig de machineonderdeel-id en stel deze terug in op de originele id. Klik op Opslaan om de koppelingsgeschiedenis tussen de ontbrekende of gewijzigde machineonderdeel-id in de geneste blueprint en onderdelen in de huidige blueprint te verwijderen.

- Wanneer u een blueprint publiceert, worden gegevens voor software-onderdeel behandeld als een momentopname. Als u later wijzigingen in de eigenschappen van het softwareonderdeel aanbrengt, worden alleen nieuwe eigenschappen herkend door de blueprint waarin het software-onderdeel bestaat. Updates voor eigenschappen die in het softwareonderdeel bestonden op het moment dat u de blueprint hebt gepubliceerd, worden niet bijgewerkt in de blueprint. Alleen de eigenschappen die zijn toegevoegd nadat u de blueprint hebt gepubliceerd, worden overgenomen door de blueprint. Echter, kunt u wijzigingen in de instanties van het software-onderdeel in blueprints waarin het software-onderdeel zich bevindt als u dat specifieke blueprint wilt wijzigen.

Netwerk- en beveiligingsregels en overwegingen voor het nesten van blueprints

- Netwerk- en beveiligingsonderdelen in buitenste blueprints kunnen worden gekoppeld aan machines die in geneste blueprints zijn gedefinieerd.
- Netwerk-, beveiligings- en load balancer-onderdelen voor NSX en hun instellingen worden niet ondersteund in geneste blueprints.
- Als app-isolatie wordt toegepast in de buitenste blueprint, overschrijft dit de instellingen voor app-isolatie die in geneste blueprints zijn opgegeven.
- Transportzone-instellingen die in de buitenste blueprint zijn gedefinieerd, overschrijven de transportzone-instellingen die in geneste blueprints zijn opgegeven.
- Wanneer u in een buitenste blueprint werkt, kunt u load balancer-instellingen configureren ten opzichte van netwerkonderdeelininstellingen en machineonderdeelininstellingen die zijn geconfigureerd in een interne of geneste blueprint.
- Voor een geneste blueprint die een netwerkonderdeel NAT op aanvraag bevat, zijn de IP-bereiken die in dit netwerkonderdeel NAT op aanvraag zijn opgegeven, niet bewerkbaar in de buitenste blueprint.
- De buitenste blueprint mag geen binnenste blueprint bevatten die instellingen voor netwerken op aanvraag of instellingen voor load balancers op aanvraag bevat. Het gebruik van een binnenste blueprint die een onderdeel voor NSX-netwerken op aanvraag of een onderdeel voor NSX-load balancers bevat, wordt niet ondersteund.

- Voor een geneste blueprint die NSX-netwerkonderdelen of -beveiligingsonderdelen bevat, kunt u de gegevens van het netwerkprofiel of het beveiligingsprofiel die in de geneste blueprint zijn opgegeven, niet wijzigen. U kunt deze instellingen echter wel hergebruiken voor andere vSphere-machineonderdelen die u aan de buitenste blueprint toevoegt.
- Om ervoor te zorgen dat NSX-netwerkonderdelen en -beveiligingsonderdelen in geneste blueprints een unieke naam krijgen in een samengestelde blueprint, voegt vRealize Automation de geneste blueprint-id als een voorvoegsel toe aan de namen van de netwerk- en beveiligingsonderdelen die nog niet uniek zijn. Als u bijvoorbeeld een blueprint met de id-naam xbp_1 aan een buitenste blueprint toevoegt, en beide blueprints bevatten een onderdeel beveiligingsgroep op aanvraag genaamd OD_Security_Group_1, dan wordt de naam van het onderdeel in de geneste blueprint gewijzigd in xbp_1_OD_Security_Group_1 in het ontwerpcanvas van de blueprint. Er worden geen voorvoegsels toegevoegd aan de namen van de netwerk- en beveiligingsonderdelen in de buitenste blueprint.
- De onderdeelinstellingen worden mogelijk gewijzigd, afhankelijk van de blueprint waarop het onderdeel zich bevindt. Als u bijvoorbeeld beveiligingsgroepen, beveiligingstags of netwerken op aanvraag hebt opgenomen op zowel de binnenste als buitenste blueprint, worden de instellingen van de binnenste blueprint overschreven door die van de buitenste blueprint. Netwerk- en beveiligingsonderdelen worden alleen ondersteund op het niveau van de buitenste blueprint, tenzij het gaat om bestaande netwerken die werken op het niveau van de binnenste blueprint. U kunt problemen vermijden door alle beveiligingsgroepen, beveiligingstags en netwerken op aanvraag alleen toe te voegen aan de buitenste blueprint.

Overwegingen voor softwareonderdelen voor het nesten van blueprints

Voor schaalbare blueprints doet u er verstandig aan om enkellaagse blueprints te maken die geen andere blueprints hergebruiken. Normaal gesproken worden updateprocedures tijdens schaalbewerking geactiveerd door impliciete afhankelijkheden, zoals afhankelijkheden die u maakt wanneer u een software-eigenschap aan een machine-eigenschap bindt. Impliciete afhankelijkheden in een geneste blueprint activeren echter niet altijd updateprocedures. Als u geneste blueprints in een schaalbare blueprint moet gebruiken, kunt u handmatig afhankelijkheden tekenen tussen onderdelen in uw geneste blueprint om expliciete afhankelijkheden te maken die altijd een update activeren.

Machine- en Software-componenten gebruiken bij het samenstellen van een blueprint.

U levert Software-onderdelen door ze boven op ondersteunde machineonderdelen te plaatsen wanneer u blueprints verzamelt.

Om Software-onderdelen te ondersteunen moet de machineblueprint die u selecteert een machineonderdeel bevatten dat gebaseerd is op een sjabloon, een momentopname of een installatiekopie van een Amazon-machine waarin zich de gastagent en de Software-bootstrapagent bevinden, en moet deze een ondersteunde inrichtingsmethode gebruiken.

Omdat de Software-agents geen Internet Protocol versie 6 (IPv6) ondersteunen, dient u de IPv4-instellingen te gebruiken.

Opmerking Software-onderdelen moeten een geordende afhankelijkheid hebben in de blueprint. Niet-geordende softwareonderdelen kunnen ertoe leiden dat de inrichting van de blueprint mislukt. Als er geen werkelijke geordende afhankelijkheid voor de softwareonderdelen is, kunt u voldoen aan de volgordevereiste voor de blueprint door een 'valse' afhankelijkheid tussen de softwareonderdelen toe te voegen.

Als u blueprints ontwerpt die schaalbaar moeten zijn, doet u er verstandig aan om enkellaagse blueprints te maken die geen andere blueprints hergebruiken. Gewoonlijk worden de bijwerkingsprocessen die tijdens schalingsbewerkingen worden gebruikt, geactiveerd door impliciete afhankelijkheden zoals eigenschapsbindingen. Impliciete afhankelijkheden in een geneste blueprint activeren echter niet altijd updateprocedures.

Hoewel IaaS-architecten, toepassingsarchitecten en softwarearchitecten allemaal blueprints kunnen verzamelen, kunnen alleen IaaS-architecten machineonderdelen configureren. Als u geen IaaS-architect bent, kunt u niet uw eigen machineonderdelen configureren, maar u kunt wel de machineblueprints hergebruiken die uw IaaS-architect heeft gemaakt en gepubliceerd.

Om softwareonderdelen met succes aan het ontwerpcanvas toe te voegen, moet u ook toegang als bedrijfsgroepslid, bedrijfsgroepbeheerder of tenantbeheerder tot de doelcatalogus hebben.

Als u geneste blueprints in een schaalbare blueprint moet gebruiken, kunt u handmatig afhankelijkheden tekenen tussen onderdelen in uw geneste blueprint om expliciete afhankelijkheden te maken die altijd een update activeren.

Opmerking Wanneer u een blueprint publiceert, worden gegevens voor software-onderdeel behandeld als een momentopname. Als u later wijzigingen in de eigenschappen van het softwareonderdeel aanbrengt, worden alleen nieuwe eigenschappen herkend door de blueprint waarin het software-onderdeel bestaat. Updates voor eigenschappen die in het softwareonderdeel bestonden op het moment dat u de blueprint hebt gepubliceerd, worden niet bijgewerkt in de blueprint. Alleen de eigenschappen die zijn toegevoegd nadat u de blueprint hebt gepubliceerd, worden overgenomen door de blueprint. Echter, kunt u wijzigingen in de instanties van het software-onderdeel in blueprints waarin het software-onderdeel zich bevindt als u dat specifieke blueprint wilt wijzigen.

Tabel 3-64. Inrichtingsmethoden die Software ondersteunen

Machinetype	Inrichtingsmethode
vSphere	Klonen
vSphere	Gekoppelde kloon
vCloud Director	Klonen
vCloud Air	Klonen
Amazon Web Services	Installatiekopie van Amazon-machine

Eigenschapsbindingen maken tussen blueprintonderdelen

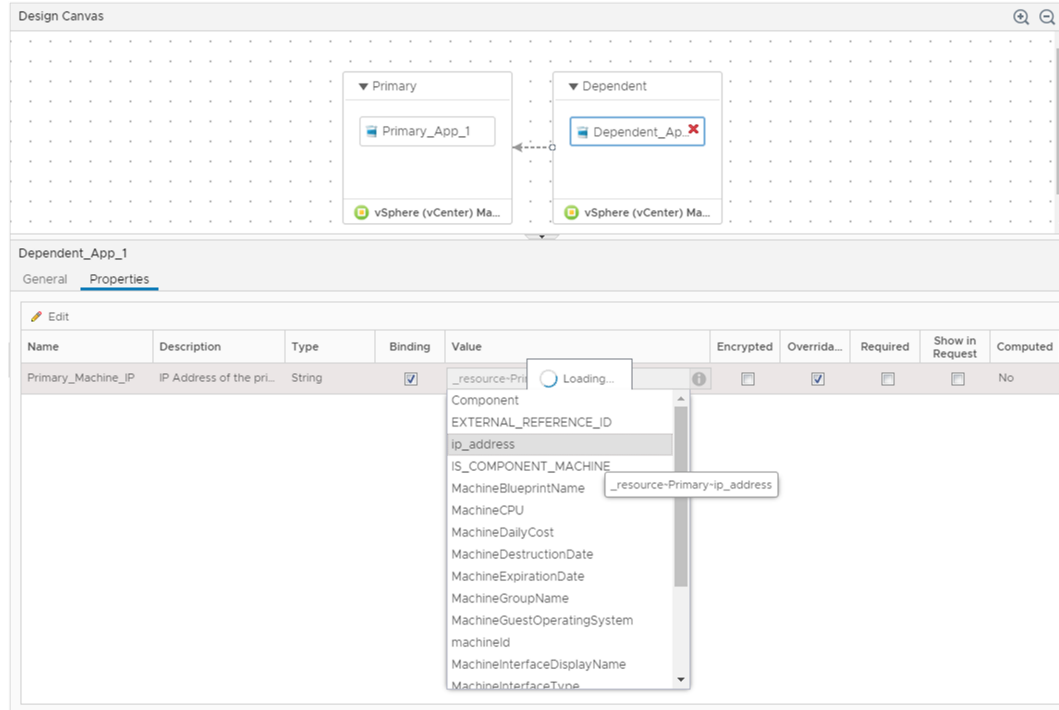
In diverse implementatiescenario's heeft een onderdeel de eigenschapswaarde van een ander onderdeel nodig om te kunnen worden aangepast. U kunt eigenschappen van XaaS, machines, Software en aangepaste eigenschappen binden aan andere eigenschappen in een blueprint.

Uw softwarearchitect kan bijvoorbeeld eigenschapsdefinities wijzigen in de levenscyclusscripts van een WAR-onderdeel. Voor een WAR-onderdeel kan de installatielocatie van het Apache Tomcat-serveronderdeel vereist zijn en dus configureert uw softwarearchitect het WAR-onderdeel zodanig dat de eigenschapswaarde `server_home` wordt ingesteld op de eigenschapswaarde `install_path` van de Apache Tomcat-server. Als de architect die de blueprint samenstelt, moet u de eigenschap `server_home` binden aan de eigenschap `install_path` voor de Apache Tomcat-server, zodat het Software-onderdeel kan worden ingericht.

U stelt eigenschapsbindingen in wanneer u onderdelen in een blueprint configureert. Op de pagina Blueprint sleept u het onderdeel naar het canvas en klikt u op het tabblad

Eigenschappen. Als u een eigenschap wilt binden aan een andere eigenschap in een blueprint, schakelt u het selectievakje **Binden** in. U kunt *onderdeelnaam~eigenschapsnaam* invoeren in het tekstvak voor de waarde of u kunt de pijl naar beneden gebruiken om een lijst met beschikbare bindopties te genereren. U gebruikt het tildeteken ~ als scheidingsteken tussen onderdelen en eigenschappen. Als u bijvoorbeeld de eigenschap `dp_port` wilt binden, kunt u in het MySQL-softwareonderdeel de waarde `mysql-db_port` typen. Als u een binding wilt maken met eigenschappen die tijdens het inrichten worden geconfigureerd, zoals het IP-adres van een machine of de hostnaam van een Software-onderdeel, voert u *_resource~onderdeelnaam~eigenschapsnaam* in. Als u bijvoorbeeld een binding wilt maken met de reserveringsnaam van een machine, kunt u *_resource~vSphere_Machine_1~MachineReservationName* invoeren.

Figuur 3-6. Een software-eigenschap binden aan het IP-adres van een machine



Afhankelijkheden maken en de inrichtingsvolgorde regelen

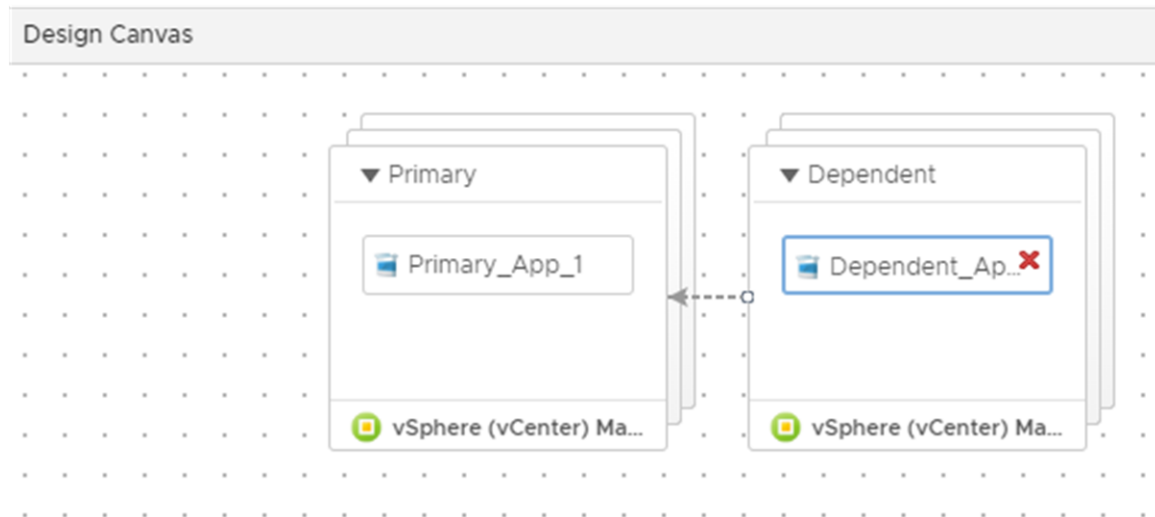
Als u meer informatie wilt over een van uw blueprintonderdelen zodat u de inrichting van andere onderdelen kunt voltooien, kunt u een expliciete afhankelijkheid op het ontwerpcanvas tekenen om de inrichting te verdelen zodat het afhankelijke onderdeel niet voortijdig wordt ingericht. Expliciete afhankelijkheden regelen de buildvolgorde van een implementatie en activeren afhankelijke updates tijdens een opschaal- of neerschaalbewerking. Softwareonderdelen moeten in een blueprint worden geordend.

Wanneer u blueprints met meerdere machines en toepassingen ontwerpt, hebt u wellicht eigenschappen van de ene machine nodig om de installatie van een toepassing op een andere machine te voltooien. Als u bijvoorbeeld een webserver bouwt, hebt u wellicht de hostnaam van de databaseserver nodig voordat u de toepassing kunt installeren en databasetabellen kunt concretiseren. Als u een expliciete afhankelijkheid koppelt, begint uw databaseserver met de inrichting wanneer uw webserver klaar is met de inrichting.

Opmerking Software-onderdelen moeten een geordende afhankelijkheid hebben in de blueprint. Niet-geordende softwareonderdelen kunnen ertoe leiden dat de inrichting van de blueprint mislukt. Als er geen werkelijke geordende afhankelijkheid voor de softwareonderdelen is, kunt u voldoen aan de volgordevereiste voor de blueprint door een 'valse' afhankelijkheid tussen de softwareonderdelen toe te voegen.

Als u een afhankelijkheid wilt toewijzen op uw ontwerpcanvas, tekent u een lijn van het onderdeel van de afhankelijkheid naar het onderdeel waarvan u afhankelijk bent. Wanneer u klaar bent, bevat het onderdeel dat u als tweede wilt bouwen een pijl die naar het onderdeel is gericht dat u als eerste wilt bouwen. In de afbeelding De bouwvolgorde regelen door afhankelijkheden toe te wijzen wordt de afhankelijke machine pas ingericht wanneer de primaire machine is gebouwd. Een andere optie is beide machines zo configureren dat ze tegelijk worden ingericht, maar wel met een afhankelijkheid tussen de softwareonderdelen.

Figuur 3-7. De bouwvolgorde regelen door afhankelijkheden toe te wijzen



Als u blueprints ontwerpt die schaalbaar moeten zijn, doet u er verstandig aan om enkellaagse blueprints te maken die geen andere blueprints hergebruiken. Normaal gesproken worden updateprocedures tijdens schaalbewerking geactiveerd door impliciete afhankelijkheden, zoals afhankelijkheden die u maakt wanneer u een software-eigenschap aan een machine-eigenschap bindt. Impliciete afhankelijkheden in een geneste blueprint activeren echter niet altijd updateprocedures. Als u geneste blueprints in een schaalbare blueprint moet gebruiken, kunt u handmatig afhankelijkheden tekenen tussen onderdelen in uw geneste blueprint om expliciete afhankelijkheden te maken die altijd een update activeren.

Aanpassen van blueprint-aanvraagformulieren

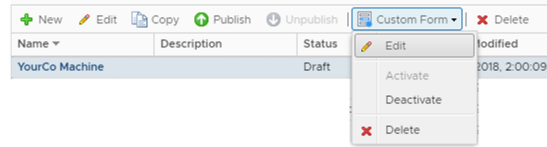
Elke blueprint die u maakt en publiceert geeft een formulier weer wanneer uw gebruikers de blueprint in de catalogus aanvragen. U kunt het standaardformulier gebruiken of u kunt de blueprint-aanvraagformulieren aanpassen wanneer u een blueprint maakt of bewerkt. U kunt een formulier aanpassen wanneer de informatie die wordt weergegeven of vereist is op het standaardformulier niet overeenkomt met wat u aan uw gebruikers wilt presenteren.

Aanvraagformulieren aanpassen

U heeft toegang tot het formulierontwerpprogramma voor het aangepaste aanvraagformulier via het blueprint-gegevensraster of vanaf het blueprintcanvas.

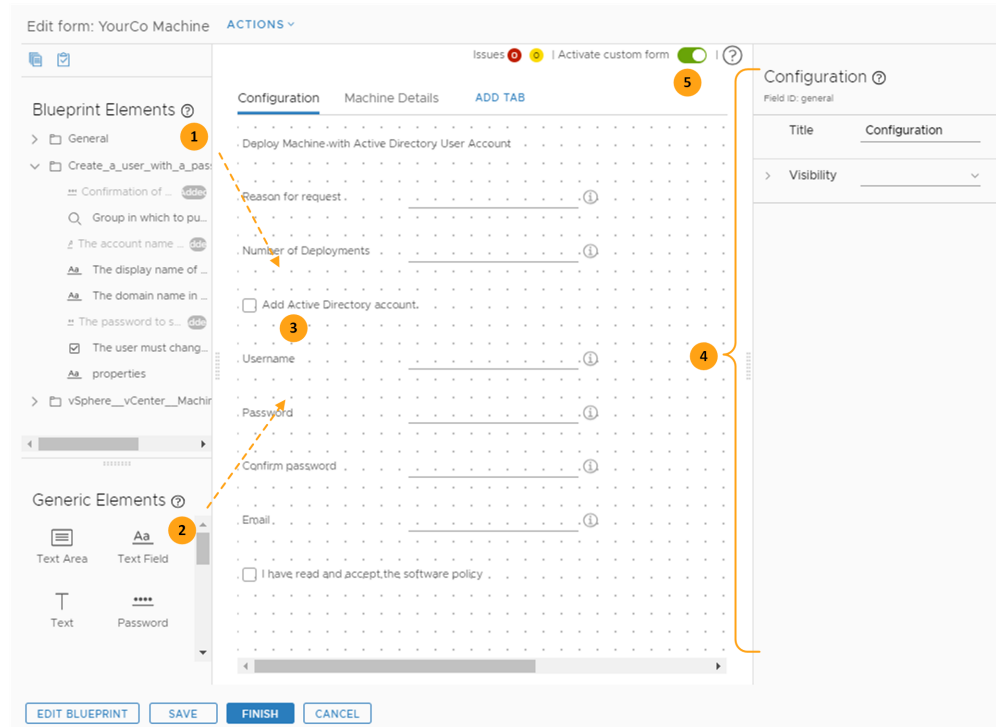
Blueprints

Create and manage blueprints. Publish a blueprint to allow architects to reuse your blueprint, administrators to entitle users to request your blueprint from the catalog.



Ontwerpprogramma voor aangepaste aanvraagformulieren

Met het formulierontwerpprogramma kunt u uw aangepast formulier maken.



Een aangepast formulier maken:

- 1 Sleep elementen (1 en 2) naar het ontwerpcanvas (3).
- 2 Configureer elk element met behulp van het deelvenster Eigenschappen (4).
- 3 Activeer het formulier (5).

Tenzij een eigenschap is geconfigureerd om overschrijven te verbieden, bevat de lijst met blueprintelementen aangepaste eigenschappen. Als de optie overschrijfbaar voor de eigenschap is ingesteld op nee, kan het veld niet worden aangepast.

Validatie en beperkingen

Het aangepaste formulierontwerpprogramma ondersteunt gegevensvalidatie door beperkingen toe te voegen aan een veld of met behulp van een externe validatie-bron. Zie voor beperkingsopties die worden toegepast wanneer u een formulier wilt maken, [Aangepaste veldeigenschappen voor formulierontwerper](#).

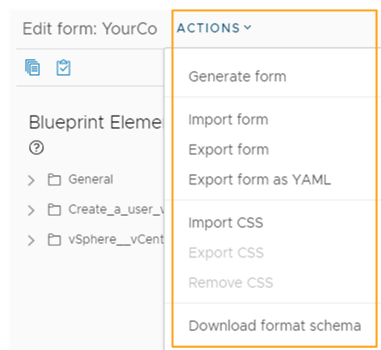
- Zie [Een aangepast aanvraagformulier met Active Directory-opties maken](#) voor een voorbeeld van een beperking.
- Zie voor de externe validatie [Externe validatie gebruiken in het ontwerpprogramma voor aangepaste formulieren](#).

Wanneer u validatie en afhankelijkheden in formulieren toevoegt, moet de aanvragende gebruiker opgeven of het systeem de velden moet valideren om te vermijden dat de afhankelijke velden niet worden weergegeven op het formulier.

Als u bijvoorbeeld velden hebt op het eerste tabblad waarvan daaropvolgende velden afhankelijk zijn, worden de afhankelijke velden mogelijk niet weergegeven op de daaropvolgende tabbladen totdat de gewenste waarde wordt opgegeven op de voorgaande tabbladen.

Acties voor aangepaste aanvraagformulieren

U kunt de actiemenu-items gebruiken om formulieren vooraf in te vullen en formulieren te delen met andere systemen.



Tabel 3-65. Actiemenu-items voor aangepaste aanvraagformulieren

Actiemenu-item	Beschrijving
Formulier genereren	<p>Voegt alle velden toe die geassocieerd worden met elk blueprintonderdeel van het formulierontwerpprogramma. Elk onderdeel wordt toegevoegd aan een tabblad. Als u dit menu-item gebruikt nadat u een formulier hebt gemaakt of gewijzigd, wordt uw huidige formulier overschreven door het gegenereerde formulier.</p> <p>Als u dit menu-item gebruikt, kunt u velden verbergen of verwijderen die u niet wilt laten zien aan uw gebruikers in de catalogus. Als u het formulier niet genereert, kunt u nog steeds tekstvelden toevoegen en configureren die u uw gebruikers wilt laten zien.</p>
Formulier importeren	<p>Importeert een aangepast formulier JSON- of YAML-bestand.</p>
Formulier exporteren	<p>Hiermee kunt u uw huidige aangepaste formulier als een JSON-bestand exporteren.</p> <p>Exporteer het bestand wanneer u een deel ervan wilt gebruiken dat overeenkomt met een onderdeel dat u in een andere blueprint wilt gebruiken.</p>
Formulier exporteren als YAML	<p>Hiermee exporteert u het huidige aangepaste formulier als YAML.</p> <p>Wanneer u een aangepast formulier van één vRealize Automation-instantie naar een andere wilt verplaatsen, kunt u het bestand exporteren als YAML. Bijvoorbeeld: van uw testomgeving naar uw productieomgeving. Als u liever het formulier als YAML wilt bewerken, kunt u het formulier exporteren, bewerken en het vervolgens weer in de blueprint importeren.</p>

Tabel 3-65. Actiemenu-items voor aangepaste aanvraagformulieren (vervolg)

Actiemenu-item	Beschrijving
CSS importeren	<p>Hiermee importeert u een CSS-bestand dat het catalogusaanvraagformulier verbetert.</p> <p>Het bestand lijkt mogelijk op het volgende voorbeeld. In dit voorbeeld wordt de tekengrootte vergroot en wordt de tekst vet gemaakt. Het veld waarnaar wordt verwezen is de implementatiemachine met Active Directory-gebruikersaccount-tekstveld dat wordt weergegeven in de afbeelding in de sectie Ontwerpprogramma voor aangepaste aanvraagformulieren hierboven.</p> <pre>#<field-ID> .grid-item { font-size: 16px; font-weight: bold; width: 600px; }</pre> <p>In dit voorbeeld is <field-ID> de ID voor het veld in het canvas. Om de waarde op te zoeken, selecteert u het veld in het canvas. De waarde bevindt zich in het rechterdeelvenster onder de naam. In de afbeelding hierboven, is de waarde text_d947bc97.</p> <p>Om het bestand te importeren. Opslaan als <filename>.css.</p>
CSS exporteren	Hiermee kunt u uw geïmporteerde CSS exporteren.
CSS verwijderen	<p>Verwijdert uw aangepaste CSS.</p> <p>De verwijderde CSS kan niet worden hersteld.</p>
Indelingsschema downloaden	<p>Downloadt een JSON-bestand met de structuur en de beschrijving van de structuur en een beschrijving van de bedieningselementen en statussen in een aangepast formulier.</p> <p>U kunt dit schema gebruiken om een formulier te maken of een bestaand formulier te wijzigen. U kunt het gewijzigde JSON-bestand importeren als het aangepaste formulier.</p>

Een aangepast aanvraagformulier met Active Directory-opties maken

U maakt een aangepast formulier wanneer het standaardformulier te veel of te weinig informatie verstrekt aan de aanvrager. U kunt meer velden aan het formulier toevoegen, u kunt velden op een formulier verbergen of u kunt velden vooraf invullen en ze weergeven of verbergen.

Dit scenario is gebaseerd op een blueprint die een virtual machine van vSphere bevat en een XaaS-blueprint waarmee een Active Directory-beheerdersaccount geconfigureerd op de virtual machine wordt geconfigureerd. De XaaS-blueprint is gebaseerd op de werkstroom Een gebruiker met een wachtwoord in een groep maken.

Uw doel in dit scenario is:

- De gebruiker de optie geven om het beheerderswachtwoord te configureren.
- De details van de machine vooraf configureren zodat zowel de CPU- als geheugenwaarden worden weergegeven in GB.

Hoe haalt u voordeel uit dit scenario? Dit scenario omvat voorbeelden van de volgende formulieraanpassingen:

- Specifieke velden toevoegen aan een leeg formulier.
- Het selectievakje Weergeven/verbergen configureren.
- Velden verbergen totdat de aanvrager een selectievakje inschakelt.
- Validatie toevoegen aan velden.
- Een geheugenveld in GB weergeven zelfs als het blueprintveld wordt berekend in MB.
- Reguliere expressies gebruiken.

Voorwaarden

- Meld u aan bij vRealize Automation als **toepassingsarchitect**, **softwarearchitect** of **infrastructuurarchitect**.
- Maak een YourCo-machine en een gebruikersblueprint die een vSphere-blueprint en een XaaS-blueprint bevat om een Active Directory-gebruikersaccount met een wachtwoord in een groep te maken. Zie [Een XaaS-blueprint maken voor het maken van een gebruiker](#) voor een voorbeeld.

Procedure

- 1 Selecteer **Ontwerpen > Blueprints**.
- 2 Markeer de rij met de YourCo-machine en een gebruikersblueprint en klik op **Aangepast formulier > Bewerken**.
- 3 Wijzig de naam van het tabblad Algemeen.
 - a Klik op de tab.
 - b Voer **Configuratie** in de eigenschap **Titel** in het betreffende eigenschappenvenster in.

- 4 Voeg op uw nieuwe tabblad Configuratie de volgende velden toe en configureer ze met de opgegeven waarden.

The screenshot displays the 'Edit form: YourCo Machine' interface in vRealize Automation. The 'ACTIONS' menu is open, showing 'Configuration' and 'Machine Details' tabs. The 'Configuration' tab is active, displaying a form with various fields and a 'Visibility' dropdown. The 'Blueprint Elements' panel on the left shows a tree structure with 'General' and 'vSphere_vCenter_Machine' elements. The 'Generic Elements' panel at the bottom left shows 'Text Area', 'Text Field', 'Text', and 'Password' options. The 'Configuration' tab contains the following fields:

- Title:** Configuration
- Visibility:** (dropdown menu)
- Deploy Machine with Active Directory User Account:** (checkbox)
- Reason for request:** (text field)
- Number of Deployments:** (text field)
- Add Active Directory account:** (checkbox)
- Username:** (text field)
- Password:** (password field)
- Confirm password:** (password field)
- Email:** (text field)
- I have read and accept the software policy:** (checkbox)

At the bottom of the interface, there are buttons for 'EDIT BLUEPRINT', 'SAVE', 'FINISH', and 'CANCEL'.

Gebruik de opgegeven waarden voor Vormgeving, Waarden en Beperkingen.

Los eventuele fouten op tijdens het samenstellen van het formulier.

Veld in schermabeelding	Bron van blueprintelement	Vormgeving	Waarden	Beperkingen
Machine met Active Directory-gebruikersaccount implementeren	Generieke elementen > Tekst	Label en type <ul style="list-style-type: none"> ■ Weergavetype = Tekst Zichtbaarheid <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Zichtbaar = Ja 	Standaardwaarde <ul style="list-style-type: none"> ■ Standaardwaarde = Machine met Active Directory-gebruikersaccount implementeren ■ Waardebron = Constante 	
Reden voor aanvraag	Blueprintelementen > vSphere_vCenter_Machine > Beschrijving	Label en type <ul style="list-style-type: none"> ■ Label = Reden voor aanvraag ■ Weergavetype = Tekstveld Zichtbaarheid <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Zichtbaar = Ja Alleen-lezen <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Alleen-lezen = Nee Aangepaste Help <ul style="list-style-type: none"> ■ Wegwijzer-Help = Geef de reden voor uw aanvraag op. 		Vereist <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Vereist = Ja
Aantal implementaties	Blueprintelementen > Algemeen > Aantal implementaties	Label en type <ul style="list-style-type: none"> ■ Label = Aantal implementaties ■ Weergavetype = Geheel getal Zichtbaarheid <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Zichtbaar = Ja Alleen-lezen <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Alleen-lezen = Nee Aangepaste Help <ul style="list-style-type: none"> ■ Wegwijzer-Help = Selecteer het aantal instanties van de blueprint dat moet worden geïmplementeerd. 	Standaardwaarde <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Standaardwaarde = 1 	Vereist <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Vereist = Ja Minimumwaarde <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Minimumwaarde = 1

Veld in schermabeelding	Bron van blueprintelement	Vormgeving	Waarden	Beperkingen
Selectievakje Active Directory-account toevoegen	Generieke elementen > Selectievakje	Label en type <ul style="list-style-type: none"> ■ Label = Active Directory-account toevoegen. ■ Weergavetype = Selectievakje Zichtbaarheid <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Zichtbaar = Ja 		
Gebruikersnaam	Blueprintelementen > Een gebruiker met een wachtwoord in een groep maken > De accountnaam voor de gebruiker	Label en type <ul style="list-style-type: none"> ■ Label = Gebruikersnaam ■ Weergavetype = Tekstveld Zichtbaarheid <p>Opmerking Deze zichtbaarheidseigenschap, die op dezelfde manier wordt geconfigureerd in de volgende velden, verbergt het veld tenzij het selectievakje Active Directory-account toevoegen is ingeschakeld.</p> <ul style="list-style-type: none"> ■ Waardebron = Voorwaardelijke waarde ■ Expressie = Waarde instellen = Ja <p>Als Active Directory-account toevoegen gelijk is aan Ja</p> Aangepaste Help <ul style="list-style-type: none"> ■ Wegwijzer-Help = Geef de naam van de beheerder op. 	Standaardwaarde <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Standaardwaarde = beheerder 	Vereist <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Vereist = Ja Reguliere expressie <p>Opmerking De reguliere expressies moeten de syntaxis voor JavaScript volgen.</p> <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Reguliere expressie = "[a-z]*" ■ Foutmelding voor validatie = Uw gebruikersnaam mag geen speciale tekens of cijfers bevatten.

Veld in schermabeelding	Bron van blueprintelement	Vormgeving	Waarden	Beperkingen
Wachtwoord	Blueprintelementen > Een gebruiker met een wachtwoord in een groep maken > Het in te stellen wachtwoord het nieuw gemaakte account	<p>Label en type</p> <ul style="list-style-type: none"> ■ Label = Wachtwoord ■ Weergavetype = Wachtwoord <p>Zichtbaarheid</p> <ul style="list-style-type: none"> ■ Waardebron = Voorwaardelijke waarde ■ Expressie = <p>Waarde instellen = Ja</p> <p>Als Active Directory-account toevoegen gelijk is aan Ja</p> <p>Aangepaste Help</p> <ul style="list-style-type: none"> ■ Wegwijzer-Help = Geef het wachtwoord voor uw beheerdersaccount op. 		<p>Vereist</p> <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Vereist = Ja <p>Reguliere expressie</p> <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Reguliere expressie = <code>"^(? = .*[A-Z])(? = .*[0-9])(? = .*[a-z]).{8,}\$"</code> ■ Bericht = Uw beheerderswachtwoord moet ten minste acht tekens bevatten en kan alfanumerieke en speciale tekens bevatten.
Wachtwoord bevestigen	Blueprintelementen > Een gebruiker met een wachtwoord in een groep maken > Bevestiging van het wachtwoord	<p>Label en type</p> <ul style="list-style-type: none"> ■ Label = Wachtwoord bevestigen <p>Weergavetype = Wachtwoord</p> <p>Zichtbaarheid</p> <ul style="list-style-type: none"> ■ Waardebron = Voorwaardelijke waarde ■ Expressie = <p>Waarde instellen op Ja</p> <p>Als Active Directory-account toevoegen gelijk is aan Ja</p> <p>Aangepaste Help</p> <ul style="list-style-type: none"> ■ Wegwijzer-Help = Geef het wachtwoord voor uw beheerdersaccount opnieuw op. 		<p>Vereist</p> <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Vereist = Ja <p>Veldovereenkomst</p> <ul style="list-style-type: none"> ■ Veldovereenkomst = Wachtwoord

Veld in schermabeelding	Bron van blueprintelement	Vormgeving	Waarden	Beperkingen
E-mail	Generieke elementen > Tekstveld	<p>Label en type</p> <ul style="list-style-type: none"> Label = E-mail Weergavetype = Tekstveld <p>Zichtbaarheid</p> <ul style="list-style-type: none"> Waardebron = Voorwaardelijke waarde Expressie = <p>Waarde instellen = Ja</p> <p>Als Active Directory-account toevoegen gelijk is aan Ja</p> <p>Aangepaste Help</p> <ul style="list-style-type: none"> Wegwijzer-Help = Geef het e-mailadres van de beheerder op. 	<p>Standaardwaarde</p> <ul style="list-style-type: none"> Waardebron = Berekende waarde Operator = Samenvoegen Waarde toevoegen = Veld. Gebruikersnaam selecteren Waarde toevoegen = Constante. @yourco.com invoeren 	<p>Reguliere expressie</p> <ul style="list-style-type: none"> Waardebron = Constante Reguliere expressie = "[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}\$" Foutmelding voor validatie = Geef geldig e-mailadres op.
Selectievakje Ik heb het softwarebeleid gelezen en geaccepteerd.	Generieke elementen > Selectievakje	<p>Label en type</p> <ul style="list-style-type: none"> Elementlabel = Ik heb het softwarebeleid gelezen en geaccepteerd Weergavetype = Selectievakje <p>Zichtbaarheid</p> <ul style="list-style-type: none"> Waardebron = Voorwaardelijke waarde Expressie = <p>Waarde instellen = Ja</p> <p>Als Active Directory-account toevoegen gelijk is aan Ja</p>		

- 5 Klik op **Tabblad toevoegen** en voer **Machinegegevens** in de eigenschap **Titel** aan de rechterkant in.

6 Configureer de volgende velden op het tabblad Machinegegevens.

Gebruik de opgegeven waarden voor Vormgeving, Waarden en Beperkingen.

Veld in schermafbeelding	Bron van blueprintelementen	Vormgeving	Waarden	Beperkingen
Opslag (GB)	Blueprint-elementen > vSphere_vCenter_Machine > Opslag (GB)	Label en type <ul style="list-style-type: none"> Label = Opslag (GB) Weergavetype = Geheel getal Zichtbaarheid <ul style="list-style-type: none"> Waardebron = Constante Zichtbaarheid = Ja Alleen-lezen <ul style="list-style-type: none"> Waardebron = Constante Alleen-lezen = Nee 	Standaardwaarde <ul style="list-style-type: none"> Waardebron = Constante Standaardwaarde = 4 	Minimumwaarde <ul style="list-style-type: none"> Waardebron = Constante Minimumwaarde = 2
Aantal CPU's	Blueprint-elementen > vSphere_vCenter_Machine > CPU's	Label en type <ul style="list-style-type: none"> Label = Aantal CPU's Weergavetype = Geheel getal Zichtbaarheid <ul style="list-style-type: none"> Waardebron = Constante Zichtbaarheid = Ja 	Standaardwaarde <ul style="list-style-type: none"> Waardebron = Constante Standaardwaarde = 1 	Minimumwaarde <ul style="list-style-type: none"> Waardebron = Constante Minimumwaarde = 1

Veld in schermabeelding	Bron van blueprintelementen	Vormgeving	Waarden	Beperkingen
Geheugen (GB)	Generieke elementen > Geheel getal	Label en type <ul style="list-style-type: none"> ■ Label = Geheugen (GB) ■ Weergavetype = Geheel getal Zichtbaarheid <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Zichtbaarheid = Ja 	Standaardwaarde <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Standaardwaarde = 1 	Minimumwaarde <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Minimumwaarde = 1
Geheugen (MB)	Blueprint-elementen > vSphere_vCenter_Machine > Geheugen (MB)	Label en type <ul style="list-style-type: none"> ■ Label = Geheugen (MB) ■ Weergavetype = Geheel getal Zichtbaarheid <ul style="list-style-type: none"> ■ Waardebron = Constante ■ Zichtbaarheid = Nee 	Standaardwaarde <ul style="list-style-type: none"> ■ Waardebron = Berekende waarde ■ Operator = Vermenigvuldigen ■ Waarde toevoegen = Veld. Geheugen (GB) selecteren ■ Waarde toevoegen = Constante. 1024 invoeren 	

- 7 Corrigeer eventuele fouten. U kunt het formulier opslaan, maar u kunt het pas activeren als het formulier geen fouten meer heeft.
- 8 Klik op **Voltooien** om het formulier op te slaan en de formulierontwerper te sluiten.
- 9 Selecteer de blueprint en klik op **Publiceren**.
- 10 Selecteer **Aangepast formulier > Activeren** op de werkbalk van de pagina Blueprints om het aangepaste formulier beschikbaar te maken in de servicecatalogus.

Wat nu te doen

- Maak de blueprint beschikbaar in de servicecatalogus. Zie [De servicecatalogus beheren](#).
- Controleer in de catalogus of het aanvraagformulier gelijk is op het volgende voorbeeld.

Two overlapping screenshots of the vRealize Automation configuration interface. The top screenshot shows the 'Machine Details' tab with fields for Storage (GB) set to 4, Number of CPUs set to 1, and Memory (GB) set to 1. The bottom screenshot shows the 'Configuration' tab with fields for Reason for request, Number of Deployments (set to 1), Username (set to admin), Password, Confirm password, and Email (set to admin@yourco.com). A checkbox 'Add Active Directory account.' is checked. Both screenshots have 'SUBMIT' and 'CANCEL' buttons at the bottom.

Aangepaste veldeigenschappen voor formulierontwerper

De veldeigenschappen bepalen hoe het geselecteerde veld eruitziet en welke standaardwaarden aan de gebruiker worden getoond. En ze bepalen welke regels u wilt toepassen op het veld om ervoor te zorgen dat de gebruiker een geldige vermelding in het catalogusaanvraagformulier in vRealize Automation opgeeft.

U configureert elk veld afzonderlijk. Selecteer het veld en bewerk de eigenschappen van het veld.

Veldweergave

U kunt de weergave-eigenschappen gebruiken om te bepalen of het veld wordt weergegeven op het formulier en welk label en aangepaste help u wilt bieden aan uw gebruikers van de Servicecatalogus.

Sommige blueprints kunnen velden met een vaste waarde bevatten. Als u dit type velden toevoegt aan een aangepast formulier, zijn alleen de weergaveopties beschikbaar en is het veld altijd alleen-lezen.

Tabel 3-66. Opties op het tabblad Weergave

Optie	Beschrijving
Label en type	<p>Geef een label op en selecteer een weergavetype.</p> <p>De beschikbare weergavetypen zijn afhankelijk van het veld. Sommige velden ondersteunen meerdere teksttypen, sommige velden ondersteunen enkele typen en andere velden ondersteunen slechts één type.</p> <p>Mogelijke waarden voor alle typen:</p> <ul style="list-style-type: none"> ■ Keuzelijst met invoervak ■ Decimaal ■ Vervolgkeuzelijst ■ Dubbele lijst ■ Image ■ Geheel getal ■ Koppeling ■ Multi-keuze ■ Kiezer met meerdere waarden ■ Wachtwoord ■ Groep keuzerondjes ■ Text ■ Tekstgebied ■ Tekstvelden <p>De veldtypen Multi-keuze en Dubbele lijst bieden dezelfde functionaliteit, waarbij de dubbele lijst een meer intuïtieve optie vormt wanneer de gebruiker meer dan één item in een lijst kan selecteren.</p> <p>Vervolgkeuzemenu en gegevensraster velden bevatten een Tijdelijke aanduiding-instelling. De ingevoerde waarde wordt weergegeven als een intern label of als instructies in het vervolgkeuzemenu, of als een algemeen label of instructies in het gegevensraster.</p> <p>De waardeselectie- en boomstructuurselectievelden bevatten een instelling voor Referentietype. Het referentietype is het vRealize Orchestrator-resourcetype dat wordt gebruikt om de zoekopdracht voor waardeselectie of boomstructuurselectie te beperken tot de vRealize Orchestrator-serverinventaris die het type ondersteunt. U kunt de zoekopdracht dan verder beperken door een actie te selecteren die het referentietype ondersteunt. Zie voor meer informatie over de twee selectievelden De elementen van het waardeselectieveld of boomstructuurselectieveld gebruiken in het ontwerpprogramma voor aangepaste formulieren.</p>
Zichtbaarheid	<p>Geef een veld weer of verberg het op het aanvraagformulier.</p> <ul style="list-style-type: none"> ■ Constante. Klik op Ja om het veld op het formulier weer te geven. Selecteer Nee om het veld te verbergen.

Tabel 3-66. Opties op het tabblad Weergave (vervolg)

Optie	Beschrijving
	<ul style="list-style-type: none"> ■ Voorwaardelijke waarde Zichtbaarheid wordt bepaald door de eerste expressie die is ingesteld op waar. Een veld is bijvoorbeeld zichtbaar indien een selectievakje is ingeschakeld op een formulier. ■ Externe bron Zichtbaarheid wordt bepaald door de resultaten van de geselecteerde vRealize Orchestrator-actie.
Alleen-lezen	<p>Voorkomt dat gebruikers de waarden in het veld wijzigen.</p> <ul style="list-style-type: none"> ■ Constante. Klik op Ja om de waarde weer te geven, maar wijzigingen te voorkomen. Selecteer Nee om wijzigingen toe te staan. ■ Voorwaardelijke waarde Status wordt bepaald door de eerste expressie die is ingesteld op waar. Een veld is bijvoorbeeld alleen-lezen indien de waarde in een opslagveld groter dan 2 GB is. ■ Externe bron Status wordt bepaald door de resultaten van de geselecteerde vRealize Orchestrator-actie.
Rijen per pagina	<p>Alleen voor gegevensraster-elementen.</p> <p>Voer het aantal rijen in.</p>
Aangepaste help	<p>Geef informatie over het veld aan uw gebruikers op. Deze informatie wordt weergegeven in wegwijzerhelp voor het veld.</p> <p>U kunt eenvoudige tekst of HTML, inclusief href-koppelingen gebruiken. Bijvoorbeeld, <code>vRealize Automation documentation</code>.</p>

Veldwaarden

U gebruikt de waardeneigenschappen om standaardwaarden op te geven.

Tabel 3-67. Opties op het tabblad Waarden

Optie	Beschrijving
Kolommen	<p>Alleen voor het gegevensrasterelement.</p> <p>Geef het label, de ID en het waardetype voor elke kolom in de tabel op.</p> <p>De standaardwaarde voor het gegevensraster moet de koptekstgegevens bevatten die overeenkomen met de gedefinieerde kolommen. Als u bijvoorbeeld de user_name-ID voor een kolom en de user_role-ID voor een andere hebt, dan is de eerste rij user_name,user_role. Zie voor configuratievoorbeelden, Het data grid-element gebruiken in het ontwerpprogramma voor aangepaste formulieren.</p>
Standaardwaarde	<p>Vult het veld vooraf in met een standaardwaarde op basis van de bronwaarde.</p> <p>Voor veel van de eigenschappen, kunt u verschillende bronwaardeopties selecteren. Niet alle bronopties zijn beschikbaar voor alle veldtypen of eigenschappen. Mogelijke bronwaarden zijn afhankelijk van het veld.</p> <ul style="list-style-type: none"> ■ Constante. De ingevoerde tekenreeks. De waarde wordt niet gewijzigd. Afhankelijk van de eigenschap, kan de waarde een tekenreeks zijn, een geheel getal, een reguliere expressie of geselecteerd worden op basis van een beperkte lijst, zoals bijvoorbeeld Ja of Nee. <p>U kunt bijvoorbeeld 1 als een standaardwaarde met geheel getal opgeven, Nee selecteren voor de alleen-lezen eigenschap of de reguliere expressie opgeven om veldinvoer te valideren.</p> <ul style="list-style-type: none"> ■ Voorwaardelijke waarde De waarde is gebaseerd op een of meer voorwaarden. De voorwaarden worden verwerkt in de weergegeven volgorde. Als aan meer dan één voorwaarde wordt voldaan, bepaalt de laatste voorwaarde het gedrag van het veld voor die eigenschap. U kunt bijvoorbeeld een voorwaarde die bepaalt of een veld zichtbaar is maken, op basis van de waarde in een ander veld. <p>De standaardwaarde van een opslagveld is bijvoorbeeld: 1 GB als het geheugenveld minder dan 512 MB is. De operator contains controleert of het geselecteerde veld de opgegeven waarde bevat. De operator within controleert of de geselecteerde velden de opgegeven tekenreeks hebben. Als de expressie bijvoorbeeld</p> <p>Veld A is binnen ontwikkeling, is de expressie waar als Veld A = dev of lop of ment, terwijl de expressie wordt geëvalueerd als onwaar als Veld A = prod of test.</p>

Tabel 3-67. Opties op het tabblad Waarden (vervolg)

Optie	Beschrijving
	<ul style="list-style-type: none"> ■ Externe bron De waarde is gebaseerd op de resultaten van een vRealize Orchestrator-actie. Bijvoorbeeld, kostenberekening op basis van een gescripte vRealize Orchestrator-actie. Zie vRealize Orchestrator-acties gebruiken in het ontwerpprogramma voor aangepaste formulieren voor een voorbeeld. ■ Veld binden De waarde is hetzelfde als het geselecteerde veld waaraan deze is gebonden. De beschikbare velden zijn beperkt tot hetzelfde veldtype. U kunt bijvoorbeeld de standaardwaarde voor een veld met selectievakje waarvoor verificatie is vereist binden aan een ander veld met selectievakje. Wanneer een doel-selectievakje is geselecteerd in het aanvraagformulier, wordt het selectievakje op het huidige veld geselecteerd. ■ Berekende waarde Waarde is gebaseerd op de resultaten van de opgegeven waarden en de geselecteerde operator. Tekstvelden gebruiken de aaneenschakelingoperator. Velden met een geheel getal gebruiken de bewerkingen optellen, aftrekken, vermenigvuldigen of delen. U kunt bijvoorbeeld een veld configureren voor een geheel getal om megabytes te converteren naar gigabytes met behulp van de bewerking vermenigvuldigen. De standaardwaarde van het geheugen in MB is gebaseerd op het geheugen in GB vermenigvuldigd met 1024.
Waarde-optie	<p>Invulling van een vervolgkeuzemenu, meervoudige selectie, keuzerondjes of waardeselectievelden.</p> <ul style="list-style-type: none"> ■ Constante. De indeling voor de lijst is Waarde Label, Waarde Label, Waarde Label. Bijvoorbeeld, 2 Small, 4 Medium, 8 Large. ■ Externe bron Waarde is gebaseerd op de resultaten van de geselecteerde vRealize Orchestrator-actie.
Stap	<p>Voor velden met gehele getallen of decimalen, geeft u de oplopende of aflopende waarden op.</p> <p>Indien de standaardwaarde bijvoorbeeld 1 is en u de oplopende waarde op 3 instelt, dan zijn de toegestane waarden 4, 7, 10, enzovoort.</p>

Veldbeperkingen

U kunt beperkingseigenschappen gebruiken om ervoor te zorgen dat de aanvrager geldige waarden in het aanvraagformulier opgeeft.

U kunt eventueel ook externe validatie gebruiken als een alternatieve methode voor opgave van geldige waarden. Zie [Externe validatie gebruiken in het ontwerpprogramma voor aangepaste formulieren](#).

Tabel 3-68. Opties op het tabblad Beperkingen

Optie	Beschrijving
Vereist	<p>De aanvrager moet een waarde opgeven voor dit veld.</p> <ul style="list-style-type: none"> ■ Constante. Klik op Ja om te vereisen dat de aanvrager een waarde opgeeft. Selecteer Nee als het veld optioneel is. ■ Voorwaardelijke waarde Of het veld verplicht is wordt bepaald door de eerste expressie die is ingesteld op waar. Dit veld is bijvoorbeeld vereist als het besturingssysteem in een ander veld met Darwin begint. ■ Externe bron Status is gebaseerd op het resultaat van de geselecteerde vRealize Orchestrator-actie.
Reguliere expressie	<p>Voer een reguliere expressie in die de waarde valideert en een bericht dat wordt weergegeven wanneer de validatie mislukt.</p> <p>De reguliere expressies moeten de syntaxis voor JavaScript volgen. Zie voor een overzicht Een reguliere expressie maken. Zie Syntaxis voor meer gedetailleerde richtlijnen.</p> <ul style="list-style-type: none"> ■ Constante. Voer een reguliere expressie in. Bijvoorbeeld: voor een e-mailadres, kan de reguliere expressie <code>^[A-Za-z0-9._%+-]+@[A-Zaz0-9.-]+\.[A-Za-z]{2,}\$</code> zijn en het foutbericht van de validatie <code>De e-mailadresindeling is niet geldig. Probeer het opnieuw.</code> ■ Voorwaardelijke waarde De reguliere expressie die wordt gebruikt wordt bepaald door de eerste expressie die is ingesteld op waar.
Minimumwaarde	<p>Geef een minimum numerieke waarde op. Een wachtwoord moet bijvoorbeeld tenminste 8 tekens hebben.</p> <p>Geef een foutbericht op. Bijvoorbeeld: het wachtwoord moet tenminste 8 tekens bevatten.</p> <ul style="list-style-type: none"> ■ Constante. Voer het geheel getal in. ■ Voorwaardelijke waarde De minimale waarde wordt bepaald door de eerste expressie die is ingesteld op waar. Een minimum CPU-waarde is bijvoorbeeld 4 als het besturingssysteem niet gelijk is aan Linux. ■ Externe bron Waarde is gebaseerd op de resultaten van de geselecteerde vRealize Orchestrator-actie.

Tabel 3-68. Opties op het tabblad Beperkingen (vervolg)

Optie	Beschrijving
Maximumwaarde	<p>Maximale numerieke waarde. Een veld is bijvoorbeeld beperkt tot 50 tekens.</p> <p>Geef een foutbericht op. Bijvoorbeeld: Deze beschrijving mag niet meer dan 50 tekens bevatten.</p> <ul style="list-style-type: none"> ■ Constante. Voer het geheel getal in. ■ Voorwaardelijke waarde De maximale waarde wordt bepaald door de eerste expressie die waar is. Een maximale opslagcapaciteitwaarde is bijvoorbeeld 2 GB als de implementatielocatie is gelijk aan AMEA. ■ Externe bron Waarde is gebaseerd op de resultaten van de geselecteerde vRealize Orchestrator-actie.
Overeenkomend veld	<p>Deze veldwaarde in het veld moet overeenkomen met de waarde van het geselecteerde veld.</p> <p>Bijvoorbeeld het wachtwoordbevestigingsveld moet overeenkomen met het wachtwoordveld.</p>

vRealize Orchestrator-acties gebruiken in het ontwerpprogramma voor aangepaste formulieren

Wanneer u het aanvraagformulier voor een vRealize Automation-blueprint aanpast, kunt u het gedrag van bepaalde velden baseren op de resultaten van een vRealize Orchestrator-actie.

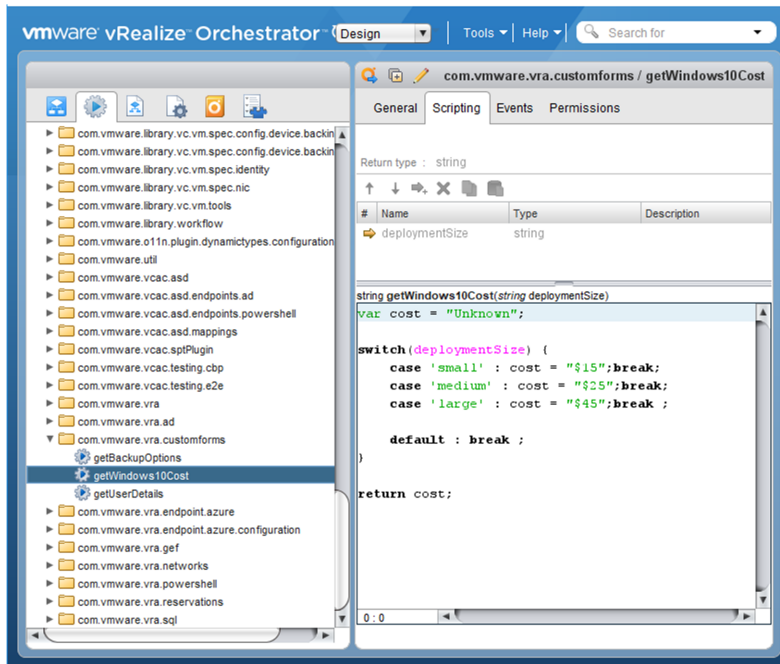
Er zijn verschillende manieren waarop u vRealize Orchestrator-acties kunt gebruiken. Mogelijk hebt u een actie die de gegevens ophaalt van een externe bron, of gebruikt u een script dat de grootte en de kosten definieert. In dit voorbeeld wordt gebruik gemaakt van een script.

Wanneer u een script maakt om velden te vullen met behulp van een actie, gebruikt u geen array van het type [Any].

Voorbeeld: Voorbeeld van de velden Kosten en Grootte

In deze situatie wilt u dat de catalogusgebruiker de grootte van een virtual machine selecteert, en dat vervolgens de kosten van die machine per dag worden weergegeven. Om dit voorbeeld uit te voeren hebt u een vRealize Orchestrator die de grootte en de kosten met elkaar in verband brengt, en u voegt een veld grootte en kosten toe aan het aangepaste formulier van de blueprint. Het veld grootte bepaalt de waarde die wordt weergegeven in het veld kosten.

- 1 In vRealize Orchestrator configureert u een actie, `getWindows10Cost`, met een script `deploymentSize` vergelijkbaar met het volgende voorbeeld.



Gebruik het volgende als voorbeeld voor een script.

```

var cost = "Unknown";

switch(deploymentSize) {
  case 'small' : cost = "$15";break;
  case 'medium' : cost = "$25";break;
  case 'large' : cost = "$45";break ;

  default : break ;
}

return cost;
  
```

- 2 In vRealize Automation, voeg en configureer een veld grootte en een veld kosten toe aan een blueprint voor een aangepast formulier.

Configureer het veld Grootte als een multi-keuze met de waarden Klein, Normaal en Groot.

 The screenshot shows the configuration interface for a field named 'Size'. The 'Values' tab is selected. It shows the 'Default value' set to 'large'. Below this, there are two sections for 'Value options', both set to 'Constant'. The first section is empty. The second section contains the text 'small|Small,mediuim|Meduim,large|Large'.

In vRealize Automation, voeg en configureer een veld grootte en een veld kosten toe aan een blueprint voor een aangepast formulier.

Op het tabblad Waarden, configureer de volgende eigenschapswaarden.

- Standaardwaarde = **Groot**
- Waardeopties
 - Waardebron = **Constant**
 - Waardedefinitie = **klein|Klein, medium|Medium, groot|Groot**

- 3 Configureer het veld kosten om de kosten weer te geven, zoals gedefinieerd in de vRealize Orchestrator-actie, gebaseerd op de geselecteerde waarde in het veld grootte.

Cost ⓘ
Field ID: cost

Appearance **Values** Constraints

▼ Default value External source

Value source External source ▼

Select action com.vmware.vra.customforms/getWindows10Cost

Action inputs

deploymentSize Field ▼ Size ▼

Op het tabblad Waarden, configureer de volgende eigenschapswaarden.

- Standaardwaarde = Externe bron
- Selecteer actie = <uw vRealize Orchestrator-actiesmap>/getWindows10Cost
- Invoer van actie
 - deploymentSize. Deze waarde is geconfigureerd in de actie.
 - Veld
 - Grootte

De elementen van het waardeselectieveld of boomstructuurselectieveld gebruiken in het ontwerpprogramma voor aangepaste formulieren

Wanneer u het aanvraagformulier aanpast, kunt u elementen opgeven waarbij de gebruiker kan selecteren uit zoekresultaten in een lijst of bladeren door een boomstructuur om een overeenkomende waarde te vinden.

Het waardeselectieveld en boomstructuurselectieveld werken met het Referentietype dat is gedefinieerd op het tabblad Uiterlijk van het aangepaste formulier. Het Referentietype is een resource van vRealize Orchestrator. Bijvoorbeeld: AD:UserGroup of VC:Datastore. Door het referentietype te definiëren wanneer de gebruiker een zoekreeks invoert, zijn de resultaten of boomstructuuropties beperkt tot de overeenkomende parameter of de resources die de overeenkomende parameter hebben.

Voor het waardeselectieveld kunt u de mogelijke waarden vervolgens verder beperken door een externe bron te configureren. Voor het boomstructuurselectieveld kunt u een standaardwaarde instellen door een externe bron te configureren.

Werken met het waardeselectieveld

Het waardeselectieveld wordt weergegeven in het catalogusformulier als een zoekoptie. De gebruiker voert een tekenreeks in en het selectieveld biedt opties op basis van de manier waarop u deze hebt geconfigureerd. U kunt het selectieveld op basis van de volgende gebruikssituaties gebruiken. Het meest waardevolle gebruik van het waardeselectieveld is het koppelen aan een externe bronwaarde.

- Waardeselectieveld met een constante waardebron. Gebruik deze methode wanneer u wilt dat de aanvragende gebruiker een vooraf gedefinieerde statische lijst van waarden selecteert. Net als bij de combobox-, dropdown-, multiselect- en radiogroepselementen biedt deze methode zoekresultaten in een lijst op basis van de gedefinieerde constante waarden en labels.
- Een waardeselectieveld zonder een gedefinieerde waardebron. Gebruik deze methode wanneer u wilt dat de aanvragende gebruiker in de vRealize Orchestrator-inventarislijst zoekt naar een specifiek object met het geconfigureerde referentietype. Het referentietype is bijvoorbeeld VC:Datastore en u wilt dat de gebruikers de gegevensopslag uit de opgehaalde lijst selecteren.
- Een waardeselectieveld met een externe waardebron. Gebruik deze methode wanneer u wilt dat de aanvragende gebruiker een keuze maakt uit resultaten die zijn gebaseerd op een vRealize Orchestrator-actie. Voor een waardeselectieveld met externe bronnen moet de actie een array met eigenschappen retourneren, geen tekenreeksarray. U hebt bijvoorbeeld een actie die twee of meer waarden uit een geïntegreerde database ophaalt en u wilt dat de gebruikers een waarde uit de opgehaalde lijst selecteren. De actie moet het filter `filter = System.getContext().getParameter("__filter");` bevatten en moet een array met eigenschappen retourneren, geen tekenreeksarray. Als u een tekenreeksarray wilt gebruiken, gebruikt u het veldtype Keuzelijst met invoervak.

Werken met het boomstructuurselectieveld

Het boomstructuurselectieveld wordt weergegeven in het catalogusformulier als een zoekoptie. De gebruiker voert een tekenreeks in en het boomstructuurselectieveld verschijnt. Met de boomstructuur kunnen de gebruikers waarden selecteren die overeenkomen met het referentietype. Als het referentietype bijvoorbeeld VC:Datastore is, kan de aanvragende gebruiker gegevensopslagobjecten selecteren. Als het referentietype VC:VirtualMachine is, kan de gebruiker virtuele machines selecteren.

- Een waardeselectieveld zonder een gedefinieerde waardebron. Gebruik deze methode wanneer u wilt dat de aanvragende gebruiker de hiërarchische boomstructuur doorzoekt voor een specifiek object met het geconfigureerde referentietype. Het referentietype is bijvoorbeeld VC:Datastore en u wilt dat de gebruikers de gegevensopslag uit de opgehaalde boomstructuur selecteren.

- Een boomstructuurselectieveld met een externe waardebron. Gebruik deze methode als u een standaardselectie in de boomstructuur wilt opgeven. De aanvragende gebruiker kan de vooraf ingestelde waarde selecteren of naar een andere waarde bladeren. Voor referentietype VC:Datastore wilt u bijvoorbeeld de gegevensopslag in de boomstructuur vooraf instellen op een bepaalde gegevensopslag op basis van de resultaten van de actie-invoerwaarde die een netwerk opgeeft.

Het data grid-element gebruiken in het ontwerpprogramma voor aangepaste formulieren

Wanneer u het aanvraagformulier voor een blueprint aanpast, kunt u informatie toevoegen in tabelformaat. De aanvragende gebruiker kan de rijen vullen met gegevens die zijn opgenomen in de provisioning-aanvraag.

U kunt een tabel toevoegen en deze invullen op basis van handmatig geleverde gegevens of op basis van een externe bron. Sommige blueprintelementen worden weergegeven als een data grid. Bijvoorbeeld schijven voor virtual machines of NIC's.

Naast het toevoegen van velden aan de data grid kunt u ook beperkingen toevoegen om ervoor te zorgen dat de gebruiker acceptabele waarden invoert.

In de volgende voorbeelden wordt de data grid gebruikt, maar u kunt ook de optie Kiezer met meerdere waarden gebruiken in het aanvraagformulier als een alternatieve manier om deze optie aan de gebruiker te presenteren. U kunt de verschillen testen door de veldeigenschap

Vormgeving > Label en type > Weergavetype te wijzigen.

Voorbeeld: Voorbeeld opgegeven CSV-gegevens

In dit voorbeeld is er een tabel met waarden die u hebt opgegeven in het ontwerpprogramma voor aangepaste formulieren, zodat deze kunnen U geeft de gegevens in de tabel op als een constante waardebron. De bron is gebaseerd op een CSV-gegevensstructuur, waarbij de eerste rij een koptekst is. De kopteksten zijn de kolom-id's, gescheiden door een komma. Elke volgende rij bevat de gegevens die worden weergegeven in elke rij in de tabel.

- 1 Voeg het algemene Data Grid-element toe aan het ontwerpcanvas.
- 2 Selecteer de data grid en geef de waarden op in het deelvenster Eigenschappen.



Data Grid ?



Field ID: datagrid_ecdf4fe3



Appearance **Values** Constraints

Columns

ADD COLUMN

Label	Username	 
Id	username	
Type	String	▼

Label	Employee ID	 
Id	employeeid	
Type	Integer	▼

Label	Manager	 
Id	manager	
Type	String	▼

Default value Constant

Value Constant ▼

source

CSV

```
username,employeeid,manager
leonardo,95621,Farah
vindhya,15496,Farah
martina,52648,Nikolai
```

Label	Id	Type
Gebruikersnaam	gebruikersnaam	String
Werknemer-ID	employeeid	Geheel getal
Manager	manager	String

De CSV-waarden definiëren.

```
username,employeeId,manager
leonardo,95621,Farah
vindhya,15496,Farah
martina,52648,Nikolai
```

- Controleer dat de data grid de verwachte gegevens bevat in het aanvraagformulier voor de blueprint.

<input type="checkbox"/>	Username	Employee ID	Manager
<input type="checkbox"/>	leonardo	95621	Farah
<input type="checkbox"/>	vindhya	15496	Farah
<input type="checkbox"/>	martina	52648	Nikolai

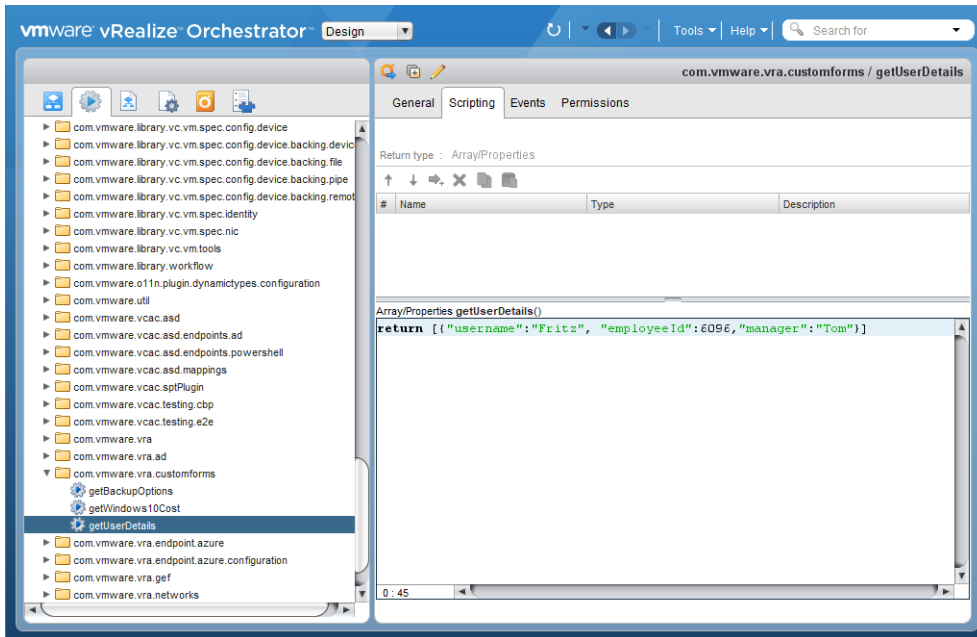
1 - 3 of 3

Voorbeeld: Voorbeeld van een externe bron

Dit voorbeeld maakt gebruik van het vorige voorbeeld, maar de waarden zijn gebaseerd op een vRealize Orchestrator-actie. Hoewel dit een voorbeeld van een eenvoudige actie is, kunt u gebruikmaken van meer complexe acties, zoals het ophalen van deze informatie uit een lokale database of systeem.

De actie die u als validatie gebruikt, moet een invoerparameter voor array/eigenschappen hebben.

- Configureer in vRealize Orchestrator een actie, `getUserDetails`, met een array die vergelijkbaar is met het volgende voorbeeld.



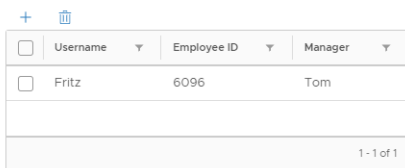
Gebruik het volgende voorbeeldscript.

```
return [{"username": "Fritz", "employeeId": 6096, "manager": "Tom"}]
```

- 2 Voeg in vRealize Automation de data grid toe, en configureer de kolommen van de data grid met de volgende waarden.

Label	Id	Type
Gebruikersnaam	gebruikersnaam	String
Werknemer-ID	employeeid	Geheel getal
Manager	manager	String

- 3 Selecteer in de lijst met bronwaarden, **Externe bron**.
- 4 In selecteeractie, voer getUserDetails in en selecteer de actie die u hebt gemaakt in vRealize Orchestrator.
- 5 Sla de tabel op in het aanvraagformulier, en controleer de tabel.



<input type="checkbox"/>	Username ▼	Employee ID ▼	Manager ▼
<input type="checkbox"/>	Fritz	6096	Tom

1 - 1 of 1

Voorbeeld: Voorbeeld van blueprintelement

Sommige blueprintelementen kunnen worden toegevoegd aan het formulier en worden weergegeven als een data grid wanneer de gebruiker de blueprint aanvraagt. Schijven en NIC's worden als data grids weergegeven.

In dit voorbeeld voegt u het element schijven toe aan het formulier zodat gebruikers extra schijven kunnen toevoegen wanneer ze het catalogusitem aanvragen. U kunt beperkingen toevoegen, zodat u beter kunt bepalen wat de gebruiker kan aanvragen. U kunt bijvoorbeeld de capaciteit beperken tot 5 GB.

De elementwaarden die in de blueprint zijn gedefinieerd, bijvoorbeeld schijven, zijn niet zichtbaar in het aangepaste formulier. Hiermee voorkomt u dat de gebruiker een configuratie wijzigt die vereist is voor de succesvolle provisioning van de aanvraag.

- 1 Maak een blueprint met een machine met een gedefinieerde opslagschijf van 6 GB.
- 2 Voeg het element schijven toe aan het canvas.
- 3 Selecteer de data grid en geef de beperkingen op in het deelvenster Eigenschappen.

In dit voorbeeld is de minimale capaciteit ingesteld op 2 en de maximale capaciteit op 5.

Disks ?

Field ID: vSphere__vCenter__Machine_1-disks

Appearance

Values

Constraints

> Drive letter / Mount path

> Volume ID

> ID

> Label

> custom_properties

> User Created

> Storage Reservation policy

> Capacity

> Required

No

▼

> Regular expression

Regular expression

> Minimum value

2

> Maximum value

5

- 4 Bewaar en controleer de tabelbeperkingen in het aanvraagformulier.
- 5 Klik in het aanvraagformulier op het plusteken in de data grid.

Merk op dat de capaciteitsbeperking wordt geactiveerd als u een waarde invoert die groter is dan 5.

☐ Is Clone

Drive letter / Mount path

Volume ID



ID

Label

custom_properties

☐ User Created

Storage Reservation policy

Capacity  

Externe validatie gebruiken in het ontwerpprogramma voor aangepaste formulieren

U kunt een aanvraagformulier personaliseren door beperkingen toe te voegen aan velden, of met behulp van een externe validatiebron, om ervoor te zorgen dat gebruikers geldige waarden opgeven tijdens de aanvraag.

Sommige veldeigenschappen, zoals minimum, maximum, reguliere expressies, overeenkomstvelden, of niet leeg, kunnen worden geconfigureerd met beperkingen om geldige waarden te garanderen. Zie [Aangepaste veldeigenschappen voor formulierontwerper](#).

Externe validatiecontroles voor geldige waarden van een externe bron met behulp van vRealize Orchestrator-acties.

Als u een waarde in een data grid valideert, moet de actie die u als validatie gebruikt, een invoerparameter voor array/eigenschappen hebben.

Voorbeelden waarbij u mogelijk gebruik wilt maken van externe validatie:

- De geldige waarden zijn in een externe bron gedefinieerd. Bijvoorbeeld, vRealize Orchestrator.
- De validatie moet gelden voor verschillende velden. Bijvoorbeeld: een vRealize Orchestrator-actie verzamelt de schijfgrootte en de opslagcapaciteit van de pool, en valideert de opgegeven grootte van de waarden op basis van de beschikbare ruimte.

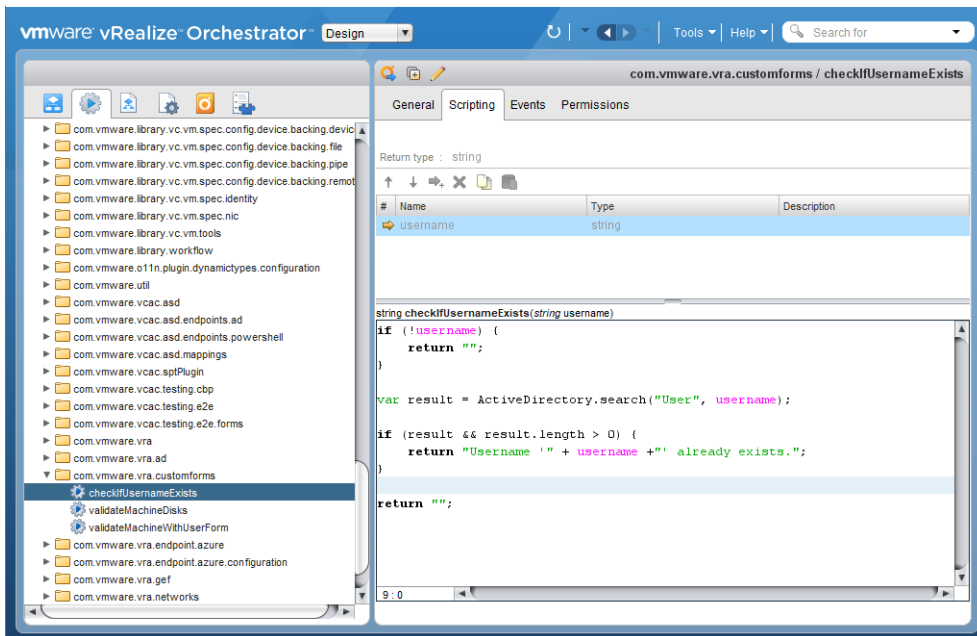
Hoe kunt u meerdere externe validaties aansturen in één blueprint? De validaties worden verwerkt in de volgorde waarin ze worden weergegeven op het externe validatiecanvas. Als u twee validaties hebt die hetzelfde veld valideren, overschrijven de validatieresultaten van de tweede de eerste. Om de validaties te herorganiseren, klikt en sleept u de kaarten op het canvas.

Voorbeeld: vRealize Orchestrator Gebruikersvoorbeeld

In dit geval wilt u dat de catalogusgebruiker alleen een nieuwe gebruikersnaam opgeeft. Om dit voorbeeld uit te voeren, is er een vRealize Orchestrator-actie nodig die controleert of de in het formulier opgegeven gebruikersnaam voorkomt in uw Active Directory-database. Als de naam bestaat verschijnt er een foutmelding in het aanvraagformulier.

Deze situatie wordt toegepast in het voorbeeld [Een aangepast aanvraagformulier met Active Directory-opties maken](#).

- 1 In vRealize Orchestrator configureert u een actie, `checkIfUsernameExists`, met een script dat vergelijkbaar is aan het volgende voorbeeld.



Gebruik het volgende als voorbeeld voor een script. In dit voorbeeld is return het bericht dat wordt weergegeven als de validatie mislukt.

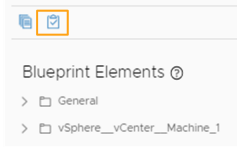
```
if (!username) {
    return "";
}

var result = ActiveDirectory.search("User", username);

if (result && result.length > 0) {
    return "Username '" + username + "' already exists.";
}

return "";
```

- 2 Open in vRealize Automation het ontwerpprogramma voor aangepaste formulieren voor uw blueprint, klikt u op **Externe validatie**, en sleept het **Orchestrator-validatie**-type naar het canvas.



- 3 Configureer de externe validatieopties.

- Validatielabel = controleer of de gebruikersnaam bestaat
- Selecteeractie = <uw vRealize Orchestrator-actiesmap>/checkIfUsernameExists
- Invoer van actie
 - gebruikersnaam = veld en gebruikersnaam
- Gemarkeerde velden
 - Klik op **Veld toevoegen** en selecteer de gebruikersnaam.

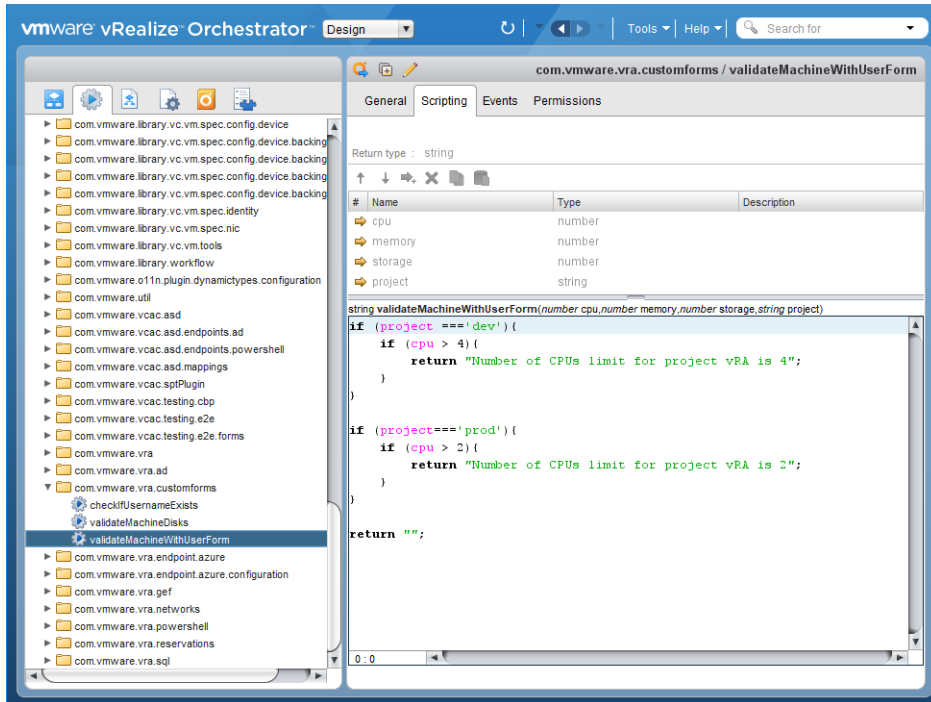
Er wordt een veld-niveau-validatiefout in het catalogusaanvraagformulier weergegeven als het resultaat van de validatie van de ingevoerde waarde negatief is. Als u een algemene fout wilt weergeven, configureer dan niet het gemarkeerde veld.

Voorbeeld: vRealize Orchestrator Voorbeeld met meerdere velden

In deze situatie wilt u de validatie van de CPU, het geheugen en de opslagwaarden baseren op de verwachte waarde. Bijvoorbeeld: als gebruikers het Dev-project selecteren, dan is 4 het maximum aantal CPU's. Als ze Prod selecteren, is 2 de maximale waarde.

Voeg voor deze situatie een projectveld toe aan het voorbeeld [Een aangepast aanvraagformulier met Active Directory-opties maken](#). Configureer het project als een vervolkeuzemenu met Dev en Prod.

- 1 In vRealize Orchestrator configureert u een actie, `validateMachineWithUserForm`, met een script dat vergelijkbaar is aan het volgende voorbeeld.



Gebruik het volgende script als een voorbeeld voor het controleren van de CPU. Ga door met het toevoegen van de geheugen- en opslagwaarden aan het script, indien nodig. In dit voorbeeld is retournering het bericht dat wordt weergegeven als de validatie mislukt.

```

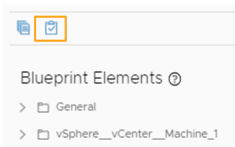
if (project === 'dev'){
    if (cpu > 4){
        return "Number of CPUs limit for project vRA is 4";
    }
}

if (project==='prod'){
    if (cpu > 2){
        return "Number of CPUs limit for project vRA is 2";
    }
}

return "";

```

- Open in vRealize Automation het ontwerpprogramma voor aangepaste formulieren voor uw blueprint, klikt u op **Externe validatie**, en sleept het **Orchestrator-validatie**-type naar het canvas.



- Configureer de externe validatieopties.

- Validatielabel = machinegegevens valideren
- Selecteer actie = <uw vRealize Orchestrator-actiesmap>/validateMachineWithUserForm
- Invoer van actie
 - cpu = veld en het aantal CPU's
 - geheugen = veld en geheugen (GB)
 - opslag = veld en opslag (GB)
 - Project = veld en project
- Gemarkeerde velden
 - Klik op **Veld toevoegen** en selecteer **Project**.

In de catalogus ziet de catalogusgebruiker een validatiefout dat vergelijkbaar is aan het volgende voorbeeld.

Mislukte provisioning-aanvragen testen en problemen oplossen

U wilt als blueprintarchitect of beheerder ervoor zorgen dat u werkende blueprints aan de gebruiker levert.

Een catalogusaanvraag kan om verschillende redenen mislukken. Dit kan te wijten zijn aan netwerkverkeer, onvoldoende eindpuntresources of een foutieve blueprintspecificatie. Of de provisioning-aanvraag is gelukt, maar de implementatie lijkt niet te werken. Als blueprintarchitect wilt u voorkomen dat u blueprints levert die uw gebruikers niet kunnen implementeren.

U kunt een testservice en rechten maken, zodat u de blueprint uit de catalogus kunt implementeren. Zie [Checklist voor het configureren van de servicecatalogus](#).

Als de resources niet met succes zijn geleverd, kunt u vRealize Automation gebruiken om problemen met de mislukte implementatie op te lossen.

Mogelijke foutstatussen

Als een provisioning-aanvraag mislukt, ziet u een van de volgende statussen.

- **Mislukt** Een aanvraag kan om verschillende redenen mislukken. Een oorzaak is dat het provisioning-proces niet werkte vanwege een gebrek aan resources op het doeleindpunt, door onvoldoende resources die beschikbaar zijn om de blueprint te ondersteunen of door een slecht ontworpen blueprint die moet worden verbeterd. Een andere oorzaak is dat de aanvraag goedkeuring van iemand anders in uw organisatie vereist en dat de goedkeurder de aanvraag heeft afgewezen. Het is ook mogelijk dat een actie die u hebt uitgevoerd voor een implementatie is mislukt. De fout kan worden veroorzaakt om de goedkeurings- of omgevingsredenen die al genoemd zijn.

Gebruik de volgende probleemoplossingsworkflow om de oorzaak van het probleem te onderzoeken. Als u het probleem kunt oplossen, bekijkt u uw actie-opties met betrekking tot **Verwijderen** en **Opnieuw indienen**. Zie [Opdrachten in het menu Actie voor ingerichte bronnen](#).

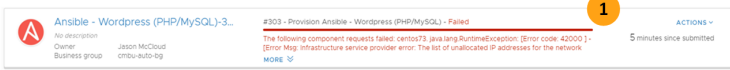
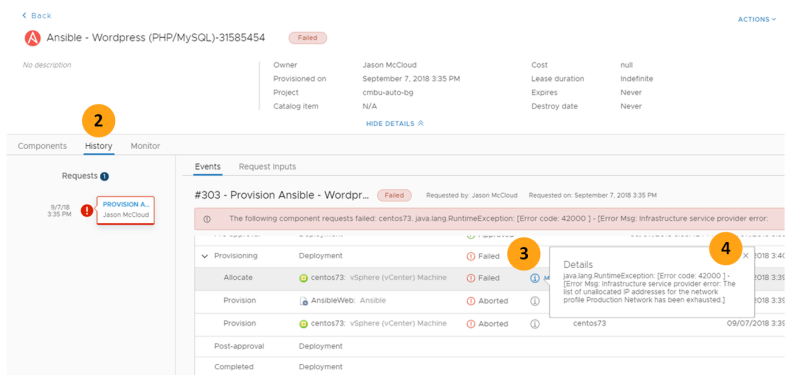
- **Gedeeltelijk succesvol.** Een aanvraag kan gedeeltelijk succesvol zijn, wat betekent dat sommige componenten geïmplementeerd zijn, maar niet alle provisioning-stappen met succes zijn afgerond.

Gebruik de volgende workflow voor probleemoplossing om te bepalen welke componenten slechts gedeeltelijk zijn gelukt en om de oorzaak van het probleem te onderzoeken. Als u het probleem kunt oplossen, bekijkt u uw actie-opties met betrekking tot **Verwijderen** en evalueert u of u **Hervatten** kunt gebruiken. Zie [Opdrachten in het menu Actie voor ingerichte bronnen](#) en [Werking van de actie Hervatten](#).

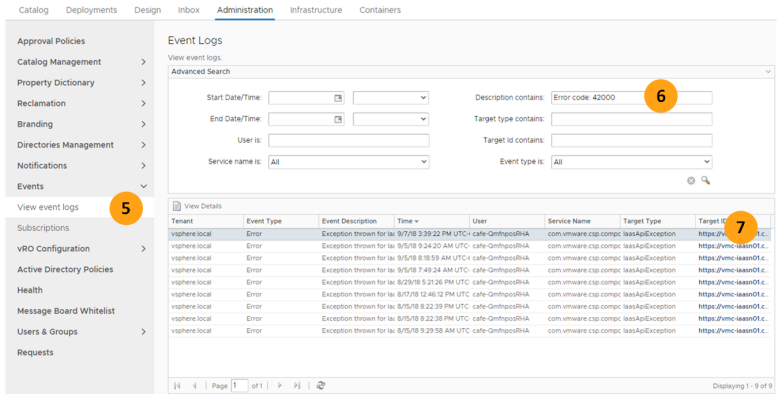
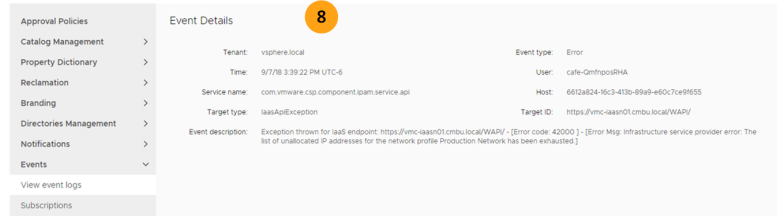
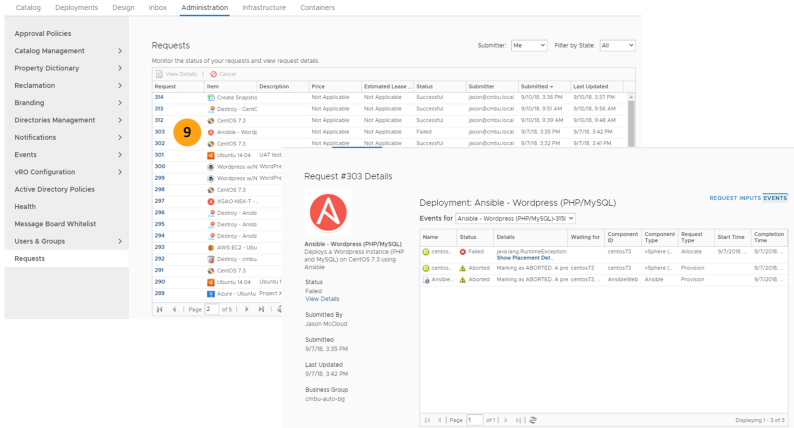
Workflow probleemoplossing

U kunt deze workflow gebruiken om een mislukte implementatie te onderzoeken. Als uit uw onderzoek blijkt dat de fout werd veroorzaakt door een tijdelijk omgevingsprobleem, kunt u de fout oplossen en de aanvraag opnieuw indienen. Als er een probleem is met de specificatie van de aanvraag, kunt u de blueprint bijwerken en een nieuwe aanvraag indienen.

Tabel 3-69. Hoe u moet beginnen met het oplossen van fouten

Werkstr oom	Stap voor probleemoplossing	Voorbeeld
1	Mislukte implementaties zijn op het tabblad Implementaties vermeld op de statusbalk. De kaart bevat het laatste foutbericht. Klik op de implementatienaam of voortgangsbalk voor meer informatie.	
2	U kunt de workflow gebeurtenissen op het tabblad Geschiedenis met implementatiegegevens gebruiken om te zien waar het provisioning-proces is mislukt. Deze workflow is ook handig wanneer u een actie voor een implementatie uitvoert, maar de wijziging mislukt.	
3	De mislukte status geeft aan waar de workflow is mislukt.	
4	De informatie biedt een meer uitgebreide versie van de foutmelding. Als deze informatie in de wegwijzerhulp niet voldoende is om het probleem te identificeren en op te lossen, kunt u aanvullend onderzoek doen in de gebeurtenislogboeken.	

Tabel 3-69. Hoe u moet beginnen met het oplossen van fouten (vervolg)

Werkstr oom	Stap voor probleemoplossing	Voorbeeld
5	De volgende stappen vereisen een beheerdersrol. Om een fout te vinden in de context van andere fouten en waarschuwingen, selecteert u Beheer > Gebeurtenissen > Gebeurtenislogboek en bekijken .	
6	U kunt de geavanceerde zoekopdracht gebruiken om de fout te vinden op basis van het bericht in de gegevens van de implementatie.	
7	Om de gegevens over de gebeurtenis weer te geven, klikt u op de koppeling van de doel-ID.	
8	De gegevens van de gebeurtenis bieden aanvullende provisioning-informatie die u kan helpen bij probleemoplossing.	
9	Als beheerder kunt u de aanvraag ook bekijken in de context van andere aanvragen van uw gebruikers. Selecteer Beheer > Aanvragen en klik op het aanvraagnummer om de invoer en gebeurtenissen van de aanvraag te controleren.	

Werking van de actie Hervatten

Met Hervatten kunt u onder bepaalde omstandigheden het inrichtingsproces van mislukte implementaties hervatten vanaf het punt waar de fout zich voordeed. Wanneer de actie Hervatten is ingeschakeld, is deze beschikbaar voor mislukte inrichtingsaanvragen of toepasselijke acties.

Als u Hervatten wilt gebruiken voor inrichtingsaanvragen, moet u de aangepaste eigenschap `_debug_deployment = true` toevoegen aan de blueprint. Standaard worden mislukte implementaties teruggedraaid en opgeschoond zodat de bronnen worden teruggewonnen. De aangepaste eigenschap `_debug_deployment = true` behoudt de implementatie tot op het punt van de fout en staat een Hervatten-actie toe waar dit wordt ondersteund en op basis van de werking ervan. Als u Hervatten alleen gebruikt voor de ondersteunde acties, hoeft u de eigenschap `_debug_deployment` niet in te schakelen.

Zie *Naslaggids voor aangepaste eigenschappen* voor meer informatie over `_debug_deployment`.

Als u Hervatten wilt gebruiken voor een inrichtingsaanvraag of voor de beschikbare acties, moet u gebruikers rechten verlenen voor de actie Hervatten. Zie [Gebruikers rechten verlenen voor services, catalogusitems en acties](#).

U kunt gebruikers rechten verlenen voor de actie Hervatten voor de volgende inrichtingsactiviteiten.

- Inrichtingsaanvragen
- Actie Hervatten
- Actie Inschalen
- Actie Uitschalen
- Actie Vernietigen

Beperkingen van de actie Hervatten

Wanneer u bepaalt of u Hervatten kunt gebruiken dan wel een nieuwe instantie van een blueprint moet aanvragen, moet u rekening houden met de beperkingen.

- De blueprint kan niet worden gewijzigd vanaf het moment van de aanvraag.

Op het moment van de aanvraag wordt een niet-wijzigbare versie van de blueprint gekoppeld aan de catalogusaanvraag. Deze statische versie bevat alle specificaties, inclusief kenmerken, aangepaste eigenschappen, instellingen enzovoort, zoals ze waren bij het starten van de inrichting. Als uw blueprint een fout bevat die tot een storing leidt, kan dit niet worden opgelost door de fout te corrigeren en de actie Hervatten uit te voeren omdat deze verwijst naar de versie die is gekoppeld aan de aanvraag. In dit scenario moet u een nieuwe instantie inrichten.

Voorbeelden

- Blueprint A vereist 5 GB RAM, maar de aanvraag mislukt omdat u slechts reserveringen hebt voor 3 GB. Als u de blueprint bijwerkt zodat deze slechts 3 GB vereist en vervolgens

Hervatten uitvoert, zal de actie mislukken. Bij het uitvoeren van de actie Hervatten wordt de oorspronkelijke aanvraag gecontroleerd en wordt nog steeds 5 GB gezocht. Als u echter de systeemreservering voor de bedrijfsgroep verhoogt tot 5 GB en Hervatten uitvoert, zal de actie slagen.

- Wanneer u blueprint B aanvraagt, die een aangepaste gastspecificatie bevat, mislukt dit. Na onderzoek blijkt dat de aangepaste gastspecificatie is hernoemd in uw vCenter Server-instantie. Als u de blueprint met de nieuwe naam bijwerkt en Hervatten uitvoert, mislukt de actie. U hebt de blueprint bijgewerkt, maar de oorspronkelijke versie wordt gebruikt voor de actie Hervatten. Als de nieuwe naam de naam is die u in de toekomst wilt gebruiken, implementeert u een nieuwe instantie van de blueprint in plaats van Hervatten te gebruiken. Anders moet u de naam van de aangepaste gastspecificatie in de vCenter Server-instantie opnieuw wijzigen in de naam die de oorspronkelijke versie verwacht en de actie Hervatten uitvoeren. Als u niet wilt dat de volgende inrichtingsaanvraag mislukt, mag u niet vergeten de blueprint bij te werken met de juiste aangepaste gastspecificatie.

Hervatten werkt als u de doelimplementatieomgeving kunt bijwerken zodat deze de blueprints specificaties ondersteunt zoals ze waren op het moment van de aanvraag.

- Opnieuw proberen kan alleen vanaf het punt van de fout.

De actie Hervatten probeert de taken van het onderdeel opnieuw uit te voeren vanaf het punt van de fout. Ze dient niet de hele inrichtingsaanvraag opnieuw in.

Voorbeelden

- Blueprint C maakt een toepassings-virtual machine en een database-virtual machine. De implementatie van de database-VM slaagt, maar de inrichting op de toepassings-VM mislukt. Als u de actie Hervatten uitvoert, wordt alleen een nieuwe poging gedaan om de toepassings-VM in te richten.

Als een onderdeel als Mislukt wordt gemarkeerd, wordt dit behandeld alsof het nooit is uitgevoerd. Als de installatie mislukt tijdens de configuratiefase op de database-VM, bijvoorbeeld vanwege een scriptfout, maar de database intact is, bestaat de database nog wanneer het script wordt uitgevoerd tijdens een Hervatten-actie. Het installatiescript, dat het configuratiescript bevat, wordt niet opnieuw uitgevoerd. Het hervatten mislukt. U moet het script corrigeren en een nieuwe instantie inrichten.

- Een andere variant om rekening mee te houden is dat de toewijzing van de stap is geslaagd, maar het inrichten is mislukt. Wanneer u in dit voorbeeld de actie Hervatten uitvoert, waarbij een nieuwe poging wordt gedaan vanaf het punt waarop de inrichting is mislukt, verwerkt de hervattingsaanvraag verouderde toewijzingsinformatie en zal het hervatten mislukken.

Werken met de actie Hervatten en werkstroomabonnementen

Als de werkstroom voor een abonnement mislukt, kunt u de actie Hervatten niet uitvoeren om die werkstroom te hervatten. De actie Hervatten kan alleen worden uitgevoerd voor mislukte inrichtingsgebeurtenissen. Op dat moment wordt een nieuwe werkstroom uitgevoerd.

Bijvoorbeeld: als u zich abonneert op de gebeurtenis Catalogusaanvraag ontvangen, voldoen zowel de mislukte inrichtingsaanvraag als de nieuwe aanvraag voor hervatting onafhankelijk aan de abonnementsvoorwaarden, maar voor het abonnement is niet bekend dat de mislukte aanvraag en de aanvraag voor hervatting gerelateerde activiteiten zijn.

Vernietiging van een implementatie forceren na een mislukte vernietigingsaanvraag

U kunt de vernietiging van een implementatie forceren die als gevolg van een mislukte aanvraag tot vernietiging een inconsistente status heeft.

Wanneer vernietiging van een implementatiebron door vRealize Automation mislukt tijdens een vernietigingsbewerking voor een implementatie, wordt de vernietigingsbewerking direct gestopt zonder de resterende implementatiebronnen te vernietigen. Het gevolg van deze mislukking is dat de implementatie in een inconsistente status achterblijft en bronnen gebruikt zonder dat er een duidelijke manier is waarop de implementatie kan worden vernietigd.

Bedrijfsgroepbeheerders kunnen de vernietiging forceren van implementaties die in deze inconsistente status zijn achtergebleven.

Voorwaarden

- Controleer of u als **bedrijfsgroepbeheerder** bent aangemeld bij vRealize Automation.
- Beoordeel eerst de beschrijving van de vernietigingsactie in [Opdrachten in het menu Actie voor ingerichte bronnen](#) voordat u de actie Geforceerd vernietigen uitvoert.

Procedure

- 1 Zoek de te vernietigen implementatie op het tabblad **Implementaties**.
- 2 Klik op **Acties** en klik op **Vernietigen**.
- 3 Voer een beschrijving in voor de aanvraag en een reden voor de aanvraag.
- 4 Selecteer **Geforceerd vernietigen** en klik op **Indienen**.

Resultaten

vRealize Automation probeert de implementatie volledig te vernietigen, ook alle bronnen in de implementatie. Als vRealize Automation een implementatiebron niet kan vernietigen, wordt die bron overgeslagen en worden de resterende bronnen in de implementatie vernietigd.

Wat nu te doen

Controleer of alle resources in de implementatie met succes zijn vernietigd. Alle bronnen die niet worden vernietigd tijdens een bewerking om bronnen geforceerd te vernietigen, moeten handmatig worden vernietigd. Zorg er ook voor dat de objecten van een ingerichte virtual machine worden vernietigd, omdat vRealize Automation tijdens de volgende bewerkingen voor de inrichting mogelijk hun hostnamen, IP-adressen en andere configuratiegegevens probeert te hergebruiken.

Problemen oplossen met een mislukte implementatie die een vRealize Orchestrator werkstroom bevat

Als een mislukte blueprintimplementatie een vRealize Orchestrator-werkstroom bevat, kunt u de token-id gebruiken om problemen met de werkstroom op te lossen. U kunt de token-id gebruiken om de logboeken in vRealize Orchestrator te zoeken.

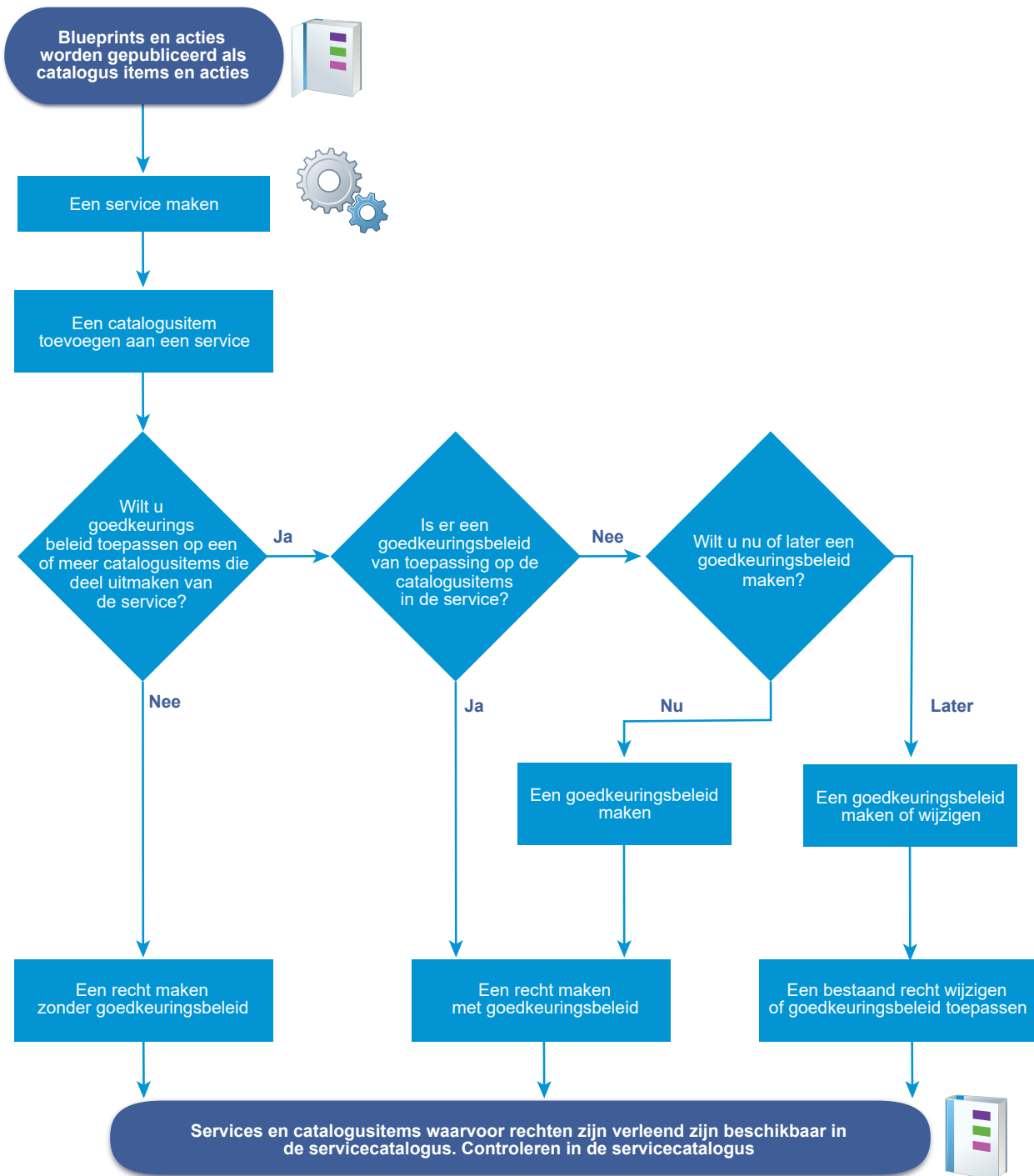
Oplossing

- 1 Zoek de token-id voor de mislukte werkstroom.
 - a Klik op het tabblad **Implementaties** in vRealize Automation en zoek naar de implementatie of actie.
 - b Klik op de implementatienaam.
De aanvraag kan een implementatie of een actie zijn.
 - c Klik op het tabblad **Geschiedenis** en vervolgens op het tabblad **Invoer aanvragen**.
Als de blueprint gebaseerd is op een vRealize Orchestrator-werkstroom, is de paginatitel vRealize Orchestrator Details uitvoering werkstroom.
 - d Zoek de token-id en kopieer deze naar het klembord of een tekstbestand.
Bijvoorbeeld: ff8080815a685352015a6c8d450801ee.
- 2 Zoek de werkstroomlogboeken in vRealize Orchestrator met behulp van het Control Center
 - a Voer de basis-URL voor vRealize Automation in een tekstvak van een browser in.
De pagina VMwarevRealize Automation-toepassing verschijnt.
 - b Klik op **vRealize Orchestrator Control Center**.
 - c Meld u aan als een gebruiker met root-rechten.
 - d Klik op **Werkstromen controleren**.
 - e Klik op **Voltooide werkstromen**.
 - f Plak het werkstroomtoken in het tekstvak Token-id.
In de lijst verschijnt de werkstroom die overeenkomt met de token-id.
 - g Klik op de rij en controleer de logboeken om de oorzaak van de mislukking te achterhalen.

De servicecatalogus beheren

In de servicecatalogus kunnen uw klanten aanvragen indienen voor machines en andere items om deze in te richten voor gebruik. U beheert de gebruikerstoegang tot de servicecatalogusitems op basis van de manier waarop u services bouwt, gebruikers rechten verleent voor een of meer items en bestuur toepast.

Met welke werkstroom u items toevoegt aan de servicecatalogus, is afhankelijk van het feit of u goedkeuringsbeleid maakt en toepast.



Checklist voor het configureren van de servicecatalogus

Na het maken en publiceren van blueprints en acties, kunt u een vRealize Automation-service maken, catalogusitems configureren en rechten en goedkeuringen toewijzen.

De checklist voor het configureren van de servicecatalogus geeft een algemeen overzicht van de vereiste stappen om de catalogus te configureren en bevat koppelingen naar beslissingspunten of gedetailleerde instructies per stap.

Tabel 3-70. Checklist voor configuratie van servicecatalogus

Taak	Vereiste rol	Details
<input type="checkbox"/> Een service toevoegen	tenantbeheerder of catalogusbeheerder	Zie Een service toevoegen .
<input type="checkbox"/> Een catalogusitem toevoegen aan een service.	tenantbeheerder of catalogusbeheerder	Zie Catalogusitems toevoegen aan een service .
<input type="checkbox"/> Het catalogusitem voor de service configureren.	tenantbeheerder of catalogusbeheerder	Zie Een catalogusitem configureren .
<input type="checkbox"/> Rechten maken en toepassen op het catalogusitem.	tenantbeheerder of bedrijfsgroepbeheerder	Zie Gebruikers rechten verlenen voor services, catalogusitems en acties .
<input type="checkbox"/> Goedkeuringsbeleid maken en toepassen op het catalogusitem.	tenantbeheerders of goedkeuringsbeheerders kunnen goedkeuringsbeleid maken tenantbeheerders of bedrijfsgroepbeheerders kunnen goedkeuringsbeleid toepassen	Zie Goedkeuringsbeleid maken .

Een service maken

Een service is een groep catalogusitems die u wilt opnemen in de servicecatalogus. U kunt rechten verlenen aan de service, waardoor gebruikers van bedrijfsgroepen rechten krijgen op alle gekoppelde catalogusitems, en u kunt een goedkeuringsbeleid toepassen op de service.

Een service werkt als een dynamische groep catalogusitems. Als u rechten verleent aan een service, zijn alle catalogusitems die gekoppeld zijn aan de service, beschikbaar in de servicecatalogus voor de opgegeven gebruikers, en worden alle catalogusitems die u toevoegt aan of verwijdert uit een service, weerspiegeld in de servicecatalogus.

Wanneer u de service maakt, kunt u deze gebruiken als een servicecategorie zodat u serviceaanbiedingen voor uw servicecatalogusgebruikers kunt samenstellen. Bijvoorbeeld een Windows-bureaubladservice met catalogusitems voor besturingssystemen Windows 7, 8 en 10 of een Linux-service die CentOS- en RHEL-besturingssysteemitems bevat.

Een service toevoegen

Voeg een service toe om catalogusitems beschikbaar te maken voor gebruikers van de servicecatalogus. Alle catalogusitems moeten aan een service worden gekoppeld zodat u rechten voor de items kunt verlenen aan de gebruikers.

Wanneer gebruikers rechten hebben voor de service, worden de catalogusitems samen weergegeven in de servicecatalogus. U kunt ook rechten aan gebruikers verlenen voor de individuele catalogusitems.

Voorwaarden

Meld u aan bij vRealize Automation als een **tenantbeheerder** of **catalogusbeheerder**.

Procedure

1 Selecteer **Beheer > Catalogusbeheer > Services**.

2 Klik op het pictogram **Nieuw (+)**.

3 Voer een naam en een beschrijving in.

Deze waarden verschijnen in de servicecatalogus voor de catalogusgebruikers.

4 Om een specifiek pictogram voor de service aan de servicecatalogus toe te voegen, klikt u op **Bladeren** en selecteert u een afbeelding.

De ondersteunde afbeeldingsbestandtypen zijn GIF, JPG en PNG. De weergegeven afbeelding is 40 x 40 pixels groot. Als u geen aangepaste afbeelding selecteert, wordt het standaardpictogram weergegeven in de servicecatalogus.

5 Selecteer een status in het vervolgkeuzemenu **Status**.

Optie	Beschrijving
Inactief	De service is niet beschikbaar in de servicecatalogus. Wanneer een service deze status heeft, kunt u wel catalogusitems aan de service koppelen, maar kunt u gebruikers geen rechten verlenen voor de service. Als u Inactief selecteert voor een service die actief is en waarvoor rechten zijn verleend, wordt deze verwijderd uit de servicecatalogus totdat u deze opnieuw activeert.
Actief	(Standaard) De service en de gekoppelde catalogusitems zijn beschikbaar om er rechten voor gebruikers aan te verlenen. Zodra de rechten zijn verleend, zijn de service en de gekoppelde catalogusitems beschikbaar in de servicecatalogus voor deze gebruikers.
Verwijderd	Verwijderd de service uit vRealize Automation. Alle gekoppelde catalogusitems zijn nog steeds aanwezig, maar items die gekoppeld zijn aan de service in de servicecatalogus, zijn niet beschikbaar voor de gebruikers van de catalogus.

6 De service-instellingen configureren.

De volgende instellingen bieden informatie aan de gebruikers van de servicecatalogus. De instellingen hebben geen invloed op de servicebeschikbaarheid.

Optie	Beschrijving
Uren	Configureer de tijd die moet samenvallen met de beschikbaarheid van het ondersteuningsteam. De tijd is gebaseerd op uw lokale tijd. De service-uren mogen niet van de ene naar de andere dag doorlopen. U kunt de service-uren bijvoorbeeld niet instellen van 16:00 tot 4:00 uur. Maak twee rechten als u de service ook na middernacht wilt verlenen. Eén recht voor 16:00 tot 24:00 uur en een ander recht voor 24:00 tot 16:00 uur.
Eigenaar	Geef de gebruiker of gebruikersgroep op die de primaire eigenaar is van de service en de gekoppelde catalogusitems.
Ondersteuningsteam	Geef de aangepaste gebruikersgroep of gebruiker op die beschikbaar is om ondersteuning te bieden voor eventuele problemen die de gebruikers van de servicecatalogus ondervinden bij het inrichten van items met behulp van de service.
Venster Wijzigen	Selecteer een datum en tijd waarop u van plan bent om een wijziging in de service te maken. De opgegeven datum en tijd zijn ter informatie en hebben geen invloed op de beschikbaarheid van de service.

7 Klik op **Toevoegen**.

Wat nu te doen

Koppel catalogusitems aan een service zodat u rechten voor de items kunt verlenen aan gebruikers. Zie [Catalogusitems toevoegen aan een service](#).

Catalogusitems toevoegen aan een service

Voeg catalogusitems toe aan services zodat u gebruikers rechten kunt verlenen om de items in de servicecatalogus aan te vragen. Een catalogusitem kan slechts aan één service worden gekoppeld.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **catalogusbeheerder**.
- Controleer of er een service bestaat. Zie [Een service toevoegen](#).
- Controleer of een of meer catalogusitems zijn gepubliceerd. Zie [Een catalogusitem configureren](#).

Procedure

- 1 Selecteer **Beheer > Catalogusbeheer > Services**.
- 2 Selecteer de service waaraan u catalogusitems wilt toevoegen en klik op **Catalogusitems beheren**.
- 3 Klik op het pictogram **Catalogusitems** (+).
 - a Selecteer de catalogusitems die u aan deze service wilt toevoegen.
Het dialoogvenster Catalogusitems selecteren geeft alleen de items weer die nog niet aan een service zijn gekoppeld.
 - b Klik op **Toevoegen**.
- 4 Klik op **Sluiten**.

Wat nu te doen

- U kunt een aangepast pictogram aan het catalogusitem toevoegen dat zal worden weergegeven met het item in de servicecatalogus. Zie [Een catalogusitem configureren](#).
- Verleen rechten voor de services of catalogusitems aan gebruikers zodat zij deze in de servicecatalogus kunnen aanvragen. Zie [Rechten maken](#).

Werken met catalogusitems en acties

Catalogusitems zijn gepubliceerde blueprints voor machines, softwareonderdelen en andere objecten. Acties in het catalogusbeheergebied zijn gepubliceerde acties die u op de ingerichte catalogusitems kunt uitvoeren. U kunt de lijsten gebruiken om te bepalen welke blueprints en acties worden gepubliceerd, zodat u deze beschikbaar kunt maken aan gebruikers van de servicecatalogus.

Gepubliceerde catalogusitems

Een catalogusitem is een gepubliceerde blueprint. Gepubliceerde blueprints kunnen ook worden gebruikt in andere blueprints. Het hergebruik van blueprints in andere blueprints wordt niet weergegeven in de lijst met catalogusitems.

De gepubliceerde catalogusitems kunnen ook items opnemen die alleen onderdelen van blueprints zijn. Gepubliceerde softwareonderdelen worden bijvoorbeeld als catalogusitems weergegeven, maar ze zijn alleen beschikbaar als onderdeel van een implementatie.

Implementatiecatalogusitems moeten worden gekoppeld aan een service, zodat u deze beschikbaar kunt maken in de servicecatalogus voor gebruikers met rechten. Alleen actieve items worden weergegeven in de servicecatalogus. U kunt catalogusitems configureren voor een andere service, ze deactiveren als u ze tijdelijk wilt verwijderen uit de servicecatalogus en er een aangepast pictogram aan toevoegen, dat wordt weergegeven in de catalogus.

Gepubliceerde acties

Acties zijn wijzigingen die u kunt maken in ingerichte catalogusitems. U kunt bijvoorbeeld een virtual machine opnieuw opstarten.

Acties kunnen ingebouwde acties of acties die zijn gemaakt met XaaS omvatten. Ingebouwde acties worden toegevoegd wanneer u een machine toevoegt aan een andere ingerichte blueprint. XaaS-acties moeten worden gemaakt en gepubliceerd.

Acties zijn niet gekoppeld aan services. U moet een actie opnemen in het recht dat het catalogusitem bevat waarop de actie wordt uitgevoerd. Acties die recht hebben op gebruikers worden niet weergegeven in de servicecatalogus. De acties zijn beschikbaar voor het geleverde item op het tabblad **Implementaties** van de servicecatalogusgebruiker, op basis van de vraag of deze van toepassing zijn op het item en op de huidige status van het item.

U kunt een aangepast pictogram toevoegen aan de actie die wordt weergegeven op het tabblad **Implementaties**.

Een catalogusitem configureren

Een catalogusitem is een gepubliceerde blueprint waarvoor u rechten kunt verlenen aan gebruikers. U kunt de opties voor catalogusitems gebruiken om de status of de gekoppelde service te wijzigen. U kunt ook de rechten weergeven die het geselecteerde catalogusitem bevatten.

Alleen catalogusitems die aan een service gekoppeld zijn en waarvoor rechten zijn verleend aan gebruikers, worden in de servicecatalogus weergegeven. Catalogusitems kunnen slechts aan één service worden gekoppeld.

Als u niet wilt dat een catalogusitem in de servicecatalogus wordt weergegeven zonder dit van een recht of de lijst met gepubliceerde catalogusitems te verwijderen, kunt u dit deactiveren. De status van een gedeactiveerd catalogusitem wordt niet langer in het raster weergegeven en is inactief in de configuratiegegevens. U kunt de status later activeren.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **catalogusbeheerder**.
- Controleer of er ten minste een blueprint is gepubliceerd als catalogusitem. Zie [Een blueprint publiceren](#).

Procedure

- 1 Selecteer **Beheer > Catalogusbeheer > Catalogusitems**.
- 2 Selecteer het catalogusitem en klik op **Configureren**.
- 3 Configureer de instellingen voor het catalogusitem.

Optie	Beschrijving
Pictogram	Zoek de gewenste afbeelding. De ondersteunde afbeeldingsbestandstypen zijn GIF, JPG en PNG. De weergegeven afbeelding is 40 x 40 pixels groot. Als u geen aangepaste afbeelding selecteert, wordt het standaard cataloguspictogram weergegeven in de servicecatalogus.
Status	<p>Mogelijke waarden zijn onder andere Actief, Inactief en Fasering.</p> <ul style="list-style-type: none"> ■ Actief Het catalogusitem wordt in de servicecatalogus weergegeven en gebruikers aan wie rechten zijn verleend kunnen het gebruiken om bronnen in te richten. Het item wordt weergegeven in de gepubliceerde lijst met catalogusitems. ■ Inactief Het catalogusitem is niet beschikbaar in de servicecatalogus. Het item wordt weergegeven in de lijst met catalogusitems als Uit de handel genomen. ■ Fasering Het catalogusitem is niet beschikbaar in de servicecatalogus. Selecteer dit menu-item als het item ooit inactief is geweest en u fasering gebruikt om aan te duiden dat u overweegt het opnieuw te activeren. Wordt in de lijst met catalogusitems als Fasering weergegeven.
Quotum	<p>Stel het aantal instanties van dit catalogusitem in dat een gebruiker kan implementeren.</p> <p>Als de gebruiker dit aantal overschrijdt, wordt een melding weergegeven in de catalogusaanvraag en wordt de aanvraag niet ingediend.</p>
Service	Selecteer een service. Alle catalogusitems moeten worden gekoppeld aan een service als u het item wilt weergeven in de servicecatalogus voor gebruikers aan wie rechten zijn verleend. De lijst bevat actieve en inactieve services.

- 4 Als u wilt zien welke rechten er voor het catalogusitem zijn verleend aan gebruikers, klikt u op het tabblad **Rechten**.
- 5 Klik op **Bijwerken**.

Wat nu te doen

- Als u het catalogusitem beschikbaar wilt maken in de servicecatalogus, moet u gebruikers rechten verlenen voor de service die is gekoppeld aan het item of voor het afzonderlijke item. Zie [Rechten maken](#).
- Als u de verwerkingsvolgorde van rechten wilt opgeven, zodat het goedkeuringsbeleid voor afzonderlijke gebruikers correct wordt toegepast, stelt u de prioriteitsvolgorde voor meerdere rechten in voor dezelfde bedrijfsgroep. Zie [Prioriteit geven aan rechten](#).

Een actie voor de servicecatalogus configureren

Een actie is een wijziging of werkstroom die op ingerichte items kan worden uitgevoerd. U kunt een pictogram toevoegen of de rechten weergeven die de geselecteerde actie omvatten.

Een actie is een ingebouwde actie voor een ingerichte machine, netwerk en andere blueprintonderdelen of het is een gepubliceerde XaaS-actie.

De ondersteunde afbeeldingsbestandstypen voor het pictogram zijn GIF, JPG en PNG. De weergegeven afbeelding is 40 x 40 pixels groot. Als u geen aangepaste afbeelding selecteert, verschijnt het standaardactiepictogram op het tabblad **Implementaties**.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **catalogusbeheerder**.
- Controleer of u ten minste één gepubliceerde actie hebt. Zie [Een blueprint publiceren](#) en [Een bronactie publiceren](#).

Procedure

- 1 Selecteer **Beheer > Catalogusbeheer > Acties**.
- 2 Selecteer de gedeelde actie en klik op **Geef details weer** of, bij XaaS-acties, op **Configureren**.
- 3 Zoek de gewenste afbeelding.
- 4 Als u wilt zien welke rechten er voor de actie zijn verleend aan gebruikers, klikt u op het tabblad **Rechten**.
- 5 Klik op **Voltooien**.

Wat nu te doen

[Gebruikers rechten verlenen voor services, catalogusitems en acties](#).

Rechten maken

Rechten bepalen welke items en acties beschikbaar zijn in de servicecatalogus voor de leden van de geselecteerde bedrijfsgroep. Een recht moet actief zijn zodat de items in de servicecatalogus kunnen worden weergegeven. Als u items hebt die bestuurd moeten worden, dan kunt u rechten gebruiken om goedkeuringsbeleidsregels toe te passen op verschillende items.

Om het recht te configureren, moeten de catalogusitems in een service zijn opgenomen. Rechten kunnen meerdere services, catalogusitems van services in andere rechten en acties die u op de geïmplementeerde catalogusitems kunt uitvoeren, bevatten.

Informatie over interactie met rechopties

De manier waarop u rechten configureert, bepaalt wat er in de servicecatalogus wordt weergegeven. De interactie van services, catalogusitems en onderdelen, acties en goedkeuringsbeleid beïnvloedt wat de gebruiker van de servicecatalogus kan aanvragen en hoe goedkeuringsbeleid wordt toegepast.

Houd rekening met de interacties van services, catalogusitems, acties en goedkeuringen wanneer u een recht maakt.

■ **Services in rechten**

Een gerechtigde service werkt als een dynamische groep catalogusitems. Als u een catalogusitem toevoegt aan een gerechtigde service, hoeft u geen aanvullende configuratie te verrichten om het nieuwe catalogusitem beschikbaar te stellen aan de opgegeven gebruikers.

■ **Catalogusitems en onderdelen in rechten**

Catalogusitems waarvoor rechten zijn verleend, zijn blueprints die u kunt aanvragen via de servicecatalogus. Onderdelen waarvoor rechten zijn verleend, zijn onderdelen van de blueprints; u kunt deze echter niet aanvragen via de servicecatalogus.

■ **Acties in rechten**

Acties worden uitgevoerd op geïmplementeerde catalogusitems. Ingerichte catalogusitems en de acties die u daarop mag uitvoeren, verschijnen op het tabblad Implementaties. Om acties uit te voeren op een geïmplementeerd item, moet de actie zijn opgenomen in hetzelfde recht als het catalogusitem dat het item heeft ingericht vanuit de servicecatalogus.

■ **Goedkeuringsbeleid in rechten**

Goedkeuringsbeleid wordt toegepast op rechten, zodat u bronnen in uw omgeving kunt beheren.

Services in rechten

Een gerechtigde service werkt als een dynamische groep catalogusitems. Als u een catalogusitem toevoegt aan een gerechtigde service, hoeft u geen aanvullende configuratie te verrichten om het nieuwe catalogusitem beschikbaar te stellen aan de opgegeven gebruikers.

Als u een goedkeuringsbeleid toepast op een service, worden alle items onderworpen aan hetzelfde goedkeuringsbeleid wanneer ze worden aangevraagd.

Catalogusitems en onderdelen in rechten

Catalogusitems waarvoor rechten zijn verleend, zijn blueprints die u kunt aanvragen via de servicecatalogus. Onderdelen waarvoor rechten zijn verleend, zijn onderdelen van de blueprints; u kunt deze echter niet aanvragen via de servicecatalogus.

Catalogusitems en onderdelen waarvoor rechten zijn verleend, kunnen een van de volgende items bevatten:

Catalogusitems

- Items van een service die u aan gebruikers met rechten wilt leveren, zelfs services die niet zijn opgenomen in het huidige recht.

Stel dat u als catalogusbeheerder verschillende versies van Red Hat Enterprise Linux hebt gekoppeld aan een Red Hat-service en rechten voor de service hebt verleend aan de kwaliteitsingenieurs voor product A. Vervolgens ontvangt u een aanvraag om servicecatalogusitems te maken die alleen betrekking heeft op de laatste versie van Linux-

gebaseerde besturingssystemen voor het trainingsteam. U maakt dan een recht voor het trainingsteam dat de laatste versies bevat van de andere besturingssystemen in een service. U hebt de laatste versie van RHEL al aan een andere service gekoppeld. Daarom voegt u RHEL toe als een catalogusitem in plaats van de volledige Red Hat-service toe te voegen.

- Items die zijn opgenomen in een service die in het huidige recht is opgenomen, maar u wilt een goedkeuringsbeleid toepassen op het individuele catalogusitem dat verschilt van het beleid dat u op de service hebt toegepast.

Stel u bent bedrijfsgroepbeheerder en verleent uw ontwikkelingsteam rechten voor een service met drie VM-catalogusitems. U past een goedkeuringsbeleid toe dat de goedkeuring vereist van de virtual infrastructuurbeheerder voor machines met meer dan vier CPU's. Een van de virtual machines wordt gebruikt voor prestatietesten. Voeg deze daarom toe als catalogusitem en pas een minder beperkend goedkeuringsbeleid toe voor dezelfde groep gebruikers.

Onderdelen

- Onderdelen zijn niet beschikbaar op naam in de servicecatalogus, omdat ze onderdeel zijn van een catalogusitem. U verleent rechten voor afzonderlijke onderdelen, zodat u een specifiek goedkeuringsbeleid kunt toepassen dat afwijkt van het catalogusitem waarvan het deel uitmaakt.

Stel dat een item een machine met software bevat. De machine is beschikbaar als een inrichtbaar item en heeft een goedkeuringsbeleid waarbij goedkeuring van de sitebeheerder is vereist. De software is niet beschikbaar als een stand-alone, inrichtbaar item, alleen als deel van een machineaanvraag, maar het goedkeuringsbeleid voor de software vereist goedkeuring van de softwarelicentiebeheerder van uw organisatie. Wanneer de machine wordt aangevraagd in de servicecatalogus, moet deze worden goedgekeurd door de sitebeheerder en de softwarelicentiebeheerder voordat deze wordt ingericht. Nadat het is ingericht, wordt de machine met de software-invoer weergegeven op het tabblad Implementaties van de aanvrager als onderdeel van de machine.

Acties in rechten

Acties worden uitgevoerd op geïmplementeerde catalogusitems. Ingerichte catalogusitems en de acties die u daarop mag uitvoeren, verschijnen op het tabblad Implementaties. Om acties uit te voeren op een geïmplementeerd item, moet de actie zijn opgenomen in hetzelfde recht als het catalogusitem dat het item heeft ingericht vanuit de servicecatalogus.

Recht 1 bevat bijvoorbeeld een vSphere Virtual Machine en een actie voor het maken van momentopnamen, en recht 2 bevat alleen een vSphere Virtual Machine. Wanneer u een vSphere-machine van recht 1 implementeert, is de actie voor het maken van momentopnamen beschikbaar. Wanneer u een vSphere-machine van recht 2 implementeert, is er geen actie. Om de actie beschikbaar te maken voor gebruikers van recht 2, voegt u de actie voor het maken van momentopnamen toe aan recht 2.

Als u een actie selecteert die niet van toepassing is op een van de catalogusitems in de machtiging, wordt deze niet weergegeven als een actie op het tabblad Implementaties. Uw recht bevat bijvoorbeeld een vSphere-machine en u verleent rechten voor een vernietigingsactie voor een cloudmachine. De vernietigingsactie kan niet worden uitgevoerd op de ingerichte machine.

U kunt een goedkeuringsbeleid toepassen op een actie die verschilt van het beleid dat wordt toegepast op het catalogusitem in het recht.

Als de servicecatalogusgebruiker lid is van meerdere bedrijfsgroepen en slechts een groep het recht heeft om in en uit te schakelen en de andere alleen het recht heeft om te vernietigen, zijn voor die gebruiker de drie acties beschikbaar voor de toepasselijke ingerichte machine.

Beste praktijken om gebruikers rechten te verlenen voor acties

Omdat blueprints gecompliceerd zijn, kan het verlenen van rechten om acties uit te voeren op ingerichte blueprints, tot onverwacht gedrag leiden. Volg de volgende beste praktijken wanneer u gebruikers van de servicecatalogus rechten verleent om acties uit te voeren voor de ingerichte items.

- Wanneer u gebruikers het recht verleent voor de actie Machine vernietigen, moet u ze tevens rechten verlenen voor Implementatie vernietigen. Een ingerichte blueprint is een implementatie.

Een implementatie kan een machine bevatten. Als gebruikers van de servicecatalogus wel gerechtigd zijn om de actie Machine vernietigen uit te voeren maar niet om de implementatie te vernietigen, krijgt een gebruiker die de actie Machine vernietigen uitvoert voor de laatste of enige machine van een implementatie, een bericht te zien met de melding dat hij of zij niet bevoegd is om deze actie uit te voeren. Als ze gerechtigd zijn om beide acties uit te voeren, wordt ook de implementatie uit uw omgeving verwijderd. U gebruikt een beleid met goedkeuring vooraf voor de actie Implementatie vernietigen om de governance voor die actie te beheren. Met dit beleid kan de aangewezen goedkeurder de aanvraag Implementatie vernietigen valideren voordat de actie wordt uitgevoerd.

- Wanneer u gebruikers van de servicecatalogus rechten verleent voor acties zoals Lease wijzigen, Eigenaar wijzigen, Vervallen, Opnieuw configureren en andere acties die zowel voor machines als implementaties gelden, moet u de rechten voor beide acties verlenen.

Goedkeuringsbeleid in rechten

Goedkeuringsbeleid wordt toegepast op rechten, zodat u bronnen in uw omgeving kunt beheren.

U kunt alleen een bestaand goedkeuringsbeleid toepassen op het recht dat u maakt. Maar ook als het gewenste beleid niet bestaat, kunt u het recht maken. Het recht krijgt dan een conceptstatus of inactieve status totdat u het vereiste goedkeuringsbeleid voor de bijbehorende catalogusitems en acties hebt gemaakt en vervolgens toepast.

U bent niet verplicht om een goedkeuringsbeleid toe te passen op een van de items of acties. Als u geen goedkeuringsbeleid toepast, worden de aangevraagde items en acties geïmplementeerd zonder dat er een goedkeuringsaanvraag wordt getriggerd.

Gebruikers rechten verlenen voor services, catalogusitems en acties

Als u een service, catalogusitem of actie toevoegt aan een recht, dan staat u toe dat de gebruikers die in het recht zijn geïdentificeerd, de inrichtbare items in de servicecatalogus kunnen aanvragen. Acties zijn gekoppeld aan items en worden weergegeven op het tabblad **Implementaties** voor de aanvragende gebruiker.

Er zijn verschillende gebruikersrollen die rechten voor bedrijfsgroepen mogen maken.

- Tenantbeheerders kunnen rechten maken voor alle bedrijfsgroepen in hun tenant.
- Bedrijfsgroepbeheerders kunnen rechten maken voor de groepen die zij beheren.
- Catalogusbeheerders kunnen rechten maken voor alle bedrijfsgroepen in hun tenant.

Wanneer u een recht maakt, moet u een bedrijfsgroep en de leden van de bedrijfsgroep selecteren voor het recht.

Raadpleeg [Rechten maken](#) als u wilt begrijpen hoe u een recht maakt, zodat u de interacties van services, catalogusitems en acties met goedkeuringen kunt gebruiken.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **catalogusbeheerder**.
- Controleer of de catalogusitems waarvoor u rechten verleent aan gebruikers, aan een service gekoppeld zijn. Zie [Catalogusitems toevoegen aan een service](#).
- Controleer of de bedrijfsgroep waarvoor u het recht definieert, bestaat en dat de gebruikers en gebruikersgroepen die lid zijn, gedefinieerd zijn. Zie [Een bedrijfsgroep maken](#).
- Controleer of de goedkeuringsbeleidsregels bestaan als u van plan bent om goedkeuringen toe te voegen wanneer u dit recht maakt. Zie [Goedkeuringsbeleid maken](#). Als u aan gebruikers het recht wilt verlenen op items in de servicecatalogus zonder goedkeuringen, kunt u het recht later aanpassen, zodat om goedkeuringen toe te voegen.

Procedure

- 1 Selecteer **Beheer > Catalogusbeheer > Rechten**.
- 2 Klik op het pictogram **Nieuw** (+).
- 3 Configureer de opties in **Details**.

Details bepalen hoe het recht wordt weergegeven in de lijst met rechten en welke gebruikers toegang hebben tot de items in de servicecatalogus.

Optie	Beschrijving
Naam en Beschrijving	Informatie over het recht dat wordt weergegeven in de lijst met rechten.
Vervaldatum	Stel de datum en tijd in als u wilt dat het recht op een bepaalde datum inactief wordt.

Optie	Beschrijving
Status	<p>Mogelijke waarden zijn onder meer: Actief, Inactief en Verwijderd.</p> <ul style="list-style-type: none"> ■ Actief. Items zijn beschikbaar in de servicecatalogus. Deze optie is beschikbaar wanneer u rechten toevoegt of bewerkt. ■ Inactief: items zijn niet beschikbaar in de servicecatalogus. Het recht is gedeactiveerd vanwege de vervaldatum of door een gebruiker. ■ Verwijderd. Het recht wordt verwijderd.
Bedrijfsgroep	<p>Selecteer een bedrijfsgroep. U kunt slechts rechten maken voor één bedrijfsgroep en gebruikers met rechten moeten lid zijn van de bedrijfsgroep.</p> <p>Als u een recht beschikbaar wilt maken voor alle gebruikers, moet u over een gebruikersgroep met alle gebruikers beschikken of moet u rechten maken voor elke bedrijfsgroep.</p> <p>Als u bent aangemeld als een bedrijfsgroepbeheerder, dan kunt u alleen rechten voor uw bedrijfsgroep maken.</p>
Gebruikers en groepen	<p>Selecteer Alle gebruikers en groepen als u aan alle leden van de bedrijfsgroep recht wilt verlenen op de catalogusitems en acties of verleen het recht aan afzonderlijke gebruikers of groepen. Als u een recht wilt activeren, moet u minstens één gebruiker of groep uit de bedrijfsgroep selecteren.</p>

4 Klik op **Volgende**.

- 5 Klik op een pictogram **Nieuw** (+) om met dit recht rechten te verlenen aan gebruikers voor services, catalogusitems of acties.

U kunt een recht maken met verschillende combinaties van de services, items en acties.

Optie	Beschrijving
Services waarvoor rechten zijn verleend	<p>Voeg een service toe wanneer u verleende gebruikerstoegang wilt toestaan tot alle gepubliceerde catalogusitems die zijn gekoppeld aan de service.</p> <p>Een service waarvoor rechten zijn verleend, is een dynamisch recht. Als een item later wordt toegevoegd aan de service, wordt het toegevoegd aan de servicecatalogus voor de gebruikers aan wie rechten zijn verleend. Rechten kunnen zowel services als individuele catalogusitems bevatten.</p>
Catalogusitems en onderdelen waarvoor rechten zijn verleend	<p>Voeg individuele items toe die beschikbaar zijn voor de gebruikers met rechten.</p> <p>Rechten kunnen zowel services als individuele catalogusitems bevatten. Als u een ander goedkeuringsbeleid wilt toepassen op een item dat is opgenomen in de service, voegt u het toe als catalogusitem. Het goedkeuringsbeleid voor een item krijgt voorrang boven het goedkeuringsbeleid voor de service waartoe dit behoort wanneer deze zich in hetzelfde recht bevinden. Als deze zich in verschillende rechten bevinden, wordt de volgorde gebaseerd op de prioriteit die is ingesteld.</p> <p>Catalogusitems moeten aan een service gekoppeld zijn om beschikbaar te zijn in de servicecatalogus. Het catalogusitem kan gekoppeld zijn aan elke service, niet alleen aan een service in het huidige recht.</p> <p>Onderdelen maken deel uit van een catalogusitem, maar zijn niet op naam beschikbaar in de servicecatalogus. Zo is de MySQL-software een onderdeel van een catalogusitem van een CentOS virtual machine. Voor onderdelen worden rechten verleend bij het catalogusitem. Als u goedkeuringsbeleid wilt toepassen dat specifiek voor de software is, kunt u voor het afzonderlijke item rechten verlenen. Anders hoeft u geen rechten voor een onderdeel te verlenen om dit onderdeel te kunnen implementeren bij het bovenliggende item.</p>
Acties waarvoor rechten zijn verleend	<p>Voeg acties toe als u gebruikers wilt toestaan om de acties voor een ingericht item uit te voeren.</p> <p>Acties die u wilt uitvoeren op de items die vanaf dit recht zijn ingericht, moeten in hetzelfde recht worden opgenomen.</p> <p>Acties waarvoor rechten zijn verleend, worden niet weergegeven in de servicecatalogus. Ze worden weergegeven op het tabblad Implementaties voor een ingericht item.</p>
Acties zijn alleen van toepassing op items die zijn gedefinieerd in dit recht	<p>Hiermee wordt bepaald of de acties met rechten in aanmerking komen voor alle van toepassing zijnde servicecatalogusitems in deze rechten.</p> <p>Als deze optie is ingeschakeld, zijn er rechten verleend op de acties aan de leden van de bedrijfsgroep voor de toepasselijke items in dit recht. Via deze methode om rechten te verlenen op acties, kunt u acties opgeven voor de specifieke items.</p> <p>Als deze optie niet wordt ingeschakeld, wordt het recht voor de acties verleend aan de gebruikers die in het recht zijn opgegeven voor alle toepasselijke catalogusitems, ongeacht of dezelfde items in dit recht zijn opgenomen. Eventueel op deze acties toegepast goedkeuringsbeleid is ook actief.</p>

- 6 Gebruik de vervolgkeuzemenu's in elke sectie om de beschikbare items te filteren.
- 7 Schakel de selectievakjes in om items in het recht op te nemen.
- 8 Als u een goedkeuringsbeleid wilt toevoegen aan geselecteerde services, items of acties, selecteert u een goedkeuringsbeleid in het vervolgkeuzemenu **Dit beleid toepassen op geselecteerde items**.

Als u een goedkeuringsbeleid toepast op een service, hebben alle items in de service hetzelfde goedkeuringsbeleid. Als u een ander beleid op een item wilt toepassen, dan voegt u dit toe als een catalogusitem en past u het goedkeuringsbeleid toe.

- 9 Klik op **OK**.

De service, het item of de actie wordt aan het recht toegevoegd.

- 10 Klik op **Voltooien** om het recht op te slaan.

Resultaten

Als de status van het recht actief is, worden de service en items aan de servicecatalogus toegevoegd.

Wat nu te doen

Controleer of de services en catalogusitems met rechten in de servicecatalogus voor de gebruikers met rechten worden weergegeven, en dat de aangevraagde items de doelobjecten zoals verwacht inrichten. U kunt het item aanvragen namens de geselecteerde gebruikers.

Prioriteit geven aan rechten

Als er meerdere rechten bestaan voor dezelfde bedrijfsgroep, kunt u verschillende prioriteiten geven aan rechten, zodat op het moment dat een gebruiker van een servicecatalogus een aanvraag plaatst, de rechten en het bijbehorende goedkeuringsbeleid worden verwerkt in de opgegeven volgorde.

Als u een goedkeuringsbeleid voor een gebruikersgroep configureert en als u wilt dat een groepslid over een uniek beleid voor één of meer services, catalogusitems of acties kan beschikken, kunt u het recht van dit lid prioriteit geven boven het recht van de groep. Wanneer het lid een item uit de servicecatalogus aanvraagt, wordt het toegepaste goedkeuringsbeleid gebaseerd op de prioriteitsvolgorde van de rechten voor de bedrijfsgroep. De eerste keer dat de naam van het lid wordt aangetroffen, als onderdeel van een aangepaste gebruikersgroep of als een afzonderlijke gebruiker, wordt het bijbehorende goedkeuringsbeleid gebruikt.

Als u bijvoorbeeld twee rechten maakt voor hetzelfde catalogusitem, zodat u het ene recht kunt toepassen voor de gebruikersgroep Accounting en een ander recht voor Chris, een lid van die groep.

Tabel 3-71. Voorbeeld van rechten

Recht 1	Recht 2
Bedrijfsgroep: Financiën	Bedrijfsgroep: Financiën
Gebruikers en groepen: Accounting	Gebruikers en groepen: Chris
Catalogusitem 1: beleid A	Catalogusitem 1: beleid C

Chris vraagt Catalogusitem 1 uit de servicecatalogus aan. Afhankelijk van de volgorde van de rechten voor de bedrijfsgroep Financiën, wordt een ander beleid toegepast op de aanvraag van Chris.


Tabel 3-72. Voorbeeld van resultaten

Configuratie en resultaat	Prioriteitsvolgorde	Prioriteitsvolgorde
Prioriteitsvolgorde	1: Recht 1 2: Recht 2	1: Recht 2 2: Recht 1
Toegepast beleid	Beleid A wordt toegepast Chris is een lid van de gebruikersgroep Accounting. De zoekopdracht naar Chris als een gebruiker met rechten stopt bij Recht 1 en het bijbehorende goedkeuringsbeleid wordt toegepast.	Beleid C wordt toegepast De zoekopdracht naar Chris als een gebruiker met rechten stopt bij Recht 2 en het bijbehorende goedkeuringsbeleid wordt toegepast.

Voorwaarden

Meld u aan bij vRealize Automation als een **tenantbeheerder** of **catalogusbeheerder**.

Procedure

- 1 Selecteer **Beheer > Catalogusbeheer > Rechten**.
- 2 Klik op het pictogram **Prioriteit geven** ().
- 3 Selecteer een bedrijfsgroep in het vervolgkeuzelijst **Bedrijfsgroep**.
- 4 Sleep een recht naar een nieuwe locatie in de lijst om de prioriteit te wijzigen.
- 5 Selecteer een bijwerkmethode.

Optie	Beschrijving
Bijwerken	Uw wijzigingen worden opgeslagen.
Bijwerken en sluiten	Uw wijzigingen worden opgeslagen en het venster Prioriteit geven aan rechten wordt gesloten.

Werken met goedkeuringsbeleid

U kunt goedkeuringsbeleid als governance toevoegen aan aanvragen voor de servicecatalogus zodat u de bronnen in uw omgeving kunt beheeren. Elk beleid bestaat uit een reeks voorwaarden die u kunt toepassen op services, catalogusitems en acties, en geldt voor gebruikers die u rechten verleent voor die items.

Proces voor goedkeuringsbeleid

Om te beginnen maakt een tenantbeheerder of goedkeuringsbeheerder goedkeuringsbeleid om de inrichting waar nodig te reguleren.

Goedkeuringsbeleid wordt gemaakt voor beleidstypen of specifieke items. Als u het beleid baseert op een beleidstype, kunt u het toepassen op overeenkomende typen catalogusitems. Als u het beleid bijvoorbeeld baseert op een softwarebeleidstype, kunt u het gedefinieerde beleid toepassen op alle software-items in de verleende rechten. Als het beleid voor een specifiek item is bedoeld, moet u het uitsluitend op dat item toepassen. Als het item bijvoorbeeld een specifiek software-item is, moet u het alleen toepassen op dat specifieke databasesoftware-item in de verleende rechten.

Het beleid kan goedkeuring vooraf of achter vereisen. Bij goedkeuring vooraf moet de aanvraag eerst goedgekeurd zijn voordat het aangevraagde item kan worden ingericht. Wanneer de goedkeuring achteraf plaatsvindt, moet de goedkeurder de aanvraag accepteren voordat het ingerichte item beschikbaar wordt gesteld aan de aanvrager.

De configuraties met goedkeuring vooraf en achteraf hebben een of meer niveaus die bepalen wanneer het goedkeuringsbeleid wordt geactiveerd en hoe en door wie de aanvraag wordt goedgekeurd. U kunt meerdere niveaus toevoegen. Een goedkeuringsbeleid kan bijvoorbeeld een niveau voor goedkeuring door een beheerder hebben, gevolgd door een niveau voor financiële goedkeuring.

Vervolgens wordt het goedkeuringsbeleid door een tenantbeheerder of bedrijfsgroepbeheerder toegepast op services, catalogusitems en acties.

Wanneer een gebruiker van een servicecatalogus ten slotte een item aanvraagt waarop een goedkeuringsbeleid wordt toegepast, keuren de goedkeurders de aanvraag goed of verwerpen deze op hun tabblad **Inbox**. De aanvragende gebruiker kan de goedkeuringsstatus voor een specifieke aanvraag volgen op het tabblad **Implementaties**.

Voorbeelden van goedkeuringsbeleid op basis van beleidstypen voor virtual machines

U kunt een goedkeuringsbeleid toepassen op dezelfde itemtypen in de catalogus, maar toch verschillend laten uitwerken wanneer een item in de servicecatalogus wordt aangevraagd. De uitwerking van het goedkeuringsbeleid op de gebruiker van de servicecatalogus en de goedkeurder verschilt afhankelijk van de wijze waarop u het hebt gedefinieerd en toegepast.

De volgende tabel bevat voorbeelden van verschillende goedkeuringsregels die allemaal zijn gebaseerd op hetzelfde type goedkeuringsbeleid. Dit zijn slechts een paar voorbeelden van de wijze waarop u goedkeuringsregels kunt configureren om verschillende soorten bestuurlijke controle mogelijk te maken.

Tabel 3-73. Voorbeelden van goedkeuringsbeleid en resultaten

Bestuurlijk doel	Geselecteerd beleidstype	Voor of na goedkeuring	Wanneer is goedkeuring vereist?	Wie zijn de goedkeurders?	Hoe wordt het beleid toegepast op de verleende rechten?	Resultaat wanneer het item wordt aangevraagd in de servicecatalogus
De bedrijfsgroep beheerder moet alle aanvragen van virtual machines goedkeuren. Het goedkeuringsbeleid moet toepasbaar zijn op meerdere bedrijfsgroepen in meerdere rechten.	Servicecatalogus - Aanvraag catalogusitem - Virtual machine	Toevoegen aan het tabblad Goedkeuring vooraf	Selecteer Altijd vereist	Selecteer Goedkeurders van de aanvraag bepalen. Selecteer de voorwaarde Bedrijfsgroep > Beheerders > Gebruikers > beheerder. Selecteer Goedkeuring door willekeurige personen mogelijk.	Rechten zijn op bedrijfsgroep en gebaseerd. Deze goedkeuring kan worden gebruikt voor alle rechten die goedkeuring van een beheerder vereisen voor de virtual machine.	Wanneer de gebruiker van de servicecatalogus een virtual machine aanvraagt die dit type goedkeuring vereist, moet de bedrijfsgroepbeheerder de aanvraag goedkeuren voordat de machine kan worden ingericht.
De beheerder van de virtuele infrastructuur moet controleren of de virtual machine goed is ingericht en de aanvraag goedkeuren voordat de virtual machine wordt vrijgegeven aan de aanvrager.	Servicecatalogus - Aanvraag catalogusitem - Virtual machine	Toevoegen aan het tabblad Goedkeuring achteraf	Selecteer Altijd vereist	Selecteer Specifieke gebruikers en groepen. Selecteer de aangepaste gebruikersgroep van de beheerder van de virtuele infrastructuur. Selecteer Goedkeuring door willekeurige personen mogelijk.	Deze goedkeuring is geschikt voor alle rechten waarbij u de virtual machine op de vCenter Server na de inrichting wilt laten controleren door de beheerder van de virtuele infrastructuur.	Wanneer de gebruiker van de servicecatalogus een virtual machine aanvraagt die dit type goedkeuring vereist, kan de machine worden ingericht. Als elk lid van de VI-beheergroep deze aanvraag heeft goedgekeurd, wordt de machine vrijgegeven voor de gebruiker.

Tabel 3-73. Voorbeelden van goedkeuringsbeleid en resultaten (vervolg)

Bestuurlijk doel	Geselecteerd beleidstype	Voor of na goedkeuring	Wanneer is goedkeuring vereist?	Wie zijn de goedkeurders?	Hoe wordt het beleid toegepast op de verleende rechten?	Resultaat wanneer het item wordt aangevraagd in de servicecatalogus
Voor het beheer van de virtuele infrastructuur bronnen en het beheersen van de prijzen, voegt u twee niveaus van goedkeuring vooraf toe. De ene goedkeuring is voor machinebronnen en de andere voor de dagelijkse machineprijzen.	Servicecatalogus - Aanvraag catalogusitem - Virtual machine	Toevoegen aan het tabblad Goedkeuring vooraf	Niveau 1 Selecteer Voorwaardelijk vereist . Configureer de voorwaarden voor CPU's > 6 of Geheugen > 8 of Opslag > 100 GB.	Selecteer Goedkeurders van de aanvraag bepalen . Selecteer de voorwaarde Aangevraagd door > beheerder. Selecteer . Klik op Systeemeigenschappen en selecteer CPU's . Geheugen en Opslag zodat de goedkeurder de waarde op een acceptabel niveau kan instellen.	Dit goedkeuringsbeleid is geschikt voor rechten waarbij u de aanvraag wilt laten goedkeuren door de manager van de aanvrager en een lid van de financiële afdeling.	Wanneer de gebruiker van de servicecatalogus een virtual machine aanvraagt, wordt de aanvraag geëvalueerd om te bepalen of de waarden voor CPU's, geheugen en opslag de opgegeven waarden bij niveau 1 niet overschrijden. Als dat het geval is, wordt de voorwaarde op niveau 2 geëvalueerd. Als de aanvraag ten minste één van de voorwaarden voor niveau 1 overschrijdt, moet de beheerder de aanvraag goedkeuren. De beheerder heeft dan de keuze om de waarden voor de aanvraag te verlagen en deze vervolgens goed te keuren, of de

Tabel 3-73. Voorbeelden van goedkeuringsbeleid en resultaten (vervolg)

Bestuurlijk doel	Geselecteerd beleidstype	Voor of na goedkeuring	Wanneer is goedkeuring vereist?	Wie zijn de goedkeurders?	Hoe wordt het beleid toegepast op de verleende rechten?	Resultaat wanneer het item wordt aangevraagd in de servicecatalogus
			Niveau 2 Selecteer Voorwaardelijk vereist. Configureer de voorwaarde Prijs > 15,00 per dag.	Selecteer Specifieke gebruikers en groepen. Selecteer de aangepaste gebruikersgroep voor financiën. Selecteer Goedkeuring door willekeurige personen mogelijk.		aanvraag in zijn geheel af te wijzen.
Voor geparameteris eerde blueprintcatalogusitems moet een cloudbeheerder implementatie aanvragen goedkeuren waarin een vSphere-machineonderdeelprofiel van size is ingesteld op Large.	Servicecatalogus - Aanvraag catalogusitem - Virtual machine	Toevoegen aan het tabblad Goedkeuring vooraf	Niveau 1 Selecteer Voorwaardelijk vereist. Niveau 2 Selecteer Enkele voorwaarde. Selecteer Onderdeelprofielen > vSphere-machinegrootte. Configureer de voorwaardegrootte = large.	Selecteer Specifieke gebruikers en groepen. Selecteer gebruikers en groepen die de aanvraag mogen goedkeuren. Selecteer Goedkeuring door willekeurige personen mogelijk.	Dit goedkeuringsbeleid is geschikt voor rechten waarbij u wilt dat de inrichtingsaanvraag wordt goedgekeurd door een cloudbeheerder.	Wanneer de gebruiker van de servicecatalogus een virtuele machine aanvraagt die dit type goedkeuring vereist, moet een cloudbeheerder de aanvraag goedkeuren voordat de machine kan worden ingericht.

Voorbeeld van acties waarop goedkeuringsbeleid is toegepast in een samengestelde implementatie

Wanneer u goedkeuringsbeleid toepast op acties die kunnen worden uitgevoerd voor verschillende onderdelen in een samengestelde blueprint, varieert het goedkeuringsproces afhankelijk van de manier waarop het recht is geconfigureerd en hoe het goedkeuringsbeleid wordt toegepast.

Dit voorbeeld maakt gebruik van specifieke details voor het bouwen van de blueprint en past vervolgens goedkeuringsbeleid toe op acties die u vanuit de servicecatalogus voor de ingerichte blueprint in verschillende rechten kunt uitvoeren. De blueprint is een samengestelde blueprint die een andere blueprint bevat. De acties worden gebruikt om de ingerichte items te vernietigen, om een implementatie voor de blueprints te vernietigen en een virtuele machine voor de machine te vernietigen. Het resulterende gedrag omvat wat wordt vernietigd en wanneer het toegepaste goedkeuringsbeleid goedkeuringsaanvragen activeert.

Voorbeeldblueprint

In dit voorbeeld configureert u een blueprint die een geneste blueprint met een virtuele machine bevat.

- Blueprint 1 - blueprint voor voortdurende integratie
 - Blueprint 2 - Blueprint vóór productie
 - Virtual Machine 1 - TestAsAService vSphere VM

Goedkeuringsbeleid voor acties Vernietigen

U configureert de twee instanties van goedkeuringsbeleid voor het vernietigen van ingerichte items. Een actie Vernietigen - Implementatie kan worden uitgevoerd op Blueprint 1 of Blueprint 2 in dit voorbeeld. Een actie Vernietigen - Virtual machine kan worden uitgevoerd op Virtual Machine 1. U maakt het goedkeuringsbeleidsinstanties zodat u deze kunt toepassen op de acties in het recht.

Naam van goedkeuringsbeleid	Type goedkeuringsbeleid
Goedkeuringsbeleid A	Servicecatalogus - Bronactieaanvraag - Vernietigen - Implementatie
Goedkeuringsbeleid B	Servicecatalogus - Bronactieaanvraag - Vernietigen - Virtual machine

Rechten en goedkeuringsbeleid toegepast op acties

U configureert drie rechten. Elk recht bevat de samengestelde blueprint. In elk recht voegt u de acties voor vernietigen toe en op elk recht past u het goedkeuringsbeleid toe.

Naam van recht	Actie waaraan recht is verleend op ingerichte machine	Toegepast goedkeuringsbeleid
Recht 1	Vernietigen - Implementatie	Goedkeuringsbeleid A
Recht 2	Vernietigen - Virtual machine	Goedkeuringsbeleid B
Recht 3	Vernietigen - Implementatie	Goedkeuringsbeleid A
	Vernietigen - Virtual machine	Goedkeuringsbeleid B

Gebruikersacties in de servicecatalogus

Wanneer de servicecatalogusgebruiker de actie uitvoert, worden blueprints of machines vernietigd afhankelijk van voor welk item de gebruiker de actie heeft uitgevoerd.

Gebruikersactie in de servicecatalogus	Geselecteerde actie	Vernietigde blueprints of machines
Actie 1	Actie Vernietigen - Implementatie wordt uitgevoerd op Blueprint 1 - Blueprint voor voortdurende integratie	Blueprint 1, Blueprint 2 en Virtual Machine 1
Actie 2	Actie Vernietigen - Implementatie wordt uitgevoerd op de geneste Blueprint 2 - Blueprint vóór productie	Blueprint 2 en Virtual Machine 1
Actie 3	Actie Vernietigen - Virtual machine wordt uitgevoerd op de machine die zich binnen een implementatie bevindt, Virtual Machine 1 - TestAsAService vSphere VM	Virtual Machine 1

Goedkeuringsbeleid toegepast op acties in de rechten

U past het goedkeuringsbeleid toe, de goedkeurders ontvangen een goedkeuringsaanvraag afhankelijk van de blueprint of machine waarop de gebruiker van de servicecatalogus de actie heeft uitgevoerd.

Naam van recht	Goedkeuringsbeleid voor acties	Gebruikersactie	Geactiveerde goedkeuringsaanvraag	Indien goedgekeurd, vernietigde blueprints of machines
Recht 1 - Goedkeuringsbeleid Implementatie vernietigen	Beleid A (Goedkeuringsbeleid Implementatie vernietigen) alleen op actie Vernietigen - Implementatie	Actie 1 (Actie Vernietigen - Implementatie uitvoeren op Blueprint 1)	Goedkeuringsaanvragen worden alleen geactiveerd voor Blueprint 1	Blueprint 1, Blueprint 2 en Virtual Machine 1
		Actie 2 (Actie Vernietigen - Implementatie uitvoeren op Blueprint 2)	Goedkeuringsaanvragen worden alleen geactiveerd voor Blueprint 2	Blueprint 2 en Virtual Machine 1
		Actie 3 (Actie Vernietigen - Virtual machine kan wordt uitgevoerd op Virtual Machine 1)	Geen goedkeuringsaanvragen worden geactiveerd	Virtual Machine 1
Recht 2	Beleid B (Beleid Vernietigen - Virtual Machine) alleen op actie Vernietigen - Virtual machine	Actie 1 (Actie Vernietigen - Implementatie uitvoeren op Blueprint 1)	Geen goedkeuringsaanvragen worden geactiveerd	Blueprint 1, Blueprint 2 en Virtual Machine 1
		Actie 2 (Actie Vernietigen - Implementatie uitvoeren op Blueprint 2)	Geen goedkeuringsaanvragen worden geactiveerd	Blueprint 2 en Virtual Machine 1

Naam van recht	Goedkeuringsbeleid voor acties	Gebruikersactie	Geactiveerde goedkeuringsaanvraag	Indien goedgekeurd, vernietigde blueprints of machines
		Actie 3 (Actie Vernietigen - Virtual machine kan wordt uitgevoerd op Virtual Machine 1)	Goedkeuringsaanvragen worden alleen geactiveerd voor Virtual Machine 1	Virtual Machine 1
Recht 3	Beleid A (Goedkeuringsbeleid Implementatie vernietigen) op actie Vernietigen - Implementatie en Beleid B (Beleid Vernietigen - Virtual Machine) op actie Vernietigen - Virtual Machine	Actie 1 (Actie Vernietigen - Implementatie uitvoeren op Blueprint 1)	Goedkeuringsaanvragen worden alleen geactiveerd voor Blueprint 1	Blueprint 1, Blueprint 2 en Virtual Machine 1
		Actie 2 (Actie Vernietigen - Implementatie uitvoeren op Blueprint 2)	Goedkeuringsaanvragen worden alleen geactiveerd voor Blueprint 2	Blueprint 2 en Virtual Machine 1
		Actie 3 (Actie Vernietigen - Virtual machine kan wordt uitgevoerd op Virtual Machine 1)	Goedkeuringsaanvragen worden alleen geactiveerd voor Virtual Machine 1	Virtual Machine 1

Voorbeeld van een goedkeuringsbeleid bij meerdere rechten

Als u goedkeuringsbeleid toepast op een item dat wordt gebruikt voor meerdere rechten die aan dezelfde gebruikers in een bedrijfsgroep worden verleend, wordt het goedkeuringsbeleid geactiveerd voor het item, en dat zelfs in een service waarop het goedkeuringsbeleid niet expliciet door het recht wordt toegepast.

U kunt bijvoorbeeld de volgende blueprints, services en rechten en het volgende goedkeuringsbeleid maken.

Blueprints

- RHEL vSphere virtual machine
- QE Testing omvat RHEL vSphere virtual machine
- QE Training omvat RHEL vSphere virtual machine

Services

- De QE Testing-blueprint wordt gekoppeld aan de Testing-service

- De QE Training-blueprint wordt gekoppeld aan de Testing-service

Rechten

- Recht 1
- Recht 2

Tabel 3-74. Configuratie van rechten

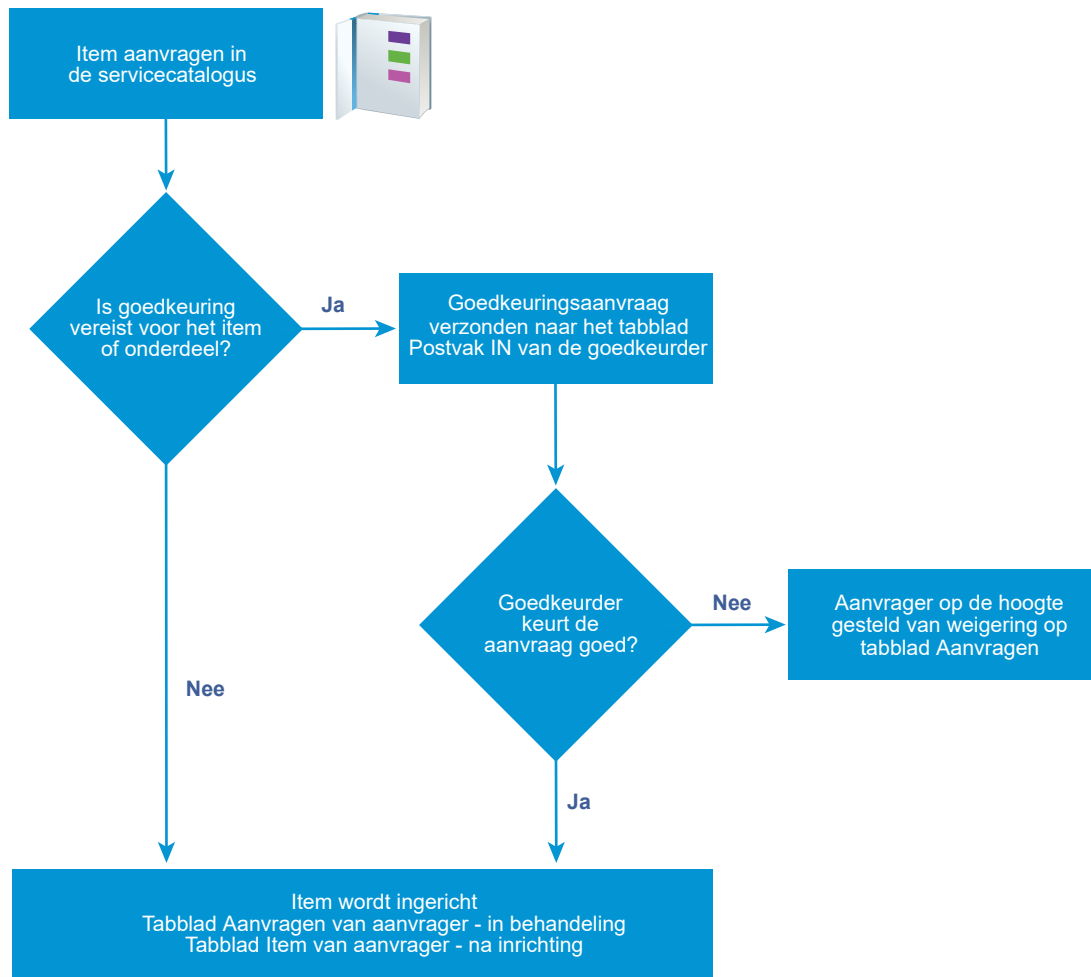
Naam van recht	Bedrijfsgroep	Service waarvoor rechten zijn verleend	Item waarvoor rechten zijn verleend
Recht 1	QE	Testing	Catalogusitemaanvraag - Virtual Machine toegepast op onderdeel Virtual Machine
Recht 2	QE	Training	

Resultaten

Wanneer de gebruiker QE Training selecteert in de servicecatalogus, wordt het goedkeuringsbeleid geactiveerd voor RHEL vSphere virtual machine omdat het een blueprint is die is gebaseerd op het onderdeel Virtual Machine dat wordt gebruikt in de QE Training-blueprint.

Goedkeuringsbeleid verwerken in de servicecatalogus

Wanneer een gebruiker een item in de servicecatalogus aanvraagt waarop goedkeuringsbeleid is toegepast, wordt de aanvraag verwerkt door de goedkeurder en de aanvragende gebruiker, op een manier die vergelijkbaar is met de volgende werkstroom.



Goedkeuringsbeleid maken

Tenantbeheerders en goedkeuringsbeheerders kunnen goedkeuringsbeleid definiëren en gebruiken in rechten. U kunt het goedkeuringsbeleid configureren met meerdere niveaus voor pre-goedkeurings- en post-goedkeuringsgebeurtenissen.

Als u een instelling in een softwareonderdeelblueprint wijzigt en het goedkeuringsbeleid de betreffende instelling gebruik om een goedkeuringsaanvraag te activeren, werkt het goedkeuringsbeleid mogelijk niet zoals verwacht. Als u een instelling in een onderdeel moet wijzigen, moet u controleren of de wijzigingen geen invloed hebben op een of meer goedkeuringsbeleidinstanties.

Voorwaarden

Meld u aan bij vRealize Automation als een **tenantbeheerder** of **goedkeuringsbeheerder**.

Procedure

1 Informatie voor goedkeuringsbeleid opgeven

Wanneer u een goedkeuringsbeleid maakt, definieert u het type, de naam, de beschrijving en de status van het goedkeuringsbeleid.

2 Een goedkeuringsniveau maken

Wanneer u een goedkeuringsbeleid maakt, kunt u niveaus voor pre- en post-goedkeuring toevoegen.

3 Het goedkeuringsformulier configureren voor het toevoegen van systeem- en aangepaste eigenschappen

U kunt systeem- en aangepaste eigenschappen toevoegen die op een goedkeuringsformulier worden weergegeven. U voegt deze eigenschappen toe zodat de goedkeurders de waarden van de systeemeigenschappen voor machine-resource-instellingen, zoals CPU of geheugen, en aangepaste eigenschappen kunnen wijzigen voordat ze een goedkeuringsverzoek voltooien.

4 Instellingen voor goedkeuringsbeleid

Wanneer u een goedkeuringsbeleid maakt, configureert u verschillende opties die bepalen wanneer een item dat is aangevraagd door een servicecatalogusgebruiker moet worden goedgekeurd. De goedkeuring kan vereist zijn voordat inrichting op basis van de aanvraag plaatsvindt of nadat het item is ingericht, maar voordat het wordt vrijgegeven aan de gebruiker die de aanvraag heeft ingediend.

Informatie voor goedkeuringsbeleid opgeven

Wanneer u een goedkeuringsbeleid maakt, definieert u het type, de naam, de beschrijving en de status van het goedkeuringsbeleid.

Voorwaarden

Meld u aan bij vRealize Automation als een **tenantbeheerder** of **goedkeuringsbeheerder**.

Procedure

- 1 Selecteer **Beheer > Goedkeuringsbeleid**.
- 2 Klik op het pictogram **Nieuw (+)**.

3 Selecteer een beleidstype of softwareonderdeel.

Optie	Beschrijving
Een goedkeuringsbeleidtype selecteren	<p>Maak een goedkeuringsbeleid op basis van het type beleidsaanvraag.</p> <p>Selecteer deze optie om een goedkeuringsbeleid te definiëren dat kan worden toegepast op alle catalogusitems van dat type. Het aanvraagtype kan een algemene aanvraag, een aanvraag voor een catalogusitem of een bronactie zijn.</p> <p>De beschikbare configuratieopties van de voorwaarden verschillen op basis van het type. Hoe specifieker het type is, des te specifieker de configuratievelden zijn. Servicecatalogus - Aanvraag catalogusitem biedt bijvoorbeeld alleen de velden die gemeenschappelijk zijn voor alle catalogusitemaanvragen, maar voor Servicecatalogus - Aanvraag catalogusitem - Virtual machine worden ook de algemene opties en de voor virtual machines specifieke opties weergegeven.</p> <p>Het aanvraagtype beperkt de catalogusitems of acties waarop u het goedkeuringsbeleid kunt toepassen.</p>
Een item selecteren	<p>Maak een goedkeuringsbeleid op basis van een specifiek item.</p> <p>Selecteer deze optie voor het definiëren van een goedkeuringsbeleid dat kan worden toegepast op specifieke items die niet beschikbaar zijn als afzonderlijke items in de servicecatalogus, maar alleen als onderdeel van een machine of andere implementatie. Dit zijn bijvoorbeeld softwareonderdelen.</p> <p>De beschikbare configuratievelden voor de voorwaarden zijn specifiek voor het item en kunnen gedetailleerder zijn dan de criteria die voor een beleidstype-item worden geboden.</p>
Lijst	<p>Geeft het beschikbare beleidstype of catalogusitems weer.</p> <p>Doorzoek of sorteer de kolommen om een specifiek item of type te vinden.</p>

4 Klik op **OK**.

5 Voer een naam in en desgewenst een beschrijving.

6 Selecteer de status van het beleid in het vervolgkeuzemenu **Status**.

Optie	Beschrijving
Concept	Slaat het goedkeuringsbeleid op in een bewerkbare status.
Actief	Slaat het goedkeuringsbeleid op in een alleen-lezen status die u kunt gebruiken in een recht.
Inactief	Slaat het goedkeuringsbeleid op in een alleen-lezen status die u niet kunt gebruiken in een recht totdat u het beleid activeert.

Wat nu te doen

Maak de niveaus voor vóór en na de goedkeuring.

Een goedkeuringsniveau maken

Wanneer u een goedkeuringsbeleid maakt, kunt u niveaus voor pre- en post-goedkeuring toevoegen.

U kunt meerdere goedkeuringsniveaus maken voor een goedkeuringsbeleid. Wanneer een servicecatalogusgebruiker een item aanvraagt waarop een goedkeuringsbeleid met meerdere niveaus is toegepast, moet het eerste niveau worden geaccepteerd voordat de goedkeuringsaanvraag naar de volgende goedkeurder wordt verzonden. Zie [Werken met goedkeuringsbeleid](#).

Als u een goedkeuringsbeleid dat wordt getriggerd door een aanvraag m.b.t. de duur van de lease configureert, moet u **Altijd vereist** als de goedkeuringsvereiste selecteren.

Voorwaarden

[Informatie voor goedkeuringsbeleid opgeven.](#)

Procedure

- 1 Klik op het tabblad **Goedkeuring vooraf** of **Goedkeuring achteraf** op het pictogram **Nieuw** (+).
- 2 Voer een naam in en desgewenst een beschrijving.
- 3 Selecteer een goedkeuringsvereiste.

Optie	Beschrijving
Altijd vereist	Het goedkeuringsbeleid wordt voor elke aanvraag geactiveerd.
Voorwaardelijk vereist	<p>Het goedkeuringsbeleid wordt gebaseerd op een of meer voorwaardecomponenten.</p> <p>Als u deze optie selecteert, moet u de voorwaarden maken. Wanneer dit goedkeuringsbeleid wordt toegepast op in aanmerking komende services, catalogusitems of acties in een recht, worden de voorwaarden geëvalueerd. Als aan de voorwaarden wordt voldaan, moet de aanvraag worden goedgekeurd via de opgegeven goedkeurdersmethode voordat inrichting plaatsvindt. Als niet aan de voorwaarden wordt voldaan, vindt inrichting naar aanleiding van de aanvraag zonder goedkeuring plaats. Een aanvraag voor een virtuele machine met 4 of meer CPU's moet bijvoorbeeld worden goedgekeurd door de virtuele-infrastructuurbeheerder.</p> <p>De beschikbaarheid van de velden waarop de voorwaarden worden gebaseerd, wordt bepaald door het geselecteerde type goedkeuringsbeleid of het catalogusitem.</p> <p>Wanneer u een waarde invoert voor een voorwaarde, moet u er rekening mee houden dat deze hoofdlettergevoelig zijn.</p> <p>Als u meer dan een voorwaardecomponent wilt configureren, selecteert u de Boole-bewerking voor de componenten.</p>

4 Selecteer de goedkeurders.

Optie	Actie
Specifieke gebruikers en groepen	Hiermee wordt de goedkeuringsaanvraag naar de geselecteerde gebruikers verzonden.
Goedkeurders van de aanvraag bepalen	<p>Hiermee wordt de goedkeuringsaanvraag naar de gebruikers verzonden op basis van de gedefinieerde voorwaarde.</p> <p>Opmerking Zorg ervoor dat alle gebruikers die dynamisch worden bepaald door de aanvraag en aanvrager aanwezig zijn in vRealize Automation, dat ze worden gesynchroniseerd in de Active Directory en dat ze kunnen worden bekeken via Beheer > Gebruiker en groepen > Directory-gebruikers en -groepen.</p> <p>Als een gebruiker niet wordt gesynchroniseerd in de identiteitsprovider van Beheer van directory's en er op een of andere manier naar deze gebruiker wordt verwezen tijdens de catalogusaanvraag, zal de aanvraag mislukken met de fout Goedkeuring van item vereist.</p>
Gebeurtenisabonnement gebruiken	<p>Hiermee wordt de goedkeuringsaanvraag verwerkt op basis van gedefinieerde gebeurtenisabonnementen.</p> <p>Het werkstroomabonnement moet worden opgegeven in Beheer > Gebeurtenissen > Abonnementen. De toepasselijke werkstroomabonnementen zijn pre-goedkeuring en post-goedkeuring.</p>

5 Geef aan wie de aanvraag of actie moet goedkeuren.

Optie	Beschrijving
Goedkeuring door willekeurige personen mogelijk	<p>Slechts een van de goedkeurders hoeft de aanvraag goed te keuren voordat deze kan worden verwerkt.</p> <p>Wanneer het item wordt aangevraagd in de servicecatalogus, worden goedkeuringsaanvragen naar alle goedkeurders verzonden. Als een van de goedkeurders de aanvraag goedkeurt, wordt de aanvraag goedgekeurd en wordt de goedkeuringsaanvraag verwijderd uit het Postvak IN van de andere goedkeurders.</p>
Goedkeuring van iedereen nodig	Alle goedkeurders moeten de aanvraag goedkeuren voordat deze kan worden verwerkt.

6 Voeg eigenschappen toe aan een goedkeuringsformulier of sla het niveau op.

- Klik op **Systeemeigenschappen** of **Aangepaste eigenschappen** als u eigenschappen wilt toevoegen aan het goedkeuringsformulier.
- Klik op **OK** om het niveau op te slaan.

Wat nu te doen

Zie [Het goedkeuringsformulier configureren voor het toevoegen van systeem- en aangepaste eigenschappen](#) voor het toevoegen van eigenschappen aan het goedkeuringsformulier.

Het goedkeuringsformulier configureren voor het toevoegen van systeem- en aangepaste eigenschappen

U kunt systeem- en aangepaste eigenschappen toevoegen die op een goedkeuringsformulier worden weergegeven. U voegt deze eigenschappen toe zodat de goedkeurders de waarden van de systeemeigenschappen voor machine-resource-instellingen, zoals CPU of geheugen, en aangepaste eigenschappen kunnen wijzigen voordat ze een goedkeuringsverzoek voltooien.

Welke systeemeigenschappen beschikbaar zijn, is afhankelijk van het type goedkeuringsbeleid en hoe de blueprint wordt geconfigureerd. Voor bepaalde eigenschappen moet het geconfigureerde veld in de blueprint een minimum- en maximumwaarde bevatten voordat de eigenschap wordt weergegeven in de lijst met systeemeigenschappen.

Aangepaste eigenschappen kunnen worden toegevoegd wanneer u het goedkeuringsniveau toevoegt. Als een aangepaste eigenschap wordt geconfigureerd en toegevoegd aan een blueprint, overschrijven de aangepaste eigenschappen die u toevoegt aan het goedkeuringsformulier andere instanties van de betreffende aangepaste eigenschap, zoals in blueprints, eigenschapsgroepen of endpoints.

De goedkeurder kan geselecteerde of geconfigureerde eigenschappen op het goedkeuringsformulier wijzigen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **goedkeuringsbeheerder**.
- [Een goedkeuringsniveau maken](#).

Procedure

- 1 Klik op het tabblad **Goedkeuring vooraf** of **Goedkeuring achteraf** op het pictogram **Nieuw** (+).
- 2 Klik op het tabblad **Systeemeigenschappen**.
- 3 Schakel het selectievakje in voor elke systeemeigenschap die u door de goedkeurder wilt laten configureren tijdens het goedkeuringsproces.
- 4 Configureer de aangepaste eigenschappen.

Voeg een of meer aangepaste eigenschappen toe die u door de goedkeurder wilt laten configureren tijdens het goedkeuringsproces.

 - a Klik op het tabblad **Aangepaste eigenschappen**.
 - b Klik op het pictogram **Nieuw** (+).

- c Voer de waarde van de aangepaste eigenschap in.

Optie	Beschrijving
Naam	Voer de eigenschapsnaam in.
Label	Voer het label in dat de goedkeurder in het goedkeuringsformulier te zien krijgt.
Beschrijving	Voer de uitgebreide informatie voor de goedkeurder in. Deze informatie wordt als knopinfo bij het veld in het formulier weergegeven.

- d Klik op **Opslaan**.
- e Selecteer de gewenste rijen en klik op **Verwijderen** als u meerdere aangepaste eigenschappen wilt verwijderen.

5 Klik op **OK**.

Wat nu te doen

- Voeg aanvullende niveaus voor goedkeuring vooraf en achteraf toe.
- Sla het goedkeuringsbeleid op. Het beleid moet actief zijn om op services, items of acties te kunnen worden toegepast in **Rechten**.

Instellingen voor goedkeuringsbeleid

Wanneer u een goedkeuringsbeleid maakt, configureert u verschillende opties die bepalen wanneer een item dat is aangevraagd door een servicecatalogusgebruiker moet worden goedgekeurd. De goedkeuring kan vereist zijn voordat inrichting op basis van de aanvraag plaatsvindt of nadat het item is ingericht, maar voordat het wordt vrijgegeven aan de gebruiker die de aanvraag heeft ingediend.

Selecteer **Beheer > Goedkeuringsbeleid**. Klik op **Nieuw**.

■ [Instellingen voor goedkeuringsbeleidstype](#)

Het goedkeuringsbeleidstype bepaalt hoe het goedkeuringsbeleid wordt geconfigureerd en op welke items of acties u het in het recht kunt toepassen. Wanneer u goedkeuringsniveaus toevoegt, is het beleidstype of item van invloed op welke velden beschikbaar zijn voor het maken van voorwaarden voor de goedkeuringsniveaus.

■ [Instellingen voor goedkeuringsbeleid toevoegen](#)

U configureert basisgegevens voor het goedkeuringsbeleid, zoals de beleidsstatus, om het beleid te kunnen beheren.

- [Niveau-informatie toevoegen aan goedkeuringsbeleidsinstellingen](#)

Een goedkeuringsniveau bevat de voorwaarden waaronder een goedkeuringsproces in gang wordt gezet op het moment dat de gebruiker van de servicecatalogus het item aanvraagt, alsmede alle overige systeem- en klanteigenschappen die u hierbij wilt betrekken. Wanneer het proces wordt getriggerd, wordt een goedkeuringsaanvraag naar de aangewezen goedkeurders verzonden.

- [Systeemeigenschappen toevoegen aan goedkeuringsbeleidsinstellingen](#)

U hebt systeemeigenschappen geselecteerd voor het goedkeuringsformulier om de goedkeurder in staat te stellen de waarde aan te passen.

- [Aangepaste eigenschappen toevoegen aan goedkeuringsbeleidsinstellingen](#)

U configureert aangepaste eigenschappen voor het goedkeuringsformulier om de goedkeurder in staat te stellen de waarde aan te passen.

Instellingen voor goedkeuringsbeleidstype

Het goedkeuringsbeleidstype bepaalt hoe het goedkeuringsbeleid wordt geconfigureerd en op welke items of acties u het in het recht kunt toepassen. Wanneer u goedkeuringsniveaus toevoegt, is het beleidstype of item van invloed op welke velden beschikbaar zijn voor het maken van voorwaarden voor de goedkeuringsniveaus.

Selecteer **Beheer > Goedkeuringsbeleid**. Klik op **Nieuw**.

Tabel 3-75. Opties voor goedkeuringsbeleidstype

Optie	Beschrijving
Een goedkeuringsbeleidstype selecteren	<p>Maak een goedkeuringsbeleid op basis van het type beleidsaanvraag.</p> <p>Selecteer deze optie om een goedkeuringsbeleid te definiëren dat kan worden toegepast op alle catalogusitems van dat type. Het aanvraagtype kan een algemene aanvraag, een aanvraag voor een catalogusitem of een bronactie zijn.</p> <p>De beschikbare configuratieopties van de voorwaarden verschillen op basis van het type. Hoe specifieker het type is, des te specifieker de configuratievelden zijn.</p> <p>Servicecatalogus - Aanvraag catalogusitem biedt bijvoorbeeld alleen de velden die gemeenschappelijk zijn voor alle catalogusitemaanvragen, maar voor Servicecatalogus - Aanvraag catalogusitem - Virtual machine worden ook de algemene opties en de voor virtual machines specifieke opties weergegeven.</p> <p>Het aanvraagtype beperkt de catalogusitems of acties waarop u het goedkeuringsbeleid kunt toepassen.</p>
Een item selecteren	<p>Maak een goedkeuringsbeleid op basis van een specifiek item.</p> <p>Selecteer deze optie voor het definiëren van een goedkeuringsbeleid dat kan worden toegepast op specifieke items die niet beschikbaar zijn als afzonderlijke items in de servicecatalogus, maar alleen als onderdeel van een machine of andere implementatie. Dit zijn bijvoorbeeld softwareonderdelen.</p> <p>De beschikbare configuratievelden voor de voorwaarden zijn specifiek voor het item en kunnen gedetailleerder zijn dan de criteria die voor een beleidstype-item worden geboden.</p>
Lijst	<p>Geeft het beschikbare beleidstype of catalogusitems weer.</p> <p>Doorzoek of sorteer de kolommen om een specifiek item of type te vinden.</p>

Instellingen voor goedkeuringsbeleid toevoegen

U configureert basisgegevens voor het goedkeuringsbeleid, zoals de beleidsstatus, om het beleid te kunnen beheren.

Om de basisgegevens voor goedkeuringsbeleid te definiëren, selecteert u **Beheer >**

Goedkeuringsbeleid. Klik op **Nieuw**. Selecteer het beleidstype en klik op **OK**.

Tabel 3-76. Opties voor goedkeuringsbeleid

Optie	Beschrijving
Naam	De naam die verschijnt wanneer u het goedkeuringsbeleid toepast op een recht.
Beschrijving	Geef een uitgebreide beschrijving van de manier waarop het goedkeuringsbeleid is samengesteld. Deze informatie is handig voor het beheer van uw goedkeuringsbeleid.
Status	<p>Mogelijke waarden zijn:</p> <ul style="list-style-type: none"> ■ Concept. Dit goedkeuringsbeleid kan niet worden gebruikt voor rechten. Als u een beleid hebt geactiveerd, kunt u de conceptstatus niet meer herstellen. ■ Actief. Dit goedkeuringsbeleid kan worden gebruikt voor rechten. ■ Inactief. Dit goedkeuringsbeleid kan niet worden gebruikt voor rechten. Als u een beleid dat niet op een recht is toegepast, inactief maakt, kunt u het beleid verwijderen maar niet meer opnieuw activeren. Als u een toegepast beleid inactief maakt, moeten de items waarop het beleid betrekking heeft aan een ander beleid worden gekoppeld. Anders gaat de beleidskoppeling voor die items verloren. Gebruikers hebben nog steeds het recht om niet-gekoppelde items en acties uit te voeren, zij het dat deze zonder goedkeuringsbeleid worden uitgevoerd.
Beleidstype	Toont het aanvraagtype voor het goedkeuringsbeleid. Als u een catalogusitem hebt geselecteerd waarop u een goedkeuringsbeleid wilt baseren, wordt het bijbehorende aanvraagtype weergegeven.
Item	<p>Toont het geselecteerde catalogusitem.</p> <p>Dit veld is leeg als u een aanvraagtype selecteert als basis voor een goedkeuringsbeleid.</p>
Laatst bijgewerkt door	De naam van de gebruiker die het goedkeuringsbeleid heeft gewijzigd.
Laatst bijgewerkt op	De datum waarop het goedkeuringsbeleid voor het laatst is gewijzigd.
Goedkeuring vooraf	Als u goedkeuring wilt vereisen voordat aangevraagde items worden ingericht of acties worden uitgevoerd, configureert u een of meer voorwaarden die een goedkeuringsproces starten zodra de gebruiker van de servicecatalogus het item aanvraagt.

Tabel 3-76. Opties voor goedkeuringsbeleid (vervolg)

Optie	Beschrijving
Goedkeuring achteraf	Als u goedkeuring wilt laten geven nadat het item ingericht maar nog voor het ingerichte of aangepaste item wordt vrijgegeven aan de aanvrager die de servicecatalogus gebruikt, configureert u een of meer voorwaarden die een goedkeuringsproces in gang zetten. Zo kan de beheerder van de virtuele infrastructuur bijvoorbeeld eerst controleren of de virtual machine bruikbaar is voordat hij deze vrijgeeft aan de gebruiker van de servicecatalogus.
Gekoppelde rechten weergeven	Toont voor welke rechten het goedkeuringsbeleid is toegepast op services, catalogusitems of acties. U kunt de items van een bepaald recht koppelen aan een ander beleid. Deze optie is alleen beschikbaar wanneer u een actief goedkeuringsbeleid weergeeft.

Niveau-informatie toevoegen aan goedkeuringsbeleidsinstellingen

Een goedkeuringsniveau bevat de voorwaarden waaronder een goedkeuringsproces in gang wordt gezet op het moment dat de gebruiker van de servicecatalogus het item aanvraagt, alsmede alle overige systeem- en klanteigenschappen die u hierbij wilt betrekken. Wanneer het proces wordt getriggerd, wordt een goedkeuringsaanvraag naar de aangewezen goedkeurders verzonden.

Om de basisgegevens voor goedkeuringsbeleid te definiëren, selecteert u **Beheer > Goedkeuringsbeleid**. Klik op **Nieuw**. Selecteer het beleidstype en klik op **OK**. Klik op het tabblad **Goedkeuring vooraf** of **Goedkeuring achteraf** op het pictogram **Nieuw** (+).

U kunt een hiërarchie van niveaus maken op basis van de volgorde waarin u ze wilt verwerken. Wanneer het goedkeuringsbeleid wordt getriggerd en het eerste niveau van goedkeuring wordt afgewezen, wordt de hele aanvraag afgewezen.

Tabel 3-77. Opties voor informatie over het niveau

Optie	Beschrijving
Naam	Voer een naam in. De niveaunaam wordt weergegeven wanneer u een aanvraag met goedkeuringsbeleid beoordeelt.
Beschrijving	Geef een beschrijving van het niveau op. Bijvoorbeeld: CPU>4 tot VI Admin.
Wanneer is goedkeuring vereist?	Selecteer wanneer het goedkeuringsbeleid moet worden geactiveerd.

Tabel 3-77. Opties voor informatie over het niveau (vervolg)

Optie	Beschrijving
Altijd vereist	<p>Het goedkeuringsbeleid wordt voor elke aanvraag geactiveerd.</p> <p>Als u deze optie inschakelt en dit goedkeuringsbeleid toepast op in aanmerking komende services, catalogusitems of acties in een recht, moet de aanvraag worden goedgekeurd via de opgegeven goedkeurdersmethode voordat inrichting plaatsvindt. Alle aanvragen moeten bijvoorbeeld worden goedgekeurd door de manager van de gebruiker die de aanvraag indient.</p>
Voorwaardelijk vereist	<p>Het goedkeuringsbeleid wordt gebaseerd op een of meer voorwaardecomponenten.</p> <p>Als u deze optie selecteert, moet u de voorwaarden maken. Wanneer dit goedkeuringsbeleid wordt toegepast op in aanmerking komende services, catalogusitems of acties in een recht, worden de voorwaarden geëvalueerd. Als aan de voorwaarden wordt voldaan, moet de aanvraag worden goedgekeurd via de opgegeven goedkeurdersmethode voordat inrichting plaatsvindt. Als niet aan de voorwaarden wordt voldaan, vindt inrichting naar aanleiding van de aanvraag zonder goedkeuring plaats. Een aanvraag voor een virtuele machine met 4 of meer CPU's moet bijvoorbeeld worden goedgekeurd door de virtuele-infrastructuurbeheerder.</p> <p>De beschikbaarheid van de velden waarop de voorwaarden worden gebaseerd, wordt bepaald door het geselecteerde type goedkeuringsbeleid of het catalogusitem.</p> <p>Wanneer u een waarde invoert voor een voorwaarde, moet u er rekening mee houden dat deze hoofdlettergevoelig zijn.</p> <p>Als u meer dan een voorwaardecomponent wilt configureren, selecteert u de Boole-bewerking voor de componenten.</p> <ul style="list-style-type: none"> ■ Alle volgende. De goedkeuring wordt geactiveerd wanneer alle componenten waar zijn. Dit staat gelijk aan de Boole-bewerking EN tussen elke component. ■ Eender welke van de volgende. Het goedkeuringsniveau wordt geactiveerd wanneer ten minste een van de componenten waar is. Dit staat gelijk aan de Boole-bewerking OF tussen elke component. ■ Niet de volgende. Het goedkeuringsniveau wordt geactiveerd als geen van de componenten waar zijn. Dit staat gelijk aan de Boole-bewerking NIET tussen elke component.
Goedkeurders	Selecteer de goedkeurdersmethode.

Tabel 3-77. Opties voor informatie over het niveau (vervolg)

Optie	Beschrijving
Specifieke gebruikers en groepen	<p>Hiermee wordt de goedkeuringsaanvraag naar de geselecteerde gebruikers verzonden.</p> <p>Selecteer de gebruikers of gebruikersgroepen die de servicecatalogusaanvraag moeten goedkeuren voordat het betreffende item wordt ingericht of een actie wordt uitgevoerd. De aanvraag wordt bijvoorbeeld aan de groep virtuele-infrastructuurbeheerders verzonden met de optie Goedkeuring door willekeurige personen mogelijk geselecteerd.</p>
Goedkeurders van de aanvraag bepalen	<p>Hiermee wordt de goedkeuringsaanvraag naar de gebruikers verzonden op basis van de gedefinieerde voorwaarde.</p> <p>Als u dit goedkeuringsbeleid bijvoorbeeld toepast op meerdere bedrijfsgroepen en u wilt dat de manager van de bedrijfsgroep de aanvraag goedkeurt, selecteert u Bedrijfsgroep > Consumenten > Gebruikers > Manager.</p>
Gebeurtenisabonnement gebruiken	<p>Hiermee wordt de goedkeuringsaanvraag verwerkt op basis van gedefinieerde gebeurtenisabonnementen.</p> <p>Het werkstroomabonnement moet worden opgegeven in Beheer > Gebeurtenissen > Abonnementen. De toepasselijke werkstroomabonnementen zijn pre-goedkeuring en post-goedkeuring.</p>

Tabel 3-77. Opties voor informatie over het niveau (vervolg)

Optie	Beschrijving
Goedkeuring door willekeurige personen mogelijk	<p>Slechts een van de goedkeurders hoeft de aanvraag goed te keuren voordat deze kan worden verwerkt.</p> <p>Wanneer het item wordt aangevraagd in de servicecatalogus, worden goedkeuringsaanvragen naar alle goedkeurders verzonden. Als een van de goedkeurders de aanvraag goedkeurt, wordt de aanvraag goedgekeurd en wordt de goedkeuringsaanvraag verwijderd uit het Postvak IN van de andere goedkeurders.</p> <p>Als de eerste goedkeurder de aanvraag weigert, ontvangt de gebruiker die de aanvraag heeft ingediend hierover een melding en wordt de goedkeuringsaanvraag verwijderd uit het Postvak IN van de goedkeurders.</p> <p>Als de eerste goedkeurder de aanvraag goedkeurt en de goedkeuringsaanvraag is geopend in de console van de tweede goedkeurder, kan de goedkeurder de goedkeuringsaanvraag niet indienen. Deze wordt als voltooid beschouwd door het antwoord van de eerste goedkeurder.</p> <p>Als u Specifieke gebruikers en groepen of Goedkeurders van de aanvraag bepalen selecteert en er meer dan een goedkeurder is, is dit een van de aanvullende opties. Als er slechts een goedkeurder is, is deze optie niet van toepassing.</p>
Goedkeuring van iedereen nodig	<p>Alle goedkeurders moeten de aanvraag goedkeuren voordat deze kan worden verwerkt.</p> <p>Als u Specifieke gebruikers en groepen of Goedkeurders van de aanvraag bepalen selecteert en er meer dan een goedkeurder is, is dit een van de aanvullende opties. Als er slechts een goedkeurder is, is deze optie niet van toepassing.</p>

Systeemeigenschappen toevoegen aan goedkeuringsbeleidsinstellingen

U hebt systeemeigenschappen geselecteerd voor het goedkeuringsformulier om de goedkeurder in staat te stellen de waarde aan te passen.

Voor de goedkeuring van een virtual machine selecteert u bijvoorbeeld CPU als u de goedkeurder een aanvraag voor 6 CPU's wilt laten wijzigen in 4 CPU's.

Voor systeemeigenschappen selecteert u **Beheer > Goedkeuringsbeleid**. Klik op **Nieuw**. Selecteer het beleidstype en klik op **OK**. Klik op het tabblad Goedkeuring vooraf of Goedkeuring achteraf op het pictogram **Nieuw** (+) en klik op het tabblad **Systeemeigenschappen**.

Tabel 3-78. Opties voor systeemeigenschappen

Optie	Beschrijving
Eigenschappen	<p>De lijst met beschikbare systeemeigenschappen hangt af van het geselecteerde aanvraagtype of catalogusitem en er moeten tevens systeemeigenschappen bestaan voor het betreffende item.</p> <p>Bepaalde eigenschappen zijn alleen beschikbaar wanneer de blueprint op een specifieke manier is geconfigureerd. Bijvoorbeeld: CPU's. De blueprint waarop u het goedkeuringsbeleid toepast met de eigenschap CPU-systeem, moet als bereik worden geconfigureerd. Het minimum voor CPU is bijvoorbeeld 2 en het maximum is 8.</p>

Aangepaste eigenschappen toevoegen aan goedkeuringsbeleidsinstellingen

U configureert aangepaste eigenschappen voor het goedkeuringsformulier om de goedkeurder in staat te stellen de waarde aan te passen.

Voor de goedkeuring van een virtual machine voegt u bijvoorbeeld

VMware.VirtualCenter.Folder toe als u de goedkeurder de map wilt laten opgeven waaraan de machine wordt toegevoegd in vCenter Server.

U kunt ook een aangepaste eigenschap aan het formulier toevoegen die specifiek is voor dit goedkeuringsbeleid.

Voor systeemeigenschappen selecteert u **Beheer > Goedkeuringsbeleid**. Klik op **Nieuw**. Selecteer het beleidstype en klik op **OK**. Klik op het tabblad Goedkeuring vooraf of Goedkeuring achteraf op het pictogram **Nieuw (+)** en klik op het tabblad **Aangepaste eigenschappen**.

Tabel 3-79. Aangepaste eigenschappen

Optie	Beschrijving
Naam	Voer de eigenschapsnaam in.
Label	Voer het label in dat de goedkeurder in het goedkeuringsformulier te zien krijgt.
Beschrijving	Voer de uitgebreide informatie voor de goedkeurder in. Deze informatie wordt als knopinfo bij het veld in het formulier weergegeven.

Een goedkeuringsbeleid wijzigen

U kunt een actief of inactief goedkeuringsbeleid niet wijzigen. U moet een kopie van het oorspronkelijke beleid maken en het beleid dat niet de vereiste resultaten produceert, vervangen. Actief en inactief goedkeuringsbeleid is alleen-lezen. U kunt goedkeuringsbeleid wijzigen dat zich in een conceptstatus bevindt.

Wanneer u de kopie van het oorspronkelijke beleid maakt, wordt het nieuwe beleid gebaseerd op het oorspronkelijke beleidstype. U kunt alle kenmerken behalve het beleidstype bewerken. U doet dit wanneer u de beleidsniveaus wilt wijzigen om niveaus te wijzigen, toe te voegen of te verwijderen of om systeemeigenschappen of aangepaste eigenschappen aan de formulieren toe te voegen.

U kunt niveaus voor vóór en na goedkeuring maken. Voor instructies over het maken van een goedkeuringsniveau raadpleegt u [Een goedkeuringsniveau maken](#).

Voorwaarden

Meld u aan bij vRealize Automation als een **tenantbeheerder** of **goedkeuringsbeheerder**.

Procedure

- 1 Selecteer **Beheer > Goedkeuringsbeleid**.
- 2 Selecteer de rij van het goedkeuringsbeleid dat u wilt kopiëren.
- 3 Klik op het pictogram **Kopiëren** ().
- Er wordt een kopie gemaakt van het goedkeuringsbeleid.
- 4 Selecteer het nieuwe goedkeuringsbeleid dat u wilt bewerken.
- 5 Geef een naam op in het tekstvak **Naam**.
- 6 (Optioneel) Geef een beschrijving op in het tekstvak **Beschrijving**.
- 7 Selecteer de status van het beleid in het vervolgkeuzemenu **Status**.

Optie	Beschrijving
Concept	Slaat het goedkeuringsbeleid op in een bewerkbare status.
Actief	Slaat het goedkeuringsbeleid op in een alleen-lezen status die u kunt gebruiken in een recht.
Inactief	Slaat het goedkeuringsbeleid op in een alleen-lezen status die u niet kunt gebruiken in een recht totdat u het beleid activeert.

- 8 Bewerk de niveaus voor vóór en na goedkeuring.
- 9 Klik op **OK**.

Resultaten

U hebt een nieuw goedkeuringsbeleid gemaakt op basis van een bestaand goedkeuringsbeleid.

Wat nu te doen

Pas het nieuwe goedkeuringsbeleid toe in een recht. Zie [Gebruikers rechten verlenen voor services, catalogusitems en acties](#).

Goedkeuringsbeleid deactiveren

Als u merkt dat een goedkeuringsbeleid achterhaald is, kunt u het deactiveren zodat het niet meer beschikbaar is voor de inrichting.

Als u een goedkeuringsbeleid wilt deactiveren, moet u een nieuw beleid toewijzen aan elk recht waarop het goedkeuringsbeleid momenteel wordt toegepast.

U kunt een gedeactiveerd goedkeuringsbeleid behouden om het op een later tijdstip weer te activeren of het desgewenst verwijderen.

Voorwaarden

Meld u aan bij vRealize Automation als een **tenantbeheerder** of **goedkeuringsbeheerder**.

Procedure

- 1 Selecteer **Beheer > Goedkeuringsbeleid**.
- 2 Klik op de naam van het goedkeuringsbeleid.
- 3 Klik op **Gekoppelde rechten weergeven**
 - a Selecteer het nieuwe goedkeuringsbeleid in het vervolgkeuzemenu **Alles vervangen door**.
Als de lijst meer dan een recht bevat, wordt het nieuwe goedkeuringsbeleid toegepast op alle weergegeven rechten.
 - b Klik op **OK**.
- 4 Controleer of er geen rechten meer aan het goedkeuringsbeleid zijn gekoppeld en selecteer vervolgens **Inactief** in het vervolgkeuzemenu Status.
- 5 Klik op **OK**.
- 6 Als u een goedkeuringsbeleid wilt verwijderen, selecteert u de rij met het inactieve beleid.
 - a Klik op **Verwijderen**.
 - b Klik op **OK**.

Resultaten

Het goedkeuringsbeleid is niet meer gekoppeld aan gebruikte rechten en wordt gedeactiveerd. U kunt het op een later tijdstip weer activeren en toepassen op items in verleende rechten.

Wat nu te doen

Als u het goedkeuringsbeleid niet meer nodig hebt, kunt u het verwijderen. Zie [Goedkeuringsbeleid verwijderen](#).

Goedkeuringsbeleid verwijderen

Als u goedkeuringsbeleid hebt gedeactiveerd en verder niet meer nodig hebt, kunt u het verwijderen uit vRealize Automation.

Voorwaarden

- Goedkeuringsbeleid loskoppelen en deactiveren. Zie [Goedkeuringsbeleid deactiveren](#).
- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **goedkeuringsbeheerder**.

Procedure

- 1 Selecteer **Beheer > Goedkeuringsbeleid**.
- 2 Selecteer de rij met het inactieve beleid.
- 3 Klik op **Verwijderen**.
- 4 Klik op **OK**.

Resultaten

Het goedkeuringsbeleid wordt verwijderd.

Scenario: goedkeuringsbeleid voor CentOS met MySQL maken en toepassen

Als tenantbeheerder voor de bedrijfsgroep voor ontwikkeling en kwaliteitscontrole wilt u strikt toezicht houden op de aangevraagde catalogusitems. Het is dan belangrijk dat gebruikers het catalogusitem CentOS met MySQL pas kunnen inrichten nadat de vSphere-beheerder van de virtuele infrastructuur de machineaanvraag heeft goedgekeurd en de softwarebeheerder de softwareaanvraag heeft goedgekeurd.

U kunt dus enerzijds een goedkeuringsbeleid voor de vSphere CentOS-servicecatalogusaanvraag met MySQL maken en toepassen waarmee onder bepaalde voorwaarden goedkeuring is vereist van de vSphere-beheerder van de virtuele infrastructuur, terwijl u in een ander goedkeuringsbeleid voor het onderdeel MySQL Software vereist dat elke aanvraag moet worden goedgekeurd door de softwarebeheerder.

Een goedkeuringsbeheerder kan alleen goedkeuringen aanmaken en moet vervolgens aan een bedrijfsgroepbeheerder vragen of ze deze willen toepassen op de rechten. Als tenantbeheerder kunt u de goedkeuringen zowel maken als toepassen op rechten.

Voorwaarden

- Meld u aan bij de vRealize Automation-console als **tenantbeheerder**. Alleen de tenantbeheerder kan goedkeuringsbeleid zowel maken als toepassen.
- Zorg ervoor dat het catalogusitem CentOS met MySQL is opgenomen in de service. Zie [Scenario: een CentOS met MySQL-toepassingsblueprint beschikbaar maken in de servicecatalogus](#).

Scenario: een goedkeuringsbeleid voor CentOS met MySQL-virtual machine maken

Als tenantbeheerder moet u ervoor zorgen dat de groep voor ontwikkelaars en kwaliteitsingenieurs virtual machines ontvangt die correct in uw omgeving zijn ingericht. Daarom maakt u een goedkeuringsbeleid dat voorafgaande goedkeuring vereist voor bepaalde typen aanvragen.


Omdat de CentOS voor MySQL-virtual machine vCenter Server-bronnen verbruikt, wilt u dat de virtuele infrastructuurbeheerder van vSphere aanvragen goedkeurt wanneer het aangevraagde geheugen meer dan 2048 MB of meer dan 2 CPU's is om te garanderen dat de bronnen op doordachte wijze worden gebruikt. U biedt de goedkeurder ook de mogelijkheid om de aangevraagde CPU- en geheugenwaarden te wijzigen voordat u een aanvraag goedkeurt.

Procedure

- 1 Selecteer **Beheer > Goedkeuringsbeleid**.
- 2 Maak een goedkeuringsbeleid voor de inrichting van virtual machines.
 - a Klik op het pictogram **Nieuw** (+).
 - b Selecteer **Een goedkeuringsbeleidtype selecteren**.
 - c Selecteer in de lijst **Servicecatalogus - Aanvraag voor catalogusitem - Virtual machine**.
 - d Klik op **OK**.
 - e Configureer de volgende opties:

Optie	Configuratie
Naam	Voer CPU of geheugen voor CentOS op vSphere VM in.
Beschrijving	Voer Vereist goedkeuring van virtual infrastructuurbeheerder voor CPU>2 of geheugen>2048 in.
Status	Selecteer Actief .

- 3 Klik op het tabblad **Goedkeuring vooraf** op het pictogram **Toevoegen** (+).
- 4 Configureer de triggercriteria en goedkeuringsacties op het tabblad **Informatie over niveau**.
 - a Voer in het tekstvak
NaamCPU>2 of geheugen>2048 – virtual infrastructuurbeheerder in.
 - b Voer in het tekstvak
BeschrijvingGoedkeuring van virtual infrastructuurbeheerder voor CPU en geheugen in.
 - c Selecteer **Voorwaardelijk vereist**.
 - d Selecteer in de vervolgkeuzelijst Component **Eender welke van de volgende**.
 - e In het nieuwe vervolgkeuzemenu Component selecteert u **CPU's** en configureert u het onderdeel met de waarden **CPU > 2**.
 - f Klik op **Expressie toevoegen** en configureer het onderdeel met de waarden **Geheugen (MB) > 2048**.
 - g Selecteer **Specifieke gebruikers en groepen**.

- h Voer in het zoekvak de naam van de beheerder van de virtuele vSphere-infrastructuur of van de groep beheerders in en klik op het zoekpictogram (.
- i Selecteer de gebruiker of groep.
- j Selecteer **Goedkeuring door willekeurige personen mogelijk**.

De aanvraag heeft slechts één virtual infrastructuurbeheerder nodig om de bronnen te controleren en de aanvraag goed te keuren.

- 5 Klik op het tabblad **Systeemeigenschappen** en selecteer de eigenschappen die de goedkeurder toestaan om de aangevraagde CPU- en geheugenwaarden te wijzigen voordat een aanvraag wordt goedgekeurd.
 - a Schakel de selectievakjes **CPU's** en **Geheugen (MB)** in.
 - b Klik op **OK**.
- 6 Klik op **OK**.

Resultaten

U hebt een goedkeuringsbeleid gemaakt voor virtual machineaanvragen maar u wilt nog een goedkeuring maken voor het MySQL-onderdeel. Totdat u beleidsregels toepast op een recht, worden er geen goedkeuringen getriggerd.

Scenario: goedkeuringsbeleid maken voor een MySQL Software-onderdeel

De softwarebeheerders hebben gevraagd of u als tenantbeheerder goedkeuringsbeleid voor MySQL-installaties wilt maken om het licentiegebruik te volgen. U maakt derhalve een beleid waarmee de beheerder van softwarelicenties wordt gewaarschuwd telkens wanneer het Software-onderdeel MySQL voor Linux virtual machines wordt aangevraagd.

Dit type goedkeuring kan nodig zijn in een omgeving waarin de softwarebeheerder licentiesleutels moet verstrekken. In dit scenario is het alleen nodig dat de softwarebeheerder de aanvraag volgt en goedkeurt. Als u het goedkeuringsbeleid hebt gemaakt, past u het toe op het catalogusitem MySQL voor Linux virtual machines. Het gaat hier om een erg specifiek goedkeuringsbeleid dat alleen kan worden toegepast op rechten voor het Software-onderdeel MySQL voor Linux virtual machines.

Procedure

- 1 Selecteer **Beheer > Goedkeuringsbeleid**.
- 2 Pas het goedkeuringsbeleid toe op het MySQL Software-onderdeel.
 - a Klik op het pictogram **Nieuw** (.
 - b Selecteer **Selecteer een item**.
 - c Selecteer **MySQL voor Linux virtual machines**.

- d Klik op **OK**.
- e Configureer de volgende opties:

Optie	Configuratie
Naam	Voer MySQL goedkeuring bijhouden in.
Beschrijving	Voer Goedkeuringsaanvraag verzonden naar softwarebeheerder in.
Status	Selecteer Actief .

- 3 Klik op het tabblad **Goedkeuring vooraf** op het pictogram **Toevoegen** (+).
- 4 Configureer de triggercriteria en goedkeuringsacties op het tabblad **Informatie over niveau**.
 - a Voer in het tekstvak **Naam** **Kennisgeving MySQL-software-implementatie** in.
 - b Voer in het tekstvak **Beschrijving** **Goedkeuring van software-installatie door softwarebeheerder**.
 - c Selecteer **Altijd vereist**.
 - d Selecteer **Specifieke gebruikers en groepen**.
 - e Voer de naam van de softwarebeheerder in het zoekvak in, klik op het pictogram Zoeken (🔍) en selecteer de gebruiker.
 - f Selecteer **Goedkeuring door willekeurige personen mogelijk**.
De aanvraag hoeft slechts door één softwarebeheerder te worden goedgekeurd.
Klik op **OK**.
- 5 Klik op **OK**.

Resultaten

U hebt het goedkeuringsbeleid voor virtual machines en voor MySQL voor Linux Virtual Machines Software-onderdelen gemaakt. Totdat u goedkeuringsbeleidsregels toepast op een recht, worden er geen goedkeuringen getriggerd.

Scenario: goedkeuringsbeleid toepassen op CentOS met MySQL-onderdelen

Als tenantbeheerder kunt u goedkeuringsbeleid en rechten maken. U wijzigt het Dev- en QE-recht om het goedkeuringsbeleid dat u hebt gemaakt, toe te passen zodat goedkeuringen worden toegepast wanneer een gebruiker van een servicecatalogus het item aanvraagt.

Hoewel het mogelijk makkelijker is om de bedrijfsgroep rechten te verlenen voor de hele catalogusservice, levert u dat minder controle en toezicht op dan wanneer u de rechten voor catalogusitems afzonderlijk verleent. Stel dat u gebruikers rechten voor een service verleent, dan kunnen ze een aanvraag indienen voor alle bestaande catalogusitems in die service en alle items die er nog aan worden toegevoegd. Bovendien moet u dan voor elk catalogusitem in de service een algemener goedkeuringsbeleid instellen, waardoor er bijvoorbeeld altijd goedkeuring van

een manager vereist is. Als u de rechten voor de catalogusitems afzonderlijk wilt verlenen, kunt u een specifiek goedkeuringsbeleid instellen voor elk item en nauwgezet bepalen wie welke items in de service kan aanvragen. U kunt de controle nog verder vergroten door de rechten voor elk catalogusitem op onderdeelniveau toe te wijzen.

Als u niet weet welk goedkeuringsbeleid u wilt toepassen op items in een recht, kunt u hier later op terugkomen en het juiste beleid toepassen. In dit scenario past u verschillende soorten goedkeuringsbeleid toe op de twee onderdelen van dezelfde gepubliceerde toepassingsblueprint.

Procedure

1 Selecteer **Beheer > Catalogusbeheer > Rechten**.

2 Klik op **Dev- en QE-recht**.

3 Klik op het tabblad **Items en goedkeuringen**.

4 Voeg de CentOS met MySQL-machine toe en pas het goedkeuringsbeleid toe.

a Klik op het pictogram **Items toevoegen (+)** naast de titel Items waarvoor rechten zijn verleend.

b Schakel het selectievakje **CentOS met MySQL** in.

c Klik op de pijl voor het vervolgkeuzemenu bij **Dit beleid toepassen op geselecteerde items**.

Het beleid CentOS voor vSphere CPU en geheugen staat niet in de lijst.

d Klik op **Alles weergeven** en klik op de pijl-omlaag om alle soorten goedkeuringsbeleid weer te geven.

e Selecteer **CentOS voor vSphere CPU en geheugen [Servicecatalogus - Catalogusitem Aanvraag - Virtual Machine]**.

De vSphere CentOS-machine is een machineblueprint in een toepassingsblueprint. Bekijk de beleidsnamen en selecteer het gewenste beleid voor uw type catalogusitem. Als u het verkeerde beleid toepast, wordt het goedkeuringsbeleid niet uitgevoerd of worden de goedkeuringsaanvragen gestart op basis van onjuiste voorwaarden.

f Klik op **OK**.

5 Voeg de het softwareonderdeel MySQL voor Linux virtual machine toe als een item en pas een goedkeuringsbeleid toe op het MySQL-item.

a Klik op het pictogram **Catalogusitems en -onderdelen toevoegen (+)** naast de titel Catalogusitems en -onderdelen waarvoor rechten zijn verleend.

b Selecteer in het vervolgkeuzemenu **Catalogusitems en -onderdelenNee**.

Softwareonderdelen zijn altijd gekoppeld aan een machine. Ze zijn niet beschikbaar voor een afzonderlijke aanvraag in de servicecatalogus.

- c Schakel het selectievakje **MySQL voor Linux virtual machines** in.
- d Klik op de pijl voor het vervolgkeuzemenu bij **Dit beleid toepassen op geselecteerde items**.
- e Selecteer **MySQL goedkeuring bijhouden [Servicecatalogus - Aanvraag catalogusitem - Softwareonderdeel]**.

U hebt deze uitgebreide optie niet nodig omdat het goedkeuringsbeleid is gemaakt voor dit specifieke softwareonderdeel, dat wordt toegevoegd aan een virtual machine.

- f Klik op **OK**.

6 Voeg acties toe die door de gebruikers kunnen worden uitgevoerd op de ingerichte machine.

Er kan geen goedkeuringsbeleid worden toegepast op de acties in dit scenario.

- a Klik op het pictogram **Acties toevoegen** (+) naast de titel Acties waarvoor rechten zijn verleend.
- b Selecteer de volgende acties.

Naam / type	Beschrijving
Momentopname / virtual machine maken	Hierdoor wordt een momentopname van een virtual machine gemaakt, inclusief de geïnstalleerde software. Hiermee kunnen ontwikkelaars momentopnamen maken waar ze naar terug kunnen keren tijdens de ontwikkeling.
Vernietigen / Implementatie	Hierdoor wordt de volledige, ingerichte blueprint vernietigd, niet alleen de machine. Gebruik deze actie om overblijvende onderdelen te vermijden.
Uitschakelen / Machine	Hierdoor wordt de virtual machine uitgeschakeld.
Inschakelen / Machine	Hierdoor wordt de virtual machine ingeschakeld.
Momentopname / virtual machine terugzetten	Hierdoor wordt een eerder gemaakte momentopname teruggezet.

- c Klik op **OK**.

7 Klik op **Voltooien**.

Resultaten

Met dit recht kunt u verschillende soorten goedkeuring vereisen voor verschillende blueprintonderdelen.

Wat nu te doen

Vraag het item CentOS met MySQL in de servicecatalogus aan als een lid van de bedrijfsgroep om te controleren of het recht en de goedkeuringen zich gedragen zoals verwacht.

Machine-inrichting aanvragen met behulp van een blueprint met parameters

Wanneer u een machine-inrichting aanvraagt voor een vSphere-machine-blueprint die ontworpen is om de onderdeelprofielen Grootte of Afbeelding te bevatten, geeft u de inrichting op door een beschikbare waardeset te selecteren.

Wanneer u de inrichting aanvraagt, kunt u kiezen uit de beschikbare opties voor Size en Image. Als u een van de waardesets kiest, worden de bijbehorende eigenschapswaarden vervolgens aan de aanvraag gekoppeld.

De waardeset van het onderdeelprofiel wordt toegepast op alle vSphere-machines in een cluster.

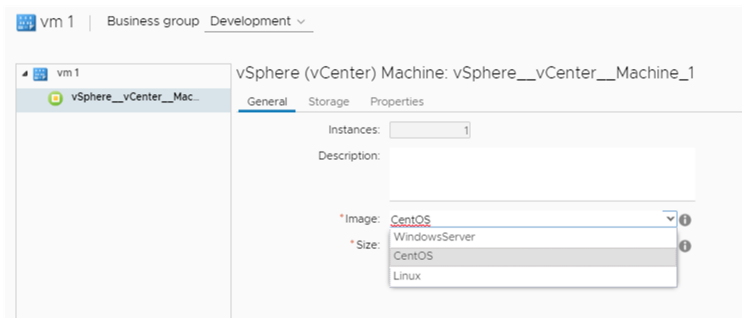
Zie [Het toewijzen van parameters aan blueprints begrijpen en gebruiken](#) voor meer informatie over de configuratie van onderdeelprofielen.

Voorwaarden

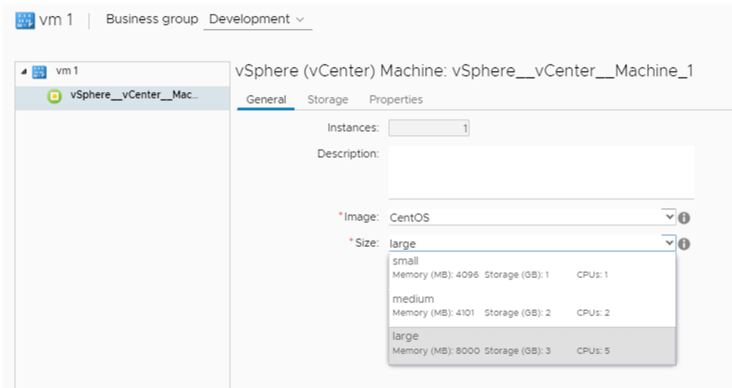
- Definieer waardesets voor de onderdeelprofielen Size of Image. Zie en in *Naslaggids voor aangepaste eigenschappen*.
- Maak een blueprint die een machineonderdeel vSphere bevat die een onderdeelprofiel Image of Size bevat. Zie [Een machineblueprint configureren](#) en [Instellingen voor vSphere-machineonderdelen in vRealize Automation](#).
- Publiceer de blueprint naar de catalogus. Zie [Een blueprint publiceren](#).
- Configureer de blueprint in de catalogus. Zie [Checklist voor het configureren van de servicecatalogus](#) en [Voorbeelden van goedkeuringsbeleid op basis van beleidstypen voor virtual machines](#).

Procedure

- 1 Klik op **Catalogus**.
- 2 Selecteer de aan te vragen catalogusservice en klik op **Aanvraag**.
- 3 Selecteer het in te richten vSphere-machineonderdeel en geef het aantal in te richten instanties op.
- 4 Selecteer een optie uit de waardeset voor Afbeelding in het vervolgkeuzemenu **Afbeelding**.



- 5 Selecteer een optie uit de waardeset voor Grootte in het vervolgkeuzemenu **Grootte**.



- 6 Klik op **Indienen**.

Wat nu te doen

De waardesets die u hebt gedefinieerd voor de onderdeelprofielen Size en Image zijn nu beschikbaar in de vervolgkeuzemenu's **Afbeelding** en **Grootte** op het tabblad **Catalogus** in het aanvraagformulier voor catalogusinrichting.

Scenario: een CentOS met MySQL-toepassingsblueprint beschikbaar maken in de servicecatalogus

Als tenantbeheerder hebt u uw blueprintarchitecten gevraagd een catalogusitem voor MySQL op CentOS te maken, waarop uw groep van ontwikkelaars en kwaliteitsingenieurs testcases kan uitvoeren. Uw softwarearchitect heeft u geïnformeerd dat het catalogusitem gereed is voor gebruikers. Om het item beschikbaar te maken voor uw bedrijfsgebruikers, moet u de blueprints en het Software-onderdeel koppelen aan een catalogusservice en vervolgens de leden van de bedrijfsgroep rechten verlenen om het catalogusitem aan te vragen.

Voorwaarden

- Meld u aan bij vRealize Automation als een **tenantbeheerder** of **catalogusbeheerder**.
- Publiceer een blueprint voor MySQL op een vSphere CentOS virtual machine. Zie de processen voor het maken van blueprints voor machine- en softwareonderdelen in [Uw ontwerpbibliotheek opbouwen](#).
- Als u blueprints maakt in een ontwikkelingsomgeving, importeert u uw blueprint in uw productieomgeving. Zie [Blueprints en inhoud exporteren en importeren](#).

- Maak een reservering om vSphere-bronnen toe te voegen aan uw bedrijfsgroep voor ontwikkelaars en kwaliteitsingenieurs. Zie [Een reservering maken voor Hyper-V, KVM, SCVMM, vSphere of XenServer](#).

Procedure

1 Scenario: een catalogusservice voor ontwikkeling en kwaliteitscontrole maken

Als tenantbeheerder wilt u een afzonderlijke catalogusservice maken voor uw ontwikkelings- en kwaliteitsteam zodat de specifieke catalogusitems onzichtbaar blijven voor andere teams van bijvoorbeeld de afdeling financiën en human resources. Voor de publicatie van alle vereiste catalogusitems die het ontwikkelings- en kwaliteitsteam nodig hebben voor hun testcases, maakt u de catalogusservice 'Dev- en QE-service'.

2 Scenario: CentOS met MySQL toevoegen aan uw service voor ontwikkelaars en kwaliteitsingenieurs

Als tenantbeheerder wilt u het catalogusitem CentOS met MySQL toevoegen aan de service voor ontwikkelaars en kwaliteitsingenieurs.

3 Scenario: gebruikers rechten geven om Dev- en QE-service-items aan te vragen als catalogusitems

Als tenantbeheerder kunt u catalogusitems en andere relevante acties toewijzen aan Dev- en QE-rechten die u maakt, zodat gebruikers op het vlak van ontwikkeling en kwaliteitscontrole het catalogusitem CentOS met MySQL kunnen aanvragen en acties kunnen uitvoeren voor de machine en implementatie.

Scenario: een catalogusservice voor ontwikkeling en kwaliteitscontrole maken

Als tenantbeheerder wilt u een afzonderlijke catalogusservice maken voor uw ontwikkelings- en kwaliteitsteam zodat de specifieke catalogusitems onzichtbaar blijven voor andere teams van bijvoorbeeld de afdeling financiën en human resources. Voor de publicatie van alle vereiste catalogusitems die het ontwikkelings- en kwaliteitsteam nodig hebben voor hun testcases, maakt u de catalogusservice 'Dev- en QE-service'.

Procedure

- 1 Selecteer **Beheer > Catalogusbeheer > Services**.
- 2 Klik op het pictogram **Nieuw** (+).
- 3 Typ de naam **Dev- en QE-service** in het tekstvak **Naam**.
- 4 Typ de beschrijving **Dev- en QE-catalogusitems voor testcases** in het tekstvak **Beschrijving**.
- 5 Selecteer **Actief** in het vervolgkeuzemenu **Status**.
- 6 Als catalogusbeheerder die de service maakt, gebruikt u de zoekoptie om uw naam als eigenaar toe te voegen.

- 7 Voeg de aangepaste gebruikersgroep Ondersteuningsteam toe.

U voegt bijvoorbeeld een aangepaste gebruikersgroep met IaaS-architecten en softwarearchitecten toe die in geval van problemen met de inrichting van catalogusitems als contactpersoon fungeren voor u en de gebruikers van de servicecatalogus.

- 8 Klik op **OK**.

Resultaten

U hebt een Dev- en QE-catalogusservice gemaakt en geactiveerd, maar er zijn nog geen catalogusitems aan toegewezen.

Scenario: CentOS met MySQL toevoegen aan uw service voor ontwikkelaars en kwaliteitsingenieurs

Als tenantbeheerder wilt u het catalogusitem CentOS met MySQL toevoegen aan de service voor ontwikkelaars en kwaliteitsingenieurs.

Procedure

- 1 Selecteer **Beheer > Catalogusbeheer > Services**.
- 2 Selecteer de rij van de service voor ontwikkelaars en kwaliteitsingenieurs in de lijst met **Services** en klik op **Catalogusitems beheren**.
- 3 Klik op het pictogram **Nieuw (+)**.
- 4 Selecteer **CentOS met MySQL**.

Alleen gepubliceerde blueprints en onderdelen die nog niet aan een service gekoppeld zijn, worden in de lijst weergegeven. Als u de blueprint niet ziet, controleert u of deze gepubliceerd is of mogelijk in een andere service is opgenomen.

- 5 Klik op **OK**.
- 6 Klik op **Sluiten**.

Resultaten

U hebt het catalogusitem CentOS met MySQL gepubliceerd in de service voor ontwikkelaars en kwaliteitsingenieurs, maar niemand kan het item zien of aanvragen totdat u gebruikers rechten verleent voor het item of de service.

Scenario: gebruikers rechten geven om Dev- en QE-service-items aan te vragen als catalogusitems

Als tenantbeheerder kunt u catalogusitems en andere relevante acties toewijzen aan Dev- en QE-rechten die u maakt, zodat gebruikers op het vlak van ontwikkeling en kwaliteitscontrole het catalogusitem CentOS met MySQL kunnen aanvragen en acties kunnen uitvoeren voor de machine en implementatie.

In dit scenario geeft u toestemming voor de service, omdat u wilt dat gebruikers toestemming houden om catalogusitems te openen die in de toekomst aan deze service worden toegevoegd. Verder wilt u gebruikers toestaan hun ingerichte implementatie te beheren. Daartoe breidt u de rechten uit met acties voor onder meer in- en uitschakelen, momentopnamen en implementatievernietiging.

Procedure

1 Selecteer **Beheer > Catalogusbeheer > Rechten**.

2 Klik op het pictogram **Nieuw** (+).

3 Configureer de details.

- a Geef de naam **Dev and QE Entitlement** op in het tekstvak **Naam**.
- b Selecteer in het vervolgkeuzemenu **Status** de optie **Actief**.
- c Selecteer in het vervolgkeuzemenu **Bedrijfsgroep** de groep **Dev & QE**.
- d Voeg een of meer gebruikers toe in het gebied Gebruikers en groepen.

Voeg alleen uzelf toe, tenzij u zeker weet dat de blueprint werkt zoals bedoeld. Als dat het geval is, kunt u afzonderlijke gebruikers en aangepaste gebruikersgroepen toevoegen.

- e Klik op **Volgende**.

4 Voeg de service toe.

Hoewel u de catalogusitems CentOS en MySQL afzonderlijk toevoegt, is het belangrijk dat u ook de service toevoegt. Zo weet u zeker dat de items die u op een later tijdstip aan de service toevoegt ook voor de leden van de bedrijfsgroep beschikbaar zijn in de servicecatalogus.

- a Klik op het pictogram **Services toevoegen** (+) naast de titel Services waarvoor rechten zijn verleend.
- b Selecteer **Dev- en QE-service**.
- c Klik op **OK**.

De Dev- en QE-service wordt toegevoegd aan de lijst Services waarvoor rechten zijn verleend.

5 Voeg acties toe.

- a Klik op het pictogram **Acties toevoegen** (+) naast de titel Acties waarvoor rechten zijn verleend.
- b Klik op de kolomkop Type om de lijst te sorteren.

Selecteer de volgende acties op basis van type. Deze acties zijn handig voor gebruikers die met testmachines werken bij de ontwikkeling en kwaliteitscontrole. Het zijn de enige acties die u instelt voor deze leden van de bedrijfsgroep.

Type	Actienaam
Machine	Inschakelen
Machine	Uitschakelen
Virtual machine	Momentopname maken
Virtual machine	Terugzetten naar momentopname
Implementatie-	Vernietigen
	Met de actie voor implementatievernietiging wordt de hele implementatie vernietigt, dus niet alleen de virtual machine.

- c Klik op **OK**.

De vijf acties worden toegevoegd aan de lijst Acties waarvoor rechten zijn verleend.

6 Klik op **Voltooien**.

Resultaten

U hebt het catalogusitem CentOS met MySQL toegevoegd aan catalogusservice Dev & QE en de leden van de bedrijfsgroep rechten verleend om het item aan te vragen en te beheren.

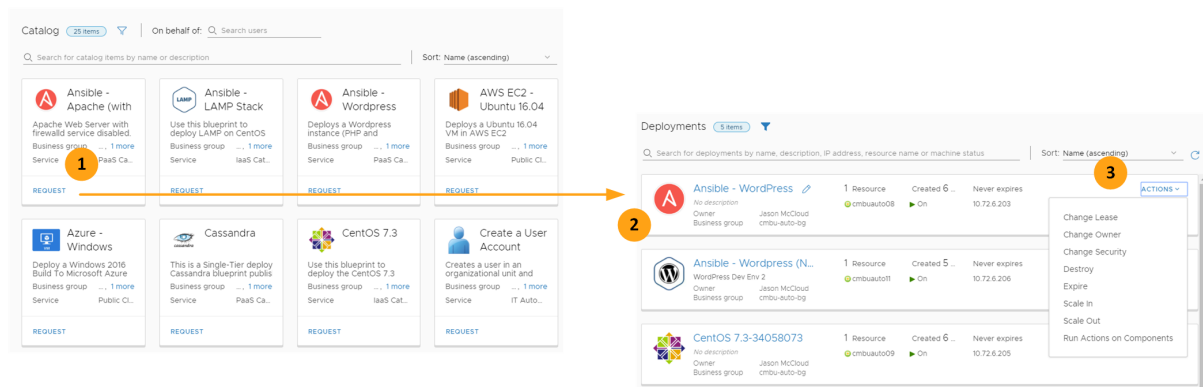
Wat nu te doen

Nadat u het catalogusitem CentOS met MySQL ter controle hebt ingericht, kunt u andere gebruikers de bijbehorende rechten verlenen zodat het catalogusitem beschikbaar wordt voor degenen die zich bezighouden met ontwikkeling en kwaliteitscontrole. Als u de inrichting van bronnen in uw omgeving verder wilt besturen, kunt u goedkeuringsbeleid maken voor het onderdeel MySQL Software en de CentOS voor softwaretestmachine. Zie [Scenario: goedkeuringsbeleid voor CentOS met MySQL maken en toepassen](#).

De catalogus gebruiken en implementaties beheren

4

De catalogus bevat uw beschikbare blueprints en implementaties zijn uw voorziene blueprints. Uw beheerder biedt de catalogusitems. U kunt dan de resources aanvragen en beheren als implementaties. Als onderdeel van het beheren van implementaties kunt u acties uitvoeren om wijzigingen te maken.



De volgende workflow begint met de catalogus.

- 1 U vraagt items aan in de catalogus. De catalogus bevat gepubliceerde blueprints waar de bedrijfsgroepen waar u lid van bent recht op hebben.
- 2 De ingerichte resources worden beheerd als implementaties. U kunt het provisioning-proces controleren, uw implementatie beheren en acties uitvoeren op uw implementaties.
- 3 De acties kunt u gebruiken om wijzigingen aan te brengen in de implementatie nadat deze is geïmplementeerd. Acties kunnen bijvoorbeeld het volgende omvatten: het vergroten van het geheugen, de CPU verlagen of de implementatie te vernietigen wanneer u deze niet langer nodig hebt.

Dit hoofdstuk omvat de volgende onderwerpen:

- [Werken met de catalogus](#)
- [Werken met uw implementaties](#)
- [Werken met de Inbox](#)

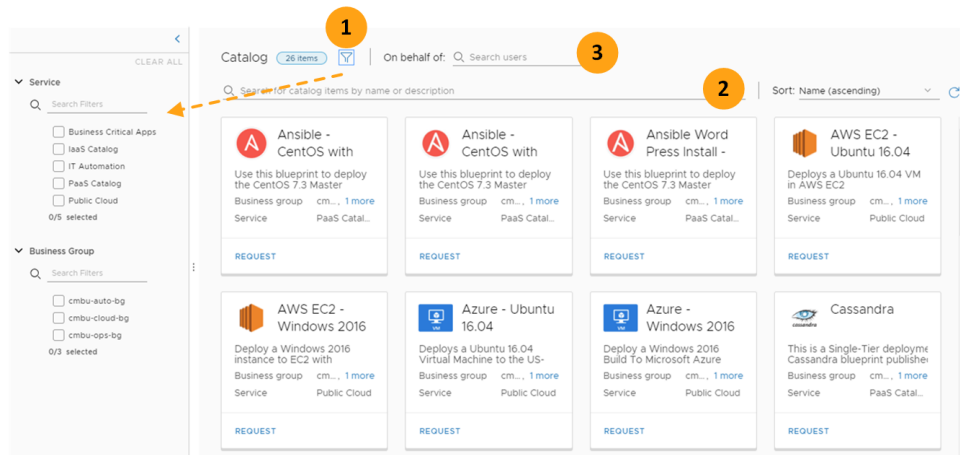
Werken met de catalogus

De catalogus is de lijst met blueprints die u kunt implementeren. De blueprintarchitect, bepaalt het ontwerp van de onderdelen, welke aangepaste opties u kunt selecteren wanneer u het item aanvraagt en waar het wordt geïmplementeerd op basis van de vRealize Automation-endpoints van uw organisatie.

De beschikbare catalogusitems zijn gebaseerd op uw lidmaatschap van een of meer bedrijfsgroepen en welke rechten uw bedrijfsgroepen hebben voor het inrichten van de blueprints.

Catalogusitems zoeken

Dit voorbeeld toont een kleine catalogus. In grotere zakelijke omgevingen heeft u misschien meer dan op één pagina past.

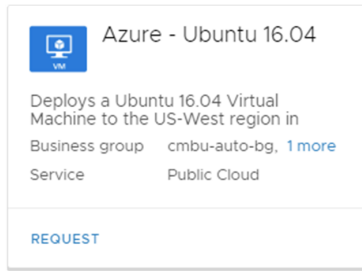


Gebruik de volgende opties om de blueprint te zoeken die u wilt implementeren.

- 1 **Filter** de lijst op basis van services en bedrijfsgroepen.
- 2 Gebruik **Zoeken** en **Sorteren** om de catalogusitems te zoeken en te ordenen.
- 3 Selecteer een **Namens**-gebruiker om het aantal catalogusitems te beperken en het item vervolgens voor die gebruiker aan te vragen. U kunt alleen blueprints implementeren waarop bedrijfsgroepen waarvan de gebruiker lid is rechten hebben. Wanneer u de naam van de gebruiker selecteert, wordt dit lidmaatschap weergegeven in de lijst met beschikbare catalogusitems. Namens-toestemming is beschikbaar voor beheerders en bedrijfsgroepmanagers en kan worden toegewezen aan een of meer bedrijfsgroepleden bij het configureren van de bedrijfsgroep. Zie [Een bedrijfsgroep maken](#).

Cataloguskaarten

Catalogus-kaarten staan voor de blueprint die de afzonderlijke machines of een volledige applicatie kunnen implementeren. Deze kunnen ook XaaS-workflows weergeven die op andere manieren voor provisioning zorgen. Bijvoorbeeld gebruikers toevoegen aan Active Directory.



De informatie op de kaart omvat de bedrijfsgroepen die het recht hebben om het catalogusitem en de service waaraan het item is gekoppeld aan te vragen.

Een catalogusaanvraag indienen

Wanneer u een catalogusaanvraag indient, kan het aanvraagformulier voor elke blueprint anders zijn. De verschillen in de formulieren worden geconfigureerd door de ontwerper van de blueprint.

De formuliers verschillen worden bepaald door de mate waarin u uw aanvraag kunt aanpassen. Mogelijk kunt u meerdere opties selecteren om uw aanvraag aan te passen, maar het kan ook zijn dat u geen opties hebt.

De blueprintarchitect kan bijvoorbeeld een blueprint ontwerpen zodat u een bepaald aantal CPU's kunt selecteren of waar u groot, gemiddeld of klein selecteert, waarvan elk een vooraf bepaald aantal CPU's is. Een blueprint kan ook verbiedend zijn en geen wijzigingen in de blueprint toestaan voordat u deze verzendt.

Nadat de aanvraag met succes is ingericht, wordt de geïmplementeerde werklust of service door u beheerd.

Voorwaarden

- U moet lid zijn van een bedrijfsgroep die rechten voor één of meer catalogusitems heeft. Zie [Rechten maken](#).
- Als u de implementatie namens een andere gebruiker uitvoert, moet de ondersteunende rol aan u zijn toegewezen in de bedrijfsgroep. Zie [Een bedrijfsgroep maken](#).

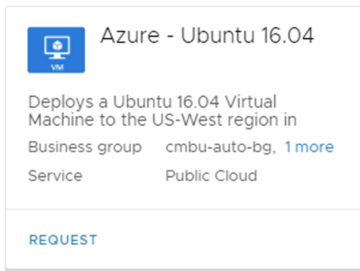
Procedure

- 1 Klik op **Catalogus**.
- 2 Als de ondersteunende rol aan u is toegewezen in een of meer bedrijfsgroepen en u de implementatie uitvoert namens een ander groepslid, voert u de naam van de gebruiker of de aangepaste groepsnaam in het zoekgebied **Namens** in.

De lijst met catalogusitems beperkt zich tot de items waarop de bedrijfsgroepen waarvan de geselecteerde gebruiker of groep lid is rechten hebben.

Als u geen gebruiker selecteert, wordt de aanvraag ingediend voor u.

- 3 Gebruik de zoek- en sorteeropties om het item te zoeken dat u wilt implementeren en klik op **Aanvragen**.



Azure - Ubuntu 16.04

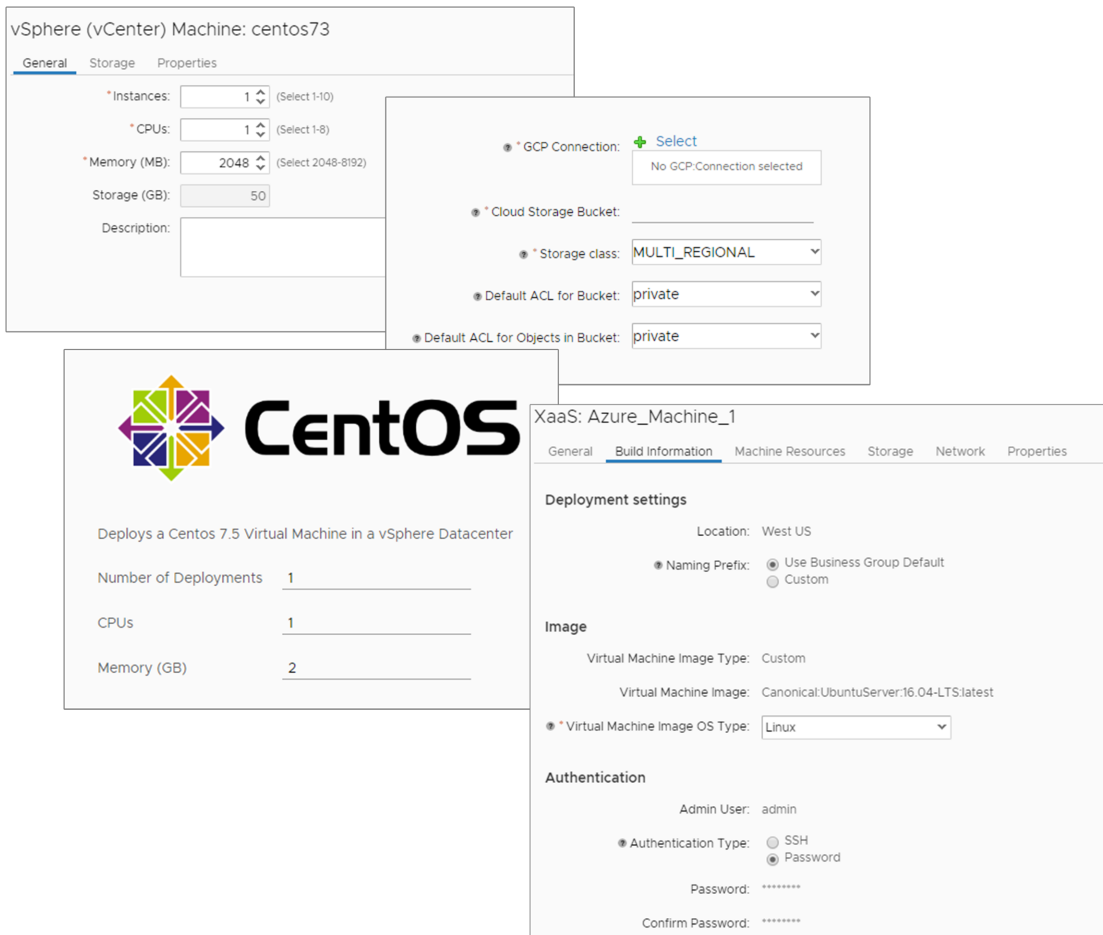
Deploys a Ubuntu 16.04 Virtual Machine to the US-West region in Business group cmbu-auto-bg, 1 more

Service Public Cloud

[REQUEST](#)

- 4 Als u lid bent van meer dan één bedrijfsgroep die rechten heeft op de blueprint, selecteert u de bedrijfsgroep die met de implementatie moet worden gekoppeld.
- 5 Configureer alle verplichte en eventuele andere beschikbare opties op het aanvraagformulier.

Het formulier kan verschillen afhankelijk van hoe de blueprint is geconfigureerd. Hieronder volgen voorbeelden die variëren van eenvoudig tot meer complex met meerdere tabbladen.



vSphere (vCenter) Machine: centos73

General Storage Properties

* Instances: 1 (Select 1-10)

* CPUs: 1 (Select 1-8)

* Memory (MB): 2048 (Select 2048-8192)

Storage (GB): 50

Description:

* GCP Connection: [Select](#)
No GCP Connection selected

* Cloud Storage Bucket:

* Storage class: MULTI_REGIONAL

* Default ACL for Bucket: private

* Default ACL for Objects in Bucket: private

XaaS: Azure_Machine_1

General **Build Information** Machine Resources Storage Network Properties

Deployment settings

Location: West US

* Naming Prefix: ☒ Use Business Group Default ☐ Custom

Image

Virtual Machine Image Type: Custom

Virtual Machine Image: Canonical.UbuntuServer:16.04-LTS.latest

* Virtual Machine Image OS Type: Linux

Authentication

Admin User: admin

* Authentication Type: ☐ SSH ☒ Password

Password: *****

Confirm Password: *****

- 6 Klik op **Indienen**.

Resultaten

De aanvraag wordt ingediend voor inrichting en het tabblad Implementaties wordt geopend, zodat u de voortgang van uw aanvraag kunt volgen.

Wat nu te doen

Controleer of uw aanvraag is geïmplementeerd. Zie [Provisioning-aanvragen controleren](#).

Werken met uw implementaties

Implementaties zijn ingerichte blueprints die u hebt aangevraagd uit de catalogus. U kunt de status van de ingediende aanvragen gedurende het provisioning-proces controleren, uw geïmplementeerde resources volgen en die geïmplementeerde resources beheren via acties.

Status aanvragen controleren

Aanvragen die uitgevoerd worden, worden weergegeven op het tabblad Implementaties. U gebruikt de kaart om het provisioning-proces tot voltooiing te volgen.

Als het provisioning-proces mislukt, kunt u het foutbericht en gebeurtenissen bekijken om te bepalen waar de aanvraag is mislukt en het probleem op te lossen. Zie [Mislukte provisioning-aanvragen testen en problemen oplossen](#).

The screenshot shows the 'Deployments' tab with a search bar and a sort dropdown set to 'Created Date (descending)'. Below the header, there is a table with one deployment item:

Icon	Name	ID	Status	Progress	Actions
	Ansible Word Press Install - PHP, MyS... <small>No description Owner: Jason McCloud Business group: cmbu-auto-bg</small>	#287 - Provision Ansible Word Press Install - PHP, MySql all in one -	In Progress	14%	CANCEL 3 minutes since submitted

Geïmplementeerde resources beheren

U beheert aanvragen op het tabblad Implementaties.

Het beheer omvat het verifiëren dat de implementatie is ingeschakeld. Het kan ook betekenen dat u de implementatie aanpast om aan uw behoeften te voldoen door deze in of uit te schalen. Of u moet mogelijk de implementatiegegevens te bekijken. Zie [Geïmplementeerde catalogusitems beheren](#) voor meer informatie.

Provisioning-aanvragen controleren

U gebruikt implementaties om de voortgang te bewaken van een aanvraag die u in de catalogus hebt gedaan. Als de resource met succes is ingericht, kunt u ook de geïmplementeerde resource beheren.

Als u geen aanvraag ziet die wordt uitgevoerd, is deze niet verzonden of is deze voltooid.

Aanvragen controleren

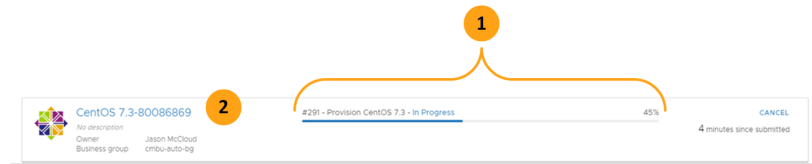
Om catalogusaanvragen te controleren, selecteert u **Implementaties**.

Volg de status van uw aanvraag in de implementatielijst.

- 1 Volg de status van uw aanvraag op de implementatiekaart (1). Als het de eerste keer is dat om het catalogusitem wordt gevraagd, geeft de statusbalk de voortgang weer zonder een percentage. Na de eerste implementatie leveren daaropvolgende aanvragen het volledige berekende percentage op.

Als u een actie uitvoert op de geïmplementeerde resource, geeft de statusbalk de status weer van de wijziging die u hebt geselecteerd.

- 2 Als u de actieve gegevens wilt bekijken, klikt u op de statusbalk van de implementatie (1) of de naam van de implementatie (2).



Bekijk de gegevens van de provisioning tijdens het implementatieproces.

- 1 Het tabblad Geschiedenis (3) biedt de implementatiegebeurtenissen en de invoerwaarden.
- 2 Het tabblad Gebeurtenissen (4) biedt de gegevens van de provisioning-aanvraag.
- 3 U kunt de provisioning-workflow (5) bekijken om te bepalen welke componenten momenteel worden geïmplementeerd.

Als een aanvraag het provisioning-proces niet voltooit, raadpleegt u [Mislukte provisioning-aanvragen testen en problemen oplossen](#).

Tasks	Component	Status	Depends On	Start Time	Completion Time
Submitted	Deployment	Successful		09/06/2018 1:50:06 PM	09/06/2018 1:50
Pre-approval	Deployment	Approved		09/06/2018 1:50:06 PM	09/06/2018 1:50
Provisioning	Deployment	In Progress		09/06/2018 1:50:08 PM	
Provision	centos73: vSphere (vCenter) Machine	Submitted	centos73		
Allocate	centos73: vSphere (vCenter) Machine	Submitted			
Post-approval	Deployment				
Completed	Deployment				

Annuleren van lopende aanvragen

Als u een aanvraag heeft ingediend maar vervolgens besluit deze te annuleren, stopt het provisioning-proces en worden alle geïmplementeerde resources teruggedraaid en opgeschoond.

Als het annuleringsproces te lang duurt, kunt u vragen dat uw beheerder de annulering forceert. Als beheerder kunt u een aanvraag annuleren die zich in de annuleringsstatus bevindt. Als u de annulering forceert, is het terugdraaien mogelijk niet voltooid en moet u handmatig resources op het doelsysteem opschonen.

Problemen oplossen met mislukte catalogusaanvragen

Wanneer u een catalogusitem aanvraagt, kan dit om verschillende redenen mislukken. Dit kan te wijten zijn aan netwerkverkeer, onvoldoende eindpuntresources of een foutieve blueprintspecificatie. Of de provisioning-aanvraag is gelukt, maar de implementatie lijkt niet te werken. U kunt vRealize Automation gebruiken om uw implementatie te onderzoeken, eventuele foutmeldingen te bekijken en te bepalen of het probleem zich in de omgeving bevindt die u kunt oplossen.

Als uw rol in vRealize Automation een catalogusconsument is en u geen beheerdersrechten hebt, kunt u deze workflow gebruiken voor een eerste probleemoplossing. U hebt misschien iemand in uw organisatie nodig om meer diepgaand onderzoek te doen.

Mogelijke foutstatussen

Als een provisioning-aanvraag mislukt, ziet u een van de volgende statussen.

- **Mislukt** Een aanvraag kan om verschillende redenen mislukken. Een oorzaak is dat het provisioning-proces niet werkte vanwege een gebrek aan resources op het doeleindpunt, door onvoldoende resources die beschikbaar zijn om de blueprint te ondersteunen of door een slecht ontworpen blueprint die moet worden verbeterd. Een andere oorzaak is dat de aanvraag goedkeuring van iemand anders in uw organisatie vereist en dat de goedkeurder de aanvraag heeft afgewezen. Het is ook mogelijk dat een actie die u hebt uitgevoerd voor een implementatie is mislukt. De fout kan worden veroorzaakt om de goedkeurings- of omgevingsredenen die al genoemd zijn.

Gebruik de volgende probleemoplossingsworkflow om de oorzaak van het probleem te onderzoeken. Als u het probleem kunt oplossen, bekijkt u uw actie-opties met betrekking tot **Verwijderen** en **Opnieuw indienen**. Zie [Opdrachten in het menu Actie voor ingerichte bronnen](#).

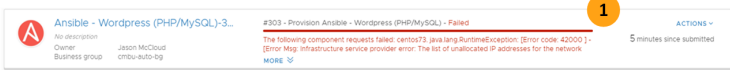
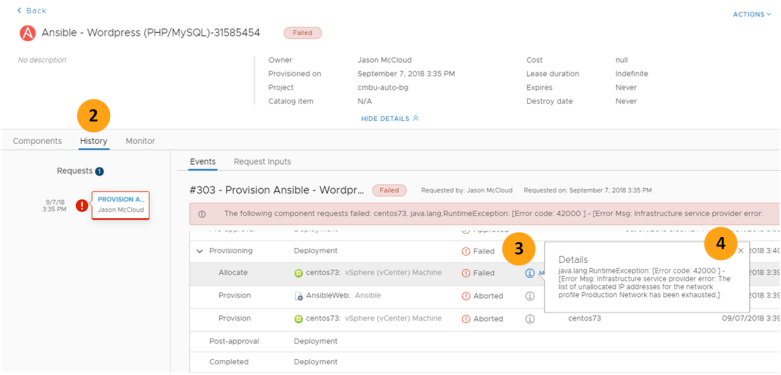
- **Gedeeltelijk succesvol.** Een aanvraag kan gedeeltelijk succesvol zijn, wat betekent dat sommige componenten geïmplementeerd zijn, maar niet alle provisioning-stappen met succes zijn afgerond.

Gebruik de volgende workflow voor probleemoplossing om te bepalen welke componenten slechts gedeeltelijk zijn gelukt en om de oorzaak van het probleem te onderzoeken. Als u het probleem kunt oplossen, bekijkt u uw actie-opties met betrekking tot **Verwijderen** en evalueert u of u **Hervatten** kunt gebruiken. Zie [Opdrachten in het menu Actie voor ingerichte bronnen](#) en [Werking van de actie Hervatten](#).

Workflow probleemoplossing voor catalogusconsumenten

U kunt deze workflow gebruiken om een mislukte implementatie te onderzoeken. Als uit uw onderzoek blijkt dat de fout werd veroorzaakt door een tijdelijk omgevingsprobleem, kunt u de fout oplossen en de aanvraag opnieuw indienen. Als het probleem de aanvraagspecificatie betreft, moet u mogelijk contact opnemen met uw blueprintarchitect.

Tabel 4-1. Hoe u moet beginnen met het oplossen van fouten

Werkstr oom	Stap voor probleemoplossing	Voorbeeld
1	Mislukte implementaties zijn op het tabblad Implementaties vermeld op de statusbalk. De kaart bevat het laatste foutbericht. Klik op de implementatienaam of voortgangsbalk voor meer informatie.	
2	U kunt de workflow gebeurtenissen op het tabblad Geschiedenis met implementatiegegevens gebruiken om te zien waar het provisioning-proces is mislukt. Deze workflow is ook handig wanneer u een actie voor een implementatie uitvoert, maar de wijziging mislukt.	

Tabel 4-1. Hoe u moet beginnen met het oplossen van fouten (vervolg)

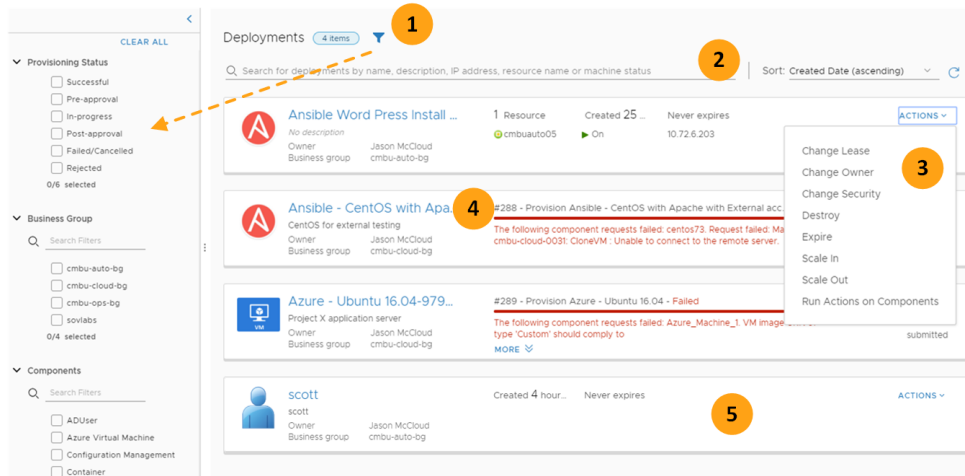
Werkstr oom	Stap voor probleemoplossing	Voorbeeld
3	De mislukte status geeft aan waar de workflow is mislukt.	
4	<p>De informatie biedt een meer uitgebreide versie van de foutmelding.</p> <p>Als deze informatie in de wegwijzerhulp niet voldoende is om het probleem te identificeren en op te lossen, kunt u aanvullend onderzoek doen in de gebeurtenislogboeken.</p> <p>Als u de gebeurtenislogboeken wilt weergeven, moet u over de benodigde gebruikersrol beschikken. Uw blueprintarchitect of beheerder kan extra probleemoplossing uitvoeren. Zie Mislukte provisioning-aanvragen testen en problemen oplossen.</p>	

Geïmplementeerde catalogusitems beheren

Als eigenaar van een implementatie of als beheerder die andere gebruikers ondersteunt, kunt u de implementatiegegevens gebruiken om de levenscyclus van geïmplementeerde items te beheren. De implementatiegegevens bieden de huidige informatie over elk component en gebruiken de geschiedenis om wijzigingen in de loop van de tijd bij te houden. Wanneer u werkt met de implementaties, kunt u de acties gebruiken om de geïmplementeerde items te wijzigen. Er zijn ook bepaalde wijzigingen die u kunt maken die de acties niet gebruiken.

Implementaties beheren vanuit de kaarten

De implementatiekaartlijst biedt een overzicht van uw implementaties. Zijn ze geslaagd? Zijn ze actief?



Gebruik de volgende opties om uw geïmplementeerde resource te vinden en beheren vRealize Automation.

- 1 **Filter** de lijst op basis van de huidige status van de aanvraag, de bedrijfsgroep waarvoor het geïmplementeerd is, welke subcomponenten worden opgenomen, de eigenaar/gebruiker en provisioning- of vervaldatum bereiken. De filters Provisioning-status en Aanvraagnummer gelden alleen voor het eerste provisioning-proces en niet voor alle daaropvolgende acties die u mogelijk uitvoert. De andere filters zijn van toepassing op de implementatie in het algemeen.
- 2 **Zoeken** en **Sorteren** om uw implementaties te vinden en te ordenen.
- 3 Als u de implementatie wilt beheren, klikt u op **Acties** om gemachtigde acties op implementatieniveau uit te voeren. U moet de implementatiegegevens openen om acties uit te voeren op afzonderlijke componenten. De acties kunnen standaardacties zijn die u hebt gemachtigd voor ontwerpblueprints, of het kunnen aangepaste XaaS-resource-acties zijn die u hebt gemaakt en gemachtigd zijn voor de XaaS-blueprint. Zie [Acties uitvoeren op geïmplementeerde resources](#) voor meer informatie over de standaardacties.
- 4 Klik op de naam van de implementatie om de details van de implementatie te bekijken en te beheren, inclusief provisioning-gebeurtenissen, geschiedenis en acties op componentniveau. De bovenste drie vertegenwoordigen initiële aanvragen voor provisioning voor standaardblueprints.
- 5 U kunt ook XaaS-implementatieaanvragen beheren die workflows uitvoeren. De workflows kunnen resulteren in resources of de workflows worden uitgevoerd op externe systemen. In dit voorbeeld heeft XaaS een gebruiker toegevoegd aan een Active Directory-domein.

Een implementatie beheren met behulp van de implementatiegegevens

U gebruikt de implementatiegegevens om de volgende managementinformatie uit te voeren.

- **Gegevens.** De algemene informatie die u aantreft op de kaart. U kunt ook de implementatienaam en -beschrijving wijzigen en acties op implementatieniveau uitvoeren.

- **Tabblad Componenten.** De volledige configuratie van ieder component. U kunt ook acties op componentniveau uitvoeren.
- **Tabblad Geschiedenis.** De complete geschiedenis van de wijzigingen in de implementatie. U kunt ook meer informatie vinden over de plaatsing en welke invoerwaarden zijn opgegeven voor elke wijziging.
- **Tabblad Controleren.** Als u met vRealize Operations Manager integreert, verschijnen de bewakingsstatistieken en waarschuwingen voor de implementatie en de componenten.
- **Acties.** Met behulp van de gegevens kunt u ook acties op implementatieniveau of op componentniveau uitvoeren.

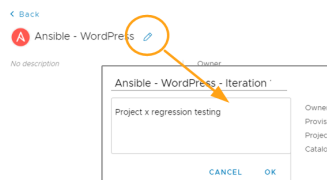
De gegevens van de implementatie gebruiken

De implementatiegegevens bieden meer dan de algemene informatie die u aantreft op de kaart. U kunt ook de implementatienaam en -beschrijving wijzigen en implementatie-acties en acties op componentniveau uitvoeren.

Controleer de algemene informatie over de implementatie, met inbegrip van de blueprint waarvan het is geïmplementeerd en de kosten.

De implementatienaam wijzigen

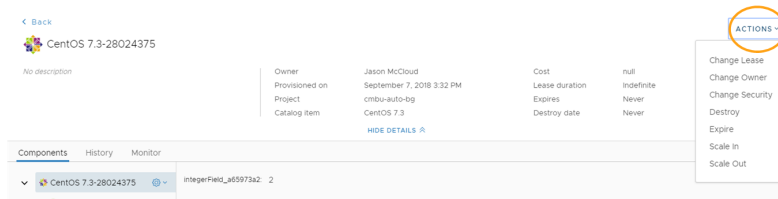
De implementatie heeft de naam van de blueprint. Deze naam heeft niet altijd een betekenis voor u als u met uw implementaties werkt. U kunt de naam en beschrijving veranderen in iets dat voldoet aan uw behoeften.



- 1 Wijs de naam aan en klik op het potloodpictogram.
- 2 Verander de naam en beschrijving in iets dat voor u betekenisvol is.

Acties op implementatieniveau uitvoeren

Acties op implementatieniveau zijn beperkt tot veranderingen die invloed hebben op de gehele implementatie. De lijst met beschikbare acties is afhankelijk van hoe uw bedrijfsgroep ze mag gebruiken.

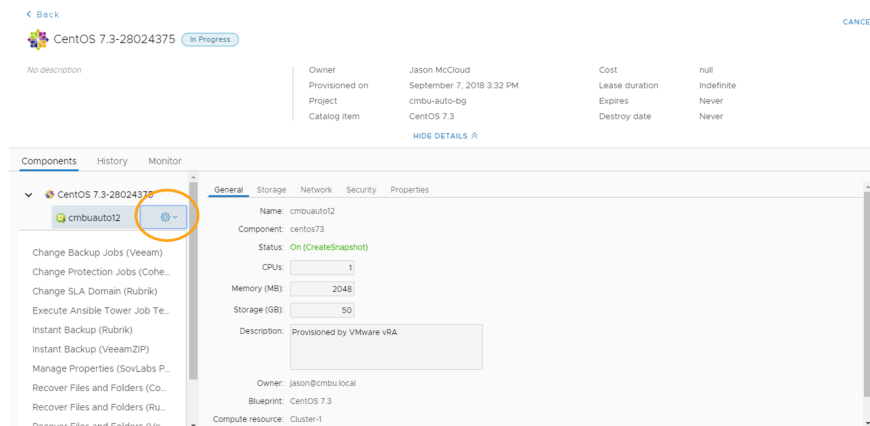


Implementatiecomponenten

Het tabblad Componenten in de implementatiegegevens biedt de volledige configuratie van alle componenten van de implementatie. U kunt zien hoe de machines en netwerken worden geconfigureerd. U kunt ook acties op componentniveau uitvoeren om de configuratie te wijzigen.

Controleer de gegevens van de component wanneer u de implementatie moet begrijpen die aan u is verstrekt of wanneer u een probleem met de instantie moet oplossen.

Alle wijzigingen die u aanbrengt met behulp van de acties worden weergegeven in de gegevens.



Acties op componentniveau uitvoeren

Acties op componentniveau zijn specifiek voor het component. De beschikbare acties zijn afhankelijk van hoe uw bedrijfsgroep deze acties mag gebruiken. Als uw beheerder u niet het recht heeft gegeven om acties uit te voeren, ziet u het tandwielpictogram of de actielijst niet.

Geschiedenis van de implementatie

Het tabblad Geschiedenis in de gegevens van de implementaties biedt de volledige geschiedenis, inclusief de implementatie van de eerste provisioning en alle veranderingen die zijn gemaakt met behulp van een of meer acties. U kunt de volledige geschiedenis van de provisioning gebruiken om te ontdekken wanneer er iets gewijzigd is en welke waarden zijn voorzien.

Controleer de gegevens van de geschiedenis indien u moet bepalen wanneer er iets is gewijzigd of wanneer u problemen met de instantie onderzoekt. U gebruikt de geschiedenis ook om mislukte implementaties op te lossen. Zie [Mislukte provisioning-aanvragen testen en problemen oplossen](#).

The screenshot displays the vRealize Automation interface for configuring a CentOS 7.3-28024375 machine. The interface is divided into several sections:

- Top Section:** Includes a 'Back' button, the machine name 'CentOS 7.3-28024375', and a status indicator 'In Progress'. Below this, there are fields for 'Owner' (Jason McCloud), 'Provisioned on' (September 7, 2018 3:32 PM), 'Project' (cmbu-auto-big), and 'Catalog item' (CentOS 7.3). There are also fields for 'Cost' (null), 'Lease duration' (indefinite), 'Expires' (never), and 'Destroy date' (never).
- Components Tab:** Shows a list of components with columns for Request ID, Component, Status, Depends On, Start Time, and Completion Time. The table includes rows for 'Submitted', 'Pre-approval', 'Create Snapshot', 'Post-approval', and 'Completed'.
- History Tab:** Shows a detailed view of the selected request, including the machine name, snapshot name, and snapshot description.
- Monitor Tab:** Shows a detailed view of the selected request, including the machine name, snapshot name, and snapshot description.

Implementatiebewaking op basis van vRealize Operations Manager

vRealize Automation kan vRealize Operations Manager-gegevens over uw implementaties tonen.

- Waarschuwingen op implementatieniveau
- Statistieken op machineniveau

Door de gefilterde reeks waarschuwingen en statistieken rechtstreeks in vRealize Automation te bekijken, hoeft u vRealize Operations Manager niet meer te openen en te doorzoeken. Hoewel starten in de context van vRealize Operations Manager niet mogelijk is, kunt u zich wel aanmelden en vRealize Operations Manager indien nodig gebruiken voor aanvullende gegevens.

vRealize Operations Manager-gegevens inschakelen

vRealize Automation kan pas vRealize Operations Manager-gegevens weergeven als u eerst instellingen en adapters configureert.

Voor de instelling zijn stappen in zowel vRealize Operations Manager als vRealize Automation vereist.

Voorwaarden

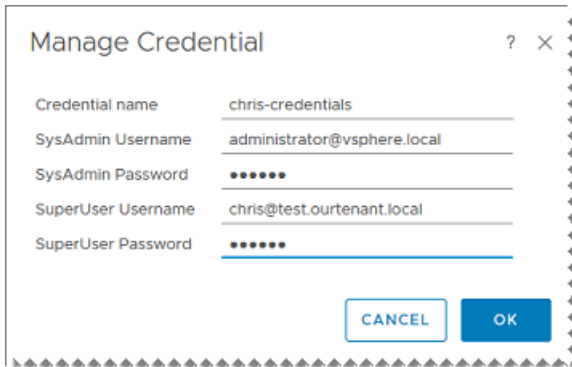
Controleer of u vRealize Operations Manager versie 6 of hoger hebt.

Procedure

- 1 Ga in vRealize Operations Manager naar **Beheer > Oplossingen**.
- 2 Controleer onder **Oplossingen** of u over de **vRealize Automation-oplossing** beschikt en of deze gegevens ontvangt.
 - a Selecteer de vRealize Automation-oplossing.
 - b Klik in de werkbalk boven de oplossingen op het tandwielpictogram voor configuratie.

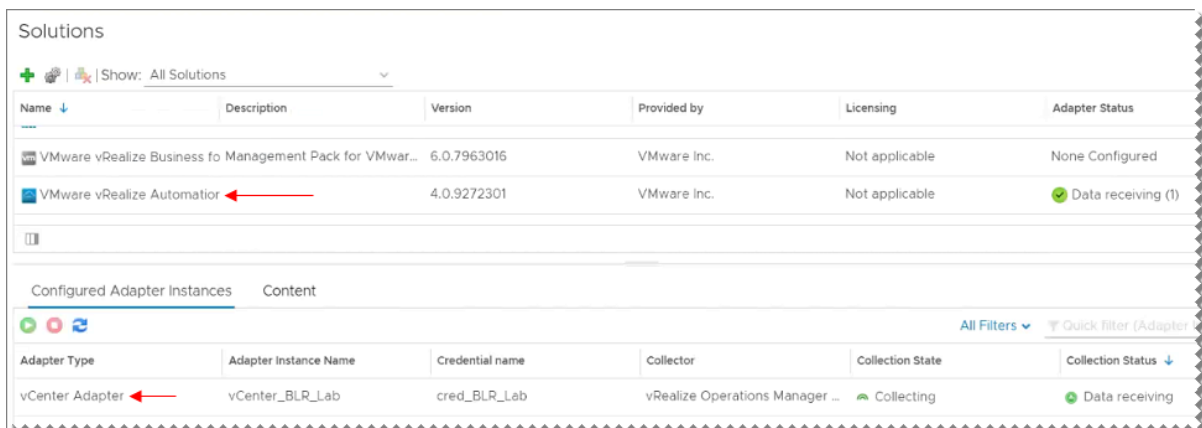
- c Ga onder **Instantie-instellingen** naar **Verificatiegegevens** en klik op het groene plusteken om verificatiegegevens toe te voegen.

Naam van verificatiegegevens	Beschrijving van deze set verificatiegegevens
SysAdmin	Gebruikersnaam en wachtwoord van de standaard vRealize Automation-tenantbeheerder, gewoonlijk administrator@vsphere.local
SuperUser	Gebruikersnaam en wachtwoord van een account met hoge toegangsrechten voor de werkende vRealize Automation-tenant



- d Sla de verificatiegegevens op en test of de verbinding werkt.
- 3 Controleer onder **Geconfigureerde adapterinstanties** of u over een **vCenter Adapter** beschikt voor het vSphere-endpoint waarop vRealize Automation is ingericht en of deze gegevens ontvangt.

Figuur 4-1. Oplossingen en adapters voor vRealize Operations Manager



- 4 Ga in vRealize Operations Manager naar **Waarschuwingen > Waarschuwinginstellingen**.

- 5 Controleer of de waarschuwings- en symptoomdefinities zo zijn ingesteld dat ze de gewenste vRealize Automation-waarschuwingen genereren.

De meeste vRealize Automation-gebruikers moeten er alleen voor zorgen dat de implementatiestatus goed blijft. Aanvullende waarschuwingen op het niveau van virtual machines kunnen verwarrend zijn en details bevatten die niet kunnen worden beheerd met vRealize Automation.

Voor [vRealize Automation-waarschuwingen](#) is de algemene implementatie het bovenliggende object. Virtual machines binnen de implementatie zijn onderliggende objecten.

Waarschuwingen worden standaard gegeven op het niveau van de implementatie, het hoofdniveau.

Het staat u vrij vRealize Operations Manager te gebruiken om waarschuwingen op implementatieniveau te maken die aanvullende specifieke symptomen blootleggen. Het kan bijvoorbeeld zijn dat u alle SQL Server-problemen in een implementatie wilt tonen.

- 6 Ga in vRealize Automation naar **Beheer > Terugwinning > Statistiekeraanbieder**.
- 7 Selecteer **vRealize Operations Manager-endpoint**.
- 8 Voer de vRealize Operations Manager URL `https://master-node-FQDN-or-IP/suite-api/` en de gebruikersnaam en het wachtwoord van een account met beheerdersrechten voor vRealize Operations Manager in.

Opmerking Wanneer er meer dan één verificatiebron is, voert u de gebruikersnaam in de notatie `user@domain@source` in, waarbij `@source` de LDAP-importbron in vRealize Operations Manager is. Het gebruikersaccount vereist minimaal de rol `ReadOnly` en objectrechten voor de vCenter-adaptor en Cloud vCenter Server.

- 9 Test de verbinding en sla deze op.
- 10 Klik op **Implementaties**, selecteer een implementatie en controleer of het tabblad Controle wordt weergegeven.

Het tabblad Controle wordt alleen weergegeven als vRealize Operations Manager is geselecteerd als statistiekeraanbieder.

Waarschuwingen van vRealize Operations Manager

Wanneer de controle is ingeschakeld, haalt vRealize Automation vRealize Operations Manager-waarschuwingen over uw implementaties op.

U opent de controle door op een implementatie te klikken en het tabblad **Controle** te selecteren. Zie [vRealize Operations Manager-gegevens inschakelen](#) als dit tabblad ontbreekt.

Markeer de implementatienaam boven aan de onderdelenstructuur aan de linkerzijde om waarschuwingen weer te geven.

- U kunt de ernst en de tekst van de waarschuwingen bekijken.
- Filter en sorteer de gegevens in de kolom om te focussen op probleemgebieden.
- Alleen statuswaarschuwingen worden weergegeven. Andere soorten waarschuwingen zoals efficiëntie of risico's worden niet ondersteund.

Components	History	Monitor																		
<div> <div>VC-65-DND Deployme...</div> <div>VC-65-DND</div> </div>																				
<div> <div>Alerts</div> <div>5</div> </div>																				
<div> <div>Total VMs</div> <div>1</div> </div>																				
<div> <div>Total CPUs</div> <div>4</div> </div>																				
<div> <div>Total Memory</div> <div>16384 MB</div> </div>																				
<div> <div>Total Storage</div> <div>270 GB</div> </div>																				
<table> <thead> <tr> <th>Criticality</th><th>Alert</th><th>Created On</th></tr> </thead> <tbody> <tr> <td>Warning</td><td>One or more VM's of Deployment is not having memory ballooning</td><td>7/26/18, 7:47 PM</td></tr> <tr> <td>Critical</td><td>One or more VM's Disk usage is above 70%</td><td>7/26/18, 7:47 PM</td></tr> <tr> <td>Immediate</td><td>One or more VM is having CPU in idle state</td><td>7/26/18, 7:47 PM</td></tr> <tr> <td>Critical</td><td>Most deployment resources have health issues</td><td>7/26/18, 7:47 PM</td></tr> <tr> <td>Critical</td><td>One or more VM of Deployment is running out of Guest file system disk space</td><td>7/26/18, 7:47 PM</td></tr> </tbody> </table>			Criticality	Alert	Created On	Warning	One or more VM's of Deployment is not having memory ballooning	7/26/18, 7:47 PM	Critical	One or more VM's Disk usage is above 70%	7/26/18, 7:47 PM	Immediate	One or more VM is having CPU in idle state	7/26/18, 7:47 PM	Critical	Most deployment resources have health issues	7/26/18, 7:47 PM	Critical	One or more VM of Deployment is running out of Guest file system disk space	7/26/18, 7:47 PM
Criticality	Alert	Created On																		
Warning	One or more VM's of Deployment is not having memory ballooning	7/26/18, 7:47 PM																		
Critical	One or more VM's Disk usage is above 70%	7/26/18, 7:47 PM																		
Immediate	One or more VM is having CPU in idle state	7/26/18, 7:47 PM																		
Critical	Most deployment resources have health issues	7/26/18, 7:47 PM																		
Critical	One or more VM of Deployment is running out of Guest file system disk space	7/26/18, 7:47 PM																		

Statistieken van vRealize Operations Manager

Wanneer de controle is ingeschakeld, haalt vRealize Automation vRealize Operations Manager-statistieken over uw implementaties op.

U opent de controle door op een implementatie te klikken en het tabblad **Controle** te selecteren. Zie [vRealize Operations Manager-gegevens inschakelen](#) als dit tabblad ontbreekt.

Vouw de onderdelenstructuur aan de linkerzijde uit en markeer een virtual machine om statistieken weer te geven.

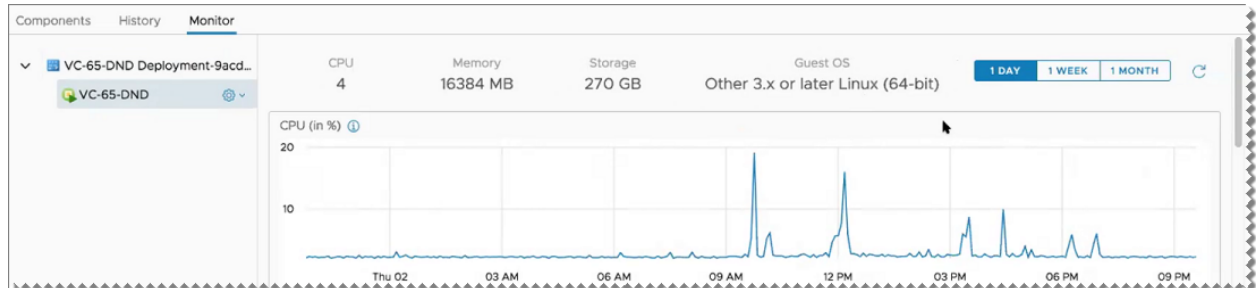
- Statistieken worden niet in cache opgeslagen. Ze zijn rechtstreeks afkomstig van vRealize Operations Manager en het kan even duren om ze te laden.
- Alleen statistieken van virtual machines worden weergegeven. Statistieken van andere componenten, zoals vCloud Director, Software of XAAS, worden niet ondersteund.
- Alleen de statistieken van vSphere virtual machines worden weergegeven. Andere cloudproviders zoals AWS of Azure worden niet ondersteund.

Statistieken worden weergegeven als tijdlijngrafieken die pieken en dalen voor de volgende meetwaarden tonen.

- CPU
- Geheugen

- Opslag IOPS
- Netwerk MBPS

Als u de naam van een specifieke statistiek wilt weergeven, klikt u op het blauwe informatiepictogram in de linkerbovenhoek van de tijdlijn.



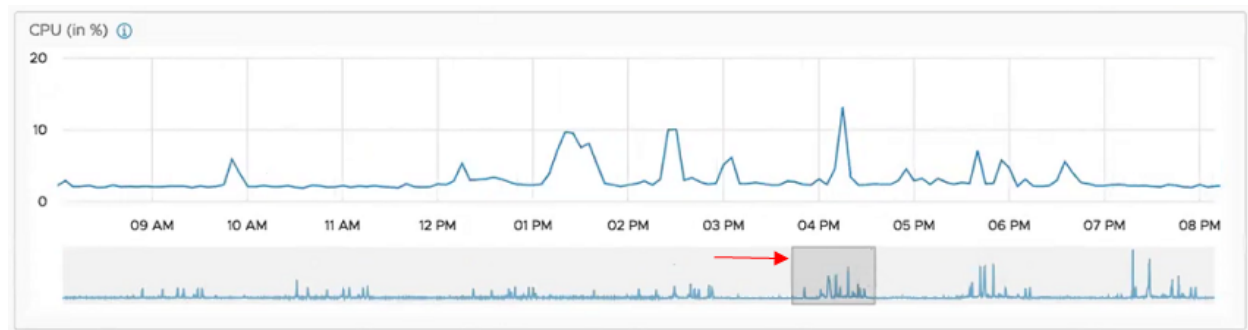
Maatregelen nemen op basis van door vRealize Operations Manager verstrekte gegevens

Wanneer door vRealize Operations Manager verstrekte statistieken op een probleem wijzen, kunt u rechtstreeks corrigerende maatregelen nemen in vRealize Automation.

Als u door vRealize Operations Manager verstrekte statistieken wilt bekijken, klikt u op een implementatie en selecteert u het tabblad **Controle**. Zie [vRealize Operations Manager-gegevens inschakelen](#) als dit tabblad ontbreekt.

Problemen opzoeken

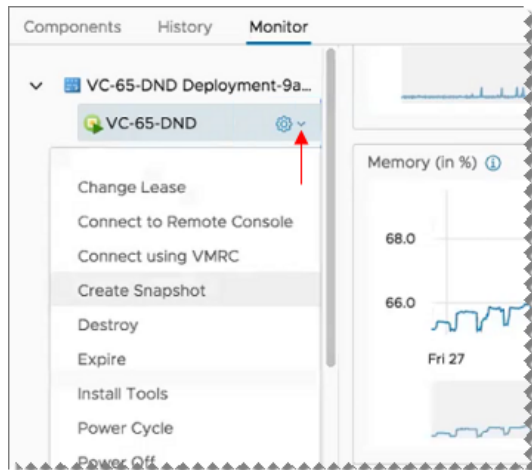
Er zijn statistieken voor de afgelopen dag, week of maand beschikbaar. Als u wilt inzoomen op een probleemgebied, selecteert u een klein gebied in het onderste, grijs weergegeven gedeelte onder een tijdlijn van een willekeurige statistiek:



Wijzigingen aanbrengen

Wanneer een probleem optreedt, kunt u direct in dezelfde interface corrigerende maatregelen nemen.

Als er bijvoorbeeld voortdurend pieken in het geheugengebruik zijn, kunt u geheugen toevoegen. Klik op het vervolgkeuzemenu voor de virtual machine in de onderdelenstructuur aan de linkerkant en gebruik de opties in het contextmenu om onderhoud uit te voeren of de configuratie te wijzigen.



Acties uitvoeren op geïmplementeerde resources

De acties die beschikbaar zijn voor een geïmplementeerde resource zijn afhankelijk van het type resource, hoe de actie is geconfigureerd en beschikbaar gemaakt voor ingerichte items en de operationele status van het item.

De geconfigureerde acties die beschikbaar zijn voor een implementatie of een onderdeel van de implementatie worden weergegeven in het menu **Acties** van de geselecteerde implementatie of het implementatieonderdeel.

De lijst met beschikbare acties wordt bepaald door wat uw bedrijfsgroep gerechtigd is uit te voeren voor de implementatie en resource of machinetypecomponent. Of een actie beschikbaar is, is afhankelijk van het machinetype of de status.

Als het item is ingericht via een XaaS-blueprint, moet u de bronacties met bijbehorende rechten maken en publiceren voor dezelfde service als die waarmee het item is ingericht. De lijst met beschikbare acties wordt bepaald door het itemtype en de huidige status van het item.

Tot de beschikbare acties voor een item dat als IaaS-machine is ingericht, behoren mogelijk ook XaaS-bronacties, voor zover deze aan het item zijn toegewezen.

Opdrachten in het menu Actie voor ingerichte bronnen

Acties zijn wijzigingen die u op ingerichte bronnen kunt uitvoeren. De acties van vRealize Automation worden gebruikt om de levenscyclus van de bronnen te beheren.

Welke commando's beschikbaar zijn in de menu's **Actie** is afhankelijk van de wijze waarop de rechten van de bron waarop de acties worden uitgevoerd zijn ingesteld door de bedrijfsgroepbeheerder of tenantbeheerder. De beschikbaarheid van een menuoptie hangt ook af van het type bron en de operationele status van het item.

U kunt slechts één actie tegelijk uitvoeren. Als u een tweede actie op een bron wilt uitvoeren, moet u wachten totdat de eerste actie de gewenste wijziging heeft voltooid.

Tabel 4-2. Opdrachten in het menu Actie

Actie	Brontype	Beschrijving
Gekoppeld zwevend IP	Machine (OpenStack)	Koppel een zwevend IP-adres met een OpenStack-machine.
Annuleren	Machine	<p>Annuleer een actie voor een nieuwe configuratie die momenteel wordt uitgevoerd.</p> <p>Alleen acties die kunnen worden teruggedraaid naar een vorige status kunnen door gebruikers worden geannuleerd.</p> <p>Als een actie het terugdraaien naar een vorige status niet ondersteunt, bijvoorbeeld Uitschakelen, kan alleen een gebruiker met tenantbeheerderrechten de aanvraag annuleren.</p>
Lease wijzigen	Implementatie en machine	Wijzig het resterende aantal dagen van de lease voor een specifieke machine of voor alle bronnen van een implementatie. Als u geen waarde opgeeft, verloopt de lease niet.
NAT-regels wijzigen	NAT-netwerk	Voeg nieuwe regels toe voor het doorsturen van NAT-poorten, orden regels opnieuw, bewerk bestaande regels of verwijder regels.
Eigenaar wijzigen	Implementatie	<p>Wijzig de eigenaar van de hele implementatie en alle bijbehorende bronnen. Alleen bedrijfsgroepbeheerders en ondersteuningsgebruikers kunnen een andere eigenaar aan een implementatie toewijzen.</p> <p>De machine moet de status Aan, Uit of Actief hebben wanneer u de eigenaar wijzigt. Anders mislukt deze actie en wordt het volgende bericht weergegeven:</p> <p><code>Deze actie is ongeldig voor de machine.</code></p>
Beveiliging wijzigen	Implementatie	<p>U kunt bestaande beveiligingsgroepen en beveiligingstags van NSX verwijderen of er nieuwe toevoegen. U kunt ook beveiligingsgroepen op aanvraag verwijderen.</p> <p>Zie Beveiligingsitems aan een implementatie toevoegen of eruit verwijderen voor meer informatie.</p>

Tabel 4-2. Opdrachten in het menu Actie (vervolg)

Actie	Brontype	Beschrijving
Verbinding maken met behulp van VMRC	Machine	<p>Maak verbinding met de virtual machine met behulp van een VMRC 8.x-toepassing.</p> <p>Deze actie kan alleen worden gebruikt als de VMRC-toepassing is geïnstalleerd op het lokale systeem van de servicecatalogusgebruiker die de actie uitvoert.</p> <p>Voor installatie- en gebruiksinstructies raadpleegt u de VMware Remote Console-documentatie. Als u de software wilt downloaden, gaat u naar VMware Remote Console downloaden.</p> <p>VMRC 8.x vervangt de vorige VMware Remote Console.</p>
Verbinding maken met externe console	Machine	<p>Maak verbinding met de geselecteerde machine met behulp van VMware Remote Console.</p> <p>De console van de virtual machine wordt weergegeven in de browser. VMRC 8.x vervangt de VMware Remote Console.</p>
Verbinding maken via consoleticket	Machine (OpenStack en KVM)	Gebruik een OpenStack- of KVM-consoleticket voor een VMware Remote Console-verbinding om verbinding te maken met de virtual machine.
Verbinding maken via ICA	Machine (Citrix)	Maak verbinding met de Citrix-machine via het protocol Independent Computing Architecture.
Verbinding maken via RDP	Machine	Gebruik Microsoft Remote Desktop Protocol om verbinding te maken met de machine.
Verbinding maken via SSH	Machine	<p>Maak verbinding met de geselecteerde machine met behulp van SSH.</p> <p>De optie Verbinden met SSH werkt alleen als uw browser over een invoegtoepassing beschikt die SSH ondersteunt, zoals de FireSSH SSH-terminalclient voor Mozilla Firefox en Google Chrome. Als de invoegtoepassing aanwezig is en u Verbinding maken via SSH selecteert, wordt een SSH-console weergegeven en wordt u gevraagd uw verificatiegegevens als beheerder in te voeren.</p> <p>Als u deze actie wilt gebruiken, moet u de aangepaste eigenschap Machine.SSH via een eigenschapsgroep of zelfstandige, aangepaste eigenschap toevoegen aan het machineonderdeel van de blueprint en op 'waar' instellen.</p>

Tabel 4-2. Opdrachten in het menu Actie (vervolg)

Actie	Brontype	Beschrijving
Verbinding maken via virtueel bureaublad	Machine	Gebruik het virtuele bureaublad van Microsoft om verbinding te maken met de geselecteerde machine.
Momentopname maken	Virtual machine	Maak een momentopname van de virtual machine. Als u toestemming hebt voor slechts twee momentopnamen en die allebei al hebt gemaakt, moet u eerst een momentopname verwijderen voordat deze opdracht weer beschikbaar is.
Momentopname verwijderen	Virtual machine	Verwijder een momentopname van de virtual machine.

Tabel 4-2. Opdrachten in het menu Actie (vervolg)

Actie	Brontype	Beschrijving
Vernietigen	Implementatie, machine en beveiligingsgroep op aanvraag	<p>Onmiddellijke vernietiging van een ingerichte bron.</p> <p>Met uitzondering van XaaS is het vernietigen van onderdelen van een implementatie geen aanbevolen werkwijze. Gebruik de inschaalactie om het aantal machines in uw implementatie te verminderen, of de hele implementatie te vernietigen.</p> <p>U moet deze actie uitvoeren om XaaS-bronnen te vernietigen, zelfs als ze deel uitmaken van een implementatie die u vernietigt. Andere bronnen worden aan het einde van hun lease- of archiefperiode vernietigd.</p> <p>De actie Vernietigen is niet beschikbaar voor de volgende implementatiescenario's:</p> <ul style="list-style-type: none"> ■ implementaties van fysieke machines ■ implementaties met een bestaand NSX-netwerk of bestaande NSX-beveiligingsbron ■ implementaties met een NSX load balancer op aanvraag als bron <p>Omdat een NSX load balancer tot een NSX edge behoort, wordt de load balancer als bron samen met de NSX edge vernietigd en worden de bronnen weer vrijgegeven. Bij de vernietiging van een machinelaag met load balancing, wordt de load balancer verwijderd uit de pool op de bijbehorende NSX Edge.</p> <p>Opmerking De actie Vernietigen kan een bericht terugsturen dat de actie is voltooid, zelfs als deze de machine-implementatie niet uit haar endpoint kan verwijderen. Bijvoorbeeld, als een vSphere-machine zich in een niet-vSAN-gegevensopslag bevindt en haar VMX-bestand beschadigde of anderszins ongeldige gegevens bevat. U kunt het aanvraaglogboek bekijken voor meer informatie, zelfs als het bericht Vernietigen aangeeft dat de actie is voltooid. Bij geforceerd vernietigen van een machine in deze status blijft deze mogelijk uitgevoerd op het endpoint waardoor er IP-conflicten optreden. Als de beschadiging wordt gecorrigeerd op het eindpunt (buiten vRealize Automation) kunt u de actie Vernietigen opnieuw proberen uit te voeren.</p>

Tabel 4-2. Opdrachten in het menu Actie (vervolg)

Actie	Brontype	Beschrijving
		<p>Beheerders van bedrijfsgroepen kunnen een implementatie geforceerd vernietigen na een mislukte vernietigingsaanvraag. Bij het forceren van een vernietiging krijgt vRealize Automation de opdracht mislukte pogingen om individuele bronnen te vernietigen te negeren tijdens het vernietigen van de implementatie. Zie Vernietiging van een implementatie forceren na een mislukte vernietigingsaanvraag voor meer informatie over het forceren van een vernietiging.</p> <p>Opmerking Opslagruimte en geheugen die door middel van een reservering zijn toegewezen aan een ingerichte machine, worden vrijgemaakt wanneer de machine waaraan ze zijn gekoppeld, in vRealize Automation wordt verwijderd door de actie Vernietigen. De opslagruimte en het geheugen worden niet vrijgemaakt als de machine wordt verwijderd in de vCenter Server.</p> <p>Wanneer u een implementatie vernietigt die een Amazon-machineonderdeel bevat, kunt u meer dan één EBS-volume tegelijk vernietigen, afhankelijk van hoe de instelling Volumes verwijderen is geconfigureerd in de blueprint. Zie Instellingen voor Amazon-machineonderdelen voor meer informatie.</p> <p>Wanneer u een implementatie vernietigt die een Amazon-machineonderdeel bevat, worden alle EBS-volumes die tijdens de levenscyclus aan de machine werden toegevoegd niet vernietigd maar verwijderd. vRealize Automation biedt geen optie voor het vernietigen van de EBS-volumes.</p>
Koppeling met zwevende IP ongedaan maken	Machine (Openstack)	Verwijder het zwevende IP van de Openstack-machine.

Tabel 4-2. Opdrachten in het menu Actie (vervolg)

Actie	Brontype	Beschrijving
Afwijzen	Geen brontype. Eerste inrichtingsaanvraag of een actie is mislukt.	<p>U wijst een mislukte aanvraag af. U annuleert een aanvraag in behandeling.</p> <ul style="list-style-type: none"> ■ Als de afgewezen aanvraag een implementatieaanvraag is, verwijdert de afwijzing de mislukte implementatie uit uw lijst met implementaties. ■ Als de afgewezen aanvraag een actie is, verwijdert de afwijzing de mislukte actieaanvraag van de kaart, zodat de implementatie weer in de vorige toestand terechtkomt. <p>U moet een mislukte actieaanvraag sluiten, zodat u andere acties kunt zien die voor de gekoppelde implementatie worden uitgevoerd. U moet ook mislukte acties afwijzen, zodat de implementatiegebruikers de machinegeschiedenis kunnen zien.</p> <p>U kunt de afwijzing niet uitvoeren op aanvragen die door de API zijn ingediend en deze blokkeert geen acties die door de API zijn ingediend.</p> <p>Deze actie is beschikbaar voor alle eerste mislukte inrichtingsaanvragen. Er is geen recht vereist.</p>
Nieuwe configuratie uitvoeren	Machine	Configureer de machine onmiddellijk opnieuw of plan de herconfiguratie voor een later tijdstip.
Vervallen	Implementatie en machine	Beëindig de implementatie- of machinelease voor alle bronnen van de implementatie.
Certificaat exporteren	Machine	Exporteer het certificaat van een cloudmachine.
Herinnering voor vervaldatum ontvangen	Machine	Downloadt een gebeurtenisbestand van de agenda voor de huidige leasevervaldatum.
VMware Tools installeren	Machine	Installeer VMware Tools op een vSphere virtual machine.
Power Cycle	Machine	Schakel de machine uit en schakel deze vervolgens weer in.
Uitschakelen	Machine	Schakel de machine uit tijdens het afsluiten van het gastbesturingssysteem.
Inschakelen	Machine	Schakel de machine in. Als de machine onderbroken was, wordt de normale werking hervat vanaf het punt waarop de machine onderbroken was.

Tabel 4-2. Opdrachten in het menu Actie (vervolg)

Actie	Brontype	Beschrijving
Reboot	Machine	Start het gastbesturingssysteem van een vSphere virtual machine opnieuw op. U kunt deze actie alleen gebruiken als VMware Tools is geïnstalleerd op de machine.

Tabel 4-2. Opdrachten in het menu Actie (vervolg)

Actie	Brontype	Beschrijving
Opnieuw configureren	Machine	<p>Een bedrijfsgroepbeheerder, ondersteunende gebruiker of machine-eigenaar kan de volgende acties uitvoeren om de geselecteerde vSphere virtual machine opnieuw te configureren:</p> <ul style="list-style-type: none"> ■ Beschrijving wijzigen ■ Instellingen voor CPU, geheugen, netwerk en schijven wijzigen ■ Aangepaste eigenschappen en eigenschapsgroepen toevoegen, bewerken en verwijderen ■ Een netwerkadapter toevoegen, bewerken, opnieuw ordenen of verwijderen voor regels voor het doorsturen van NAT-poorten ■ Afsluiten opnieuw configureren ■ Machine-eigenaar wijzigen (alleen beschikbaar voor bedrijfsgroepbeheerders en ondersteuningsgebruikers) <p>U kunt geen opslagreserveringsbeleid wijzigen als hierdoor het opslagprofiel op een schijf kan worden gewijzigd.</p> <p>Zie Machineherconfiguratie-instellingen opgeven en overwegingen voor herconfiguratie voor meer informatie.</p> <p>Als u de optie Updates voor bestaande implementaties doorvoeren op de pagina Blueprintinstellingen in de bronblueprint hebt geselecteerd, wordt elke verhoging of uitbreiding van de minimum- of maximuminstellingen voor de CPU, het geheugen of de opslag in de blueprint gepusht naar actieve implementaties die via die blueprint zijn ingericht. Zie Instellingen voor blueprunteigenschappen voor meer informatie.</p> <p>Beheer geen door vRealize Automation beheerde NSX-objecten buiten vRealize Automation. Als u bijvoorbeeld de lidpoort van een geïmplementeerde load balancer in NSX wijzigt in plaats van in vRealize Automation, dan kan de NSX gegevensverzameling worden onderbroken. In- en uitschaalbewerkingen leveren ook onverwachte resultaten op.</p>

Tabel 4-2. Opdrachten in het menu Actie (vervolg)

Actie	Brontype	Beschrijving
Opnieuw configureren	Load balancer	<p>Een eigenaar van een machine, ondersteunende gebruiker, tenantbeheerder of bedrijfsgroepbeheerder met rechten kan de instellingen in een virtuele server wijzigen en virtuele servers in de NSX-load balancer toevoegen of verwijderen:</p> <p>Zie Een load balancer in een implementatie opnieuw configureren voor meer informatie.</p> <p>Zie Het onderdeel load balancer op aanvraag toevoegen voor meer informatie over instellingen voor virtuele servers in de load balancer.</p> <p>Beheer geen door vRealize Automation beheerde NSX-objecten buiten vRealize Automation. Als u bijvoorbeeld de lidpoort van een geïmplementeerde load balancer in NSX wijzigt in plaats van in vRealize Automation, dan kan de NSX gegevensverzameling worden onderbroken. In- en uitschaalbewerkingen leveren ook onverwachte resultaten op.</p>
VDI registreren	Virtual machine (XenServer)	Registreer de installatiekopie van de virtuele schijf op XenServer-items.
Uit catalogus verwijderen	Implementaties	Verwijder door XaaS ingerichte bronnen uit de catalogus. U kunt deze bewerking uitvoeren op bestaande objecten en objecten die niet langer beschikbaar zijn in de Orchestrator-inventaris.

Tabel 4-2. Opdrachten in het menu Actie (vervolg)

Actie	Brontype	Beschrijving
Opnieuw inrichten	Machine	<p>Vernietigt de machine en start daarna een inrichtingswerkstroom om een machine met dezelfde naam te maken.</p> <p>Bij de aanvraag voor het opnieuw inrichten van een machine kan een bekend probleem optreden. vRealize Automation geeft dan in de catalogus de status Voltooid voor de hernieuwde inrichting, terwijl de werkelijke status In behandeling is. Als u de hernieuwde inrichting van een machine hebt aangevraagd, hebt u de volgende mogelijkheden om de status van de opnieuw ingerichte machine te controleren:</p> <ul style="list-style-type: none"> ■ Infrastructuur > Beheerde machines ■ Tabblad Implementaties ■ Beheer > Gebeurtenissen > Gebeurtenislogboeken <hr/> <p>Opmerking Het is niet mogelijk om een Amazon-machine in te richten.</p> <hr/> <p>Zie het VMware Knowledge Base-artikel Reprovisioned machine tasks... (2065873) op http://kb.vmware.com/kb/2065873.</p>
Opnieuw indienen	Geen brontype. Eerste inrichtingsaanvraag is mislukt.	<p>Dien een mislukte inrichtingsaanvraag opnieuw in. De opnieuw ingediende aanvraag begint bij het begin van het inrichtingsproces met de waarden die al zijn ingevoerd.</p> <p>Als een aanvraag mislukt en u het probleem kunt oplossen, kunt u de aanvraag opnieuw indienen in plaats van een nieuwe aanvraag te maken. Als de fout het gevolg is van onjuiste waarden, bijvoorbeeld gegevensopslag die geen ondersteuning biedt voor uw aanvraag, moet u een nieuwe aanvraag maken met de nieuwe waarden.</p> <p>Deze actie is beschikbaar voor alle eerste mislukte inrichtingsaanvragen. Er is geen recht vereist.</p>

Tabel 4-2. Opdrachten in het menu Actie (vervolg)

Actie	Brontype	Beschrijving
Hervatten	Implementatie	<p>Hervat een gedeeltelijk gelukke inrichtingsaanvraag. Hervatten gaat verder vanaf het punt van de mislukking.</p> <p>Als een implementatie tijdens het inrichtingsproces mislukt vanwege tijdelijke omgevings- of infrastructuurproblemen, time-outs of andere problemen die kunnen worden verholpen buiten de aanvraag om, kunt u het inrichtingsproces hervatten in plaats van een nieuwe inrichtingsaanvraag te maken. Als het probleem is veroorzaakt door fouten in de blueprint, is hervatten niet mogelijk. U moet dan niet proberen om het proces te hervatten, maar een nieuwe implementatie aanvragen.</p> <p>Als de aanvraag van een implementatie slechts een gedeeltelijk succes is en u het probleem kunt oplossen, kunt u de actie hervatten. De hervatte aanvraag gaat verder vanaf het punt van de mislukking.</p> <p>Zie Werking van de actie Hervatten voor meer informatie.</p>
Momentopname terugzetten	Virtual machine	<p>De vorige momentopname van de machine terugzetten. U kunt deze actie alleen gebruiken als u een bestaande momentopname hebt.</p>

Tabel 4-2. Opdrachten in het menu Actie (vervolg)

Actie	Brontype	Beschrijving
Inschalen	Implementatie	<p>Vernietigt niet-gebruikte instanties van machines in uw implementatie voor aanpassing aan een kleinere capaciteitsvraag. De machineonderdelen en alle softwareonderdelen die erop zijn geïnstalleerd, worden vernietigd. Afhankelijke softwareonderdelen en netwerk- en beveiligingsonderdelen worden bijgewerkt voor de nieuwe configuratie van de implementatie. XaaS-onderdelen zijn niet schaalbaar en kunnen niet worden bijgewerkt tijdens schalingsbewerkingen.</p> <p>U kunt gedeeltelijk gelukke schalingsbewerkingen proberen te repareren door de implementatie opnieuw te schalen. U kunt een implementatie echter niet naar de huidige grootte schalen, en als u op deze manier een gedeeltelijk gelukke schaling probeert te repareren, wordt de toewijzing van hangende bronnen niet opgeheven. U kunt de details van de uitvoering van aanvragen bekijken en erachter komen welke taken op welke knooppunten zijn mislukt zodat u beter kunt bepalen of u de gedeeltelijk gelukke schaling kunt oplossen met een andere schalingsbewerking.</p> <p>Mislukte en gedeeltelijk gelukke schalingsbewerkingen hebben geen impact op de werking van uw oorspronkelijke implementatie, en u kunt uw catalogusitems blijven gebruiken wanneer u fouten oplost.</p>

Tabel 4-2. Opdrachten in het menu Actie (vervolg)

Actie	Brontype	Beschrijving
Uitschalen	Implementatie	<p>Richt extra instanties van machines in uw implementatie in om aan een groeiende capaciteitsvraag te voldoen. De machineonderdelen en alle softwareonderdelen die erop zijn geïnstalleerd, worden vernietigd. Afhankelijke softwareonderdelen en netwerk- en beveiligingsonderdelen worden bijgewerkt voor de nieuwe configuratie van de implementatie. XaaS-onderdelen zijn niet schaalbaar en kunnen niet worden bijgewerkt tijdens schalingsbewerkingen.</p> <p>U kunt gedeeltelijk gelukke schalingsbewerkingen proberen te repareren door de implementatie opnieuw te schalen. U kunt een implementatie echter niet naar de huidige grootte schalen, en als u op deze manier een gedeeltelijk gelukke schaling probeert te repareren, wordt de toewijzing van hangende bronnen niet opgeheven. U kunt de details van de uitvoering van aanvragen bekijken en erachter komen welke taken op welke knooppunten zijn mislukt zodat u beter kunt bepalen of u de gedeeltelijk gelukke schaling kunt oplossen met een andere schalingsbewerking.</p> <p>Mislukte en gedeeltelijk gelukke schalingsbewerkingen hebben geen impact op de werking van uw oorspronkelijke implementatie, en u kunt uw catalogusitems blijven gebruiken wanneer u fouten oplost.</p> <p>Als u de optie Updates voor bestaande implementaties doorvoeren op de pagina Blueprintinstellingen in de bronblueprint hebt geselecteerd, wordt elke verhoging van de minimum- of maximuminstellingen voor de CPU, het geheugen of de opslag in de blueprint gepusht naar actieve implementaties die via die blueprint zijn ingericht. Zie Instellingen voor blueprunteigenschappen voor meer informatie.</p>
Afsluiten	Machine	Sluit het gastbesturingssysteem af en schakel de machine uit. U kunt deze actie alleen gebruiken als VMware Tools is geïnstalleerd op de machine.
Onderbreken	Machine	Onderbreek de machine zodat deze niet kan worden gebruikt en deze geen systeembronnen verbruikt behalve de opslag die de machine gebruikt.

Tabel 4-2. Opdrachten in het menu Actie (vervolg)

Actie	Brontype	Beschrijving
Registratie ongedaan maken	Machine	Verwijder de machine uit de inventaris zonder ze te verwijderen. Niet-geregistreerde machines zijn onbruikbaar.
Registratie ongedaan maken	Netwerk	Verwijder het netwerk uit de inventaris zonder het te vernietigen. Niet-geregistreerde netwerken zijn onbruikbaar.
Registratie VDI ongedaan maken	Virtual machine (XenServer)	Maak de registratie van de installatiekopie van de virtuele schijf op XenServer-items ongedaan.

Problemen met ontbrekende acties in het menu met bronacties oplossen

U krijgt als machine- of broneigenaar niet alle acties te zien waarvoor rechten zijn verleend voor een ingericht item.

Probleem

In een omgeving waarvan u weet dat uw gebruiker of bedrijfsgroep recht had op een actie, verwacht u alle acties te zien wanneer u een item in uw lijst **Implementatie** selecteert.

Oorzaak

Welke acties beschikbaar zijn, is afhankelijk van het type ingerichte bron, de operationele status van de bron en hoe deze is geconfigureerd en beschikbaar is gesteld. De volgende lijst bevat een aantal redenen waarom u niet alle geconfigureerde acties te zien krijgt.

- De actie is niet van toepassing door de huidige status van de ingerichte bron. Uitschakelen is bijvoorbeeld alleen beschikbaar wanneer de machine is ingeschakeld.
- De actie is niet van toepassing op het geselecteerde itemtype. De actie wordt niet in de lijst weergegeven als het item de actie niet ondersteunt. De actie Momentopname maken is bijvoorbeeld niet beschikbaar voor een fysieke machine, terwijl de actie Verbinding maken met behulp van RDP niet beschikbaar is als het geselecteerde item een Linux-machine is.
- De actie is weliswaar van toepassing op het ingerichte brontype, maar is gedeactiveerd in de infrastructuurblueprint. Een gedeactiveerde actie wordt nooit als beschikbaar weergegeven voor de items die zijn ingericht op basis van de blueprint.
- Er zijn bij de inrichting van het item waarvoor u de actie wilt uitvoeren, geen rechten verleend voor die actie. Het menu Acties bevat alleen acties waarvoor rechten zijn verleend, hetzij via een IaaS-blueprint of als XaaS-bronactie.
- De actie is gemaakt als XaaS-bronactie, maar er zijn hiervoor geen rechten verleend bij de inrichting van het item waarvoor u de actie wilt uitvoeren. Het menu Acties toont alleen acties waarvoor rechten zijn verleend.
- De actie is mogelijk beperkt door de geconfigureerde doelcriteria voor XaaS-bronacties of brontoewijzingen voor ingerichte IaaS-machines.

Oplossing

- ◆ Controleer of de actie van toepassing is op het ingerichte item of op de status van het ingerichte item.
- ◆ Controleer of de actie is geconfigureerd en is opgenomen in de verleende rechten waarmee het item is ingericht.

Een momentopname van uw machine maken

Afhankelijk van de manier waarop uw beheerders uw omgeving hebben geconfigureerd, kunt u mogelijk een momentopname van uw virtual machine maken. Een momentopname is een installatiekopie van een virtual machine op een specifiek tijdstip. Het is een ruimtebesparende kopie van de oorspronkelijke VM-installatiekopie. Momentopnamen zijn een eenvoudige manier om een systeem te herstellen na beschadigingen, gegevensverlies of beveiligingsrisico's. Nadat u een momentopname van uw virtual machine hebt gemaakt, kunt u deze toepassen en uw systeem terugzetten naar het punt waarop de momentopname is gemaakt.

Wanneer u een momentopname van het geheugen maakt, legt de momentopname de status vast van de energie-instellingen van de virtual machine en, optioneel, het geheugen van de virtual machine. Wanneer u de geheugenstatus van de virtual machine vastlegt, duurt het langer om een momentopname te maken. U ervaart mogelijk een tijdelijke vertraging in de reactie via het netwerk.

Voorwaarden

- Een bestaande virtual machine die is ingeschakeld, uitgeschakeld of onderbroken.
- Als uw virtual machine is geconfigureerd voor een of meer onafhankelijke schijven, schakelt u de machine uit voordat u een momentopname maakt. U kunt geen momentopname maken wanneer de machine is ingeschakeld. Voor informatie over schijfconfiguratie raadpleegt u *Tabel aangepaste eigenschappen met V*.
- De tenantbeheerder of bedrijfsgroepbeheerder heeft u het recht gegeven voor de actie momentopname.

Procedure

- 1 Klik op **Implementaties**.
- 2 Zoek de implementatie met de machine waarvan u een snapshot wilt maken en klik op de implementatienaam.
- 3 Klik op de virtuele machine en klik op het tandwielpictogram voor acties op het tabblad **Componenten**.
Het actiemenu van het component wordt weergegeven.
- 4 Klik op **Momentopname maken** in het menu Acties.
- 5 Voer een naam in en desgewenst een beschrijving.

- 6 Als u de geheugen- en energie-instellingen van de machine wilt vastleggen, selecteert u **Geheugen opnemen**.
- 7 Klik op **Indienen**.

Externe verbinding maken met een machine

Via de vRealize Automation-console kunt u extern verbinding maken met een machine.

Als u VMware Remote Console gebruikt om verbinding te maken, raadpleegt u het Knowledge Base-artikel [VMRC-verbindingsproblemen oplossen in vRealize Automation \(2114235\)](#).

Voorwaarden

- Meld u aan bij vRealize Automation als een **machine-eigenaar, tenantbeheerder** of **bedrijfsgroepbeheerder**.
- Controleer of VMware Tools is geïnstalleerd.

VMware Tools moet zijn geïnstalleerd op de vRealize Automation-client om volledige toegang te krijgen bij de verbinding vanuit de VMware Remote Console. Als VMware Tools niet is geïnstalleerd, kunnen er problemen optreden nadat de verbinding met de doelmachine is gemaakt, waardoor bijvoorbeeld de muisaanwijzer en de muisknoppen niet werken. Zie de *Ondersteuningsmatrix voor vRealize Automation* in de [productdocumentatie voor vRealize Automation](#) voor meer informatie over ondersteunde versies van VMware Tools.

- Controleer of de ingerichte machine is ingeschakeld.
- Sta netwerkverkeer tussen de vRealize Automation-toepassing(en) en de ESXi-server via poort 902 toe.
- Sta netwerkverkeer tussen de vRealize Automation-toepassing(en) en de clientbrowser via poort 8444 toe.
- Sta netwerkverkeer tussen de Windows-server(s) van IaaS-webonderdelen en gekoppelde vSphere-endpoint(s) via poort 443 toe.

Procedure

- 1 Klik op **Implementaties**.
- 2 Zoek de implementatie met de machine waarmee u moet worden verbonden en klik op de implementatienaam.
- 3 Zoek de machine en klik op het tandwielpictogram voor acties op het tabblad **Componenten**. Het actiemenu van het component wordt weergegeven.
- 4 Selecteer de methode voor externe verbindingen.
 - Selecteer **Verbinding maken via RDP** om verbinding te maken via RDP.
 - Selecteer **Verbinden met remote console** om verbinding te maken via VMware Remote Console.
 Reageer op alle prompts.

5 Klik op **Verbinden** en volg de procedure om u aan te melden bij de machine.

6 Als u klaar bent, meldt u zich af en sluit u het browservenster.

Externe consoles voor vSphere configureren met niet-vertrouwde SSL-certificaten

Als uw vRealize Automation-implementatie gebruikmaakt van niet-vertrouwde certificaten, moet u uw clientbrowser configureren zodat het certificaat wordt vertrouwd voordat u externe consoles kunt gebruiken met VMware Remote Console. Hoe u dit doet, verschilt per browser.

Als vRealize Automation is geconfigureerd met een vertrouwd SSL-certificaat voor uw omgeving, hoeft VMware Remote Console niet verder meer te worden geconfigureerd voor clientbrowsers. Wanneer een vRealize Automation-toepassingscertificaat wordt vervangen en een vertrouwd certificaat is, hoeft u de certificaatgegevens voor de browserclient niet bij te werken.

Als u het certificaat wilt vervangen, raadpleegt u het onderwerp over het vervangen van een vRealize Automation-toepassing-certificaat in de *Systeembeheer*-handleiding voor vRealize Automation.

Externe verbindingen waarbij VMware Remote Console wordt gebruikt voor machines die worden ingericht op vSphere, worden beveiligd door vRealize Automation-toepassingscertificaten via een proxyconsole. VMware Remote Console vereist een browser met WebSockets-ondersteuning die het vRealize Automation-toepassingscertificaat vertrouwt. U verkrijgt het certificaat op het rootniveau van de virtuele toepassing via een van de adressen op <https://vra-vx.eng.mycompany.com/>.

Meer informatie over ondersteuningsvereisten voor browsers en vSphere vindt u in de *Ondersteuningsmatrix voor vRealize Automation*.

Firefox configureren om een certificaat van vRealize Automation te vertrouwen

U moet niet-vertrouwde certificaten van de vRealize Automation-toepassing handmatig importeren in browsers op de client om VMware Remote Console te gebruiken op clients die worden ingericht op vSphere.

Zie de *VMware vRealize Support Matrix* in het vRealize Automation [Informatiecentrum](#) voor meer informatie over ondersteunde versies van Firefox.

Opmerking Als vRealize Automation is geconfigureerd met een vertrouwd SSL-certificaat voor uw omgeving, hoeft VMware Remote Console niet verder meer te worden geconfigureerd voor clientbrowsers.

Procedure

- 1** Meld u vanuit een Firefox-browser aan bij de vRealize Automation-toepassing.
Er verschijnt een bericht dat aangeeft dat het certificaat niet wordt vertrouwd.
- 2** Selecteer **Menu openen > Opties**.
- 3** Klik op **Privacy & beveiliging** en klik vervolgens op **Certificaten bekijken**.
- 4** Klik in het dialoogvenster Certificatenbeheerder op **Servers** en klik vervolgens op **Uitzondering toevoegen**.

- 5 Voeg de URL voor uw vRealize Automation-appliance toe met als poort 8444.

Bijvoorbeeld, `https://your-vra-fqdn-domain:8444`.

- 6 Klik op **Certificaat ophalen** en klik vervolgens op **Beveiligingsuitzondering bevestigen**.
- 7 Klik op **OK**.

Resultaten

U kunt nu zonder certificaatfouten verbinding maken met de externe console.

Internet Explorer configureren om een certificaat voor vRealize Automation Appliance te vertrouwen

U moet niet-vertrouwde vRealize Automation-toepassing-certificaten handmatig importeren in browsers op de client om VMware Remote Console te gebruiken op clients die worden ingericht op vSphere.

Opmerking Als vRealize Automation is geconfigureerd met een vertrouwd SSL-certificaat voor uw omgeving, hoeft VMware Remote Console niet verder meer te worden geconfigureerd voor clientbrowsers.

De stappen in deze procedure gelden voor zelfondertekende certificaten en certificaten die zijn uitgegeven door een certificeringsinstantie.

Voor meer informatie over de ondersteunde versies van Internet Explorer, raadpleegt u de *Ondersteuningsmatrix voor VMware vRealize* op de VMware-website.

Procedure

- 1 Meld u vanuit een Internet Explorer-browser aan bij vRealize Automation-toepassing.
- 2 Klik op **Certificaat weergeven** in het foutbericht voor het certificaat dat in de adresbalk van de browser verschijnt.
- 3 Klik op het tabblad **Algemeen** van het venster Certificaatgegevens.
- 4 Controleer of de gegevens van het certificaat kloppen en klik op **Certificaat installeren**.
- 5 Selecteer **Alle certificaten in het onderstaande archief opslaan** in het dialoogvenster Certificaatarchief.
- 6 Klik op **Bladeren** om het certificaatarchief te zoeken.
- 7 Selecteer **Vertrouwde basiscertificeringsinstantie** en klik op **OK**.
- 8 Klik op **Volgende** in het dialoogvenster Certificaatarchief.
- 9 Klik op **Ja** in het dialoogvenster Beveiligingswaarschuwing om het certificaat te installeren.
- 10 Start de browser opnieuw.

Resultaten

U kunt nu zonder certificaatfouten verbinding maken met de externe console.

Chrome configureren om een certificaat voor vRealize Automation Appliance te vertrouwen

U moet niet-vertrouwde vRealize Automation-toepassing-certificaten handmatig importeren in browsers op de client om VMware Remote Console te gebruiken op clients die worden ingericht op vSphere.

Zie voor meer informatie over ondersteunde versies van Chrome de *Ondersteuningsmatrix voor vRealize Automation* in de [productdocumentatie voor vRealize Automation](#).

Opmerking Als vRealize Automation is geconfigureerd met een vertrouwd SSL-certificaat voor uw omgeving, hoeft VMware Remote Console niet verder meer te worden geconfigureerd voor clientbrowsers.

Chrome en Internet Explorer gebruiken onder Windows hetzelfde certificaatarchief. Dit betekent dat de certificaten die door Internet Explorer worden vertrouwd, ook door Chrome worden vertrouwd. Als u vertrouwde certificaten voor Chrome wilt instellen, importeert u ze vanuit Internet Explorer. Zie [Internet Explorer configureren om een certificaat voor vRealize Automation Appliance te vertrouwen](#) voor meer informatie over deze procedure.

Start Chrome na afloop van deze procedure opnieuw.

Als u een certificaat op een Mac-besturingssysteem permanent wilt vertrouwen, downloadt u het certificaatbestand en installeert u het certificaat als vertrouwd in uw certificaatbeheer.

Procedure

- 1 Meld u vanuit een Chrome-browser aan bij vRealize Automation-toepassing.
- 2 Klik op het pictogram *Sitegegevens bekijken* naast de adresbalk in de browser en klik op het pictogram **Certificaat** om de certificaatinformatie weer te geven.
- 3 Sla het certificaat op.
- 4 Start de toepassing Sleutelhangertoegang, die zich doorgaans in de map Hulpprogramma's van de map Programma's bevindt.
- 5 Selecteer **Bestand > Items importeren**.
- 6 Selecteer het eerder opgeslagen certificaatbestand in het scherm voor toegang tot de sleutelhanger.

Stel de waarde van **Doelsleutel** in op **Systeem**.
- 7 Klik op **Openen** om het certificaat te importeren.
- 8 Start de browser opnieuw.

Machineherconfiguratie-instellingen opgeven en overwegingen voor herconfiguratie

De platforms vSphere, vCloud Air en vCloud Director bieden ondersteuning voor de herconfiguratie van bestaande machines in een implementatie om specificaties zoals CPU, geheugen en opslag te wijzigen.

Aanvragen voor nieuwe configuraties zijn onderhevig aan goedkeuring op basis van rechten, beleidsregels en de acties die zijn ingeschakeld voor het machineonderdeel in de blueprint.

Het herconfigureren van een virtual machine die is toegewezen aan een netwerk op aanvraag, wordt niet ondersteund. U kunt een NIC die is aangesloten in een netwerk op aanvraag, niet herconfigureren. Als u een NAT op aanvraag of een geleid netwerk probeert te herconfigureren, wordt de fout `Original network [<network>] is not selected in the machine's reservation.` weergegeven, blijven de netwerken op de machine intact en blijven de IP-adressen op de machine ongewijzigd.

Als u rechten hebt voor de acties **Nieuwe configuratie annuleren (machine)** en **Nieuwe configuratie uitvoeren (machine)**, kunt u een hernieuwde configuratie annuleren of een mislukte nieuwe configuratie opnieuw proberen uit te voeren.

Een schijf uitbreiden op een VM die is ingericht met een gekoppelde kloonblueprint wordt niet ondersteund.

U kunt machines niet opnieuw configureren met behulp van onderdeelprofielen van **Size of Image**. Het bereik van de CPU, het geheugen en de opslag wordt berekend op basis van het profiel en blijft beschikbaar voor het opnieuw configureren van acties. Gebruik bijvoorbeeld een kleine waardeset (1 CPU, 1024 MB geheugen en 10 GB opslag), een middelgrote waardeset (3 CPU's, 2048 MB geheugen, 12 GB opslag) en een grote waardeset (5 CPU's, 3072 MB geheugen, 15 GB opslag) voor **Size**. De beschikbare bereiken tijdens de herconfiguratie van de machine zijn 1-5 CPU's, 1024-3072 MB geheugen en 1-15 GB opslag.

vRealize Automation maakt een momentopname van de blueprint tijdens de implementatie. Als u herconfiguratieproblemen ondervindt tijdens het bijwerken van de machine-eigenschappen zoals CPU en RAM in een implementatie, raadpleegt u het Knowledge Base-artikel [2150829 vRA 7.x Blueprint Snapshotting](#).

Voorwaarden

- Meld u aan bij vRealize Automation als een **machine-eigenaar, ondersteuningsgebruiker, bedrijfsgroepsgebruiker met een rol voor gedeelde toegang** of **bedrijfsgroepbeheerder**.
- De machine die u opnieuw wilt configureren moet de status **Aan** of **Uit** hebben en geen actieve configuratiestatus.
- Het machinetype moet vSphere, vCloud Air of vCloud Director zijn, hoewel de instellingen van NSX alleen gelden voor vSphere.
- Controleer of u over het recht beschikt om een machine opnieuw te configureren.

Procedure

- 1 Klik op **Implementaties**.
- 2 Zoek de implementatie met de machine die u opnieuw moet configureren en klik op de implementatiennaam.
- 3 Klik op de virtuele machine en klik op het tandwielpictogram voor acties op het tabblad **Componenten**.

Het actiemenu van het component wordt weergegeven.

- 4 Selecteer **Opnieuw configureren**.
- 5 Selecteer het juiste tabblad voor de instellingen die u opnieuw wilt configureren.

Tabel 4-3. Herconfiguratiewijzigingen aanvragen

Tabblad	Onderwerp
Algemeen	CPU's en geheugen opnieuw configureren
Opslag	Opslaginstellingen bewerken
Netwerk	Netwerkinstellingen wijzigen Zie NAT-regels in een implementatie wijzigen als u NAT-regels wilt wijzigen.
Beveiliging	Zie Beveiligingsitems aan een implementatie toevoegen of eruit verwijderen als u beveiligingsinstellingen opnieuw wilt configureren.
Propertes	De instellingen van aangepaste eigenschappen en eigenschapsgroepen wijzigen

Wat nu te doen

[De aangevraagde machineherconfiguratie uitvoeren](#) .

CPU's en geheugen opnieuw configureren

U kunt het aantal CPU's of de hoeveelheid geheugen en opslag die wordt gebruikt door de machine die wordt ingericht, wijzigen binnen de grenzen die worden gesteld door de blueprint voor de inrichting.

Voor ingerichte Amazon-implementaties kunt u alle opslagvolumes in de implementatie opnieuw configureren met uitzondering van het rootvolume.

Een schijf uitbreiden op een VM die is ingericht met een gekoppelde kloonblueprint wordt niet ondersteund.

Voorwaarden

[Machineherconfiguratie-instellingen opgeven en overwegingen voor herconfiguratie](#).

Procedure

- 1 Klik op het tabblad **Algemeen**.
- 2 Geef het aantal CPU's op in het tekstvak **CPU's**.
- 3 Geef de hoeveelheid geheugen op in het tekstvak **Geheugen (MB)**.
- 4 Geef de hoeveelheid opslag op in het tekstvak **Opslag (GB)**.

Wat nu te doen

Geef aanvullende nieuwe machineconfiguratie-instellingen op. Als u klaar bent met het wijzigen van machine-instellingen, start u de aanvraag voor de nieuwe machineconfiguratie. Zie [De aangevraagde machineherconfiguratie uitvoeren](#) .

Opslaginstellingen bewerken

U kunt een opslagvolume toevoegen, verwijderen of wijzigen op een virtual machine die is ingericht.

U kunt de opslag op een schijf van het IDE-type niet opnieuw configureren.

Opslagruimte en geheugen die door middel van een reservering zijn toegewezen aan een ingerichte machine, worden vrijgemaakt wanneer de machine waaraan ze zijn gekoppeld, in vRealize Automation wordt verwijderd door de actie Vernietigen. De opslagruimte en het geheugen worden niet vrijgemaakt als de machine wordt verwijderd in de vCenter Server.

Bijvoorbeeld: u kunt geen reservering verwijderen die is gekoppeld aan machines in een bestaande implementatie. Als u geïmplementeerde machines handmatig verplaatst of verwijdt in de vCenter Server, blijft vRealize Automation de geïmplementeerde machines als live herkennen en voorkomen dat u bijbehorende reserveringen verwijdt.

U kunt sommige instellingen, zoals capaciteit en het opslagreserveringsbeleid, wijzigen na de inrichting en implementatie van machine.

De waarden voor **Stationsletter/Koppelingspad** en **Label** worden toegepast op de gastagent tijdens de inrichting. Deze waarden worden niet bijgewerkt na de inrichting en zijn dus mogelijk niet actueel. Als u gegevens wilt verzamelen en hun huidige waarden wilt weergeven, kunt u een aangepaste vRealize Orchestrator-werkstroom maken en uitvoeren.

Voorwaarden

[Machineherconfiguratie-instellingen opgeven en overwegingen voor herconfiguratie.](#)

Voor ingerichte Amazon-implementaties kunt u alle opslagvolumes in de implementatie opnieuw configureren met uitzondering van het rootvolume.

Procedure

1 Klik op het tabblad **Opslag**.

2 Bekijk of bewerk de opslagopties naar wens.

- Voeg een nieuw volume toe, indien beschikbaar.
- Verwijder een volume, indien beschikbaar.

Een pictogram dat niet geselecteerd kan worden geeft aan dat het volume niet verwijderd kan worden, zoals bijvoorbeeld het volume van een gekoppelde kloon.

- Wijzig de grootte van een volume, indien beschikbaar.

U kunt de grootte van bestaande volumes niet verminderen. De grootte van het volume wordt beperkt door de totale hoeveelheid opslag die is opgegeven in de blueprint, min de hoeveelheid aan opslag die is toegewezen aan andere volumes.

Wat nu te doen

Geef aanvullende nieuwe machineconfiguratie-instellingen op. Als u klaar bent met het wijzigen van machine-instellingen, start u de aanvraag voor de nieuwe machineconfiguratie. Zie [De aangevraagde machineherconfiguratie uitvoeren](#).

Netwerkinstellingen wijzigen

U kunt een netwerkadapter toevoegen, bewerken of verwijderen.

U kunt de volgende netwerkinstellingen wijzigen tijdens het proces van de machineherconfiguratie:

- Voeg NIC's toe of verwijder NIC's.
- Wijs IP-adressen toe of geef ze vrij voor bestaande NIC's.
- Wijs nieuwe IP-adressen toe aan NIC's, op voorwaarde dat het netwerk geen NAT-netwerk op aanvraag is of een geleid netwerk op aanvraag is.

Een geleid netwerk op aanvraag of een NAT-netwerk op aanvraag kunt u niet opnieuw configureren.

Voor een herconfiguratie van een netwerk moeten de bron- en doelnetwerken in de reservering worden geselecteerd.

Wanneer u NIC's toevoegt, worden IP-adressen toegewezen. Wanneer u NIC's verwijdert, worden IP-adressen vrijgegeven.

Wanneer u netwerkinstellingen wijzigt op basis van reserverings- en netwerkprofielgegevens, wordt het nieuwe IP-adres voor het netwerk in vRealize Automation toegewezen, maar wordt de geïmplementeerde machine niet bijgewerkt met de nieuwe IP-informatie. U moet het IP-adres handmatig aan de machine toewijzen nadat het reconfiguratieproces is voltooid.

Het herconfigureren van een virtual machine die is toegewezen aan een netwerk op aanvraag, wordt niet ondersteund. U kunt een NIC die is aangesloten in een netwerk op aanvraag, niet herconfigureren. Als u een NAT op aanvraag of een geleid netwerk probeert te herconfigureren, wordt de fout `Original network [<network>] is not selected in the machine's reservation.` weergegeven, blijven de netwerken op de machine intact en blijven de IP-adressen op de machine ongewijzigd.

NSX-netwerkinstellingen wijzigen wordt niet ondersteund voor implementaties die vanuit vRealize Automation 6.2.x zijn geüpgraded of gemigreerd naar deze vRealize Automation-versie.

Voorwaarden

[Machineherconfiguratie-instellingen opgeven en overwegingen voor herconfiguratie.](#)

Procedure

- 1 Klik op het tabblad **Netwerk**.

2 (Optioneel) Voeg een netwerkadapter toe.

a Klik op **Nieuwe netwerkadapter**.

b Selecteer een netwerk in het vervolgkeuzemenu **Netwerkpad**.

Alle netwerken die zijn geselecteerd op de reservering van de machine, zijn beschikbaar.


c Typ een statisch IP-adres voor het netwerk in het tekstvak **Adres**.

Het IP-adres moet nog niet zijn toegewezen in het netwerkprofiel dat is toegewezen in de reservering.

d Klik op het pictogram **Opslaan** ()

3 (Optioneel) Verwijder een netwerkadapter.

a Zoek de netwerkadapter.

b Klik op het pictogram **Verwijderen** ()

U kunt de netwerkadapter 0 niet verwijderen.

4 (Optioneel) Bewerk een netwerkadapter.

a Zoek de netwerkadapter.

b Klik op het pictogram **Bewerken** ()

c Selecteer een netwerk in het vervolgkeuzemenu **Netwerkpad**.

d Klik op het pictogram **Opslaan** ()

Wat nu te doen

Geef aanvullende nieuwe machineconfiguratie-instellingen op. Als u klaar bent met het wijzigen van machine-instellingen, start u de aanvraag voor de nieuwe machineconfiguratie. Zie [De aangevraagde machineherconfiguratie uitvoeren](#).

De instellingen van aangepaste eigenschappen en eigenschapsgroepen wijzigen

U kunt aangepaste eigenschappen in de geïmplementeerde machine bewerken, toevoegen of verwijderen.

U kunt aangepaste eigenschappen niet gebruiken om waarden in te voeren voor het schijfnummer, de capaciteit, het label of het opslagreserveringsbeleid van het volume. U moet deze waarden invoeren door een volume toe te voegen of te bewerken in de tabel Opslagvolumes. Zie [Opslaginstellingen bewerken](#).

Voorwaarden

[Machineherconfiguratie-instellingen opgeven en overwegingen voor herconfiguratie](#).

Procedure**1** Klik op het tabblad **Eigenschappen**.

- 2 Klik op **Nieuwe eigenschap** om een eigenschap toe te voegen.
- 3 Geef de naam voor de eigenschap op in het tekstvak **Naam**.
- 4 Geef de eigenschapswaarde op in het tekstvak **Waarde**.
- 5 Schakel het selectievakje **Gecodeerd** in om de waarde te versleutelen.
- 6 Schakel het selectievakje **Vragen aan gebruiker** in om gebruikers naar de waarde te vragen wanneer ze de machine aanvragen.
- 7 Voeg nog een eigenschap toe, bewerk een bestaande eigenschap of verwijder een eigenschap.

Wat nu te doen

Geef aanvullende nieuwe machineconfiguratie-instellingen op. Als u klaar bent met het wijzigen van machine-instellingen, start u de aanvraag voor de nieuwe machineconfiguratie. Zie [De aangevraagde machineherconfiguratie uitvoeren](#).

De aangevraagde machineherconfiguratie uitvoeren

U kunt de aangevraagde machineherconfiguratie direct starten of deze inplannen om er op een later tijdstip aan te beginnen. U kunt ook opgeven hoe de machine wordt ingeschakeld, voordat u deze opnieuw configureert.

Voorwaarden

[Machineherconfiguratie-instellingen opgeven en overwegingen voor herconfiguratie.](#)

Procedure

- 1 Als het tabblad **Uitvoering** zichtbaar is, kunt u het selecteren om extra herconfiguratie-instellingen op te geven. Als het niet zichtbaar is, klikt u op **Indienen** om de herconfiguratie van de machine te starten.
- 2 Als het tabblad **Uitvoering** zichtbaar is, klikt u op **Uitvoering** om de herconfiguratie-actie in te plannen.
- 3 (Optioneel) Selecteer een optie in het vervolgkeuzemenu **Aanvraag uitvoeren**.

Optie	Beschrijving
Onmiddellijk	Begin zo snel mogelijk na goedkeuring met het opnieuw configureren.
Gepland	Begin op de opgegeven datum en tijd met het opnieuw configureren. Voer de datum en tijd in de tekstvakken in die worden weergegeven.

De geplande tijd wordt aangegeven in de lokale tijd op de locatie waar de vRealize Automation-webserver zich bevindt. Als **Aanvraag uitvoeren** niet beschikbaar is, wordt direct begonnen met opnieuw configureren.

4 (Optioneel) Selecteer een actie voor in-/uitschakelen in het vervolgkeuzemenu **Actie voor in-/uitschakelen**.

Optie	Beschrijving
Opnieuw opstarten indien nodig	(Standaard) Start indien nodig de machine opnieuw, voordat u deze opnieuw configureert.
Reboot	Start de machine opnieuw, voordat u deze opnieuw configureert, ongeacht of opnieuw starten is vereist.
Niet opnieuw opstarten	Start de machine niet opnieuw, voordat u deze opnieuw configureert, ook al is opnieuw starten vereist.

Onder de volgende voorwaarden is het vereist om de machine opnieuw te starten, voordat u deze opnieuw configureert:

- Wijziging van CPU, waarbij dynamisch toevoegen niet wordt ondersteund of is gedeactiveerd.
- Wijziging van geheugen, waarbij geheugenwijzigingen zonder opnieuw starten niet worden ondersteund of zijn gedeactiveerd.
- Wijziging van opslag waarbij opslagwijzigingen zonder opnieuw starten zijn gedeactiveerd

Als de machine de status Afsluiten heeft, is deze niet opnieuw gestart.

Opmerking U kunt de vSphere-optie Dynamisch toevoegen deactiveren door de aangepaste eigenschap `VirtualMachine.Reconfigure.DisableHotCpu` te gebruiken.

5 Klik op **OK**.

Wat nu te doen

U kunt de voortgang van het opnieuw configureren controleren door de statussen van de werkstroom te volgen die worden weergegeven in de gebruikersinterface. Zie [Werkstroomstatussen van Bewerkingen opnieuw configureren](#).

Werkstroomstatussen van Bewerkingen opnieuw configureren

Wanneer het opnieuw configureren van start gaat en zijn weg vervolgt door de werkstroom, kunt u de voortgang controleren in de pagina Bewerken.

Tabel 4-4. Werkstroomstatussen van Bewerkingen opnieuw configureren

Status	Beschrijving
Opnieuw configureren in behandeling	De statusbewerking is gemaakt.
Gepland	Er is een geplande werkstroom gemaakt voor de DEM (Distributed Execution Manager).
Opnieuw configureren	De werkstroom die specifiek is voor de interface, wordt uitgevoerd.

Tabel 4-4. Werkstroomstatussen van Bewerkingen opnieuw configureren (vervolg)

Status	Beschrijving
Opnieuw configureren is mislukt. Wachten tot opnieuw wordt geprobeerd.	Het opnieuw configureren is mislukt. Het wachten is op de eigenaar om een nieuwe aanvraag in te dienen. Als de eigenaar van de machine rechten heeft voor de acties 'opnieuw configureren' of 'opnieuw configureren annuleren', kan de eigenaar het opnieuw proberen of het opnieuw configureren annuleren.
ReconfigureFailed	Het opnieuw configureren is mislukt. Er wordt gewacht om de volgende actie uit te voeren.
ReconfigureSuccessful	Het opnieuw configureren is geslaagd. Er wordt gewacht tot de werkstroom de volgende actie uitvoert.
Canceled	De gebruiker heeft het opnieuw configureren geannuleerd. Machine-eigenaren die rechten hebben, kunnen een nieuwe configuratie annuleren.
Complete	De voltooiingswerkstroom stelt deze status in nadat het opschonen is voltooid, zodat de werkstroom kan doorgaan met het opschonen van de statusbewerkingen en goedkeuringen. De status Complete geeft aan dat de aanvraag van vRealize Automation is voltooid, maar dit betekent niet dat het opnieuw configureren van de machine als helemaal is geslaagd.

Een load balancer in een implementatie opnieuw configureren

U kunt in een geïmplementeerde NSX-load balancer een virtuele server toevoegen, bewerken of verwijderen.

De volgende overwegingen gelden voor implementaties die oorspronkelijk zijn uitgevoerd in vRealize Automation 7.2 of lager:

- Het opnieuw configureren van load balancers is beperkt tot implementaties die één load balancer bevatten.
- Op de detailpagina Items voor een load balancer in een implementatie worden de virtuele servers weergegeven die door alle load balancers in de implementatie worden gebruikt. Zie het [Knowledge Base-artikel 2150276](#) voor meer informatie.
- De optie Load balancer opnieuw configureren wordt niet ondersteund voor implementaties die zijn geüpgraded of gemigreerd van vRealize Automation 6.2.x naar deze versie van vRealize Automation.

Voor geüpgradede load balancers en load balancers die in de huidige vRealize Automation-versie zijn geïmplementeerd, mag u geen virtuele server bewerken terwijl u in dezelfde aanvraag een virtuele server toevoegt. Zie het [Knowledge Base-artikel 2150240](#) voor meer informatie.

Opmerking De actie **Herconfigureren** wordt niet ondersteund voor NSX-T-load balancers.

Als u een aanvraag indient om een load balancer opnieuw te configureren terwijl op de implementatie een andere actie wordt uitgevoerd, wanneer bijvoorbeeld een uitschalingsbewerking in uitvoering is, zal het opnieuw configureren mislukken met een ondersteunend bericht. In die situatie kunt u wachten tot de actie is voltooid en daarna uw aanvraag voor opnieuw configureren indienen.

Opmerking Als de blueprint die is gekoppeld aan de implementatie, geïmporteerd is uit een YAML-bestand dat een load balancer op aanvraag bevat waarvan het naamveld een andere waarde bevat dan het ID-veld, mislukt de actie **Opnieuw configureren**. Om de optie voor het opnieuw configureren van de load balancer in te schakelen voor een implementatie die gebaseerd is op een geïmporteerde blueprint, voert u de volgende stappen in de blueprint uit om acties na inrichting voor load balancer-onderdelen in toekomstige implementaties toe te staan.

- 1 Selecteer de blueprint in de vRealize Automation-console.
- 2 Klik op **Bewerken** en wijzig de naam van de blueprint. Hiermee stelt u de naam en de ingesloten id in op dezelfde waarde.
- 3 Selecteer het load balancer-onderdeel in de blueprint.
- 4 Klik op **Bewerken** en voer de onderdeelnaam opnieuw in. Hiermee stelt u de naam en de ingesloten id in op dezelfde waarde.
- 5 Herhaal dit voor alle load balancer-onderdelen in de blueprint.
- 6 Sla de blueprint op.

Wanneer u een nieuwe implementatie inricht met gebruikmaking van de bewerkte blueprint, werkt de actie Load balancer herconfigureren. Als u dit probleem wilt vermijden, zorgt u ervoor dat alle YAML-bestanden identieke naam- en id-waarden hebben voor alle load balancer-, netwerk- en beveiligingsonderdelen voordat u deze importeert.

Beheer geen door vRealize Automation beheerde NSX-objecten buiten vRealize Automation. Als u bijvoorbeeld de lidpoort van een geïmplementeerde load balancer in NSX wijzigt in plaats van in vRealize Automation, dan kan de NSX gegevensverzameling worden onderbroken. In- en uitschaalbewerkingen leveren ook onverwachte resultaten op.

Zie [Het onderdeel load balancer op aanvraag toevoegen](#) voor meer informatie over de instellingen die beschikbaar zijn wanneer u een virtuele server toevoegt of bewerkt.

Wanneer u in vRealize Automation een load balancer opnieuw configureert, worden bepaalde instellingen die in NSX werden geconfigureerd en die niet als instellingen beschikbaar zijn in vRealize Automation, weer op hun standaardwaarde ingesteld. Nadat u de actie voor het opnieuw configureren van de load balancer in vRealize Automation uitvoert, controleert u in NSX de volgende instellingen en werkt u deze bij indien dat nodig is:

- Insert-X-Forwarded for HTTP Header
- HTTP Redirect URL
- Service Monitor Extension

Voorwaarden

- Meld u aan bij vRealize Automation als een **machine-eigenaar, ondersteuningsgebruiker, bedrijfsgroepsgebruiker met een rol voor gedeelde toegang** of **bedrijfsgroepbeheerder**.
- Controleer of u over het recht beschikt om load balancers in een implementatie opnieuw te configureren. Het vereiste catalogusrecht is Opnieuw configureren (load balancer).

Procedure

- 1 Klik op **Implementaties**.
- 2 Zoek de implementatie met de load balancer die u opnieuw moet configureren en klik op de implementatiennaam
- 3 Klik op de load balancer en klik op het tandwielpictogram acties op het tabblad **Componenten**.
Het actiemenu van het component wordt weergegeven.
- 4 Selecteer **Opnieuw configureren**.
- 5 Voeg virtuele servers toe, bewerk ze of verwijder ze.

Virtual servers:

N...

E...

Del...

Protocol	Port	Description	Member Protocol	Member Port	Health Check Protocol	Health Check Port
HTTP	80		HTTP	80	HTTP	80
HTTP	81		HTTP	81	HTTP	81

- 6 Klik op **Indienen**.

NAT-regels in een implementatie wijzigen

U kunt bestaande NAT-regels van NSX toevoegen, bewerken en verwijderen in een geïmplementeerd één-op-veel NAT-netwerk.

Ook kunt u de volgorde wijzigen waarin de NAT-regels worden verwerkt.

Opmerking Als de bronblueprint van de implementatie is geïmporteerd uit een YAML-bestand dat een NAT-netwerkonderdeel bevat en de naam en id-waarden van het NAT-netwerkonderdeel niet identiek zijn, mislukt de actie **NAT-regels wijzigen**. Als u toestemming wilt geven aan de actie **NAT-regels wijzigen** voor een implementatie die is gebaseerd op een geïmporteerde blueprint, voert u de volgende stappen uit in de blueprint voordat u een implementatie inricht.

- 1 Start vRealize Automation, klik op het tabblad Ontwerpen en open de blueprint.
- 2 Klik op **Bewerken** en wijzig de naam van de blueprint. Hiermee stelt u de naam en de ingesloten id in op dezelfde waarde.
- 3 Selecteer het NAT-netwerkonderdeel in de blueprint.
- 4 Klik op **Bewerken** en voer de onderdeelnaam opnieuw in. Hiermee stelt u de naam en de ingesloten id in op dezelfde waarde.
- 5 Herhaal dit voor alle NAT-netwerkonderdelen in de blueprint.
- 6 Sla de blueprint op.

Als u dit probleem wilt vermijden, zorgt u ervoor dat alle YAML-bestanden identieke naam- en id-waarden hebben voor alle blueprints en load balancer-, netwerk- en beveiligingsonderdelen voordat u deze importeert.

Zie [NAT-regels maken en gebruiken voor NSX for vSphere](#) en [Het onderdeel NAT-netwerk op aanvraag of Geleid netwerk op aanvraag toevoegen in vRealize Automation](#) voor gerelateerde informatie.

Voorwaarden

- Meld u aan bij vRealize Automation als een **machine-eigenaar, ondersteuningsgebruiker, bedrijfsgroepsgebruiker met een rol voor gedeelde toegang** of **bedrijfsgroepbeheerder**.
- Controleer of u bent gerechtigd de NAT-regels in een netwerk te wijzigen.
- Controleer of het NAT-netwerk is geconfigureerd als een één-op-veel netwerk. De actie is niet beschikbaar voor één-op-veel NAT-netwerken.

NSX for vSphere ondersteunt een-op-een en een-op-veel NAT-netwerken, maar NSX-T ondersteunt alleen een-op-veel NAT-netwerken.

Procedure

- 1 Klik op **Implementaties**.
- 2 Zoek de implementatie met het netwerkcomponent dat u moet wijzigen en klik op de implementatienaam

3 Klik op het tabblad **Componenten** op het NAT-netwerkcomponent.

U kunt het onderdeel niet bewerken in het geval van een NAT-netwerk op aanvraag gekoppeld aan een externe IPAM-provider. U kunt echter handmatig een nieuw IP-adres van de bestemming toevoegen. Wanneer u een nieuw IP-adres van de bestemming toevoegt, krijgt het onderdeel de waarde Null. Het nieuwe IP-adres van de bestemming en de machine-id met waarde Null worden verwerkt wanneer u de aanvraag voor opnieuw configureren indient.

4 Klik op het tandwielpictogram voor acties.

Het actiemenu van het component wordt weergegeven.

5 Klik op **NAT-regels wijzigen**.

6 Voeg nieuwe regels toe voor het doorsturen van NAT-poorten, orden regels opnieuw, bewerk bestaande regels of verwijder regels.

7 Klik op **Indienen**.

Alle NAT-regels weergeven van een bestaande NSX Edge

U kunt NAT-regelinformatie weergeven over de NSX Edges die in actieve implementaties worden gebruikt.

Alle NAT-regels die in de implementatie worden gebruikt, worden samengevoegd en weergegeven in de Edge-weergave. De regels in de Edge-weergave worden niet noodzakelijkerwijs weergegeven in de volgorde waarin zij worden verwerkt.

Zie [NAT-regels in een implementatie wijzigen](#) als u de volgorde wilt zien en eventueel wilt wijzigen waarin de NAT-regels worden verwerkt in een één-op-veel NAT-netwerk.

Voorwaarden

- Meld u aan bij vRealize Automation als een **machine-eigenaar, ondersteuningsgebruiker, bedrijfsgroepsgebruiker met een rol voor gedeelde toegang** of **bedrijfsgroepbeheerder**.

Procedure

1 Klik op **Implementaties**.

2 Zoek de implementatie met de NSX Edge die u bekijkt en klik op de implementatiennaam.

3 Zoek het tabblad **Componenten** en zoek het component NSX Edge.

4 Selecteer de NSX Edge die u wilt bekijken.

5 Klik op **Sluiten** wanneer u klaar bent.

Beveiligingsitems aan een implementatie toevoegen of eruit verwijderen

U kunt bestaande NSX-beveiligingsgroepen en -beveiligingstags toevoegen aan of verwijderen uit de implementatie van een machine. Het is niet mogelijk beveiligingsgroepen op aanvraag toe te voegen, maar u kunt ze wel verwijderen.

De actie om de beveiliging te wijzigen, is gebaseerd op een machineonderdeel of -cluster. Een voorbeeld: als beveiliging is geassocieerd met een cluster genaamd AppTier2 dat bestaat uit 2 machines, voert u de beveiligingswijziging door in het AppTier2-cluster, niet op de afzonderlijke machines in het cluster.

De actie Beveiliging wijzigen wordt niet ondersteund voor implementaties die zijn bijgewerkt of gemigreerd vanaf vRealize Automation 6.2.x naar deze vRealize Automation-release.

Voorwaarden

- Meld u aan bij vRealize Automation als een **machine-eigenaar, ondersteuningsgebruiker, bedrijfspgroepsgebruiker met een rol voor gedeelde toegang** of **bedrijfspgroepbeheerder**.
- Controleer of u bent gerechtigd de beveiliging in een implementatie te wijzigen. Het vereiste catalogusrecht is Beveiliging wijzigen (implementatie).

Procedure

- 1 Klik op **Implementaties**.
- 2 Zoek de implementatie waarin de beveiligingsgroepen en tags zitten en klik op de implementatiennaam.
- 3 Klik op het beveiligingscomponent en klik op het tandwielpictogram voor acties op het tabblad **Componenten**.
Het actiemenu van het component wordt weergegeven.
- 4 Klik op **Beveiliging wijzigen**.
- 5 Selecteer het geïmplementeerde machineonderdeel of het cluster waaraan u beveiligingsitems wilt toevoegen of waaruit u deze wilt verwijderen.
- 6 U kunt bestaande beveiligingsgroepen en beveiligingstags voor elk machineonderdeel of cluster in de implementatie naar behoefte toevoegen of verwijderen.
- 7 Verwijder beveiligingsgroepen op aanvraag waar nodig voor elk machineonderdeel of cluster in de implementatie.
- 8 (Optioneel) Klik op het tabblad **Reden** en voer een reden voor de aanvraag in.
- 9 Klik op **Indienen**.

Extra implementatiebeheermethoden

Geïmplementeerde resources kunnen worden beheerd met gebruik van acties waarvoor rechten zijn verleend, maar er zijn extra methoden die niet zijn opgenomen als acties.

Deze methoden zijn niet beschikbaar op het tabblad Implementaties, maar u gebruikt deze om wijzigingen aan te brengen in ingerichte resources.

Terugwinning van resources op basis van vRealize Operations Manager-statistieken

Terugwinning helpt u om uw resources efficiënt te gebruiken. Als u vRealize Operations Manager ook gebruikt om resources te beheren in uw omgeving, kunt u vRealize Automation configureren

om de statistieken te gebruiken om te berekenen waar u implementatieresources kan terugwinnen.

Procedure

1 Een metriekprovider configureren

U kunt vRealize Automation configureren om status- en bronmetrieke van vRealize Operations Manager te gebruiken voor vSphere virtual machines.

2 Aanvragen voor terugwinning verzenden

U kunt implementaties weergeven en beheren en aanvragen voor terugwinning verzenden naar eigenaars van een implementatie. In de aanvraag voor terugwinning wordt een nieuwe leasduur in dagen opgegeven, de tijd die de eigenaar van de implementatie heeft om te reageren en aan te geven welke machines in aanmerking komen voor terugwinning.

3 Aanvragen voor terugwinning bijhouden

U kunt de huidige status van aanvragen voor terugwinning en andere details bijhouden.

Een metriekprovider configureren

U kunt vRealize Automation configureren om status- en bronmetrieke van vRealize Operations Manager te gebruiken voor vSphere virtual machines.

Voor meer informatie over statusbadges en -metrieke van vRealize Operations Managerraadpleegt u de vRealize Operations Manager-documentatie.

Voorwaarden

- Meld u aan bij de vRealize Automation-console als **tenantbeheerder**, **bedrijfsgroepbeheerder** of **machine-eigenaar**.

Terugwinningen: gebruikers die aanvragen voor terugwinning maken hebben de rol van tenantbeheerder nodig en hetzelfde tenantbeheerdersaccount moet lid zijn van ten minste één bedrijfsgroep in de tenant.

Het mislukken van het toevoegen van het tenantbeheerdersaccount aan een bedrijfsgroep veroorzaakt een systeemuitzondering bij het openen van het tabblad **Terugwinning > Implementaties**.

- Maak een vRealize Operations Manager-gebruikersaccount met weergave- en bronmetrieke voor alle vSphere-servers die u integreert met vRealize Automation.
- Maak vRealize Operations Manager-adapterinstanties voor alle vSphere-servers die u als endpoints toevoegt in vRealize Automation. Voor informatie over het maken van adapterinstanties raadpleegt u de vRealize Operations Manager-documentatie.

Procedure

- 1 Selecteer **Beheer > Terugwinning > Metriekprovider**.

2 Selecteer een metriekprovider.

Optie	Beschrijving
(Standaard) vRealize Automation-metriekprovider	Als u geen vRealize Operations Manager-instantie hebt, biedt vRealize Automation basismachinemetrieken.
vRealize Operations Manager-endpoint	Geef verbindinginformatie op voor de vRealize Operations Manager-instantie die u wilt gebruiken als uw metriekprovider voor vSphere virtual machines.

3 Klik op **Testverbinding**.

4 Klik op **Opslaan**.

Resultaten

Tenantbeheerders, machine-eigenaars en bedrijfsgroepbeheerders van de groep waarin de machine zich bevindt, kunnen statusbadges en statuswaarschuwingen weergeven op de pagina's met itemdetails voor virtual machines van vSphere. Zij kunnen ook de metrische waarden en statusbadges van vRealize Operations Manager weergeven wanneer ze filteren op het platformtype vSphere op de pagina met terugwinningen.

Wat nu te doen

[Aanvragen voor terugwinning verzenden.](#)

Aanvragen voor terugwinning verzenden

U kunt implementaties weergeven en beheren en aanvragen voor terugwinning verzenden naar eigenaars van een implementatie. In de aanvraag voor terugwinning wordt een nieuwe leaseduur in dagen opgegeven, de tijd die de eigenaar van de implementatie heeft om te reageren en aan te geven welke machines in aanmerking komen voor terugwinning.

Voorwaarden

- Meld u bij vRealize Automation aan als **tenantbeheerder**.
- (Optioneel) Voor het bekijken van health badges of metriek geleverd door vRealize Operations Manager, raadpleegt u [Een metriekprovider configureren](#).

Procedure

1 Selecteer **Beheer > Terugwinning > Implementaties**.

2 Zoek implementaties van virtual machines die aan uw zoekcriteria voldoen.

U moet het platformtype voor vSphere selecteren om de metriekeken weer te geven die door vRealize Operations Manager worden verzorgd.

- a Klik op de pijl-omlaag bij **Geavanceerd zoeken** om het zoekvak te openen.
- b Geef één of meer zoekwaarden op of selecteer de gewenste zoekwaarden.

Optie	Actie
Naam virtual machine bevat	Geef één of meer letertekens op in het tekstvak om de namen van de virtual machines te zoeken die met deze tekens overeenstemmen.
Naam eigenaar bevat	Geef een naam op in het tekstvak om de namen van eigenaren te zoeken die hiermee overeenstemmen.
Naam bedrijfsgroep bevat	Geef een naam op in het tekstvak om de namen van bedrijfsgroepen te zoeken die hiermee overeenstemmen.
Platformtype	Selecteer een platformtype in het vervolgkeuzemenu. SelecteervSphere om de metriekeken weer te geven die door vRealize Operations Manager worden verzorgd. Vereist voor vRealize Operations Manager.
Energieniveau	Selecteer een waarde voor het energieniveau in de vervolgkeuzelijst om virtual machines te zoeken waarvan het energieniveau overeenstemt met uw keuze.
Vervaldatum tussen	Klik op de kalenderpictogrammen en selecteer de begin- en einddatums waartussen de vervaldatum valt.
CPU-gebruik	Selecteer een waarde in het vervolgkeuzemenu om virtual machines te zoeken met een Hoog CPU-verbruik: meer dan 80%, een Laag CPU-verbruik: minder dan 5% of Geen: geen waarde. Als u een query wilt uitvoeren op de vRealize Operations Manager-metriekeken, kunt u deze filter niet gebruiken om de query uit te voeren en kunt u de resultaten niet sorteren op CPU-verbruik.
Geheugengebruik	Selecteer een waarde in het vervolgkeuzemenu om virtual machines te zoeken met een Hoog geheugenverbruik: meer dan 80%, een Laag geheugenverbruik: minder dan 10% of Geen: geen waarde. Als u een query wilt uitvoeren op de vRealize Operations Manager-metriekeken, kunt u deze filter niet gebruiken om de query uit te voeren en kunt u de resultaten niet sorteren op geheugenverbruik.
Schijfgebruik	Selecteer een waarde in het vervolgkeuzemenu om virtual machines te zoeken met een Laag verbruik harde schijf: minder dan 2 KB per seconde of Geen: geen waarde. Als u een query wilt uitvoeren op de vRealize Operations Manager-metriekeken, kunt u deze filter niet gebruiken om de query uit te voeren en kunt u de resultaten niet sorteren op het verbruik van de harde schijf.
Netwerkgebruik	Selecteer een waarde in het vervolgkeuzemenu om virtual machines te zoeken met een Laag netwerkverbruik: minder dan 1 KB per seconde of Geen: geen waarde.

Optie	Actie
	Als u een query wilt uitvoeren op de vRealize Operations Manager-metrieken, kunt u deze filter niet gebruiken om de query uit te voeren en kunt u de resultaten niet sorteren op het netwerkverbruik.
Complexe metriek	<p>Selecteer een waarde in het vervolgkeuzemenu om virtual machines te zoeken op basis van complexe metrieken. Zo kunt u bijvoorbeeld Niet-actief selecteren om machines te zoeken waarvoor het CPU-verbruik, het netwerkverbruik, het geheugenverbruik en het verbruik harde schijf allemaal onder 20% liggen.</p> <p>U kunt deze filter niet gebruiken als u een query uitvoert op vRealize Operations Manager-metrieken.</p>

c Klik op het pictogram Zoeken (.

- 3 Selecteer op de pagina Implementaties een of meer machines waarvan de bovenliggende implementatie moet worden teruggewonnen.

Alleen geselecteerde machines die zichtbaar zijn op de huidige resultatenpagina, worden teruggewonnen.

- 4 Klik op **Terugwinnen**.

De implementaties die virtual machines bevatten die op de huidige pagina zijn geselecteerd, worden opgenomen in de aanvraag.

Opmerking Op de pagina Implementatie terugwinnen kunnen machines worden weergegeven die niet beschikbaar zijn voor terugwinning, zoals machines waarvan de lease is verlopen. Als u een machine wilt opgeven die niet beschikbaar is voor terugwinning, wordt de volgende fout weergegeven:

Selection Error: Virtual machine *naam* is not in valid state for reclamation.

- 5 Geef de duur van de nieuwe lease op in het tekstvak **Nieuwe leasheduur (dagen)**.

Het minimum is 1 dag, het maximum is 365 dagen en de standaardwaarde is 7 dagen.

- 6 Geef op hoeveel dagen de eigenaar van de implementatie de tijd heeft om te reageren op de terugwinningsaanvraag in het tekstvak **Wacht alvorens lease af te dwingen (dagen)**.

Na het verstrijken van die tijd, haalt de implementatie zelf een nieuwe lease op met een nieuwe leasheduur. De minimum wachtperiode is 1 dag, het maximum is 365 dagen en de standaardwaarde is 3 dagen.

- 7 Voer in het tekstvak **Reden voor aanvraag** een reden voor de aanvraag in.
- 8 Klik op **Indienen**.
- 9 Klik op **OK**.

Resultaten

Wanneer u een aanvraag voor terugwinning indient, wordt deze weergegeven in het Postvak IN van de eigenaar van de implementatie. Als de eigenaar niet binnen het vereiste aantal dagen op de aanvraag reageert, krijgt de implementatie een nieuwe lease met de opgegeven leaseduur, tenzij de huidige leaseduur korter is. Als de eigenaar klikt op **Item in gebruik** in de terugwinningsaanvraag, blijft de lease van de implementatie ongewijzigd. Als de eigenaar klikt op **Vrijgeven voor terugwinning**, verloopt de lease van de implementatie onmiddellijk.

Wat nu te doen

[Aanvragen voor terugwinning bijhouden.](#)

Aanvragen voor terugwinning bijhouden

U kunt de huidige status van aanvragen voor terugwinning en andere details bijhouden.

De volgende alternatieve methoden zijn beschikbaar om een recente aanvraag voor terugwinning te controleren:

- Klik op het tabblad **Postvak IN** en selecteer **Aanvragen voor terugwinning** om gegevens over de aanvraag voor terugwinning te bekijken.
- Klik op het tabblad **Aanvragen voor terugwinning** en bekijk de lijst met recente aanvragen.
- Klik op **Implementaties** om recente implementatiewijzigingen weer te geven.


Voorwaarden

Meld u bij vRealize Automation aan als **tenantbeheerder**.

Procedure

- 1 Selecteer **Beheer > Terugwinning > Aanvragen voor terugwinning**.
- 2 De virtual machines zoeken die aan uw zoekcriteria voldoen.
 - a Klik op de pijl-omlaag bij **Geavanceerd zoeken** om het zoekvak te openen.
 - b Typ één of meer zoekwaarden of selecteer de gewenste zoekwaarden.

Optie	Actie
Naam virtual machine bevat	Typ één of meer lettertekens in het tekstvak om de namen van de virtual machines te zoeken die hiermee overeenstemmen.
Naam eigenaar bevat	Typ één of meer lettertekens in het tekstvak om de namen van de eigenaren te zoeken die hiermee overeenstemmen.
Reden voor aanvraag bevat	Typ één of meer lettertekens in het tekstvak om de redenen voor de aanvraag te zoeken die hiermee overeenstemmen.
Aanvraagstatus	Selecteer een waarde voor de aanvraagstatus in de vervolgkeuzelijst om virtual machines te zoeken waarvan de aanvraagstatus overeenstemt met uw keuze.

- c Klik op het pictogram **Zoeken** () of druk op Enter om de zoekopdracht te starten.
 - d Klik op de pijl-omhoog bij **Geavanceerd zoeken** om het zoekvak te sluiten.
- 3** (Optioneel) Klik op **Gegevens vernieuwen** om de weergave van de aanvragen voor terugwinning bij te werken.

De reservering van een beheerde machine wijzigen

U kunt de instelling voor de reservering of opslag wijzigen voor een beheerde machine. Dit is handig wanneer de machine wordt verplaatst naar een nieuw opslagpad dat niet beschikbaar is in de huidige reservering. Voor een implementatie van één machine kunt u ook de bedrijfsgroep van de machine wijzigen.

U kunt de machine in een implementatie met één machine verplaatsen naar een andere bedrijfsgroep als de eigenaar van de machine lid is van de doelbedrijfsgroep. Om de instelling voor de bedrijfsgroep te kunnen wijzigen, moet u bedrijfsgroepbeheerder zijn van zowel de originele bedrijfsgroep als de doelbedrijfsgroep.

Opmerking Als de machine een reserveringsbeleid heeft, kunt u de bedrijfsgroep niet veranderen.

U kunt extra reserveringen voor de gekoppelde computingbron maken met de menuopties **Beheer > Computingbron**.

Opslagruimte en geheugen die door middel van een reservering zijn toegewezen aan een ingerichte machine, worden vrijgemaakt wanneer de machine waaraan ze zijn gekoppeld, in vRealize Automation wordt verwijderd door de actie Vernietigen. De opslagruimte en het geheugen worden niet vrijgemaakt als de machine wordt verwijderd in de vCenter Server.

Bijvoorbeeld: u kunt geen reservering verwijderen die is gekoppeld aan machines in een bestaande implementatie. Als u geïmplementeerde machines handmatig verplaatst of verwijdert in de vCenter Server, blijft vRealize Automation de geïmplementeerde machines als live herkennen en voorkomen dat u bijbehorende reserveringen verwijdert.

Als door het wijzigen van de reservering een machine in vCenter Server wordt verplaatst naar een nieuw opslagpad dat geen deel uitmaakt van de reservering van de machine in vRealize Automation, moet u controleren of het doel of een nieuw opslagpad is geselecteerd in de reservering van de machine voordat u de reservering van de machine wijzigt.

Voorwaarden

Meld u aan bij vRealize Automation als een **materiaalbeheerder**.

Procedure

- 1** Selecteer **Infrastructuur > Beheerde machines**.
- 2** Zoek de machine met de reservering die u wilt wijzigen.

- 3 Klik op **Reservering wijzigen** in het vervolgkeuzemenu.

U kunt informatie over de beheerde machine, zoals de gekoppelde blueprint en computingbron, weergeven door op **Weergeven** te klikken in het vervolgkeuzemenu.

- 4 (Optioneel) Selecteer een bedrijfsgroep in het vervolgkeuzemenu **Bedrijfsgroep**.
- 5 (Optioneel) Selecteer een reservering in het vervolgkeuzemenu **Reservering**.
- 6 (Optioneel) Selecteer een opslagbeleid in het vervolgkeuzemenu **Opslag**.
- 7 Klik op **OK**.

Werken met de Inbox

De Inbox biedt in-product-meldingen met betrekking tot goedkeuringen voor catalogusaanvragen en interacties die tijdens het provisioningproces worden aangevraagd, en de status van aanvragen voor terugwinning op basis van vRealize Operations Manager-statistieken.

U kunt elk tabblad bekijken om te zien of er meldingen in behandeling zijn die actie vereisen.

- **Goedkeuringen** U kunt uw catalogusaanvragen bijhouden waarvoor goedkeuring vereist is. Als u bent aangewezen als goedkeurder voor een catalogusaanvraag, kunt u reageren op een goedkeuringsaanvraag. Zie [Niveau-informatie toevoegen aan goedkeuringsbeleidsinstellingen](#).
- **Handmatige gebruikersactie** Sommige catalogusaanvragen vereisen interactie tijdens het provisioning-proces. U kunt reageren op de aanvraag voor interactie. Zie [vRealize Orchestrator-integratie in vRealize Automation](#).
- **Aanvragen voor terugwinning.** Als u vRealize Operations Manager gebruikt om te bepalen waar u resources kunt terugwinnen, kunt u de aanvragen voor terugwinning volgen. Zie [Aanvragen voor terugwinning bijhouden](#).