

Gebruik en beheer van vRealize Automation Cloud Assembly

December 2022

vRealize Automation 8.7

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 © 2022 VMware, Inc. Alle rechten voorbehouden. [Informatie over copyright en handelsmerken.](#)

Inhoud

1	Wat is Cloud Assembly	8
	Hoe werkt Cloud Assembly	9
2	Tutorials	12
	Een virtuele machine implementeren	14
	vSphere-infrastructuur en -implementaties instellen en testen	21
	Een productieworkload configureren en inrichten	39
	Tags gebruiken om alle vSphere-resources te beheren	46
	Een cloudsjabloon aan de Service Broker-catalogus toevoegen met een aangepast aanvraagformulier	57
	Onboarding en beheer van vSphere-resources	68
	Infrastructuur en implementaties met meerdere clouds	78
	Deel 1: het voorbeeld van de infrastructuur configureren	79
	Deel 2: het voorbeeld van een project maken	85
	Deel 3: het voorbeeld van een privécloudsjabloon ontwerpen en implementeren	86
	VMware Cloud on AWS configureren	103
	Een VMware Cloud on AWS-basiswerkstroom configureren	104
	Een geïsoleerd netwerk in VMware Cloud on AWS configureren	117
	Een externe IPAM-integratie voor Infoblox configureren	122
	Vereiste uitbreidbaarheidskenmerken in de Infoblox-applicatie toevoegen voordat u het downloadpakket implementeert	124
	Een extern IPAM-providerpakket downloaden en implementeren	125
	Een uitvoeringsomgeving voor een IPAM-integratiepunt maken	127
	Een extern IPAM-integratiepunt voor Infoblox toevoegen	129
	Een netwerk en netwerkprofiel configureren om externe IPAM voor een bestaand netwerk te gebruiken	133
	Een cloudsjabloon definiëren en implementeren die gebruikmaakt van bereiktoewijzing van een externe IPAM-provider	135
	Infoblox-specifieke eigenschappen voor IPAM-integraties in cloudsjablonen gebruiken	138
	De verzameling van netwerkgegevens beheren met behulp van Infoblox-filters	142
3	Cloud Assembly voor uw organisatie instellen	145
	Wat zijn de vRealize Automation-gebruikersrollen	145
	Organisatie- en servicegebruikersrollen	147
	Custom gebruikersrollen	165
	Toepassingsvoorbeelden: hoe kunnen gebruikersrollen mij helpen bij het toegangsbeheer	169
	Ingebouwde rol van infrastructuurbeheerder	190
	Cloudaccounts toevoegen	192

Inloggegevens vereist voor het werken met cloudaccounts	193
Een Microsoft Azure-cloudaccount maken	211
Een Amazon Web Services-cloudaccount maken	216
Een Google Cloud Platform-cloudaccount maken	217
Een vCenter-cloudaccount maken	219
Een NSX-V-cloudaccount maken	220
Een NSX-T-cloudaccount maken	222
Een VMware Cloud on AWS-cloudaccount maken	226
Een VMware Cloud Foundation-cloudaccount maken	227
Een VMware Cloud Director-cloudaccount maken in vRealize Automation	229
Integreren met andere applicaties	235
Hoe gebruik ik GitLab- en GitHub-integratie?	236
Externe IPAM-integratie configureren	242
Upgraden naar een hoger extern IPAM-integratiepakket	244
My VMware-integratie configureren in Cloud Assembly	245
vRealize Orchestrator-integratie in Cloud Assembly configureren	246
Hoe werk ik met Kubernetes in Cloud Assembly?	251
Wat is configuratiebeheer in Cloud Assembly	278
Een SaltStack Config-integratie maken	294
Hoe maak ik een Active Directory-integratie in Cloud Assembly?	299
Een VMware SDDC Manager-integratie configureren	302
Integreren met vRealize Operations Manager	303
Wat zijn onboardingplannen	320
Geselecteerde machines als één implementatie onboarden	322
Geavanceerde configuratie	326
Hoe configureer ik een internetproxyserver server	326
Wat kan ik doen met NSX-T-toewijzing aan meerdere vCenters	330
Wat gebeurt er als ik een NSX-cloudaccountassociatie verwijder	331
Hoe kan ik met de IPAM SDK een providerspecifiek extern IPAM-integratiepakket maken	331
vRealize Automation gebruiken met VMware-oplossing in Azure	332
vRealize Automation gebruiken met Google Cloud VMware Engine	333
vRealize Automation gebruiken met de VMware-oplossing in de Oracle Cloud	333
vRealize Automation gebruiken met VMware Cloud on Dell EMC	334

4 Uw resource-infrastructuur maken 335

Cloudzones toevoegen	335
Meer informatie over cloudzones	336
Soorttoewijzingen toevoegen	339
Meer informatie over soorttoewijzingen	340
Imagetoewijzingen toevoegen	340
Meer informatie over imagetoewijzingen	341

Netwerkprofielen toevoegen	347
Meer informatie over netwerkprofielen	347
Netwerkinstellingen gebruiken	355
Instellingen voor beveiligingsgroepen gebruiken	359
Instellingen voor load balancers gebruiken	360
Hoe configureer ik een netwerkprofiel om een netwerk op aanvraag te ondersteunen voor een externe IPAM-integratie	361
Hoe configureer ik een netwerkprofiel om een bestaand netwerk te ondersteunen voor een externe IPAM-integratie	365
Opslagprofielen toevoegen	365
Meer informatie over opslagprofielen	365
Hoe gebruik ik prijskaarten	369
Prijskaarten voor vSphere en VMC maken	371
Tags gebruiken	376
Een tagstrategie maken	379
Capaciteitstags in Cloud Assembly gebruiken	380
Beperkingstags in Cloud Assembly gebruiken	382
Standaardtags	384
Hoe Cloud Assembly tags verwerkt	385
Hoe kan ik een eenvoudige tagstructuur instellen?	385
Werken met resources	387
Berekeningsresources	387
Netwerkreources	388
Beveiligingsresources	391
Opslagresources	393
Meer informatie over resources	394
Tenantresources voor meerdere providers configureren met vRealize Automation	416
Hoe maak ik een Virtuele privézone voor vRealize Automation	417
Configuratie van virtuele privézone beheren voor vRealize Automation-tenants	421
Algemene image- en soorttoewijzing voor vRealize Automation-tenants maken	422
Tenantspecifieke image- en soorttoewijzingen voor vRealize Automation configureren	426
Uitbreidbaarheidsabonnementen voor providers of tenants maken	427
Werken met oude virtuele privézones in nieuwere versies van vRealize Automation	428

5 Projecten toevoegen en beheren 430

Hoe voeg ik een project toe voor mijn ontwikkelingsteam	430
Meer informatie over projecten	433
Projecttags en aangepaste eigenschappen gebruiken	433
Plaatsingsbeleid op projectniveau gebruiken	435
Wat zijn de projectkosten	440
Hoe werken projecten tijdens het implementeren	441

6 Uw implementaties ontwerpen	443
Aan de slag met ontwerpen	445
Hulp bij het voltooiën van code	448
Bindingen en afhankelijkheden	450
Versies van sjablonen	452
Gebruikersinvoer in aanvragen	454
vRealize Orchestrator-acties als invoer	461
Eigenschapsgroepen	465
Eigenschapsgroepen invoeren	466
Constance eigenschapsgroepen	476
Meer informatie over eigenschapsgroepen	479
Resourcevlaggen voor aanvragen	481
Expressies	483
Syntaxis voor expressie	487
Geheime eigenschappen	494
Externe toegang	495
SCSI-schijfplaatsing	498
Machine-initialisatie	502
vSphere-aanpassingsspecificaties	502
Configuratieopdrachten	503
Statische IP-adressen van vSphere	506
Vertraagde implementatie	512
Windows-gast aanpassen	513
Machine- en schijfclusters	517
Aangepaste naamgeving voor geïmplementeerde resources	519
SaltStack Config-resource	522
Terraform-configuraties	529
Een Terraform-runtimeomgeving voorbereiden	529
Terraform-configuraties voorbereiden	536
Ontwerpen voor Terraform-configuraties	538
Meer informatie over Terraform-configuraties	543
Typen aangepaste resources	546
Hoe maak ik een cloudsjabloon waarmee gebruikers aan Active Directory worden toegevoegd	551
Een cloudsjabloon maken die SSH bevat	556
Voorbereiden op dag 2	560
Cloudsjablooninvoer voor updates voor dag 2 gebruiken	561
Een aangepaste resourceactie maken voor een virtuele machine met vMotion	562
Meer codevoorbeelden	571
Weer te geven cloudsjabloon	572
Voorbeelden van vSphere-resources	579

Kernen per socket en aantal CPU's	582
Netwerken, beveiligingsgroepen en load balancers	583
Voor Puppet ingeschakelde cloudsjabloon met gebruikersnaam- en wachtwoordtoegang	612
Schema met eigenschappen voor aangepaste resources	622
Speciale eigenschappen	622
Andere manieren om sjablonen te maken	622
Levenscycli van applicaties uitbreiden en automatiseren	623
Abonnementen op uitbreidbaarheidsacties	624
Abonnementen op uitbreidbaarheidswerkstromen	653
Meer informatie over uitbreidbaarheidsabonnementen	660
7 Implementaties en resources beheren	675
Implementaties beheren	675
Hoe kan ik implementaties controleren	679
Wat kan ik doen als een Cloud Assembly-implementatie mislukt	681
Hoe kan ik de levenscyclus van een voltooide implementatie beheren?	684
Welke acties kan ik op implementaties uitvoeren	689
Resources beheren	708
Werken met individuele resources	712
Werken met gedetecteerde machines	714

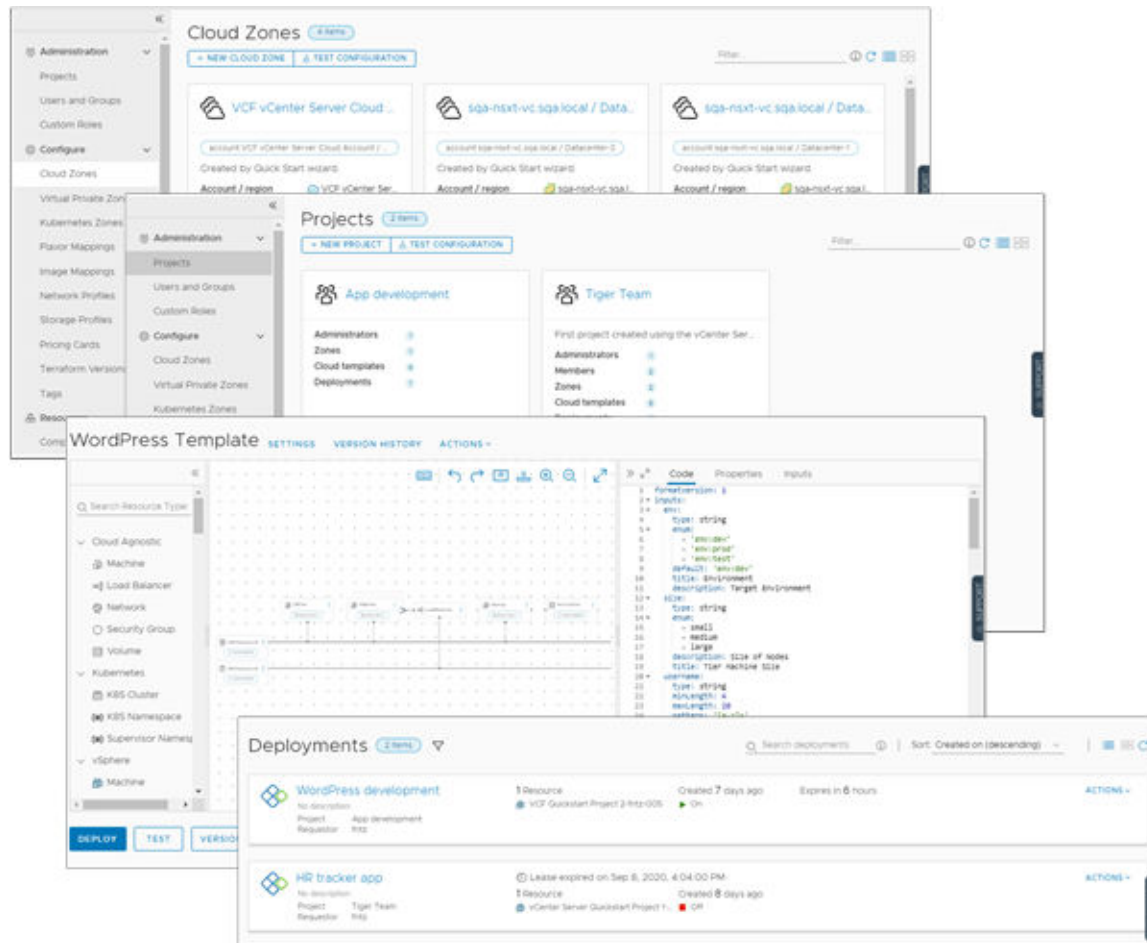
Wat is Cloud Assembly

1

U gebruikt vRealize Automation Cloud Assembly om verbinding te maken met uw openbare en particuliere cloudproviders, zodat u machines, applicaties en services die u maakt kunt implementeren voor die resources. U en uw teams ontwikkelen cloudsjablonen-als-code in een omgeving die een iteratieve werkstroom ondersteunt, van ontwikkeling en test tot productie. Tijdens het inrichten kunt u naar een groot aantal cloudleveranciers implementeren. De service is een beheerd VMware SaaS- en NaaS-gebaseerd framework.

Een overzicht van Cloud Assembly bevat de volgende basisfuncties.

- Op het tabblad Resources wordt de huidige status van uw ingerichte, gedetecteerde, geonboarde en andere resources weergegeven. U heeft toegang tot resourcedetails en acties voor dag 2 die u gebruikt om uw resources te beheren.
- Het tabblad Ontwerp is uw plek voor ontwikkeling. U gebruikt het canvas en de YAML-editor om uw machines en applicaties te ontwikkelen en vervolgens te implementeren.
- Op het tabblad Infrastructuur kunt u uw cloudleveranciers en -gebruikers toevoegen en organiseren. Dit tabblad bevat ook informatie over geïmplementeerde cloudsjablonen.
- Op het tabblad Uitbreidbaarheid kunt u de levenscyclus van applicaties uitbreiden en automatiseren. U kunt zich abonneren op gebeurtenissen die worden gebruikt om uitbreidbaarheidsacties of vRealize Orchestrator-werkstromen te activeren.
- Op het tabblad Waarschuwingen worden meldingen weergegeven over de capaciteit, prestaties en beschikbaarheid van uw infrastructuurresources. U moet een geconfigureerde integratie met vRealize Operations Manager hebben om de waarschuwingen te zien en te gebruiken.
- Het tabblad Tenantbeheer bevat de verschillende tenants die u hebt geconfigureerd als u een serviceprovider bent, en stelt u in staat om virtuele privézones toe te wijzen of de toewijzing op te heffen.



Dit hoofdstuk omvat de volgende onderwerpen:

- [Hoe werkt Cloud Assembly](#)

Hoe werkt Cloud Assembly

Cloud Assembly is een service voor het ontwikkelen en implementeren van cloudsjablonen. U en uw teams gebruiken de service om machines, applicaties en services te implementeren op uw cloudleveranciersresources.

Als Cloud Assembly-beheerder, die in het algemeen een cloudbeheerder wordt genoemd, zet u de inrichtingsinfrastructuur op en maakt u de projecten waarin gebruikers en resources worden gegroepeerd.

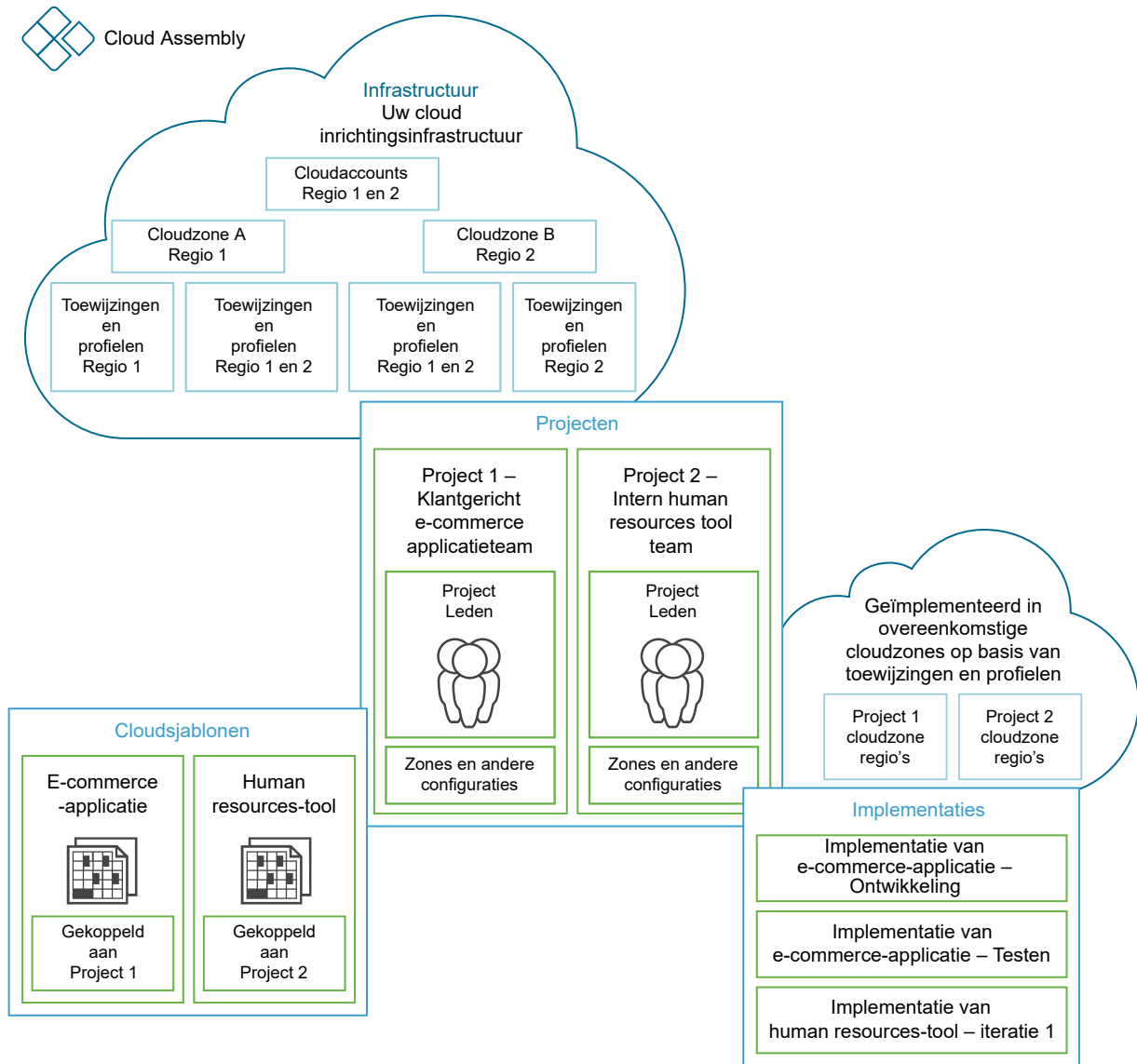
- Voeg uw cloudleveranciersaccounts toe. Zie [Cloudaccounts aan Cloud Assembly toevoegen](#).
- Bepaal welke regio's of gegevensopslagplaatsen de cloudzones zijn waarin uw ontwikkelaars gaan implementeren. Zie [Meer informatie over Cloud Assembly-cloudzones](#).
- Maak beleidsregels die de cloudzones definiëren. Zie [Hoofdstuk 4 Uw Cloud Assembly-resource-infrastructuur maken](#).

- Maak projecten die de ontwikkelaars en de cloudzones groeperen. Zie [Cloud Assembly-projecttags en aangepaste eigenschappen gebruiken](#) .

Als cloudsjabloonontwikkelaar bent u lid van een of meer projecten. U maakt en implementeert sjablonen in de cloudzones die zijn gekoppeld aan een van uw projecten.

- Ontwikkel cloudsjablonen voor projecten met behulp van het ontwerpcanvas. Zie [Aan de slag met Cloud Assembly-ontwerpen](#).
- Implementeer uw cloudsjablonen in projectcloudzones op basis van beleidsregels en beperkingen.
- Beheer uw implementaties, inclusief het verwijderen van niet-gebruikte applicaties. Zie [Cloud Assembly-implementaties beheren](#).

Welkom bij Cloud Assembly. Zie [Tutorial: Infrastructuur en implementaties met meerdere clouds instellen en testen in Cloud Assembly](#) voor een voorbeeld van hoe u de infrastructuur definieert en vervolgens een cloudsjabloon maakt en implementeert.



Cloud Assembly-tutorials


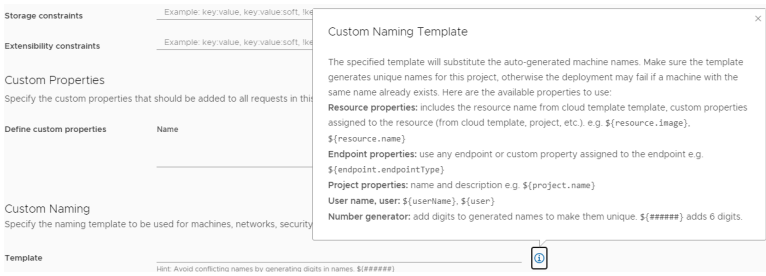

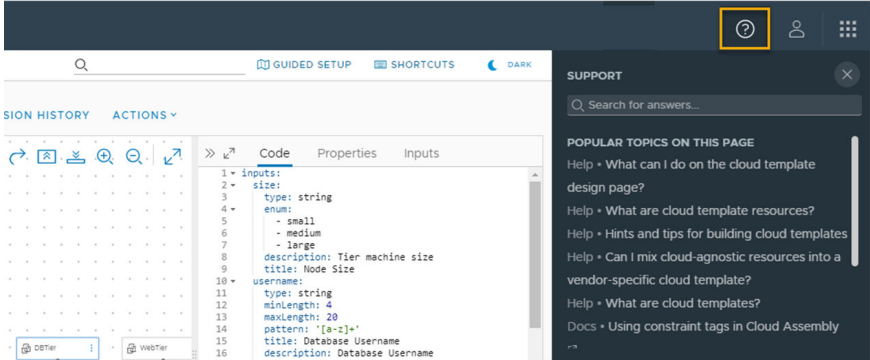
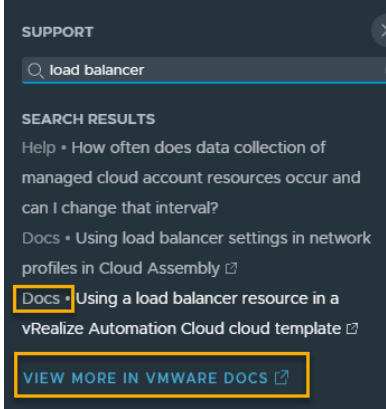
2

De tutorials laten zien hoe u algemene taken kunt uitvoeren die u helpen uw Cloud Assembly-vaardigheden aan te scherpen.

Wanneer u begint, willen wij u eraan herinneren dat naast de stappen in de tutorials extra informatie wordt geboden in deze handleiding. Er worden links naar relevante onderwerpen gegeven.

Toegang tot gebruikersondersteuning

Even belangrijk is de gebruikersondersteuning die in de applicatie wordt aangeboden. De gebruikersondersteuning helpt u bij het begrijpen van functies en biedt informatie waarmee u beslissingen kunt nemen over het vullen van tekstvakken. De externe documentatie biedt meer diepte, codevoorbeelden en gebruiksscenario's.

Type ondersteuning	Toegang tot ondersteuning	Voorbeeld
Wegwijzerhulp op veldniveau	Klik op het pictogram Informatie (het Informatie-pictogram  naast een veld.	
Help-paneel voor contextuele ondersteuning	Klik op het pictogram Help (het Informatie-pictogram  naast uw naam en organisatie.	
Toegang tot de externe documentatie	Klik op een artikeltitel met het label Docs of klik op de link View More in VMware Docs .	

Dit hoofdstuk omvat de volgende onderwerpen:

- Tutorial: Een virtuele machine in Cloud Assembly implementeren
- Tutorial: vSphere-infrastructuur en -implementaties in Cloud Assembly instellen en testen
- Tutorial: Cloud Assembly configureren voor het inrichten van een productieworkload
- Tutorials: tags in Cloud Assembly gebruiken om vSphere-resources te beheren
- Tutorial: Een Cloud Assembly-cloudsjabloon aan de Service Broker-catalogus toevoegen met een aangepast aanvraagformulier
- Tutorial: onboarding en beheer van vSphere-resources in vRealize Automation

- [Tutorial: Infrastructuur en implementaties met meerdere clouds instellen en testen in Cloud Assembly](#)
- [Tutorial: VMware Cloud on AWS voor vRealize Automation configureren](#)
- [Tutorial: Een providerspecifieke externe IPAM-integratie voor vRealize Automation configureren](#)

Tutorial: Een virtuele machine in Cloud Assembly implementeren

Als Cloud Assembly-beheerder kunt u een eenvoudige virtuele machine implementeren waarbij niet is vereist dat u weet hoe u een cloudsjabloon kunt maken. Als Cloud Assembly nieuw is voor u, begeleidt deze tutorial u bij het instelproces, het maken van de virtuele machine, en laat deze u zien waar u de geïmplementeerde machine kunt beheren.

Deze methode is een eenvoudige manier om snel een machine te implementeren op basis van imagesjablonen, groottesoorten, opslag en netwerken die door de cloudprovider zijn gedefinieerd. Het is een snelle test van uw cloudaccount en projecten.

U kunt een virtuele machine maken voor een van de volgende cloudserviceproviders.

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- vCenter Server
- VMware Cloud on AWS

Het Google Cloud Platform is het voorbeeld in deze tutorial.

Voordat u begint

- Controleer of u de rol van Cloud Assembly-beheerder hebt. Zie [Organisatie- en servicegebruikersrollen in vRealize Automation](#). Als u deze gebruikersrol niet heeft, ziet u ook niet de optie om een nieuwe VM te maken.

Stap 1: Een cloudaccount toevoegen

De cloudaccounts bieden de verificatiegegevens die Cloud Assembly gebruikt om verbinding te maken met de cloudprovider.

- 1 Selecteer **Infrastructuur > Verbindingen > Cloudaccounts**.
- 2 Klik op **Cloudaccount toevoegen** en selecteer het accounttype.

U krijgt toegang tot de configuratiedetails met de volgende links.

- [Een Amazon Web Services-cloudaccount maken in vRealize Automation](#)
- [Een Google Cloud Platform-cloudaccount maken in vRealize Automation](#)

- Een Microsoft Azure-cloudaccount maken in vRealize Automation
- Een vCenter-cloudaccount maken in vRealize Automation
- Een VMware Cloud on AWS-cloudaccount maken in vRealize Automation

Nadat u het cloudaccount heeft toegevoegd, verzamelt Cloud Assembly resourcegegevens van het doelcloudprovideraccount dat u later gebruikt om een virtuele machine te implementeren.

Stap 2: een project maken

Het project koppelt de gebruikers en de cloudzones van het cloudaccount.

In deze tutorial wordt de projectnaam Create VM Project gebruikt. Dit project is een demonstratieproject met cloudzones voor alle ondersteunde platformen.

1 Selecteer **Infrastructuur > Beheer > Projecten**.

2 Klik op **Nieuw project**.

3 Voer een naam in.

In deze tutorial is de naam **Create VM Project**.

4 Als u wilt dat andere gebruikers dit project gebruiken, klikt u op het tabblad **Gebruikers** en voegt u gebruikers toe aan het project.

5 Klik op het tabblad **Inrichting** en klik op **Zone toevoegen** om ten minste één cloudzone toe te voegen voor de cloudaccounts waarop u implementeert.

Onthoud dat dit een demonstratieproject is dat een cloudzone bevat voor elke ondersteuning van het platform van de cloudleverancier.

Create VM Project DELETE

Summary Users **Provisioning** Kubernetes Provisioning Integrations

Zones
Specify the zones that can be used when users provision deployments in this project. ⓘ

+ ADD ZONE × REMOVE

<input type="checkbox"/>	Name	Status	Description	Priority	Instances	Memory Limit (MB)	CPU Limit	Storage Limit (GB)	Capability Tags
<input type="checkbox"/>	dsadsa-vsphere / SDDC-Datacenter	--		0	Unlimited	Unlimited	Unlimited	Unlimited	
<input type="checkbox"/>	yingzhi-GCP / us-east1	--		0	Unlimited	Unlimited	Unlimited	Unlimited	
<input type="checkbox"/>	AWS / af-south-1	--		0	Unlimited	Unlimited	Unlimited	Unlimited	
<input type="checkbox"/>	vc65 / Datacenter	--		0	Unlimited	Unlimited	Unlimited	Unlimited	
<input type="checkbox"/>	Azure Test / West US	--		0	Unlimited	Unlimited	Unlimited	Unlimited	

1 - 5 of 5 zones

6 Klik op **Maken**.

Stap 3: Een virtuele machine maken en implementeren

1 Selecteer **Resources > Resources > Virtuele machines** en klik vervolgens op **Nieuwe VM**.

- 2 Configureer de vereiste instellingen op de pagina Algemeen van de wizard en klik op **Volgende**.

Deze tutorial gebruikt Google Cloud Platform als het cloudaccount waarop u de virtuele machine wilt implementeren.

General Location and basic information.

Select the project, cloud zone, and other basic information for your virtual machine.

Name * Google Cloud Create VM
Enter a name for your machine. A suffix or naming policy may also be applied during provisioning

Project * Create VM Project
Select a project with access to your desired cloud zone

Cloud zone * yingzhi-GCP / us-east1
Select the cloud zone where you want to provision this machine

Tags Enter a new tag
Tags are added to the machine when provisioned

NEXT CANCEL

Houd er rekening mee dat deze waarden alleen voorbeelden zijn. Uw waarden moeten specifiek zijn voor uw omgeving.

Tabel 2-1. Voorbeeldwaarden voor de eerste wizardpagina

Instelling	Voorbeeldwaarde
Naam	Google Cloud Create VM
Project	Create VM Project
Cloudzone	yingzhi-GCP/us-east1

- 3 Selecteer de image en soort die worden gebruikt om de virtuele machine te maken.

De beschikbare waarden worden verzameld van de doelcloudzone. De image is het besturingssysteem en de soort is de gedefinieerde grootteopties. Voor sommige doelprovidertypen moet u de CPU en het geheugen opgeven. Voor dit doel moet u een selectie maken uit de gedefinieerde opties.

4 Klik op **Volgende**.

Als u alleen de machine wilt implementeren, klikt u op **Maken**. Klik voor deze tutorial op **Volgende** om de optionele opslag en het netwerk voor deze virtuele machine toe te voegen.

5 Als u een nieuwe schijf wilt toevoegen, klikt u op **Harde schijf toevoegen** en voert u een **Naam** en **Grootte** in.

6 Klik op **Volgende**.

7 Klik op **Netwerkadapter toevoegen** om een netwerkadapter toe te voegen.

8 Selecteer uit de zoekresultaten.

9 Klik op **Maken**.

Uw weergave schakelt naar de pagina Implementaties, zodat u de voortgang van de implementatie kunt controleren.

Stap 4: De nieuwe virtuele machine beheren als implementatie

Wanneer het implementatieproces is voltooid, kunt u beginnen met het beheren van de implementatie.

Zie [Cloud Assembly-implementaties beheren](#) voor meer informatie over het beheren van uw implementaties.

Zie [Welke acties kan ik op Cloud Assembly-implementaties uitvoeren](#) voor een lijst met alle mogelijke acties voor dag 2 voor alle resourcetypes.

1 Selecteer **Resources > Implementaties** en zoek uw virtuele machine.

In deze tutorial is de implementatienaam Google Cloud Create VM.

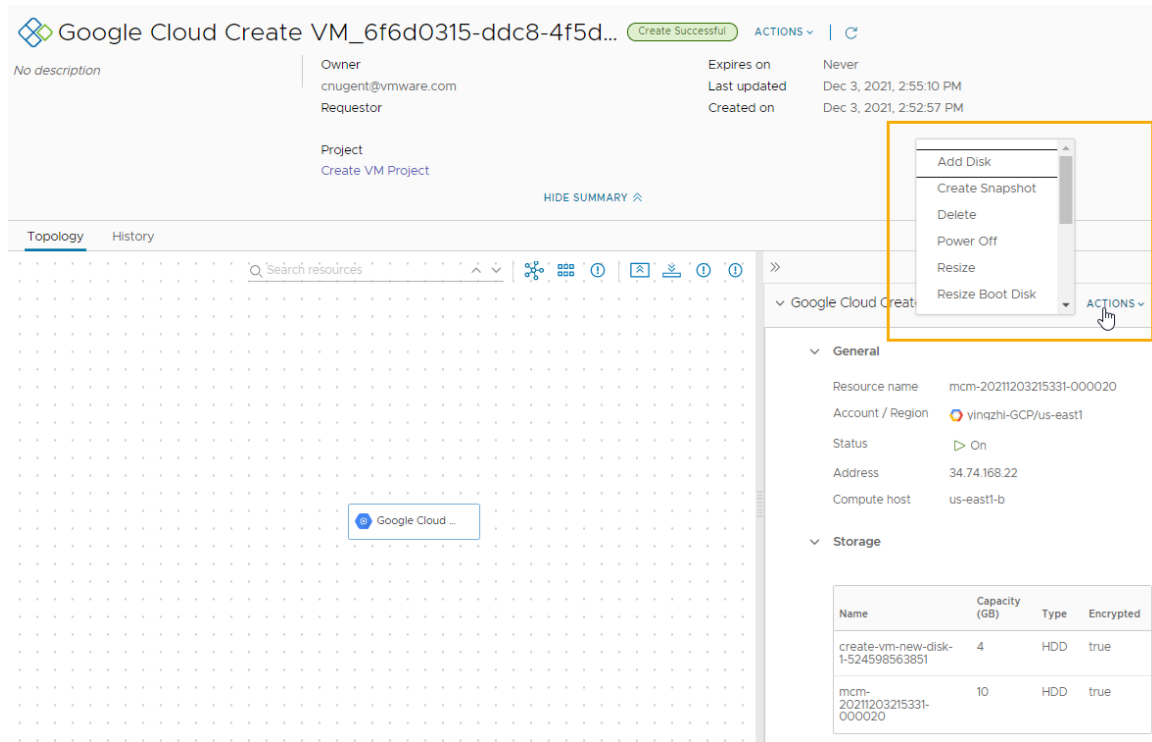
2 Als u een toegestane actie op implementatieniveau wilt uitvoeren voor de implementatie vanuit deze weergave, klikt u op de verticale punten en selecteert u de actie.

	Name	Address	Owner	Project	Status	Expires on	Price
>	gcp_811d09ff-efe1-4da4-a949-5be98ab62c...		@vmware.com	Create VM Project		Never	
>	Google Cloud Create VM_6f6d0315-ddc8-4...		@vmware.com	Create VM Project		Never	
>	Change Owner		@vmware.com	cmbu-08-project		Never	
>	Change Project	le-f792-43d5-885d-2b45e...	@vmware.com	Create VM Project		Never	
>	Delete		@vmware.com				
>	Edit Deployment	-South	@vmware.com	Sales		Never	
>	Edit Tags		@vmware.com	Sales		Never	
>	Power Off		@vmware.com				
>	Power On		@vmware.com				

3 Klik op de implementatienaam voor meer informatie over de implementatie, inclusief de topologie.

U ziet dat de topologie van deze implementatie eenvoudig is. Complexere implementaties leveren ook de complete topologie die mogelijk machines, load balancers, netwerkverbindingen en andere onderdelen kan bevatten.

U kunt ook de implementatiegeschiedenis bekijken (een logboek van alle acties op de implementatieonderdelen) en toegestane acties op machineniveau uitvoeren.



Stap 5: De nieuwe virtuele machine beheren als resource

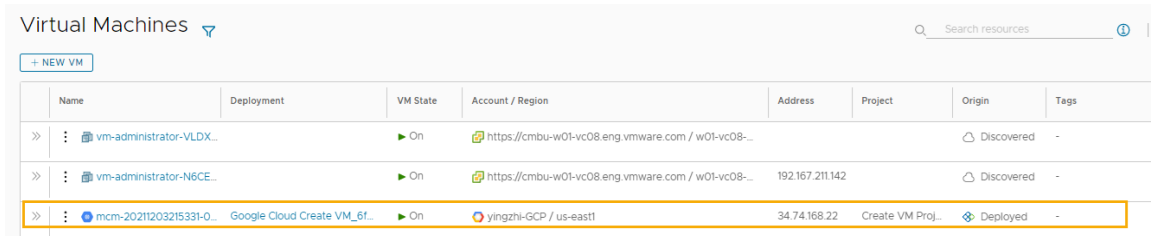
U kunt de virtuele machine niet alleen als implementatie beheren, maar ook samen met andere resources beheren. Resources kunnen onder meer geïmplementeerde, gedetecteerde en geonboarde virtuele machines, opslagvolumes en netwerk- en beveiligingsresources zijn.

Gedetecteerde resources zijn resources die worden verzameld van de cloudinstantie. U kunt gedetecteerde resources beheren met een beperkte set acties voor dag 2, zoals in- en uitschakelen. Zie [Hoe werk ik met gedetecteerde resources in Cloud Assembly?](#) voor meer informatie over het werken met gedetecteerde resources.

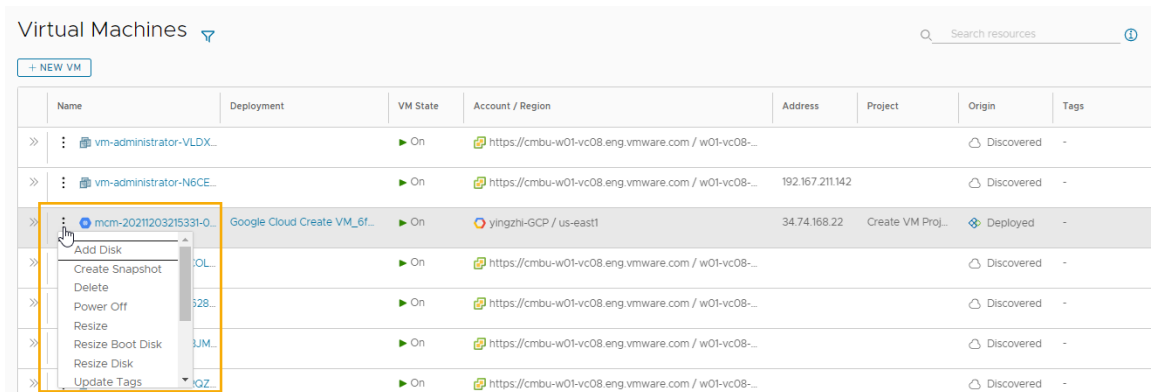
Geonboarde resources zijn gedetecteerde resources die u onder volledig beheer heeft gebracht. Ze kunnen worden beheerd met de meer robuuste opties voor acties voor dag 2. Zie [Wat zijn onboardingplannen in Cloud Assembly](#) voor meer informatie over het onboarden van gedetecteerde resources.

Wanneer u met deze geïmplementeerde machine werkt, komt deze in aanmerking voor meer acties voor dag 2. De beschikbaarheid van de acties is afhankelijk van de status van de machine en voor welke acties voor dag 2 u rechten heeft om ze uit te voeren.

- 1 Selecteer **Resources > Resources > Virtuele machines**.
- 2 Zoek de machine.

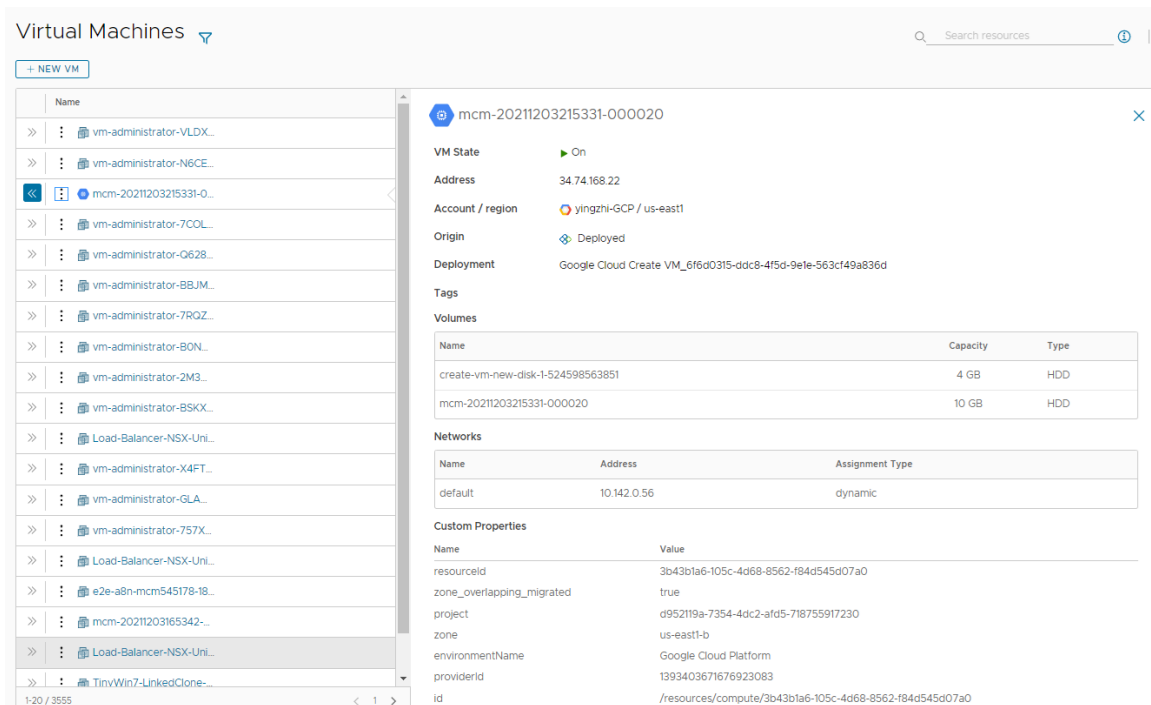


- 3 Als u een toegestane actie op machineniveau wilt uitvoeren voor de machine vanuit deze weergave, klikt u op de verticale drie punten en selecteert u de actie.



- 4 Klik op de machinenaam om de details van de machineresource te bekijken.

De nuttige details in dit voorbeeld zijn onder meer de opslag-, netwerk- en aangepaste eigenschappen.



Tutorial: vSphere-infrastructuur en -implementaties in Cloud Assembly instellen en testen

Als u nieuw bent in vRealize Automation of als u alleen een opfrissing nodig hebt, leidt deze tutorial u door het Cloud Assembly-configuratieproces. U voegt eindpunten voor het vSphere-account toe, definieert de infrastructuur, voegt gebruikers toe aan projecten en ontwerpt en implementeert vervolgens een workload met behulp van VMware Cloud Templates op basis van vSphere-resourcetypes, zodat u het proces al doende leert.

Hoewel deze tutorial slechts het begin is, bevindt u zich op het pad om selfservice-automatiserings- en iteratieve ontwikkeling te leveren die in meerdere publieke en privéclouds werkt. Deze tutorial richt zich op VMware vCenter Server en NSX-T. Nadat u deze werkstroom hebt voltooid, kunt u toepassen wat u hebt geleerd om meer typen cloudaccounts toe te voegen en meer geavanceerde cloudsjablonen te leveren.

Terwijl u de stappen doorloopt, bieden we gegevensvoorbeelden. Vervang de voorbeelden door waarden die geschikt zijn voor uw omgeving.

U voert alle stappen in deze tutorial in Cloud Assembly uit.

Dit configuratieproces is de basis van uw Cloud Assembly-ontwikkelingservaring. Wanneer u uw infrastructuur bouwt en uw vaardigheden voor de ontwikkeling van cloudsjablonen verbetert, herhaalt u deze werkstroom en breidt u deze uit.

Wat moet u eerst doen

- Controleer of u de rol van Cloud Assembly-beheerder hebt. Zie [Organisatie- en servicegebruikersrollen in vRealize Automation](#).
- Als u de VMware vCenter Server of de wizards VMware Cloud Foundation-snelstart niet hebt gebruikt in de vRealize Automation-console, kunt u dit nu doen.

Deze werkstromen op basis van wizards bevatten de meeste, maar niet alle configuraties in deze tutorial.

Deze tutorial is een praktische ervaring die u meer inzicht geeft in hoe u een werkende infrastructuur kunt samenstellen en een workload kunt implementeren.

Zie [Hoe stel ik Cloud Assembly in](#) in de handleiding *Aan de slag*.

- Als u de stapsgewijze instelling die beschikbaar is in Cloud Assembly nog niet hebt gebruikt, kunt u dit nu doen. De stapsgewijze instelling leidt u door de meeste, maar niet alle procedures die u in deze tutorial uitvoert. Als u de stapsgewijze instelling wilt openen, klikt u op **Stapsgewijze instelling** aan de rechterkant van de tabbladbalk.
- Zorg ervoor dat u vCenter Server- en NSX-verificatiegegevens hebt. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#) voor meer informatie over de rechten die de verificatiegegevens moeten hebben. Als u van plan bent om extra gebruikers aan projecten toe te voegen, controleert u of deze lid zijn van de Cloud Assembly-service.

Stap 1: de vCenter Server- en NSX-cloudaccounts toevoegen

De cloudaccounts bieden de verificatiegegevens die vRealize Automation gebruikt om verbinding te maken met vCenter Server en de bijbehorende NSX-server.

- 1 Voeg het vCenter Server-cloudaccount toe.

Het vCenter Server-cloudaccount biedt de vCenter-verificatiegegevens die Cloud Assembly gebruikt om resources te detecteren en cloudsjablonen te implementeren.

Zie [Een vCenter-cloudaccount maken in vRealize Automation](#) voor meer informatie over vCenter Server-cloudaccounts.

- a Selecteer **Infrastructuur > Verbindingen > Cloudaccounts**.
- b Klik op **Cloudaccount toevoegen** en selecteer **vCenter**.
- c Voer de waarden in.

New Cloud Account

Name * vCenter Server Account

Description

vCenter Server Credentials

vCenter IP address / FQDN * sc2vc05.cmbu.local ⓘ

Username * mgmt@cmbu.local

Password *

VALIDATE ✓ Credentials validated successfully. ✕

Configuration

Allow provisioning to these datacenters * ☒ wld01-DC

☒ Create a cloud zone for the selected datacenters

NSX cloud account

Capabilities

Capability tags ⓘ

ADD **CANCEL**

Houd er rekening mee dat deze waarden alleen voorbeelden zijn. Uw waarden zijn specifiek voor uw omgeving.

Instelling	Voorbeeldwaarde
Naam	vCenter Server-account
IP-adres/FQDN voor vCenter	your-dev-vcenter.company.com
Gebruikersnaam en wachtwoord	vCenterCredentials@yourCompany.com

- d Om de verificatiegegevens te verifiëren, klikt u op **Valideren**.
 - e Als u de **inrichting in deze datacenters wilt toestaan**, selecteert u een of meer datacenters.
 - f Sla het NSX-cloudaccount over. We configureren dat later om het vCenter Server-account te koppelen aan het NSX-cloudaccount.
 - g Klik op **Toevoegen**.
- 2 Voeg een gekoppeld NSX-cloudaccount toe.

Het NSX-T-cloudaccount biedt de NSX-T-verificatiegegevens die Cloud Assembly gebruikt om netwerkresources te detecteren en netwerken met cloudsjablonen te implementeren.

Zie [Een vCenter-cloudaccount maken in vRealize Automation](#) voor meer informatie over NSX-T-cloudaccounts.

- a Selecteer **Infrastructuur > Verbindingen > Cloudaccounts**.
- b Klik op **Cloudaccount toevoegen** en selecteer NSX-T of NSX-V. Deze tutorial gebruikt **NSX-T**.
- c Voer de waarden in.

New Cloud Account

Name * NSX-T Account

Description

NSX-T Credentials

NSX-T IP address / FQDN * sc2vc05-vip-nsx-mgmt.cmbu.local ⓘ

Username * mgmt@cmbu.local

Password *

NSX mode Policy ⓘ

VALIDATE ✔ Credentials validated successfully ✕

Associations

vCenter cloud accounts + ADD ✕ REMOVE

<input type="checkbox"/>	Name	Status	Identifier	Type
<input type="checkbox"/>	vCenter Server Account	✔ OK	sc2vc05.cmbu.local	vCenter

1 - 1 of 1 cloud accounts

Capabilities

Capability tags Enter capability tags ⓘ

ADD CANCEL

Deze waarden zijn alleen voorbeelden. Uw waarden zijn specifiek voor uw omgeving.

Instelling	Voorbeeldwaarde
Naam	NSX-T-account
IP-adres/FQDN voor vCenter	your-dev-NSX-vcenter.company.com
Gebruikersnaam en wachtwoord	NSXCredentials@yourCompany.com
NSX-modus	<p>Weet u niet wat u moet selecteren?</p> <p>Hier is een goede gelegenheid om de hulp in het product te gebruiken. Klik op het informatiepictogram rechts van het veld. U ziet dat de hulp op veldniveau informatie bevat die u kan helpen bij het configureren van de optie.</p> <p>Selecteer Beleid in dit voorbeeld.</p>

- d Om de verificatiegegevens te verifiëren, klikt u op **Valideren**.
- e Als u het vCenter-cloudaccount wilt koppelen dat u in de vorige stap hebt gemaakt, klikt u op **Toevoegen** en selecteert u vervolgens het **vCenter-account**.
Deze vCenter-cloudaccountkoppeling zorgt voor de netwerkbeveiliging.
- f Klik op de pagina NSX-cloudaccount op **Toevoegen**.

Stap 2: de computerbronnen voor de cloudzone definiëren


De cloudzones zijn groepen van computerbronnen in een account/regio die vervolgens beschikbaar worden gemaakt voor projecten. De projectleden implementeren cloudsjablonen met behulp van de resources in de toegewezen cloudzones. Als u meer gedetailleerde controle wilt over waar projectcloudsjablonen worden geïmplementeerd, kunt u meerdere cloudzones met verschillende computerbronnen maken.

Accounts/regio's zijn de manier waarop cloudleveranciers resources koppelen aan geïsoleerde regio's of gegevensopslagruimten. Het account geeft het cloudaccounttype aan en de regio geeft de regio of gegevensopslag aan. vCenter Server gebruikt gegevensopslagruimten en de inrichtingsresources zijn de geselecteerde clusters en resourcepools.

Voor deze tutorial moet u ervoor zorgen dat de cloudzones de resources bevatten die de doelstellingen van het projectontwikkelingsteam en uw budget- en beheervereisten ondersteunen.

Zie [Meer informatie over Cloud Assembly-cloudzones](#) voor informatie over cloudzones.

- 1 Selecteer **Infrastructuur > Configureren > Cloudzones**.
- 2 Klik op de cloudzone die is toegevoegd voor uw vCenter Server-instantie en voer de waarden in.


vCenter Account Cloud Zone
DELETE

Summary
Compute
Projects

A cloud zone defines a set of compute resources that can be used for provisioning.

Account / region *

vCenter Account / wld01-DC

Name *

vCenter Account Cloud Zone

Description

Placement policy *

DEFAULT

Folder

Select folder

Capabilities

Capability tags are effectively applied to all compute resources in this cloud zone, but only in the context of this cloud zone.

Capability tags

Enter capability tags

SAVE

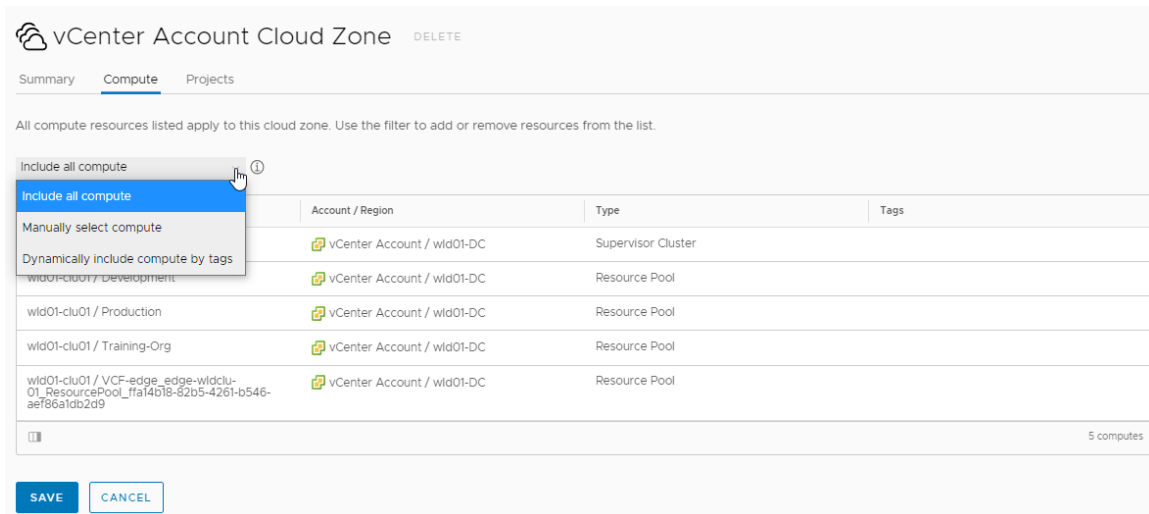
CANCEL

Instelling	Voorbeeldwaarde
Account/regio	vCenter-account / datacenternaam
Naam	vCenter Server-cloudzone Deze waarde kan niet worden gewijzigd nadat u deze hebt gemaakt. Als u een ander datacenter wilt configureren voor een andere vCenter Server, moet u een nieuwe cloudzone maken waarin u het account en de regio kunt selecteren.
Beschrijving	Alle vCenter Server-computerbronnen voor ontwikkeling.
Beleid	Standaard Vergeet niet om de Help te raadplegen als u vragen hebt over een veldwaarde.

Houd er rekening mee dat alle waarden alleen voorbeelden zijn. Uw zonespecificaties zijn specifiek voor uw omgeving.

- Klik op het tabblad **Berekenen** en controleer of de computerbronnen allemaal aanwezig zijn.

Als u er één wilt uitsluiten, schakelt u over naar **Berekeningen handmatig selecteren** en voegt u alleen de bronnen toe die u wilt opnemen in de cloudzone.



4 Klik op **Opslaan**.

5 Herhaal het proces voor aanvullende cloudzones, maar u moet unieke zonenamen gebruiken.

Stap 3: de mogelijke resources configureren die beschikbaar zijn voor het account/de regio

U hebt het account/de regio aan de cloudzone toegevoegd. Nu kunt u de mogelijke machinegrootten (soorttoewijzingen), imago-toewijzingen, netwerkprofielen en opslagprofielen voor het cloudaccount definiëren. De toewijzings- en profieldefinities worden geëvalueerd om een overeenkomst te bepalen wanneer u een cloudsjabloon implementeert, zodat de workload de juiste machinegrootte (soort), image, netwerken en opslag bevat.

1 Configureer de soorttoewijzingen voor de accounts/regio's.

Naar soorten wordt soms ook verwezen als t-shirt-maten. Afhankelijk van hoe uw cloudsjabloon is geconfigureerd, bepaalt de toegewezen soorttoewijzing het aantal CPU's en geheugen.

Zie [Meer informatie over soorttoewijzingen in vRealize Automation](#) voor informatie over soorttoewijzingen.

a Selecteer **Infrastructuur > Configureren > Soorttoewijzingen**.

b Klik op **Nieuwe soorttoewijzing** en voer waarden in die kleine, middelgrote en grote machines definiëren.

Onthoud dat dit voorbeeldwaarden zijn. U moet relevante accounts/regio's selecteren en de grootten definiëren.

The screenshot shows a configuration page for a flavor named 'small'. It includes a 'Flavor name' field with the value 'small' and a 'Configuration' table. The table has two columns: 'Account / Region' and 'Value'. The first row shows 'vCenter Account / wld01-DC' for the account/region and '2' for the value. The second row shows '1' for the value. There are also fields for 'CPU' and 'Memory' (labeled 'GB') with values '2' and '1' respectively. A 'DELETE' button is visible at the top right.

Instelling	Voorbeeldwaarde
Soortnaam	small
Account/regio	vCenter-account/datacenter
CPU-waarde	2
Geheugenwaarde	1 GB

- c Klik op **Maken**.
- d Als u extra grootten wilt maken, configureert u de toewijzingen voor middelgrote en grote soorttoewijzingen voor het account/de regio.

Instelling	Voorbeeldwaarde
Soortnaam	medium
Account/regio	vCenter-account/datacenter
CPU-waarde	4
Geheugenwaarde	2 GB
Soortnaam	large
Account/regio	vCenter-account/datacenter
CPU-waarde	8
Geheugenwaarde	4 GB

- 2 Configureer de imageroewijzingen voor de accounts/regio's.

De images zijn het besturingssysteem voor machines in de cloudsjabloon. Wanneer u met vCenter Server-images werkt, selecteert u vCenter-sjablonen.

Zie [Meer informatie over imageroewijzingen in vRealize Automation](#) voor informatie over imageroewijzingen.

- a Selecteer **Infrastructuur > Configureren > Imageroewijzingen**.
- b Klik op **Nieuwe imageroewijzing** en zoek naar de images voor het account/de regio.
Onthoud dat dit voorbeeldwaarden zijn. U moet relevante images selecteren die in uw account/regio zijn gedetecteerd.

centos [DELETE](#)

Allows you to define images or machine templates by name in a cloud-agnostic way. ⓘ

Image name * centos

Configuration * Account / Region Image Constraints Cloud Configuration

Q vCenter Account / wldf Q centos7 Example: license:none ⓘ [+ ADD](#) ⓘ

Instelling	Voorbeeldwaarde
Imagenaam	centos
Account/regio	vCenter-account
Image	centos7

- c Klik op **Maken**.
 - d Herhaal dit proces om aanvullende imagedtoewijzingen te maken. Bijvoorbeeld een Ubuntu-toewijzing voor het account/de regio.
- 3 Configureer netwerkprofielen.
- Netwerkprofielen definiëren de netwerken en netwerkinstellingen die beschikbaar zijn voor een account/regio. De profielen moeten de doelimplementatieomgevingen ondersteunen. Deze taak biedt de minimale configuratie-informatie voor succes. Als u meer informatie wilt over netwerkprofielen, begint u met [Meer informatie over netwerkprofielen in vRealize Automation](#).
- a Selecteer **Infrastructuur > Configureren > Netwerkprofiel**.
 - b Klik op **Nieuw netwerkprofiel** en maak een profiel voor account/regio vCenter-account/datacenter.

Network Profile DELETE

Summary Networks Network Policies Load Balancers Security Groups

A network profile defines a group of networks and network settings used when machines are provisioned.

Account / region vCenter Account / wld01-DC

Name Network Profile

Description Networks for development teams.

Capabilities
Capability tags listed here are matched to constraint tags in the cloud template.

Capability tags Enter capability tags

Instelling	Voorbeeldwaarde
Account/regio	vCenter-account/datacenter
Naam	Netwerkprofiel
Beschrijving	Netwerken voor ontwikkelingsteams.

- c Klik op het tabblad **Netwerken** en klik vervolgens op **Netwerk toevoegen**.

Network Profile DELETE

Summary **Networks** Network Policies Load Balancers Security Groups

Networks listed here are used when provisioning to existing, on-demand, or public networks.

+ ADD NETWORK TAGS MANAGE IP RANGES REMOVE

<input type="checkbox"/>	Name	Account / Region	Zone	Network Domain	CIDR	Support Public IP	Default for Zone	Origin	Tags
<input type="checkbox"/>	DevProject-004	NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	192.168.1.64/27	--	--	Deployed	
<input type="checkbox"/>	External-mcm13/3520-150877845350	NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	172.16.1.64/28	--	--	Discovered	
<input type="checkbox"/>	seg-domain-c8e2a5390e-2772-43f5-9eaa-eddc05e35996-vmware-system-nsx-0	NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	10.244.0.0/28	--	--	Discovered	external_id:8... ncp/project_u... ncp/cluster.d... ncp/version.1... ncp/project.v...

1 - 3 of 3 networks

- d Selecteer de NSX-netwerken die u beschikbaar wilt stellen voor het ontwikkelingsteam voor applicaties.

In dit voorbeeld hadden we een NSX-T-netwerk met de naam DevProject-004.

- e Klik op het tabblad **Netwerkbeleid** en maak een beleid.

Instelling	Voorbeeldwaarde
Isolatiebeleid	Geen
Logische laag-0-router	Laag-0-router
Edge-cluster	EdgeCluster

f Klik op **Maken**.

4 Configureer opslagprofielen.

Opslagprofielen definiëren de schijven voor een account/regio. De profielen moeten de doelimplementatieomgevingen ondersteunen.

Als u meer informatie over opslagprofielen wilt, raadpleegt u [Meer informatie over opslagprofielen in vRealize Automation](#).

a Selecteer **Infrastructuur > Configureren > Opslagprofiel**.

b Klik op **Nieuw opslagprofiel** en maak een profiel voor account/regio vCenter Server/datacenter.

Behoud de standaardwaarden, tenzij waarden zijn opgegeven in de tabel.

Storage Profile

Account / region: vCenter Account / wld01-DC

Name: Storage Profile

Description: [Empty text box]

Disk type: ☒ Standard disk ☐ First class disk (FCD) ⓘ

Storage policy: Datastore default ⓘ

Datastore / cluster: Q_ wld01-sc2vc05-wld01-clu01-vsan01 ⓘ

Provisioning type: Unspecified ⓘ

Shares: Unspecified ⓘ

Limit IOPS: ⓘ

Disk mode: Dependent ⓘ

☐ Supports encryption ⓘ

☒ Preferred storage for this region ⓘ

Capability tags: Enter capability tags ⓘ

SAVE **CANCEL**

Instelling	Voorbeeldwaarde
Account/regio	vCenter-account/datacenter
Naam	Opslagprofiel
Gegevensopslag/cluster	Gegevensopslag met voldoende capaciteit geselecteerd die toegankelijk is voor alle hosts.
Voorkeursopslag voor deze regio	Schakel het selectievakje in.

c Klik op **Maken**.

Stap 4: een project maken

Hier gaat u daadwerkelijk aan de slag met de doelstellingen van het project.

- Welke gebruikers hebben toegang nodig tot de computerbronnen zodat ze een applicatiecloudsjabloon kunnen maken en implementeren? Zie [Organisatie- en servicegebruikersrollen in vRealize Automation](#) voor meer informatie over wat de verschillende projectrollen kunnen zien en doen.
- Zullen de leden van het project applicaties maken die van ontwikkeling naar productie gaan? Wat zijn de nodige resources?
- Welke cloudzones zijn er nodig? Welke prioriteit en limieten moeten voor elke zone van het project worden ingesteld?

Voor deze tutorial zullen we het ontwikkelingsteam ondersteunen terwijl ze een interne softwareapplicatie maken en uitbreiden.

Deze taak biedt de minimale configuratie-informatie voor succes. Als u meer informatie over projecten wilt, begint u met [Meer informatie over Cloud Assembly-projecten](#).

- 1 Selecteer **Infrastructuur > Beheer > Projecten**.

- 2 Klik op **Nieuw project** en voer de naam **Development Project** in.

- 3 Klik op het tabblad **Gebruikers** en klik vervolgens op **Gebruikers toevoegen**.

U bent op dit moment niet verplicht om gebruikers toe te voegen. Maar als u andere gebruikers met cloudsjablonen wilt laten werken, moeten ze lid zijn van het project.

- 4 Voer e-mailadressen in om gebruikers toe te voegen als projectleden of beheerders, afhankelijk van de rechten die u elke persoon wilt geven.

- 5 Klik op **Inrichting** en klik vervolgens op **Zones toevoegen > Cloudzone**.

- 6 Voeg de cloudzones toe waarop de gebruikers kunnen worden geïmplementeerd.

U kunt ook resourcelimieten voor de cloudzone in het project instellen. In de toekomst kunt u verschillende limieten voor andere projecten instellen.

Instelling voor projectcloudzone	Voorbeeldwaarde
Cloudzone	vCenter-accountcloudzone
Inrichtingsprioriteit	1
Limiet voor instanties	5

- 7 Voeg aanvullende cloudzones toe aan het project.

- 8 Klik op **Maken**.

- 9 Om te controleren of het project is toegevoegd aan de cloudzone, selecteert u **Infrastructuur > Configureren > Cloudzones** en opent u de zonekaart van de vCenter-accountzonecloud zodat u het tabblad **Projecten** kunt bekijken. U ziet nu het ontwikkelingsproject.

Stap 5: een basiscloudsjabloon ontwerpen en implementeren

U ontwerpt en implementeert de cloudsjabloon om ervoor te zorgen dat uw infrastructuur correct is geconfigureerd om de sjabloon te ondersteunen. Later kunt u voortbouwen op de sjabloon wanneer u een applicatie maakt die aan uw projectbehoeften voldoet.

De beste manier om een cloudsjabloon te bouwen is onderdeel per onderdeel. Controleer hierbij of deze tussen elke wijziging wordt geïmplementeerd. Deze tutorial begint met een eenvoudige machine en voegt vervolgens meer resources toe.

De voorbeelden in deze procedure maken gebruik van de YAML-code-editor. Dit is een eenvoudigere manier om u te voorzien van codefragmenten. Als u echter de voorkeur geeft aan een gebruikersinterface met dialoogvensters, klikt u op **Invoer**.

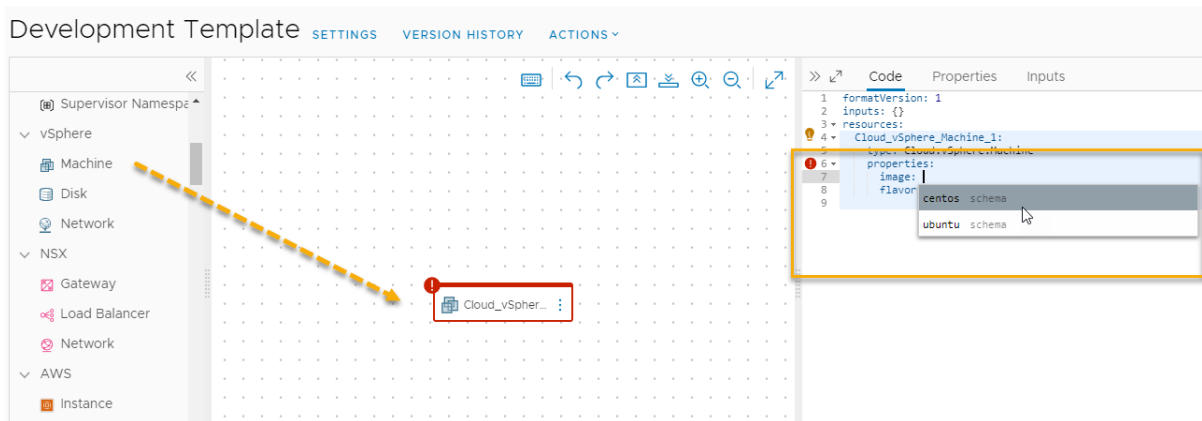
Er is zoveel meer dat u kunt doen met cloudsjablonen dan in deze tutorial wordt vermeld. Als u meer informatie wilt, begint u met [Hoofdstuk 6 Uw Cloud Assembly-implementaties ontwerpen](#).

Deze tutorial gebruikt vSphere- en NSX-resourcetypes. Deze resourcetypes kunnen alleen worden geïmplementeerd op eindpunten van het vCenter Server-cloudaccount. U kunt ook de cloudonafhankelijke resourcetypes gebruiken om cloudsjablonen te maken die op elk eindpunt kunnen worden geïmplementeerd. Zie [Tutorial: Infrastructuur en implementaties met meerdere clouds instellen en testen in Cloud Assembly](#) voor een voorbeeld van het configureren van de infrastructuur en het ontwerpen van de sjabloon voor elk eindpunt.



Zie [Een basiscloudsjabloon ontwerpen en implementeren](#) voor een video met de basisstappen in deze procedure.

- 1 Selecteer **Ontwerp > Cloudsjablonen**.
- 2 Selecteer **Nieuw van > leeg canvas**.
- 3 Voer de naam **Development Template** in, selecteer het project **Development Project** en klik op **Maken**.
- 4 Voeg een vSphere-machine toe aan het ontwerpcanvas, test en implementeer.



- a Sleep een **vSphere-machine** naar het canvas in het deelvenster Resourcetype.

Het deelvenster **Code** toont de YAML voor de machine, met een lege waarde voor image en vooraf gedefinieerde CPU en geheugeneigenschappen. U gaat deze sjabloon zo instellen dat deze flexibele formaataanpassing wordt ondersteund.

- b Als u een imagewaarde wilt selecteren, plaatst u de aanwijzer tussen de enkele aanhalingstekens voor `image` en selecteert u **centos** in de lijst met images die u hebt geconfigureerd.

Onthoud dat dit voorbeeldwaarden zijn. Als u geen centos-image hebt geconfigureerd, selecteert u een image die u hebt geconfigureerd.

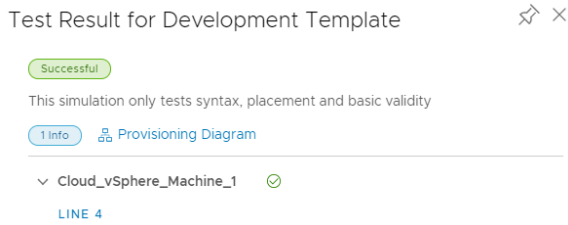
- c Maak een regel onder de image-eigenschap en voer `flavor` in of selecteer het en selecteer vervolgens `small` in de lijst.
- d Verwijder `cpuCount` en `totalMemory`.

Uw YAML moet er ongeveer als volgt uitzien.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
```

- e Klik op **Test**.

Met Test kunt u de syntaxis en plaatsing van uw cloudsjabloon valideren. Een succesvolle test garandeert niet dat u de sjabloon zonder fouten kunt implementeren.



Als de test mislukt, klikt u op **Inrichtingsdiagram** en zoekt u de foutpunten. Zie [Een basiscloudsjabloon testen](#) voor meer informatie over het gebruik van het diagram.

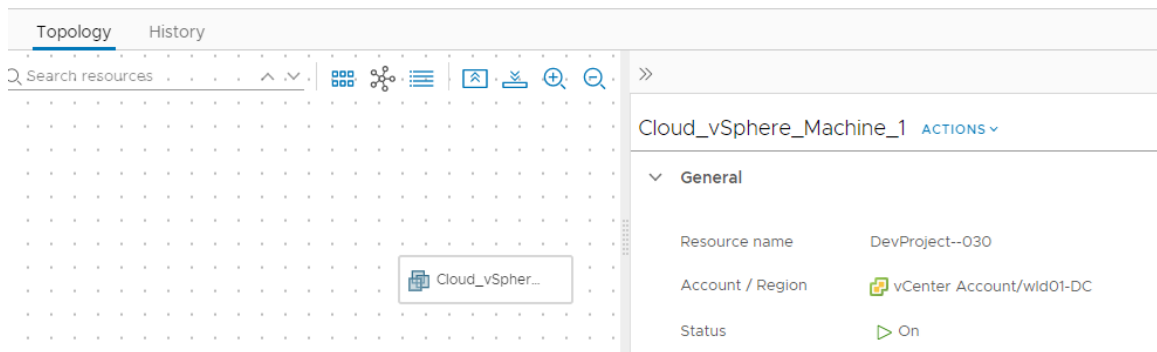
f Klik op **Implementeren**.

g Voer de **implementatienaam** **DevTemplate - machine** in en klik op **Implementeren**.

U kunt de voortgang van de implementatie volgen op de pagina met de DevTemplate-implementatiedetails of op de pagina Implementaties. Selecteer **Resources > Implementaties**.

Als de implementatie mislukt, kunt u het probleem oplossen en uw sjabloon herzien. Zie [Wat kan ik doen als een Cloud Assembly-implementatie mislukt](#).

Een succesvolle implementatie ziet eruit als in dit voorbeeld op de pagina Implementaties.



5 Stel de versie van de sjabloon in en voeg een netwerk toe.

Het versienummer van een cloudsjabloon is vereist om deze beschikbaar te maken in de Service Broker-catalogus, maar het is handig om een goede versie te hebben waarnaar u kunt teruggaan tijdens de ontwikkeling.

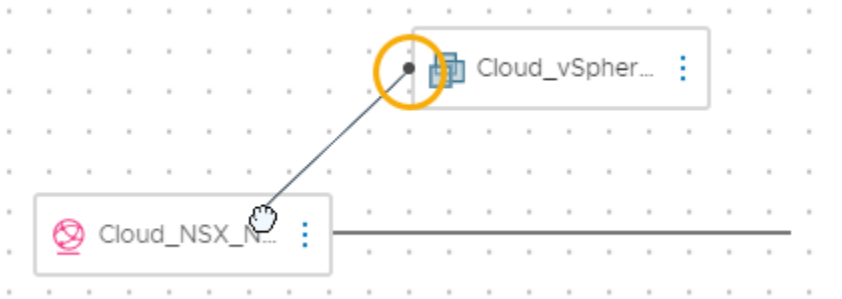
a Open de sjabloon op het ontwerpcanvas.

b Klik op **Versie**, voer een **beschrijving** in zoals **Simple deployable machine** en klik op **Maken**.

c Sleep in het deelvenster Resourcetype een resourcetype **NSX-netwerk** naar het canvas.

d Verbind de machine met het netwerk.

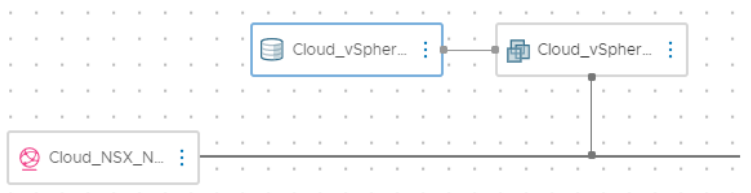
Klik op de kleine cirkel op het machineonderdeel en sleep de verbinding naar het netwerk.



De YAML ziet er nu ongeveer uit als in dit voorbeeld.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks: []
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
```

- e Klik op **Test** om de sjabloon te valideren.
 - f Klik op **Implementeren**.
 - g Voer de naam **DevTemplate - machine - network** in en klik op **Implementeren**.
 - h Volg de voortgang en controleer de succesvolle implementatie.
- 6 Stel de versie van de sjabloon in en voeg gegevensschijf toe.
- a Open de sjabloon op het ontwerpcanvas.
 - b Stel de versie van de sjabloon in.
- Voer **Machine with existing network** in als beschrijving.
- c Sleep in het deelvenster Resourcetype een resourcetype **vSphere-schijf** naar het canvas.
 - d Verbind de schijf met de machine.



De YAML ziet er nu ongeveer uit als in dit voorbeeld.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
```

- e Test de sjabloon.
- f Implementeer de sjabloon met behulp van de naam **DevTemplate - machine - network - storage**.
- g Volg de voortgang en controleer de succesvolle implementatie.
- h Stel de versie van de sjabloon in.

Voer **Machine with existing network and storage disk** in als beschrijving.

Deze definitieve versie zorgt ervoor dat u een werkende sjabloon aan de servicecatalogus kunt toevoegen.

Tutorialresultaten

U hebt de werkstroom voltooid die Cloud Assembly als een werkend systeem heeft geconfigureerd. U bent nu vertrouwd met de volgende concepten.

- Cloudaccounts zijn de verificatiegegevens die Cloud Assembly verbinden met de eindpunten van uw cloudleverancier.
- Cloudzones zijn de geselecteerde computerbronnen in account/regio's die u vervolgens aan verschillende projecten toewijst op basis van de behoeften van het project en uw doelen voor het beheren van de kosten.
- Infrastructuurresources zijn definities van resources die zijn gekoppeld aan accounts/regio's die worden gebruikt in cloudsjablonen.

- Met projecten kunt u uw gebruikers toegang geven tot de cloudzones op basis van de applicatieontwikkelingsdoelen van het project.
- Cloudsjablonen zijn de definities van uw applicatieworkloads die u iteratief ontwikkelt en implementeert.

Deze tutorial vormt de basis voor uw Cloud Assembly-ontwikkelingservaring. U kunt dit proces gebruiken om uw infrastructuur te bouwen en uw vaardigheden voor de ontwikkeling van cloudsjablonen te verbeteren.

Tutorial: Cloud Assembly configureren voor het inrichten van een productieworkload

Als cloudbeheerder wilt u het implementatieproces voor een project automatiseren, zodat Cloud Assembly het werk voor u doet wanneer de cloudsjabloonontwerpers sjablonen maken en implementeren. Bijvoorbeeld: de workloads worden geïmplementeerd met een bepaald aangepast naamgevingspatroon voor machines, de machines worden toegevoegd aan een specifieke organisatie-eenheid van Active Directory en er worden specifieke DNS- en IP-bereiken gebruikt.

Door het proces voor de projectimplementaties te automatiseren, kunt u gemakkelijker meerdere projecten in verschillende datacenters en cloudomgevingen beheren.

U bent niet verplicht om alle hier opgegeven taken uit te voeren. U kunt deze taken combineren en aan elkaar koppelen, afhankelijk van uw beheerdoelen.

Voordat u begint

Deze tutorial vereist dat u uw infrastructuur hebt geconfigureerd en dat u een cloudsjabloon met een machine en een netwerk hebt geïmplementeerd. Controleer of de volgende al zijn geconfigureerd op uw systeem.

- U hebt alle stappen uitgevoerd die zijn opgegeven in de infrastructuurtutorial. Zie [Tutorial: vSphere-infrastructuur en -implementaties in Cloud Assembly instellen en testen](#).
- U hebt de rol van Cloud Assembly-beheerder. Zie [Organisatie- en servicegebruikersrollen in vRealize Automation](#).

De machinenamen aanpassen

Het doel van deze taak is om ervoor te zorgen dat de geïmplementeerde machines voor het ontwikkelingsproject worden benoemd op basis van de kostenplaats voor het project, het resourcetype dat tijdens de implementatie is geselecteerd en oplopende nummers om een uniekheid te garanderen. Bijvoorbeeld: DevProject-centos-021.

U kunt dit voorbeeld aanpassen aan uw naamgevingsvereisten.

Zie [Hoofdstuk 5 Cloud Assembly-projecten toevoegen en beheren](#) voor meer informatie over projecten.



Zie [Een aangepaste naamsjabloon voor implementaties maken](#) voor een video met een voorbeeld van aangepaste naamgeving.

1 Selecteer **Infrastructuur > Projecten**.

2 Selecteer een bestaand project of maak een nieuw.

Voor deze tutorial is de projectnaam Development Project.

3 Klik op **Maken**.

4 Op de pagina Projecten klikt u op de projectnaam op de tegel zodat u het project kunt configureren.

5 Klik op het tabblad **Gebruikers** en voeg de gebruikers toe die deel uitmaken van dit project.

6 Klik op het tabblad **Inrichting**.

a Klik in de sectie Zones op **Zone toevoegen** en voeg de mogelijke cloudzones toe waar de workloads voor dit project worden geïmplementeerd.

b In de sectie Aangepaste eigenschappen voegt u een aangepaste eigenschap toe met de naam **costCenter** en de waarde **DevProject**.

c Voeg in de sectie Aangepaste naamgeving de volgende naamgevingssjabloon toe.

```
${resource.costCenter}-${resource.installedOS}-${###}
```

`${resource.installedOS}` is gebaseerd op het besturingssysteem dat is geselecteerd bij de implementatie van de cloudsjabloon.

7 Klik op **Opslaan**.

8 Werk de cloudsjabloon bij met een invoerwaarde voor het type besturingssysteem.

Invoerwaarden zijn de directe manier waarop u het implementatie-aanvraagformulier voor gebruikers kunt aanpassen en uw ontwikkelingsproces kunt vereenvoudigen. Door invoerwaarden te maken, kunt u één cloudsjabloon gebruiken om workloads met verschillende configuraties te implementeren. Bijvoorbeeld: grootte of besturingssysteem.

In dit voorbeeld wordt de ontwikkelingssjabloon van een vorige tutorial gebruikt. Zie [Stap 5: een basiscloudsjabloon ontwerpen en implementeren](#).

a Selecteer **Ontwerp** en open de ontwikkelingssjabloon.

- b Werk de YAML bij met de volgende wijzigingen in het deelvenster Code.

- Voeg **installedOS** toe in de sectie `Inputs`.

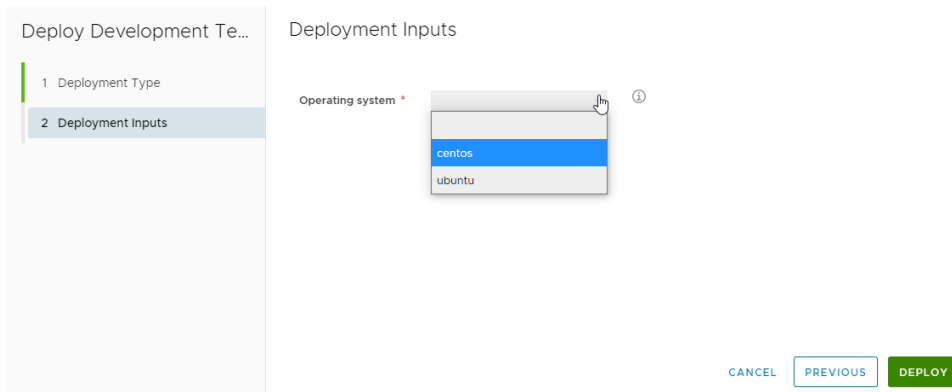
In de volgende stap kunt u zien dat de invoer voor `installedOS` ook wordt gebruikt om de image op te geven. Wanneer u de tekenreeksen in de sectie `enum` toevoegt, moeten de waarden, in dit voorbeeld zijn dat `centos` en `ubuntu`, overeenstemmen met de imagenamen die u hebt gedefinieerd in **Infrastructuur > Configureren > Imagetoewijzingen**. Als de naam van de imagetoewijzing bijvoorbeeld CentOS is en niet centos, gebruikt u CentOS in de invoersectie.

```
inputs:
  installedOS:
    type: string
    title: OS Type
    description: Select the operating system.
    enum:
      - centos
      - ubuntu
```

- In de sectie `Cloud_vSphere_Machine_1` werkt u de `image` bij naar een `installedOS`-invoerparameter (`${input.installedOS}`) en voegt u een aangepaste `installedOS`-eigenschap met dezelfde invoerparameter toe.

```
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: ${input.installedOS}
      installedOS: ${input.installedOS}
      flavor: small
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
```

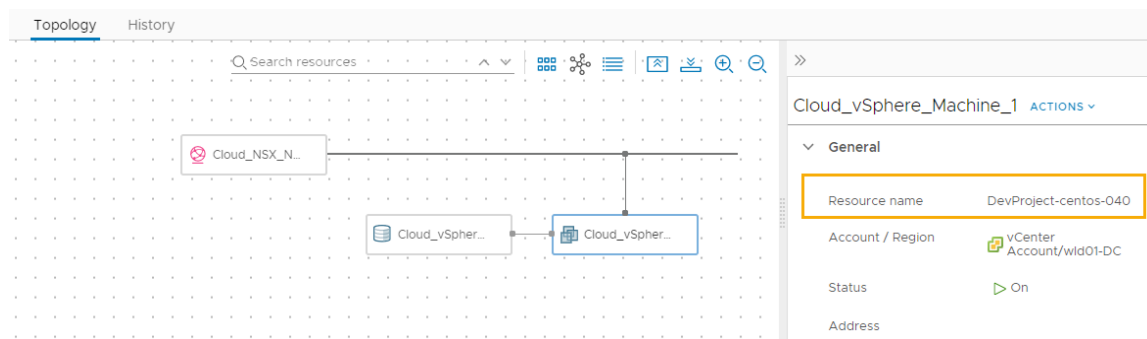
- c Klik op **Implementeren** en voer de naam **Custom name deployment test** in.
- d Klik op **Volgende**.
- e Selecteer het besturingssysteem **centos** in het vervolgkeuzemenu.



f Klik op **Implementeren**.

9 Volg de voortgang en controleer de succesvolle implementatie.

De machinenaam in dit voorbeeld is DevProject-centos-026. Ter herinnering: dit voorbeeld is gebaseerd op de tutorial waarnaar wordt verwezen aan het begin van deze taak.



Active Directory-machinerecords maken

Wanneer u een workload inricht, kunt u machinerecords maken in Active Directory. Door Cloud Assembly te configureren om deze taak automatisch uit te voeren voor projectimplementaties, hebt u uw eigen workload als cloudbeheerder gemarkeerd.

1 Voeg een Active Directory-server toe.

a Selecteer **Infrastructuur > Verbindingen > Integraties**.

Deze stappen beschrijven de basisconfiguratie van Active Directory die is gerelateerd aan deze tutorial voor de AD-machinerecords. Zie [Hoe maak ik een Active Directory-integratie in Cloud Assembly?](#) voor meer informatie over de integratie van Active Directory.

b Klik op **Integratie toevoegen** en klik op **Active Directory**.

- c Voer de naam in die u voor deze integratie gebruikt.
- d Voer de **LDAP-host/IP** en de bijbehorende verificatiegegevens in.
- e Voer de **Base DN** in.

In deze tutorial is het voorbeeld **ou=AppDev,dc=cmbu,dc=local**. AppDev is de bovenliggende organisatie-eenheid voor de computerafdeling die u wilt toevoegen voor het project.

- f Klik op **Toevoegen**.

- 2 Voeg het project toe aan de integratie.
 - 3 Klik in de Active Directory-integratie op het tabblad **Projecten** en klik op **Project toevoegen**.
- Add Projects

Select a project and the OU it will be mapped to by adding its relative DN. The effective DN is created by appending the RDN to the integration base DN (**dc=cmbu,dc=local**).

CANCEL ADD

- a Selecteer het project App Deployment.
- b Voer de relatieve DN's in. Bijvoorbeeld: **OU=AppDev-Computers**.

- c Schakel de schakelaars Overschrijven en Negeren niet in.

Deze procedure is gericht op het automatiseren van het proces voor een project. Het gaat niet om aanpassingen die u in sjablonen kunt aanbrengen.

- d Klik op **Toevoegen**.

- 4 Klik op **Opslaan** om uw wijzigingen in de integratie op te slaan.
- 5 Implementeer een cloudsjabloon voor het project en controleer of de machine is toegevoegd aan de juiste organisatie-eenheid van Active Directory.

Uw netwerk-DNS en intern IP-bereik instellen

Voeg een netwerkprofiel toe of werk het bij om uw DNS-servers en interne IP-bereiken op te nemen.

U moet al een cloudaccount hebben gemaakt voor vSphere, NSX-V of NSX-T. Zie [Tutorial: vSphere-infrastructuur en -implementaties in Cloud Assembly instellen en testen](#) of [Cloudaccounts aan Cloud Assembly toevoegen](#).

- 1 Selecteer **Infrastructuur > Configureren > Netwerkprofielen**.
- 2 Selecteer een bestaand profiel of maak een profiel.
- 3 Selecteer op het tabblad **Samenvatting** een **account/regio** en voer een naam in.
Voor deze tutorial is de naam van het netwerkprofiel Network Profile.
- 4 Voeg netwerken toe.
 - a Klik op het tabblad **Netwerken**.
 - b Klik op **Netwerk toevoegen**.
 - c Voeg een of meer NSX- of vSphere-netwerken toe.
 - d Klik op **Toevoegen**.
- 5 Configureer de DNS-servers.
 - a Klik in de lijst met netwerken op het tabblad **Netwerken** op de netwerknaam.

Summary

Networks

Network Policies

Load Balancers

Security

Networks listed here are used when provisioning to existing, on-demand, or p

+ ADD NETWORK

TAGS

MANAGE IP RANGES

REMOVE

<input type="checkbox"/>	Name ↑	Account / Region	Zone	Network Domain	CIDR
<input type="checkbox"/>	DevProject --004	NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	192.168.1.64 /27

- b Voer de IP-adressen van de DNS-server in die u door dit netwerk wilt laten gebruiken.

DevProject--004

DNS servers

192.168.1.22
192.168.1.23

DNS search domains

company.local

DNS Servers

Use a comma separated list or new lines.

- c Klik op **Opslaan**.

- 6 Geef het IP-adres van het netwerk op.

- a In de lijst met netwerken schakelt u het selectievakje naast de netwerknaam in.

Network Profile [DELETE](#)

Summary **Networks** Network Policies Load Balancers Security Groups

Networks listed here are used when provisioning to existing, on-demand, or public networks. ⓘ

[+ ADD NETWORK](#) [TAGS](#) [MANAGE IP RANGES](#) [REMOVE](#)

<input type="checkbox"/>	Name	Account / Region	Zone	Network Domain	CIDR	Su Pu
<input type="checkbox"/>	External-mcm1343745-148168716643	NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	172.16.12.64/28	
<input type="checkbox"/>	NSX-mcm1376447-151082888186	NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	192.168.100.32/28	
<input checked="" type="checkbox"/>	NSX-mcm39835-146434698964	NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	192.168.1.0/27	

1

- b Klik op **IP-bereiken beheren**.

- c Klik in het dialoogvenster IP-bereiken beheren op **Nieuw IP-bereik**.

New IP Range

Network *	NSX-mcm1376447-151082888186
Source	<input checked="" type="radio"/> Internal <input type="radio"/> External
Name *	DevProject Range
Description	<div></div>
CIDR	192.168.100.32/28
Start IP address *	192.168.100.34
End IP address *	192.168.100.46

- d Voer een naam in.
Bijvoorbeeld: **DevProject Range**.
 - e Als u het bereik wilt definiëren, voert u het **Eerste IP-adres** en **Laatste IP-adres** in.
 - f Klik op **Toevoegen**.
 - g Voeg extra bereiken toe of klik op **Sluiten**.
- 7 Voeg de cloudzone toe die het gekoppelde netwerkaccount of de gekoppelde regio bevat die u hebt geconfigureerd voor uw ontwikkelingsproject.
 - 8 Implementeer een cloudsjabloon voor het project en controleer of de machine is ingericht binnen het opgegeven IP-bereik.

Tutorials: tags in Cloud Assembly gebruiken om vSphere-resources te beheren

Tags zijn krachtige metagegevens die u kunt koppelen aan resources en in sjablonen kunt opnemen. U kunt tags in verschillende beheerscenario's gebruiken, waaronder verdeling van workloads en resourcelabeling.

Snelle inleiding tot tags

Deze sectie is een eenvoudige inleiding tot tags zoals deze gelden voor de opgegeven stappen. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#) voor meer gedetailleerde informatie over tags.

- Capaciteits- en beperkingstags

U kunt tags gebruiken om implementaties te bepalen op basis van resourcemogelijkheden. Als cloudbeheerder wilt u bijvoorbeeld dat de iteratief ontwikkelde cloudsjablonen worden geïmplementeerd op een resourcepool die specifiek is voor ontwikkeling en dat de productiewaardige sjablonen worden geïmplementeerd in een andere resourcepool.

- Capaciteitstags worden aan resources toegevoegd en definiëren daarbij hun mogelijkheden.
- Beperkingstags worden in cloudsjablonen gebruikt, en definiëren welke resources de geïmplementeerde resources moeten gebruiken.
- Labeltags

Om resources te beheren, kunt u tags toevoegen als objectlabels of beschrijvingen. De beheermogelijkheden zijn onder andere betere zoekresultaten voor resources, het differentiëren tussen vergelijkbare objecten, het annoteren van objecten met aangepaste informatie, het bieden van informatie aan systemen van derden, het maken van lidmaatschapscriteria voor beveiligingsgroepen en het zorgen voor consistentie in gekoppelde SDDC-domeinen.

Voordat u begint

- Controleer de resources en de cloudsjabloon die in [Tutorial: vSphere-infrastructuur en -implementaties in Cloud Assembly instellen en testen](#) is gedefinieerd. De voorbeeldwaarden uit de tutorial worden ook hier gebruikt.

Tags gebruiken om verdeling van workloads te beheren

Dit eenvoudige voorbeeld maakt gebruik van ontwikkelings- en productieomgevingstags om te demonstreren hoe u capaciteits- en beperkingstags kunt gebruiken. Eerst voegt u capaciteitstags toe aan computerbronnen voor vCenter Server-resourcepools en vervolgens voegt u de tags toe in de cloudsjabloon. In het voorbeeld van de cloudsjabloon wordt getoond hoe u invoer gebruikt om de implementerende gebruiker te laten selecteren of hij of zij deze wil implementeren in een resourcepool voor ontwikkeling of productie.

Zie [Tutorial: Infrastructuur en implementaties met meerdere clouds instellen en testen in Cloud Assembly](#) voor een voorbeeld van hoe u dezelfde tags gebruikt om plaatsing in een omgeving met meerdere clouds te definiëren.

- 1 Voeg capaciteitstags toe aan uw resourcepools.
 - a Selecteer **Infrastructuur > Resources > Berekenen**.

- b Open de cloudzone en klik op **Berekenen**.

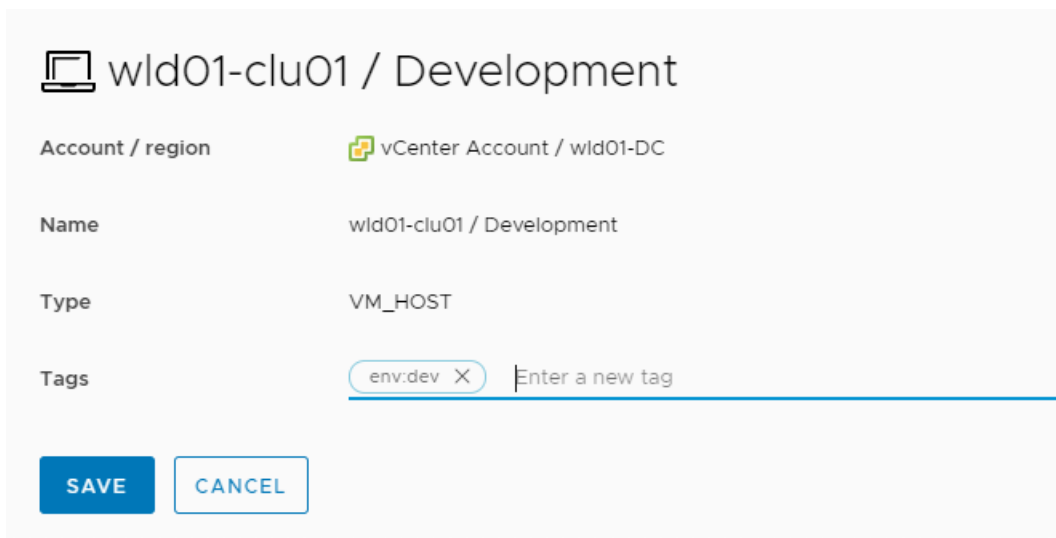


- c Zoek de resourcepool waarin u ontwikkelingsworkloads wilt implementeren.

Deze tutorial gebruikt de volgende voorbeeldwaarden. Houd er rekening mee dat deze waarden alleen voorbeelden zijn. Uw waarden zijn specifiek voor uw omgeving.

Voorbeeld van resourcepool	Voorbeeld van tag
wld01-clu01 / Development	env:dev
wld01-clu01 / Production	env:prod

- d Voeg de tag **env:dev** toe en klik op **Opslaan**.



- e Herhaal het proces voor de resourcepool waarin u productieworkloads wilt implementeren en voeg de tag **env:prod** toe.
- 2 Controleer of de capaciteitstags zijn toegevoegd aan de resourcepools in uw cloudzone.
- a Selecteer **Infrastructuur > Configureren > Cloudzones**.
- b Open de cloudzone die aan het project is gekoppeld en klik op **Berekenen**.

In dit voorbeeld is de cloudzone 'vCenter Account Cloud Zone' en zijn de tags toegevoegd aan de twee resourcepools, wld01-clu01 / Development en wld01-clu01 / Production.

The screenshot shows the vCenter Account Cloud Zone interface. On the left is a navigation menu with 'Administration' and 'Configure' sections. The 'Configure' section is expanded, showing 'Cloud Zones' as the selected option. The main panel is titled 'vCenter Account Cloud Zone' with a 'DELETE' button. Below the title are tabs for 'Summary', 'Compute', and 'Projects'. The 'Compute' tab is active, displaying a message: 'All compute resources listed apply to this cloud zone. Use the filter to add or remove resources from the list.' Below this is a filter dropdown set to 'Include all compute'. A table lists the compute resources:

Name	Account / Region	Type	Tags
10.176.152.27	vCenter Account / wld01-DC	Host	
wld01-clu01	vCenter Account / wld01-DC	Supervisor Cluster	
wld01-clu01 / Development	vCenter Account / wld01-DC	Resource Pool	env:dev
wld01-clu01 / Production	vCenter Account / wld01-DC	Resource Pool	env:prod
wld01-clu01 / Training-Org	vCenter Account / wld01-DC	Resource Pool	
wld01-clu01 / VCF-edge_edge-wldclu-01_ResourcePool_ffa14b18-82b5-4261-b546-aef86a1db2d9	vCenter Account / wld01-DC	Resource Pool	

3 Voeg beperkingstags toe aan de cloudsjabloon.

Beperkingstags worden gebruikt om te beperken waar de sjabloon wordt geïmplementeerd.

- Selecteer **Ontwerp > Cloudsjablonen** en open vervolgens uw sjabloon.

In deze tutorial is de sjabloonnaam 'Development Template'.

- Controleer de YAML voor de sjabloon in het deelvenster Code.

Deze YAML is het beginpunt voor deze tutorial.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: medium
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 5
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
```

- Voeg de beperkingstag toe aan de resource `Cloud_vSphere_Machine_1` met `${input.placement}` als variabele.

```
resources:
  Cloud_vSphere_Machine_1:
```

```

type: Cloud.vSphere.Machine
properties:
  image: centos
  flavor: medium
  constraints:
    - tag: '${input.placement}'
networks:
  - network: '${resource.Cloud_NSX_Network_1.id}'
attachedDisks:
  - source: '${resource.Cloud_vSphere_Disk_1.id}'

```

- d Definieer de plaatsingsvariabele in de sectie Invoer.

```

inputs:
  placement:
    type: string
    enum:
      - env:dev
      - env:prod
    default: env:dev
    title: Select Placement for Deployment
    description: Target Environment

```

- e Controleer of de laatste YAML eruitziet als in het volgende voorbeeld.

```

formatVersion: 1
inputs:
  placement:
    type: string
    enum:
      - 'env:dev'
      - 'env:prod'
    default: 'env:dev'
    title: Select Placement for Deployment
    description: Target Environment
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
      constraints:
        - tag: '${input.placement}'
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 5

```

```
Cloud_NSX_Network_1:
  type: Cloud.NSX.Network
  properties:
    networkType: existing
```

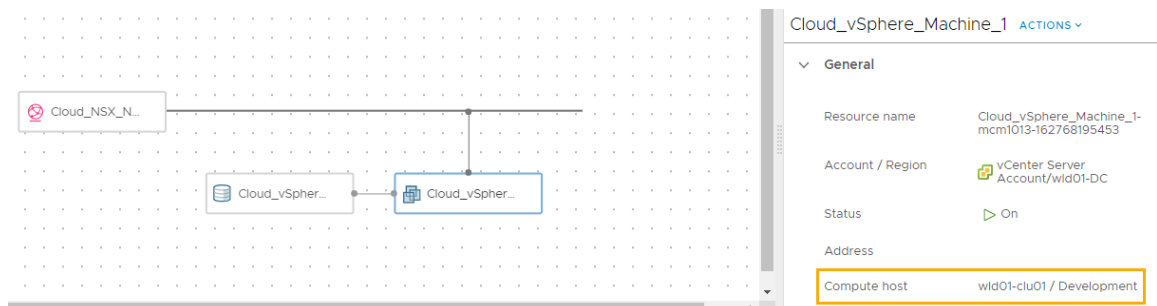
- f Om de tagvariabele uit te proberen met de beschikbare resources, klikt u op **Test** en selecteert u vervolgens **env:dev**.



Herhaal de test met **env:prod**. Wanneer beide tests zijn gelukt, bevestigt u of de sjabloon werkt door deze te implementeren.

- 4 Implementeer de sjabloon om de verdeling van workloads te testen.
 - a Klik in de cloudsjabloonontwerper op **Implementeren**.
 - b Voer **Deployment Tag Dev** in als **Implementatienaam** en klik op **Volgende**.
 - c Selecteer **env:dev** in het vervolgkeuzemenu **Select Placement for Deployment** en klik op **Implementeren**.
- 5 Controleer of de sjabloon de resources in de geselecteerde resourcepool heeft geïmplementeerd.
 - a Selecteer **Resources > Implementaties** en zoek de implementatie Deployment Tag Dev.
 - b Open de implementatiedetails en klik op **Topologie**.
 - c Klik op de vSphere-machine en vouw de machinegegevens in het rechterdeelvenster uit.
 - d Zoek in de sectie **Algemeen** naar **Berekeningshost** en controleer of de waarde overeenkomt met de resourcepool die overeenkomt met uw tag env:dev.

In dit voorbeeld is de waarde `wid01-clu01 / Development`, die laat zien dat de workload is geïmplementeerd om de resourcepool te corrigeren op basis van de geselecteerde beperkingstag.



- e Herhaal het implementatieproces en selecteer dit keer **env:prod**.

Tags toevoegen als labels die u kunt gebruiken in vCenter Server en NSX-T

U kunt tags toevoegen aan implementaties die u vervolgens kunt gebruiken om resources te beheren.

In dit voorbeeld voegt u tags toe om de MySQL-machine en het netwerk te identificeren.

U voegt ook een tag toe om het webnetwerk te identificeren. Vanwege de manier waarop tags op bestaande netwerken werken in vergelijking met netwerken op aanvraag, hebt u twee mogelijkheden.

- Als u het bestaande netwerkprofiel gebruikt dat u in de vorige sectie hebt gebruikt, wordt de tag NGINX:web niet toegevoegd aan bestaande objecten in NSX-T. U kunt de verificatiestappen met betrekking tot deze tag in NSX-T negeren.
- Als u een netwerkprofiel op aanvraag maakt, kunt u het netwerk in de YAML bijwerken om het gerouteerde netwerk of netwerk op aanvraag te gebruiken. In dit voorbeeld wordt het netwerk op aanvraag gebruikt, zodat we de tag NGINX:web kunnen demonstreren op het nieuwe object in NSX-T.

De volgende YAML komt uit het vorige voorbeeld, met uitzondering dat deze een gerouteerd netwerktype op aanvraag gebruikt. Deze bevat de beperkingstags.

Deze tutorial gebruikt de volgende voorbeeldwaarden. Houd er rekening mee dat deze waarden alleen voorbeelden zijn. Uw waarden zijn specifiek voor uw omgeving.

```
formatVersion: 1
inputs:
  placement:
    type: string
    enum:
      - 'env:dev'
      - 'env:prod'
    default: 'env:dev'
    title: Select Placement for Deployment
    description: Target Environment
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
      constraints:
        - tag: '${input.placement}'
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
```



```

    capacityGb: 5
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: routed
    constraints:
      - tag: 'net:od'

```

- 1 Selecteer **Ontwerp > Cloudsjablonen** en open vervolgens uw sjabloon.
- 2 Voeg de volgende tag toe in de eigenschappen Cloud_vSphere_Machine_.

```

tags:
  - key: db
    value: mysql

```

- 3 Voeg VM NIC-tags toe.

```

tags:
  - key: db
    value: mysql

```

- 4 Voeg logische NSX-schakeloptie/segmenttags toe.

```

tags:
  - key: NGINX
    value: web

```

- 5 Controleer of de YAML eruitziet als in het volgende voorbeeld.

```

formatVersion: 1
inputs:
  placement:
    type: string
    enum:
      - 'env:dev'
      - 'env:prod'
    default: 'env:dev'
    title: Select Placement for Deployment
    description: Target Environment
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
    constraints:
      - tag: '${input.placement}'

```

```

tags:
  - key: db
    value: mysql
networks:
  - network: '${resource.Cloud_NSX_Network_1.id}'
    tags:
      - key: db
        value: mysql
attachedDisks:
  - source: '${resource.Cloud_vSphere_Disk_1.id}'
Cloud_vSphere_Disk_1:
  type: Cloud.vSphere.Disk
  properties:
    capacityGb: 5
Cloud_NSX_Network_1:
  type: Cloud.NSX.Network
  properties:
    networkType: routed
  constraints:
    - tag: 'net:od'
  tags:
    - key: NGINX
      value: web

```

6 Implementeer de sjabloon.

In dit voorbeeld wordt de naam **Development template w tags** gebruikt.

7 Om de tags in de implementatie te controleren, opent u de implementatie en klikt u op het tabblad **Topologie**.

- a Klik op de machine in de topologie.
- b Vouw de sectie **Algemeen** uit voor de machine en zoek naar het label Tags.

De tagwaarde is `db:mysql`.

- c Vouw de sectie **Netwerk** uit en zoek naar de kolom Tags voor het netwerk.

De tagwaarde is `db:mysql`.

Development template w tags Create Successful ACTIONS | [C](#)

No description

Owner: fritz
Requestor: fritz
Project: Development Project
Cloud Template: Development Template [↓](#)

Expires on: Never
Last updated: Mar 8, 2021, 4:31:01 PM
Created on: Mar 8, 2021, 4:09:14 PM

[HIDE SUMMARY](#)

Topology History

Search resources

Cloud_NSX_N...

Cloud_vSphere...

Cloud_vSphere...

Cloud_vSphere_Machine_1 ACTIONS

General

Resource name: Cloud_vSphere_Machine_1-mcm1019-163638575175
Account / Region: vCenter Server Account/wld01-DC
Status: On
Address:
Compute host: wld01-clu01 / Development
Tags: db.mysql

Storage

Network

Index	Name	Address	Assignment Type	Security Groups	Tags
0	DevProject-004		dynamic		db.mysql

Custom properties

- d Klik op het netwerk in de topologie en vouw de sectie **Algemeen** uit om het label Tag te zoeken.

De tagwaarde is NGINX:web.

Topology History

Search resources

Cloud_NSX_N...

Cloud_vSphere...

Cloud_vSphere...

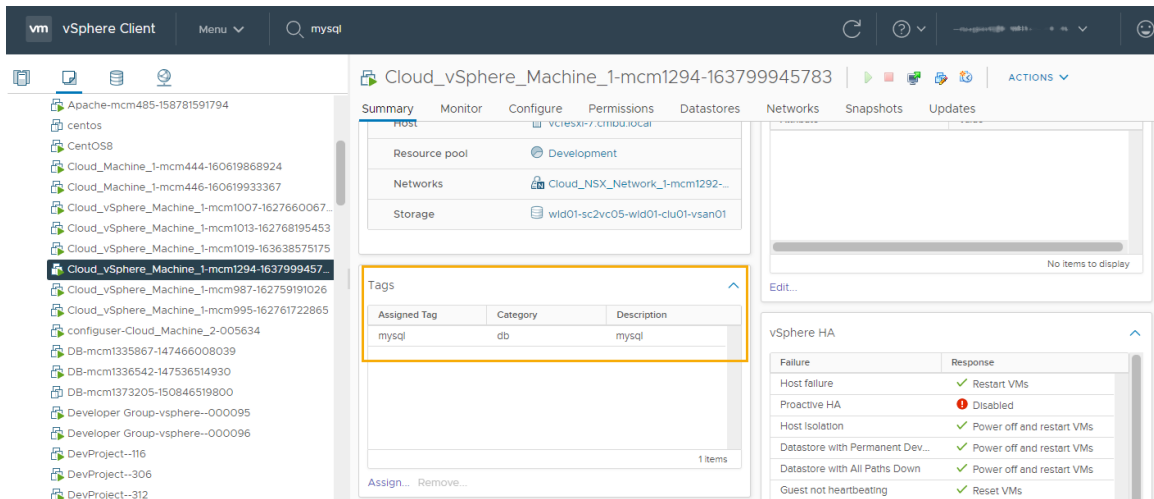
Cloud_NSX_Network_1 ACTIONS

General

Resource name: Cloud_NSX_Network_1-mcm1292-163799928607
Account: NSX-T Account
Network type: routed
CIDR: 192.168.150.0/28
Tags: nginx:web

Custom properties

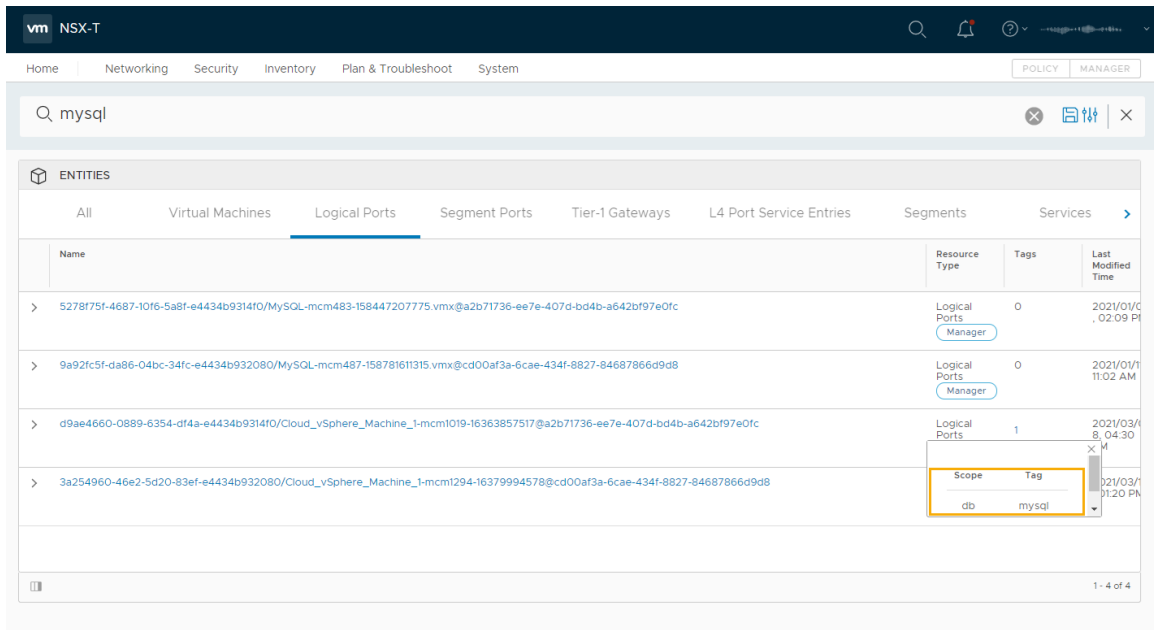
- 8 Als u de tags in vCenter Server wilt verifiëren, meldt u zich aan bij de vCenter Server-instantie waar deze workload is geïmplementeerd.
- a Zoek de virtuele machine en zoek naar het deelvenster Tags.



9 Om de tags in NSX-T te verifiëren, meldt u zich aan bij de NSX-T-instantie waar dit netwerk is geconfigureerd.

- Klik op **Beleid** in de rechterbovenhoek.
- Als u de `db:mysql`-tag wilt vinden die is gekoppeld aan de NIC, zoekt u naar **mysql**.
- Klik op **Logische poorten** en zoek de geïmplementeerde vSphere-machine.
- Klik op het getal in de kolom Tags.

Het bereik en de tag zijn respectievelijk `db` en `mysql`.

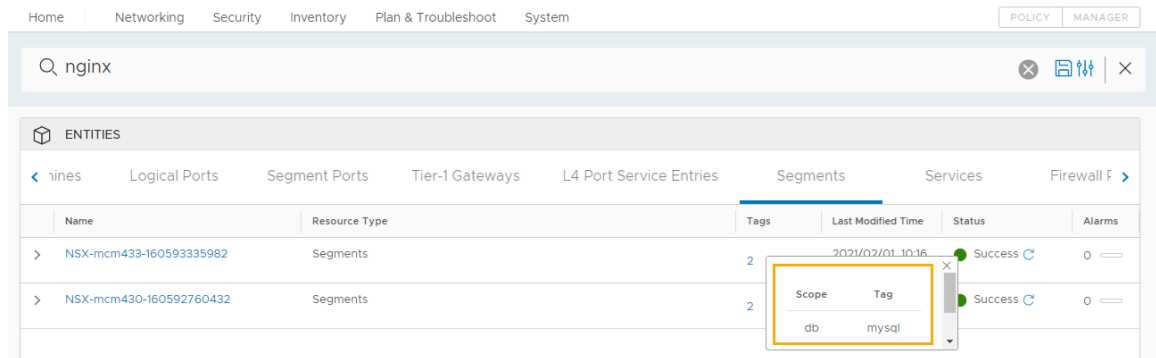


- Als u de `NGINX:web`-tag wilt vinden die aan het segment is gekoppeld, zoekt u naar het netwerk.

In dit voorbeeld is de netwerkn naam **Cloud_NSX_Network_1-mcm1292-163799928607**.

- Zoek de rij Segmenten en klik op het getal in de kolom Tags.

Het bereik en de tag zijn respectievelijk NGINX en web.



Tutorial: Een Cloud Assembly-cloudsjabloon aan de Service Broker-catalogus toevoegen met een aangepast aanvraagformulier

Tijdens de itererende ontwikkeling van uw cloudsjablonen of wanneer u een definitieve sjabloon hebt, kunt u de sjablonen beschikbaar maken voor gebruikers in de Service Broker-selfservicecatalogus. Om de gebruikerservaring verder te verbeteren, kunt u een aangepast aanvraagformulier maken. Het aangepaste formulier is krachtiger dan de eenvoudige opties voor sjablooninvoer.

Wat moet u eerst doen

- Controleer of u over de infrastructuur voor de sjabloon beschikt. Als dat niet zo is, begint u met [Tutorial: vSphere-infrastructuur en -implementaties in Cloud Assembly instellen en testen](#) en kunt u verder met de andere tutorials.
- Controleer of u bepaalde resourcepools hebt getagd als `env:dev` en `env:prod`. Zie [Tutorials: tags in Cloud Assembly gebruiken om vSphere-resources te beheren](#) voor meer informatie.
- Zorg ervoor dat u een implementeerbare cloudsjabloon hebt, vergelijkbaar met onderstaande sjabloon. Deze tutorial begint met de volgende sjabloon.

```
formatVersion: 1
inputs:
  installedOS:
    type: string
    title: Operating System
    description: Select the operating system.
    enum:
      - centos
      - ubuntu
  placement:
    type: string
    enum:
      - 'env:dev'
      - 'env:prod'
```

```

default: 'env:dev'
title: Select Placement for Deployment
description: Target Environment
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: '${input.installedOS}'
      installedOS: '${input.installedOS}'
      flavor: small
      constraints:
        - tag: '${input.placement}'
      tags:
        - key: db
          value: mysql
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
          tags:
            - key: db
              value: mysql
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
      tags:
        - key: NGINX
          value: web

```

Stap 1: Invoer toevoegen aan de cloudsjabloon

Deze procedure werkt de plaatsingsinvoer bij, naast de invoer voor het bestaande type besturingssysteem, en voegt een invoer voor grootte toe. Wanneer u het aanvraagformulier in Service Broker aanpast, zijn dit de drie velden in het aanvraagformulier die worden aangepast.

- 1 Selecteer **Ontwerp > Cloudsjabloon** in Cloud Assembly en maak of open de bovenstaande sjabloon.

De voorbeeldsjabloon wordt gebruikt om de verschillende opties uit te leggen en bevat voorbeeldwaarden. Pas deze aan uw omgeving aan.

- 2 Voeg de groottevariabele toe en definieer de grootten in de sectie Invoer.
 - a Voeg in de sectie Cloud_vSphere_Machine_1 een variabele toe aan de eigenschap `flavor`.

```
flavor: '${input.size}'
```

- b Voeg in de sectie Invoer een naamgrootte voor de gebruikersinvoer toe zodat de gebruiker de grootte van de implementatie kan selecteren. Hier wordt soms naar verwezen als de T-shirtmaat die u hebt gedefinieerd voor de cloudzones.

```
size:
  type: string
  title: Deployment size
  description: Select the the deployment t-shirt size.
  enum:
    - small
    - medium
    - large
```

- 3 Werk de invoer voor plaatsing met een beschrijvende term bij, en niet de tagtekenreeks.

Deze beperkingstags worden afgestemd op de capaciteitstags die u in [Tutorials: tags in Cloud Assembly gebruiken om vSphere-resources te beheren](#) hebt toegevoegd.

- a Voeg in de sectie Invoer een gebruikersinvoer toe met de naam **plaatsing** zodat de gebruiker ontwikkeling of productie kan selecteren als plaatsing van de implementatie.

In dit voorbeeld wordt het kenmerk `oneOf` gebruikt, waarmee u een label in een natuurlijke taal kunt presenteren en tegelijkertijd tekenreeksen kunt indienen die het implementatieproces vereist. Bijvoorbeeld: de tags `env:dev` en `env:prod`.

```
placement:
  type: string
  oneOf:
    - title: Development
      const: 'env:dev'
    - title: Production
      const: 'env:prod'
  default: 'env:dev'
  title: Select Deployment Placement
  description: Target Environment
```

- 4 Controleer de volledige YAML om er zeker van te zijn dat deze eruitziet als in het volgende voorbeeld.

```
formatVersion: 1
inputs:
  installedOS:
    type: string
    title: Operating system
    description: Select the operating system.
    enum:
      - centos
      - ubuntu
  placement:
    type: string
    oneOf:
```

```

- title: Development
  const: 'env:dev'
- title: Production
  const: 'env:prod'
default: 'env:dev'
title: Select Deployment Placement
description: Target Environment
size:
  type: string
  title: Deployment size
  description: Select the the deployment t-shirt size.
  enum:
    - small
    - medium
    - large
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: '${input.installedOS}'
      installedOS: '${input.installedOS}'
      flavor: '${input.size}'
    constraints:
      - tag: '${input.placement}'
    tags:
      - key: db
        value: mysql
    networks:
      - network: '${resource.Cloud_NSX_Network_1.id}'
        tags:
          - key: db
            value: mysql
    attachedDisks:
      - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
    tags:
      - key: NGINX
        value: web

```

- 5 Klik op **Implementeren**. Controleer of de tweede pagina van de aanvraag er als volgt uitziet. Vervolgens kunt u na de implementatie controleren of de implementatie zich in de geselecteerde ontwikkeling met resourcepool voor productie bevindt.

The screenshot shows a configuration window titled 'Deploy Development Te...'. On the left is a sidebar with two items: '1 Deployment Type' and '2 Deployment Inputs', with the second item selected. The main area is titled 'Deployment Inputs' and contains three dropdown menus, each with an information icon (i) to its right:

- Operating system ***: Set to 'centos'.
- Select Deployment Placement**: Set to 'Development'.
- Deployment size ***: A dropdown menu is open, showing three options: 'small' (highlighted in blue), 'medium', and 'large'.

At the bottom right of the window are three buttons: 'CANCEL' (light blue), 'PREVIOUS' (light blue), and 'DEPLOY' (green).

Stap 2: Versie en release van de cloudsjabloon maken

Wanneer u een implementeerbare sjabloon hebt, kunt u deze nu beschikbaar maken in de Service Broker-catalogus voor andere toepassingen. Als u de cloudsjabloon vindbaar wilt maken zodat u deze aan de catalogus kunt toevoegen, moet u deze vrijgeven. In deze procedure wordt een versie gemaakt van de sjabloon, om een momentopname van de sjabloon vast te leggen, en vervolgens wordt de sjabloon vrijgegeven.

- 1 Selecteer **Ontwerp > Cloudsjabloon** en open de sjabloon in het ontwerpcanvas.
- 2 Klik op **Versie** en voer een beschrijving in.

The screenshot shows a 'Creating Version' dialog box with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Version ***: A text input field containing the number '7'. Below it, it says 'Last Version: 6'.
- Description**: A text area containing the text 'Placement inputs added and tested.' with a small icon in the bottom right corner.
- Change Log**: An empty text area with a small icon in the bottom right corner.
- Release**: A section with a checked checkbox and the text 'Release this version to the catalog'. Below this, a smaller note reads: 'This cloud template is restricted to this project in the catalog. Edit shareability in cloud template level settings.'

At the bottom of the dialog are two buttons: 'CANCEL' (light blue) and 'CREATE' (dark blue).

- 3 Schakel het selectievakje **Vrijgeven** in en klik op **Maken**.

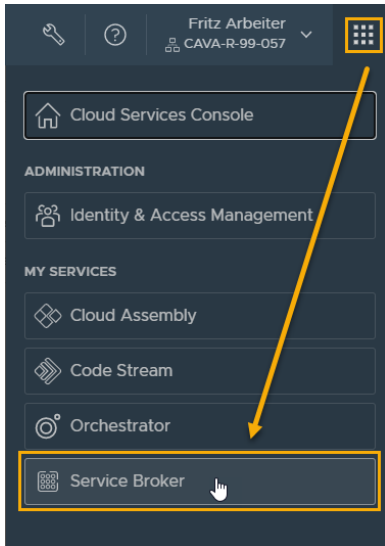
Als u de cloudsjabloon vrijgeeft, wordt deze niet automatisch aan de Service Broker toegevoegd. Als u de sjabloon vrijgeeft, is deze detecteerbaar, zodat u deze aan de catalogus kunt toevoegen.

Stap 3: De cloudsjabloon toevoegen aan de Service Broker-catalogus

U kunt de Service Broker-catalogus gebruiken om cloudsjablonen te bieden aan andere gebruikers in uw organisatie waar ze niet hoeven te weten hoe ze een sjabloon moeten maken. In de catalogus kunnen zij de sjabloon implementeren.

Voordat u de sjabloon als catalogusitem kunt toevoegen, moet u deze in Service Broker importeren. U kunt alleen vrijgegeven cloudsjablonen importeren.

- 1 Als u Service Broker vanuit Cloud Assembly wilt openen, klikt u op het applicatiemenu in de rechterbovenhoek.



- 2 Klik op **Service Broker**.
- 3 Importeer de cloudsjabloon.
 - a Selecteer **Inhoud en beleidsregels > Inhoudsbronnen** in Service Broker.
 - b Klik op **Nieuw** en selecteer vervolgens **VMware Cloud Templates**.
 - c Voer een **naam** in.
Voer in deze tutorial **Cloud Assembly DevProject** in.
 - d Voor het **project** selecteert u het **Development Project** dat u in Cloud Assembly hebt gemaakt.
 - e Klik op **Valideren**.
Het systeem moet aangeven dat het ten minste één item heeft gevonden.
 - f Wanneer dit is gevalideerd, klikt u op **Maken en importeren**.
Cloud Assembly DevProject wordt als inhoudsbron aan de lijst toegevoegd.
- 4 Maak de cloudsjabloon beschikbaar in de catalogus.
 - a Selecteer **Inhoud en beleidsregels > Inhoud delen**.
 - b Selecteer **Development Project** in de vervolgkeuzelijst **Project**.

- c Klik op **Items toevoegen** en selecteer vervolgens
 - d Selecteer **Cloud Assembly DevProject** in het dialoogvenster **Items delen** en klik op **Opslaan**.
- 5 Om te controleren of de ontwikkelingssjabloon aan de catalogus is toegevoegd, klikt u op **Catalogus**.
 - 6 Klik op **Aanvraag** op de kaart Development Template.

De invoer die u op de cloudsjabloon hebt gezien, moet ook hier te zien zijn. De volgende stap is het aanpassen van het aanvraagformulier.

The screenshot shows a 'New Request' form for the 'Development Template' (Version 8). The form contains the following fields:

- Project ***: A dropdown menu with 'Development Project' selected.
- Deployment Name ***: A text input field.
- Operating system ***: A dropdown menu with an information icon (i) to its right.
- Select Deployment Placement**: A dropdown menu with 'Development' selected and an information icon (i) to its right.
- Deployment size ***: A dropdown menu with an information icon (i) to its right.

Stap 4: Een aangepast formulier voor de sjabloon maken

Het doel voor dit aangepaste formulier is om een formulier te bieden waarin de gebruiker het besturingssysteem en de plaatsing selecteert op basis van de tags env:dev of env:prod. Vervolgens kan de gebruiker met de optie env:dev small of medium selecteren, large is geen optie. Als de gebruiker echter env:prod selecteert, is er geen optie om large te selecteren, de grootte is verborgen voor de gebruiker, maar wordt opgenomen in de aanvraag.

- 1 Als u een aangepast formulier wilt maken in Service Broker, selecteert u **Inhoud en beleidsregels > Inhoud**.
- 2 Klik op de verticale drie puntjes links van de vermelding Development Template en klik op **Formulier aanpassen**.
- 3 Pas de invoeroptie aan.
 - a Klik op velden in het canvas en configureer de eigenschappen zoals opgegeven in de volgende tabel.

Naam van canvasveld	Vormgeving	Waarden	Beperkingen
Besturingssysteem	Label en type <ul style="list-style-type: none"> Label = Besturingssysteem 	Waardeopties <ul style="list-style-type: none"> Waardeopties = Constante Waardebron = centos CentOS, ubuntu Ubuntu In dit voorbeeld worden de waardeopties gebruikt voor het vervangen van alle namen van besturingssystemen met kleine letters door de voorkeursnaam van het besturingssysteem.	
Implementatieplaatsing selecteren		Waardeopties <ul style="list-style-type: none"> Waardeopties = Constante Waardebron = env:dev Development, env:prod Production 	
Implementatiegrootte	Zichtbaarheid <ul style="list-style-type: none"> Waardebron = Voorwaardelijke waarde Stel waarde in op Ja als Implementatieplaatsing selecteren gelijk is aan env:dev 	Standaardwaarde <ul style="list-style-type: none"> Waardebron = Voorwaardelijke waarde Stel waarde in op large als Implementatie selecteren gelijk is aan env:prod Waardeopties <ul style="list-style-type: none"> Waardeopties = Constante Waardebron = small Small, medium Medium Merk op dat de waardebron large niet bevat. Large is uitgesloten omdat deze alleen beschikbaar is voor Productie en de vereiste waarde is. De grote waarde wordt opgenomen in de	

Naam van canvasveld	Vormgeving	Waarden	Beperkingen
		implementatieaanvraag zonder een door de gebruiker geïnitieerde actie.	

- b Als u het formulier in de catalogus wilt inschakelen, klikt u op **Inschakelen**.
 - c Klik op **Opslaan**.
- 4 Test het formulier in de catalogus om de juiste resultaten te garanderen door ten minste een aanvraag Development Small en Production in te dienen.

Gebruik de volgende voorbeelden om de resultaten te controleren.

- a Test het aanvraagformulier Development Small door een naam op te geven, Test small in dit voorbeeld, en CentOS, Development en Small te selecteren voor de opties.

New Request

Development Template Version 8

Project * Development Project

Deployment Name * Test small

Operating system * CentOS

Select Deployment Placement * Development

Deployment size * Small

- b Als u de implementatie Development Small wilt controleren, selecteert u **Resources > Implementaties** en klikt u op de implementatie Test small.
- c Klik op het tabblad Topologie op Cloud_vSphere_Machine en zoek vervolgens in het rechterdeelvenster naar de sectie Aangepaste eigenschappen.

Enkele waarden die moeten worden gecontroleerd zijn cpuCount = 2 en flavor = small.

Test small Create Successful ACTIONS ▾ | ↻

No description

Owner	fritz	Expires on	Never
Requestor	fritz	Last updated	May 21, 2021, 5:14:56 PM
Project	Development Project	Created on	May 21, 2021, 4:52:38 PM
Cloud Template	Development Template, version: 6		

↓

HIDE SUMMARY ⤴

Topology History

Search resources

Properties:

costCenter	DevProject
cpuCount	2
datastoreName	wid01-sc2vc05-wid01-clu
endpointId	d827e01c-df9e-4c80-9f1d
flavor	small
image	centos

- d Test het aanvraagformulier Production door een naam in te voeren, **Test large** in dit voorbeeld, en selecteer CentOS en Production voor de opties.

Onthoud dat u het formulier zo hebt geconfigureerd dat de grootte niet wordt weergegeven noch door de gebruiker moet worden geselecteerd.

New Request

Development Template Version **3** ▾

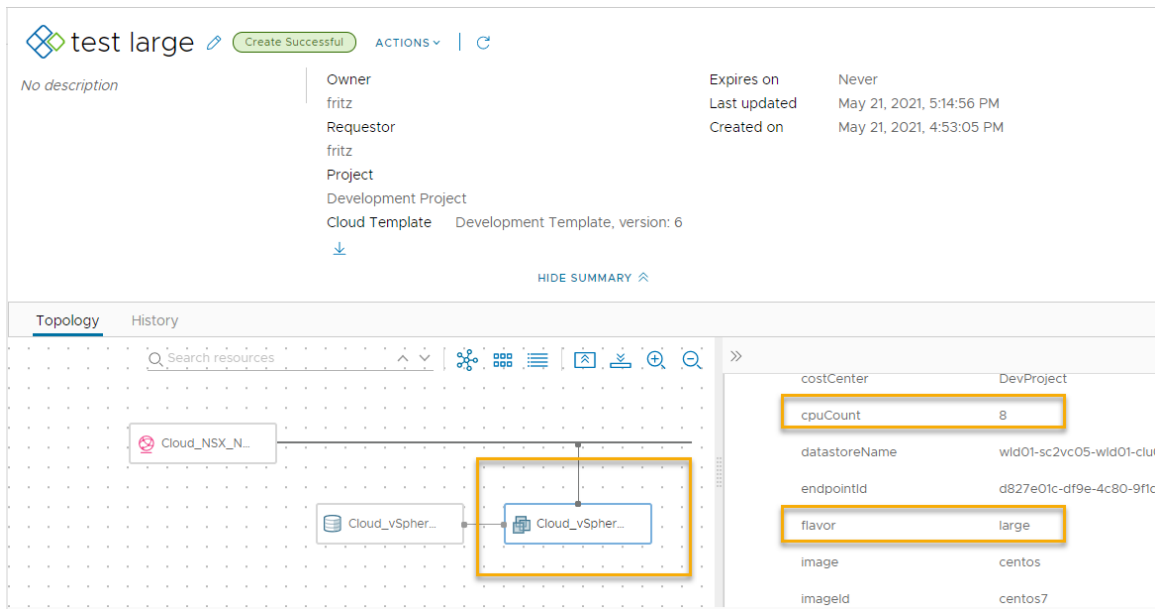
Project * Development Project ▾

Deployment Name * Test large

Operating System * CentOS ▾ ⓘ

Select Deployment Placement Production ▾ ⓘ

- e Om de implementatie Production te controleren, selecteert u **Resources > Implementaties** en klikt u op de implementatie Test large.
- f Klik op het tabblad Topologie op Cloud_vSphere_Machine en zoek vervolgens in het rechterdeelvenster naar de sectie Aangepaste eigenschappen.
- Enkele waarden die moeten worden gecontroleerd zijn cpuCount = 8 en flavor = large.



Stap 5: de cloudsjabloonversies in de catalogus beheren

In de meeste gevallen wilt u alleen de nieuwste cloudsjablonen beschikbaar maken in de Service Broker-catalogus. De volgende procedure ondersteunt iteratieve ontwikkeling, waarbij u een versie van een sjabloon vrijgeeft en deze aan de catalogus toevoegt, maar u hebt de sjabloon verbeterd en wilt de huidige versie vervangen door de nieuwere versie.

In stap 2 hebt u versies gemaakt en vrijgegeven voor een sjabloon. U bent dus vertrouwd met het proces. In stap 3 hebt u deze aan de catalogus toegevoegd. De procedure koppelt de twee stappen aan elkaar terwijl u iteratieve ontwikkeling uitvoert en de catalogus bijwerkt met de nieuwste versie.

U hebt de optie om meerdere versies beschikbaar te maken in de catalogus.

- 1 Maak in Cloud Assembly een versie van de sjabloon die u beschikbaar wilt maken in de catalogus.

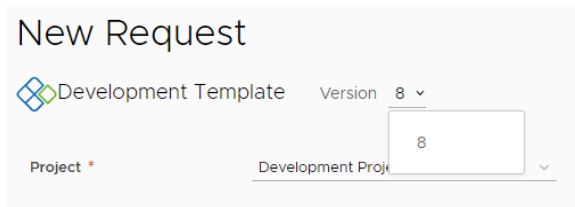
- a Selecteer **Ontwerp > Cloudsjabloon** en open de sjabloon in het ontwerpcanvas.
- b Klik op **Versiegeschiedenis**.
- c Zoek de versie die u aan de catalogus wilt toevoegen en klik op **Versie**.
- d Voer een **beschrijving** in, schakel het selectievakje **Vrijgeven** in en klik op **Maken**.

Op dit moment hebt u de optie om de oude versie in de catalogus te behouden. Als u meerdere versies wilt, negeert u de volgende stap waar u de vrijgave van een versie ongedaan wilt maken.

- e Als u slechts één versie van de sjabloon beschikbaar wilt maken in de catalogus, bekijkt u de lijst met de versiegeschiedenis en klikt u op **Vrijgave ongedaan maken** voor elke versie die u niet in de catalogus wilt hebben.

- 2 Als u de Service Broker-catalogus wilt bijwerken met de nieuwste versie, en elke oude versie wilt vervangen, moet u de nieuwe versie verzamelen.
 - a Selecteer **Inhoud en beleidsregels > Inhoudsbronnen** in Service Broker.
 - b Klik op de Cloud Assembly DevProject-inhoudsbron die in deze tutorial wordt gebruikt.
 - c Klik op **Valideren**.
In een bericht wordt gemeld dat er een item is gevonden.
 - d Klik op **Opslaan en importeren**.
- 3 Controleer of de vereiste versies of geen versies worden weergegeven in de catalogus.
 - a Klik in Service Broker op **Catalogus**.
 - b Zoek het catalogusitem en klik op **Aanvragen**.
 - c Klik bovenaan het aanvraagformulier op de **versie** en bekijk de versie of versies.

De volgende schermafbeelding toont 8.



Tutorial: onboarding en beheer van vSphere-resources in vRealize Automation

Als cloudbeheerder hebt u onlangs een nieuwe cloudaccount toegevoegd en wilt u nu een deel van de vCenter Server-workload beheren met behulp van Cloud Assembly en Service Broker. Deze tutorial begeleidt u door het onboardingsproces en laat zien hoe u een aantal beheeropties instelt voor uw bestaande vSphere-workloads.

Als voorbeeld worden beheertaken genomen zoals het toevoegen van resources aan een project, het maken en toepassen van een goedkeuringsbeleid in Service Broker en het uitvoeren van enkele resource-acties voor dag 2 die laten zien hoe u de tools voor levenscyclusbeheer gebruikt en het goedkeuringsbeleid activeert.

Hoewel u mogelijk relatief onbekend bent met Cloud Assembly, gaat deze tutorial ervan uit dat u uw nieuwe vSphere-cloudaccount hebt geconfigureerd. Wanneer u de cloudaccount toevoegt, detecteert Cloud Assembly de momenteel onbeheerde resources op uw vSphere-instantie.

Wat moet u eerst doen

- Voeg uw nieuwe vCenter Server-account toe. Zie [Een vCenter-cloudaccount maken in vRealize Automation](#) voor meer instructies.

- Controleer of uw gebruikersaccount ten minste beschikt over de rollen van Cloud Assembly-beheerder en Service Broker-beheerder. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Om het goedkeuringsbeleid goed te kunnen testen vanuit het perspectief van een van uw gebruikers, dient u een gebruikersaccount te hebben met alleen de volgende gebruikersrollen. De gebruiker in deze tutorial heet Sylvia.
 - Lid van de organisatie
 - Cloud Assembly-gebruiker
 - Service Broker-gebruiker

Zie [Wat zijn de vRealize Automation-gebruikersrollen](#) voor meer informatie over gebruikersrollen.

Stap 1: controleren of Cloud Assembly de resources heeft gedetecteerd

Wanneer u een vCenter Server-account toevoegt, detecteert Cloud Assembly de resources op de vCenter Server-instantie. U kunt controleren of de machines die u wilt beheren, beschikbaar zijn voor onboarding.

- 1 Selecteer **Resources > Resources > Virtuele machines** in Cloud Assembly.
- 2 Controleer de **Afkomst** en **Account/regio** in het raster.

Het afkomsttype Gedetecteerd geeft aan dat de machine is gedetecteerd op uw vSphere-instantie en nog niet is geonboard of geïmplementeerd door vRealize Automation.

In dit voorbeeld is de account/regio vCenter Account / wld01-DC.

Name	Status	Account / Region	Address	Project	Owner	Creation Time	Origin	Tags
DevProject-116	▶ On	vCenter Account / wld01-DC	N/A			Jul 26, 2021, 2:29:15 PM	Discover d	
DevProject-centos-010	▶ On	vCenter Account / wld01-DC	N/A	Onboarding Project	fritz	Jul 26, 2021, 2:29:18 PM	Deployed	db:mysql
DevProject-centos-012	▶ On	vCenter Account / wld01-DC	N/A			Jul 26, 2021, 2:29:18 PM	Discover d	
DevProject-centos-013	▶ On	vCenter Account / wld01-DC	N/A			Jul 26, 2021, 2:29:15 PM	Discover d	db:mysql
DevProject-centos-016	▶ On	vCenter Account / wld01-DC	N/A	Onboarding Project	sylvia	Jul 26, 2021, 2:29:15 PM	Deployed	db:mysql

Stap 2: een doelproject maken

Maak een project waaraan u de geonboarde machines kunt toewijzen. Om de resources te beheren, moeten ze deel uitmaken van een project dat de broncloudzone bevat waarop ze oorspronkelijk zijn geïmplementeerd.

Als u deze tutorial wilt testen, moet u een andere gebruiker hebben die geen beheerder is. In deze stap voegt u als beheerder het projectlid genaamd Sylvia toe.

Zie [Hoofdstuk 5 Cloud Assembly-projecten toevoegen en beheren](#) voor meer informatie over projecten.

1 Selecteer **Infrastructuur > Projecten >** in Cloud Assembly.

2 Klik in de pagina Projecten op **Nieuw project**.

3 Voer de **naam** van het project in.

In deze tutorial wordt de projectnaam **Onboarding Project** gebruikt.

4 Klik op het tabblad **Gebruikers**.

a Klik op **Gebruikers toevoegen** en voeg ten minste één gebruiker als projectlid toe.

In deze tutorial voegt u Sylvia toe.

b Klik op **Toevoegen**.

5 Klik op **Inrichting**.

a Klik op **Zone toevoegen**.

b Klik op **Cloudzone**.

c Selecteer de account/regio die u in stap 1 hebt opgegeven.

In deze tutorial wordt de waarde vCenter Account / wld01-DC als voorbeeld gebruikt.

New Project

Summary Users **Provisioning** Kubernetes Provisioning

Zones

Specify the zones that can be used when users provision deployments in this project. ⓘ

+ ADD ZONE × REMOVE

<input type="checkbox"/>	Name	Status	Description	Priority	Instances	Memory Limit (MB)	CPU Limit	Storage Limit (GB)	Capability Tags
<input type="checkbox"/>	vCenter Account / wld01-DC	--		0	Unlimited	Unlimited	Unlimited	Unlimited	

1 - 1 of 1 zones

Specify the placement policy that will be applied when selecting a cloud zone for provisioning.

Placement policy **DEFAULT** ⓘ

d Klik op **Toevoegen**.

6 Klik op **Maken**.

Stap 3: een onboardingsplan maken en uitvoeren

Als cloudbeheerder onboardt u gedetecteerde machines vanuit uw vSphere-instantie, zodat u governance kunt toepassen en de resources kunt beheren met acties voor dag 2.

Zie [Wat zijn onboardingplannen in Cloud Assembly](#) voor meer informatie over onboardingsplannen.

- 1 Selecteer in Cloud Assembly **Infrastructuur > Onboarding** en klik vervolgens op **Nieuw onboardingsplan**.
- 2 Voer de onboardingsgegevens in.

Instelling	Voorbeeldwaarde
Naam van plan	wld01-DC onboardingsplan
Cloudaccount	vCenter-account
Standaardproject	Onboardingsproject

- 3 Klik op **Maken**.
- 4 Voeg de machines toe die u wilt onboarden.

Voer het onboardingsplan pas uit nadat u alle volgende stappen hebt voltooid.

- a Klik op **Machines** en klik vervolgens op **Machines toevoegen**.
- b Selecteer de machines die u in het plan wilt opnemen en klik vervolgens op **OK**.
Voor deze tutorial zijn slechts twee machines geselecteerd.
- c Selecteer in het dialoogvenster Implementaties maken de optie **Implementatieplanning maken voor elke machine** en klik vervolgens op **Maken**.
U selecteert deze optie wanneer u de machines als afzonderlijke implementaties wilt aanmerken zodat u ze als afzonderlijke resources kunt beheren.
- d De geselecteerde machines worden toegevoegd aan de lijst.

Summary Machines Deployments							
Machines listed here are onboarded when the plan runs.							
ADD MACHINES		REMOVE		Filter...			
<input type="checkbox"/>	Name	Status	Power	Address	Deployment	Custom properties	Tags
<input type="checkbox"/>	DevProject-centos-013	Pending	On		Deployment-5e3ac...	Inherited	db:mysql
<input type="checkbox"/>	DevProject-centos-204	Pending	On		Deployment-50507...	Inherited	db:mysql

- 5 Wijzig de naam van de implementaties.
 - a Klik op **Implementaties** op de onboardingspagina.
 - b Als u de gegenereerde implementatienaam wilt wijzigen, selecteert u een implementatie en klikt u op **Naam wijzigen**.
 - c Voer de nieuwe naam in en klik vervolgens op **Opslaan**.
Bijvoorbeeld: geonboarde machine 1.
 - d Herhaal dit zo vaak als nodig.

6 Wijs een eigenaar toe aan de implementaties.

Als u geen eigenaar toewijst, wordt u de eigenaar. De eigenaar moet lid zijn van het doelproject.

Deze tutorial wijst alle implementaties toe aan dezelfde eigenaar. U kunt desgewenst verschillende implementaties toewijzen aan verschillende eigenaars.

- Selecteer alle implementaties en klik op **Eigenaar bewerken**.
- Selecteer de gewenste eigenaar en klik op **Opslaan**.

Controleer de gewijzigde implementatienamen en eigenaren in het raster.

The screenshot shows the 'wld01-DC Onboarding Plan' interface. It has tabs for 'Summary', 'Machines', and 'Deployments'. Below the tabs, a message states: 'These deployments will be created or updated when the plan runs. By default each added machine is placed in its own Cloud Assembly deployment.' There are buttons for 'RENAME', 'EDIT OWNER', 'CLOUD TEMPLATE', and 'REMOVE'. A table lists the deployments:

<input type="checkbox"/>	Deployment Name	Status	Create Cloud Template	Owner	Components
<input type="checkbox"/>	> Onboarded deployment 1	✓		sylvia	1
<input type="checkbox"/>	> Onboarded deployment 2	✓		sylvia	1

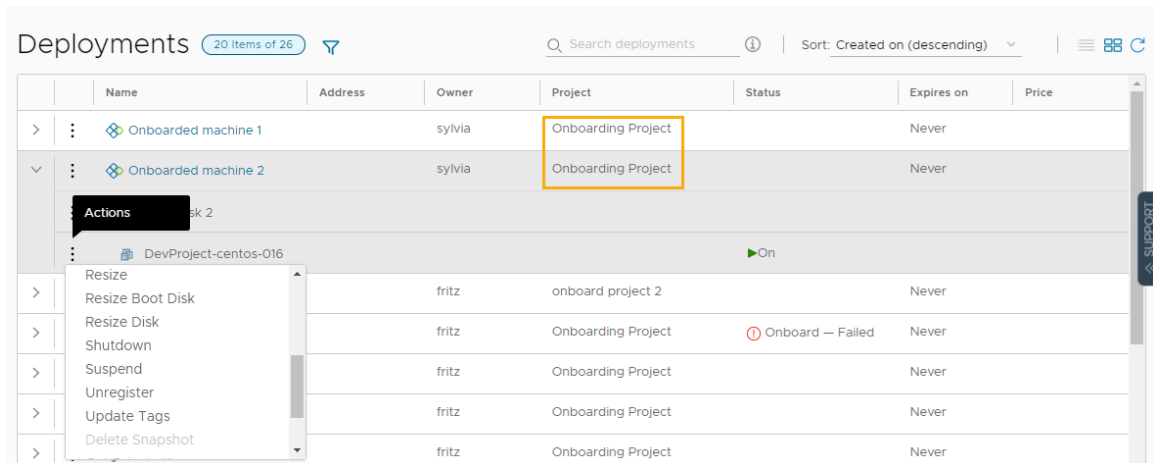
At the bottom, there are buttons for 'SAVE', 'RUN', and 'CANCEL'. A status bar at the bottom right indicates '2 deployments'.

7 Klik op **Uitvoeren**.

Nadat u het onboardingsplan hebt uitgevoerd, kunt u de naam niet meer wijzigen en geen andere eigenaren meer toewijzen. Als u meer machines aan het plan toevoegt, kunt u de naam of de eigenaar wijzigen.

8 Controleer de resources die u als implementaties hebt geonboard.

- Selecteer **Resources > Implementaties**.
- U kunt implementaties opzoeken op implementatienaam, project of eigenaar.



U hebt de machines nu naar vRealize Automation overgebracht en kunt deze vervolgens gaan beheren.

Stap 4: omvang van een implementatie aanpassen

Voer deze stap uit als cloudbeheerder en maak uzelf vertrouwd met de werking van acties voor dag 2. De wijzigingen die u in implementaties kunt aanbrengen, worden acties voor dag 2 genoemd. Het gebruik van acties voor dag 2 is de eerste stap in het beheren van uw resources.

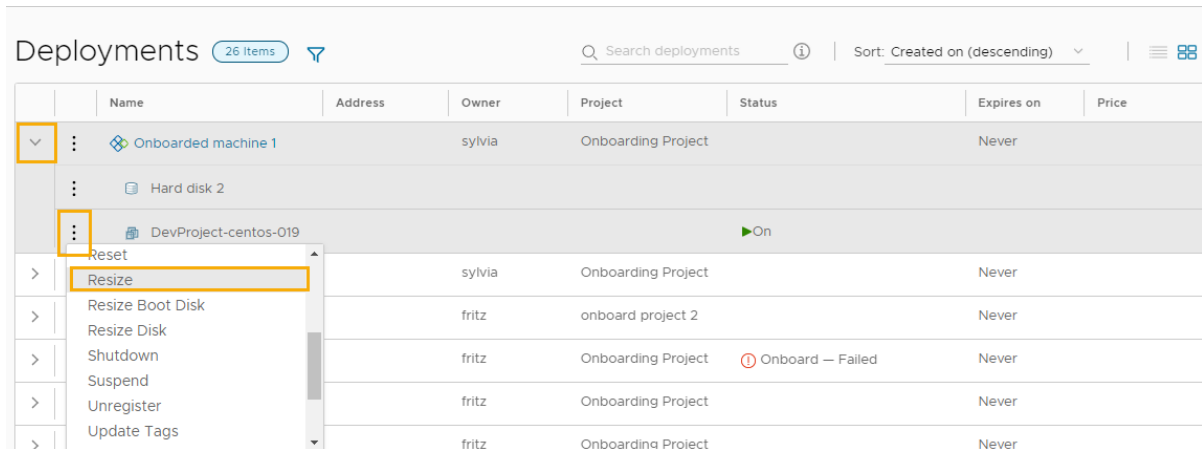
In deze tutorial gaat u het CPU-gebruik verlagen omdat u vindt dat het aantal CPU's voor een machine te hoog is. Bij deze procedure wordt ervan uitgegaan dat u de actie voor het wijzigen van de omvang uitvoert op een vSphere-machine die is ingeschakeld. Er wordt ook verondersteld dat u geen beleidsregels voor dag 2 hebt die een gebruiker verbieden deze actie uit te voeren.

De beschikbare acties zijn afhankelijk van het resourcetype, de resourcestatus en het beleid voor dag 2. Zie [Welke acties kan ik op Cloud Assembly-implementaties uitvoeren](#) voor meer informatie over acties voor dag 2.

- 1 Selecteer **Resources > Implementaties** in Cloud Assembly en zoek vervolgens uw geonboarde implementaties.

U kunt zoek- of filteropties gebruiken.

- 2 Vouw de implementatie uit met de linkerpijl, klik vervolgens op de drie verticale puntjes bij de naam van de machine en klik op **Omvang wijzigen**.

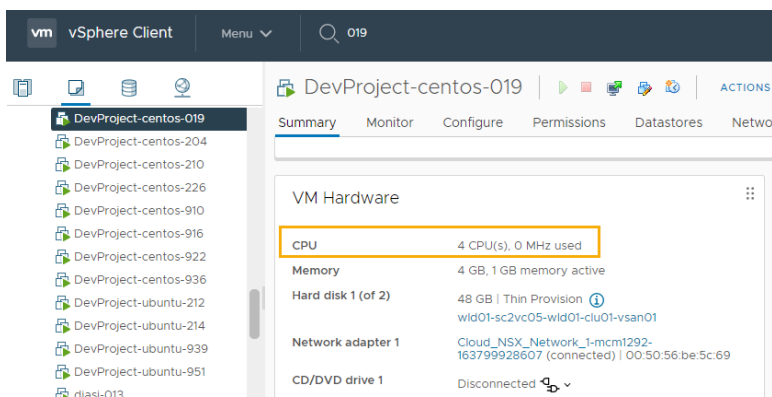


- In het dialoogvenster **Omvang wijzigen** vermindert u het aantal CPU's tot **4** en klikt u op **Indienen**.

De voorgestelde waarde is een voorbeeld. Wijzig het aantal CPU's in een waarde die het beste past in uw omgeving.

De actie wordt uitgevoerd voor de machine.

- Om te controleren of het aantal CPU's is gewijzigd, opent u de implementatie en controleert u de aangepaste eigenschap `cpuCount` van de machine.
- U kunt ook het aantal in vCenter Server controleren.



Stap 5: goedkeuringsbeleid toepassen

Als cloudbeheerder kunt u in vRealize Automation governance toepassen om de mogelijkheden van gebruikers te beperken of te vereisen dat ze bepaalde bewerkingen niet zonder voorafgaande goedkeuring mogen doen. Deze tutorial laat zien hoe u goedkeuringsbeleid toepast op de actie voor de omvangswijziging, zodat gebruikers niet zonder uw goedkeuring of die van een andere beheerder een machine kunnen configureren (met mogelijk ernstige gevolgen).

De beleidsregels worden gemaakt in Service Broker. Ze zijn echter van toepassing op de relevante aanvragen in Cloud Assembly en Service Broker.

Als goedkeurder moet u reageren op de goedkeuringsaanvraag in Service Broker.

- 1 Selecteer in Service Broker **Inhoud en beleidsregels > Beleidsregels > Definities** en klik vervolgens op **Nieuw beleid**.
- 2 Klik op **Goedkeuringsbeleid**.
- 3 Configureer het goedkeuringsbeleid.

Resize Approval Policy [DELETE](#)

Approval policies control who must agree to a deployment or day 2 action before the request is provisioned. ⓘ

Type: Approval

Name *:

Description:

Scope *: ☐ Organization / Multiple Projects
 Apply the policy to all or a selection of projects in this organization. To target multiple projects, select project based criteria. ⓘ
 ☒ Project
 Apply the policy to a single project in this organization.
 Onboarding Project

Criteria: ⓘ

Approval type *: ☒ User based ☐ Role based ⓘ

Approver mode *: ☒ Any ☐ All ⓘ

Approvers *: ⓘ

<input type="checkbox"/>	Name	Email	Type
<input type="checkbox"/>	Fritz Arbeter	fritz	User
			1 user

Auto expiry decision *: ⓘ

Auto expiry trigger *: days ⓘ

Actions *: ⓘ ⓘ

<input type="checkbox"/>	Actions
<input type="checkbox"/>	Cloud.vSphere.Machine.Resize

De volgende tabel bevat voorbeeldwaarden die illustreren hoe u het beleid kunt maken.

Instelling	Voorbeeldwaarde
Naam	Goedkeuringsbeleid voor omvang wijzigen
Scope	Selecteer Project en selecteer vervolgens Onboardingsproject . Het goedkeuringsbeleid wordt geactiveerd wanneer een gebruiker die lid is van het project, de actie Omvang wijzigen voor dag 2 uitvoert.
Goedkeuringstype	Op basis van gebruiker Met deze waarde kunt u de goedkeurders een naam geven.
Goedkeurdersmodus	Willekeurig Als u meerdere goedkeurders hebt, kan minimaal één goedkeurder de goedkeuringsaanvraag afhandelen.
Goedkeurders	Voeg uzelf toe als goedkeurder.

Instelling	Voorbeeldwaarde
Beslissing automatisch verval	Weigeren Door een niet beoordeelde aanvraag te weigeren, vermindert u het risico dat een machine onbruikbaar wordt of te veel resources heeft.
Trigger automatisch verval	1
Acties	Selecteer de actie voor de omvangswijziging die het goedkeuringsbeleid activeert. <ol style="list-style-type: none"> 1 Voer machine.resize in het zoekveld in. 2 Klik op Meervoudige selectie in de vervolgkeuzelijst met zoekresultaten. 3 Selecteer Cloud.vSphere.Machine.Resize. <p>Omdat deze tutorial is gebaseerd op vSphere, selecteert u de actie vSphere.Machine. Als u het actiebeleid op andere resourcetypes wilt toepassen, kunt u nog meer acties Machine.Resize toevoegen.</p>

Stap 6: een aanvraag voor omvangswijziging aanvragen als gebruiker

In deze stap meldt u zich als organisatielid en Service Broker-gebruiker aan bij Service Broker en voert u een aanvraag voor een omvangswijziging voor dag 2 uit. Met deze aanvraag wordt een goedkeuringsaanvraag gemaakt. De gebruiker kan ook dezelfde stappen uitvoeren in Cloud Assembly.

In de stap hierna meldt u zich aan als de gebruiker die u in stap 5 als goedkeurder hebt aangewezen en keurt u de aanvraag vervolgens goed.

- 1 Meld u als gebruiker aan bij Service Broker.

In deze tutorial is de gebruiker Sylvia.

- 2 Selecteer **Resources > Implementaties** en zoek de geonboarde machine 1.

Dit is de implementatie waarbij u in stap 4 de actie voor een omvangswijziging van de machine hebt uitgevoerd door het aantal CPU's van 8 naar 4 te verlagen. Als u een andere waarde hebt gebruikt, kiest u de gewenste aanpassing van de machine om de test uit te voeren.

- 3 Voer de actie **Omvang wijzigen** voor de machine uit en verhoog het aantal CPU's tot **6**.
- 4 U ziet dat de aanvraag op goedkeuring wacht.

Als u de status In behandeling wilt zien, plaatst u de muisaanwijzer op het informatiepictogram in het raster of opent u de implementatie en gaat u naar het tabblad **Geschiedenis**.

	Name	Address	Owner	Project	Status	Expires on	Price
▼	Onboarded ma...		sylvia	Onboarding P...	Approval Pending	Never	
	Hard disk 2						
	DevProject-c...						
>	Onboarded ma...		sylvia	Onboarding P...			

5 De wijziging die Sylvia als gebruiker heeft aangevraagd, wordt pas uitgevoerd nadat deze is goedgekeurd.

6 Meld u af als gebruiker bij Service Broker.

In stap 7 meldt u zich aan als de toegewezen goedkeurder en beantwoordt u de aanvraag.

Stap 7: reageren op een goedkeuringsaanvraag

Wanneer een aanvraag goedkeuring vereist en u de goedkeurder bent, ontvangt u een e-mailbericht. Voor deze tutorial hoeven we dat bericht niet af te wachten. In plaats daarvan leidt het proces u direct door naar de reactie op een goedkeuringsaanvraag op het tabblad Goedkeuringen van Service Broker.

1 Meld u in stap 5 aan bij Service Broker als de gebruiker die u als goedkeurder hebt toegewezen.

In deze tutorial is Fritz de goedkeurder.

2 Selecteer **Resources > Implementaties** en zoek de geonboarde machine 1.

De status in het raster ziet er hetzelfde uit als voor Sylvia.

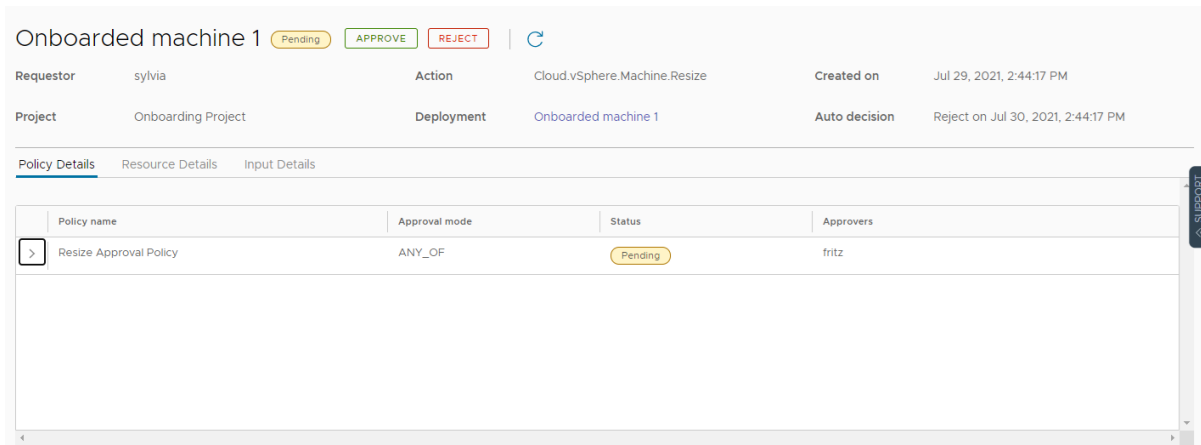
	Name	Address	Owner	Project	Status	Expires on	Price
▼	Onboarded ma...		sylvia	Onboarding P...	Approval Pending	Never	
	Hard disk 2						
	DevProject-c...						
>	Onboarded ma...		sylvia	Onboarding P...			

3 Klik op het tabblad **Goedkeuringen**.

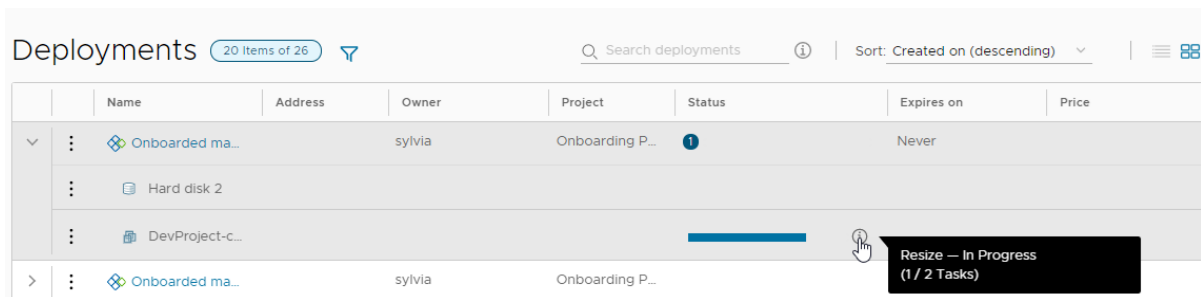
U ziet dat er een goedkeuringsaanvraag in behandeling is.

Approval Requests (1 item of 1)			
Onboarded machine 1	Pending	Expires on Jul 30, 2021, 2:44:17 PM	Action: Cloud.vSphere.Machine.Resize Created on: Jul 29, 2021, 2:44:17 PM Policy details: Resize Approval Policy

4 Klik op de naam van de implementatie om de details van de aanvraag te bekijken.



- 5 Klik op **Goedkeuren**, voeg indien nodig een opmerking toe en klik op **Goedkeuren**.
- 6 Ga terug naar de pagina **Implementaties** om te zien of de door Sylvia aangevraagde actie voor de omvangswijziging nu wordt uitgevoerd.



- 7 Wanneer de actie voor de omvangswijziging is voltooid, kunt u het aantal CPU's controleren in de implementatiedetails en in de vSphere Client.

In deze tutorial werd u begeleid door het overdrachtsproces van machines naar vRealize Automation, zodat u de levenscyclus van de resource kunt gaan beheren.

Tutorial: Infrastructuur en implementaties met meerdere clouds instellen en testen in Cloud Assembly

Deze volledige Cloud Assembly-tutorial laat zien hoe u kunt implementeren in een omgeving met meerdere clouds. U implementeert dezelfde cloudsjabloon voor meer dan één provider, in dit geval AWS en Microsoft Azure.

In dit voorbeeld is de applicatie een WordPress-site. Bekijk de sequentiële setup om inzicht te krijgen in het proces dat het hele ontwerp voltooit.

Houd er rekening mee dat de namen en waarden die u ziet alleen voorbeelden zijn. U kunt deze niet letterlijk overnemen in uw eigen omgeving.

Om uw eigen cloudinfrastructuur- en implementatiebehoeften aan te passen, kunt u overwegen waar u uw eigen vervangingen wilt aanbrengen voor de voorbeeldwaarden.

Deel 1: het voorbeeld van de Cloud Assembly-infrastructuur configureren

Configureer eerst de resources waar Cloud Assembly-engineeringgebruikers later de applicatie kunnen ontwikkelen en testen en in productie kunnen brengen.

De infrastructuur omvat clouddoelen en definities met betrekking tot de beschikbare machines, netwerken en opslag die de WordPress-site nodig heeft.

Vereisten

Meld u als Cloud Assembly-beheerder aan bij Cloud Assembly.

1. Cloudaccounts toevoegen

In deze stap voegt de cloudbeheerder twee cloudaccounts toe. Het voorbeeldproject zal ontwikkelings- en testwerk uitvoeren in AWS en in productie gaan in Azure.

- 1 Ga naar **Infrastructuur > Verbindingen > Cloudaccounts**.
- 2 Klik op **Cloudaccount toevoegen**, selecteer Amazon Web Services en voer waarden in.

Instelling	Voorbeeldwaarde
Toegangssleutel-id	R5SDR3PXVV2ZW8B7YNSM
Geheime toegangssleutel	SZXAINXU4UHNAQ1E156S
Naam	OurCo-AWS
Beschrijving	WordPress

Houd er rekening mee dat alle waarden alleen voorbeelden zijn. Uw accountgegevens zullen hiervan verschillen.

- 3 Klik op **Valideren** om de verificatiegegevens te controleren.
- 4 Klik op **Toevoegen**.
- 5 Bewerk de **configuratie** van het zojuist toegevoegde account en sta inrichting in de regio's us-east-1 en us-west-2 toe.
- 6 Klik op **Cloudaccount toevoegen**, selecteer Microsoft Azure en voer waarden in.

Instelling	Voorbeeldwaarde
Abonnements-id	ef2avpf-dfdv-zxlugi7i-g4h0-i8ep2jwp4c9arbf
Tenant-id	dso9wv3-4zgc-5nrcy5h3m-4skf-nnovp40wfxsro22r
Clientapplicatie-id	bg224oq-3ptp-mbhi6aa05-q511-uflyjr2sttyik6bs
Geheime sleutel clientapplicatie	7uqxi57-0wtn-kymgf9wcj-t2l7-e52e4nu5fig4pmd

Instelling	Voorbeeldwaarde
Naam	OurCo-Azure
Beschrijving	WordPress

- 7 Klik op **Valideren** om de verificatiegegevens te controleren.
- 8 Klik op **Toevoegen**.
- 9 Bewerk de **configuratie** van het zojuist toegevoegde account en sta inrichting in de regio East US toe.

2. Cloudzones toevoegen

In deze voorbeeldstap voegt de cloudbeheerder drie cloudzones toe voor ontwikkelings-, test- en productiedoeleinden.

- 1 Ga naar **Infrastructuur > Configureren > Cloudzones**.
- 2 Klik op **Nieuwe cloudzone** en voer waarden in voor de ontwikkelingsomgeving.

Instelling voor cloudzone	Voorbeeldwaarde
Account/regio	OurCo-AWS/us-east-1
Naam	OurCo-AWS-US-East
Beschrijving	WordPress
Plaatsingsbeleid	Standaard
Mogelijkheidstags	env:dev

Houd er rekening mee dat alle waarden alleen voorbeelden zijn. Uw zonegegevens zullen hiervan verschillen.

- 3 Klik op **Berekenen** en controleer of de zones die u verwacht, zich daar bevinden.
- 4 Klik op **Maken**.
- 5 Herhaal het proces tweemaal met waarden voor de test- en productieomgevingen.

Instelling voor cloudzone	Voorbeeldwaarde
Account/regio	OurCo-AWS/us-west-2
Naam	OurCo-AWS-US-West
Beschrijving	WordPress
Plaatsingsbeleid	Standaard
Mogelijkheidstags	env:test

Instelling voor cloudzone	Voorbeeldwaarde
Account/regio	OurCo-Azure/East US
Naam	OurCo-Azure-East-US
Beschrijving	WordPress
Plaatsingsbeleid	Standaard
Mogelijkheidstags	env:prod

3. Soorttoewijzingen toevoegen

In deze voorbeeldstap voegt de cloudbetreiber soorttoewijzingen toe aan het account voor capaciteitsbehoeften die afhankelijk van de implementatie kunnen variëren.

Soorttoewijzing heeft betrekking op machine-implementaties van verschillende grootten en hiernaar wordt informeel verwezen als T-shirtmaat.

- 1 Ga naar **Infrastructuur > Configureren > Soorttoewijzingen**. In elke cloudzone moeten kleine, gemiddelde en grote soorten zijn toegestaan.
- 2 Klik op **Nieuwe soorttoewijzing** en voer waarden in voor de cloudzone voor ontwikkeling.

Instelling	Voorbeeldwaarde
Soortnaam	small
Account/regio	OurCo-AWS/us-east-1
Waarde	t2.micro
Account/regio	OurCo-AWS/us-west-2
Waarde	t2.micro
Account/regio	OurCo-Azure/East US
Waarde	Standard_A0

Houd er rekening mee dat alle waarden alleen voorbeelden zijn. Uw soorten zullen hiervan verschillen.

- 3 Klik op **Maken**.
- 4 Herhaal het proces tweemaal met waarden voor middelgrote en grote soorten.

Instelling	Voorbeeldwaarde
Soortnaam	medium
Account/regio	OurCo-AWS/us-east-1
Waarde	t2.medium

Instelling	Voorbeeldwaarde
Account/regio	OurCo-AWS/us-west-2
Waarde	t2.medium
Account/regio	OurCo-Azure/East US
Waarde	Standard_A3

Instelling	Voorbeeldwaarde
Soortnaam	large
Account/regio	OurCo-AWS/us-east-1
Waarde	t2.large
Account/regio	OurCo-AWS/us-west-2
Waarde	t2.large
Account/regio	OurCo-Azure/East US
Waarde	Standard_A7

4. Imagetoewijzingen toevoegen

In deze voorbeeldstap voegt de cloudbbeheerder een imagetoewijzing toe voor Ubuntu, de host voor de WordPress-server en de MySQL-databaseserver.

Plan het besturingssysteem door imagetoewijzingen toe te voegen. Elke cloudzone heeft een Ubuntu-imagetoewijzing nodig.

- 1 Ga naar **Infrastructuur > Configureren > Imagetoewijzingen**.
- 2 Klik op **Nieuwe imagetoewijzing** en voer waarden in voor Ubuntu-servers.

Instelling	Voorbeeldwaarde
Imagenaam	ubuntu
Account/regio	OurCo-AWS/us-east-1
Waarde	ubuntu-16.04-server-cloudimg-amd64
Account/regio	OurCo-AWS/us-west-2
Waarde	ubuntu-16.04-server-cloudimg-amd64
Account/regio	OurCo-Azure/East US
Waarde	azul-zulu-ubuntu-1604-923eng

Houd er rekening mee dat alle waarden alleen voorbeelden zijn. Uw images zullen hiervan verschillen.

- 3 Klik op **Maken**.

5. Netwerkprofielen toevoegen

In deze voorbeeldstap voegt de cloudbbeheerder een netwerkprofiel toe aan elke cloudzone.

In elk profiel voegt de beheerder een netwerk toe voor de WordPress-machines en een tweede netwerk dat zich aan de andere kant van een uiteindelijke load balancer zal bevinden. Het tweede netwerk is het netwerk waarmee gebruikers uiteindelijk verbinding maken.

- 1 Ga naar **Infrastructuur > Configureren > Netwerkprofielen**.
- 2 Klik op **Nieuw netwerkprofiel** en maak een profiel voor de cloudzone voor ontwikkeling.

Instelling voor netwerkprofiel	Voorbeeldwaarde
Account/regio	OurCo-AWS/us-east-1
Naam	devnets
Beschrijving	WordPress

- 3 Klik op **Netwerken** en klik op **Netwerk toevoegen**.
- 4 Selecteer wpnet, appnet-public en klik op **Toevoegen**.
Houd er rekening mee dat alle waarden alleen voorbeelden zijn. Uw netwerknamen zullen hiervan verschillen.
- 5 Klik op **Maken**.

In dit WordPress-voorbeeld is niet vereist dat u netwerkbeleid of netwerkbeveiligingsinstellingen opgeeft.

- 6 Herhaal het proces tweemaal om een netwerkprofiel te maken voor de test- en productiecloudzones in het WordPress-voorbeeld. Voeg in elk geval de wpnet- en appnet-public-netwerken toe.

Instelling voor netwerkprofiel	Voorbeeldwaarde
Account/regio	OurCo-AWS/us-west-2
Naam	testnets
Beschrijving	WordPress

Instelling voor netwerkprofiel	Waarde
Account/regio	OurCo-Azure/East US
Naam	prodnets
Beschrijving	WordPress

6. Opslagprofielen toevoegen

In deze voorbeeldstap voegt de cloudbeheerder een opslagprofiel toe aan elke cloudzone.

De beheerder plaatst snelle opslag in de productiezone en algemene opslag in de ontwikkelings- en testzone.

- 1 Ga naar **Infrastructuur > Configureren > Opslagprofielen**.
- 2 Klik op **Nieuw opslagprofiel** en maak een profiel voor de cloudzone voor ontwikkelingsdoeleinden.

Er worden extra velden weergegeven nadat u het account/de regio hebt geselecteerd.

Instelling voor opslagprofiel	Voorbeeldwaarde
Account/regio	OurCo-AWS/us-east-1
Naam	OurCo-AWS-US-East-Disk
Beschrijving	WordPress
Apparaattype	EBS
Volumetype	SSD voor algemeen gebruik
Mogelijkheidstags	storage:general

Houd er rekening mee dat alle waarden alleen voorbeelden zijn.

- 3 Klik op **Maken**.
- 4 Herhaal het proces om een profiel te maken voor de cloudzone voor testdoeleinden.

Instelling voor opslagprofiel	Voorbeeldwaarde
Account/regio	OurCo-AWS/us-west-2
Naam	OurCo-AWS-US-West-Disk
Beschrijving	WordPress
Apparaattype	EBS
Volumetype	SSD voor algemeen gebruik
Mogelijkheidstags	storage:general

- 5 Herhaal het proces om een profiel voor de cloudzone voor productie te maken. Deze heeft verschillende instellingen omdat het een Azure-zone is.

Instelling voor opslagprofiel	Voorbeeldwaarde
Account/regio	OurCo-Azure/East US
Naam	OurCo-Azure-East-US-Disk
Beschrijving	WordPress
Opslagtype	Beheerde schijven

Instelling voor opslagprofiel	Voorbeeldwaarde
Schijftype	Premium-LRS
Opslaan in cache van besturingssysteemschijf	Alleen-lezen
Opslaan in cache van gegevensschijf	Alleen-lezen
Mogelijkheids-tags	storage:fast

Wat moet u nu doen

Maak een project om gebruikers te identificeren en om inrichtingsinstellingen te definiëren. Zie [Deel 2: het voorbeeld van een Cloud Assembly-project maken](#).

Deel 2: het voorbeeld van een Cloud Assembly-project maken

Het voorbeeld van een Cloud Assembly-project stelt gebruikers in staat om in te richten en configureert hoeveel inrichting mogelijk is.

Projecten definiëren de gebruikers- en inrichtingsinstellingen.

- Gebruikers en het machtigingsniveau van hun rol
- Prioriteit voor implementaties zoals deze in een cloudzone worden ingericht
- Maximaal aantal implementatie-instanties per cloudzone

Procedure

- 1 Ga naar **Infrastructuur > Beheer > Projecten**.
- 2 Klik op **Nieuw project** en voer de naam WordPress in.
- 3 Klik op **Gebruikers** en klik op **Gebruikers toevoegen**.
- 4 Voeg e-mailadressen en rollen voor de gebruikers toe.

Om een gebruiker toe te voegen, moet een VMware Cloud Services-beheerder toegang tot Cloud Assembly hebben ingeschakeld voor de gebruiker.

De hier weergegeven adressen zijn alleen bedoeld als voorbeeld.

- chris.ladd@ourco.com, Lid
 - kerry.mott@ourco.com, Lid
 - pat.tubb@ourco.com, Beheerder
- 5 Klik op **Inrichting** en klik vervolgens op **Cloudzone toevoegen**.

6 Voeg de cloudzones toe waarop de gebruikers kunnen worden geïmplementeerd.

Instelling voor projectcloudzone	Voorbeeldwaarde
Cloudzone	OurCo-AWS-US-East
Inrichtingsprioriteit	1
Limiet voor instanties	5
Cloudzone	OurCo-AWS-US-West
Inrichtingsprioriteit	1
Limiet voor instanties	5
Cloudzone	OurCo-Azure-East-US
Inrichtingsprioriteit	0
Limiet voor instanties	1

7 Klik op **Maken**.

8 Ga naar **Infrastructuur > Configureren > Cloudzones** en open een zone die u eerder hebt gemaakt.

9 Klik op **Projecten** en controleer of WordPress een project is dat is toegestaan om de zone in te richten.

10 Controleer de andere zones die u hebt gemaakt.

Wat nu te doen

Maak een basiscloudsjabloon.

Deel 3: het voorbeeld van een Cloud Assembly-sjabloon ontwerpen en implementeren

Vervolgens definieert u de voorbeeldapplicatie, de WordPress-site, in de vorm van een generieke cloudsjabloon. De sjabloon kan naar verschillende cloudleveranciers worden geïmplementeerd zonder dat u het ontwerp hoeft te wijzigen.

Het voorbeeld bestaat uit een WordPress-applicatieserver, MySQL-databaseserver en ondersteunende resources. De sjabloon begint met een paar resources en groeit naarmate u ze aanpast en meer resources toevoegt.

Hier zijn de waarden van [Deel 1: het voorbeeld van de Cloud Assembly-infrastructuur configureren](#), de infrastructuur die door een cloudbeheerder is ingesteld:

- Twee cloudaccounts: AWS en Azure.
- Drie cloudzoneomgevingen:
 - Ontwikkeling — OurCo-AWS-US-East
 - Test — OurCo-AWS-US-West
 - Productie — OurCo-Azure-East-US
- Soorttoewijzingen met kleine, middelgrote en grote berekeningsresources voor elke zone.

- Imago-toewijzingen voor Ubuntu die in elke zone zijn geconfigureerd.
- Netwerkprofielen met interne en externe subnetten voor elke zone.
- Opslag waarop moet worden geïmplementeerd. Algemene opslag voor de ontwikkelings- en testzone en snelle opslag voor de productiezone.
- Het voorbeeldproject bevat alle drie de cloudzone-omgevingen plus de gebruikers die ontwerpen kunnen maken.

Voorwaarden

Om te kunnen volgen, moet u vertrouwd zijn met uw eigen infrastructuurwaarden. Dit voorbeeld gebruikt AWS voor ontwikkelings- en testdoeleinden, en Azure voor productiedoeleinden. Wanneer u uw eigen cloudsjabloon maakt, vult u uw eigen waarden in, doorgaans ingesteld door de cloudbeheerder.

Procedure

1 Een basiscloudsjabloon maken

In dit voorbeeld van een Cloud Assembly-ontwerp begint u met een cloudsjabloon die alleen minimale WordPress-resources bevat, bijvoorbeeld als u alleen een applicatieserver hebt.

2 Een basiscloudsjabloon testen

Tijdens een ontwerp bouwt u vaak een cloudsjabloon door te beginnen met de essentiële onderdelen en implementeert en test u vervolgens wanneer de sjabloon groeit. Dit voorbeeld demonstreert een aantal in behandeling zijnde tests die zijn ingebouwd in Cloud Assembly.

3 Een cloudsjabloon uitbreiden

Nadat u de Cloud Assembly-basisjabloon hebt gemaakt en getest voor het voorbeeld van de applicatie, kunt u deze uitbreiden naar een applicatie met meerdere lagen die voor ontwikkelings-, test- en uiteindelijk productiedoeleinden kan worden geïmplementeerd.

Een basiscloudsjabloon maken

In dit voorbeeld van een Cloud Assembly-ontwerp begint u met een cloudsjabloon die alleen minimale WordPress-resources bevat, bijvoorbeeld als u alleen een applicatieserver hebt.

Cloud Assembly is een Infrastructure-as-code-tool. U sleept resources naar het ontwerpcanvas om aan de slag te gaan. Vervolgens vult u de gegevens in met de code-editor rechts van het canvas.

Met de code-editor kunt u code direct typen, knippen en plakken. Als u niet vertrouwd bent met het bewerken van code, selecteert u een resource in het canvas, klikt u op het tabblad **Eigenschappen** in de code-editor en voert u daar waarden in. Waarden die u invoert, worden in de code weergegeven alsof u ze direct hebt getypt.

Procedure

- 1 Ga naar **Ontwerp > Cloudsjablonen** en klik op **Nieuw van > Leeg canvas**.
- 2 Geef de cloudsjabloon de naam **WordPress-BP**.

- 3 Selecteer het **WordPress**-project en klik op **Maken**.
- 4 Sleep twee cloudonafhankelijke machines vanuit de resources links op de ontwerppagina voor cloudsjablonen naar het canvas.

De machines fungeren als WordPress-applicatieserver (WebTier) en MySQL-databaseserver (DBTier).

- 5 Bewerk YAML-code van de machine rechts om namen, afbeeldingen, soorten en beperkingstags toe te voegen:

```
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      image: ubuntu
      flavor: small
      constraints:
        - tag: env:dev
  DBTier:
    type: Cloud.Machine
    properties:
      name: mysql
      image: ubuntu
      flavor: small
      constraints:
        - tag: env:dev
```

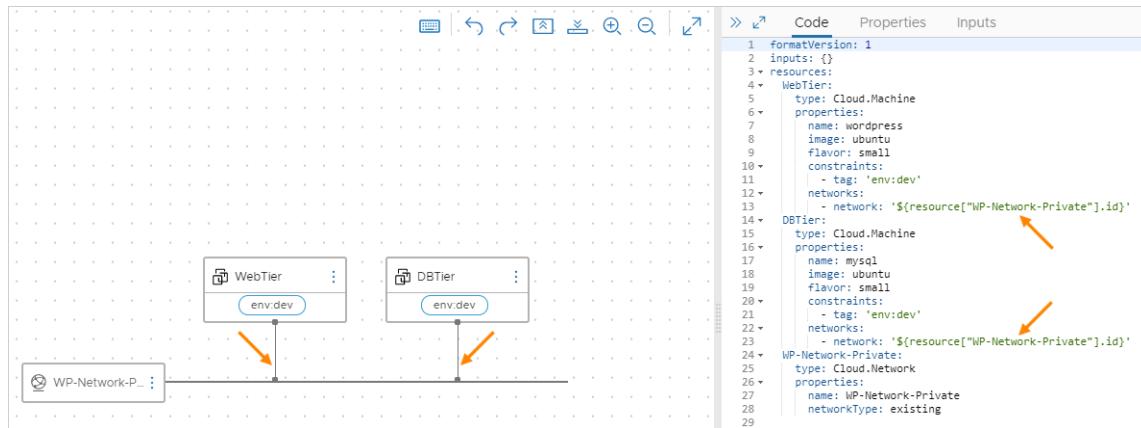
- 6 Sleep een cloudonafhankelijk netwerk naar het canvas en bewerk de code ervan:

```
WP-Network-Private:
  type: Cloud.Network
  properties:
    name: WP-Network-Private
    networkType: existing
```

- 7 Verbind de machines met het netwerk:

Houd in het canvas de muis over het netwerkblok, klik en houd de ballon vast waar de lijn het blok raakt, sleep deze naar een machineblok en laat deze los.

Wanneer u de verbidingsregels maakt, wordt netwerkcode automatisch toegevoegd aan de machines in de editor.



8 Voeg prompt voor gebruikersinvoer toe.

Op sommige plaatsen is het voorbeeld van de infrastructuur voor meerdere opties ingesteld. Bijvoorbeeld:

- Cloudzoneomgevingen voor ontwikkeling, test en productie
- Soorttoewijzingen voor kleine, middelgrote en grote machines

U kunt een specifieke optie rechtstreeks in de cloudsjabloon instellen, maar u kunt ook de gebruiker de optie laten selecteren bij het implementeren van de sjabloon. Met behulp van prompts voor gebruikersinvoer kunt u één sjabloon maken die op vele manieren kan worden geïmplementeerd, in plaats van een groot aantal in code vastgelegde sjablonen te gebruiken.

- a Maak een sectie `inputs` in de code zodat gebruikers de grootte en de doelomgeving van de machine tijdens het implementeren kunnen selecteren. Definieer de selecteerbare waarden.

```
inputs:
  env:
    type: string
    enum:
      - env:dev
      - env:prod
      - env:test
    default: env:dev
    title: Environment
    description: Target Environment
  size:
    type: string
    enum:
      - small
      - medium
      - large
    description: Size of Nodes
    title: Tier Machine Size
```

- b Voeg in de sectie `resources` van de code de code `${input.input-name}` toe om gebruikers om hun selectie te vragen:

```
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      image: ubuntu
      flavor: '${input.size}'
    constraints:
      - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
  DBTier:
    type: Cloud.Machine
    properties:
      name: mysql
      image: ubuntu
      flavor: '${input.size}'
    constraints:
      - tag: '${input.env}'
    networks:
```

```
        - network: '${resource["WP-Network-Private"].id}'  
WP-Network-Private:  
  type: Cloud.Network  
  properties:  
    name: WP-Network-Private  
    networkType: existing
```

- 9** Verbeter ten slotte de code `WebTier` en `DBTier` met behulp van de volgende voorbeelden. Voor de `WP-Network-Private`-code hoeven geen aanvullende wijzigingen te worden aangebracht.

Tot de verbeteringen behoren aanmeldingstoegang tot de databaseserver en `cloudConfig`-initialisatiescripts tijdens het implementeren.

Onderdeel	Voorbeeld
Aanvullende DBTier-invoer	<pre> username: type: string minLength: 4 maxLength: 20 pattern: '[a-z]+' title: Database Username description: Database Username userpassword: type: string pattern: '[a-z0-9A-Z@#]+\$' encrypted: true title: Database Password description: Database Password </pre>
DBTier-resource	<pre> DBTier: type: Cloud.Machine properties: name: mysql image: ubuntu flavor: '\${input.size}' constraints: - tag: '\${input.env}' networks: - network: '\${resource["WP-Network-Private"].id}' assignPublicIpAddress: true remoteAccess: authentication: usernamePassword username: '\${input.username}' password: '\${input.userpassword}' cloudConfig: #cloud-config repo_update: true repo_upgrade: all packages: - mysql-server runcmd: - sed -e '/bind-address/ s/^#*\/#/' -i /etc/mysql/mysql.conf.d/ mysql.cnf - service mysql restart - mysql -e "CREATE USER 'root'@'%' IDENTIFIED BY 'mysqlpassword';" - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%';" - mysql -e "FLUSH PRIVILEGES;" attachedDisks: [] </pre>
WebTier-resource	<pre> WebTier: type: Cloud.Machine properties: name: wordpress image: ubuntu flavor: '\${input.size}' constraints: - tag: '\${input.env}' networks: - network: '\${resource["WP-Network-Private"].id}' assignPublicIpAddress: true cloudConfig: </pre>

Onderdeel	Voorbeeld
	<pre> #cloud-config repo_update: true repo_upgrade: all packages: - apache2 - php - php-mysql - libapache2-mod-php - mysql-client - gcc - make - autoconf - libc-dev - pkg-config - libmcrypt-dev - php-pear - php-dev runcmd: - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/ latest.tar.gz -C /var/www/html/mywordpresssite --strip-components 1 - i=0; while [\$i -le 10]; do mysql --connect-timeout=3 -h \$ {DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break sleep 15; i=\$((i+1)); done - mysql -u root -pmysqlpassword -h \${DBTier.networks[0].address} -e "create database wordpress_blog;" - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/ html/mywordpresssite/wp-config.php - pecl channel-update pecl.php.net - pecl update-channels - pecl install mcrypt - sed -i -e s/"define('DB_NAME', 'database_name_here');"/"define('DB_NAME', 'wordpress_blog');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i -e s/"define('DB_USER', 'username_here');"/"define('DB_USER', 'root');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i -e s/"define('DB_PASSWORD', 'password_here');"/"define('DB_PASSWORD', 'mysqlpassword');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i -e s/"define('DB_HOST', 'localhost');"/"define('DB_HOST', '\${DBTier.networks[0].address}');"/ /var/www/html/mywordpresssite/wp- config.php - sed -i '950i extension=mcrypt.so' /etc/php/7.4/apache2/php.ini - service apache2 reload </pre>

Voorbeeld: Voorbeeld van voltooide code voor basiscloudsjabloon

```

formatVersion: 1
inputs:
  env:
    type: string
    enum:
      - env:dev
      - env:prod
      - env:test
    default: env:dev
    title: Environment
    description: Target Environment
  size:
    type: string

```

```

enum:
  - small
  - medium
  - large
description: Size of Nodes
title: Tier Machine Size
username:
  type: string
  minLength: 4
  maxLength: 20
  pattern: '[a-z]+'
  title: Database Username
  description: Database Username
userpassword:
  type: string
  pattern: '[a-z0-9A-Z@#]+$'
  encrypted: true
  title: Database Password
  description: Database Password
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      image: ubuntu
      flavor: '${input.size}'
      constraints:
        - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
        assignPublicIpAddress: true
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
      packages:
        - apache2
        - php
        - php-mysql
        - libapache2-mod-php
        - mysql-client
        - gcc
        - make
        - autoconf
        - libc-dev
        - pkg-config
        - libmcrypt-dev
        - php-pear
        - php-dev
      runcmd:
        - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
mywordpresssite --strip-components 1
        - i=0; while [ $i -le 10 ]; do mysql --connect-timeout=3 -h $
{DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;

```

```

i=$((i+1)); done
    - mysql -u root -pmysqlpassword -h ${DBTier.networks[0].address} -e "create database
wordpress_blog;"
    - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/mywordpresssite/
wp-config.php
    - pecl channel-update pecl.php.net
    - pecl update-channels
    - pecl install mcrypt
    - sed -i -e s/"define( 'DB_NAME', 'database_name_here' );"/"define( 'DB_NAME',
'wordpress_blog' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_USER', 'username_here' );"/"define( 'DB_USER',
'root' );"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
-e s/"define( 'DB_PASSWORD', 'password_here' );"/"define( 'DB_PASSWORD',
'mysqlpassword' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_HOST', 'localhost' );"/"define( 'DB_HOST', '$
${DBTier.networks[0].address}' );"/ /var/www/html/mywordpresssite/wp-config.php
    - sed -i '950i extension=mcrypt.so' /etc/php/7.4/apache2/php.ini
    - service apache2 reload
DBTier:
  type: Cloud.Machine
  properties:
    name: mysql
    image: ubuntu
    flavor: '${input.size}'
    constraints:
      - tag: '${input.env}'
  networks:
    - network: '${resource["WP-Network-Private"].id}'
      assignPublicIpAddress: true
  remoteAccess:
    authentication: usernamePassword
    username: '${input.username}'
    password: '${input.userpassword}'
  cloudConfig: |
    #cloud-config
    repo_update: true
    repo_upgrade: all
    packages:
      - mysql-server
    runcmd:
      - sed -e '/bind-address/ s/^#/#/' -i /etc/mysql/mysql.conf.d/mysqld.cnf
      - service mysql restart
      - mysql -e "CREATE USER 'root'@'%' IDENTIFIED BY 'mysqlpassword';"
      - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%;'"
      - mysql -e "FLUSH PRIVILEGES;"
  attachedDisks: []
WP-Network-Private:
  type: Cloud.Network
  properties:
    name: WP-Network-Private
    networkType: existing

```

Wat nu te doen

Test de cloudsjabloon door de syntaxis te controleren en te implementeren.

Een basiscloudsjabloon testen

Tijdens een ontwerp bouwt u vaak een cloudsjabloon door te beginnen met de essentiële onderdelen en implementeert en test u vervolgens wanneer de sjabloon groeit. Dit voorbeeld demonstreert een aantal in behandeling zijnde tests die zijn ingebouwd in Cloud Assembly.

Om er zeker van te zijn dat een implementatie werkt zoals u dat wilt, moet u de cloudsjabloon mogelijk meerdere keren testen en implementeren. Geleidelijk aan voegt u meer resources toe en tegelijk voert u nieuwe tests en implementaties uit.

Voorwaarden

Maak de basiscloudsjabloon. Zie [Een basiscloudsjabloon maken](#).

Procedure

- 1 Klik op **Cloudsjablonen** en open de WordPress-BP-cloudsjabloon.
De basiscloudsjabloon wordt weergegeven in het ontwerpcanvas en de code-editor.
- 2 Als u de sjabloonsyntaxis, plaatsing en basisgeldigheid wilt controleren, klikt u op **Testen** in de linkerbenedenhoek.
- 3 Voer invoerwaarden in en klik op **Testen**.

Testing Basic

Environment ⓘ

Tier Machine Size ⓘ

Database Username

Database Password

De test is slechts een simulatie en implementeert geen virtuele machines of andere resources.

← Test Result for Basic ⓘ

Successful This simulation only tests syntax, placement and basic validity

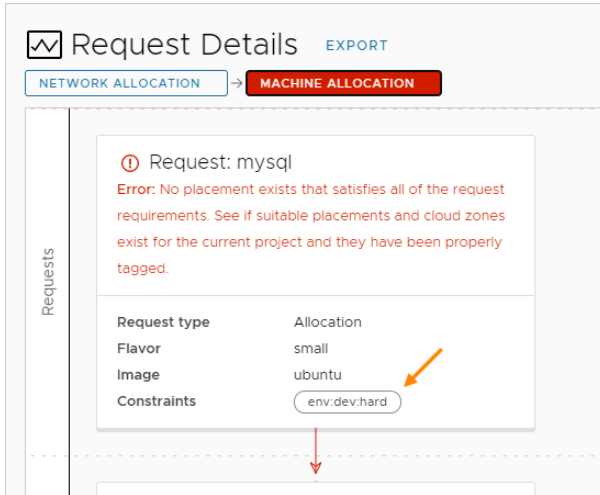
3 Infos Provisioning Diagram

WP-Network-Private ✓
LINE 96

DBTier ✓
LINE 69

WebTier ✓

De test bevat een link naar een **Inrichtingsdiagram**, waar u de gesimuleerde implementatiestroom kunt controleren en ziet wat er zich heeft voorgedaan. De simulatie onthult mogelijke problemen, zoals het ontbreken van gedefinieerde resourcemogelijkheden die voldoen aan harde beperkingen in de cloudsjabloon. In de volgende voorbeeldfout is een cloudzone met capaciteitstag `env:dev` nog niet in de gedefinieerde infrastructuur gevonden.



Een succesvolle simulatie garandeert niet dat u de sjabloon zonder fouten kunt implementeren.

- 4 Nadat de sjabloon de simulatie heeft doorstaan, klikt u op **Implementeren** in de linkerbenedenhoek.
- 5 Selecteer **Een nieuwe implementatie maken**.
- 6 Geef de implementatie de naam **WordPress for OurCo** en klik op **Volgende**.
- 7 Voer invoerwaarden in en klik op **Implementeren**.
- 8 Kijk onder **Resources > Implementaties** of de sjabloon correct is geïmplementeerd.

Als een implementatie mislukt, klikt u op de naam en klikt u op het tabblad **Geschiedenis** om berichten te bekijken die u kunnen helpen het probleem op te lossen.

Timestamp	Status	Resource type	Resource name
Sep 8, 2020, 1...	CREATE_IN_PROGRESS	Cloud.Machine	WebTier
Sep 8, 2020, 1...	CREATE_FINISHED	Cloud.Machine	DBTier
Sep 8, 2020, 1...	CREATE_IN_PROGRESS	Cloud.Machine	DBTier
Sep 8, 2020, 1...	CREATE_FINISHED	Cloud.Network	WP-Network-Private
Sep 8, 2020, 1...	CREATE_IN_PROGRESS	Cloud.Network	WP-Network-Private

Bepaalde geschiedenisvermeldingen hebben mogelijk de link **Inrichtingsdiagram** uiterst rechts. Het diagram lijkt op het gesimuleerde diagram, waar u het stroomdiagram van Cloud Assembly-beslissingspunten in het inrichtingsproces controleert.

Er zijn meer stroomdiagrammen beschikbaar onder **Infrastructuur > Activiteit > Aanvragen**.

- 9 Om te controleren of de applicatie werkt, opent u de WordPress-startpagina in een browser.

- a Wacht totdat de WordPress-servers volledig zijn gemaakt en geïnitieerd.

Het kan 30 minuten of langer duren voordat de initialisatie is uitgevoerd, afhankelijk van de omgeving.

- b Ga naar **Resources > Implementaties > Topologie** om de FQDN of het IP-adres van de site te vinden.

- c Klik in het canvas op de WebTier en zoek het IP-adres in het paneel aan de rechterkant.

- d Voer het IP-adres in als onderdeel van de volledige URL naar de WordPress-startpagina.

In dit voorbeeld is de volledige URL:

`http://{IP-address}/mywordpresssite`

of

`http://{IP-address}/mywordpresssite/wp-admin/install.php`

- 10 Als de applicatie nadat u WordPress in een browser hebt bekeken nog moet worden bewerkt, brengt u wijzigingen in de sjabloon aan en implementeert u deze opnieuw onder de optie **Een bestaande implementatie bijwerken**.

- 11 Overweeg om versies van de cloudsjabloon te beheren. U kunt teruggaan naar een werkende versie als de implementatie na een wijziging mislukt.

- a Klik op **Versie** op de ontwerppagina voor cloudsjablonen.

- b Voer **WP-1.0** in op de pagina Versie maken.

Gebruik geen spaties in versienamen.

- c Klik op **Maken**.

Als u versies wilt bekijken of wilt teruggaan naar een versie, klikt u op de ontwerppagina op het tabblad **Versiegeschiedenis**.

- 12 Nu een basisimplementatie mogelijk is, kunt u uw eerste verbeteringen tijdens het implementeren aanbrengen door de CPU en het geheugen op de applicatie- en databaseservers te vergroten.

Update naar een middelgrote knooppuntgrootte voor beide. Gebruik dezelfde sjabloon en selecteer **medium** tijdens het implementeren, implementeer opnieuw en controleer de applicatie nogmaals.

Wat nu te doen

Breid de cloudsjabloon uit naar een productiewaardige applicatie door nog meer resources toe te voegen.

Een cloudsjabloon uitbreiden

Nadat u de Cloud Assembly-basisjabloon hebt gemaakt en getest voor het voorbeeld van de applicatie, kunt u deze uitbreiden naar een applicatie met meerdere lagen die voor ontwikkelings-, test- en uiteindelijk productiedoeleinden kan worden geïmplementeerd.

Om de cloudsjabloon uit te breiden, voegt u de volgende uitbreidingen toe.

- Een optie om applicatieservers te clusteren voor een grotere capaciteit
- Een publiekgericht netwerk en load balancer vóór de applicatieservers
- Een back-upserver met archiefopslag

Voorwaarden

Maak de basiscloudsjabloon en test deze. Zie [Een basiscloudsjabloon maken](#) en [Een basiscloudsjabloon testen](#).

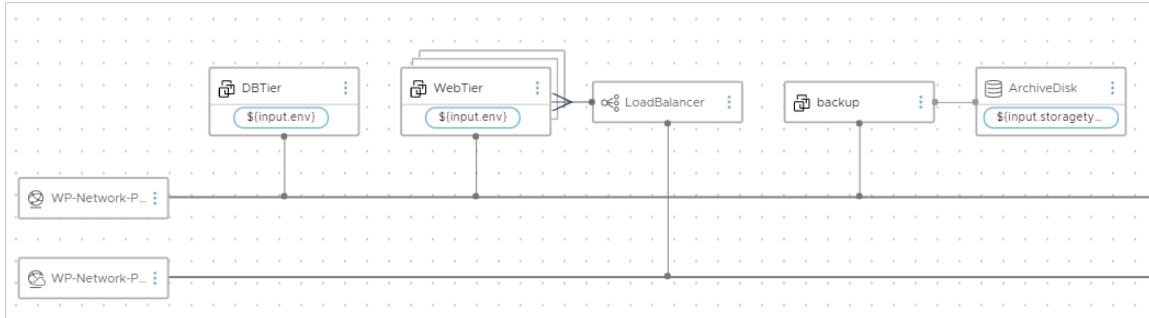
Procedure

- 1 Klik op **Cloudsjablonen** en open de WordPress-BP-cloudsjabloon.
De basissjabloon wordt weergegeven in het ontwerpcanvas en de code-editor.
- 2 Breng toevoegingen en wijzigingen aan met behulp van het codevoorbeeld en de afbeelding.
Gebruik de grafische gebruikersinterface om nieuwe resources, zoals de load balancer, naar het canvas te slepen en voltooi vervolgens de configuratie in de code-editor.
 - a Voeg de invoerprompt `count` toe om de WordPress-applicatieserver in een cluster te brengen.
 - b Voeg een cloudonafhankelijke load balancer toe.
 - c Verbind de load balancer met het WordPress-applicatieservercluster.
 - d Voeg een cloudonafhankelijke back-upmachine toe.
 - e Verbind de back-upmachine met het privé-/interne netwerk.
 - f Voeg een cloudonafhankelijk openbaar/extern netwerk toe.
 - g Verbind de load balancer met het openbare netwerk.
 - h Voeg een cloudonafhankelijk opslagvolume toe voor gebruik als archiefschijf.
 - i Verbind de archiefschijf met de back-upmachine.
 - j Voeg de invoerprompt toe voor de snelheid van de archiefschijf.

3 Implementeer, test en wijzig op dezelfde manier als voor de basiscloudsjabloon.

U kunt bestaande implementaties bijwerken of zelfs nieuwe instanties implementeren zodat u implementaties kunt vergelijken.

Het doel is om een betrouwbare, herhaalbare sjabloon te krijgen die kan worden gebruikt voor productie-implementaties.



Voorbeeld: Voorbeeld van voltooide code voor uitgebreide cloudsjabloon

```
formatVersion: 1
inputs:
  env:
    type: string
    enum:
      - env:dev
      - env:prod
      - env:test
    default: env:dev
    title: Environment
    description: Target Environment
  size:
    type: string
    enum:
      - small
      - medium
      - large
    description: Size of Nodes
    title: Tier Machine Size
  username:
    type: string
    minLength: 4
    maxLength: 20
    pattern: '[a-z]+'
    title: Database Username
    description: Database Username
  userpassword:
    type: string
    pattern: '[a-z0-9A-Z@#]+$'
    encrypted: true
```



```

    title: Database Password
    description: Database Password
  count:
    type: integer
    default: 2
    maximum: 5
    minimum: 2
    title: WordPress Cluster Size
    description: WordPress Cluster Size (Number of Nodes)
  storagetype:
    type: string
    enum:
      - storage:general
      - storage:fast
    description: Archive Storage Disk Type
    title: Archive Disk Type
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      image: ubuntu
      flavor: '${input.size}'
      count: '${input.count}'
      constraints:
        - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
        assignPublicIpAddress: true
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
      packages:
        - apache2
        - php
        - php-mysql
        - libapache2-mod-php
        - mysql-client
        - gcc
        - make
        - autoconf
        - libc-dev
        - pkg-config
        - libmcrypt-dev
        - php-pear
        - php-dev
      runcmd:
        - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
mywordpresssite --strip-components 1
        - i=0; while [ $i -le 10 ]; do mysql --connect-timeout=3 -h $
{DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;
i=$((i+1)); done
        - mysql -u root -pmysqlpassword -h ${DBTier.networks[0].address} -e "create database

```

```

wordpress_blog;"
  - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/mywordpresssite/
wp-config.php
  - pecl channel-update pecl.php.net
  - pecl update-channels
  - pecl install mcrypt
  - sed -i -e s/"define( 'DB_NAME', 'database_name_here' );"/"define( 'DB_NAME',
'wordpress_blog' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_USER', 'username_here' );"/"define( 'DB_USER',
'root' );"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
-e s/"define( 'DB_PASSWORD', 'password_here' );"/"define( 'DB_PASSWORD',
'mysqlpassword' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_HOST', 'localhost' );"/"define( 'DB_HOST', '$
{DBTier.networks[0].address}' );"/ /var/www/html/mywordpresssite/wp-config.php
  - sed -i '950i extension=mcrypt.so' /etc/php/7.4/apache2/php.ini
  - service apache2 reload
DBTier:
  type: Cloud.Machine
  properties:
    name: mysql
    image: ubuntu
    flavor: '${input.size}'
    constraints:
      - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
        assignPublicIpAddress: true
    remoteAccess:
      authentication: usernamePassword
      username: '${input.username}'
      password: '${input.userpassword}'
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
      packages:
        - mysql-server
      runcmd:
        - sed -e '/bind-address/ s/^#*#/' -i /etc/mysql/mysql.conf.d/mysqld.cnf
        - service mysql restart
        - mysql -e "CREATE USER 'root'@'%' IDENTIFIED BY 'mysqlpassword';"
        - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%;'"
        - mysql -e "FLUSH PRIVILEGES;"
    attachedDisks: []
LoadBalancer:
  type: Cloud.LoadBalancer
  properties:
    name: myapp-lb
    network: '${resource["WP-Network-Public"].id}'
    instances:
      - '${WebTier.id}'
    routes:
      - protocol: HTTP
        port: '80'
        instanceProtocol: HTTP

```

```

    instancePort: '80'
    healthCheckConfiguration:
      protocol: HTTP
      port: '80'
      urlPath: /mywordpresssite/wp-admin/install.php
      intervalSeconds: 6
      timeoutSeconds: 5
      unhealthyThreshold: 2
      healthyThreshold: 2
    internetFacing: true
  WP-Network-Private:
    type: Cloud.Network
    properties:
      name: WP-Network-Private
      networkType: existing
  WP-Network-Public:
    type: Cloud.Network
    properties:
      name: WP-Network-Public
      networkType: public
  backup:
    type: Cloud.Machine
    properties:
      name: backup
      flavor: '${input.size}'
      image: ubuntu
      networks:
        - network: '${resource["WP-Network-Private"].id}'
      attachedDisks:
        - source: '${resource.ArchiveDisk.id}'
  ArchiveDisk:
    type: Cloud.Volume
    properties:
      name: ArchiveDisk
      capacityGb: 5
      constraints:
        - tag: '${input.storagetype}'

```

Wat nu te doen

Definieer uw eigen infrastructuur en maak uw eigen cloudsjablonen.

Zie [Hoofdstuk 4 Uw Cloud Assembly-resource-infrastructuur maken](#) en [Hoofdstuk 6 Uw Cloud Assembly-implementaties ontwerpen](#).

Tutorial: VMware Cloud on AWS voor vRealize Automation configureren

Deze tutorial voor vRealize Automation illustreert het proces voor het definiëren van de resource-infrastructuur en cloudsjablooninstellingen voor implementatie in een VMware Cloud on AWS-omgeving.

Voor de procedure is vereist dat een cloudbeheerder het SDDC-datacenter voor VMware Cloud on AWS van uw organisatie al heeft geconfigureerd, zoals beschreven in *Deploying and Managing a Software-Defined Data Center* in de documentatie [VMware Cloud on AWS Getting Started](#).

Bekijk de sequentiële setup om inzicht te krijgen in het proces voor het configureren van uw omgeving voor VMware Cloud on AWS. Houd er rekening mee dat de waarden die u ziet, alleen toepassingsvoorbeelden zijn. Denk er dus goed over na waar u uw eigen vervangingen zou maken, of leid dit af uit de voorbeeldwaarden, om te voldoen aan uw eigen cloudinfrastructuur- en implementatiebehoeften.



Raadpleeg de video [How to Configure VMware Cloud on AWS for Cloud Assembly](#) voor meer informatie.

Procedure

1 Een VMware Cloud on AWS-basiswerkstroom configureren in vRealize Automation

Dit gebruiksscenario toont het proces voor het definiëren van de resource-infrastructuur en een overeenkomstige cloudsjabloon voor implementatie in een VMware Cloud on AWS-omgeving.

2 Een geïsoleerd netwerk in een VMware Cloud on AWS-werkstroom in vRealize Automation configureren

In deze procedure voegt u een geïsoleerd netwerk toe voor uw VMware Cloud on AWS-implementatie in vRealize Automation.

Een VMware Cloud on AWS-basiswerkstroom configureren in vRealize Automation

Dit gebruiksscenario toont het proces voor het definiëren van de resource-infrastructuur en een overeenkomstige cloudsjabloon voor implementatie in een VMware Cloud on AWS-omgeving.

In deze procedure configureert u ook een infrastructuur die de implementatie van cloudsjablonen ondersteunt op resources in uw bestaande VMware Cloud on AWS-omgeving.

Voorwaarden

- Voordat u een VMware Cloud on AWS-cloudaccount in Cloud Assembly kunt maken en configureren, moet u lid zijn van een organisatie in een bestaande VMware Cloud on AWS SDDC-omgeving. Voor informatie over het configureren van de service VMware Cloud on AWS, zie de [documentatie van VMware Cloud on AWS](#).
- Als u de benodigde verbinding tussen uw bestaande host-SDDC van VMware Cloud on AWS in vCenter en een VMware Cloud on AWS-cloudaccount in Cloud Assembly wilt mogelijk

maken, moet u een netwerkverbinding opgeven en firewallregels toevoegen met behulp van een VPN of een soortgelijke netwerkmethod. Zie [Uw SDDC voor VMware Cloud on AWS voorbereiden om verbinding te maken met VMware Cloud on AWS-cloudaccounts in vRealize Automation](#).

Procedure

1 [Uw SDDC voor VMware Cloud on AWS voorbereiden om verbinding te maken met VMware Cloud on AWS-cloudaccounts in vRealize Automation](#)

Wanneer u VMware Cloud on AWS-cloudaccounts in uw vRealize Automation-omgeving gebruikt, moet u een netwerkverbinding maken en regels configureren om de communicatie tussen uw SDDC in vCenter- en VMware Cloud on AWS-cloudaccounts in vRealize Automation te ondersteunen.

2 [Een VMware Cloud on AWS-cloudaccount in vRealize Automation maken in een voorbeeldwerkstroom](#)

In deze stap maakt u een VMware Cloud on AWS-cloudaccount in vRealize Automation.

3 [Een cloudzone voor VMware Cloud on AWS-implementaties in vRealize Automation maken](#)

In deze stap maakt u een cloudzone om een berekeningsresource op te geven die de CloudAdmin-gebruiker kan openen wanneer hij of zij met VMware Cloud on AWS in vRealize Automation werkt.

4 [Netwerk- en opslagprofielen voor VMware Cloud on AWS-implementaties in vRealize Automation configureren](#)

In deze stap configureert u een netwerk- en opslagprofiel om resources op te geven die voor een CloudAdmin-gebruiker van VMware Cloud on AWS in vRealize Automation beschikbaar zijn.

5 [Een project maken om VMware Cloud on AWS-implementaties in vRealize Automation te ondersteunen](#)

In deze stap definieert u een vRealize Automation-project waarmee u kunt bepalen welke resources beschikbaar zijn voor VMware Cloud on AWS-implementaties.

6 [Een vCenter-machineresource in een cloudsjabloonontwerp definiëren om VMware Cloud on AWS-implementatie te ondersteunen in vRealize Automation](#)

In deze stap sleept u een vCenter-machineresource naar een ontwerpcanvas en voegt u instellingen voor een VMware Cloud on AWS-implementatie toe in vRealize Automation.

Uw SDDC voor VMware Cloud on AWS voorbereiden om verbinding te maken met VMware Cloud on AWS-cloudaccounts in vRealize Automation

Wanneer u VMware Cloud on AWS-cloudaccounts in uw vRealize Automation-omgeving gebruikt, moet u een netwerkverbinding maken en regels configureren om de communicatie tussen uw SDDC in vCenter- en VMware Cloud on AWS-cloudaccounts in vRealize Automation te ondersteunen.

Configureer de benodigde verbindingen en regels om SDDC-communicatie te ondersteunen.

Om de vereiste verbinding tussen uw bestaande host-SDDC voor VMware Cloud on AWS in vCenter en een VMware Cloud on AWS-cloudaccount in vRealize Automation mogelijk te maken, moet u een netwerkverbinding tussen de twee elementen opgeven met behulp van een VPN of een soortgelijke netwerkmethod.

- 1 Configureer een VPN-verbinding via het openbare internet of AWS Direct Connect.

Zie *VMware Cloud on AWS Networking and Security* in de [documentatie voor VMware Cloud on AWS](#) voor informatie over het configureren van VPN-connectiviteit met het datacentrum op locatie, evenals het configureren van AWS Direct Connect voor VMware Cloud on AWS.

- 2 Controleer of de vCenter Server FQDN kan worden omgezet op een privé-IP-adres in het beheernetwerk.

Zie informatie over het instellen van het vCenter Server FQDN-omzettingsadres in *VMware Cloud on AWS Networking and Security* in de [documentatie voor VMware Cloud on AWS](#).

- 3 Configureer de vereiste firewallregels.

U moet de firewallregels van de beheergateway in de VMware Cloud on AWS-console van de SDDC configureren om communicatie te ondersteunen. De regels moeten zich in de sectie met firewallregels voor de **beheergateway** bevinden. Maak de firewallregels met de opties op het tabblad **Netwerk en beveiliging** in de SDDC-console.

- Beperk het netwerkverkeer naar ESXi voor HTTPS-services (TCP 443) tot het gedetecteerde IP-adres van de vRealize Automation-appliance/server of het VIP van de vRealize Automation load balancer.
- Beperk het netwerkverkeer naar vCenter voor ICMP-services (alle ICMP), SSO-services (TCP 7444) en HTTPS-services (TCP 443) tot het gedetecteerde IP-adres van de vRealize Automation-appliance/server of het VIP van de vRealize Automation load balancer.
- Beperk het netwerkverkeer naar de NSX-T Manager voor HTTPS-services (TCP 443) tot het gedetecteerde IP-adres van de vRealize Automation-appliance/server of het VIP van de vRealize Automation load balancer.

De vereiste firewallregels worden in de volgende tabel samengevat.

Tabel 2-2. Samenvatting van vereiste firewallregels voor beheergateway

Naam	Bron	Bestemming	Service
vCenter	CIDR-blok van datacenter op locatie	vCenter	Willekeurig (alle verkeer)
vCenter-ping	Willekeurig	vCenter	ICMP (alle ICMP)
NSX Manager	CIDR-blok van datacenter op locatie	NSX Manager	Willekeurig (alle verkeer)
Op locatie naar ESXi-ping	CIDR-blok van datacenter op locatie	Alleen ESXi-beheer	ICMP (alle ICMP)
Op locatie naar de externe console en inrichting van ESXi	CIDR-blok van datacenter op locatie	Alleen ESXi-beheer	TCP 902

Tabel 2-2. Samenvatting van vereiste firewallregels voor beheergateway (vervolg)

Naam	Bron	Bestemming	Service
Op locatie naar SDDC VM	CIDR-blok van datacenter op locatie	CIDR-blok van logisch netwerk van SDDC	Willekeurig (alle verkeer)
SDDC VM naar op locatie	CIDR-blok van logisch netwerk van SDDC	CIDR-blok van datacenter op locatie	Willekeurig (alle verkeer)

Zie *VMware Cloud on AWS Networking and Security* en *VMware Cloud on AWS Operations Guide* in de [documentatie voor VMware Cloud on AWS](#).

Nadat u de vereiste gatewaytoegang en firewallregels hebt geconfigureerd, kunt u doorgaan met het proces voor het maken van een VMware Cloud on AWS-cloudaccount. Zie [Een VMware Cloud on AWS-cloudaccount in vRealize Automation maken in een voorbeeldwerkstroom](#).

Een VMware Cloud on AWS-cloudaccount in vRealize Automation maken in een voorbeeldwerkstroom

In deze stap maakt u een VMware Cloud on AWS-cloudaccount in vRealize Automation.

Zie [VMware Cloud on AWS-documentatie](#) voor gerelateerde informatie.

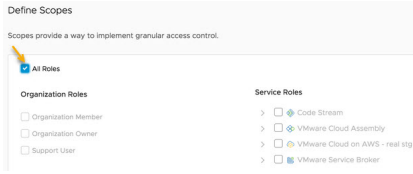
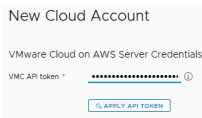
Voorwaarden

- Bij deze procedure wordt ervan uitgegaan dat u over de vereiste beheerdersreferenties beschikt, inclusief CloudAdmin-verificatiegegevens van VMware Cloud on AWS voor het doel-SDDC in vCenter en of u HTTPS-toegang op poort 443 hebt ingeschakeld. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Bij deze procedure wordt ervan uitgegaan dat u de gebruikersrol Cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Als u de benodigde verbinding tussen uw bestaande host-SDDC van VMware Cloud on AWS in vCenter en een VMware Cloud on AWS-cloudaccount in vRealize Automation wilt mogelijk maken, moet u een netwerkverbinding en firewallregels opgeven met behulp van een VPN of een soortgelijke netwerkmethode. Zie [Uw SDDC voor VMware Cloud on AWS voorbereiden om verbinding te maken met VMware Cloud on AWS-cloudaccounts in vRealize Automation](#). Als u een externe HTTP-internetproxy gebruikt, moet deze zijn geconfigureerd voor IPv4.
- Als u geen externe internettoegang hebt, configureert u een internetserverproxy. Zie [Hoe configureer ik een internetproxyserver voor vRealize Automation](#).

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Cloudaccounts**.
- 2 Klik op **Cloudaccount toevoegen**, selecteer VMware Cloud on AWS en voer waarden in.

In de volgende tabel vindt u voorbeeldwaarden en ondersteunende informatie.

Instelling	Voorbeeldwaarde en instructie	Beschrijving
VMC API-token	<ol style="list-style-type: none"> Klik op het help pictogram / aan het einde van de regel VMC API-token en klik op de pagina API-tokens in het helptekstvak om het tabblad API-tokens op de pagina Mijn account van uw organisatie te openen. Klik op Token genereren om de opties Een nieuw API-token genereren weer te geven. Voer een nieuwe tokennaam in, bijvoorbeeld myinitials_mytoken. Stel de TTL van het token in om nooit te verlopen. <p>Als u een token maakt dat is ingesteld op verlopen, werken de VMware Cloud on AWS-bewerkingen van vRealize Automation niet meer wanneer het token verloopt en werken deze niet totdat u het cloudaccount met een nieuw token bijwerkt.</p> <ol style="list-style-type: none"> Selecteer Alle rollen in het gedeelte Bereiken definiëren.  <ol style="list-style-type: none"> Klik op Genereren. Klik op de pagina met het gegenereerde token op Kopiëren en klik op Doorgaan. Ga terug naar de pagina Nieuw cloudaccount, plak het gekopieerde token op de rij VMC API-token en klik op API-token toepassen. 	<p>U kunt een nieuwe token maken of een bestaande token voor uw organisatie gebruiken op de gekoppelde pagina API-tokens.</p> <p>In het gedeelte Bereiken definiëren zijn de minimaal vereiste rollen voor het API-token:</p> <ul style="list-style-type: none"> ■ Organisatirollen <ul style="list-style-type: none"> ■ Organisatielid ■ Organisatie-eigenaar ■ Servicerollen - VMware Cloud on AWS <ul style="list-style-type: none"> ■ Beheerder ■ NSX Cloud-beheerder ■ NSX Cloud-auditor <p>Opmerking Het gegenereerde token kopiëren, downloaden of afdrucken. Wanneer u deze pagina verlaat, kunt u het gegenereerde token niet ophalen.</p> <p>Pas het gegenereerde of opgegeven token toe om verbinding te maken met de beschikbare SDDC-omgeving in het VMware Cloud on AWS-abonnement van uw organisatie en vul de lijst met SDDC-namen in.</p> <p>Als de vRealize Automation- en VMware Cloud on AWS-services zich in verschillende organisaties bevinden, moet u overschakelen naar de VMware Cloud on AWS-organisatie en vervolgens het token genereren.</p> <p>Zie API-tokens genereren voor meer informatie over API-tokens.</p>
SDDC-naam	<p>Selecteer Datacenter:Datacenter-abz voor dit voorbeeld.</p> <p>De geldige SDDC-naam wordt automatisch ingevuld voor de FQDN-vermeldingen van vCenter en NSX-T. Als een cloudproxy al in de SDDC is geïmplementeerd, wordt de cloudproxywaarde ook automatisch ingevuld.</p>	<p>Selecteer uit de lijst met beschikbare SDDC's van uw VMware Cloud on AWS-abonnement. De lijst met SDDC's is gebaseerd op het API-token van VMware Cloud on AWS.</p> <p>NSX-V SDDC's worden niet ondersteund met vRealize Automation en worden niet weergegeven in de lijst met beschikbare SDDC's.</p>

Instelling	Voorbeeldwaarde en instructie	Beschrijving
IP-adres/FQDN van vCenter	Het adres wordt automatisch ingevuld op basis van uw SDDC-selectie.	Voer het IP-adres of de FQDN van vCenter Server in de opgegeven SDDC in. Het IP-adres wordt standaard ingesteld op het privé IP-adres. Op basis van het type netwerkconnectiviteit dat wordt gebruikt om toegang te krijgen tot uw SDDC kan het standaardadres afwijken van het IP-adres van de NSX Manager-server in het opgegeven SDDC.
IP-adres/FQDN van NSX Manager	Het adres wordt automatisch ingevuld op basis van uw SDDC-selectie.	Geeft het IP-adres of de FQDN van NSX Manager op in de opgegeven SDDC. Het IP-adres wordt standaard ingesteld op het privé IP-adres. Op basis van het type netwerkconnectiviteit dat wordt gebruikt om toegang te krijgen tot uw SDDC kan het standaardadres afwijken van het IP-adres van de NSX Manager-server in het opgegeven SDDC. VMware Cloud on AWS ondersteuning voor cloudaccounts NSX-T.
vCenter-gebruikersnaam en -wachtwoord	De gebruikersnaam wordt automatisch als cloudadmin@vmc.local ingevuld.	Voer uw vCenter-gebruikersnaam voor de opgegeven SDDC in als deze anders is dan de standaardwaarde. Voor de opgegeven gebruiker zijn CloudAdmin-verificatiegegevens vereist. De gebruiker heeft geen CloudGlobalAdmin-verificatiegegevens nodig. Voer het gebruikerswachtwoord in.
Valideren	Klik op Valideren . Als u een <code>Error updating endpoint <naam>: Endpoint already exists</code> ontvangt, is er al een cloudaccount gekoppeld aan dat SDDC.	De validatieactie bevestigt uw toegangsrechten voor de opgegeven vCenter en controleert of de vCenter wordt uitgevoerd.
Naam en beschrijving	Voer OurCo-VMC in voor de naam van het cloudaccount. Voer Sample deployment for VMC in voor de beschrijving van het cloudaccount.	
Inrichting in deze datacenters toestaan	Deze informatie is alleen-lezen.	Geeft beschikbare datacenters in uw opgegeven SDDC-omgeving van VMware Cloud on AWS weer.

Instelling	Voorbeeldwaarde en instructie	Beschrijving
Een cloudzone maken	Schakel het selectievakje uit. Voor dit voorbeeld maakt u later in de werkstroom een cloudzone.	Zie Meer informatie over Cloud Assembly-cloudzones .
Mogelijkheidstags	Laat dit leeg. Deze werkstroom gebruikt geen capaciteitstags.	Gebruik tags volgens de tagstrategie van uw organisatie. Zie Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren en Een tagstrategie maken .

Zoals met VM's die zijn geïmplementeerd op vSphere, kunt u machinetags configureren voor een VM die op VMware Cloud on AWS moet worden geïmplementeerd. U kunt de machinetag ook bijwerken na de eerste implementatie. Met deze machinetags kan vRealize Automation dynamisch een VM toewijzen aan een geschikte NSX-T-beveiligingsgroep tijdens de implementatie. Zie [Meer informatie over beveiligingsgroep- en tagresources in vRealize Automation-cloudsjablonen](#) voor gerelateerde informatie.

3 Klik op **Toevoegen**.

Resultaten

Voor resources zoals machines en volumes worden gegevens uit het VMware Cloud on AWS-SDDC-datacentrum verzameld en deze resources worden in het gedeelte **Resources** van vRealize Automation op het tabblad **Infrastructuur** weergegeven.

Wat nu te doen

[Een cloudzone voor VMware Cloud on AWS-implementaties in vRealize Automation maken.](#)

Een cloudzone voor VMware Cloud on AWS-implementaties in vRealize Automation maken

In deze stap maakt u een cloudzone om een berekeningsresource op te geven die de CloudAdmin-gebruiker kan openen wanneer hij of zij met VMware Cloud on AWS in vRealize Automation werkt.

In VMware Cloud on AWS zijn de verificatiegegevens voor de primaire beheerders: CloudGlobalAdmin en CloudAdmin. Cloud Assembly is ontworpen om de CloudAdmin-gebruiker te ondersteunen. Implementeer naar resources die voor een VMware Cloud on AWS CloudAdmin-gebruiker beschikbaar zijn. Implementeer niet naar resources waarvoor VMware Cloud on AWS CloudGlobalAdmin-verificatiegegevens zijn vereist.

Cloudzones identificeren de computerbronnen waarop een projectcloudsjabloon machines, netwerken en opslag implementeert. Zie [Meer informatie over Cloud Assembly-cloudzones](#).

Tenzij anders vermeld, zijn de stapwaarden die u in deze procedure invoert alleen bedoeld voor deze voorbeeldwerkstroom.

Voorwaarden

- Voltooi de procedure [Een VMware Cloud on AWS-cloudaccount in vRealize Automation maken in een voorbeeldwerkstroom](#).
- Bij deze procedure wordt ervan uitgegaan dat u over de vereiste verificatiegegevens als beheerder beschikt, inclusief VMware Cloud on AWS CloudAdmin-verificatiegegevens voor de doel-SDDC in vCenter. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Bij deze procedure wordt ervan uitgegaan dat u de gebruikersrol Cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).

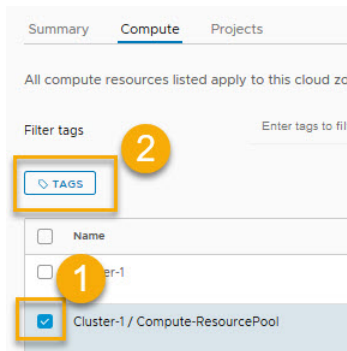
Procedure

- 1 Selecteer **Infrastructuur > Configureren > Cloudzones**.
- 2 Klik op **Nieuwe cloudzone** en voer waarden in voor de VMware Cloud on AWS-omgeving.

Instelling	Voorbeeldwaarde
Account/regio	OurCo-VMC/Datacenter:Datacenter-abz Dit is het cloudaccount en de gekoppelde regio die u heeft gedefinieerd in de vorige stap, Een VMware Cloud on AWS-cloudaccount in vRealize Automation maken in een voorbeeldwerkstroom .
Naam	VMC_cloud_zone-1
Beschrijving	Alleen VMware Cloud on AWS-resources
Plaatsingsbeleid	Standaard
Mogelijkheidstags	Laat dit leeg. Deze werkstroom gebruikt geen capaciteitstags.

- 3 Klik op het tabblad **Berekenen**.
- 4 Zoek en selecteer een berekeningsresource die beschikbaar is voor de CloudAdmin-gebruiker, zoals hieronder in gebied 1. Gebruik voor dit voorbeeld de resource met de naam `Cluster 1/ Compute-ResourcePool`.

`Cluster 1/ Compute-ResourcePool` is de standaardberekeningsresource voor VMware Cloud on AWS.

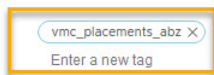


- 5 Voeg de tagnaam `vmc_placements_abz` toe, zoals in gebied 2 hierboven.

Tags

1 object(s) selected

Add tags



Remove tags

no tags ⓘ

- 6 Filter de berekeningsresources die in deze cloudzone worden gebruikt, door `vmc_placements_abz` in het gedeelte **Tags filteren** in te voeren.

- 7 Klik op **Opslaan**.

<input type="checkbox"/>	Name	Account / region	Type	Tags
<input type="checkbox"/>	Cluster-1		Cluster	
<input checked="" type="checkbox"/>	Cluster-1 / Compute-ResourcePool	OurCo-VMC / SDDC_test1_abz	ResourcePool	vmc_placements_abz
<input type="checkbox"/>	Cluster-1 / Mgmt-ResourcePool		ResourcePool	

Voor dit voorbeeld is alleen de berekeningsresource met de naam `Cluster 1/ Compute-ResourcePool` beschikbaar voor de CloudAdmin-gebruiker.

Wat nu te doen

[Netwerk- en opslagprofielen voor VMware Cloud on AWS-implementaties in vRealize Automation configureren.](#)

Netwerk- en opslagprofielen voor VMware Cloud on AWS-implementaties in vRealize Automation configureren

In deze stap configureert u een netwerk- en opslagprofiel om resources op te geven die voor een CloudAdmin-gebruiker van VMware Cloud on AWS in vRealize Automation beschikbaar zijn.

Hoewel er ook een image en een soortwaarde nodig zijn, is er niets uniek aan dat specifiek is voor de verificatiegegevens van VMware Cloud on AWS-gebruikers. Voor dit voorbeeld gebruikt u de soortwaarde `small` en de imagewaarde `ubuntu-16` wanneer u de cloudsjabloon definieert.

Zie [Hoofdstuk 4 Uw Cloud Assembly-resource-infrastructuur maken](#) voor algemene informatie over toewijzingen en profielen.

Tenzij anders vermeld, zijn de stapwaarden die u in deze procedure invoert alleen bedoeld voor deze voorbeeldwerkstroom.

Voorwaarden

- Maak een cloudzone. Zie [Een cloudzone voor VMware Cloud on AWS-implementaties in vRealize Automation maken](#).
- Bij deze procedure wordt ervan uitgegaan dat u over de vereiste verificatiegegevens als beheerder beschikt, inclusief VMware Cloud on AWS CloudAdmin-verificatiegegevens voor de doel-SDDC in vCenter. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Bij deze procedure wordt ervan uitgegaan dat u de gebruikersrol Cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).

Procedure

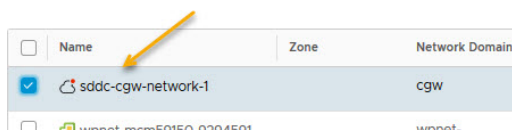
- 1 Definieer een netwerkprofiel voor VMware Cloud on AWS-implementaties.

- a Selecteer **Infrastructuur > Configureren > Netwerkprofielen** en klik op **Nieuw netwerkprofiel**.

Instelling	Voorbeeldwaarde
Account/regio	OurCo-VMC/Datacenter:Datacenter-abz Opmerking Selecteer het VMware Cloud on AWS-cloudaccount en het overeenkomstige SDDC-datacenter dat u in Een VMware Cloud on AWS-cloudaccount in vRealize Automation maken in een voorbeeldwerkstroom hebt gemaakt.
Naam	vmc-network1
Beschrijving	Bevat netwerken die toegankelijk zijn voor cloudsjabloonbeheerders die CloudAdmin-verificatiegegevens voor VMware Cloud on AWS hebben.

- b Klik op het tabblad **Netwerk** en klik vervolgens op **Netwerk toevoegen**.
 - c Selecteer een netwerk waarin een VMware Cloud on AWS-gebruiker met CloudAdmin-verificatiegegevens kan implementeren, bijvoorbeeld `sddc-cgw-network-1`.

Add Network



- 2 Sla het netwerkprofiel op.

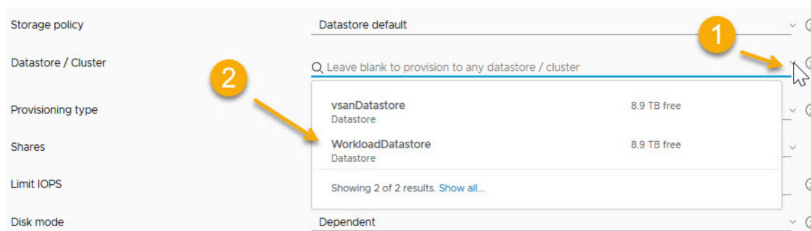
3 Definieer een opslagprofiel voor VMware Cloud on AWS-implementaties.

Configureer een opslagprofiel dat een gegevensopslag/cluster als doel heeft dat toegankelijk is voor de CloudAdmin-gebruiker.

- a Selecteer **Infrastructuur > Configureren > Opslagprofielen** en klik op **Nieuw opslagprofiel**.

Instelling	Voorbeeldwaarde
Account/regio	OurCo-VMC/Datacenter:Datacenter-abz Selecteer het VMware Cloud on AWS-cloudaccount en het overeenkomstige SDDC-datacenter dat u in Een VMware Cloud on AWS-cloudaccount in vRealize Automation maken in een voorbeeldwerkstroom hebt gemaakt.
Naam	vmc-storage1
Beschrijving	Bevat het gegevensopslagcluster waarop kan worden geïmplementeerd door cloudsjabloonbeheerders die CloudAdmin-verificatiegegevens voor VMware Cloud on AWS hebben.

- b Selecteer in de vervolgkeuzelijst **Gegevensopslag/cluster** de gegevensopslag **WorkloadDatastore**.



Voor VMware Cloud on AWS in Cloud Assembly moet het opslagbeleid de gegevensopslag **WorkloadDatastore** gebruiken om een VMware Cloud on AWS-implementatie te ondersteunen.

4 Sla het opslagprofiel op.

Wat nu te doen

[Een project maken om VMware Cloud on AWS-implementaties in vRealize Automation te ondersteunen.](#)

Een project maken om VMware Cloud on AWS-implementaties in vRealize Automation te ondersteunen

In deze stap definieert u een vRealize Automation-project waarmee u kunt bepalen welke resources beschikbaar zijn voor VMware Cloud on AWS-implementaties.

Zie [Hoe werken Cloud Assembly-projecten tijdens het implementeren](#) voor informatie over projecten.

Tenzij anders vermeld, zijn de stapwaarden die u in deze procedure invoert alleen bedoeld voor deze voorbeeldwerkstroom.

Voorwaarden

- Voltooi de procedure [Netwerk- en opslagprofielen voor VMware Cloud on AWS-implementaties in vRealize Automation configureren](#).
- Bij deze procedure wordt ervan uitgegaan dat u over de vereiste verificatiegegevens als beheerder beschikt, inclusief VMware Cloud on AWS CloudAdmin-verificatiegegevens voor de doel-SDDC in vCenter. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Bij deze procedure wordt ervan uitgegaan dat u de gebruikersrol Cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).

Procedure

- 1 Selecteer **Infrastructuur > Beheer > Projecten**.
- 2 Klik op **Nieuw project** en voer de projectnaam `VMC_proj-1_abz` in.
- 3 Klik op **Gebruikers** en klik vervolgens op **Gebruikers toevoegen**.

De gebruikers hebben CloudAdmin-verificatiegegevens nodig voor het VMware Cloud on AWS-abonnement van hun organisatie.

- `chris.gray@ourco.com`, Beheerder
- `kerry.white@ourco.com`, Lid

- 4 Klik op **Inrichting** en klik vervolgens op **Cloudzone toevoegen**.
- 5 Voeg de cloudzone toe die u in de vorige stap hebt geconfigureerd.

Instelling	Voorbeeldwaarde
Cloudzone	VMC_cloud_zone-1 U heeft deze cloudzone gemaakt in de vorige stap, Een cloudzone voor VMware Cloud on AWS-implementaties in vRealize Automation maken .
Inrichtingsprioriteit	1
Limiet voor instanties	3

- 6 Negeer de overige opties voor dit voorbeeld.

Wat nu te doen

Maak een cloudsjablonen om in uw VMware Cloud on AWS-omgeving te implementeren. Zie [Een vCenter-machineresource in een cloudsjabloonontwerp definiëren om VMware Cloud on AWS-implementatie te ondersteunen in vRealize Automation](#).

Een vCenter-machineresource in een cloudsjabloonontwerp definiëren om VMware Cloud on AWS-implementatie te ondersteunen in vRealize Automation

In deze stap sleept u een vCenter-machineresource naar een ontwerpcanvas en voegt u instellingen voor een VMware Cloud on AWS-implementatie toe in vRealize Automation.

Maak een cloudsjabloonontwerp dat u op beschikbare VMware Cloud on AWS-resources kunt implementeren.

Tenzij anders vermeld, zijn de stapwaarden die u in deze procedure invoert alleen bedoeld voor deze voorbeeldwerkstroom.

Voorwaarden

- Bij deze procedure wordt ervan uitgegaan dat u verificatiegegevens voor de cloudsjabloonontwerper hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Bij deze procedure wordt ervan uitgegaan dat u over CloudAdmin-verificatiegegevens van VMware Cloud on AWS beschikt voor het doel-SDDC in vCenter (Datacenter:Datacenter-abz). Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Configureer de resource-infrastructuur en het project zoals beschreven in de voorgaande gedeelten.

Procedure

- 1 Klik op het tabblad **Ontwerp** en klik vervolgens op **Nieuw**.

Instelling	Voorbeeldwaarde
Naam	vmc-bp_abz
Beschrijving	1
Project	VMC_proj-1_abz Dit is het project dat u eerder hebt gemaakt en de cloudzone ondersteunt die u ook eerder hebt gemaakt. Het project is nu aan de cloudzone gekoppeld, die zelf aan het cloudaccount en de regio van VMware Cloud on AWS is gekoppeld die u eerder heeft gemaakt.

- 2 Sleep een vSphere-machineresource naar het canvas.
- 3 Bewerk de volgende (vetgedrukte) cloudsjabloonresourcecode in de machineresource.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
```



```
image: ubuntu-1604
cpuCount: 1
totalMemoryMB: 1024
folderName: Workloads
```

De `image` kan elke waarde zijn die geschikt is voor uw implementatiebehoeften.

U moet de instructie `folderName: Workloads` aan de cloudsjabloonontwerpcodes toevoegen om een VMware Cloud on AWS-implementatie te ondersteunen. De instelling `folderName: Workloads` ondersteunt de CloudAdmin-verificatiegegevens in de SDDC-omgeving van VMware Cloud on AWS en is vereist.

Opmerking: hoewel de instelling `folderName: Workloads` in bovenstaand codevoorbeeld is vereist, kunt u deze direct toevoegen aan de cloudsjablooncode zoals hierboven is aangegeven of kunt u deze toevoegen in de gekoppelde cloudzone of het project. Als de instelling op meer dan een van deze drie plaatsen is opgegeven, is de prioriteit als volgt:

- De projectinstelling heeft voorrang op de ontwerpinstelling van de cloudsjabloon en de instelling voor de cloudzone.
- De instelling voor de cloudsjabloon overschrijft de instelling voor de cloudzone.

Opmerking: u kunt desgewenst de instellingen `cpuCount` en `totalMemoryMB` vervangen door een vermelding voor `flavor` (grootte), zoals hieronder wordt weergegeven:

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: ubuntu-1604
      flavor: small
      folderName: Workloads
```

Als de mapwaarde in de cloudzone is ingesteld op **Workloads**, hoeft u de `folderName`-eigenschap niet in te stellen in de cloudsjabloon, tenzij u de mapwaarde voor de cloudzone wilt overschrijven.

Wat nu te doen

Vouw deze basiswerkstroom van VMware Cloud on AWS uit door netwerkisolatie toe te voegen. Zie [Een geïsoleerd netwerk in een VMware Cloud on AWS-werkstroom in vRealize Automation configureren](#).

Een geïsoleerd netwerk in een VMware Cloud on AWS-werkstroom in vRealize Automation configureren

In deze procedure voegt u een geïsoleerd netwerk toe voor uw VMware Cloud on AWS-implementatie in vRealize Automation.

Wanneer u uw VMware Cloud on AWS-cloudaccount definieert, zijn de NSX-T-instellingen beschikbaar die in uw VMware Cloud on AWS-service zijn geconfigureerd. Zie de [productdocumentatie](#) voor VMware Cloud on AWS voor informatie over het configureren van NSX-T-instellingen in uw VMware Cloud on AWS-service.

vRealize Automation ondersteunt VMware Cloud on AWS met NSX-T. VMware Cloud on AWS met NSX-V wordt niet ondersteund.

vRealize Automation ondersteunt netwerkisolatie voor VMware Cloud on AWS-implementaties. Er worden geen andere netwerkmethoden voor VMware Cloud on AWS ondersteund.

Deze uitbreiding van de VMware Cloud on AWS-basiswerkstroom beschrijft de volgende methoden voor het maken van een geïsoleerd netwerk voor gebruik in uw cloudsjabloon:

- Configureer netwerkgebaseerde isolatie op aanvraag.
- Configureer beveiligingsgroepgebaseerde isolatie op aanvraag.

Voorwaarden

Deze procedure zorgt voor een uitbreiding van de VMware Cloud on AWS-basiswerkstroom. Deze gebruikt uw cloudaccount en -regio, cloudzone, project en netwerkprofiel die u allemaal eerder in de [Tutorial: VMware Cloud on AWS voor vRealize Automation configureren](#)-werkstroom hebt geconfigureerd.

Procedure

1 Een geïsoleerd netwerk voor een VMware Cloud on AWS-implementatie in vRealize Automation definiëren

U kunt de netwerkisolatie voor een VMware Cloud on AWS-implementatie configureren met behulp van een van de volgende procedures:

2 Een netwerkonderdeel in een cloudsjabloon definiëren om netwerkisolatie voor VMware Cloud on AWS in vRealize Automation te ondersteunen

In deze stap sleept u een netwerkmachineonderdeel naar een cloudsjablooncanvas van vRealize Automation en voegt u instellingen voor een geïsoleerde netwerkimplementatie toe aan uw VMware Cloud on AWS-doelomgeving.

Een geïsoleerd netwerk voor een VMware Cloud on AWS-implementatie in vRealize Automation definiëren

U kunt de netwerkisolatie voor een VMware Cloud on AWS-implementatie configureren met behulp van een van de volgende procedures:

- [Isolatie op basis van on-demand netwerk in vRealize Automation configureren](#)
- [Isolatie op basis van on-demand beveiligingsgroep in vRealize Automation configureren](#)

Isolatie op basis van on-demand netwerk in vRealize Automation configureren

U kunt de netwerkisolatie voor uw VMware Cloud on AWS-implementatiebehoeften configureren door instellingen voor netwerken op aanvraag op te geven en in een netwerkprofiel te gebruiken.

U kunt een geïsoleerd netwerk opgeven met behulp van een beveiligingsgroep of met behulp van de instellingen voor een on-demand netwerk. In dit voorbeeld configureert u netwerkisolatie door instellingen voor on-demand netwerken in het netwerkprofiel op te geven. Later opent u het netwerk in een cloudsjabloon en gebruikt u de cloudsjabloon in een VMware Cloud on AWS-implementatie.

Tenzij anders vermeld, zijn de stapwaarden die u in deze procedure invoert alleen bedoeld voor deze voorbeeldwerkstroom.

Voorwaarden

- Voltooi de werkstroom [Een VMware Cloud on AWS-basiswerkstroom configureren in vRealize Automation](#).
- Bekijk [Een geïsoleerd netwerk in een VMware Cloud on AWS-werkstroom in vRealize Automation configureren](#).
- Bij deze procedure wordt ervan uitgegaan dat u over de vereiste verificatiegegevens als beheerder beschikt, inclusief VMware Cloud on AWS CloudAdmin-verificatiegegevens voor de doel-SDDC in vCenter. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Bij deze procedure wordt ervan uitgegaan dat u de gebruikersrol Cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).

Procedure

- 1 Open het netwerkprofiel dat u heeft gebruikt in de basiswerkstroom van VMware Cloud on AWS, bijvoorbeeld `vmc-network1`. Zie [Netwerk- en opslagprofielen voor VMware Cloud on AWS-implementaties in vRealize Automation configureren](#).
- 2 U hoeft niets te selecteren op het tabblad **Netwerken**.
- 3 Klik op het tabblad **Netwerkbeleid**.
- 4 Selecteer de optie **Een on-demand netwerk maken** en selecteer het standaardnetwerkdomein `cgw`. Geef een geschikte CIDR en subnetgrootte op.
- 5 Klik op **Opslaan**.

Wanneer u dit netwerkprofiel gebruikt, worden machines in een netwerk in het standaardnetwerkdomein geïmplementeerd. Het netwerk wordt met behulp van privé- of uitgaande netwerktoegang geïsoleerd van andere netwerken.

Wat nu te doen

Configureer een netwerkonderdeel in uw cloudsjabloon. Zie [Een netwerkonderdeel in een cloudsjabloon definiëren om netwerkisolatie voor VMware Cloud on AWS in vRealize Automation te ondersteunen](#).

Isolatie op basis van on-demand beveiligingsgroep in vRealize Automation configureren

U kunt de netwerkisolatie voor uw VMware Cloud on AWS-implementatiebehoeften configureren door een beveiligingsgroep op aanvraag op te geven en in een netwerkprofiel te gebruiken.

U kunt een geïsoleerd netwerk opgeven met behulp van een beveiligingsgroep of met behulp van de instellingen voor een on-demand netwerk. In dit voorbeeld configureert u netwerkisolatie door een on-demand beveiligingsgroep in het netwerkprofiel op te geven. Later geeft u het netwerk in een cloudsjabloon op en gebruikt u de cloudsjabloon in een VMware Cloud on AWS-implementatie.

Tenzij anders vermeld, zijn de stapwaarden die u in deze procedure invoert alleen bedoeld voor deze voorbeeldwerkstroom.

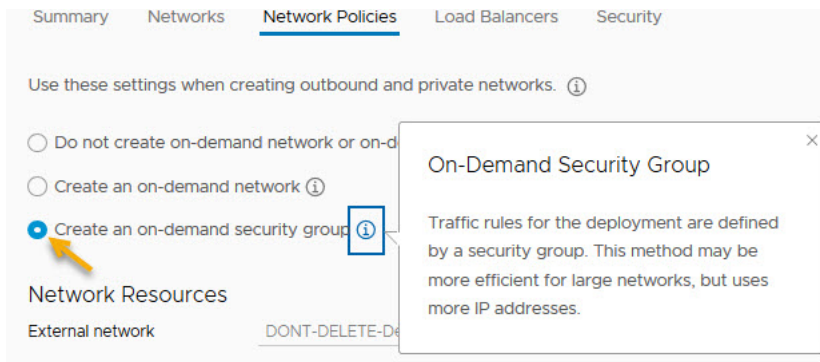
Voorwaarden

- Voltooi de werkstroom [Een VMware Cloud on AWS-basiswerkstroom configureren in vRealize Automation](#).
- Bekijk [Een geïsoleerd netwerk in een VMware Cloud on AWS-werkstroom in vRealize Automation configureren](#).
- Bij deze procedure wordt ervan uitgegaan dat u over de vereiste verificatiegegevens als beheerder beschikt, inclusief VMware Cloud on AWS CloudAdmin-verificatiegegevens voor de doel-SDDC in vCenter. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Bij deze procedure wordt ervan uitgegaan dat u de gebruikersrol Cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).

Procedure

- 1 Open het netwerkprofiel dat u heeft gebruikt in de basiswerkstroom van VMware Cloud on AWS, bijvoorbeeld `vmc-network1`. Zie [Netwerk- en opslagprofielen voor VMware Cloud on AWS-implementaties in vRealize Automation configureren](#).
- 2 Selecteer het bestaande netwerk dat u heeft gebruikt in de basiswerkstroom van VMware Cloud on AWS, bijvoorbeeld `sddc-cgw-network-1`. Zie [Netwerk- en opslagprofielen voor VMware Cloud on AWS-implementaties in vRealize Automation configureren](#).
- 3 Klik op het tabblad **Netwerkbeleid**.

4 Selecteer de optie **Een on-demand beveiligingsgroep maken**.



5 Klik op **Opslaan**.

Wanneer u dit netwerkprofiel gebruikt, worden machines in het geselecteerde netwerk geïmplementeerd en worden deze door een nieuw beveiligingsgroepsbeleid geïsoleerd. Het nieuwe beveiligingsbeleid staat privé- of uitgaande netwerktoegang toe.

Wat nu te doen

Configureer een netwerkonderdeel in uw cloudsjabloon. Zie [Een netwerkonderdeel in een cloudsjabloon definiëren om netwerkisolatie voor VMware Cloud on AWS in vRealize Automation te ondersteunen](#).

Een netwerkonderdeel in een cloudsjabloon definiëren om netwerkisolatie voor VMware Cloud on AWS in vRealize Automation te ondersteunen

In deze stap sleept u een netwerkmachineonderdeel naar een cloudsjablooncanvas van vRealize Automation en voegt u instellingen voor een geïsoleerde netwerkimplementatie toe aan uw VMware Cloud on AWS-doelomgeving.

Voeg netwerkisolatie toe aan de cloudsjabloon die u eerder hebt gemaakt. De cloudsjabloon is al gekoppeld aan een project en een cloudzone die de implementatie in uw VMware Cloud on AWS-omgeving ondersteunen, alsook aan het netwerkprofiel en het netwerk die u voor isolatie hebt geconfigureerd.

Tenzij anders vermeld, zijn de stapwaarden die u in deze procedure invoert alleen bedoeld voor deze voorbeeldwerkstroom.

Voorwaarden

- Voltooi de procedure [Isolatie op basis van on-demand beveiligingsgroep in vRealize Automation configureren](#) of [Isolatie op basis van on-demand netwerk in vRealize Automation configureren](#).
- Bij deze procedure wordt ervan uitgegaan dat u verificatiegegevens voor de cloudsjabloonontwerper hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).

- Bij deze procedure wordt ervan uitgegaan dat u over CloudAdmin-verificatiegegevens voor VMware Cloud on AWS beschikt voor de doel-SDDC in vCenter. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).

Procedure

- 1 Open de cloudsjabloon die u in de vorige werkstroom hebt gemaakt. Zie [Een vCenter-machineresource in een cloudsjabloonontwerp definiëren om VMware Cloud on AWS-implementatie te ondersteunen in vRealize Automation](#).
- 2 Sleep een netwerkonderdeel vanuit de onderdelen aan de linkerkant van de ontwerppagina voor cloudsjablonen naar het canvas.
- 3 Bewerk de YAML-code van het netwerkonderdeel om het netwerktype `private` of `outbound` op te geven, zoals in het vet wordt weergegeven.

```
resources: Cloud_Network_1:
  type: Cloud.Network
  properties:
    name: vmc_isolated
    networkType: private
```

OF

```
resources: Cloud_Network_1:
  type: Cloud.Network
  properties:
    name: vmc_isolated
    networkType: outbound
```

Wat nu te doen

U bent klaar om de cloudsjabloon te implementeren of te sluiten.

Tutorial: Een providerspecifieke externe IPAM-integratie voor vRealize Automation configureren

U kunt een externe IPAM-provider gebruiken om IP-adrestoewijzingen voor uw cloudsjabloonimplementaties te beheren. In deze tutorial wordt beschreven hoe u externe IPAM-integratie in vRealize Automation configureert met behulp van Infoblox als externe IPAM-provider.

In deze procedure gebruikt u een bestaand IPAM-providerpakket, in dit geval een Infoblox-pakket, en een bestaande uitvoeringsomgeving om een providerspecifiek IPAM-integratiepunt te bouwen. U configureert een bestaand netwerk en maakt een netwerkprofiel ter ondersteuning van de toewijzing van IP-adressen van de externe IPAM-provider. Tot slot maakt u een cloudsjabloon die wordt gekoppeld aan het netwerk en netwerkprofiel en implementeert u netwerkmachines met IP-waarden die zijn verkregen van de externe IPAM-provider.

Informatie over het verkrijgen en configureren van het IPAM-providerpakket en het configureren van een uitvoeringsomgeving die een clouduitbreidbaarheidsproxy opent om de integratie van de IPAM-provider te ondersteunen, wordt als referentie opgenomen.

De waarden die u in deze voorbeeldwerkstroom ziet, zijn voorbeeldwaarden. U kunt deze waarden niet identiek overnemen in uw omgeving. Denk er dus goed over na waar u uw eigen vervangingen zou maken om te voldoen aan de behoeften van uw organisatie.



Als u wilt verwijzen naar een soortgelijk vRealize Automation-scenario dat een Infoblox IPAM-integratiewerkstroom in een video-indeling illustreert, raadpleegt u [Infoblox IPAM Plug-in Integration met vRealize Automation / vRealize Automation Cloud](#).

Procedure

1 Vereiste uitbreidbaarheidskenmerken in de Infoblox-applicatie toevoegen voor integratie met vRealize Automation

Voordat u het pakket van de Infoblox-provider (`Infoblox.zip`) kunt downloaden en implementeren voor integratie met vRealize Automation vanaf de Infoblox-website of via de VMware Marketplace, moet u de vereiste uitbreidbaarheidskenmerken toevoegen in Infoblox.

2 Een extern IPAM-providerpakket downloaden en implementeren voor gebruik in vRealize Automation

Voordat u een extern IPAM-integratiepunt in vRealize Automation kunt definiëren, hebt u een geconfigureerd IPAM-providerpakket nodig.

3 Een uitvoeringsomgeving voor een IPAM-integratiepunt maken in vRealize Automation

Voordat u een extern IPAM-integratiepunt in vRealize Automation kunt definiëren, moet u een bestaande uitvoeringsomgeving maken of gebruiken om als intermediair tussen de IPAM-provider en vRealize Automation te fungeren. De uitvoeringsomgeving is vaak een Amazon Web Services- of Microsoft Azure-cloudaccount of een integratiepunt op locatie voor actiegebaseerde uitbreidbaarheid dat is gekoppeld aan een clouduitbreidbaarheidsproxy.

4 Een extern IPAM-integratiepunt voor Infoblox toevoegen in vRealize Automation

vRealize Automation ondersteunt integratie met een externe IPAM-provider. In dit voorbeeld wordt Infoblox als externe IPAM-provider gebruikt.

5 Configureer een netwerk en netwerkprofiel voor het gebruik van externe IPAM voor een bestaand netwerk in vRealize Automation

U kunt een bestaand netwerk definiëren om IP-adreswaarden te gebruiken die worden opgehaald van en beheerd door een externe IPAM-provider in plaats van intern via vRealize Automation.

6 Een cloudsjabloon definiëren en implementeren die gebruikmaakt van een bereiktoewijzing van een externe IPAM-provider in vRealize Automation

U kunt een cloudsjabloon definiëren om IP-adrestoewijzingen van uw externe IPAM-provider te krijgen en te beheren. In dit voorbeeld wordt Infoblox als externe IPAM-provider gebruikt.

7 [Infoblox-specifieke eigenschappen en uitbreidbaarheidskenmerken voor IPAM-integraties in vRealize Automation-cloudsjablonen gebruiken](#)

U kunt Infoblox-specifieke eigenschappen gebruiken voor vRealize Automation-projecten die externe IPAM-integraties voor Infoblox bevatten.

8 [De verzameling van netwerkgegevens beheren met behulp van Infoblox-filters in vRealize Automation](#)

Voor Infoblox kunt u het aantal netwerken waarvoor gegevens worden verzameld, beperken tot alleen die netwerken die nodig zijn voor vRealize Automation-bewerkingen. Dit vermindert de hoeveelheid overgedragen gegevens en verbetert de systeemprestaties.

Vereiste uitbreidbaarheidskenmerken in de Infoblox-applicatie toevoegen voor integratie met vRealize Automation

Voordat u het pakket van de Infoblox-provider (`Infoblox.zip`) kunt downloaden en implementeren voor integratie met vRealize Automation vanaf de Infoblox-website of via de VMware Marketplace, moet u de vereiste uitbreidbaarheidskenmerken toevoegen in Infoblox.

Deze procedure is van toepassing als u een extern IPAM-integratiepunt maakt voor Infoblox-integratie met Cloud Assembly.

Voordat u de download `infoblox.zip` kunt gebruiken, moet u zich aanmelden bij uw Infoblox-account met de verificatiegegevens van uw beheerdersaccount voor de organisatie en de volgende Infoblox-uitbreidbaarheidskenmerken vooraf maken:

- `VMware NIC index`
- `VMware resource ID`

Voorwaarden

- Controleer of u een account hebt met [Infoblox](#) en of u de juiste verificatiegegevens hebt voor het Infoblox-account van uw organisatie.
- Controleer of de Infoblox WAPI-versie wordt ondersteund. IPAM-integratie met Infoblox is afhankelijk van Infoblox WAPI versie 2.7. Infoblox-appliances die WAPI versie 2.7 ondersteunen, worden ondersteund.
- Bekijk [Infoblox-specifieke eigenschappen en uitbreidbaarheidskenmerken voor IPAM-integraties in vRealize Automation-cloudsjablonen gebruiken](#).

Procedure

- 1 Meld u aan bij uw Infoblox-account met uw verificatiegegevens als beheerder.

Dit zijn uw gebruikersnaam en wachtwoord als beheerder die u opgeeft wanneer u een extern IPAM-integratiepunt in Cloud Assembly maakt via **Infrastructuur > Verbindingen > Integraties > .**

- 2 Gebruik de procedure zoals beschreven in de Infoblox-documentatie om de volgende vereiste uitbreidbaarheidskenmerken in uw Infoblox-applicatie te maken.

- VMware NIC index - type geheel getal
- VMware resource ID - type tekenreeks

De procedure wordt beschreven in de sectie *Uitbreidbaarheidskenmerken toevoegen* van het onderwerp [Over uitbreidbaarheidskenmerken](#) in de Infoblox-documentatie. Zie ook [Uitbreidbaarheidskenmerken beheren](#).

Wat nu te doen

Nadat u de vereiste kenmerken hebt toegevoegd, kunt u het proces voor het downloaden en implementeren van het Infoblox-pakket hervatten, zoals beschreven in [Een extern IPAM-providerpakket downloaden en implementeren voor gebruik in vRealize Automation](#).

Een extern IPAM-providerpakket downloaden en implementeren voor gebruik in vRealize Automation

Voordat u een extern IPAM-integratiepunt in vRealize Automation kunt definiëren, hebt u een geconfigureerd IPAM-providerpakket nodig.

U kunt een integratiepakket specifiek voor de provider verkrijgen op de website van uw IPAM-provider of in de [VMware Marketplace](#).

Opmerking Dit voorbeeld gebruikt het door VMware geleverde Infoblox-pakket `Infoblox.zip`, dat als volgt kan worden gedownload via de [VMware Marketplace](#):

- [Infoblox-invoegtoepassing versie 1.4](#) - Compatibel met vRealize Automation release 8.3 - 8.7 en biedt alle functionaliteit van eerdere versies. Met deze versie kunt u dezelfde hostnaam gebruiken met een ander DNS-achtervoegsel voor twee NIC's. Zie de release notes bij de invoegtoepassing voor meer informatie.
- [Infoblox-invoegtoepassing versie 1.3](#) - Compatibel met vRealize Automation 8.3.x en biedt extra filters voor het verzamelen van netwerkgegevens. Zie [De verzameling van netwerkgegevens beheren met behulp van Infoblox-filters in vRealize Automation](#). Als u vRealize Automation 8.3.x gebruikt, kunt u in plaats daarvan Infoblox-invoegtoepassing 1.4 gebruiken om voordeel te halen uit de extra mogelijkheden.

De [Infoblox-plug-in versie 1.3](#) kan worden gebruikt met vRealize Automation 8.1 of 8.2, maar alleen in bepaalde situaties en met de nodige voorzichtigheid zoals beschreven in het KB-artikel over de [compatibiliteit van Infoblox 1.3 met vRealize Automation 8.x \(82142\)](#).

- [vRA Cloud Infoblox-invoegtoepassing versie 1.2](#) - Compatibel met vRealize Automation 8.1.x en 8.2.x
- [vRA Cloud Infoblox-invoegtoepassing versie 1.1](#) - Compatibel met vRealize Automation 8.1.x
- [vRA Cloud Infoblox-invoegtoepassing versie 1.0](#) - Compatibel met vRealize Automation 8.0.1.x met of zonder een internetverbinding met het globale netwerk.
- [vRA Cloud Infoblox-invoegtoepassing versie 0.4](#) - Compatibel met vRealize Automation 8.0.0.x en 8.0.1.x wanneer er een internetverbinding is met het globale netwerk.

IPAM-integratie met Infoblox is afhankelijk van Infoblox WAPI versie 2.7. Alle Infoblox-appliances die WAPI versie 2.7 ondersteunen, worden ondersteund.

Zie [Hoe kan ik met de IPAM SDK een providerspecifiek extern IPAM-integratiepakket voor vRealize Automation maken](#) voor informatie over het maken van een IPAM-integratiepakket voor andere IPAM-providers, als er nog geen bestaat in de [VMware Marketplace](#).

Het pakket van de IPAM-provider bevat scripts die zijn verpakt met metagegevens en andere configuraties. De scripts bevatten de broncode die wordt gebruikt voor de bewerkingen die vRealize Automation uitvoert in combinatie met de externe IPAM-provider. Voorbeeldbewerkingen zijn `Allocate an IP address for a virtual machine`, `Fetch a list of IP ranges from the provider` en `Update the MAC address of a host record in the provider`.

Voorwaarden

- Controleer of u over cloudbeheerdersreferenties beschikt. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).

- Controleer of u de gebruikersrol van cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Controleer of u een account bij de externe IPAM-provider hebt, bijvoorbeeld [Infoblox](#) of [Bluecat](#), en of u de juiste toegangsgegevens hebt voor het account van uw organisatie bij de IPAM-provider.
- Als u Infoblox als uw externe IPAM-provider gebruikt, controleert u of u de vereiste uitbreidbaarheidskenmerken hebt toegevoegd aan uw Infoblox-account voordat u doorgaat. Zie [Vereiste uitbreidbaarheidskenmerken in de Infoblox-applicatie toevoegen voor integratie met vRealize Automation](#).

Opmerking Er bestaat een probleem met de certificaatketen dat is gerelateerd aan hoe het Python-element in de Infoblox-invoegtoepassing SSL-handshakes verwerkt. Voor informatie over het probleem en de vereiste acties om het probleem op te lossen, raadpleegt u het Knowledge Base-artikel [vRA Cloud Infoblox Plugin throws a certificate chain error during authentication process \(88057\)](#).

Procedure

- 1 Ga naar de juiste downloadpagina voor de Infoblox-invoegtoepassing. Zie hierboven voor links naar een specifieke versie van de Infoblox-invoegtoepassing.

Zie hierboven voor de opties voor de Infoblox-invoegtoepassing die beschikbaar zijn op de [VMware Marketplace](#).
- 2 Meld u aan en download het plug-inpakket.
- 3 Als u dit nog niet hebt gedaan, voegt u de vereiste uitbreidbaarheidskenmerken toe in Infoblox. Zie [Vereiste uitbreidbaarheidskenmerken in de Infoblox-applicatie toevoegen voor integratie met vRealize Automation](#).

Resultaten

Het pakket is nu beschikbaar om te implementeren via **Integraties > Integratie toevoegen > IPAM > Providers beheren > Pakket importeren** zoals beschreven in [Een extern IPAM-integratiepunt voor Infoblox toevoegen in vRealize Automation](#).

Een uitvoeringsomgeving voor een IPAM-integratiepunt maken in vRealize Automation

Voordat u een extern IPAM-integratiepunt in vRealize Automation kunt definiëren, moet u een bestaande uitvoeringsomgeving maken of gebruiken om als intermediair tussen de IPAM-provider en vRealize Automation te fungeren. De uitvoeringsomgeving is vaak een Amazon Web Services- of Microsoft Azure-cloudaccount of een integratiepunt op locatie voor actiegebaseerde uitbreidbaarheid dat is gekoppeld aan een clouduitbreidbaarheidsproxy.

Voor externe IPAM-integratie is een uitvoeringsomgeving vereist. Wanneer u het IPAM-integratiepunt definieert, maakt u een verbinding tussen Cloud Assembly en uw IPAM-provider door een beschikbare uitvoeringsomgeving op te geven.

IPAM-integratie maakt gebruik van een set gedownloade providerspecifieke scripts of plug-ins in een uitvoeringsomgeving die wordt mogelijk gemaakt door een FaaS-provider, zoals Amazon Web Services Lambda, Microsoft Azure Functions of een ingesloten integratiepunt op locatie voor actiegebaseerde uitbreidbaarheid (ABX). De uitvoeringsomgeving wordt gebruikt om verbinding te maken met de externe IPAM-provider, bijvoorbeeld Infoblox.

Opmerking Voor een Infoblox IPAM-integratiepunt is een ingesloten integratiepunt op locatie voor actiegebaseerde uitbreidbaarheid (ABX) vereist.

Elk type runtimeomgeving heeft voor- en nadelen:

- Integratiepunt voor actiegebaseerde uitbreidbaarheid (ABX):
 - is gratis, geen extra verbruikskosten bij leveranciers.
 - kan verbinding maken met appliances van een IPAM-leverancier die zich in een datacenter op locatie bevinden achter een NAT/firewall die niet openbaar toegankelijk is, bijvoorbeeld Infoblox.
 - is trager met enigszins minder beschikbare prestaties dan de commerciële cloud.
- Amazon Web Services
 - resulteert in kosten voor FaaS-verbinding/gebruik bij leveranciers.
 - kan geen verbinding maken met appliances van IPAM-leveranciers die zich in een datacenter op locatie bevinden achter een NAT/firewall die niet openbaar toegankelijk is.
 - biedt snelle en uiterst betrouwbare prestaties.
- Microsoft Azure
 - resulteert in kosten voor FaaS-verbinding/gebruik bij leveranciers.
 - kan geen verbinding maken met appliances van IPAM-leveranciers die zich in een datacenter op locatie bevinden achter een NAT/firewall die niet openbaar toegankelijk is.
 - biedt snelle en uiterst betrouwbare prestaties.

Voorwaarden

- Controleer of u over cloudbeheerdersreferenties beschikt. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Controleer of u de gebruikersrol van cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Controleer of u een account bij de externe IPAM-provider hebt, bijvoorbeeld [Infoblox](#) of [Bluecat](#), en of u de juiste toegangsgegevens hebt voor het account van uw organisatie bij de IPAM-provider.

- Controleer of u toegang hebt tot een geïmplementeerd integratiepakket voor uw IPAM-provider, zoals Infoblox of BlueCat. Het geïmplementeerde pakket wordt in eerste instantie als ZIP-download verkregen van de website van uw IPAM-provider of in de [VMware Marketplace](#) en wordt vervolgens geïmplementeerd in Cloud Assembly.

Zie [Een extern IPAM-providerpakket downloaden en implementeren voor gebruik in vRealize Automation](#) voor informatie over het implementeren van het ZIP-bestand met het providerpakket en het beschikbaar maken ervan als **providerwaarde** op de pagina IPAM-integratie.

Procedure

- 1 Als u een FaaS-gebaseerde uitbreidbaarheidsactie op locatie wilt maken voor gebruik als uitvoeringsomgeving voor IPAM-integratie, selecteert u **Uitbreidbaarheid > Bibliotheek > Acties**.
- 2 Klik op **Nieuwe actie**, voer een actienaam en beschrijving in en geef een project op.
- 3 Selecteer **Op locatie** in het vervolgkeuzemenu **FaaS-provider**.
- 4 Vul het formulier in om de uitbreidbaarheidsactie te definiëren.

Zie [Levenscycli van applicaties uitbreiden en automatiseren met uitbreidbaarheid](#) voor meer informatie over uitbreidbaarheidsacties.



Voor gerelateerde informatie over de actieve omgeving raadpleegt u de blogvideo over [de integratie van de Infoblox IPAM-invoegtoepassing](#), ongeveer vanaf minuut 24 in de video.

Een extern IPAM-integratiepunt voor Infoblox toevoegen in vRealize Automation

vRealize Automation ondersteunt integratie met een externe IPAM-provider. In dit voorbeeld wordt Infoblox als externe IPAM-provider gebruikt.

U kunt een providerspecifiek IPAM-integratiepunt gebruiken om IP-adressen en gerelateerde netwerkeigenschappen voor cloudsjabloonimplementaties te verkrijgen en te beheren.

In dit voorbeeld maakt u een extern IPAM-integratiepunt om toegang tot het account van uw organisatie met een externe IPAM-provider te ondersteunen. In deze voorbeeldwerkstroom is Infoblox de IPAM-provider en bestaat het providerspecifieke integratiepakket al. Hoewel deze instructies specifiek zijn voor een Infoblox-integratie, kunnen ze als referentie worden gebruikt als u een IPAM-integratie maakt voor een andere externe IPAM-provider.

U kunt een providerpakket verkrijgen op de website van uw IPAM-provider of in de [VMware Marketplace](#).

Dit voorbeeld gebruikt het door VMware geleverde Infoblox-pakket `Infoblox.zip`, dat kan worden gedownload via de [VMware Marketplace](#). Zie [Een extern IPAM-providerpakket downloaden en implementeren voor gebruik in vRealize Automation](#) voor informatie over de meest recente versies van de Infoblox-invoegtoepassing die beschikbaar zijn in de [VMware Marketplace](#).

Voorwaarden

- Controleer of u over cloudbeheerdersreferenties beschikt. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Controleer of u de gebruikersrol van cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Controleer of u een account hebt met een externe IPAM-provider en of u de juiste verificatiegegevens voor uw organisatieaccount bij de IPAM-provider hebt.
- Controleer of u toegang hebt tot een geïmplementeerd integratiepakket voor uw IPAM-provider. Het geïmplementeerde pakket wordt in eerste instantie verkregen als ZIP-download van uw IPAM-providerwebsite, of via de VMware Solutions Exchange Marketplace en vervolgens geïmplementeerd in vRealize Automation.

Zie [Een extern IPAM-providerpakket downloaden en implementeren voor gebruik in vRealize Automation](#) voor informatie over het downloaden en implementeren van het ZIP-bestand met het providerpakket en het beschikbaar maken ervan als **Provider**-waarde op de pagina IPAM-integratie.

- Controleer of u toegang hebt tot een geconfigureerde uitvoeringsomgeving voor de IPAM-provider. De uitvoeringsomgeving is doorgaans een ingesloten integratiepunt op locatie voor actiegebaseerde uitbreidbaarheid (ABX).

Zie [Een uitvoeringsomgeving voor een IPAM-integratiepunt maken in vRealize Automation](#) voor informatie over kenmerken van de uitvoeringsomgeving.

- Schakel de vereiste uitbreidbaarheidskenmerken in uw Infoblox-applicatie in. Zie [Vereiste uitbreidbaarheidskenmerken in de Infoblox-applicatie toevoegen voor integratie met vRealize Automation](#).
- Als u geen externe internettoegang hebt, kunt u een internetserverproxy configureren. Zie [Hoe configureer ik een internetproxyserver voor vRealize Automation](#).
- Controleer of u over de vereiste gebruikersreferenties beschikt om uw Infoblox IPAM-product te openen en te gebruiken. Open bijvoorbeeld het tabblad Beheer in de Infoblox-appliance en pas de vermeldingen voor beheerder, groepen en rollen aan. U moet lid zijn van een groep met de rechten van beheerder of supergebruiker of van een aangepaste groep met rechten voor DHCP, DNS, IPAM en rasters. Met deze instellingen krijgt u toegang tot alle functies die beschikbaar zijn in de Infoblox-invoegtoepassing, zodat u een Infoblox IPAM-integratie en -ontwerpers kunt maken om die IPAM-integratie in cloudsjablonen en implementaties te gebruiken. Raadpleeg de Infoblox-productdocumentatie voor meer informatie over gebruikersrechten.

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Integraties** en klik op **Integratie toevoegen**.
- 2 Klik op **IPAM**.
- 3 Selecteer een geconfigureerd IPAM-providerpakket in de vervolgkeuzelijst **Provider**, bijvoorbeeld *Infoblox_hrg*.

Als de lijst leeg is, klikt u op **Providerpakket importeren**, navigeert u naar een bestaand ZIP-bestand met providerpakket en selecteert u het. Als u het ZIP-bestand van de provider niet heeft, kunt u het verkrijgen op de website van uw IPAM-provider of via de [VMware Marketplace](#).

Zie [Een extern IPAM-providerpakket downloaden en implementeren voor gebruik in vRealize Automation](#) voor informatie over het implementeren van het ZIP-bestand met het providerpakket in vCenter en het beschikbaar maken ervan als **Provider**-waarde op de pagina Integratie.

Voor informatie over het upgraden van een bestaande IPAM-integratie om een recentere versie van het IPAM-integratiepakket van een leverancier te gebruiken, raadpleegt u [Upgraden naar een hoger extern IPAM-integratiepakket in vRealize Automation](#).

- 4 Voer uw gebruikersnaam en wachtwoord in voor uw beheerdersaccount bij de externe IPAM-provider, samen met alle andere verplichte velden (indien aanwezig), zoals de hostnaam van uw provider.

In dit voorbeeld haalt u de hostnaam van uw Infoblox IPAM-provider op door de volgende stappen uit te voeren:

- a Meld u op een apart browsertabblad aan bij uw IPAM-provideraccount met uw Infoblox-verificatiegegevens als beheerder.
- b Kopieer de URL van de hostnaam.
- c Plak de URL van de hostnaam in het veld **Hostnaam** op de pagina IPAM-integratie.

- 5 Selecteer in de vervolgkeuzelijst **Uitvoeringsomgeving** een bestaand integratiepunt op locatie voor actiegebaseerde uitbreidbaarheid, bijvoorbeeld *Infoblox_abx_intg*.

De uitvoeringsomgeving ondersteunt communicatie tussen vRealize Automation en de externe IPAM-provider.

Opmerking Als u een Amazon Web Services- of Microsoft Azure-cloudaccount gebruikt als uitvoeringsomgeving voor de integratie, moet u ervoor zorgen dat de appliance van de IPAM-provider toegankelijk is via internet en zich niet achter een NAT of firewall bevindt en dat deze een openbaar omzetbare DNS-naam heeft. Als de IPAM-provider niet toegankelijk is, kunnen de Amazon Web Services Lambda of Microsoft Azure Functions geen verbinding maken met de appliance en mislukt de integratie. Zie [Een uitvoeringsomgeving voor een IPAM-integratiepunt maken in vRealize Automation](#) voor gerelateerde informatie.

Het IPAM-framework ondersteunt alleen een ingesloten uitvoeringsomgeving op locatie voor actiegebaseerde uitbreidbaarheid (ABX).

Opmerking Voor een Infoblox IPAM-integratiepunt is een ingesloten integratiepunt op locatie voor actiegebaseerde uitbreidbaarheid (ABX) vereist.

Het geconfigureerde cloudaccount of integratiepunt staat communicatie toe tussen vRealize Automation en de IPAM-provider, in dit voorbeeld Infoblox, via een gekoppelde clouduitbreidbaarheidsproxy. U kunt een provider selecteren die al is gemaakt, of u kunt er een maken.

Voor informatie over hoe u een uitvoeringsomgeving kunt maken, raadpleegt u [Een uitvoeringsomgeving voor een IPAM-integratiepunt maken in vRealize Automation](#).

6 Klik op **Valideren**.

Omdat in dit voorbeeld de integratie op locatie voor actiegebaseerde uitbreidbaarheid wordt gebruikt voor de uitvoeringsomgeving, kunt u de validatieactie bekijken.

- a Klik op het tabblad **Uitbreidbaarheid**.
- b Klik op **Activiteit > Actie-uitvoeringen** en selecteer **Alle uitvoeringen** of **Integratie-uitvoeringen** in het filter om aan te geven dat een validatieactie voor een eindpunt is gestart en wordt uitgevoerd.

7 Wanneer u wordt gevraagd het zelfondertekende certificaat van de IPAM-provider te vertrouwen, klikt u op **Accepteren**.

Nadat u het zelfondertekende certificaat hebt geaccepteerd, kan de validatieactie verder worden voltooid.

8 Voer een **naam** in voor dit IPAM-integratiepunt, zoals *Infoblox_Integration*, en een **beschrijving**, zoals *Infoblox IPAM met ABX-integratie voor team-HRG*.

9 Klik op **Toevoegen** om het nieuwe externe IPAM-integratiepunt op te slaan.

Er wordt een actie voor gegevensverzameling nagebootst. Gegevens voor netwerken en IP-bereiken worden verzameld bij de IPAM-provider. U kunt de gegevensverzamelingsactie als volgt bekijken:

- a Klik op het tabblad **Uitbreidbaarheid**.
- b Klik op **Activiteit > Actie-uitvoeringen**. Er wordt een gegevensverzamelingsactie gestart en uitgevoerd. U kunt de inhoud van de actie-uitvoering openen en bekijken.

Resultaten

De providerspecifieke externe IPAM-integratie is nu beschikbaar voor gebruik met netwerken en netwerkprofielen.

Configureer een netwerk en netwerkprofiel voor het gebruik van externe IPAM voor een bestaand netwerk in vRealize Automation

U kunt een bestaand netwerk definiëren om IP-adreswaarden te gebruiken die worden opgehaald van en beheerd door een externe IPAM-provider in plaats van intern via vRealize Automation.

U kunt een netwerk definiëren om toegang te krijgen tot bestaande IP-instellingen die u heeft gedefinieerd in het externe IPAM-provideraccount van uw organisatie. Deze stap beschrijft de integratie van de Infoblox-provider die u in de vorige stap hebt gemaakt.

In dit voorbeeld configureert u een netwerkprofiel met bestaande netwerken waarvoor de gegevens zijn verzameld bij vCenter. Vervolgens configureert u deze netwerken om IP-informatie van een externe IPAM-provider te krijgen, in dit geval Infoblox. Virtuele machines die u inricht vanaf vRealize Automation die met dit netwerkprofiel kunnen worden gevonden, krijgen hun IP en andere TCP/IP-gerelateerde instellingen van de externe IPAM-provider.

Zie [Netwerkkresources in vRealize Automation](#) voor meer informatie over netwerken. Zie [Netwerkprofielen toevoegen in vRealize Automation](#) en [Meer informatie over netwerkprofielen in vRealize Automation](#) voor meer informatie over netwerkprofielen.

Zie [Hoe configureer ik een netwerkprofiel om een netwerk op aanvraag te ondersteunen voor een externe IPAM-integratie in vRealize Automation](#) voor gerelateerde informatie.

Voorwaarden

Deze reeks stappen wordt weergegeven in de context van een integratiewerkstroom van de IPAM-provider. Zie [Tutorial: Een providerspecifieke externe IPAM-integratie voor vRealize Automation configureren](#).

- Controleer of u over cloudbeheerdersreferenties beschikt. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Controleer of u de gebruikersrol van cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Controleer of u een account bij de externe IPAM-provider hebt, bijvoorbeeld [Infoblox](#) of [Bluecat](#), en of u de juiste toegangsgegevens hebt voor het account van uw organisatie bij de IPAM-provider. In deze voorbeeldwerkstroom is Infoblox de IPAM-provider.
- Controleer of u een IPAM-integratiepunt hebt voor de IPAM-provider. Zie [Een extern IPAM-integratiepunt voor Infoblox toevoegen in vRealize Automation](#).

Procedure

- 1 Als u een netwerk wilt configureren, klikt u op **Infrastructuur > Resources > Netwerken**.
- 2 Selecteer op het tabblad **Netwerken** een bestaand netwerk dat u wilt gebruiken met het integratiepunt van de IPAM-provider. In dit voorbeeld is de netwerknaam *net.23.117-only-IPAM*.

Voor netwerken in de lijst zijn gegevens verzameld door vRealize Automation vanuit een vCenter in uw organisatie.

- 3 Als u waarden wilt ophalen van de externe IPAM-provider, controleert u of buiten de instellingen **Account/regio**, **Naam** en **Netwerkdomein**, alle andere netwerkinstellingen leeg zijn, waaronder de volgende:
 - Domein (zie opmerking in stap 8)
 - CIDR
 - Standaardgateway
 - DNS-servers
 - DNS-zoekdomeinen
- 4 Klik op het tabblad **IP-bereiken** en klik op **IPAM IP-bereik toevoegen**.
- 5 Selecteer in het menu **Netwerk** het netwerk dat u zojuist hebt geconfigureerd, bijvoorbeeld *net.23.117-only-IPAM*.
- 6 Selecteer in het menu **Provider** het IPAM-integratiepunt *Infoblox_Integration* dat u eerder in de werkstroom hebt gemaakt.
- 7 Selecteer een van de weergegeven netwerkweergaven in het vervolgkeuzemenu **Adresruimte** dat nu zichtbaar is.

Een adresruimte in Infoblox wordt aangeduid als netwerkweergave.

De netwerkweergaven worden opgehaald uit uw IPAM-provideraccount. In dit voorbeeld wordt het subnet van het netwerk gebruikt dat u zojuist hebt geconfigureerd, bijvoorbeeld *net.23.117-IPAM*, het integratiepunt *Infoblox_Integration* dat u eerder in de werkstroom hebt gemaakt en een adresruimte met de naam *standaard*.

Weergegeven waarden voor de adresruimte worden opgehaald van de externe IPAM-provider.

- 8 Selecteer een of meer netwerken in de lijst met weergegeven netwerken die beschikbaar zijn voor de geselecteerde adresruimte. Selecteer bijvoorbeeld 10.23.117.0/24.

In dit voorbeeld bevatten de waarden van de kolom **Domeinen** en **DNS-servers** voor het geselecteerde netwerk Infoblox-waarden.

Opmerking Als u in stap 3 een netwerk selecteert waarvoor een domein is opgegeven voor vRealize Automation en vervolgens een netwerk selecteert uit de adresruimte van de externe IPAM-provider die een domeinwaarde bevat, krijgt de domeinwaarde in het externe IPAM-providernetwerk voorrang op het domein dat is opgegeven in vRealize Automation. Als de instelling voor het IPAM IP-bereik geen domeinwaarde bevat, die is opgegeven in Cloud Assembly of in de externe IPAM-provider zoals hierboven beschreven, mislukt de inrichting.

Voor Infoblox kunt u de blueprinteigenschap `Infoblox.IPAM.Network.dnsSuffix` op machineniveau gebruiken om de domeinwaarde te overschrijven. Zie [Infoblox-specifieke eigenschappen en uitbreidbaarheidskenmerken voor IPAM-integraties in vRealize Automation-cloudsjablonen gebruiken](#) voor gerelateerde informatie.

- 9 Klik op **Toevoegen** om het IPAM IP-bereik voor het netwerk op te slaan.

Het bereik is zichtbaar in de tabel **IP-bereiken**.

- 10 Klik op het tabblad **IP-adressen**.

Nadat u een machine hebt ingericht met behulp van het nieuwe adresbereik van de externe IPAM-provider, wordt een nieuwe record weergegeven in de tabel **IP-adressen**.

- 11 Als u een netwerkprofiel wilt configureren om het netwerk te gebruiken, klikt u op **Infrastructuur > Configureren > Netwerkprofielen**.

- 12 Geef het netwerkprofiel een naam, bijvoorbeeld *Infoblox-NP* en voeg de volgende voorbeeldinstellingen toe.

- Tabblad Samenvatting

- Geef een vSphere-cloudaccount/-regio op.
- Voeg een capaciteitstag voor het netwerkprofiel toe voor het netwerkprofiel, bijvoorbeeld *infoblox_abx*.

Noteer de capaciteitstag, aangezien u deze ook als cloudsjabloonbeperkingstag moet gebruiken om de inrichtingskoppeling in de cloudsjabloon te maken.

- Tabblad Netwerken

- Voeg het netwerk toe dat u eerder hebt gemaakt, bijvoorbeeld *net.23.117-only-IPAM*.

- 13 Klik op **Opslaan** om het netwerkprofiel met deze instellingen op te slaan.

Resultaten

De netwerk- en netwerkprofielinstelling wordt nu geconfigureerd voor een bestaand netwerktype dat wordt gebruikt voor de Infoblox IPAM-integratie in een cloudsjabloon.

Een cloudsjabloon definiëren en implementeren die gebruikmaakt van een bereiktoewijzing van een externe IPAM-provider in vRealize Automation

U kunt een cloudsjabloon definiëren om IP-adrestoewijzingen van uw externe IPAM-provider te krijgen en te beheren. In dit voorbeeld wordt Infoblox als externe IPAM-provider gebruikt.

In deze laatste stap in de integratiewerkstroom voor de externe IPAM definieert en implementeert u een cloudsjabloon die uw eerder gedefinieerde netwerk en netwerkprofiel verbindt met het Infoblox-account van uw organisatie om IP-adrestoewijzingen voor geïmplementeerde VM's van de externe IPAM-provider te krijgen en te beheren, en niet van vRealize Automation.

Deze werkstroom gebruikt Infoblox als externe IPAM-provider en in sommige stappen zijn de voorbeeldwaarden uniek voor Infoblox, hoewel het de bedoeling is dat de procedure kan worden toegepast op andere externe IPAM-integraties.



De blogpost [Automate IPAM and DNS for VMs using VMware vRealize Automation and Infoblox DDI](#) biedt gerelateerde informatie.

Nadat u de cloudsjabloon hebt geïmplementeerd en de VM is gestart, wordt het IP-adres dat voor elke VM in de implementatie wordt gebruikt, weergegeven als netwerkvermelding op de pagina **Resources > Netwerken**, als een nieuwe hostrecord in het IPAM-providernetwerk in het account bij uw IPAM-provider en in de vSphere Web Client-record voor elke geïmplementeerde VM in de host-vCenter.

Voorwaarden

Deze reeks stappen wordt weergegeven in de context van een integratiewerkstroom voor de externe IPAM-provider. Zie [Tutorial: Een providerspecifieke externe IPAM-integratie voor vRealize Automation configureren](#).

- Controleer of u over cloudbeheerdersreferenties beschikt. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Controleer of u de gebruikersrol van cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Controleer of u een account bij de externe IPAM-provider hebt, bijvoorbeeld Infoblox of BlueCat, en of u de juiste toegangsgegevens hebt voor het account van uw organisatie bij de IPAM-provider.
- Controleer of u beheerderstoegang hebt tot het hostaccount en rolvereisten die nodig zijn statusrecords weer te geven in de vSphere-webclientrecord voor uw geïmplementeerde VM's in de host-vCenter.
- Controleer of u een IPAM-integratiepunt hebt voor de externe IPAM-provider. Zie [Een extern IPAM-integratiepunt voor Infoblox toevoegen in vRealize Automation](#).
- Controleer of u een vRealize Automation-netwerk en -netwerkprofiel hebt geconfigureerd dat externe IPAM-integratie ondersteunt voor uw beoogde IPAM-integratiepunt. Zie [Configureer een netwerk en netwerkprofiel voor het gebruik van externe IPAM voor een bestaand netwerk in vRealize Automation](#).
- Controleer of uw project- en cloudzone zijn getagd om overeen te komen met tags in het IPAM-integratiepunt en het netwerk of netwerkprofiel. Configureer het project optioneel om aangepaste naamgeving van resources te ondersteunen.

Zie [Tutorial: Infrastructuur en implementaties met meerdere clouds instellen en testen in Cloud Assembly](#) voor aanvullende informatie over de rol van een project en cloudzone, evenals de rol van andere infrastructuurelementen in uw cloudsjabloon. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#) voor meer informatie over taggen.

Zie [Aangepaste naamgeving voor geïmplementeerde resources in Cloud Assembly](#) voor informatie over aangepaste naamgeving van VM's met behulp van instellingen in uw project.

Procedure

- 1 Klik op **Cloudsjablonen > Nieuw**, voer de volgende informatie in op de pagina **Nieuwe cloudsjabloon** en klik op **Maken**.
 - **Naam** = ipam-bpa
 - **Beschrijving** = Cloudsjabloon die Infoblox IPAM-integratie gebruikt
 - **Project** = 123VC
- 2 Voeg voor dit voorbeeld een cloudfanafhankelijk machineonderdeel en een cloudfanafhankelijk netwerkonderdeel toe aan het cloudsjablooncanvas en verbind de twee onderdelen.
- 3 Bewerk de cloudsjablooncode om een beperkingstag toe te voegen aan het netwerkonderdeel dat overeenkomt met de capaciteitstag die u aan het netwerkprofiel hebt toegevoegd. In dit voorbeeld is de tagwaarde *infoblox_abx*.
- 4 Bewerk de cloudsjablooncode om op te geven dat het toewijzingstype van het netwerk *statisch* is.

Wanneer u een externe IPAM-provider gebruikt, is de instelling `assignment: static` vereist.

Voor dit voorbeeld is het opgegeven IP-adres 10.23.117.4 momenteel beschikbaar in de externe IPAM-adresruimte die we in het gekoppelde netwerkprofiel voor het netwerk hebben geselecteerd. Hoewel de instelling `assignment: static` vereist is, is dit niet het geval voor de instelling `address: waarde`. U kunt ervoor kiezen om een externe IP-adresselectie te starten bij een bepaalde adreswaarde, maar dit is niet vereist. Als u geen instelling `address: waarde` opgeeft, selecteert de externe IPAM-provider het volgende beschikbare adres in het externe IPAM-netwerk.

- 5 Controleer de cloudsjablooncode aan de hand van het volgende voorbeeld.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: existing
      name: ipam
      constraints:
        - tag: infoblox_abx
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: ubuntu
      flavor: small
      networks:
        - network: '${resource.Cloud_Network_1.id}'
          assignment: static
          address: 10.23.117.4
          name: '${resource.Cloud_Network_1.name}'
```

Zie [Infoblox-specifieke eigenschappen en uitbreidbaarheidskenmerken voor IPAM-integraties in vRealize Automation-cloudsjablonen gebruiken](#) voor voorbeelden van Infoblox-eigenschappen die beschikbaar zijn voor het opgeven van DNS- en DHCP-instellingen in cloudsjablonen.

- 6 Klik op **Implementeren** op de cloudsjabloonpagina, geef de implementatie de naam *Infoblox-1* en klik op **Implementeren** op de pagina **Implementatietype**.
- 7 Wanneer de cloudsjabloon wordt geïmplementeerd, klikt u op het tabblad **Uitbreidbaarheid** en selecteert u **Activiteit > Actie-uitvoeringen** om de uitvoering van de uitbreidbaarheidsactie *Infoblox_AllocateIP_n* te zien.

Nadat de uitbreidbaarheidsactie is voltooid en de machine is ingericht, wordt het MAC-adres door de actie *Infoblox_Update_n* doorgegeven aan Infoblox.

- 8 U kunt zich aanmelden bij uw Infoblox-account en het account openen om de nieuwe hostrecord voor het IPAM-adres in het gekoppelde 10.23.117.0/24-netwerk te zien. U kunt ook het tabblad DNS in Infoblox openen om de nieuwe DNS-hostrecord te zien.
- 9 Om te controleren of de VM wordt ingericht, meldt u zich aan bij uw host-vCenter en -vSphere Web Client om de ingerichte machine te vinden en de DNS-naam en het IP-adres weer te geven.

Nadat de ingerichte VM is gestart, wordt het MAC-adres doorgegeven aan Infoblox door de uitbreidbaarheidsactie *Infoblox_AllocateIP*.

- 10 Als u de nieuwe netwerkrecord in vRealize Automation wilt weergeven, selecteert u **Infrastructuur > Resources > Netwerken** en klikt u om het tabblad **IP-adressen** te openen.
- 11 Als u de implementatie verwijdert, worden de IPAM-adressen van VM's in de implementatie vrijgegeven en zijn de IP-adressen weer beschikbaar voor de externe IPAM-provider voor andere toewijzingen. De uitbreidbaarheidsactie voor deze gebeurtenis in vRealize Automation is *Infoblox_Deallocate*.

Infoblox-specifieke eigenschappen en uitbreidbaarheidskenmerken voor IPAM-integraties in vRealize Automation-cloudsjablonen gebruiken

U kunt Infoblox-specifieke eigenschappen gebruiken voor vRealize Automation-projecten die externe IPAM-integraties voor Infoblox bevatten.

De volgende Infoblox-eigenschappen zijn beschikbaar voor gebruik met uw Infoblox-IPAM-integraties in cloudsjabloonontwerpen en -implementaties. U kunt deze in vRealize Automation gebruiken om de toewijzing van IP-adressen tijdens de cloudsjabloonimplementatie verder te beheren. Het gebruik van deze eigenschappen is optioneel.

Opmerking Als u de Infoblox-invoegtoepassing 1.4 of lager gebruikt, overschrijft een algemene Infoblox-eigenschap een lokale Infoblox-eigenschap voor de eigenschappen `dnsSuffix`, `dnsView`, `enableDns` en `enableDhcp`. De algemene eigenschap is van toepassing op alle NIC's.

De volgende eigenschappen zijn beschikbaar en opgenomen in de meest recente versie van de Infoblox-plug-in voor vRealize Automation. Zie [Een extern IPAM-providerpakket downloaden en implementeren voor gebruik in vRealize Automation](#) voor informatie over versies van de Infoblox-plug-in en waar de meest recente versie van de Infoblox-plug-in voor uw IPAM-integratie kan worden verkregen in vRealize Automation.

- `Infoblox.IPAM.createFixedAddress`

Met deze eigenschap kunt u een vaste adresrecord in Infoblox maken. Mogelijke waarden zijn True en False. Er wordt standaard een hostrecord gemaakt. De standaardwaarde is Onwaar.

- `Infoblox.IPAM.Network.dnsView`

Met deze eigenschap kunt u een DNS-weergave gebruiken bij het maken van een hostrecord in Infoblox.

- `Infoblox.IPAM.Network.enableDns`

Wanneer u een IP toewijst in Infoblox, kunt u met deze eigenschap ook een DNS-record maken. Mogelijke waarden zijn True en False. De standaardwaarde is Waar.

- `Infoblox.IPAM.Network.enableDhcp`

Met deze eigenschap kunt u de DHCP-configuratie voor het hostadres instellen. Mogelijke waarden zijn True en False. De standaardwaarde is Waar.

- `Infoblox.IPAM.Network.dnsSuffix`

Met deze eigenschap kunt u de DHCP-optie *domain* van een Infoblox-netwerk overschrijven met een nieuwe. Deze mogelijkheid is handig als op het Infoblox-netwerk de DHCP-optie *domain* niet is ingesteld of als de DHCP-optie *domain* moet worden overschreven. De standaardwaarde is null (lege tekenreeks)

Wanneer u een externe IPAM-provider zoals Infoblox gebruikt, moet u een DNS-achtervoegsel opgeven wanneer u een machine inricht. Hoewel het DNS-achtervoegsel vereist is, kunt u het op een van de volgende manieren opgeven:

- Geef het DNS-achtervoegsel op in het vSphere-netwerksubnet in vRealize Automation.
- Geef de eigenschap `Infoblox.IPAM.Network.dnsSuffix` op in de code van de machineresource in de vRealize Automation-cloudsjabloon.

Hieronder wordt een voorbeeld weergegeven in de sectie `Infoblox.IPAM.Network.hostnameNicSuffix`.

`Infoblox.IPAM.Network.dnsSuffix` is alleen van toepassing als `Infoblox.IPAM.Network.enableDns` is ingesteld op True.

- `Infoblox.IPAM.Network.hostnameNicSuffix`

U kunt deze eigenschap gebruiken om een NIC-indexachtervoegsel op te geven bij het genereren van een hostnaam.

Hierdoor kunt u een machine inrichten met meer dan één NIC, zodat de hostnamen voor elke NIC worden onderscheiden door een aangepast achtervoegsel. Zoals u in het volgende voorbeeld ziet, kunt u een machine inrichten, bijvoorbeeld *my-machine* met 2 NIC's, zodat de hostnaam voor de eerste NIC het achtervoegsel `-nic1` heeft en de andere het achtervoegsel `-nic2` heeft.

U kunt ook een DNS-achtervoegsel opgeven, zoals in het voorbeeld wordt weergegeven. De eigenschap `Infoblox.IPAM.Network.dnsSuffix` wordt gebruikt met een waarde voor `test.local` zodat de eerste NIC de naam *my-machine-nic1.test.local* heeft en de andere de naam *my-machine-nic2.test.local* heeft.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      Infoblox.IPAM.Network.dnsSuffix: test.local
      Infoblox.IPAM.Network0.hostnameNicSuffix: -nic1
      Infoblox.IPAM.Network1.hostnameNicSuffix: -nic2
      image: ubuntu
      flavor: small
      networks:
        - network: '${resource.Cloud_Network_1.id}'
          deviceIndex: 0
        - network: '${resource.Cloud_Network_2.id}'
          deviceIndex: 1
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: existing
  Cloud_Network_2:
    type: Cloud.Network
    properties:
      networkType: existing
```

Deze eigenschap is geïntroduceerd met Infoblox-invoegtoepassing versie 1.3. Zie [Een extern IPAM-providerpakket downloaden en implementeren voor gebruik in vRealize Automation](#).

- U kunt eigenschappen ook opgeven met behulp van een uitbreidbaarheidsabonnement.

Zie [Vereiste uitbreidbaarheidskenmerken in de Infoblox-applicatie toevoegen voor integratie met vRealize Automation](#) voor gerelateerde informatie over Infoblox-uitbreidbaarheidskenmerken voor dit toepassingsvoorbeeld.

Infoblox-eigenschappen gebruiken op verschillende machine-NIC's in een cloudsjabloon

De volgende Infoblox-eigenschappen kunnen een andere waarde ondersteunen voor elke machine-NIC in de cloudsjabloon:

- `Infoblox.IPAM.Network.enableDhcp`

- `Infoblox.IPAM.Network.dnsView`
- `Infoblox.IPAM.Network.enableDns`
- `Infoblox.IPAM.Network.hostnameNicSuffix`

Als u bijvoorbeeld een andere `Infoblox.IPAM.Network.dnsView`-waarde wilt gebruiken voor elke NIC, gebruikt u voor elke NIC een `Infoblox.IPAM.Network<nicIndex>.dnsView`-vermelding. In het volgende voorbeeld ziet u verschillende waarden voor `Infoblox.IPAM.Network.dnsView` voor twee NIC's.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      Infoblox.IPAM.Network0.dnsView: default
      Infoblox.IPAM.Network1.dnsView: my-net
      image: ubuntu
      flavor: small
      networks:
        - network: '${resource.Cloud_Network_1.id}'
          deviceIndex: 0
        - network: '${resource.Cloud_Network_2.id}'
          deviceIndex: 1
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: existing
  Cloud_Network_2:
    type: Cloud.Network
    properties:
      networkType: existing
```

De Infoblox-integratie maakt standaard een DNS-hostrecord in de *standaard* DNS-weergave in Infoblox. Als uw Infoblox-beheerder *aangepaste* DNS-weergaven heeft gemaakt, kunt u het standaard integratiegedrag overschrijven en een benoemde weergave opgeven met behulp van de eigenschap `Infoblox.IPAM.Network.dnsView` in het machineonderdeel. U kunt bijvoorbeeld de volgende eigenschap aan het `Cloud_Machine_1`-onderdeel toevoegen om een benoemde DNS-weergave in Infoblox op te geven.

```
Cloud_Machine_1:
  type: Cloud.Machine
  properties:
    image: ubuntu
    flavor: small
    Infoblox.IPAM.Network.dnsView:<dns-view-name>
```

Zie [DNS Views](#) in de Infoblox-productdocumentatie voor informatie over het configureren en gebruiken van DNS-weergaven. Zie [Een cloudsjabloon definiëren en implementeren die gebruikmaakt van een bereiktoewijzing van een externe IPAM-provider in vRealize Automation](#) voor voorbeelden in de Infoblox-integratiewerkstroom.

Infoblox-eigenschappen opgeven

U kunt een Infoblox-eigenschap opgeven met een van de volgende methoden in Cloud Assembly:

- U kunt eigenschappen in een project opgeven met behulp van de sectie **Custom eigenschappen** op uw **Infrastructuur > Beheer > Projecten**-pagina. Met deze methode worden de opgegeven eigenschappen toegepast op alle machines die zijn ingericht in het bereik van dit project.
- U kunt eigenschappen opgeven voor elk machineonderdeel in een cloudsjabloon. Voorbeeld van cloudsjablooncode die het gebruik van de eigenschap `Infoblox.IPAM.Network.dnsView` illustreert, wordt hieronder weergegeven:

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      Infoblox.IPAM.Network.dnsView: default
      image: ubuntu
      cpuCount: 1
      totalMemoryMB: 1024
      networks:
        - network: '${resource.Cloud_Network_1.id}'
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: existing
      constraints:
        - tag: mk-ipam-demo
```

De verzameling van netwerkgegevens beheren met behulp van Infoblox-filters in vRealize Automation

Voor Infoblox kunt u het aantal netwerken waarvoor gegevens worden verzameld, beperken tot alleen die netwerken die nodig zijn voor vRealize Automation-bewerkingen. Dit vermindert de hoeveelheid overgedragen gegevens en verbetert de systeemprestaties.

vRealize Automation verzamelt elke 10 minuten gegevens van het externe IPAM-systeem. Voor Infoblox kunt u op verschillende manieren filteren om slechts een subset van netwerken te detecteren en hiervoor gegevens te verzamelen die door vRealize Automation-bewerkingen worden gebruikt.

Als u gegevensverzameling wilt filteren voor netwerken die door Infoblox gegenereerde IP-adressen gebruiken, gebruikt u de volgende eigenschappen op het tabblad IPAM-integratie. De filtereigenschappen zijn beschikbaar wanneer u het externe IPAM-integratiepunt voor Infoblox maakt of bewerkt.

Deze filters zijn alleen beschikbaar met vRealize Automation 8.3 en hoger en met [Infoblox-invoegtoepassing versie 1.3](#) en hoger (bijvoorbeeld [Infoblox-invoegtoepassing versie 1.4](#)).

Opmerking [Infoblox-invoegtoepassing versie 1.3](#) kan worden gebruikt met vRealize Automation 8.1 of 8.2, maar alleen in bepaalde situaties en met de nodige voorzichtigheid zoals is beschreven in het KB-artikel over de [compatibiliteit van Infoblox 1.3 met vRealize Automation 8.x \(82142\)](#).

- `Infoblox.IPAM.NetworkContainerFilter`

Filtert op netwerkcontainers.

- `Infoblox.IPAM.NetworkFilter`

Filter op netwerken.

- `Infoblox.IPAM.RangeFilter`

Filter op IP-adresbereiken.

Wees voorzichtig met het toepassen van deze gegevensverzamelingsfilters op netwerken waarvoor al gegevens zijn verzameld. Als u filters toepast om te voorkomen dat voor bepaalde netwerken gegevens worden verzameld, worden de netwerken waarvoor geen gegevens worden verzameld, beschouwd als overbodig en verwijderd uit vRealize Automation. De uitzondering hierop zijn netwerken die zijn gekoppeld aan vRealize Automation-subnetten. Netwerken waarvoor eerder gegevens werden verzameld maar die niet meer worden gedetecteerd en waarvoor geen gegevens meer worden verzameld, bijvoorbeeld omdat ze uit de taak voor het verzamelen van gegevens zijn gefilterd, worden verwijderd uit de vRealize Automation-database. Als de netwerken waarvoor eerder gegevens werden verzameld echter in gebruik zijn in vRealize Automation, worden ze niet verwijderd.

Deze filters worden als queryparameters toegepast in de zoekopdrachten voor de verschillende netwerkobjecten. U kunt alle zoekparameters gebruiken die door Infoblox worden ondersteund. U filtert op CIDR- of uitbreidbare kenmerken die zijn gebaseerd op reguliere expressies of exacte overeenkomsten. De indeling gebruikt de Infoblox WAPI-filtratie-indeling, zoals beschreven in [Infoblox WAPI-documentatie](#). Methoden voor filtering op CIDR of uitbreidbare kenmerken worden weergegeven in de volgende voorbeelden:

- Filter gebaseerd op CIDR voor netwerken en netwerkcontainers. Voorbeelden:

- Exacte overeenkomst - `Infoblox.IPAM.NetworkFilter: network=192.168.0.0`

- Vergelijken op uitbreidbaar kenmerk - `Infoblox.IPAM.NetworkFilter: network~=192.168`

- Filter gebaseerd op CIDR voor IP-adresbereik. Voorbeeld:

Vergelijken op reguliere expressie en netwerkweergavenaam - `Infoblox.IPAM.RangeFilter: network~=192.168.&network_view=my_view`

- Filter op basis van uitbreidbare kenmerken voor netwerken, IP-bereiken en netwerkcontainers.

Syntaxis gebruikt de indeling *filter_name=*ext_attr=ext_attr_value*. Voorbeelden:

- Exacte overeenkomst - `*Building=Data Center`
- Vergelijken op reguliere expressie met '~' - `*Building~=*Center`
- Hoofdlettergevoelig vergelijken met ':' - `*Building:=data center`
- Overeenkomst uitsluiten met '!' - `*Building!=Data Center`
- Vergelijken op reguliere expressie (hoofdlettergevoelig en uitsluiten kunnen worden gecombineerd): `*Building! ~:=Data Cent / *Building~:=center`
- Filter gebaseerd op CIDR- en uitbreidbaarheidskenmerken met behulp van de syntaxis uit de bovenstaande filtermethoden. Voorbeeld:

```
network=192.168.&*Building=Data Center
```

Zie [Infoblox Supported Expressions for Search Parameters](#) en de [Infoblox REST API Reference Guide](#) voor meer informatie over het gebruik van uitbreidbaarheidskenmerken en reguliere expressies in deze eigenschappen.

Cloud Assembly voor uw organisatie instellen

3

Als Cloud Assembly-beheerder moet u inzicht hebben in de gebruikersrollen en verbindingen met uw cloudaccountleverancier en integratieapplicaties instellen.

Wanneer u de cloudaccounts en -integraties configureert, configureert u de communicatie tussen Cloud Assembly en die doelsystemen.

Dit hoofdstuk omvat de volgende onderwerpen:

- [Wat zijn de vRealize Automation-gebruikersrollen](#)
- [Cloudaccounts aan Cloud Assembly toevoegen](#)
- [vRealize Automation integreren met andere applicaties](#)
- [Wat zijn onboardingplannen in Cloud Assembly](#)
- [Geavanceerde configuratie voor Cloud Assembly-omgeving](#)

Wat zijn de vRealize Automation-gebruikersrollen

vRealize Automation heeft verschillende niveaus van gebruikersrollen. Dit niveau beheerst de toegang tot de organisatie, de services, de projecten die de cloudsjablonen, catalogusitems en pijplijnen produceren of gebruiken, en de mogelijkheid om gebruik te maken van de afzonderlijke onderdelen van de gebruikersinterface, of deze te bekijken. Deze verschillende niveaus geven cloudbeheerders verschillende tools om elk niveau van granulariteit toe te passen dat nodig is voor hun operationele behoeften.

Algemene beschrijvingen van functies

De gebruikersrollen worden op verschillende niveaus gedefinieerd. De serviceniveaurollen worden voor elke service gedefinieerd.

Onder deze tabel vindt u meer informatie over de servicerollen.

Rol	Algemene machtigingen	Waar de rol is gedefinieerd
Eigenaar van de organisatie	<p>Heeft toegang tot de console en voegt gebruikers toe aan de organisatie.</p> <p>De eigenaar van de organisatie kan geen toegang krijgen tot een service, tenzij hij een servicerol heeft.</p> <p>Meer informatie over de Organisatiegebruikersrollen</p>	Organisatieconsole
Lid van de organisatie	<p>Kan toegang krijgen tot de console. Het organisatielid kan geen service openen, tenzij hij een servicerol heeft.</p> <p>Meer informatie over de Organisatiegebruikersrollen</p>	Organisatieconsole
Servicebeheerder	<p>Heeft toegang tot de console en heeft volledige bevoegdheden voor bekijken, bijwerken en verwijderen in de service.</p> <ul style="list-style-type: none"> ■ Cloud Assembly-servicerollen ■ Service Broker-servicerollen ■ Code Stream-servicerollen ■ Servicerollen voor de vRA-migratieassistent ■ Servicerollen voor Orchestrator ■ De servicerol voor SaltStack Config 	Organisatieconsole
Servicegebruiker	<p>Kan toegang krijgen tot de console en de service met beperkte machtigingen.</p> <p>Het servicelid heeft een beperkte gebruikersinterface. Wat hij kan zien of doen is afhankelijk van zijn projectlidmaatschap.</p> <ul style="list-style-type: none"> ■ Cloud Assembly-servicerollen ■ Service Broker-servicerollen ■ Code Stream-servicerollen 	Organisatieconsole
Servicebekijker	<p>Heeft toegang tot de console en de service in de modus Alleen weergeven.</p> <ul style="list-style-type: none"> ■ Cloud Assembly-servicerollen ■ Service Broker-servicerollen ■ Code Stream-servicerollen ■ Servicerollen voor de vRA-migratieassistent ■ Servicerollen voor Orchestrator 	Organisatieconsole
Uitvoerder (alleen Code Stream)	<p>Kan toegang krijgen tot de console en de uitvoering van pijplijnen beheren.</p> <p>Code Stream-servicerollen</p>	Organisatieconsole

Rol	Algemene machtigingen	Waar de rol is gedefinieerd
Orchestrator-werkstroomontwerper (alleen Orchestrator)	Kan eigen vRealize Orchestrator-clientinhoud maken, uitvoeren, bewerken en verwijderen. Kan eigen inhoud toevoegen aan de toegewezen groep. Heeft geen toegang tot de functies voor beheer en probleemoplossing van de vRealize Orchestrator-client. Servicerollen voor Orchestrator	Organisatieconsole
Projectrollen	Kan projectresources weergeven en beheren, afhankelijk van de rol van het project. Projectrollen zijn onder meer beheerder, lid en bekijker. Organisatie- en servicegebruikersrollen in vRealize Automation	Cloud Assembly, Service Broker en Code Stream
Custom rollen	De rechten worden gedefinieerd door de Cloud Assembly-beheerder voor alle services. De gebruiker moet ten minste de rol van servicebekijker in de relevante services hebben, zodat hij toegang heeft tot de service. De custom rollen hebben voorrang op de servicerollen. Custom gebruikersrollen in vRealize Automation	Cloud Assembly en Service Broker
Ingebouwde rol van infrastructuurbeheerder	Geeft vooraf gedefinieerde rechten voor taken in vRealize Automation. Hoe kan ik de ingebouwde rol van Cloud Assembly-infrastructuurbeheerder aan een gebruiker toewijzen?	De API gebruiken

Organisatie- en servicegebruikersrollen in vRealize Automation

De organisatie- en servicegebruikersrollen die u heeft gedefinieerd voor de Cloud Assembly-, Service Broker- en Code Stream-services bepalen wat de gebruiker in elke service kan zien en doen.

Organisatiegebruikersrollen

Gebruikersrollen worden voor de organisatie in de vRealize Automation-console gedefinieerd door een organisatie-eigenaar. Er zijn twee typen rollen: organisatierollen en servicerollen.

De organisatierollen zijn algemeen en van toepassing op alle services in de organisatie. De rollen op organisatieniveau zijn de rol Organisatie-eigenaar of Organisatielid.

Zie [vRealize Automation beheren](#) voor meer informatie over de organisatierollen.

De Cloud Assembly-servicerollen, die servicespecifieke rechten zijn, worden ook toegewezen op organisatieniveau in de console.

Servicerollen

Deze servicerollen worden toegewezen door de eigenaar van de organisatie.

Dit artikel bevat informatie over de volgende services.

- [Cloud Assembly-servicerollen](#)
- [Service Broker-servicerollen](#)
- [Code Stream-servicerollen](#)
- [Servicerollen voor de vRA-migratieassistent](#)
- [Servicerollen voor Orchestrator](#)
- [De servicerol voor SaltStack Config](#)

Cloud Assembly-servicerollen

De Cloud Assembly-servicerollen bepalen wat u kunt zien en doen in Cloud Assembly. Deze servicerollen worden in de console gedefinieerd door een organisatie-eigenaar.

Tabel 3-1. Beschrijvingen van Cloud Assembly-servicerollen

Rol	Beschrijving
Cloud Assembly-beheerder	Een gebruiker die lees- en schrijftoegang heeft tot de volledige gebruikersinterface en API-resources. Dit is de enige gebruikersrol die alles kan zien en doen, inclusief cloudaccounts toevoegen, nieuwe projecten maken en een projectbeheerder toewijzen.
Cloud Assembly-gebruiker	Een gebruiker die niet de rol van Cloud Assembly-beheerder heeft. In een Cloud Assembly-project voegt de beheerder gebruikers toe aan projecten als projectleden, beheerders of lezers. De beheerder kan ook een projectbeheerder toevoegen.
Cloud Assembly-kijker	Een gebruiker die leestoegang heeft om informatie te bekijken, maar geen waarden kan maken, bijwerken of verwijderen. Dit is een alleen-lezenrol in alle projecten. Gebruikers met de rol van lezer kunnen alle informatie zien die beschikbaar is voor de beheerder. Ze kunnen geen acties uitvoeren tenzij u ze projectbeheerder of projectlid maakt. Als de gebruiker is gekoppeld aan een project, hebben ze de rechten voor de rol. De projectkijker breidt hun rechten niet uit zoals de rol van beheerder of lid dit doet.

Naast de servicerollen heeft Cloud Assembly projectrollen. Elk project is beschikbaar in alle services.

De projectrollen worden gedefinieerd in Cloud Assembly en kunnen verschillen tussen projecten.

In de volgende tabellen, waarin wordt uitgelegd wat de verschillende service- en projectrollen kunnen zien en doen, moet u er rekening mee houden dat de servicebeheerders volledige rechten hebben voor alle gebieden van de gebruikersinterface.

De beschrijvingen van projectrollen helpen u te bepalen welke rechten u aan uw gebruikers geeft.

- Projectbeheerders gebruiken de infrastructuur die door de servicebeheerder is gemaakt, om ervoor te zorgen dat hun projectleden de resources hebben die nodig zijn voor hun ontwikkelingstaken.
- Projectleden werken binnen hun projecten om cloudsjablonen te ontwerpen en te implementeren. Uw projecten kunnen alleen resources bevatten waarvan u eigenaar bent, of resources die met andere projectleden worden gedeeld.
- Projectkijkers zijn beperkt tot alleen-lezen toegang, behalve in een paar gevallen waarin zij niet-destructieve handelingen kunnen uitvoeren, zoals het downloaden van cloudsjablonen.
- Projectsupervisors zijn goedkeurders in Service Broker voor hun projecten waar een goedkeuringsbeleid is gedefinieerd met een projectsupervisorgoedkeurder. Om de supervisor enige context te geven voor goedkeuringen, kunt u ook overwegen om deze de rol van projectlid of kijker te geven.

Tabel 3-2. Cloud Assembly-servicerollen en -projectrollen

UI-context	Taak	Cloud Assembly-beheerder	Cloud Assembly-kijker	Cloud Assembly-gebruiker		
				Gebruiker moet een projectbeheerder of -lid zijn om projectgerelateerde taken te zien en uit te voeren		
				Projectbeheerder	Projectleden	Projectkijker
Toegang krijgen tot Cloud Assembly						
Console	In de vRA-console kunt u Cloud Assembly zien en openen	Ja	Ja	Ja	Ja	Ja
Infrastructuur						
	Het tabblad Infrastructuur zien en openen	Ja	Ja	Ja	Ja	Ja
Configureren - Projecten	Projecten maken	Ja				
	Waarden van projectsamenvatting, inrichting, Kubernetes, integraties en testprojectconfiguraties bijwerken of verwijderen.	Ja				
	Gebruikers en groepen toevoegen en rollen aan projecten toewijzen.	Ja		Ja. Uw projecten.		
	Projecten weergeven	Ja	Ja	Ja. Uw projecten	Ja. Uw projecten	Ja. Uw projecten

Tabel 3-2. Cloud Assembly-servicerollen en -projectrollen (vervolg)

UI-context	Taak	Cloud Assembly-beheerder	Cloud Assembly-kijker	Cloud Assembly-gebruiker		
				Gebruiker moet een projectbeheerder of -lid zijn om projectgerelateerde taken te zien en uit te voeren		
				Projectbeheerder	Projectleden	Projectkijkers
Configureren - Cloudzones	Cloudzones maken, bijwerken of verwijderen	Ja				
	Cloudzones weergeven	Ja	Ja			
	Het dashboard Inzichten van de cloudzone weergeven	Ja	Ja			
	Waarschuwingen voor cloudzones weergeven	Ja	Ja			
Configureren - Kubernetes-zones	Kubernetes-zones maken, bijwerken of verwijderen	Ja				
	Kubernetes-zones weergeven	Ja	Ja			
Configureren - Soorten	Soorten maken, bijwerken of verwijderen	Ja				
	Soorten weergeven	Ja	Ja			
Configureren - Imago-toewijzingen	Imago-toewijzingen maken, bijwerken of verwijderen	Ja				
	Imago-toewijzingen weergeven	Ja	Ja			
Configureren - Netwerkprofielen	Netwerkprofielen maken, bijwerken of verwijderen	Ja				
	Netwerkprofielen voor images weergeven	Ja	Ja			
Configureren - Opslagprofielen	Opslagprofielen maken, bijwerken of verwijderen	Ja				
	Opslagprofielen voor images weergeven	Ja	Ja			
Configureren - Prijskaarten	Prijskaarten maken, bijwerken of verwijderen	Ja				
	De prijskaarten weergeven	Ja	Ja			
Configureren - Tags	Tags maken, bijwerken of verwijderen	Ja				
	Tags weergeven	Ja	Ja			
Resources - Berekenen	Tags aan gedetecteerde computerbronnen toevoegen	Ja				
	Gedetecteerde computerbronnen weergeven	Ja	Ja			

Tabel 3-2. Cloud Assembly-servicerollen en -projectrollen (vervolg)

UI-context	Taak	Cloud Assembly-beheerder	Cloud Assembly-kijker	Cloud Assembly-gebruiker		
				Gebruiker moet een projectbeheerder of -lid zijn om projectgerelateerde taken te zien en uit te voeren		
				Projectbeheerder	Projectleden	Projectkijkers
Resources - Netwerken	Netwerktags, IP-bereiken en IP-adressen aanpassen	Ja				
	Gedetecteerde netwerkresources weergeven	Ja	Ja			
Resources - Beveiliging	Tags aan gedetecteerde beveiligingsgroepen toevoegen	Ja				
	Gedetecteerde beveiligingsgroepen weergeven	Ja	Ja			
Resources - Opslag	Tags aan gedetecteerde opslag toevoegen	Ja				
	Opslag weergeven	Ja	Ja			
Resources - Kubernetes	Kubernetes-clusters implementeren of toevoegen en naamruimten maken of toevoegen	Ja				
	Kubernetes-clusters en -naamruimten weergeven	Ja	Ja	Ja. Uw projecten	Ja. Uw projecten	Ja. Uw projecten
Activiteit - Aanvragen	Records voor implementatieaanvragen verwijderen	Ja				
	Records voor implementatieaanvragen weergeven	Ja	Ja	Ja. Uw projecten	Ja. Uw projecten	Ja. Uw projecten
Activiteit - Gebeurtenislogboeken	Gebeurtenislogboeken weergeven	Ja	Ja	Ja. Uw projecten	Ja. Uw projecten	Ja. Uw projecten
Verbindingen - Cloudaccounts	Cloudaccounts maken, bijwerken of verwijderen	Ja				
	Cloudaccounts weergeven	Ja	Ja			
Verbindingen - Integraties	Integraties maken, bijwerken of verwijderen	Ja				
	Integraties weergeven	Ja	Ja			
Onboarding	Onboardingplannen maken, bijwerken of verwijderen	Ja				
	Onboardingplannen weergeven	Ja	Ja			Ja. Uw projecten
Uitbreidbaarheid						

Tabel 3-2. Cloud Assembly-servicerollen en -projectrollen (vervolg)

UI-context	Taak	Cloud Assembly-beheerder	Cloud Assembly-kijker	Cloud Assembly-gebruiker Gebruiker moet een projectbeheerder of -lid zijn om projectgerelateerde taken te zien en uit te voeren		
				Projectbeheerder	Projectleden	Projectkijkers
	Het tabblad Uitbreidbaarheid zien en openen	Ja	Ja			Ja
Gebeurtenissen	Uitbreidbaarheidsgebeurtenissen weergeven	Ja	Ja			
Abonnementen	Uitbreidbaarheidsabonnementen maken, bijwerken of verwijderen	Ja				
	Abonnementen deactiveren	Ja				
	Abonnementen weergeven	Ja	Ja			
Bibliotheek - Gebeurtenisonderwerpen	Gebeurtenisonderwerpen weergeven	Ja	Ja			
Bibliotheek - Acties	Uitbreidbaarheidsacties maken, bijwerken of verwijderen	Ja				
	Uitbreidbaarheidsacties weergeven	Ja	Ja			
Bibliotheek - Werkstromen	Uitbreidbaarheidswerkstromen weergeven	Ja	Ja			
Activiteit - Actie-uitvoeringen	Uitvoeringen van uitbreidbaarheidsacties annuleren of verwijderen	Ja				
	Uitvoeringen van uitbreidbaarheidsacties weergeven	Ja	Ja			Ja. Uw projecten
Activiteit - Werkstroomuitvoeringen	Uitvoeringen voor uitbreidbaarheidswerkstromen weergeven	Ja	Ja			
Ontwerp						
Ontwerp	Open het tabblad Ontwerp	Ja	Ja	Ja.	Ja.	Ja.
Cloudsjablonen	Cloudsjablonen maken, bijwerken en verwijderen	Ja		Ja. Uw projecten	Ja. Uw projecten	
	Cloudsjablonen weergeven	Ja	Ja	Ja. Uw projecten	Ja. Uw projecten	Ja. Uw projecten
	Cloudsjablonen downloaden	Ja	Ja	Ja. Uw projecten	Ja. Uw projecten	Ja. Uw projecten
	Cloudsjablonen uploaden	Ja		Ja. Uw projecten	Ja. Uw projecten	
	Cloudsjablonen implementeren	Ja		Ja. Uw projecten	Ja. Uw projecten	

Tabel 3-2. Cloud Assembly-servicerollen en -projectrollen (vervolg)

UI-context	Taak	Cloud Assembly-beheerder	Cloud Assembly-kijker	Cloud Assembly-gebruiker Gebruiker moet een projectbeheerder of -lid zijn om projectgerelateerde taken te zien en uit te voeren		
				Projectbeheerder	Projectleden	Projectkijkers
	Versie van cloudsjablonen weergeven en herstellen	Ja		Ja. Uw projecten	Ja. Uw projecten	
	Cloudsjablonen vrijgeven aan de catalogus	Ja		Ja. Uw projecten	Ja. Uw projecten	
Custom resources	Aangepaste resources maken, bijwerken of verwijderen	Ja				
	Custom resources weergeven	Ja	Ja	Ja. Uw projecten	Ja. Uw projecten	Ja. Uw projecten
Aangepaste acties	Aangepaste acties maken, bijwerken of verwijderen	Ja				
	Aangepaste acties weergeven	Ja	Ja	Ja. Uw projecten	Ja. Uw projecten	Ja. Uw projecten
Resources						
	Het tabblad Resources bekijken en openen	Ja	Ja	Ja	Ja	Ja
Implementaties	Implementaties, inclusief implementatiedetails, implementatiegeschiedenis en informatie over prijs, bewaking, waarschuwingen, optimalisatie en probleemoplossing weergeven	Ja	Ja	Ja. Uw projecten	Ja. Uw projecten	Ja. Uw projecten
	Waarschuwingen beheren	Ja		Ja. Uw projecten	Ja. uw projecten	
	Acties voor dag 2 uitvoeren op implementaties op basis van beleidsregels	Ja		Ja. Uw projecten	Ja. Uw projecten	
Resources - Alle resources	Alle gedetecteerde resources weergeven	Ja	Ja			
	Voer acties voor dag 2 uit op gedetecteerde resources. Acties zijn alleen beschikbaar op machines en zijn beperkt tot in- en uitschakelen voor alle machines, en remote console voor vSphere-machines.	Ja				
Resources - Alle resources	Geïmplementeerde, geonboarde en gemigreerde resources weergeven	Ja	Ja	Ja. Uw projecten.	Ja. Uw projecten.	Ja. Uw projecten.

Tabel 3-2. Cloud Assembly-servicerollen en -projectrollen (vervolg)

UI-context	Taak	Cloud Assembly-beheerder	Cloud Assembly-kijker	Cloud Assembly-gebruiker		
				Gebruiker moet een projectbeheerder of -lid zijn om projectgerelateerde taken te zien en uit te voeren		
				Projectbeheerder	Projectleden	Projectkijkers
	Acties voor dag 2 uitvoeren op geïmplementeerde, geonboarde en gemigreerde resources op basis van beleidsregels	Ja	Ja	Ja. Uw projecten.	Ja. Uw projecten.	
Resources - Virtuele machines	Gedetecteerde machines weergeven	Ja	Ja			
	Voer acties voor dag 2 uit op gedetecteerde machines. Acties zijn beperkt tot in- en uitschakelen en remote console voor vSphere-machines.	Ja				
	Nieuwe VM maken	Ja				
	Bekijk geïmplementeerde, geonboarde en gemigreerde resources.	Ja		Ja. Uw projecten.	Ja. Uw projecten.	Ja. Uw projecten.
	Acties voor dag 2 uitvoeren op geïmplementeerde, geonboarde en gemigreerde resources op basis van beleidsregels	Ja		Ja. Uw projecten.	Ja. Uw projecten.	
Resources - Volumes	Gedetecteerde volumes weergeven	Ja	Ja			
	Geen acties voor dag 2 beschikbaar					
	Geïmplementeerde, geonboarde en gemigreerde volumes weergeven	Ja	Ja	Ja. Uw projecten.	Ja. Uw projecten.	Ja. Uw projecten.
	Acties voor dag 2 uitvoeren op geïmplementeerde, geonboarde en gemigreerde volumes op basis van beleidsregels	Ja		Ja. Uw projecten.	Ja. Uw projecten.	
Resources - Netwerk en beveiliging	Gedetecteerde netwerken, load balancers en beveiligingsgroepen weergeven	Ja	Ja			
	Geen acties voor dag 2 beschikbaar					
	Geïmplementeerde, geonboarde en gemigreerde netwerken, load balancers en beveiligingsgroepen weergeven	Ja	Ja	Ja. Uw projecten.	Ja. Uw projecten.	Ja. Uw projecten.

Tabel 3-2. Cloud Assembly-servicerollen en -projectrollen (vervolg)

UI-context	Taak	Cloud Assembly-beheerder	Cloud Assembly-kijker	Cloud Assembly-gebruiker		
				Gebruiker moet een projectbeheerder of -lid zijn om projectgerelateerde taken te zien en uit te voeren		
				Projectbeheerder	Projectleden	Projectkijker
	Acties voor dag 2 uitvoeren op geïmplementeerde, geïmplementeerde en gemigreerde netwerken, load balancers en beveiligingsgroepen op basis van beleidsregels	Ja		Ja. Uw projecten.	Ja. Uw projecten.	
Waarschuwingen						
	Het tabblad Catalogus bekijken en openen	Ja	Ja	Ja	Ja	Ja
	Waarschuwingen beheren	Ja		Ja. Uw projecten	Ja. Uw projecten	
	Waarschuwingen weergeven	Ja	Ja	Ja. Uw projecten	Ja. Uw projecten	Ja. Uw projecten

Service Broker-servicerollen

De Service Broker-servicerollen bepalen wat u kunt zien en doen in Service Broker. Deze servicerollen worden in de console gedefinieerd door een organisatie-eigenaar.

Tabel 3-3. Beschrijvingen van Service Broker-servicerollen

Rol	Beschrijving
Service Broker-beheerder	Moet lees- en schrijftoegang hebben tot de volledige gebruikersinterface en API-resources. Dit is de enige gebruikersrol die alle taken kan uitvoeren, waaronder het maken van een nieuw project en het toewijzen van een projectbeheerder.
Service Broker-gebruiker	Elke gebruiker die niet de rol van Service Broker-beheerder heeft. In een Service Broker-project voegt de beheerder gebruikers toe aan projecten als projectleden, beheerders of lezers. De beheerder kan ook een projectbeheerder toevoegen.
Service Broker-kijker	Een gebruiker die leestoegang heeft om informatie te bekijken, maar geen waarden kan maken, bijwerken of verwijderen. Gebruikers met de rol van lezer kunnen alle informatie zien die beschikbaar is voor de beheerder. Ze kunnen geen acties uitvoeren tenzij u ze projectbeheerder of projectlid maakt. Als de gebruiker is gekoppeld aan een project, hebben ze de rechten voor de rol. De projectkijker breidt hun rechten niet uit zoals de rol van beheerder of lid dit doet.

Naast de servicerollen heeft Service Broker projectrollen. Elk project is beschikbaar in alle services.

De projectrollen worden gedefinieerd in Service Broker en kunnen verschillen tussen projecten.

In de volgende tabellen, waarin wordt uitgelegd wat de verschillende service- en projectrollen kunnen zien en doen, moet u er rekening mee houden dat de servicebeheerders volledige rechten hebben voor alle gebieden van de gebruikersinterface.

Gebruik de volgende beschrijvingen van projectrollen om u te helpen bepalen welke rechten u uw gebruikers wilt geven.

- Projectbeheerders gebruiken de infrastructuur die door de servicebeheerder is gemaakt, om ervoor te zorgen dat hun projectleden de resources hebben die nodig zijn voor hun ontwikkelingstaken.
- Projectleden werken binnen hun projecten om cloudsjablonen te ontwerpen en te implementeren. In de volgende tabel kunnen uw projecten alleen resources bevatten waarvoor u eigenaar bent, of resources die met andere projectleden worden gedeeld.
- Projectkijkers zijn beperkt tot alleen-lezen toegang.
- Projectsupervisors zijn goedkeurders in Service Broker voor hun projecten waar een goedkeuringsbeleid is gedefinieerd met een projectsupervisorgoedkeurder. Om de supervisor enige context te geven voor goedkeuringen, kunt u ook overwegen om deze de rol van projectlid of kijker te geven.

Tabel 3-4. Service Broker-servicerollen en -projectrollen

UI-context	Taak	Service Broker-beheerder	Service Broker-kijker	Service Broker-gebruiker			
				De gebruiker moet een projectbeheerder zijn om projectrollen te zien en uit te voeren.			
				Projectbeheerder	Projectleden	Projectkijker	Projectsupervisor
Toegang krijgen tot Service Broker							
Console	In de console kunt u Service Broker zien en openen	Ja	Ja	Ja	Ja	Ja	Ja
Infrastructuur							
	Het tabblad Infrastructuur zien en openen	Ja	Ja				
Configureren - Projecten	Projecten maken	Ja					
	Waarden van projectsamenvatting, inrichting, Kubernetes, integraties en testprojectconfiguraties bijwerken of verwijderen.	Ja					

Tabel 3-4. Service Broker-servicerollen en -projectrollen (vervolg)

UI-context	Taak	Service Broker-beheerder	Service Broker-kijker	Service Broker-gebruiker De gebruiker moet een projectbeheerder zijn om projectrollen te zien en uit te voeren.			
				Projectbeheerder	Projectleden	Projectkijker	Projectbeheerder
	Gebruikers en groepen toevoegen en rollen aan projecten toewijzen.	Ja		Ja. Uw projecten.			
	Projecten weergeven	Ja	Ja	Ja. Uw projecten	Ja. Uw projecten	Ja. Uw projecten	
Configureren - Cloudzones	Cloudzones maken, bijwerken of verwijderen	Ja					
	Cloudzones weergeven	Ja	Ja				
Configureren - Kubernetes-zones	Kubernetes-zones maken, bijwerken of verwijderen	Ja					
	Kubernetes-zones weergeven	Ja	Ja				
Verbindingen - Cloudaccounts	Cloudaccounts maken, bijwerken of verwijderen	Ja					
	Cloudaccounts weergeven	Ja	Ja				
Verbindingen - Integraties	Integraties maken, bijwerken of verwijderen	Ja					
	Integraties weergeven	Ja	Ja				
Activiteit - Aanvragen	Records voor implementatieaanvragen verwijderen	Ja					
	Records voor implementatieaanvragen weergeven	Ja					
Activiteit - Gebeurtenislogboeken	Gebeurtenislogboeken weergeven	Ja					
Inhoud en beleidsregels							
	Het tabblad Inhoud en beleidsregels zien en openen	Ja	Ja				
Inhoudsbronnen	Inhoudsbronnen maken, bijwerken of verwijderen	Ja					
	Inhoudsbronnen weergeven	Ja	Ja				
Inhoud delen	Gedeelde inhoud toevoegen of verwijderen	Ja					

Tabel 3-4. Service Broker-servicerollen en -projectrollen (vervolg)

UI-context	Taak	Service Broker-beheerder	Service Broker-kijker	Service Broker-gebruiker De gebruiker moet een projectbeheerder zijn om projectrollen te zien en uit te voeren.			
				Projectbeheerder	Projectleden	Projectkijker	Projectkijker
Inhoud	Gedeelde inhoud weergeven	Ja	Ja				
	Formulier aanpassen en item configureren	Ja					
	Inhoud weergeven	Ja	Ja				
Beleidsregels - Definities	Beleidsdefinities maken, bijwerken of verwijderen	Ja					
	Beleidsdefinities weergeven	Ja	Ja				
Beleidsregels - Afdwinging	Afdwingingslogboek weergeven	Ja	Ja				
Meldingen - E-mailserver	Een e-mailserver configureren	Ja					
Catalogus							
	Het tabblad Catalogus zien en openen	Ja	Ja	Ja	Ja	Ja	Ja
	Beschikbare catalogusitems weergeven	Ja	Ja	Ja. Uw projecten	Ja. Uw projecten	Ja. Uw projecten	
	Een catalogusitem aanvragen	Ja		Ja. Uw projecten	Ja. Uw projecten		
Resources							
	Het tabblad Resources bekijken en openen	Ja	Ja	Ja.	Ja	Ja	Ja
Implementaties	Implementaties, inclusief implementatiedetails, implementatiegeschiedenis en informatie over prijs, bewaking, waarschuwingen, optimalisatie en probleemoplossing weergeven	Ja	Ja	Ja. Uw projecten	Ja. Uw projecten	Ja. Uw projecten	
	Waarschuwingen beheren	Ja		Ja. Uw projecten	Ja. Uw projecten		
	Acties voor dag 2 uitvoeren op implementaties op basis van beleidsregels	Ja		Ja. Uw projecten	Ja. Uw projecten		

Tabel 3-4. Service Broker-servicerollen en -projectrollen (vervolg)

UI-context	Taak	Service Broker-beheerder	Service Broker-kijker	Service Broker-gebruiker De gebruiker moet een projectbeheerder zijn om projectrollen te zien en uit te voeren.			
				Projectbeheerder	Projectleden	Projectkijker	Projectbeheerder
Resources - Alle resources	Alle gedetecteerde resources weergeven	Ja	Ja				
	Voer acties voor dag 2 uit op gedetecteerde resources. Acties zijn alleen beschikbaar op machines en zijn beperkt tot in- en uitschakelen voor alle machines, en remote console voor vSphere-machines.	Ja					
Resources - Alle resources	Geïmplementeerde, geonboarde en gemigreerde resources weergeven	Ja	Ja	Ja. Uw projecten.	Ja. Uw projecten.	Ja. Uw projecten.	
	Acties voor dag 2 uitvoeren op geïmplementeerde, geonboarde en gemigreerde resources op basis van beleidsregels	Ja	Ja	Ja. Uw projecten.	Ja. Uw projecten.		
Resources - Virtuele machines	Gedetecteerde machines weergeven	Ja	Ja				
	Voer acties voor dag 2 uit op gedetecteerde machines. Acties zijn beperkt tot in- en uitschakelen en remote console voor vSphere-machines.	Ja					
	Nieuwe VM maken	Ja					
	Bekijk geïmplementeerde, geonboarde en gemigreerde resources.	Ja		Ja. Uw projecten.	Ja. Uw projecten.	Ja. Uw projecten.	
	Acties voor dag 2 uitvoeren op geïmplementeerde, geonboarde en gemigreerde resources op basis van beleidsregels	Ja		Ja. Uw projecten.	Ja. Uw projecten.		

Tabel 3-4. Service Broker-servicerollen en -projectrollen (vervolg)

UI-context	Taak	Service Broker-beheerder	Service Broker-kijker	Service Broker-gebruiker De gebruiker moet een projectbeheerder zijn om projectrollen te zien en uit te voeren.			
				Projectbeheerder	Projectleden	Projectkijker	Projectkrijger
Resources - Volumes	Gedetecteerde volumes weergeven	Ja	Ja				
	Geen acties voor dag 2 beschikbaar						
	Geïmplementeerde, geonboarde en gemigreerde volumes weergeven	Ja	Ja	Ja. Uw projecten.	Ja. Uw projecten.	Ja. Uw projecten.	
	Acties voor dag 2 uitvoeren op geïmplementeerde, geonboarde en gemigreerde volumes op basis van beleidsregels	Ja		Ja. Uw projecten.	Ja. Uw projecten.		
Resources - Netwerk en beveiliging	Gedetecteerde netwerken, load balancers en beveiligingsgroepen weergeven	Ja	Ja				
	Geen acties voor dag 2 beschikbaar						
	Geïmplementeerde, geonboarde en gemigreerde netwerken, load balancers en beveiligingsgroepen weergeven	Ja	Ja	Ja. Uw projecten.	Ja. Uw projecten.	Ja. Uw projecten.	
	Acties voor dag 2 uitvoeren op geïmplementeerde, geonboarde en gemigreerde netwerken, load balancers en beveiligingsgroepen op basis van beleidsregels	Ja		Ja. Uw projecten.	Ja. Uw projecten.		
Goedkeuringen							

Tabel 3-4. Service Broker-servicerollen en -projectrollen (vervolg)

UI-context	Taak	Service Broker-beheerder	Service Broker-kijker	Service Broker-gebruiker De gebruiker moet een projectbeheerder zijn om projectrollen te zien en uit te voeren.			
				Projectbeheerder	Projectleden	Projectkijker	Projectbeheerder
	Het tabblad Goedkeuringen zien en openen	Ja	Ja	Ja	Ja	Ja	Ja
	Reageren op goedkeuringsaanvragen	Ja		Ja. Uw projecten en de beleidsgoedkeurder is projectbeheerder	Alleen als u een benoemde goedkeurder bent	Alleen als u een benoemde goedkeurder bent	Ja. Uw projecten en de beleidsgoedkeurder is projectbeheerder

Code Stream-servicerollen

De Code Stream-servicerollen bepalen wat u kunt zien en doen in Code Stream. Deze rollen worden in de console gedefinieerd door de eigenaar van de organisatie. Elk project is beschikbaar in alle services.

Tabel 3-5. Beschrijvingen van Code Stream-servicerollen

Rol	Beschrijving
Code Stream-beheerder	Een gebruiker die lees- en schrijftoegang heeft tot de volledige gebruikersinterface en API-resources. Dit is de enige gebruikersrol die alles kan zien en doen, inclusief projecten maken, eindpunten integreren, triggers toevoegen, pijplijnen en custom dashboards maken, eindpunten en variabelen markeren als beperkte resources, pijplijnen uitvoeren die beperkte resources gebruiken en verzoeken dat pijplijnen worden gepubliceerd in Service Broker.
Code Stream-ontwikkelaar	Een gebruiker die met pijplijnen kan werken, maar die niet met beperkte eindpunten of variabelen kan werken. Als een pijplijn een beperkt eindpunt of beperkte variabele bevat, moet deze gebruiker goedkeuring krijgen voor de pijplijntaak die het beperkte eindpunt of de beperkte variabele gebruikt.
Code Stream-uitvoerder	Een gebruiker die pijplijnen kan uitvoeren en gebruikersbewerkingstaken kan goedkeuren of weigeren. Deze gebruiker kan pijplijnuitvoeringen hervatten, onderbreken en annuleren, maar kan pijplijnen niet wijzigen.
Code Stream-gebruiker	Een gebruiker die toegang heeft tot Code Stream, maar geen andere machtigingen heeft in Code Stream.
Code Stream-lezer	Een gebruiker die leestoegang heeft om pijplijnen, eindpunten, pijplijnuitvoeringen en dashboards te zien, maar deze niet kan maken, bijwerken of verwijderen. Een gebruiker die ook over de rol van de Servicekijker beschikt, kan alle informatie zien die beschikbaar is voor de beheerder. Ze kunnen geen acties uitvoeren tenzij u ze projectbeheerder of projectlid maakt. Als de gebruiker is gekoppeld aan een project, hebben ze de rechten voor de rol. De projectkijker breidt hun rechten niet uit zoals de rol van beheerder of lid dit doet.

Naast de servicerollen heeft Code Stream projectrollen. Elk project is beschikbaar in alle services. De projectrollen worden gedefinieerd in Code Stream en kunnen verschillen tussen projecten.

Wanneer u de volgende tabellen bekijkt, die u laten zien wat de verschillende service- en projectrollen kunnen zien en doen, moet u onthouden dat de servicebeheerders volledige rechten hebben voor alle gebieden van de gebruikersinterface.

Gebruik de volgende beschrijvingen van projectrollen om u te helpen beslissen welke rechten u wilt toewijzen aan uw gebruikers.

- Projectbeheerders gebruiken de infrastructuur die door de servicebeheerder is gemaakt, om ervoor te zorgen dat hun projectleden de resources hebben die nodig zijn voor hun ontwikkelingstaken. De projectbeheerder kan leden toevoegen.
- Projectleden met een servicefunctie kunnen services gebruiken.
- Projectbekijkers kunnen projecten zien, maar ze kunnen ze niet maken, bijwerken of verwijderen.

Alle acties behalve beperkte betekent dat deze rol toestemming heeft om de acties maken, lezen, bijwerken en verwijderen uit te voeren op entiteiten, behalve voor beperkte variabelen en eindpunten.

Tabel 3-6. Mogelijkheden van Code Stream-servicerol

UI-context	Capaciteiten	Code Stream-beheerdersrol	Code Stream-ontwikkelaarsrol	Code Stream-uitvoerdersrol	Code Stream-kijkersrol	Code Stream-gebruikersrol
Pijplijnen						
	Pijplijnen weergeven	Ja	Ja	Ja	Ja	
	Pijplijnen maken	Ja	Ja			
	Pijplijnen uitvoeren	Ja	Ja	Ja		
	Pijplijnen uitvoeren die beperkte eindpunten of variabelen bevatten	Ja				
	Pijplijnen bijwerken	Ja	Ja			
	Pijplijnen verwijderen	Ja	Ja			
Pijplijnuitvoeringen						
	Pijplijnuitvoeringen weergeven	Ja	Ja	Ja	Ja	

Tabel 3-6. Mogelijkheden van Code Stream-servicerol (vervolg)

UI-context	Capaciteiten	Code Stream-beheerdersrol	Code Stream-ontwikkelaarsrol	Code Stream-uitvoerdersrol	Code Stream-kijkersrol	Code Stream-gebruikersrol
	De pijplijnuitvoeringen hervatten, pauzeren en annuleren	Ja	Ja	Ja		
	Pijplijnen hervatten die stoppen voor goedkeuring bij beperkte resources	Ja				
Aangepaste integraties						
	Aangepaste integraties maken	Ja	Ja			
	Aangepaste integraties lezen	Ja	Ja	Ja	Ja	
	Aangepaste integraties bijwerken	Ja	Ja			
Eindpunten						
	Uitvoeringen weergeven	Ja	Ja	Ja	Ja	
	Uitvoeringen maken	Ja	Ja			
	Uitvoeringen bijwerken	Ja	Ja			
	Uitvoeringen verwijderen	Ja	Ja			
Resources als beperkt markeren						
	Een eindpunt of variabele als beperkt markeren	Ja				
Dashboards						
	Dashboards weergeven	Ja	Ja	Ja	Ja	

Tabel 3-6. Mogelijkheden van Code Stream-servicerol (vervolg)

UI-context	Capaciteiten	Code Stream-beheerdersrol	Code Stream-ontwikkelaarsrol	Code Stream-uitvoerdersrol	Code Stream-kijkersrol	Code Stream-gebruikersrol
	Dashboards maken	Ja	Ja			
	Dashboards bijwerken	Ja	Ja			
	Dashboards verwijderen	Ja	Ja			

Servicerollen voor de vRA-migratieassistent

De servicerollen voor de vRA-migratieassistent bepalen wat u kunt zien en doen in de vRA-migratieassistent en Cloud Assembly. Deze servicerollen worden in de console gedefinieerd door een organisatie-eigenaar.

Tabel 3-7. Beschrijvingen van de servicerollen voor de vRealize Automation-migratieassistent

Rol	Beschrijving
Beheerder van migratieassistent	Een gebruiker die volledige rechten voor bekijken, bijwerken en verwijderen heeft in de vRA-migratieassistent en Cloud Assembly. Deze rol moet ook ten minste de rol van Cloud Assembly-bekijker hebben.
Bekijker van migratieassistent	Een gebruiker die leestoegang heeft om informatie te bekijken, maar geen waarden kan maken, bijwerken of verwijderen in de vRA-migratieassistent of in Cloud Assembly. Deze rol moet ook ten minste de rol van Cloud Assembly-bekijker hebben.

Servicerollen voor Orchestrator

De servicerollen voor Orchestrator bepalen wat u kunt zien en doen in de vRealize Orchestrator-client. Deze servicerollen worden in de console gedefinieerd door een organisatie-eigenaar.

Tabel 3-8. Beschrijvingen van servicerollen voor vRealize Orchestrator

Rol	Beschrijving
Orchestrator-beheerder	Een gebruiker die over volledige rechten voor weergeven, bijwerken en verwijderen beschikt in vRealize Orchestrator. Een beheerder heeft ook toegang tot de inhoud die is gemaakt door specifieke groepen.
Bekijker van Orchestrator	Een gebruiker die leestoegang heeft tot functies en inhoud, inclusief alle groepen en groepsinhoud, maar die geen inhoud kan maken, bijwerken, uitvoeren, verwijderen of exporteren.
Orchestrator-werkstroomontwerper	Een gebruiker die de eigen vRealize Orchestrator-clientinhoud kan maken, uitvoeren, bewerken en verwijderen. De gebruiker kan de eigen inhoud toevoegen aan de toegewezen groep. De werkstroomontwerper heeft geen toegang tot de functies voor beheer en probleemoplossing van de vRealize Orchestrator-client.

De servicerol voor SaltStack Config

De servicerol voor SaltStack Config bepaalt wat u kunt zien en doen in de vRealize Automation. Deze servicerol wordt in de console gedefinieerd door een organisatie-eigenaar.

Tabel 3-9. Beschrijving van de servicerol voor vRealize Automation SaltStack Config

Rol	Beschrijving
Beheerder van SaltStack Config	Een gebruiker die toegang heeft tot de SaltStack Config-tegel op de console wanneer de integratie met Cloud Assembly is geconfigureerd. Als u zich wilt aanmelden op de SaltStack Config-instantie, moet de gebruiker over SaltStack-beheerdersrechten beschikken die zijn gedefinieerd in SaltStack Config. De gebruiker moet ook de rol van Cloud Assembly-beheerder hebben.

Custom gebruikersrollen in vRealize Automation

Als Cloud Assembly-beheerder kunt u custom rollen maken die bepalen wat gebruikers kunnen zien en doen in vRealize Automation. Vervolgens kunt u gebruikers aan deze rollen toewijzen.

Custom rechten voor gebruikersrollen

Met behulp van Cloud Assembly kunt u meer gedetailleerde gebruikersrollen definiëren en vervolgens gebruikers aan deze rollen toewijzen. De custom rollen hebben twee categorieën: weergeven en beheren.

- **Weergeven.** Een gebruiker die aan een rol is toegewezen met deze machtiging kan alle items voor alle projecten in de geselecteerde secties van de gebruikersinterface zien. Deze rol is nuttig voor gebruikers die accounts, configuraties of toegewezen waarden moeten zien.

- **Beheren.** Een gebruiker die is toegewezen aan een rol met deze machtiging kan alle items zien en heeft volledige rechten om toe te voegen, te bewerken en te verwijderen voor alle projecten in de geselecteerde secties van de gebruikersinterface.

Deze machtigingen breiden de rechten uit die worden verleend door de andere rollen en worden niet beperkt door het lidmaatschap van een project. U kunt bijvoorbeeld de rechten van een projectbeheerder uitbreiden om delen van de infrastructuur te beheren of een servicelezer de mogelijkheid geven om goedkeuringsverzoeken te bekijken en deze te beantwoorden.

Als u de gebruikersrollen wilt definiëren en gebruikers wilt toewijzen, opent u Cloud Assembly of Service Broker als servicebeheerder en selecteert u **Infrastructuur > Beheer > Custom rollen**. U kunt de custom rollen in Code Stream niet configureren, maar de rollen zijn van toepassing op alle services.

Tabel 3-10. Custom rollen

Gebruikersinterface	Recht	Beschrijving
Infrastructuur		
	Cloudaccounts weergeven.	Cloudaccounts weergeven.
	Cloudaccounts beheren	Cloudaccounts maken, bijwerken of verwijderen.
	Imagetoewijzingen weergeven	Imagetoewijzingen weergeven.
	Imagetoewijzingen beheren	Imagetoewijzingen maken, bijwerken of verwijderen.
	Soorttoewijzingen weergeven	Soorttoewijzingen weergeven.
	Soorttoewijzingen beheren	Soorttoewijzingen maken, bijwerken of verwijderen.
	Cloudzones weergeven	Cloudzones, inzichten en waarschuwingen weergeven.
	Cloudzones beheren	Cloudzones maken, bijwerken of verwijderen. Waarschuwingen beheren.
	Aanvragen weergeven	Activiteitsaanvragen weergeven.
	Aanvragen beheren	Verwijder aanvragen uit de lijst.
	Integraties weergeven	Integraties weergeven.
	Integraties beheren	Integraties maken, bijwerken of verwijderen.
	Projecten weergeven	Projecten weergeven.

Tabel 3-10. Custom rollen (vervolg)

Gebruikersinterface	Recht	Beschrijving
	Projecten beheren	Projecten maken. Gebruikers toevoegen en rollen aan projecten toewijzen. Waarden van projectsamenvatting, gebruikers, inrichting, Kubernetes, integraties en testprojectconfiguraties bijwerken of verwijderen.
	Onboardingplannen weergeven	Onboardingplannen weergeven
	Onboarding-plannen beheren	Onboarding-plannen maken, bijwerken, uitvoeren of verwijderen
Catalogus		
	Inhoud weergeven	
	Content beheren	Contentresources toevoegen, bijwerken, verwijderen. Content delen. Pas de inhoud aan, inclusief de cataloguspictogrammen en aanvraagformulieren.
Beleidsregels		
	Beleidsregels weergeven	Beleidsdefinities weergeven.
	Beleidsregels beheren.	Beleidsdefinities maken, bijwerken of verwijderen.
Implementaties		
	Implementaties weergeven	Bekijk alle implementaties, inclusief implementatiedetails, implementatiegeschiedenis, waarschuwingen en informatie over probleemoplossing.
	Implementaties beheren	Bekijk alle implementaties, reageer op waarschuwingen en voer alle acties voor dag 2 uit die een beheerder volgens het beleid voor dag 2 mag uitvoeren op implementaties en implementatieonderdelen.
Cloudsjablonen		
	Cloudsjablonen weergeven	Cloudsjablonen weergeven.
	Cloudsjablonen beheren	Maak, update, test, verwijder, beheer versies van, deel cloudsjablonen en geef een cloudsjabloonversie vrij of maak de vrijgave ongedaan.

Tabel 3-10. Custom rollen (vervolg)

Gebruikersinterface	Recht	Beschrijving
	Cloudsjablonen bewerken	Maak, update, test, beheer versies van, deel cloudsjablonen en geef een cloudsjabloonversie vrij of maak de vrijgave ongedaan. De rol heeft geen rechten om cloudsjablonen te verwijderen.
	Cloudsjablonen implementeren	Test en implementeer een cloudsjabloon in een willekeurig project.
	Content in-line cloudsjabloon implementeren	Implementeer een cloudsjabloon in de projecten waaraan de toegewezen personen zijn gekoppeld. De projectrollen kunnen beheerder, lid of lezer zijn.
XaaS		
	Custom resources weergeven	Custom resources weergeven.
	Custom resources beheren	Aangepaste resources maken, bijwerken of verwijderen.
	Resourceacties weergeven	Custom acties weergeven.
	Resourceacties beheren	Aangepaste acties maken, bijwerken of verwijderen
Uitbreidbaarheid		
	Uitbreidbaarheidsresources weergeven	Bekijk gebeurtenissen, abonnementen, gebeurtenisonderwerpen, acties, werkstromen, actie-uitvoeringen en werkstroom-uitvoeringen.
	Uitbreidbaarheidsresources beheren	Maak, update, verwijder en deactiveer uitbreidbaarheidsabonnementen. Uitbreidbaarheidsacties maken, bijwerken of verwijderen. Uitbreidbaarheidsactie-uitvoeringen annuleren of verwijderen.
Pijplijn		
	Pijplijnen beheren	Maak, bewerk en verwijder pijplijn-, eindpunt-, variabele- en triggerconfiguraties. Beperkte modellen worden uitgesloten.

Tabel 3-10. Custom rollen (vervolg)

Gebruikersinterface	Recht	Beschrijving
	Beperkte pijplijnen beheren	Maak, bewerk en verwijder pijplijn-, eindpunt-, variabele- en triggerconfiguraties. Beperkte modellen zijn opgenomen.
	Custom integraties beheren	Aangepaste integraties toevoegen, bewerken en verwijderen.
	Pijplijnen uitvoeren	Voer uitvoeringen en triggers van pijplijnmodellen uit en onderbreek, annuleer, hervat of voer de uitvoeringen en triggers opnieuw uit.
	Beperkte pijplijnen uitvoeren	Voer uitvoeringen en triggers van pijplijnmodellen uit en onderbreek, annuleer, hervat of voer de uitvoeringen en triggers opnieuw uit. Verhelp beperkte eindpunten en variabelen.
	Uitvoeringen beheren	Voer uitvoeringen en triggers van pijplijnmodellen uit en onderbreek, annuleer, hervat of voer de uitvoeringen en triggers opnieuw uit. Verhelp beperkte eindpunten en variabelen. Uitvoeringen verwijderen.
Goedkeuring		
	Goedkeuringen beheren	Bekijk het tabblad Goedkeuringen waar u goedkeuringsaanvragen kunt goedkeuren of afwijzen. Een goedkeurder met deze rol ontvangt geen e-mailmelding over een goedkeuringsaanvraag, tenzij hij een goedkeurder is in het beleid.

Toepassingsvoorbeelden: hoe kunnen gebruikersrollen mij helpen bij het toegangsbeheer voor vRealize Automation

Als cloudbeheerder wilt u kunnen bepalen welke taken uw gebruikers in vRealize Automation kunnen uitvoeren. Afhankelijk van uw beheerdoelstellingen en de verantwoordelijkheden van het team voor applicatieontwikkeling, zijn er verschillende manieren waarop u de gebruikersrollen kunt configureren om deze doelstellingen in te vullen.

De volgende voorbeelden uit Cloud Assembly en Service Broker zijn gebaseerd op drie gebruikssituaties. Deze toepassingsvoorbeelden geven slechts een globaal beeld van de toepassing van gebruikersrollen.

De cloudbeheerder en servicebeheerders vormen de doelgroep van deze toepassingsvoorbeelden.

De toepassingsvoorbeelden zijn op elkaar gebaseerd. Ook als u direct naar toepassingsvoorbeeld 3 wilt gaan, is het raadzaam om eerst de toepassingsvoorbeelden 1 en 2 te bekijken om te snappen waarom u de rollen op de opgegeven wijze configureert.

Het doel van deze gebruiksscenario's is te laten zien hoe gebruikersrollen werken, niet om gedetailleerde informatie te geven over het configureren van de infrastructuur, het beheren van projecten, het maken van cloudsjablonen en het werken met implementaties.

Voordat u begint, moet u weten welke niveaus van gebruikersrollen de cloudbeheerder in de vRealize Automation-console heeft geconfigureerd.

■ Organisatierollen

De organisatierollen bepalen wie de console kan openen.

Als organisatie-eigenaar moet u ervoor zorgen dat alle gebruikers van de services ten minste de rol van organisatielid krijgen.

Rol	Beschrijving
Eigenaar van de organisatie	Een beheerder kan gebruikers toevoegen, de rol van gebruikers wijzigen en gebruikers uit de organisatie verwijderen. De eigenaar bepaalt tot welke services gebruikers toegang hebben.
Lid van de organisatie	Een algemene gebruiker kan zich aanmelden bij de organisatieconsole. Om gebruikers toegang te geven tot de services, moet de organisatie-eigenaar servicerollen toewijzen aan de gebruikers.

■ Servicerollen

De servicerollen bepalen wie toegang heeft tot de toegewezen services.

Als organisatie-eigenaar moet u ervoor zorgen dat de gebruikers die toegang tot de services nodig hebben, de juiste rol krijgen. U gebruikt deze rollen om te bepalen wat een gebruiker met elke service kan doen.

Tabel 3-11. Beschrijvingen van Cloud Assembly-servicerollen

Rol	Beschrijving
Cloud Assembly-beheerder	Een gebruiker die lees- en schrijftoegang heeft tot de volledige gebruikersinterface en API-resources. Dit is de enige gebruikersrol die alles kan zien en doen, inclusief cloudaccounts toevoegen, nieuwe projecten maken en een projectbeheerder toewijzen.
Cloud Assembly-gebruiker	Een gebruiker die niet de rol van Cloud Assembly-beheerder heeft. In een Cloud Assembly-project voegt de beheerder gebruikers toe aan projecten als projectleden, beheerders of lezers. De beheerder kan ook een projectbeheerder toevoegen.
Cloud Assembly-kijker	Een gebruiker die leestoegang heeft om informatie te bekijken, maar geen waarden kan maken, bijwerken of verwijderen. Dit is een alleen-lezenrol in alle projecten. Gebruikers met de rol van lezer kunnen alle informatie zien die beschikbaar is voor de beheerder. Ze kunnen geen acties uitvoeren tenzij u ze projectbeheerder of projectlid maakt. Als de gebruiker is gekoppeld aan een project, hebben ze de rechten voor de rol. De projectkijker breidt hun rechten niet uit zoals de rol van beheerder of lid dit doet.

Tabel 3-12. Beschrijvingen van Service Broker-servicerollen

Rol	Beschrijving
Service Broker-beheerder	Moet lees- en schrijftoegang hebben tot de volledige gebruikersinterface en API-resources. Dit is de enige gebruikersrol die alle taken kan uitvoeren, waaronder het maken van een nieuw project en het toewijzen van een projectbeheerder.
Service Broker-gebruiker	Elke gebruiker die niet de rol van Service Broker-beheerder heeft. In een Service Broker-project voegt de beheerder gebruikers toe aan projecten als projectleden, beheerders of lezers. De beheerder kan ook een projectbeheerder toevoegen.
Service Broker-kijker	Een gebruiker die leestoegang heeft om informatie te bekijken, maar geen waarden kan maken, bijwerken of verwijderen.

Tabel 3-12. Beschrijvingen van Service Broker-servicerollen (vervolg)

Rol	Beschrijving
	Gebruikers met de rol van lezer kunnen alle informatie zien die beschikbaar is voor de beheerder. Ze kunnen geen acties uitvoeren tenzij u ze projectbeheerder of projectlid maakt. Als de gebruiker is gekoppeld aan een project, hebben ze de rechten voor de rol. De projectkijker breidt hun rechten niet uit zoals de rol van beheerder of lid dit doet.

Tabel 3-13. Beschrijvingen van Code Stream-servicerollen

Rol	Beschrijving
Code Stream-beheerder	Een gebruiker die lees- en schrijftoegang heeft tot de volledige gebruikersinterface en API-resources. Dit is de enige gebruikersrol die alles kan zien en doen, inclusief projecten maken, eindpunten integreren, triggers toevoegen, pijplijnen en custom dashboards maken, eindpunten en variabelen markeren als beperkte resources, pijplijnen uitvoeren die beperkte resources gebruiken en verzoeken dat pijplijnen worden gepubliceerd in Service Broker.
Code Stream-ontwikkelaar	Een gebruiker die met pijplijnen kan werken, maar die niet met beperkte eindpunten of variabelen kan werken. Als een pijplijn een beperkt eindpunt of beperkte variabele bevat, moet deze gebruiker goedkeuring krijgen voor de pijplijntaak die het beperkte eindpunt of de beperkte variabele gebruikt.
Code Stream-uitvoerder	Een gebruiker die pijplijnen kan uitvoeren en gebruikersbewerkingstaken kan goedkeuren of weigeren. Deze gebruiker kan pijplijnuitvoeringen hervatten, onderbreken en annuleren, maar kan pijplijnen niet wijzigen.
Code Stream-gebruiker	Een gebruiker die toegang heeft tot Code Stream, maar geen andere machtigingen heeft in Code Stream.
Code Stream-lezer	Een gebruiker die leesttoegang heeft om pijplijnen, eindpunten, pijplijnuitvoeringen en dashboards te zien, maar deze niet kan maken, bijwerken of verwijderen. Een gebruiker die ook over de rol van de Servicekijker beschikt, kan alle informatie zien die beschikbaar is voor de beheerder. Ze kunnen geen acties uitvoeren tenzij u ze projectbeheerder of projectlid maakt. Als de gebruiker is gekoppeld aan een project, hebben ze de rechten voor de rol. De projectkijker breidt hun rechten niet uit zoals de rol van beheerder of lid dit doet.

- Rollen voor projectlidmaatschap

Het projectlidmaatschap bepaalt welke infrastructuurresources en cloudsjablonen beschikbaar zijn.

Het projectlidmaatschap wordt in de service zelf gedefinieerd door een gebruiker met de rol van servicebeheerder. Deze servicebeheerder moet ervoor zorgen dat gebruikers die toegang nodig hebben tot een of meer projecten, de juiste projectrol voor elk project krijgen toegewezen.

Tabel 3-14. Projectrollen

Rol	Beschrijving
Projectbeheerder	Een projectbeheerder kan diens eigen projecten beheren, bijbehorende cloudsjablonen voor deze projecten maken en implementeren, en projectimplementaties voor alle projectleden beheren.
Projectleden	Een projectlid kan cloudsjablonen maken en implementeren die aan hun projecten zijn gekoppeld, zijn eigen implementaties beheren en gedeelde implementaties beheren.
Projectkijker	Een projectlezer is lid van het project, maar heeft slechts alleen-lezen toegang tot de resources, cloudsjablonen en implementaties van dit project.

■ Custom rollen

De custom rollen worden gemaakt door de Cloud Assembly om de rollen van leden en de bekijker te verfijnen.

De procedures in deze toepassingsvoorbeelden zijn bedoeld als toelichting op de gebruikersrollen. Ze bieden geen gedetailleerde of definitieve procedures voor het instellen van vRealize Automation.

Wanneer u rollen configureert, moet u er rekening mee houden dat gebruikers die API-bewerkingen uitvoeren, onderworpen zijn aan de rollen die u hier toewijst.

Voorwaarden

- Controleer of u de rol van eigenaar van de organisatie hebt. Als u inlogt op de console moet het tabblad **Identiteits- en toegangsbeheer** beschikbaar zijn voor u. Zo niet, neem dan contact op met de eigenaar van de organisatie.
- Controleer of u de rol van servicebeheerder hebt voor de verschillende services. Als u niet zeker weet wat uw rol is, neemt u contact op met de eigenaar van de organisatie.
- Controleer of uw gebruikers zijn toegevoegd aan vRealize Automation.

Wanneer u vRealize Automation installeert, worden uw Active Directory-gebruikers toegevoegd als onderdeel van het proces.

- Zie [Organisatie- en servicegebruikersrollen in vRealize Automation](#) voor een gedetailleerdere taak- en rollijst voor verschillende rollen.

Procedure

1 [Eerste toepassingsvoorbeeld voor gebruikersrollen: de vRealize Automation-gebruikersrollen voor een klein applicatieontwikkelingsteam instellen](#)

Als vRealize Automation-cloudbeheerder bent u verantwoordelijk voor het toegangs- en budgetbeheer voor uw infrastructuurresources. U voegt zichzelf en twee anderen toe als beheerders. Dit kleine team kan de ontwikkeling van infrastructuur en cloudsjablonen volledig afstemmen op de zakelijke doelstellingen van de teams die de cloudsjablonen gebruiken. Samen met dit kleine team van beheerders kunt u de cloudsjablonen vervolgens implementeren voor de consumenten zonder beheerdersrechten. Geef niet-beheerders geen toegang tot vRealize Automation.

2 [Gebruiksscenario voor gebruiker 2: vRealize Automation-gebruikersrollen instellen om grotere ontwikkelingsteams en de catalogus te ondersteunen](#)

Als vRealize Automation-organisatie-eigenaar bent u verantwoordelijk voor het toegangs- en budgetbeheer voor uw infrastructuurresources. U beschikt over een team van cloudsjabloonontwikkelaars die op iteratieve wijze sjablonen maken en implementeren voor verschillende projecten totdat deze klaar zijn voor levering aan de consumenten. Vervolgens levert u de implementeerbare resources aan de consumenten in een catalogus.

3 [Gebruikersrol voor gebruiksscenario 3: custom vRealize Automation-gebruikersrollen instellen om systeemrollen te verfijnen](#)

Als vRealize Automation-organisatie-eigenaar of -servicebeheerder beheert u gebruikerstoegang via de rollen van de organisatie- en servicesystemen. U wilt echter ook custom rollen maken voor die geselecteerde gebruikers en taken uitvoeren of content zien die buiten hun systeemrollen valt.

Eerste toepassingsvoorbeeld voor gebruikersrollen: de vRealize Automation-gebruikersrollen voor een klein applicatieontwikkelingsteam instellen

Als vRealize Automation-cloudbeheerder bent u verantwoordelijk voor het toegangs- en budgetbeheer voor uw infrastructuurresources. U voegt zichzelf en twee anderen toe als beheerders. Dit kleine team kan de ontwikkeling van infrastructuur en cloudsjablonen volledig afstemmen op de zakelijke doelstellingen van de teams die de cloudsjablonen gebruiken. Samen met dit kleine team van beheerders kunt u de cloudsjablonen vervolgens implementeren voor de consumenten zonder beheerdersrechten. Geef niet-beheerders geen toegang tot vRealize Automation.

In dit gebruiksscenario bent u de organisatie-eigenaar en hebt u een klein team waarin iedereen de rol van servicebeheerder heeft.

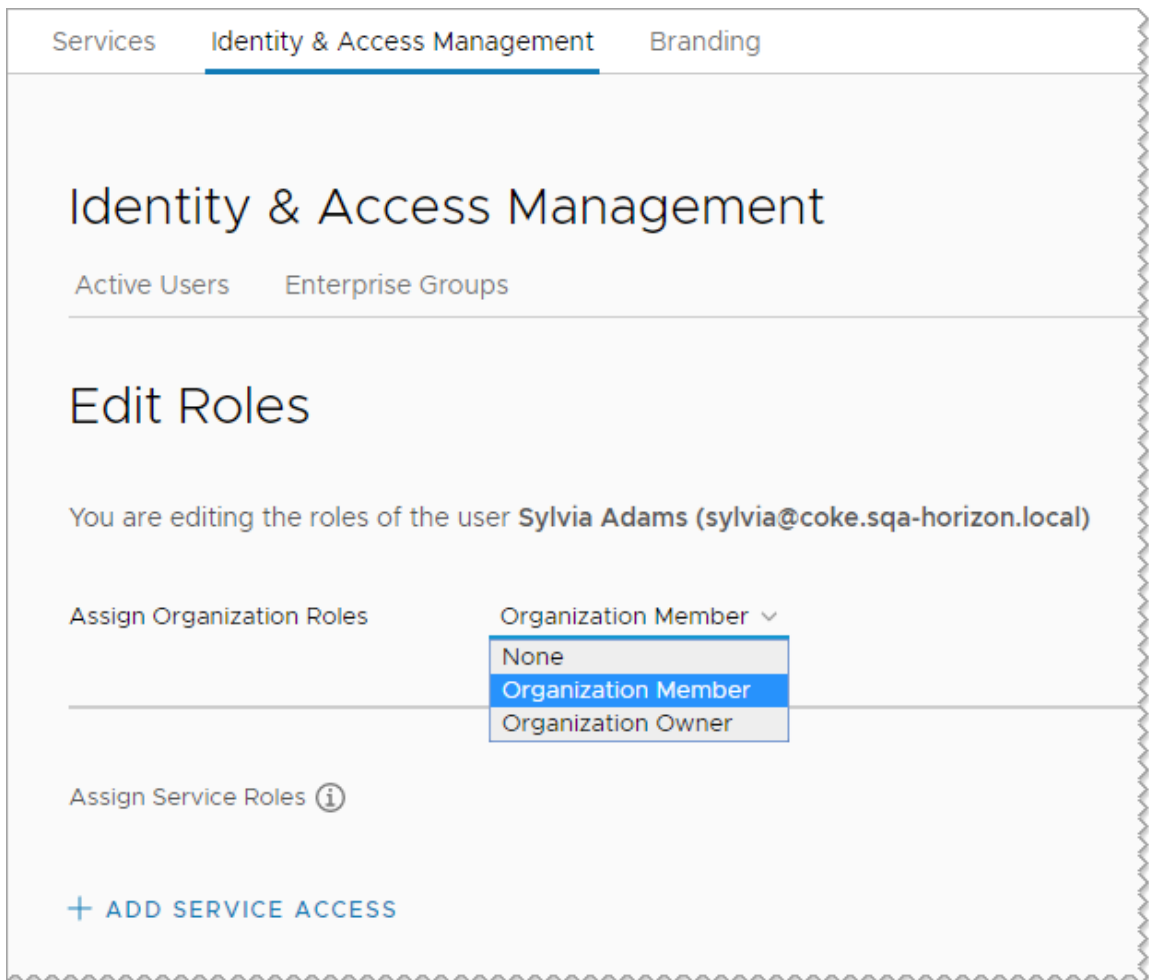
In de volgende procedure ziet u hoe één gebruiker het hele proces doorloopt. U kunt elke stap uitvoeren voor meerdere gebruikers.

Voorwaarden

- Controleer of u voldoet aan alle vereisten zoals vermeld in de inleiding van de toepassingsvoorbeelden. Zie [Toepassingsvoorbeelden: hoe kunnen gebruikersrollen mij helpen bij het toegangsbeheer voor vRealize Automation](#).

Procedure

- 1 Wijs de organisatirollen toe. Klik op **Identiteits- en toegangsbeheer**.
 - a Meld u aan bij de vRealize Automation-console.
 - b Klik op **Identiteits- en toegangsbeheer**.
 - c Selecteer de gebruikersnaam en klik op **Rollen bewerken**.
 - d Selecteer in het vervolgkeuzemenu **Organisatirollen toewijzen** de optie **Organisatielid**.



De rol van organisatielid geeft de gebruiker toegang tot de console en alle services die u aan de organisatieleden toewijst. Ze kunnen geen gebruikers binnen de organisatie beheren.

Laat de pagina Rol bewerken open voor deze gebruiker en ga door met de volgende stap.

- 2 Wijs in dit scenario de Cloud Assembly-beheerdersrol toe aan uzelf en aan niet meer dan twee andere beheerders.

De rol van servicebeheerder heeft volledige rechten om infrastructuur, projecten, cloudsjablonen en implementaties toe te voegen, te bewerken en te verwijderen. Het toewijzen van de beheerdersrol aan één persoon en de gebruikersrol aan iemand anders wordt behandeld in scenario 2. In dit voorbeeld wordt Sylvia gebruikt.

- a Klik op **Servicetoegang toevoegen**.
- b Configureer de gebruiker met de volgende waarde.

Service	Rol
Cloud Assembly	Cloud Assembly-beheerder

[Services](#)
[Identity & Access Management](#)
[Branding](#)

Identity & Access Management

Active Users Enterprise Groups

Edit Roles

You are editing the roles of the user **Sylvia Adams** (sylvia@coke.sqa-horizon.local)

Assign Organization Roles Organization Member ▾

Assign Service Roles ⓘ

Cloud Assembly ▾
 with roles
 Cloud Assembly Administrator ▾
 ×

[+ ADD SERVICE ACCESS](#)

- 3 Maak een project in Cloud Assembly waarmee u resources groepeert en de facturering van resources voor verschillende bedrijfsgroepen beheert.

- a Klik in de console op het tabblad **Services** en klik vervolgens op **Cloud Assembly**.
- b Selecteer **Infrastructuur > Projecten > Nieuw project**.

Dit toepassingsvoorbeeld voor gebruikersrollen beperkt zich tot de implementatie van gebruikersrollen en gaat niet in op de samenstelling van het volledige systeem.

Voor informatie over het configureren van de infrastructuur raadpleegt u [Hoofdstuk 4 Uw Cloud Assembly-resource-infrastructuur maken](#). Zie [Hoofdstuk 5 Cloud Assembly-projecten toevoegen en beheren](#) voor meer informatie over projecten.

- c Voer **WebAppTeam** als projectnaam in.

- d Klik op **Gebruikers** en klik vervolgens op **Gebruikers toevoegen**.
- e Voer de e-mailadressen in van de personen die u kunnen helpen bij het bouwen en beheren van de infrastructuur en cloudsjablonen.

Bijvoorbeeld: tony@mycompany.com,syliva@mycompany.com.

- f Selecteer **Beheerder** in het vervolgkeuzemenu **Rol toewijzen**.

Als Cloud Assembly-beheerder hebben deze twee gebruikers al beheerderstoegang tot de cloudaccounts, infrastructuur en alle projecten. Deze stap geeft u meer inzicht in de rollen die worden gebruikt in de verdere gebruiksscenario's. In de latere scenario's definieert u de rollen van projectbeheerder en projectleden, die verschillende rechten hebben.

- g Klik op het tabblad **Inrichting** en voeg een of meer cloudzones toe.

Ter herinnering. Dit toepassingsvoorbeeld gaat over gebruikersrollen.

4 Ontwikkel een eenvoudige cloudsjabloon zodat u het WebAppTeam-project kunt testen.

Dit gedeelte over cloudsjablonen is ingekort. De focus ligt op de vereiste gebruikers en gebruikersrollen voor projecten, en niet op hoe u een cloudsjabloon maakt.

- a Selecteer **Cloudsjablonen > Nieuw**.
- b Voer **WebApp** in als naam voor de nieuwe cloudsjabloon.
- c Selecteer WebAppTeam bij **Project**.

New Cloud Template

Name * WebApp

Description

Project * Q WebAppTeam

Cloud template sharing in Service Broker

☒ Share only with this project

☐ Allow an administrator to share with any project in this organization

CANCEL CREATE

- d Selecteer **Alleen delen met het project**.

Deze instelling zorgt ervoor dat de cloudsjabloon alleen beschikbaar is voor projectleden. Wanneer u klaar bent om de cloudsjablonen beschikbaar te stellen aan andere teams, selecteert u 'Toestaan dat een beheerder met elk project in deze organisatie deelt'. Als u de cloudsjabloon met andere projecten deelt, hoeft u geen dubbele instanties van dezelfde basissjablonen bij te houden. U kunt cloudsjablonen van ontwikkelingsprojecten verplaatsen naar productieprojecten, zodat consumenten van de catalogus deze in hun productieomgeving kunnen inzetten voor infrastructuurresources.

- e Klik op **Maken**.

- f Sleep in de cloudsjabloonontwerper het onderdeel **Cloudonafhankelijk > Machine** naar het canvas.

Zie [Hoofdstuk 6 Uw Cloud Assembly-implementaties ontwerpen](#) voor meer informatie over het configureren van cloudsjablonen.

- g Klik op **Implementeren**.
- h Voltooi de cloudsjabloon op iteratieve wijze zodat u de definitieve versie beschikbaar kunt stellen aan uw consumenten.
- i Klik op **Versie** en geef de versie van de cloudsjabloon vrij.

5 Stuur de gebruikers hun inloggegevens zoals u gewend bent.

Resultaten

In dit gebruiksscenario hebt u uw twee collega's tot organisatieleden gemaakt. Vervolgens hebt u Sylvia de rol van Cloud Assembly-beheerder gegeven. U hebt Tony de rol van WebApp-projectbeheerder gegeven. Deze configuratie van gebruikersrollen werkt alleen voor kleine teams waarin u geïmplementeerde applicaties aan de consumenten levert en niet via een selfservice-toegang of catalogus beschikbaar stelt.

Gebruiksscenario voor gebruiker 2: vRealize Automation-gebruikersrollen instellen om grotere ontwikkelingsteams en de catalogus te ondersteunen

Als vRealize Automation-organisatie-eigenaar bent u verantwoordelijk voor het toegangs- en budgetbeheer voor uw infrastructuurresources. U beschikt over een team van cloudsjabloonontwikkelaars die op iteratieve wijze sjablonen maken en implementeren voor verschillende projecten totdat deze klaar zijn voor levering aan de consumenten. Vervolgens levert u de implementeerbare resources aan de consumenten in een catalogus.

In dit scenario wordt ervan uitgegaan dat u begrijpt dat in het eerste toepassingsvoorbeeld wordt uitgegaan van een gebruiksscenario alleen voor beheerders. U wilt uw systeem nu uitbreiden om meer teams en grotere doelen te ondersteunen.

- Laat ontwikkelaars hun eigen applicatiecloudsjablonen maken en implementeren tijdens de ontwikkeling. U voegt zichzelf toe als beheerder en voegt vervolgens aanvullende gebruikers toe met de rol van zowel servicegebruiker als servicelezer. Vervolgens voegt u de gebruikers als projectleden toe. Deze projectleden kunnen hun eigen cloudsjablonen ontwikkelen en implementeren.
- Publiceer cloudsjablonen in een catalogus waar u deze voor niet-ontwikkelaars beschikbaar maakt om te implementeren. Nu wijst u gebruikersrollen toe voor Service Broker. Service Broker biedt een catalogus voor de cloudsjabloonconsumenten. U kunt hiermee ook beleid maken, inclusief leases en rechten, maar die functionaliteit maakt geen deel uit van dit toepassingsvoorbeeld voor gebruikersrollen.

Voorwaarden

- Bekijk het eerste toepassingsvoorbeeld. Zie [Eerste toepassingsvoorbeeld voor gebruikersrollen: de vRealize Automation-gebruikersrollen voor een klein applicatieontwikkelingsteam instellen](#).
- Identificeer de volgende gebruikers op basis van welke rechten u ze wilt geven:
 - Cloudsjabloonontwikkelaars die Cloud Assembly-gebruikers en -kijkers worden
 - Een Service Broker-beheerder
 - Gebruikers die geen ontwikkelaar zijn en die catalogusgebruikers zullen zijn als Service Broker-gebruikers

Procedure

- 1 Geef uw cloudsjabloonontwikkelaars de rol van organisatielid.

Raadpleeg voor instructies het [Eerste toepassingsvoorbeeld voor gebruikersrollen: de vRealize Automation-gebruikersrollen voor een klein applicatieontwikkelingsteam instellen](#).

2 Wijs de rol van Cloud Assembly-servicelid toe aan uw cloudsjabloonontwikkelaars.

a Klik op **Servicetoegang toevoegen**.

The screenshot shows the 'Identity & Access Management' console. The 'Edit Roles' page is active for the user 'Tony Anteater (tony@coke.sqa-horizon.local)'. Under 'Assign Organization Roles', 'Organization Member' is selected. Under 'Assign Service Roles', 'Cloud Assembly' is selected, and the role 'Cloud Assembly User' is assigned. A '+ ADD SERVICE ACCESS' button is visible at the bottom.

b Configureer de gebruiker met de volgende waarde.

Service	Rol
Cloud Assembly	Cloud Assembly-gebruiker
Cloud Assembly	Cloud Assembly-lezer

In dit gebruiksscenario moeten uw ontwikkelaars inzage hebben in de infrastructuur zodat zij zeker weten dat zij implementeerbare cloudsjablonen bouwen. Wijst u deze gebruikers in volgende stap toe als projectbeheerders en projectleden, dan kunnen ze de infrastructuur niet zien. Als servicelezer kunnen ze zien hoe de infrastructuur is geconfigureerd, maar kunnen ze geen wijzigingen aanbrengen. Als cloudbeheerder behoudt u dan de controle en geeft u ze alleen toegang tot de informatie die zij nodig hebben om cloudsjablonen te ontwikkelen.

3 Maak projecten in Cloud Assembly waarmee u resources en gebruikers groepeer.

In dit toepassingsvoorbeeld maakt u twee projecten. Het eerste project heet PersonnelAppDev en het tweede PayrollAppDev.

- Klik in de console op het tabblad **Services** en klik vervolgens op **Cloud Assembly**.
- Selecteer **Infrastructuur > Projecten > Nieuw project**.
- Voer **PersonnelAppDev** als naam in.
- Klik op **Gebruikers** en klik vervolgens op **Gebruikers toevoegen**.

- e Voeg projectleden toe en wijs een projectbeheerder toe.

Projectrol	Beschrijving
Projectgebruiker	Een projectlid is de primaire gebruikersrol van de ontwikkelaar in een project. Projecten bepalen welke cloudresources beschikbaar zijn wanneer u uw ontwikkelingswerk wilt testen door een cloudsjabloon te implementeren.
Projectbeheerder	Een projectbeheerder ondersteunt zijn ontwikkelaars door gebruikers voor uw projecten toe te voegen en te verwijderen. U kunt uw projecten ook verwijderen. Als u een project wilt maken, moet u beschikken over de rechten van een servicebeheerder.

- f Als u gebruikers als projectlid wilt toevoegen, voert u hun e-mailadres in, gescheiden door een komma, en selecteert u **Gebruiker** in het vervolgkeuzemenu **Rol toewijzen**.

Bijvoorbeeld: tony@mycompany.com,sylvia@mycompany.com.

PersonnelAppDev DELETE

Summary **Users** Provisioning Kubernetes Provisioning Integrations

Deployment sharing ☒ Deployments are shared between all users in the project

User roles Specify the users and groups related to this project.

+ ADD USERS + ADD GROUPS X REMOVE

Q Search users or groups

<input type="checkbox"/>	Name	Account	Role
<input type="checkbox"/>	Sylvia Adams	sylvia	Administrator
<input type="checkbox"/>	Gloria Martinez	gloria	Member
<input type="checkbox"/>	Tony Anteater	tony	Member

1 - 3 of 3 users

SAVE CANCEL

- g Selecteer voor de aangewezen beheerders **Beheerder** in het vervolgkeuzemenu **Rol toewijzen** en geef het benodigde e-mailadres op.

- h Klik op het tabblad **Inrichting** en voeg een of meer cloudzones toe.

Wanneer de deelnemende cloudsjabloonontwikkelaars aan dit project een sjabloon implementeren, gebeurt dit in de beschikbare resources in de cloudzones. U moet ervoor zorgen dat de resources van de cloudzone toereikend zijn voor de sjablonen die door het projectteam worden ontwikkeld.

- i Herhaal dit proces om de vereiste gebruikers en een beheerder toe te voegen aan het project PayrollAppDev.

- 4 Geef de servicegebruiker de vereiste inloggegevens en controleer of de leden van elk project de volgende taken kunnen uitvoeren.
 - a Open Cloud Assembly.
 - b Bekijk de infrastructuur voor alle projecten.
 - c Maak een cloudsjabloon voor het project waarvan zij lid zijn.
 - d Implementeer de cloudsjabloon in de resources van de cloudzone die voor het project zijn gedefinieerd.
 - e Beheer hun implementaties.
- 5 Geef uw cloudsjabloonontwikkelaars de rol van organisatielid.

Raadpleeg voor instructies het [Eerste toepassingsvoorbeeld voor gebruikersrollen: de vRealize Automation-gebruikersrollen voor een klein applicatieontwikkelingsteam instellen](#).
- 6 Wijs op basis van hun taak rollen toe aan de catalogusbeheerder, catalogusconsumenten en cloudsjabloonontwikkelaars.
 - a Klik op **Service toegang toevoegen**.
 - b Configureer de catalogusbeheerder met de volgende waarde.

Als cloudbeheerder kunt u deze rol zelf opeisen maar ook toewijzen aan iemand anders in uw applicatieontwikkelingsteam.

Service	Rol
Service Broker	Service Broker-beheerder

- c Configureer de cloudsjabloonconsumenten met de volgende waarde.

Service	Rol
Service Broker	Service Broker-gebruiker

Identity & Access Management

Active Users Enterprise Groups

Edit Roles

You are editing the roles of the user **Gloria Martinez** (gloria@coke.sqa-horizon.local)

Assign Organization Roles Organization Member ▾

Assign Service Roles ⓘ

Service Broker ▾

with roles

Service Broker User ▾

×

[+ ADD SERVICE ACCESS](#)

- d Configureer de cloudsjabloonontwikkelaars met de volgende waarde.

Service	Rol
Cloud AssemblyCloud Assembly	Cloud Assembly-gebruiker

- 7 Maak projecten in Cloud Assembly waarmee u resources en gebruikers groepeert.

In dit toepassingsvoorbeeld maakt u twee projecten. Het eerste project heet PersonnelAppDev en het tweede PayrollAppDev.

Raadpleeg voor instructies het [Gebruiksscenario voor gebruiker 2: vRealize Automation-gebruikersrollen instellen om grotere ontwikkelingsteams en de catalogus te ondersteunen](#).

- 8 Maak de cloudsjablonen voor elk projectteam en geef deze vrij.

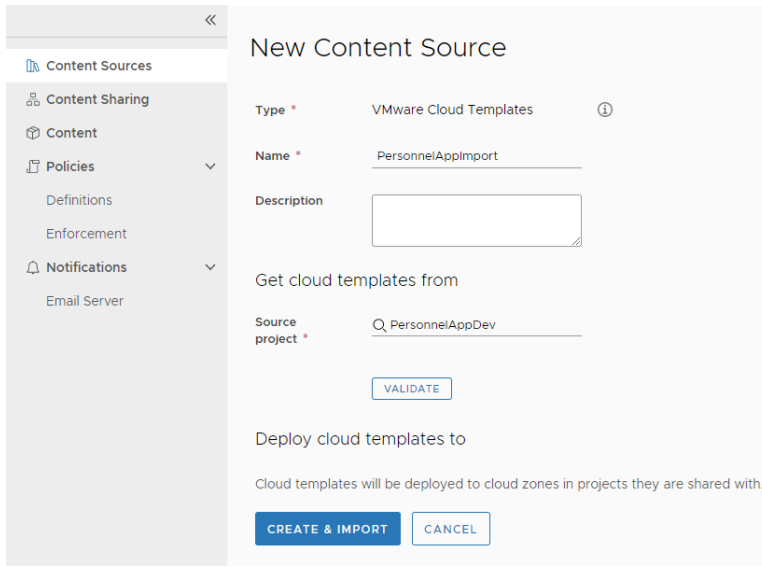
Raadpleeg voor instructies het [Eerste toepassingsvoorbeeld voor gebruikersrollen: de vRealize Automation-gebruikersrollen voor een klein applicatieontwikkelingsteam instellen](#).

- 9 Importeer een Cloud Assembly-cloudsjabloon in Service Broker.

U moet inloggen als gebruiker met de rol van Service Broker-beheerder.

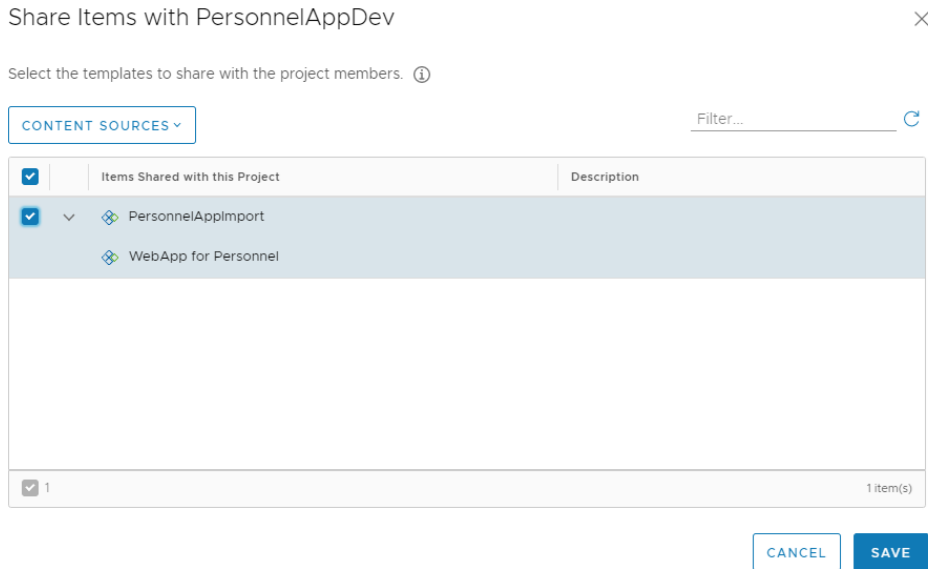
- Log in als gebruiker met de rol van Service Broker-beheerder.
- Klik in de console op Service Broker.

- c Selecteer **Inhoud en beleidsregels > Inhoudsbronnen** en klik op **Nieuw**.

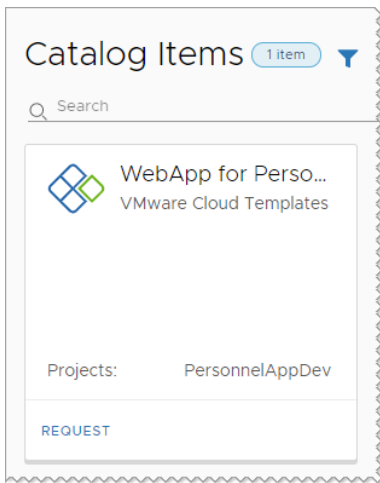


- d Selecteer **Cloud Assembly-cloudsjabloon**.
- e Voer **PersonnelAppImport** als naam in.
- f Selecteer PersonnelAppDev in het vervolgkeuzemenu **Bronproject** en klik op **Valideren**.
- g Wanneer de bron is gevalideerd, klikt u op **Maken en importeren**.
- h Herhaal dit voor PayrollAppDev en gebruik daarbij PayrollAppImport als naam voor de contentbron.
- 10 Deel een geïmporteerde cloudsjabloon met een project.
- Hoewel de cloudsjabloon al aan een project is gekoppeld, deelt u deze in Service Broker om deze beschikbaar te maken in de catalogus.
- a Ga door als gebruiker met de rol van Service Broker-beheerder.
- b Selecteer in Service Broker **Inhoud en beleidsregels > Inhoud delen**.
- c Selecteer het project **PersonnelAppDev** met de gebruikers die de cloudsjabloon uit de catalogus moeten kunnen implementeren.

- d Klik op **Items toevoegen** en selecteer vervolgens de cloudsjabloon PersonnelApp om met de projectleden te delen.



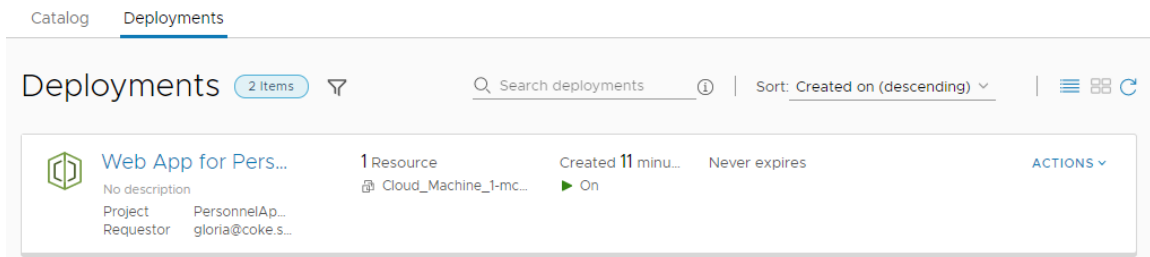
- e Klik op **Opslaan**.
- 11 Controleer of de cloudsjabloon in de Service Broker-catalogus beschikbaar is voor de leden van het project.
- a Vraag een projectlid zich aan te melden en op het tabblad **Catalogus** te klikken.



- b Klik op Aanvragen op de PersonnelApp-cloudsjabloonkaart.
- c Vul het formulier in en klik op **Verzenden**.

12 Controleer of het projectlid het implementatieproces kan controleren.

- a Vraag het projectlid **Resources > Implementaties** te selecteren en zoek de inrichtingsaanvraag.



- b Wanneer de cloudsjabloon wordt geïmplementeerd, controleert u of de aanvragende gebruiker toegang heeft tot de applicatie.

13 Herhaal dit proces voor de overige projecten.

Resultaten

Aangezien de cloudsjabloonontwikkeling in dit gebruiksscenario aan de ontwikkelaars wordt gedelegeerd, hebt u meerdere organisatieleden gemaakt. U hebt ze toegevoegd als Cloud Assembly-gebruikers. Vervolgens hebt u ze lid gemaakt van relevante projecten, zodat zij cloudsjablonen kunnen maken en implementeren. Als projectleden kunnen ze de door u beheerde infrastructuur niet bekijken of wijzigen, maar geeft u ze wel leesrechten voor de hele service zodat ze snappen aan welke beperkingen de infrastructuur waarvoor ze hun ontwerpen maken onderhevig is.

In dit toepassingsvoorbeeld configureert u gebruikers met verschillende rollen, waaronder die van Service Broker-beheerder en -gebruikers. Vervolgens stelt u de Service Broker-catalogus beschikbaar aan de gebruikers die geen ontwikkelaar zijn.

Wat nu te doen

Zie [Gebruikersrol voor gebruiksscenario 3: custom vRealize Automation-gebruikersrollen instellen om systeemrollen te verfijnen](#) voor meer informatie over het definiëren en toewijzen van custom rollen aan gebruikers.

Gebruikersrol voor gebruiksscenario 3: custom vRealize Automation-gebruikersrollen instellen om systeemrollen te verfijnen

Als vRealize Automation-organisatie-eigenaar of -servicebeheerder beheert u gebruikerstoegang via de rollen van de organisatie- en servicesystemen. U wilt echter ook custom rollen maken voor die geselecteerde gebruikers en taken uitvoeren of content zien die buiten hun systeemrollen valt.

In dit scenario wordt ervan uitgegaan dat u de servicegebruiker en bekijker begrijpt, evenals rollen van het projectlid en de bekijker die zijn gedefinieerd in gebruiksscenario 2. U kunt zien dat ze restrictiever zijn dan de service- en projectbeheerdersrollen die in gebruiksscenario 1 werden gebruikt. Nu hebt u enkele lokale gebruiksscenario's geïdentificeerd waarin u wilt dat sommige gebruikers volledige beheerrechten hebben voor sommige functies, u machtigingen voor andere gebruikers wilt bekijken en u niet wilt dat ze nog een andere reeks functies zien. U gebruikt custom rollen om die rechten te definiëren.

Dit gebruiksscenario is gebaseerd op drie mogelijke lokale gebruiksscenario's. Deze procedure laat zien hoe u rechten kunt maken voor de volgende custom rollen.

- **Beperkte infrastructuurbeheerder.** U wilt dat bepaalde servicegebruikers, die geen servicebeheerders zijn, over grotere infrastructuurrechten beschikken. Als beheerder wilt u dat ze helpen bij het opzetten van cloudzones, images en soorten. U wilt ook dat ze in staat zijn om ontdekte bronnen te onboarden en te beheren. Merk op dat ze geen cloudaccounts of integraties kunnen toevoegen; ze kunnen alleen de infrastructuur voor die eindpunten definiëren.
- **Uitbreidbaarheidsontwikkelaar.** U wilt dat sommige servicegebruikers volledige rechten hebben om de uitbreidbaarheidsacties en -abonnementen te gebruiken als onderdeel van cloudsjabloonontwikkeling voor hun projectteam en voor andere projecten. Ze zullen ook custom resourcetypen en custom acties voor meerdere projecten ontwikkelen.
- **XaaS-ontwikkelaar.** U wilt dat sommige servicegebruikers volledige rechten hebben om custom resourcetypen en custom acties voor meerdere projecten te ontwikkelen.
- **Probleemoplosser implementatie.** U wilt dat uw projectbeheerders rechten hebben die nodig zijn om problemen op te lossen en een analyse van de hoofdoorzaak uit te voeren op mislukte implementaties. U geeft ze de bevoegdheid om rechten te beheren voor niet-destructieve of goedkopere categorieën zoals image- en soorttoewijzingen. U wilt ook dat de projectbeheerders toestemming hebben om goedkeuringen en dag 2-beleidsregels in te stellen als onderdeel van de mislukte rol van probleemoplosser implementatie.

Voorwaarden

- Raadpleeg de tabellen met Cloud Assembly- en Service Broker-servicerollen en -projectrollen in [Wat zijn de vRealize Automation-gebruikersrollen](#). U moet begrijpen wat elke servicegebruikersrol kan zien en doen in die services.
- Bekijk de [Custom gebruikersrollen in vRealize Automation](#)-beschrijvingen zodat u meer weet over hoe u de rechten voor uw gebruikers kunt verfijnen.
- Controleer het eerste gebruiksscenario zodat u de organisatirollen en de rollen van de servicebeheerder begrijpt. Zie [Eerste toepassingsvoorbeeld voor gebruikersrollen: de vRealize Automation-gebruikersrollen voor een klein applicatieontwikkelingsteam instellen](#).
- Controleer het tweede gebruiksscenario zodat u de rol van servicegebruiker en projectleden begrijpt. Zie [Gebruiksscenario voor gebruiker 2: vRealize Automation-gebruikersrollen instellen om grotere ontwikkelingsteams en de catalogus te ondersteunen](#).

- Maak uzelf vertrouwd met Service Broker. Zie [Inhoud toevoegen aan de catalogus](#).

Procedure

- 1 Geef uw cloudsjabloonontwikkelaars de rol van organisatielid.

Raadpleeg voor instructies het [Eerste toepassingsvoorbeeld voor gebruikersrollen: de vRealize Automation-gebruikersrollen voor een klein applicatieontwikkelingsteam instellen](#).

- 2 Wijs Cloud Assembly- en Service Broker-servicerollen toe voor uw cloudsjabloonontwikkelaars en catalogusconsumenten.

Als u instructies nodig hebt, raadpleegt u het [Gebruiksscenario voor gebruiker 2: vRealize Automation-gebruikersrollen instellen om grotere ontwikkelingsteams en de catalogus te ondersteunen](#).

- 3 Maak projecten in Cloud Assembly waarmee u resources en gebruikers groepeert.

De volgende stappen voor de custom rollen omvatten ook projectrollen.

Als u instructies nodig hebt voor het maken van projecten raadpleegt u het [Gebruiksscenario voor gebruiker 2: vRealize Automation-gebruikersrollen instellen om grotere ontwikkelingsteams en de catalogus te ondersteunen](#).

- 4 Maak de cloudsjablonen voor elk projectteam en geef deze vrij.

Raadpleeg voor instructies het [Eerste toepassingsvoorbeeld voor gebruikersrollen: de vRealize Automation-gebruikersrollen voor een klein applicatieontwikkelingsteam instellen](#).

- 5 Meld u aan bij Cloud Assembly als servicebeheerder en selecteer **Infrastructuur > Beheer > Custom rollen**.

- 6 Maak een beperkte rol van infrastructuurbeheerder.

In dit voorbeeld hebt u een gebruiker, Tony, die een expert is in het opzetten van de infrastructuur voor verschillende projecten, maar u wilt hem geen volledige servicerechten geven. In plaats daarvan bouwt Tony de kerninfrastructuur die het werk van alle projecten ondersteunt. U geeft hem beperkte rechten voor infrastructuurbeheer. Tony, of een externe contractant, kan ook vergelijkbare rechten hebben voor de onboarding van ontdekte machines en deze onder vRealize Automation-beheer brengen.

- a Voeg Tony toe aan Cloud Assembly als servicegebruiker en bekijker.

Met zijn bekijkersrechten kan hij de onderliggende cloudaccounts en integraties zien als hij problemen met zijn werk moet oplossen, maar hij kan geen wijzigingen aanbrengen.

- b Maak een project en voeg Tony toe als lid van het project.

- c Als u de custom rol wilt maken, selecteert u **Infrastructuur > Beheer > Custom rollen** en klikt u op **Nieuwe custom rol**.

- d Voer de naam **Beperkte infrastructuurbeheerder** in en selecteer de volgende rechten.

Selecteer dit recht...	Zodat de gebruikers...
Infrastructuur > Cloudzones kunnen beheren	Cloudzones kunnen maken, bijwerken en verwijderen.
Infrastructuur > Soorttoewijzingen kunnen beheren	Soorttoewijzingen kunnen maken, bijwerken en verwijderen.
Infrastructuur > Imageroewijzingen kunnen beheren	Imageroewijzingen kunnen maken, bijwerken en verwijderen.

- e Klik op **Maken**.
- f Selecteer de rol van de Beperkte infrastructuurbeheerder op de pagina Custom rollen en klik op **Toewijzen**.
- g Voer het e-mailaccount van Tony in en klik op **Toevoegen..**
Voer bijvoorbeeld Tony@yourcompany.com in.
U kunt ook alle gedefinieerde Active Directory-gebruikersgroepen invoeren.
- h Laat Tony verifiëren dat hij waarden kan toevoegen, bewerken en verwijderen in de gebieden die zijn gedefinieerd door de custom rol wanneer hij inlogt.

7 Maak een rol van Uitbreidbaarheidsontwikkelaar.

In dit voorbeeld hebt u verschillende cloudsjabloonontwikkelaars, Sylvia en Igor, die goed geïnformeerd zijn over het gebruik van uitbreidbaarheidsacties en -abonnementen om dagelijkse ontwikkelingstaken te beheren. Ze hebben ook ervaring met vRealize Orchestrator, dus u geeft ze de opdracht om custom bronnen en acties voor verschillende projecten te leveren. U geeft ze extra rechten om uitbreidbaarheid te beheren door custom resources en acties te beheren, en door uitbreidbaarheidsacties en -abonnementen te beheren.

- a Voeg Sylvia en Igor toe als Cloud Assembly-gebruikers.
- b Voeg ze toe als leden van de projecten waaraan ze met hun uitbreidbaarheidsvaardigheden bijdragen.
- c Maak een custom gebruikersrol die u **Uitbreidbaarheidsontwikkelaar** noemt en selecteer de volgende rechten.

Selecteer dit recht...	Zodat de gebruikers...
XaaS > Custom resources beheren	Custom resources maken, bijwerken of verwijderen.
XaaS > Resourceacties beheren	Custom acties maken, bijwerken of verwijderen.
Uitbreidbaarheid > Uitbreidbaarheidsresources beheren	Uitbreidbaarheidsacties en -abonnementen maken, bijwerken of verwijderen. Abonnementen uitschakelen. Actie-uitvoeringen annuleren en verwijderen.

- d Klik op **Maken**.

- e Geef Sylvia en Igor de rol van uitbreidbaarheidsontwikkelaar.
- f Controleer of Sylvia en Igor de custom resources en acties kunnen beheren, en dat ze de verschillende opties op het tabblad Uitbreidbaarheid kunnen beheren.

8 Maak een rol van Probleemoplosser implementatie.

In dit voorbeeld geeft u uw projectbeheerders meer beheerrechten om de implementatiefouten te verhelpen voor hun teams.

- a Voeg uw projectbeheerders, Shauna, Pratap en Wei, toe als Cloud Assembly- en Service Broker-servicegebruikers.
- b Voeg ze in hun projecten toe als projectbeheerders.
- c Maak een custom gebruikersrol met de naam **Probleemoplosser implementatie** en selecteer de volgende rechten.

Selecteer dit recht...	Zodat de gebruikers...
Infrastructuur > Soorttoewijzingen kunnen beheren	Soorttoewijzingen kunnen maken, bijwerken en verwijderen.
Infrastructuur > Imagetoewijzingen kunnen beheren	Imagetoewijzingen kunnen maken, bijwerken en verwijderen.
Implementaties > Implementaties beheren	Bekijk alle implementaties in alle projecten en voer alle dag 2-acties uit op implementaties en implementatiecomponenten.
Beleid > Beleid beheren	Beleidsdefinities maken, bijwerken of verwijderen.

- d Klik op **Maken**.
- e Wijs Shauna, Pratap en Wei toe aan de rol Probleemoplosser implementatie.
- f Controleer of ze soorttoewijzingen, imagetoewijzingen en beleid in Service Broker kunnen beheren.

Resultaten

In dit gebruiksscenario configureert u verschillende gebruikers met verschillende rollen, inclusief custom rollen die hun service- en projectrollen uitbreiden.

Wat nu te doen

Maak custom rollen die uw lokale gebruiksscenario's omvatten.

Hoe kan ik de ingebouwde rol van Cloud Assembly-infrastructuurbeheerder aan een gebruiker toewijzen?

De rol van infrastructuurbeheerder is een ingebouwde rol die u aan geselecteerde gebruikers kunt toewijzen. U kunt de rol niet toewijzen in de gebruikersinterface.

Wanneer moet ik deze gebruikersrol toewijzen

U kunt de rechten dupliceren met behulp van de opties voor aangepaste gebruikersrollen. U kunt deze ingebouwde rol echter geven aan gebruikers die beperkte beheerders zijn.

Rechten voor de rol van infrastructuurbeheerder

De volgende tabel bevat de lijst met beheerrechten en andere rechten die infrastructuurbeheerders nodig hebben. Deze rechten kunnen niet worden gewijzigd. Als u wilt dat een gebruiker beperktere rechten heeft, kunt u de aangepaste rollen gebruiken om een gebruikersrol te maken die aan uw specifieke behoeften voldoet.

Tabel 3-15. Rechten voor de ingebouwde rol van infrastructuurbeheerder opgegeven

Recht voor maken, bewerken, bijwerken of verwijderen	Andere rechten
<ul style="list-style-type: none"> ■ Cloudaccounts ■ Integraties ■ Cloudzones ■ Soorttoewijzingen ■ Imagetoeuwijzingen ■ Netwerkprofielen ■ Opslagprofielen ■ Tags ■ Onboarding 	<ul style="list-style-type: none"> ■ Gedetecteerde resources weergeven en taggen ■ Computerbronnen weergeven ■ IP-adressen beheren ■ Load balancers weergeven en taggen ■ Netwerkdomeinen weergeven ■ Beveiliging weergeven ■ Opslag weergeven ■ Aanvragen weergeven en verwijderen

Hoe wijs ik de rol van infrastructuurbeheerder toe

Deze ingebouwde rol wordt toegewezen met behulp van de RBAC API. Eerst krijgt u de rol en vervolgens wijst u de rol toe aan een gebruiker.

Voordat u begint:

- Raak vertrouwd met de API. Zie de [API-programmeergids voor vRealize Automation](#).
 - Raak vertrouwd met de API. Zie de [API-programmeergids voor vRealize Automation 8.6](#).
 - Haal een API-bearertoken op. Zie het artikel [Uw toegangstoken ophalen in de API-programmeergids voor vRealize Automation](#).
 - Haal een API-bearertoken op. Zie het artikel [Uw toegangstoken ophalen in de API-programmeergids voor vRealize Automation 8.6](#)
- 1 Ga naar `$vra/project/api/swagger/swagger-ui.html?urls.primaryName=rba` waar `$vra` de basis-URL voor uw instantie is.
 - 2 Selecteer **rbac: 2020-08-10** in het vervolgkeuzemenu **Een definitie selecteren** in de rechterbovenhoek van de pagina.
 - 3 Om de gebruikersrol op te halen, opent u de sectie **Rol** en voert u `GET /rbac-service/api/roles` uit.

De resultaten moeten op het volgende voorbeeld lijken.

```
"content": [
  {
    "description": "Infrastructure Administrator",
    "hidden": false,
    "id": "infrastructure_administrator",
    "name": "Infrastructure Administrator",
    "orgId": "string",
    "permissions": [
      "string"
    ],
    "projectScope": true
  }
]
```

- 4 Als u een gebruiker wilt toevoegen aan de rol, opent u de sectie **Roltoewijzing** en opent en bewerkt u het commando `PUT /rbac-service/api/role-assignments` met de bijbehorende gebruikersnaam.

Bijvoorbeeld:

```
{
  "orgId": "string",
  "principalId": "Username@domain",
  "principalType": "user",
  "projectId": "string",
  "rolesToAdd": [
    "infrastructure_administrator"
  ],
  "rolesToRemove": [
    "string"
  ]
}
```

- 5 Voer het aangepaste PUT-commando uit.
- 6 Om de resultaten te controleren, instrueert u de toegewezen gebruiker om zich aan te melden en te controleren of de bovenstaande rechten zijn gedefinieerd.

Cloudaccounts aan Cloud Assembly toevoegen

Cloudaccounts zijn de geconfigureerde rechten die Cloud Assembly gebruikt om gegevens te verzamelen uit de regio's of datacenters en om cloudsjablonen in die regio's te implementeren.

De verzamelde gegevens omvatten de regio's die u later aan cloudzones koppelt.

Wanneer u later cloudzones, toewijzingen en profielen configureert, selecteert u het cloudaccount waaraan deze zijn gekoppeld.

Als cloudbeheerder maakt u cloudaccounts voor de projecten waarin de teamleden werken. Resource-informatie zoals netwerk en beveiliging, berekeningsresource, opslag en taginhoud wordt verzameld uit uw cloudaccounts.

Opmerking Als het cloudaccount gekoppelde machines heeft die al in de regio zijn geïmplementeerd, kunt u deze machines onder beheer van Cloud Assembly plaatsen met behulp van een onboardingplan. Zie [Wat zijn onboardingplannen in Cloud Assembly](#).

Als u een cloudaccount verwijderd die wordt gebruikt in een implementatie, worden resources die deel uitmaken van die implementatie onbeheerd.

Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation

Om cloudaccounts in vRealize Automation te configureren en te gebruiken, controleert u of u over de volgende verificatiegegevens beschikt.

Vereiste inloggegevens voor het cloudaccount

Om het volgende te doen...	U moet...
U registreren voor en aanmelden bij Cloud Assembly	<p>Een VMware-id.</p> <ul style="list-style-type: none"> ■ Stel een My VMware-account in met uw zakelijke e-mailadres.
Verbinding maken met vRealize Automation-services	<p>HTTPS-poort 443 open voor uitgaand verkeer met toegang via de firewall naar:</p> <ul style="list-style-type: none"> ■ *.vmwareidentity.com ■ gaz.csp-vidm-prod.com ■ *.vmware.com <p>Zie VMware Ports and Protocols voor meer informatie over poorten en protocollen.</p> <p>Zie <i>Poortvereisten</i> in de Help bij Referentie-architectuur voor meer informatie over poorten en protocollen.</p>

Om het volgende te doen...	U moet...
Een vCenter-cloudaccount toevoegen	<p>Voor de vSphere-agent zijn rechten vereist om de vCenter Server-instantie te beheren. Geef een account op met de volgende bevoegdheden voor lezen en schrijven:</p> <ul style="list-style-type: none"> ■ IP-adres of FQDN voor vCenter <p>De rechten die nodig zijn om VMware Cloud on AWS- en vCenter-cloudaccounts te beheren, worden weergegeven. Rechten moeten worden ingeschakeld voor alle clusters in de vCenter Server, niet alleen clusters die eindpunten hosten.</p> <p>Voor alle vCenter Server-gebaseerde cloudaccounts, inclusief NSX-V, NSX-T, vCenter en VMware Cloud on AWS, moet de beheerder verificatiegegevens voor het vSphere-eindpunt hebben of de verificatiegegevens waaronder de agentservice wordt uitgevoerd in vCenter, die beheerders toegang bieden tot de host vCenter Server.</p> <p>Voor meer informatie over de vSphere-agentvereisten raadpleegt u de VMware vSphere-productdocumentatie.</p> <ul style="list-style-type: none"> ■ Gegevensopslag <ul style="list-style-type: none"> ■ Ruimte toewijzen ■ Bladeren in gegevensopslag ■ Bestandsbewerkingen op een laag niveau ■ Gegevensopslagcluster <ul style="list-style-type: none"> ■ Een gegevensopslagcluster configureren ■ Map <ul style="list-style-type: none"> ■ Map maken ■ Map verwijderen ■ Globaal <ul style="list-style-type: none"> ■ Aangepaste kenmerken beheren ■ Aangepast kenmerk instellen ■ Netwerk <ul style="list-style-type: none"> ■ Netwerk toewijzen ■ Rechten <ul style="list-style-type: none"> ■ Rechten wijzigen ■ Resource <ul style="list-style-type: none"> ■ VM toewijzen aan resourcepool ■ Uitgeschakelde virtuele machine migreren ■ Ingeschakelde virtuele machine migreren ■ Profile-Driven Storage <ul style="list-style-type: none"> ■ Weergave Profile-driven storage <p>Als u een lijst met opslagbeleidsregels wilt retourneren die kunnen worden toegewezen aan een opslagprofiel, verleent u het recht <code>StorageProfile.View</code> aan alle accounts die vRealize Automation verbinden met vCenter Server.</p> ■ Inhoudsbibliotheek

Om het volgende te doen...**U moet...**

Als u een recht voor een inhoudsbibliotheek wilt toewijzen, moet een beheerder het recht aan de gebruiker verlenen als algemeen recht. Zie [Hiërarchische overname van rechten voor contentbibliotheek](#) in *vSphere-beheer van virtuele machines* in [VMware vSphere-documentatie](#) voor gerelateerde informatie.

- Bibliotheekitem toevoegen
- Lokale bibliotheek maken
- Geabonneerde bibliotheek maken
- Bibliotheekitem verwijderen
- Lokale bibliotheek verwijderen
- Geabonneerde bibliotheek verwijderen
- Bestanden downloaden
- Bibliotheekitem onbeschikbaar maken
- Abonnementsinformatie controleren
- Opslag lezen
- Bibliotheekitem synchroniseren
- Geabonneerde bibliotheek synchroniseren
- Type introspectie
- Configuratie-instellingen bijwerken
- Bestanden bijwerken
- Bibliotheek bijwerken
- Bibliotheekitem bijwerken
- Lokale bibliotheek bijwerken
- Geabonneerde bibliotheek bijwerken
- Configuratie-instellingen weergeven
- vSphere-tags
 - vSphere-tag toewijzen of de toewijzing annuleren
 - vSphere-tag toewijzen aan een object of de toewijzing annuleren
 - Een vSphere-tag maken
 - Een vSphere-tagcategorie maken
 - De vSphere-tag verwijderen
 - De vSphere-tagcategorie verwijderen
 - De vSphere-tag bewerken
 - De vSphere-tagcategorie bewerken
 - Het veld of de categorie UsedBy wijzigen
 - Het veld UsedBy wijzigen voor de tag
- vApp
 - Importeren
 - vApp-applicatieconfiguratie

De configuratie van de vApp.Import-applicatie is vereist voor OVF-sjablonen en voor het inrichten van VM's vanuit de inhoudsbibliotheek.

Om het volgende te doen...**U moet...**

De configuratie van de vApp.vApp-applicatie is vereist wanneer u cloud-init voor cloudconfiguratiescripts gebruikt. Met deze instelling kan de interne structuur van een vApp, zoals de productinformatie en de eigenschappen, worden gewijzigd.

- Virtuele machine - Inventaris
 - Maken op basis van bestaand item
 - Nieuwe maken
 - Verplaatsen
 - Verwijderen
- Virtuele machine - Interactie
 - CD-media configureren
 - Interactie met console
 - Apparaatverbinding
 - Uitschakelen
 - Inschakelen
 - Opnieuw instellen
 - Opheffen
 - Tools installeren
- Virtuele machine - Configuratie
 - Bestaande schijf toevoegen
 - Nieuw toevoegen
 - Schijf verwijderen
 - Geavanceerd
 - Aantal CPU's wijzigen
 - Resource wijzigen
 - Virtuele disk uitbreiden
 - Bijhouden van schijf wijzigen
 - Geheugen
 - Apparaatinstellingen wijzigen
 - Naam wijzigen
 - Annotatie instellen
 - Instellingen
 - Plaatsing wisselbestand
- Virtuele machine - Provisioning
 - Aanpassen
 - Sjabloon klonen
 - Virtuele machine klonen
 - Sjabloon implementeren
 - Specificatie aanpassing lezen
- Virtuele machine - Status
 - Momentopname maken
 - Momentopname verwijderen
 - Terugzetten naar momentopname

Om het volgende te doen...	U moet...
Voeg een Amazon Web Services-cloudaccount (AWS) toe	<p data-bbox="432 289 1398 411">Geef een hoofdgebruikersaccount op met bevoegdheden voor lezen en schrijven. Het gebruikersaccount moet lid zijn van het Power Access-beleid (PowerUserAccess) in het AWS Identity and Access Management (IAM)-systeem.</p> <ul data-bbox="432 422 1206 478" style="list-style-type: none"> ■ 20-cijferige toegangssleutel-ID en bijbehorende geheime toegangssleutel <p data-bbox="432 489 1233 548">Als u een externe HTTP-internetproxy gebruikt, moet deze zijn geconfigureerd voor IPv4.</p> <p data-bbox="432 558 1390 646">Voor de op acties gebaseerde uitbreidbaarheid (ABX) en externe IPAM-integratie van vRealize Automation zijn mogelijk aanvullende machtigingen vereist.</p> <p data-bbox="432 657 1334 716">De volgende AWS-machtigingen worden aanbevolen om functies voor automatisch schalen toe te staan:</p> <ul data-bbox="432 726 1051 1121" style="list-style-type: none"> ■ Acties voor automatisch schalen: <ul style="list-style-type: none"> ■ autoscaling:DescribeAutoScalingInstances ■ autoscaling:AttachInstances ■ autoscaling>DeleteLaunchConfiguration ■ autoscaling:DescribeAutoScalingGroups ■ autoscaling>CreateAutoScalingGroup ■ autoscaling:UpdateAutoScalingGroup ■ autoscaling>DeleteAutoScalingGroup ■ autoscaling:DescribeLoadBalancers ■ Resources automatisch schalen: <ul style="list-style-type: none"> ■ * <p data-bbox="509 1146 1219 1173">Geef alle resourcerechten voor automatisch schalen op.</p> <p data-bbox="432 1184 1374 1272">De volgende machtigingen zijn vereist om AWS Security Token Service-functies (AWS STS) toe te staan om tijdelijke inloggegevens met beperkte rechten te ondersteunen voor AWS-identiteit en toegang:</p> <ul data-bbox="432 1283 738 1341" style="list-style-type: none"> ■ AWS STS-resources: <ul style="list-style-type: none"> ■ * <p data-bbox="509 1367 948 1394">Geef alle STS-resourcerechten op.</p> <p data-bbox="432 1404 1378 1432">De volgende AWS-machtigingen zijn vereist om EC2-functies toe te staan:</p> <ul data-bbox="432 1442 963 1879" style="list-style-type: none"> ■ EC2-acties: <ul style="list-style-type: none"> ■ ec2:AttachVolume ■ ec2:AuthorizeSecurityGroupIngress ■ ec2>DeleteSubnet ■ ec2>DeleteSnapshot ■ ec2:DescribeInstances ■ ec2>DeleteTags ■ ec2:DescribeRegions ■ ec2:DescribeVolumesModifications ■ ec2>CreateVpc ■ ec2:DescribeSnapshots ■ ec2:DescribeInternetGateways

Om het volgende te doen...**U moet...**

- ec2:DeleteVolume
- ec2:DescribeNetworkInterfaces
- ec2:StartInstances
- ec2:DescribeAvailabilityZones
- ec2:CreateInternetGateway
- ec2:CreateSecurityGroup
- ec2:DescribeVolumes
- ec2:CreateSnapshot
- ec2:ModifyInstanceAttribute
- ec2:DescribeRouteTables
- ec2:DescribeInstanceTypes
- ec2:DescribeInstanceTypeOfferings
- ec2:DescribeInstanceStatus
- ec2:DetachVolume
- ec2:RebootInstances
- ec2:AuthorizeSecurityGroupEgress
- ec2:ModifyVolume
- ec2:TerminateInstances
- ec2:DescribeSpotFleetRequestHistory
- ec2:DescribeTags
- ec2:CreateTags
- ec2:RunInstances
- ec2:DescribeNatGateways
- ec2:StopInstances
- ec2:DescribeSecurityGroups
- ec2:CreateVolume
- ec2:DescribeSpotFleetRequests
- ec2:DescribeImages
- ec2:DescribeVpcs
- ec2>DeleteSecurityGroup
- ec2>DeleteVpc
- ec2:CreateSubnet
- ec2:DescribeSubnets
- ec2:RequestSpotFleet

Opmerking Het SpotFleet-aanvraagrecht is niet vereist voor op acties gebaseerde uitbreidbaarheid (ABX) of externe IPAM-integraties van vRealize Automation.

- EC2-resources:

- *

Geef alle EC2-resourcerechten op.

Om het volgende te doen...**U moet...**

De volgende AWS-machtigingen zijn vereist om functies voor elastische load balancing toe te staan:

- Load balancer-acties:
 - elasticloadbalancing:DeleteLoadBalancer
 - elasticloadbalancing:DescribeLoadBalancers
 - elasticloadbalancing:RemoveTags
 - elasticloadbalancing>CreateLoadBalancer
 - elasticloadbalancing:DescribeTags
 - elasticloadbalancing:ConfigureHealthCheck
 - elasticloadbalancing:AddTags
 - elasticloadbalancing>CreateTargetGroup
 - elasticloadbalancing>DeleteLoadBalancerListeners
 - elasticloadbalancing:DeregisterInstancesFromLoadBalancer
 - elasticloadbalancing:RegisterInstancesWithLoadBalancer
 - elasticloadbalancing>CreateLoadBalancerListeners
- Load balancer-resources:
 - *

Geef alle rechten voor de load-balancerresources op.

De volgende rechten voor AWS Identity and Access Management (IAM) kunnen worden ingeschakeld, maar zijn niet vereist:

- iam:SimulateCustomPolicy
- iam:GetUser
- iam:ListUserPolicies
- iam:GetUserPolicy
- iam:ListAttachedUserPolicies
- iam:GetPolicyVersion
- iam:ListGroupsForUser
- iam:ListGroupPolicies
- iam:GetGroupPolicy
- iam:ListAttachedGroupPolicies
- iam:ListPolicyVersions

Om het volgende te doen...	U moet...
Een Microsoft Azure-cloudaccount toevoegen	<p>Configureer een Microsoft Azure-instantie en verkrijg een geldig Microsoft Azure-abonnement waarvan u de abonnements-id kunt gebruiken.</p> <p>Maak een Active Directory-applicatie zoals beschreven in Procedure: gebruik de portal om een Azure AD-applicatie en service-principal te maken die toegang hebben tot resources in de Microsoft Azure-productdocumentatie.</p> <p>Als u een externe HTTP-internetproxy gebruikt, moet deze zijn geconfigureerd voor IPv4.</p> <p>Merk de volgende informatie op:</p> <ul style="list-style-type: none"> ■ Abonnements-id <p>Geeft u toegang tot uw Microsoft Azure-abonnementen.</p> ■ Tenant-id <p>Het autorisatie-eindpunt voor de Active Directory-applicaties die u in uw Microsoft Azure-account maakt.</p> ■ Clientapplicatie-id <p>Biedt toegang tot Microsoft Active Directory in uw individuele Microsoft Azure-account.</p> ■ Geheime sleutel clientapplicatie <p>De unieke geheime sleutel die is gegenereerd om te koppelen met uw klantapplicatie-ID.</p> <p>De volgende machtigingen zijn vereist voor het maken en valideren van Microsoft Azure-cloudaccounts:</p> <ul style="list-style-type: none"> ■ Microsoft Compute <ul style="list-style-type: none"> ■ Microsoft.Compute/virtualMachines/extensions/write ■ Microsoft.Compute/virtualMachines/extensions/read ■ Microsoft.Compute/virtualMachines/extensions/delete ■ Microsoft.Compute/virtualMachines/deallocate/action ■ Microsoft.Compute/virtualMachines/delete ■ Microsoft.Compute/virtualMachines/powerOff/action ■ Microsoft.Compute/virtualMachines/read ■ Microsoft.Compute/virtualMachines/restart/action ■ Microsoft.Compute/virtualMachines/start/action ■ Microsoft.Compute/virtualMachines/write ■ Microsoft.Compute/availabilitySets/write ■ Microsoft.Compute/availabilitySets/read ■ Microsoft.Compute/availabilitySets/delete ■ Microsoft.Compute/disks/delete ■ Microsoft.Compute/disks/read ■ Microsoft.Compute/disks/write ■ Microsoft Network <ul style="list-style-type: none"> ■ Microsoft.Network/loadBalancers/backendAddressPools/join/action ■ Microsoft.Network/loadBalancers/delete ■ Microsoft.Network/loadBalancers/read

Om het volgende te doen...**U moet...**

- Microsoft.Network/loadBalancers/write
- Microsoft.Network/networkInterfaces/join/action
- Microsoft.Network/networkInterfaces/read
- Microsoft.Network/networkInterfaces/write
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/join/action
- Microsoft.Network/networkSecurityGroups/read
- Microsoft.Network/networkSecurityGroups/write
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Network/publicIPAddresses/delete
- Microsoft.Network/publicIPAddresses/join/action
- Microsoft.Network/publicIPAddresses/read
- Microsoft.Network/publicIPAddresses/write
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/delete
- Microsoft.Network/virtualNetworks/subnets/join/action
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Network/virtualNetworks/subnets/write
- Microsoft.Network/virtualNetworks/write
- Microsoft Resources
 - Microsoft.Resources/subscriptions/resourcegroups/delete
 - Microsoft.Resources/subscriptions/resourcegroups/read
 - Microsoft.Resources/subscriptions/resourcegroups/write
- Microsoft-opslag
 - Microsoft.Storage/storageAccounts/delete
 - Microsoft.Storage/storageAccounts/listKeys/action
 - Microsoft.Storage/storageAccounts/read
 - Microsoft.Storage/storageAccounts/write
- Microsoft Web
 - Microsoft.Web/sites/read
 - Microsoft.Web/sites/write
 - Microsoft.Web/sites/delete
 - Microsoft.Web/sites/config/read
 - Microsoft.Web/sites/config/write
 - Microsoft.Web/sites/config/list/action
 - Microsoft.Web/sites/publishxml/action
 - Microsoft.Web/serverfarms/write
 - Microsoft.Web/serverfarms/delete
 - Microsoft.Web/sites/hostruntime/functions/keys/read
 - Microsoft.Web/sites/hostruntime/host/read
 - Microsoft.web/sites/functions/masterkey/read

Om het volgende te doen...**U moet...**

Als u Microsoft Azure gebruikt met op een actie gebaseerde uitbreidbaarheid, zijn de volgende machtigingen vereist, naast de minimale machtigingen:

- Microsoft.Web/sites/read
- Microsoft.Web/sites/write
- Microsoft.Web/sites/delete
- Microsoft.Web/sites/*/action
- Microsoft.Web/sites/config/read
- Microsoft.Web/sites/config/write
- Microsoft.Web/sites/config/list/action
- Microsoft.Web/sites/publishxml/action
- Microsoft.Web/serverfarms/write
- Microsoft.Web/serverfarms/delete
- Microsoft.Web/sites/hostruntime/functions/keys/read
- Microsoft.Web/sites/hostruntime/host/read
- Microsoft.Web/sites/functions/masterkey/read
- Microsoft.Web/apimanagementaccounts/apis/read
- Microsoft.Authorization/roleAssignments/read
- Microsoft.Authorization/roleAssignments/write
- Microsoft.Authorization/roleAssignments/delete
- Microsoft.Insights/Components/Read
- Microsoft.Insights/Components/Write
- Microsoft.Insights/Components/Query/Read

Als u Microsoft Azure gebruikt met op een actie gebaseerde uitbreidbaarheid met extensies, zijn de volgende machtigingen ook vereist:

- Microsoft.Compute/virtualMachines/extensions/write
- Microsoft.Compute/virtualMachines/extensions/read
- Microsoft.Compute/virtualMachines/extensions/delete

Zie [Microsoft Azure configureren](#) voor gerelateerde informatie over het maken van een Microsoft Azure-cloudaccount.

Om het volgende te doen...	U moet...
Een Google Cloud Platform-cloudaccount (GCP) toevoegen	<p>De Google Cloud Platform-cloudaccount werkt interactief met de Google Cloud Platform-berekeningsengine.</p> <p>De verificatiegegevens van de Projectbeheerder en de Eigenaar zijn vereist voor het maken en valideren van Google Cloud Platform-cloudaccounts.</p> <p>Als u een externe HTTP-internetproxy gebruikt, moet deze zijn geconfigureerd voor IPv4.</p> <p>De service Engine berekenen moet zijn ingeschakeld. Wanneer u het cloudaccount in vRealize Automation maakt, gebruikt u het serviceaccount dat is gemaakt toen de berekeningsengine werd geïnitieerd.</p> <p>De volgende berekeningsengine-machtigingen zijn ook vereist, afhankelijk van de acties die de gebruiker kan uitvoeren:</p> <ul style="list-style-type: none"> ■ <code>rollen/compute.admin</code> <p>Biedt volledige controle over alle resources van de berekeningsengine.</p> ■ <code>rollen/iam.serviceAccountUser</code> <p>Biedt toegang tot gebruikers die instanties van virtuele machines beheren die zijn geconfigureerd om als serviceaccount te worden uitgevoerd. Verleen toegang tot de volgende resources en services:</p> <ul style="list-style-type: none"> ■ <code>berekenen.*</code> ■ <code>resourcemanager.projects.get</code> ■ <code>resourcemanager.projects.list</code> ■ <code>serviceusage.quotas.get</code> ■ <code>serviceusage.services.get</code> ■ <code>serviceusage.services.list</code> ■ <code>rollen/compute.imageUser</code> <p>Geeft toestemming om images op te geven en te lezen zonder andere rechten op de image te hebben. Als u de <code>compute.imageUser</code>-rol op projectniveau verleent, krijgen gebruikers de mogelijkheid om alle images in het project weer te geven. Ook kunnen gebruikers resources, zoals instanties en persistente schijven, maken op basis van images in het project.</p> <ul style="list-style-type: none"> ■ <code>compute.images.get</code> ■ <code>compute.images.getFromFamily</code> ■ <code>compute.images.list</code> ■ <code>compute.images.useReadOnly</code> ■ <code>resourcemanager.projects.get</code> ■ <code>resourcemanager.projects.list</code> ■ <code>serviceusage.quotas.get</code> ■ <code>serviceusage.services.get</code> ■ <code>serviceusage.services.list</code> ■ <code>rollen/compute.instanceAdmin</code> <p>Biedt rechten om instanties van virtuele machines te maken, te wijzigen en te verwijderen. Dit omvat rechten om schijven te maken, te wijzigen en te verwijderen, en ook om afgeschermd VMBETA-instellingen te configureren.</p>

Om het volgende te doen...**U moet...**

Voor gebruikers die instanties van virtuele machines beheren (maar geen netwerk- of beveiligingsinstellingen of -instanties die worden uitgevoerd als serviceaccounts), moet u deze rol toekennen aan de organisatie, de map of het project dat de instanties bevat, of aan de individuele instanties.

Gebruikers die instanties van virtuele machines beheren die zijn geconfigureerd om als serviceaccount te worden uitgevoerd, hebben ook de rol `iam.serviceAccountUser` nodig.

- `compute.acceleratorTypes`
- `compute.addresses.get`
- `compute.addresses.list`
- `compute.addresses.use`
- `compute.autoscalers`
- `compute.diskTypes`
- `compute.disks.create`
- `compute.disks.createSnapshot`
- `compute.disks.delete`
- `compute.disks.get`
- `compute.disks.list`
- `compute.disks.resize`
- `compute.disks.setLabels`
- `compute.disks.update`
- `compute.disks.use`
- `compute.disks.useReadOnly`
- `compute.globalAddresses.get`
- `compute.globalAddresses.list`
- `compute.globalAddresses.use`
- `compute.globalOperations.get`
- `compute.globalOperations.list`
- `compute.images.get`
- `compute.images.getFromFamily`
- `compute.images.list`
- `compute.images.useReadOnly`
- `compute.instanceGroupManagers`
- `compute.instanceGroups`
- `compute.instanceTemplates`
- `compute.instances`
- `compute.licenses.get`
- `compute.licenses.list`
- `compute.machineTypes`
- `compute.networkEndpointGroups`
- `compute.networks.get`
- `compute.networks.list`
- `compute.networks.use`

Om het volgende te doen...**U moet...**

- compute.networks.useExternalIp
- compute.projects.get
- compute.regionOperations.get
- compute.regionOperations.list
- compute.regions
- compute.reservations.get
- compute.reservations.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.targetPools.get
- compute.targetPools.list
- compute.zoneOperations.get
- compute.zoneOperations.list
- compute.zones
- resourceManager.projects.get
- resourceManager.projects.list
- serviceusage.quotas.get
- serviceusage.services.get
- serviceusage.services.list
- rollen/compute.instanceAdmin.v1

Biedt volledige controle over instanties van de compute engine, instantiegroepen, schijven, momentopnamen en images. Biedt ook leestoeegang tot alle netwerkresources van de compute engine.

Opmerking Als u een gebruiker deze rol verleent op het niveau van de instantie, kan die gebruiker geen nieuwe instanties maken.

- compute.acceleratorTypes
- compute.addresses.get
- compute.addresses.list
- compute.addresses.use
- compute.autoscalers
- compute.backendBuckets.get
- compute.backendBuckets.list
- compute.backendServices.get
- compute.backendServices.list
- compute.diskTypes
- compute.disks
- compute.firewalls.get
- compute.firewalls.list
- compute.forwardingRules.get
- compute.forwardingRules.list
- compute.globalAddresses.get

Om het volgende te doen...**U moet...**

- compute.globalAddresses.list
- compute.globalAddresses.use
- compute.globalForwardingRules.get
- compute.globalForwardingRules.list
- compute.globalOperations.get
- compute.globalOperations.list
- compute.healthChecks.get
- compute.healthChecks.list
- compute.httpHealthChecks.get
- compute.httpHealthChecks.list
- compute.httpsHealthChecks.get
- compute.httpsHealthChecks.list
- compute.images
- compute.instanceGroupManagers
- compute.instanceGroups
- compute.instanceTemplates
- compute.instances
- compute.interconnectAttachments.get
- compute.interconnectAttachments.list
- compute.interconnectLocations
- compute.interconnects.get
- compute.interconnects.list
- compute.licenseCodes
- compute.licenses
- compute.machineTypes
- compute.networkEndpointGroups
- compute.networks.get
- compute.networks.list
- compute.networks.use
- compute.networks.useExternallp
- compute.projects.get
- compute.projects.setCommonInstanceMetadata
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.regionOperations.get
- compute.regionOperations.list
- compute.regions
- compute.reservations.get
- compute.reservations.list
- compute.resourcePolicies
- compute.routers.get
- compute.routers.list
- compute.routes.get

Om het volgende te doen...	U moet...
	<ul style="list-style-type: none"> ■ compute.routes.list ■ compute.snapshots ■ compute.sslCertificates.get ■ compute.sslCertificates.list ■ compute.sslPolicies.get ■ compute.sslPolicies.list ■ compute.sslPolicies.listAvailableFeatures ■ compute.subnetworks.get ■ compute.subnetworks.list ■ compute.subnetworks.use ■ compute.subnetworks.useExternalIp ■ compute.targetHttpProxies.get ■ compute.targetHttpProxies.list ■ compute.targetHttpsProxies.get ■ compute.targetHttpsProxies.list ■ compute.targetInstances.get ■ compute.targetInstances.list ■ compute.targetPools.get ■ compute.targetPools.list ■ compute.targetSslProxies.get ■ compute.targetSslProxies.list ■ compute.targetTcpProxies.get ■ compute.targetTcpProxies.list ■ compute.targetVpnGateways.get ■ compute.targetVpnGateways.list ■ compute.urlMaps.get ■ compute.urlMaps.list ■ compute.vpnTunnels.get ■ compute.vpnTunnels.list ■ compute.zoneOperations.get ■ compute.zoneOperations.list ■ compute.zones ■ resourcemanager.projects.get ■ resourcemanager.projects.list ■ serviceusage.quotas.get ■ serviceusage.services.get ■ serviceusage.services.list
Een NSX-T-cloudaccount toevoegen	<p>Geef een account op met de volgende bevoegdheden voor lezen en schrijven:</p> <ul style="list-style-type: none"> ■ IP-adres of FQDN voor NSX-T ■ NSX-T-datacenter - Bedrijfsbeheerdersrol en inloggegevens <p>Beheerders hebben <i>ook</i> toegang tot de vCenter Server nodig zoals is beschreven in de sectie <i>Een vCenter-cloudaccount toevoegen</i> van deze tabel.</p>

Om het volgende te doen...	U moet...
Een NSX-V-cloudaccount toevoegen	<p>Geef een account op met de volgende bevoegdheden voor lezen en schrijven:</p> <ul style="list-style-type: none"> ■ Bedrijfsbeheerdersrol en inloggegevens voor NSX-V ■ IP-adres of FQDN voor NSX-V <p>Beheerders hebben <i>ook</i> toegang tot de vCenter Server nodig zoals is beschreven in de sectie <i>Een vCenter-cloudaccount toevoegen</i> van deze tabel.</p>
Een VMware Cloud on AWS-cloudaccount (VMC) toevoegen	<p>Geef een account op met de volgende bevoegdheden voor lezen en schrijven:</p> <ul style="list-style-type: none"> ■ Het cloudadmin@vmc.local-account of een gebruikersaccount in de CloudAdmin-groep ■ Bedrijfsbeheerdersrol en inloggegevens voor NSX ■ NSX-cloudbeheerderstoegang tot de VMware Cloud on AWS SDDC-omgeving van uw organisatie ■ Beheerderstoegang tot de VMware Cloud on AWS SDDC-omgeving van uw organisatie ■ Het API-token van VMware Cloud on AWS voor uw VMware Cloud on AWS-omgeving in de VMware Cloud on AWS-service van uw organisatie ■ IP-adres of FQDN voor vCenter <p>Beheerders hebben <i>ook</i> toegang tot de vCenter Server nodig zoals is beschreven in de sectie <i>Een vCenter-cloudaccount toevoegen</i> van deze tabel.</p> <p>Voor meer informatie over de rechten die nodig zijn om VMware Cloud on AWS-cloudaccounts te maken en te gebruiken, zie <i>VMware Cloud on AWS-datacentrum beheren</i> in de VMware Cloud on AWS-productdocumentatie.</p>
Integreren met vRealize Operations Manager	<p>Geef een lokaal of niet-lokaal aanmeldingsaccount bij vRealize Operations Manager op met de volgende leesrechten.</p> <ul style="list-style-type: none"> ■ Adapterinstantie vCenter-adapter > VC-adapterinstantie voor <i>vCenter-FQDN</i> <p>Mogelijk moet een niet-lokaal account eerst worden geïmporteerd, voordat u de alleen-lezen rol kunt toewijzen.</p>

Microsoft Azure configureren voor gebruik met Cloud Assembly

U moet informatie verzamelen en een configuratie uitvoeren om een Microsoft Azure-cloudaccount in Cloud Assembly 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 uw Azure-portal om de abonnements-id weer te geven.
 - Tenant-id: klik op het Help-pictogram en selecteer Diagnostische gegevens weergeven in uw Azure-portal. Zoek naar de tenant en noteer de id wanneer u deze hebt gevonden.

- 2 U kunt een nieuw opslagaccount en een resourcegroep 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 uw 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 resourcegroep wilt gebruiken of een nieuwe wilt maken. Noteer de naam van uw resourcegroep. 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 resourcegroep 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 virtuele machines of andere objecten als de locatie niet overeenkomt voor alle toepasselijke onderdelen 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 het veld **Adresruimte** in.
- 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-applicatie in zodat vRA 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 applicatie die voldoet aan de Azure-naamvalidatie.
- d Behoud Web-app/API als applicatietype.
- 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 te verifiëren in Cloud Assembly.
 - a Klik op de naam van uw applicatie in Azure.
Noteer uw applicatie-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-applicatie om verbinding te maken met uw Azure-abonnement zodat u virtuele machines kunt implementeren en beheeren.
 - 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 tools voor de opdrachtregelinterface van Microsoft Azure installeren. Deze tools zijn vrij beschikbaar voor zowel Windows- als Mac-besturingssystemen. Raadpleeg de Microsoft-documentatie voor meer informatie over het downloaden en installeren van deze tools.

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 applicatie op uw apparaat 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 virtuele machines op te halen. U kunt de gewenste image kiezen, de opgegeven URN voor de image vastleggen en deze later in blueprints gebruiken.

Een Microsoft Azure-cloudaccount maken in vRealize Automation

Als cloudbeheerder kunt u een Microsoft Azure-cloudaccount maken voor accountregio's waarop uw team vRealize Automation-cloudsjablonen gaat implementeren.

Zie [Tutorial: Infrastructuur en implementaties met meerdere clouds instellen en testen in Cloud Assembly](#) om een voorbeeld te zien van hoe een Microsoft Azure-cloudaccount werkt in vRealize Automation.

Voorwaarden

- Controleer of u over de vereiste beheerdersreferenties beschikt en HTTPS-toegang hebt ingeschakeld op poort 443. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Controleer of u de vereiste gebruikersrol hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Configureer een Microsoft Azure-account voor gebruik met vRealize Automation. Zie [Microsoft Azure configureren voor gebruik met Cloud Assembly](#).
- Als u geen externe internettoegang hebt, configureert u een internetserverproxy. Zie [Hoe configureer ik een internetproxyserver voor vRealize Automation](#).

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Cloudaccounts** en klik op **Cloudaccount toevoegen**.

- 2 Selecteer het Microsoft Azure-accounttype en voer de inloggegevens en andere waarden in.
- 3 Klik op **Valideren**.

De accountregio's die aan het account zijn gekoppeld worden verzameld.

- 4 Selecteer de regio's waarin u deze resource wilt inrichten.
- 5 Klik op **Een cloudzone maken voor de geselecteerde regio's** om efficiënt te werken.
- 6 Als u tags moet toevoegen om een tagstrategie te ondersteunen, voert u mogelijkheidstags in. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#) en [Een tagstrategie maken](#).



Voor meer informatie over hoe capaciteitstags en beperkingstags helpen bij het beheren van implementatieplaatsingen raadpleegt u de [Beperkingstags en plaatsing](#)-videotutorial.

- 7 Klik op **Opslaan**.

Resultaten

Het account wordt toegevoegd aan vRealize Automation en de geselecteerde regio's zijn beschikbaar voor de opgegeven cloudzone.

Wat nu te doen

Maak infrastructuurresources voor dit cloudaccount.

Wanneer u een Azure-cloudaccount aan een cloudsjabloon toevoegt, kunt u ervoor kiezen om beschikbaarheidssets desgewenst opnieuw te gebruiken. Abonnementen hebben een limiet van 2000 beschikbaarheidssets en 25.000 virtuele machines. Het is daarom zinvol om beschikbaarheidssets waar mogelijk opnieuw te gebruiken. Er zijn twee YAML-eigenschappen die u kunt gebruiken om te bepalen hoe implementaties beschikbaarheidssets gebruiken. Met de eigenschap `availabilitySetName` kunt u een beschikbaarheidsset opgeven die moet worden gebruikt. De tweede eigenschap is `doNotAttachAvailabilitySet` die standaard op onwaar is ingesteld. Als deze eigenschap op waar is ingesteld, maakt vRealize Automation de implementatie zonder beschikbaarheidsset.

U kunt geen implementatie maken zonder beschikbaarheidsset als u een load balancer gebruikt die aan de virtuele machine is gekoppeld.

In de volgende tabel wordt beschreven hoe vRealize Automation zich gedraagt, afhankelijk van of een resourcegroep en een beschikbaarheidsset zijn opgegeven in de cloudsjabloon.

Een beschikbaarheidsset kan niet bestaan zonder deel uit te maken van een resourcegroep. De beschikbaarheidssets in een bepaalde resourcegroep moeten unieke namen hebben. Beschikbaarheidssets kunnen alleen dezelfde naam hebben als ze deel uitmaken van verschillende resourcegroepen.

Als u geen resourcegroepnaam opgeeft, maakt vRealize Automation een nieuwe resourcegroep. Dit houdt in dat een nieuwe beschikbaarheidsset ook moet worden gemaakt, zelfs als een naam wordt doorgegeven. De nieuwe set gebruikt de naam die wordt doorgegeven.

Tabel 3-16.

Resourcegroep opgegeven	Beschikbaarheidsset opgegeven	Resultaat
Nee	Nee	vRealize Automation maakt een nieuwe resourcegroep en een nieuwe beschikbaarheidsset voor de virtuele machine.
Ja	Nee	vRealize Automation hergebruikt een bestaande resourcegroep en maakt een nieuwe beschikbaarheidsset voor de virtuele machine.
Nee	Ja	vRealize Automation maakt een nieuwe resourcegroep en een nieuwe beschikbaarheidsset met de opgegeven naam.
Ja	Ja	vRealize Automation hergebruikt de bestaande resourcegroep. Als er al een beschikbaarheidsset met de opgegeven naam in die groep bestaat, wordt deze ook opnieuw gebruikt. Als er geen beschikbaarheidsset is met de opgegeven naam in de groep, wordt er een nieuwe met die naam gemaakt.

Cloud Assembly ondersteunt momentopnamen van Azure-schijven voor geïmplementeerde virtuele machines. Zie [Werken met momentopnamen voor schijven van virtuele Microsoft Azure-machines in vRealize Operations Manager](#) voor meer informatie.

Cloud Assembly ondersteunt verschillende opties voor opstartdiagnose voor Azure-implementaties. Opstartdiagnose maakt foutopsporing mogelijk bij virtuele Azure-machines en kan daarbij logboekinformatie en relevante schermafbeeldingen verzamelen. Zie [Opstartdiagnose en logboekanalyse gebruiken met een virtuele Microsoft Azure-machine](#) voor meer informatie.

Opstartdiagnose en logboekanalyse gebruiken met een virtuele Microsoft Azure-machine

U kunt Microsoft Azure-opstartdiagnose aanroepen en configureren vanaf een Azure-instantie in een cloudsjabloon. Daarnaast kunt u ook logboekanalyse configureren voor een instantie van een virtuele Azure-machine. De opstartdiagnose is een foutopsporingsfunctie voor virtuele machines in Azure die de diagnose van de opstartfouten van de virtuele machines mogelijk maakt. Met behulp van de opstartdiagnose kan een gebruiker de status van een virtuele machine controleren wanneer deze wordt opgestart, door seriële logboekinformatie en schermafbeeldingen te verzamelen.

Opstartdiagnose

Opstartdiagnose legt seriële logboekinformatie en schermafbeeldingen vast en deze moeten op de schijf worden opgeslagen. Er zijn twee typen schijven mogelijk: een beheerde Azure-schijf of een niet-beheerde schijf.

De YAML-eigenschap `bootDiagnostics` wordt ondersteund in Azure-cloudsjablonen. Wanneer deze eigenschap is ingesteld op `true`, wordt de opstartdiagnose ingeschakeld voor de toepasselijke implementatie van de virtuele Azure-machine.

In het volgende YAML-fragment ziet u een voorbeeld van hoe de `bootDiagnostics`-eigenschap wordt gebruikt.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Azure_Machine_1:
    type: Cloud.Azure.Machine
    metadata:
      layoutPosition:
        - 0
        - 0
    properties:
      image: ubuntu
      flavor: small
      bootDiagnostics: true
```

Opstartdiagnose kan ook als een bewerking voor dag 2 worden aangeroepen voor een geïmplementeerde virtuele Azure-machine. Ga naar de pagina Implementaties in Cloud Assembly en selecteer de Azure-implementatie. In het menu Acties op deze pagina kunt u de opstartdiagnose desgewenst in- of uitschakelen.

Nadat u een cloudsjabloon hebt geïmplementeerd met opstartdiagnose ingeschakeld, geeft de pagina Cloud Assembly-implementaties aan dat de opstartdiagnose is ingeschakeld. Als u de opstartdiagnose wilt uitschakelen, klikt u op het menu Acties op de pagina Implementaties en selecteert u Opstartdiagnose uitschakelen.

Logboekanalyse

Logboekanalyse stelt u in staat om logboekquery's te bewerken en uit te voeren op basis van gegevens die door Azure Monitor-logboeken worden verzameld, en vervolgens de resultaten interactief te analyseren. U kunt query's voor logboekanalyse gebruiken om records op te halen die overeenkomen met specifieke criteria om trends en patronen te identificeren en verschillende gegevensinzichten te bieden. Door Logboekanalyse in te schakelen op een virtuele Azure-machine, zal die machine als gegevensbron fungeren.

Voordat u logboekanalyse in een Cloud Assembly-cloudsjabloon kunt configureren, moet u een werkruimte voor Azure-logboekanalyse maken en configureren. U kunt dit doen met de optie Virtuele machines in het Azure Monitor-menu. Zie de documentatie voor Microsoft Azure voor meer informatie.

Als u logboekanalyse wilt configureren, moet u de werkruimte-id en de werkruimtesleutel van Azure hebben. U kunt deze vinden op het tabblad Agentbeheer in Azure onder de Log Analytics-werkruimte.

In het volgende voorbeeld van een cloudsjabloon ziet u hoe logboekanalyse kan worden geconfigureerd met behulp van extensies.

```
formatVersion: 1
inputs: {}
resources:
```

```

Cloud_Azure_Machine_1:
  type: Cloud.Azure.Machine
  properties:
    image: ubuntu
    flavor: small
  extensions:
    - autoUpgradeMinorVersion: true
      name: test-loga
      protectedSettings:
        workspaceKey: xxxxxxxxxx
      publisher: Microsoft.EnterpriseCloud.Monitoring
      settings:
        workspaceId: aaaaaaaaaa
        type: OmsAgentForLinux
        typeHandlerVersion: '1.0'

```

Nadat u een cloudsjabloon hebt geïmplementeerd met logboekanalyse ingeschakeld, kunt u deze in- of uitschakelen met de opties in het menu Acties op de pagina Cloud Assembly-implementaties voor de implementatie.

Werken met momentopnamen voor schijven van virtuele Microsoft Azure-machines in vRealize Operations Manager

U kunt volledige of incrementele momentopnamen maken van door Microsoft Azure beheerde schijven.

De pagina Implementaties van Cloud Assembly voor een Azure-implementatie bevat een menu Acties met verschillende opties voor het maken en verwijderen van momentopnamen uit Azure-implementaties op beheerde schijven van een virtuele machine en op onafhankelijke beheerde schijven. In de volgende lijst wordt de specifieke functionaliteit voor momentopnamen beschreven die wordt ondersteund.

- Een momentopname van een schijf maken - ondersteund voor zowel externe als computerschijven. U kunt ook momentopnamen maken van een schijf in een andere resourcegroep.
- Een momentopname van een schijf verwijderen - alleen ondersteund voor externe schijven
- Versleutel de momentopnamen met behulp van een versleutelingsset voor Azure-schijven.
- U kunt sleutelwaardeparen als tags opgeven tijdens het maken van een momentopname.

Momentopnamen op onbeheerde schijven worden momenteel niet ondersteund.

Als u versleuteling gebruikt, ondersteunt de huidige implementatie van momentopnamen de versleuteling van platformbeheerde sleutels. Het netwerkbeleid staat toegang standaard van overal toe, zodat toegang tot momentopnamen via het netwerkbeleid niet kan worden beperkt.

Zie [Welke acties kan ik op Cloud Assembly-implementaties uitvoeren](#) voor meer informatie over het gebruik van de Cloud Assembly-acties en de pagina Implementaties.

Raadpleeg [Een momentopname van een virtuele harde schijf maken](#) in de Microsoft-productdocumentatie voor meer informatie over ondersteuning voor Microsoft Azure-momentopnamen.

Een Amazon Web Services-cloudaccount maken in vRealize Automation

Als cloudbeheerder kunt u een Amazon Web Services-cloudaccount (AWS) maken voor accountregio's waarop uw team vRealize Automation-cloudsjablonen gaat implementeren.

In de volgende procedure wordt beschreven hoe u een AWS-cloudaccount configureert.

Voorwaarden

- Controleer of u over de vereiste beheerdersreferenties beschikt en HTTPS-toegang hebt ingeschakeld op poort 443. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Controleer of u de vereiste gebruikersrol hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Controleer of u over de vereiste AWS-beheerdersreferenties beschikt.
- Als u geen externe internettoegang hebt, configureert u een internetserverproxy. Zie [Hoe configureer ik een internetproxyserver voor vRealize Automation](#).

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Cloudaccounts** en klik op **Cloudaccount toevoegen**.
- 2 Selecteer het accounttype AWS en voer de verificatiegegevens en andere waarden in.
- 3 Klik op **Valideren**.
De accountregio's die aan het account zijn gekoppeld worden verzameld.
- 4 Selecteer de regio's waarin u deze resource wilt inrichten.
- 5 Klik op **Een cloudzone maken voor de geselecteerde regio's** om efficiënt te werken.
- 6 Als u tags moet toevoegen om een tagstrategie te ondersteunen, voert u mogelijkheidstags in. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#) en [Een tagstrategie maken](#).



Voor meer informatie over hoe capaciteitstags en beperkingstags helpen bij het beheren van implementatieplaatsingen raadpleegt u de [Beperkingstags en plaatsing](#)-videotutorial.

- 7 Klik op **Toevoegen**.

Resultaten

Het account wordt toegevoegd aan vRealize Automation en de geselecteerde regio's zijn beschikbaar voor de opgegeven cloudzone.

Wat nu te doen

Configureer infrastructuurbronnen voor dit cloudaccount.

Een Google Cloud Platform-cloudaccount maken in vRealize Automation

Als cloudbeheerder kunt u een Google Cloud Platform-cloudaccount (GCP) maken voor accountregio's waarop uw team vRealize Automation-cloudsjablonen gaat implementeren.

Voorwaarden

- Controleer of u over de vereiste beheerdersreferenties beschikt en HTTPS-toegang hebt ingeschakeld op poort 443. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Controleer of u de vereiste gebruikersrol hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Controleer of u toegang hebt tot de JSON-beveiligingssleutel voor het Google Cloud Platform.
- Controleer of u over de vereiste beveiligingsinformatie voor uw Google Cloud Platform-instantie beschikt. De meeste informatie kunt u verkrijgen via uw instantie of de Google-documentatie.
- Als u geen externe internettoegang hebt, configureert u een internetserverproxy. Zie [Hoe configureer ik een internetproxyservice voor vRealize Automation](#).

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Cloudaccounts** in Cloud Assembly en klik vervolgens op **Cloudaccount toevoegen**.
- 2 Selecteer het Google Cloud Platform-accounttype en voer de juiste verificatiegegevens en bijbehorende informatie in. Gebruik het serviceaccount dat is gemaakt bij het initialiseren van de berekeningsengine van het GCP-bronaccount.

Zoals beschreven in de sectie **Voorwaarden** hierboven zijn de vereisten voor inloggegevens beschikbaar op [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#). Om het cloudaccount in vRealize Automation te maken, moet voor het GCP-bronaccount de berekeningsengineservice zijn ingeschakeld.

In vRealize Automation is de project-id onderdeel van het Google Cloud Platform-eindpunt. U geeft deze op wanneer u het cloudaccount maakt. Tijdens het verzamelen van gegevens van projectspecifieke privé-images, bevraagt de vRealize Automation GCP-adapter de Google Cloud Platform API.

3 Klik op Valideren.

De accountregio's die aan het account zijn gekoppeld worden verzameld.

4 Selecteer de regio's waarin u deze resource wilt inrichten.**5 Klik op Een cloudzone maken voor de geselecteerde regio's om efficiënt te werken.****6 Als u tags nodig hebt om een tagstrategie te ondersteunen, voert u mogelijkheidstags in. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#) en [Een tagstrategie maken](#).**

Voor meer informatie over hoe capaciteitstags en beperkingstags helpen bij het beheren van implementatieplaatsingen raadpleegt u de [Beperkingstags en plaatsing](#)-videotutorial.

7 Klik op Toevoegen.**Resultaten**

Het account wordt toegevoegd aan vRealize Automation en de geselecteerde regio's zijn beschikbaar voor de opgegeven cloudzone.

Wat nu te doen

Maak infrastructuurresources voor dit cloudaccount.

In de volgende alinea's wordt informatie gegeven over het implementeren van een virtuele machine van Google Cloud Platform vanuit Cloud Assembly.

Wanneer u een Google Cloud Platform-cloudaccount toevoegt aan een Cloud Assembly-cloudsjabloon, kunt u de YAML-eigenschap `useSoleTenant` gebruiken om aan te geven dat u een virtuele machine wilt implementeren op een knooppunt met één tenant. Met deze configuratie kunt u virtuele machines isoleren bij beveiligings-, privacy- of andere problemen.

Om deze functionaliteit te vereenvoudigen, worden affiniteitslabels voor het Google Cloud Platform-knooppunt geconverteerd naar tags in Cloud Assembly. Deze tags worden toegepast op relevante vRealize Automation-beschikbaarheidszones waar zich knooppuntgroepen bevinden. Wanneer de eigenschap `useSoleTenant` is ingesteld op waar, moeten beperkingstags een van de affiniteitslabels van het knooppunt zijn. Als u een machine alleen in een modus met één tenant wilt implementeren, moet u de eigenschap `useSoleTenant` in de cloudsjabloon, evenals de beperkingstags, opnemen.

Voordat u deze functie gebruikt, moet u de juiste knooppuntsjabloon en de affiniteitslabels van het knooppunt maken in Google Cloud Platform en vervolgens een knooppuntgroep maken.

In het volgende YAML-voorbeeld ziet u hoe de eigenschap `useSoleTenant` in Cloud Assembly-cloudsjablonen kan worden gebruikt. De beperkingstags zijn de affiniteitslabels van het knooppunt die automatisch zijn verzameld van uw Google Cloud Platform-server.

```
resources:
  Cloud_GCP_Machine_1:
    type: Cloud.GCP.Machine
```

```

properties:
  image: ubuntu
  flavor: c2-family
  name: demo-vm
  useSoleTenant: true
  constraints:
    -tag: 'env:prod'
    -tag: 'region:asia-east1'

```

Een vCenter-cloudaccount maken in vRealize Automation

U kunt een vCenter-cloudaccount toevoegen voor de accountregio's waarop u vRealize Automation-cloudsjablonen wilt implementeren.

Voor netwerk- en beveiligingsdoeleinden kunt u een vCenter-cloudaccount koppelen aan een NSX-T- of NSX-V-cloudaccount.

Een NSX-T-cloudaccount kan worden gekoppeld aan een of meer vCenter-cloudaccounts. Een NSX-V-cloudaccount kan echter alleen worden gekoppeld aan een vCenter-cloudaccount.

Voorwaarden

- Controleer of u over de vereiste beheerdersreferenties beschikt en HTTPS-toegang hebt ingeschakeld op poort 443. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Controleer of u de gebruikersrol van cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Controleer of u uw poorten en protocollen correct hebt geconfigureerd om het cloudaccount te ondersteunen. Raadpleeg het onderwerp *Poorten en protocollen voor vRealize Automation* in *vRealize Automation installeren met vRealize Easy-installatieprogramma* en het onderwerp *Poortvereisten* in *Handleiding Referentie-architectuur vRealize Automation* in de [vRealize Automation-productdocumentatie](#).

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Cloudaccounts** en klik op **Cloudaccount toevoegen**.
- 2 Selecteer het vCenter-accounttype en voer het IP-adres van de vCenter Server-host in.
- 3 Voer uw vCenter Server-beheerdersreferenties in en klik op **Valideren**.

Gegevens van alle datacenters die aan het account zijn gekoppeld worden verzameld. Gegevens van de volgende elementen worden verzameld, evenals alle vSphere-labels voor de volgende elementen:

- Machines
- Clusters en hosts
- Poortgroepen

■ Gegevensopslag

- 4 Selecteer ten minste één van de beschikbare datacenters op de opgegeven vCenter Server om inrichting voor dit cloudaccount toe te staan.

- 5 Een efficiënte werkwijze is het maken van een cloudzone voor inrichting op de geselecteerde datacenters.

U kunt ook cloudzones maken in een afzonderlijke stap in overeenstemming met de cloudstrategie van uw organisatie.

Zie [Meer informatie over Cloud Assembly-cloudzones](#) voor informatie over cloudzones.

- 6 Selecteer nu een bestaand NSX-cloudaccount.

U kunt het NSX-account nu selecteren, of later wanneer u het cloudaccount bewerkt.

Zie [Een NSX-V-cloudaccount maken in vRealize Automation](#) voor informatie over NSX-V-cloudaccounts.

Zie [Een NSX-T-cloudaccount maken in vRealize Automation](#) voor informatie over NSX-T-cloudaccounts.

Zie [Wat gebeurt er als ik een NSX-cloudaccountassociatie in vRealize Automation verwijder](#) voor informatie over het maken van associatiewijzigingen nadat u een cloudsjabloon heeft geïmplementeerd.

- 7 Als u tags wilt toevoegen om een tagstrategie te ondersteunen, voert u capaciteitstags in.

U kunt nu tags toevoegen, of later wanneer u het cloudaccount bewerkt. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#) voor informatie over taggen.



Voor meer informatie over hoe capaciteitstags en beperkingstags helpen bij het beheren van implementatieplaatsingen raadpleegt u de [Beperkingstags en plaatsing](#)-videotutorial.

- 8 Klik op **Opslaan**.

Resultaten

Het cloudaccount wordt toegevoegd en de geselecteerde datacenters zijn beschikbaar voor de opgegeven cloudzone. Verzamelde gegevens, zoals machines, netwerken, opslag en volumes, worden weergegeven in het gedeelte **Resources** van het tabblad **Infrastructuur**.

Wat nu te doen

Configureer resterende infrastructuurresources voor dit cloudaccount. Zie [Hoofdstuk 4 Uw Cloud Assembly-resource-infrastructuur maken](#).

Een NSX-V-cloudaccount maken in vRealize Automation

Voor netwerk- en beveiligingsdoeleinden kunt u een NSX-V-cloudaccount koppelen aan een vCenter-cloudaccount.

Een NSX-V-cloudaccount kan alleen worden gekoppeld aan één vCenter-cloudaccount.

De associatie tussen NSX-V en een vCenter-cloudaccount moet buiten vRealize Automation worden geconfigureerd, met name in uw NSX-applicatie. vRealize Automation maakt geen associatie tussen NSX en vCenter. In vRealize Automation geeft u een associatie op die al bestaat in NSX.

Voorwaarden

- Controleer of u over de vereiste beheerdersreferenties beschikt en HTTPS-toegang hebt ingeschakeld op poort 443. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Controleer of u de gebruikersrol van cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Controleer of u een vCenter-cloudaccount hebt dat u kunt gebruiken met dit NSX-cloudaccount. Zie [Een vCenter-cloudaccount maken in vRealize Automation](#).
- Controleer of u uw poorten en protocollen correct hebt geconfigureerd om het cloudaccount te ondersteunen. Raadpleeg het onderwerp *Poorten en protocollen voor vRealize Automation in vRealize Automation installeren met vRealize Easy-installatieprogramma* en het onderwerp *Poortvereisten in Handleiding Referentie-architectuur vRealize Automation* in de [vRealize Automation-productdocumentatie](#).

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Cloudaccounts** en klik op **Cloudaccount toevoegen**.

- 2 Selecteer het NSX-V-accounttype en voer het IP-adres van de NSX-V-host in.

- 3 Voer uw NSX-beheerdersreferenties in en klik op **Valideren**.

De assets die aan het account zijn gekoppeld worden verzameld.

Als het IP-adres van de NSX-host niet beschikbaar is, mislukt de validatie.

- 4 Selecteer, indien beschikbaar, het vCenter-endpoint dat het vCenter-cloudaccount vertegenwoordigt dat u aan dit NSX-V-account koppelt.

Alleen vCenter-cloudaccounts die momenteel niet zijn gekoppeld aan een NSX-T- of NSX-V-cloudaccount zijn beschikbaar voor selectie.

Zie [Wat gebeurt er als ik een NSX-cloudaccountassociatie in vRealize Automation verwijder](#) voor informatie over het maken van associatiewijzigingen nadat u een cloudsjabloon heeft geïmplementeerd.

- 5 Als u tags wilt toevoegen om een tagstrategie te ondersteunen, voert u capaciteitstags in.

U kunt later mogelijkheidstags toevoegen of verwijderen. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#).



Voor informatie over hoe capaciteitstags en beperkingstags helpen bij het beheren van implementatieplaatsingen raadpleegt u de [Beperkingstags en plaatsing-videotutorial](#).

6 Klik op **Opslaan**.

Wat nu te doen

U kunt een vCenter-cloudaccount maken of bewerken om het te koppelen aan dit NSX-cloudaccount. Zie [Een vCenter-cloudaccount maken in vRealize Automation](#).

Maak en configureer een of meer cloudzones voor gebruik met de datacenters die worden gebruikt door dit cloudaccount. Zie [Meer informatie over Cloud Assembly-cloudzones](#).

Configureer infrastructuurbronnen voor dit cloudaccount. Zie [Hoofdstuk 4 Uw Cloud Assembly-resource-infrastructuur maken](#).

Een NSX-T-cloudaccount maken in vRealize Automation

Voor netwerk- en beveiligingsdoeleinden kunt u een NSX-T-cloudaccount maken en deze koppelen aan een of meer vCenter-cloudaccounts.

Een NSX-T-cloudaccount kan worden gekoppeld aan een of meer vCenter-cloudaccounts. Een NSX-V-cloudaccount kan echter alleen worden gekoppeld aan een vCenter-cloudaccount.

De associatie tussen NSX-T en een of meer vCenter-cloudaccounts moet buiten vRealize Automation worden geconfigureerd, met name in uw NSX-applicatie. vRealize Automation maakt geen associatie tussen NSX en vCenter. In vRealize Automation geeft u een of meer configuratie-associaties op die al bestaan in NSX.

Wanneer u een NSX-T-cloudaccount in vRealize Automation maakt, geeft u een managertype en een NSX-modus. Deze selecties kunnen niet worden gewijzigd nadat u het cloudaccount hebt gemaakt.

U kunt verbinding maken met een algemene NSX-T-manager en een koppeling tussen een algemene NSX-T-manager en lokale managers in de context van NSX-T Federation configureren.

Zie de [productdocumentatie voor het NSX-T Data Center](#) voor gerelateerde informatie over opties en mogelijkheden voor NSX-T in het algemeen.

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. Als u deze optie gebruikt, ontvangt één NSX-manager de API-aanroepen van vRealize Automation.
- vRealize Automation kan verwijzen naar het virtuele IP-adres van het cluster. Als u deze optie gebruikt, neemt een NSX-manager de controle over van de VIP. Die NSX 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.

Zie voor meer informatie over de VIP-configuratie voor NSX *Een Virtueel IP-adres (VIP) voor een cluster configureren* in de *NSX-T Data Center-installatiehandleiding* bij [VMware NSX-T Data Center-documentatie](#).

- vRealize Automation kan naar een load balancer-VIP verwijzen om de aanroepen over 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 omgevingen op grote schaal kunt u deze optie gebruiken om de vRealize Automation-API-aanroepen tussen de drie NSX-managers te verdelen.

Zie het VMware-blogbericht [VMware Network Automation met NSX-T 3.2 en vRealize Automation](#) voor een gedetailleerd overzicht van het gebruik van NSX-T 3.2 met vRealize Automation.

Voorwaarden

- Controleer of u over de vereiste beheerdersreferenties beschikt en HTTPS-toegang hebt ingeschakeld op poort 443. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Controleer of u de gebruikersrol van cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Controleer of u een vCenter-cloudaccount hebt dat u kunt gebruiken met dit NSX-cloudaccount. Zie [Een vCenter-cloudaccount maken in vRealize Automation](#).
- Controleer of u uw poorten en protocollen correct hebt geconfigureerd om het cloudaccount te ondersteunen. Raadpleeg het onderwerp *Poorten en protocollen voor vRealize Automation* in *vRealize Automation installeren met vRealize Easy-installatieprogramma* en het onderwerp *Poortvereisten* in *Handleiding Referentie-architectuur vRealize Automation* in de [vRealize Automation-productdocumentatie](#).

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Cloudaccounts** en klik op **Cloudaccount toevoegen**.
- 2 Selecteer het NSX-T-accounttype en geef een naam en beschrijving van een cloudaccount op.
- 3 Voer het IP-adres van de host in voor de NSX-T-managerinstantie of VIP (zie hierboven voor informatie over het verwachte gedrag dat betrekking heeft op de NSX-manager en VIP-opties).
- 4 Voer uw NSX-verificatiegegevens met gebruikersnaam en wachtwoord in.
- 5 Selecteer **Algemeen** of **Lokaal** (standaard) als **Managertype**.
 - Algemene manager
De instelling Algemene manager is alleen beschikbaar voor gebruik met de beleidsinstelling **NSX-modus**. Deze functie is niet beschikbaar wanneer u de managerinstelling **NSX-modus** gebruikt.

De instelling Algemeen verwijst naar de mogelijkheden van NSX-T Federation, inclusief algemene netwerksegmenten. Alleen NSX-T-cloudaccounts met de instelling Algemeen ondersteunen NSX-T Federation.

Wanneer u de instelling Algemene manager gebruikt, wordt u gevraagd een NSX-T-cloudaccount voor een lokale manager en een gekoppeld vCenter Server-cloudaccount te identificeren.

U kunt geen NSX-T-cloudaccount voor een algemene manager aan een vCenter-cloudaccount koppelen, zoals u dat met een NSX-T-cloudaccount voor een lokale manager doet. Net zoals u een NSX-T-cloudaccount voor een lokale manager kunt koppelen aan meerdere vCenter-cloudaccounts, kan een NSX-T-cloudaccount voor een algemene manager aan meerdere lokale NSX-T-cloudaccounts voor een lokale manager worden gekoppeld.

- Lokale manager

Gebruik de instelling Lokaal voor het definiëren van een traditioneel NSX-T-cloudaccount, dat kan worden gekoppeld aan een of meer vSphere-cloudaccounts. U kunt een NSX-T-cloudaccount voor een algemene manager koppelen aan lokale NSX-T-cloudaccounts. Dit is ook de instelling die wordt gebruikt als u een nieuw en leeg NSX-T-doelcloudaccount maakt voor de migratie van NSX-V naar NSX-T.

U kunt de instelling **Managertype** niet wijzigen nadat u het cloudaccount hebt gemaakt.

6 Selecteer **Beleid** of **Manager** voor **NSX-modus**.

- Beleidsmodus (standaard)

De beleidsmodus is beschikbaar voor NSX-T 3.0 en NSX-T 3.1 of hoger. Met deze optie kan vRealize Automation de extra mogelijkheden gebruiken die beschikbaar zijn in de NSX-T-Beleids-API.

Als u NSX-T gebruikt met een VMware Cloud on AWS-cloudaccount in een cloudsjabloon, moet het NSX-T-cloudaccount de **NSX-modus** van het beleid gebruiken.

De instelling Beleid verwijst naar het API-formulier voor het NSX-T-beleid van NSX-T.

- Managermodus

Bestaande NSX-T-eindpunten of cloudaccounts die worden geüpgraded van een eerdere versie van vRealize Automation die geen beleidsoptie heeft, worden als NSX-T-cloudaccounts in de managermodus behandeld.

De managermodus wordt ondersteund voor NSX-T 2.4, NSX-T 3.0 en NSX-T 3.1 en hoger.

Als u de managermodus opgeeft, gebruikt u de optie Managermodus voor andere NSX-T-cloudaccounts totdat vRealize Automation een managermodus in het migratiepad van de beleidsmodus introduceert.

Sommige vRealize Automation-opties voor NSX-T vereisen NSX-T 3.0 of hoger, inclusief het toevoegen van labels aan de NIC-onderdelen van de virtuele machine in de cloudsjabloon.

De instelling Manager verwijst naar het API-formulier voor NSX-T Manager van NSX-T.

Als u bestaande NSX-T-cloudaccounts hebt die zijn gemaakt vóór de invoering van de beleidsmodus in vRealize Automation 8.2, gebruiken ze de Manager-API-methode. We raden u aan te wachten tot de tool voor de migratie van Manager-API naar Beleids-API beschikbaar is gesteld in vRealize Automation. Als u liever niet wacht, moet u uw bestaande NSX-T-cloudaccounts vervangen door nieuwe NSX-T-cloudaccounts die de API-methode van het beleid opgeven.

U kunt de waarde **NSX-modus** niet wijzigen nadat u het cloudaccount hebt gemaakt.

- 7 Klik op **Valideren** om de verificatiegegevens voor het geselecteerde type NSX Manager en de NSX-modus te bevestigen.

De assets die aan het account zijn gekoppeld worden verzameld.

Als het IP-adres van de NSX-host niet beschikbaar is, mislukt de validatie.

- 8 Voeg in **Associaties** een of meer vCenter-cloudaccounts toe om te koppelen aan dit NSX-T-cloudaccount. U kunt ook bestaande vCenter-cloudaccountassociaties verwijderen.

Alleen vCenter-cloudaccounts die momenteel niet in vRealize Automation zijn gekoppeld aan een NSX-T- of NSX-V-cloudaccount zijn beschikbaar voor selectie.

Zie [Wat kan ik doen met NSX-T-toewijzing aan meerdere vCenters in vRealize Automation](#).

Zie [Wat gebeurt er als ik een NSX-cloudaccountassociatie in vRealize Automation verwijder](#) voor informatie over het maken van associatiewijzigingen nadat u een cloudsjabloon hebt geïmplementeerd, of over het verwijderen van cloudaccount nadat u een cloudsjabloon hebt geïmplementeerd.

- 9 Als u tags wilt toevoegen om een tagstrategie te ondersteunen, voert u capaciteitstags in.

U kunt later mogelijkheidstags toevoegen of verwijderen. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#).



Voor meer informatie over hoe capaciteitstags en beperkingstags helpen bij het beheren van implementatieplaatsingen raadpleegt u de [Beperkingstags en plaatsing](#)-videotutorial.

- 10 Klik op **Opslaan**.

Wat nu te doen

U kunt een vCenter-cloudaccount maken of bewerken om het te koppelen aan dit NSX-cloudaccount. Zie [Een vCenter-cloudaccount maken in vRealize Automation](#).

Maak en configureer een of meer cloudzones voor gebruik met de datacenters die worden gebruikt door dit cloudaccount. Zie [Meer informatie over Cloud Assembly-cloudzones](#).

Configureer infrastructuurbronnen voor dit cloudaccount. Zie [Hoofdstuk 4 Uw Cloud Assembly-resource-infrastructuur maken](#).

Zie [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#) voor voorbeelden van het gebruik van NSX-T-opties in vRealize Automation-cloudsjablonen.

Een VMware Cloud on AWS-cloudaccount maken in vRealize Automation

Als cloudbeheerder kunt u een VMware Cloud on AWS-cloudaccount maken voor accountregio's waarop uw team vRealize Automation-cloudsjablonen gaat implementeren.

Voor VMware Cloud on AWS zijn enkele unieke configuratieprocedures in vRealize Automation vereist. Voor een correcte configuratie van vRealize Automation voor VMware Cloud on AWS, inclusief het instellen van API-tokenwaarden voor het cloudaccount en het instellen van gateway-firewallregels voor de bijbehorende cloudproxy, zie de werkstroom [Tutorial: VMware Cloud on AWS voor vRealize Automation configureren](#).

Voorwaarden

- Controleer of u over de vereiste VMware Cloud on AWS-beheerdersreferenties beschikt, inclusief CloudAdmin-verificatiegegevens van VMware Cloud on AWS voor het doel-SDDC in vCenter en of u HTTPS-toegang op poort 443 hebt ingeschakeld. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Controleer of u de gebruikersrol van cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Als u geen externe internettoegang hebt, configureert u een internetserverproxy. Zie [Hoe configureer ik een internetproxyserver voor vRealize Automation](#).
- Controleer of u de benodigde toegangs- en firewallregels in de SDDC hebt geconfigureerd. Zie [Uw SDDC voor VMware Cloud on AWS voorbereiden om verbinding te maken met VMware Cloud on AWS-cloudaccounts in vRealize Automation](#).

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Cloudaccounts**, klik op **Cloudaccount toevoegen** en selecteer het VMware Cloud on AWS-accounttype.

- 2 Voeg de **VMC API-token** voor uw organisatie toe om toegang te krijgen tot de beschikbare SDDC's.

U kunt een nieuwe token maken of een bestaande token voor uw organisatie gebruiken op de gekoppelde pagina **API-tokens**. Zie [Een VMware Cloud on AWS-cloudaccount in vRealize Automation maken in een voorbeeldwerkstroom](#) voor meer informatie.

- 3 Selecteer de SDDC die u beschikbaar wilt maken voor implementaties.

NSX-V SDDC's worden niet ondersteund en worden niet weergegeven in de lijst.

De IP-adres-/FQDN-waarden voor vCenter en NSX-T Manager worden automatisch ingevuld op basis van de SDDC.

- 4 Voer uw gebruikersnaam en wachtwoord voor vCenter in voor de opgegeven SDDC indien deze verschillen van de standaardwaarden voor cloudadmin@vmc.local.

- 5 Klik op **Valideren** om uw toegangsrechten voor de opgegeven vCenter te valideren en controleer of de vCenter actief is.

De datacenters die aan het account zijn gekoppeld worden verzameld.

- 6 Een efficiënte werkwijze is het maken van een cloudzone voor inrichting op de geselecteerde SDDC.

U kunt ook cloudzones maken in een afzonderlijke stap in overeenstemming met de cloudstrategie van uw organisatie.

- 7 Als u tags wilt toevoegen om een tagstrategie te ondersteunen, voert u capaciteitstags in.

U kunt later mogelijkheidstags toevoegen of verwijderen. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#).



Voor meer informatie over hoe capaciteitstags en beperkingstags helpen bij het beheren van implementatieplaatsingen raadpleegt u de [Beperkingstags en plaatsing](#)-videotutorial.

Zoals met VM's die zijn geïmplementeerd op vSphere, kunt u machinetags configureren voor een VM die op VMware Cloud on AWS moet worden geïmplementeerd. U kunt de machinetag ook bijwerken na de eerste implementatie. Met deze machinetags kan vRealize Automation dynamisch een VM toewijzen aan een geschikte NSX-T-beveiligingsgroep tijdens de implementatie. Zie [Meer informatie over beveiligingsgroep- en tagresources in vRealize Automation-cloudsjablonen](#) voor gerelateerde informatie.

- 8 Klik op **Opslaan**.

Resultaten

Het cloudaccount wordt toegevoegd en de geselecteerde SDDC is beschikbaar voor de opgegeven cloudzone.

Wat nu te doen

Voor een correcte configuratie van vRealize Automation voor VMware Cloud on AWS, zie [Tutorial: VMware Cloud on AWS voor vRealize Automation configureren](#).

Voor meer informatie over VMware Cloud on AWS buiten vRealize Automation, zie de documentatie van [VMware Cloud on AWS](#).

Een VMware Cloud Foundation-cloudaccount maken

U kunt een VMware Cloud Foundation (VCF) configureren als cloudaccount binnen Cloud Assembly om workloaddomeinen te gebruiken.

Met een VCF-cloudaccount kunt u een VCF-workload in Cloud Assembly integreren om een allesomvattende hybride cloudbeheeroplossing mogelijk te maken. Cloud Assembly biedt verschillende ingangspunten waarmee u de configuratiepagina van het VCF-cloudaccount kunt activeren. Als u deze pagina opent met de knop **Cloudaccount toevoegen** op het tabblad Workloaddomein voor de SDDC-integratie, is de workload vooraf geselecteerd, inclusief de basisinformatie voor vCenter en NSX Manager.

Voorwaarden

U moet een instantie van VMware SDDC Manager 4.1 of hoger als Cloud Assembly-integratie hebben geconfigureerd voor gebruik met dit cloudaccount. Zie [Een VMware SDDC Manager-integratie configureren](#) voor meer informatie.

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Cloudaccounts** en klik op **Cloudaccount toevoegen**.
- 2 Selecteer het type VCF-cloudaccount en voer een **naam** en **beschrijving** in.
- 3 Voer de FQDN en verificatiegegevens in voor de SDDC Manager-instantie die u gebruikt met dit cloudaccount.

U kunt deze stap overslaan als u de SDDC Manager-instantie die u met dit account wilt gebruiken, al hebt geconfigureerd.
- 4 Selecteer een of meer workloaddomeinen die u wilt gebruiken met dit VCF-cloudaccount.
- 5 Als u wilt dat Cloud Assembly met Cloud Foundation beheerde verificatiegegevens voor de service voor vCenter en NSX wilt gebruiken, selecteert u **Automatisch verificatiegegevens voor service maken**. Als u later deze verificatiegegevens wilt wijzigen, moet u het VCF-mechanisme gebruiken voor wachtwoordbeheer.

Als u deze optie selecteert, kunt u stappen 7 en 8 overslaan.
- 6 Voer de vereiste verificatiegegevens in voor toegang tot het vCenter dat aan dit cloudaccount is gekoppeld.
- 7 Voer onder NSX Manager de NSX-verificatiegegevens in als u handmatig verificatiegegevens voor het VCF-cloudaccount wilt invoeren, of klik op Verificatiegegevens voor de service maken en valideren als u wilt dat Cloud Assembly NSX-verificatiegegevens maakt en valideert.
- 8 Voer de vereiste verificatiegegevens in voor toegang tot het NSX-T-netwerk dat aan dit cloudaccount is gekoppeld.
- 9 Selecteer indien van toepassing de NSXodus.
- 10 Klik op **Valideren** om een verbinding met de SDDC Manager te bevestigen.
- 11 Selecteer indien van toepassing de datacenters die u wilt inrichten onder de kop Configuratie. Klik op het selectievakje als u een cloudzone wilt maken voor de geselecteerde datacenters.

12 Als u tags nodig hebt om een tagstrategie te ondersteunen, voert u capaciteitstags in. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#) en [Een tagstrategie maken](#).

13 Klik op **Opslaan**.

Resultaten

Met dit cloudaccount wordt het geselecteerde workloaddomein dat aan de opgegeven SDDC Manager is gekoppeld, in Cloud Assembly toegevoegd voor gebruik.

Als u aanvullende workloaddomeinen wilt beheren met behulp van vRealize Automation, moet u deze processen voor elk domein herhalen.

Wat nu te doen

Nadat u het VCF-cloudaccount hebt geconfigureerd, kunt u het account selecteren op de pagina voor het hoofdcloudaccount en klikt u op **Cloud instellen** om de VMware Cloud Foundation-wizard Snelstart te starten die uw cloud zal configureren.

Zie [Aan de slag met vRealize Automation via de VMware Cloud Foundation Snelstart](#) in Aan de slag voor meer informatie over de wizard Snelstart.

Een VMware Cloud Director-cloudaccount maken in vRealize Automation

U kunt een VMware Cloud Director-cloudaccount in vRealize Automation maken om virtuele Cloud Director-machines te implementeren met cloudonafhankelijke objecten. Cloud Director ondersteunt de flexibele inrichting van netwerk, opslag en computerbronnen en biedt een portalgebaseerde ervaring om vCenters en hun NSX-T- en NSX-V-netwerkappliances en bijbehorende virtuele datacenters te beheren via een catalogus.

Het VMware Cloud Director-cloudaccount ondersteunt het maken van standalone virtuele Cloud Director-machines zonder vApp. Er worden drie scenario's voor het inrichten van virtuele Cloud Director-machines via Cloud Assembly-cloudsjablonen ondersteund:

- Virtual machines
- Gekoppelde netwerken van virtuele machines
- Virtuele machines met een of meer extra schijven

Zie de officiële documentatie op <https://docs.vmware.com/nl/VMware-Cloud-Director/index.html> voor meer informatie over het werken met VMware Cloud Director, inclusief informatie over het instellen van meerdere servers voor hoge beschikbaarheid.

Het VMware Cloud Director-cloudaccount ondersteunt maximaal 1000 virtuele machines met vRealize Automation in aanhoudende modus.

In de volgende procedure wordt beschreven hoe u een VMware Cloud Director-cloudaccount binnen vRealize Automation Cloud Assembly instelt.

Voorwaarden

- Stel een implementatie van VMware Cloud Director 10.2.0, 10.2.1, 10.2.2, 10.3 of 10.3.1 in met een of meer geschikte organisaties.
- Gebruikers die zijn opgegeven voor deze integratie moeten beschikken over de privileges van de organisatiebeheerder om de toepasselijke sjablonen te lezen en om virtuele machines te maken, evenals om andere resources zoals computerbeleid, schijven, virtuele datacenters, enz. weer te geven. Het VCD-cloudaccount voor vRealize Automation werkt binnen een tenantcontext in Cloud Director, dus maakt u verbinding met een afzonderlijke organisatie in Cloud Director met uw tenantverificatiegegevens. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#) voor meer informatie over de vereiste verificatiegegevens.
- U moet uw geschikte opslag, netwerk, image en soorten of groottebeleidsregels configureren in uw VMware Cloud Director-instantie en deze objecten toewijzen in vRealize Automation Cloud Assembly, voordat of nadat u uw integratie configureert. In de volgende lijst wordt uitgelegd hoe virtuele VMware Cloud Director-objecten moeten worden toegewezen aan vRealize Automation-objecten in Cloud Assembly.
 - VMware Cloud Director-organisatienetwerken (geïsoleerd, direct, gerouteerd) - toewijzen aan vRealize Automation-netwerken. Er kan geen statische IP-pool worden ingesteld voor de netwerkadapter.
 - Groottebeleidsregels voor virtuele VMware Cloud Director-machines - toewijzen aan vRealize Automation-soorten.
 - VMware Cloud Director-opslagbeleidsregels - toewijzen aan vRealize Automation-opslagprofielen.
 - VMware Cloud Director-images (OVF, ISO-opstartmedia) - toewijzen aan vRealize Automation-images. Images kunnen vApp-sjablonen of -media zijn zoals ISO-bestanden. Als u ISO gebruikt, wordt een 'lege' virtuele machine gemaakt en worden de media gekoppeld als opstartmedia.
 - Virtuele VMware Cloud Director-machines - toewijzen aan vRealize Automation-computerbronnen.
 - Schijven van virtuele VMware Cloud Director-machines - toewijzen aan vRealize Automation-cloudvolumes.

U wijst deze VMware Cloud Director-objecten toe aan vRealize Automation-objecten met behulp van de opties op de pagina's **Infrastructuur > Configureren >** in Cloud Assembly. Zie de relevante onderwerpen onder [Hoofdstuk 4 Uw Cloud Assembly-resource-infrastructuur maken](#) voor gedetailleerde informatie over het toewijzen van objecten in vRealize Automation.

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Cloudaccounts** en klik op **Cloudaccount toevoegen**.

- 2 Selecteer het type VMware Cloud Director-cloudaccount en voer een **naam** en **beschrijving** in.
- 3 Voer de accountinformatie in die nodig is om toegang te krijgen tot de VMware Cloud Director-server.
- 4 Voer de basis-URL in die moet worden gebruikt om verbinding te maken met de VMware Cloud Director-server.
- 5 Voer een geschikte **gebruikersnaam** en geschikt **wachtwoord** in voor een geldig account dat toegang heeft tot de opgegeven Cloud Director-instantie.
- 6 Voer de gewenste naam voor de **organisatie** in voor gebruik met deze integratie.

In vCloud Director bevat een organisatie gebruikers, de vApps die ze maken en de resources die de vApps gebruiken.
- 7 Klik op **Valideren**.

Tijdens de validatie wordt u mogelijk gevraagd een certificaat te accepteren. Wanneer de verbinding is gevalideerd, kunt u aanvullende instellingen selecteren.
- 8 Als u tags nodig hebt om een tagstrategie te ondersteunen, voert u capaciteitstags in. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#) en [Een tagstrategie maken](#).
- 9 Na de validatie wordt op de pagina een lijst met virtuele datacentrums van Cloud Director weergegeven waaruit u kunt kiezen. Selecteer het juiste datacentrum. Met deze selectie bepaalt u in welke Director-regio's u kunt implementeren.
- 10 Klik op **Toevoegen** om het VMware Cloud Director-cloudaccount toe te voegen aan vRealize Automation.

Resultaten

Het VMware Cloud Director-cloudaccount is beschikbaar voor configuratie in vRealize Automation. De netwerken die zijn gekoppeld aan de Cloud Director-instantie, zijn beschikbaar voor configuratie op de pagina Cloud Assembly **Resources > Netwerken**. U kunt de betreffende opslagprofielen instellen en vervolgens het cloudaccount gebruiken om implementaties in cloudsjablonen te maken. Zorg er ook voor dat een geschikt project in Cloud Assembly is geconfigureerd voor gebruik met de Cloud Director-instantie.

Wat nu te doen

Het VMware Cloud Director-cloudaccount is klaar voor gebruik in Cloud Assembly-cloudsjablonen.

Het volgende voorbeeld is een cloudsjabloon voor een basisimplementatie van VMware Cloud Director.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Network_1:
    type: Cloud.Network
```

```

    properties:
      networkType: existing
      constraints:
        - tag: net1:isolated
  Cloud_Volume_1:
    type: Cloud.Volume
    properties:
      capacityGb: 2
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: image1
      flavor: small
      storage:
        constraints:
          - tag: storage:development
      attachedDisks:
        - source: '${resource.Cloud_Volume_1.id}'
      networks:
        - network: '${resource.Cloud_Network_1.id}'

```

De volgende acties voor dag 2 worden ondersteund op geïmplementeerde virtuele VMware Cloud Director-machines:

- Inschakelen
- Uitschakelen
- Opheffen
- Momentopname maken
- Terugzetten naar momentopname
- Momentopname verwijderen
- Schijf toevoegen
- Schijf verwijderen
- Schijfgrootte wijzigen (opmerking: alleen het vergroten van de schijf wordt ondersteund)
- Grootte van opstartschijf wijzigen

Nadat een blueprint is geïmplementeerd, kunnen gebruikers tags toepassen op nieuw ingerichte machines in vRealize Automation. Deze vRealize Automation-tags worden toegewezen aan VMware Cloud Director-metagegevens die kunnen worden opgehaald met de VMware Cloud Director API. Gebruikers kunnen ook andere vRealize Automation-resources taggen, maar alleen machines aan de VMware Cloud Director-zijde worden bijgewerkt, omdat dit het enige ondersteunde resourcetype van deze functie is.

Nadat een blueprint is geïmplementeerd, kunnen gebruikers de grootte van de opstartschijf van een virtuele machine wijzigen. Er worden ook normale schijven ondersteund. In dit geval hoeven klanten alleen een schijfresource te koppelen aan een machineresource. Wanneer alles is geïmplementeerd, kunt u de optie voor het bijwerken van de opstartschijf of het bijwerken van de schijf gebruiken om de gewenste schijf te vergroten, maar niet te verkleinen.

Nadat een blueprint is geïmplementeerd, kunnen gebruikers een groottebeleid voor virtuele machines wijzigen met de optie Grootte wijzigen voor de soortconfiguratie in vRealize Automation. Nadat deze is geselecteerd, gebruikt de virtuele machine met VMware Cloud Director het opgegeven groottebeleid.

Deze functie vereist dat de **Standaardrechtenbundel** die is toegewezen aan de rol Organisatiebeheerder het recht 'Computerbeleid wijzigen' bevat, waarvoor `VAPP_EDIT_VM_COMPUTE_POLICY` de interne code is. Dit recht moet worden geactiveerd voor de organisatiebeheerder. Anders mislukt het wijzigen van de grootte met de fout 403: `Either you need some or all of the following rights [VAPP_EDIT_VM_COMPUTE_POLICY] to perform operations.`

U kunt de grootte van de opstartschijf van een VMware Cloud Director VM als een bewerking voor dag 2 wijzigen door de virtuele machine te selecteren op de pagina Implementaties. U moet echter Fast provisioning uitschakelen voordat u probeert de grootte van de opstartschijf te wijzigen. Anders kan de volgende fout optreden:

```
Request timed out after 120 minutes. Please configure project request timeout
parameter for long running resource requests.
```

Houd er rekening mee dat deze vereiste alleen van toepassing is op virtuele machines die zijn gemaakt op basis van vApp-sjabloon-schijven. Deze is niet van toepassing op virtuele machines die zijn gemaakt op basis van ISO-bestanden.

In de volgende procedure wordt beschreven hoe u Fast provisioning uitschakelt.

- 1 Meld u aan bij VMware Cloud Director als systeembeheerder: `https://vcd_url/provider` met de systeemgebruiker
- 2 Klik op organisatie-VDC's.
- 3 Selecteer de doelorganisatie.
- 4 Klik op Opslag (onder Beleidsregels).
- 5 Schakel **Fast Provisioning** uit.

Logboeken en andere resources gebruiken om problemen met VMware Cloud Director-cloudaccounts in vRealize Automation op te lossen

Als u problemen ondervindt bij het configureren of gebruiken van een VMware Cloud Director-cloudaccount in vRealize Automation, kunt u logboeken en andere resources raadplegen zoals hieronder wordt beschreven.

Verbindingsproblemen met VMware Cloud Director-cloudaccounts oplossen

Als de VMware Cloud Director-adapter niet wordt weergegeven in het scherm voor het maken van het cloudaccount of niet reageert, kunt u het volgende commando gebruiken om de status te verifiëren door u aan te melden bij de vRealize Automation Kubernetes-host en de status van de adapterpod te controleren:

```
root@host [ ~ ]# kubectl -n prelude get pods | grep adapter-host-service-app
adapter-host-service-app-65f5c945bb-p6hpn      1/1      Running    0          4dlh
```

Als de VMware Cloud Director-adapter niet kan communiceren met de fysieke Cloud Director-machine, wordt een fout weergegeven in het scherm van het cloudaccount met instructies over verbindings- en verwerkingsuitzonderingen. De fout wordt ook in de logboeken weergegeven.

Werken met VMware Cloud Director-logboeken

Het hoofdlogbestand van de VMware Cloud Director-adapter bevindt zich onder het lokale dir /var/log/adapter-host-service-app.log (pod). In het geval van de adapter die in de host van de vRealize Automation-appliance wordt uitgevoerd, wordt dit logboek ook gekopieerd naar /services-logs/prelude/adapter-host-service-app/file-logs/. De meeste logboekregistraties zijn standaard beperkt tot de niveaus FOUTOPSPORING of INFO. U kunt de configuratie voor de volgende loggers wijzigen om meer uitgebreide logboekregistratie voor foutopsporing mogelijk te maken:

- `org.apache.cxf.services=INFO` - Deze logger biedt uitgebreide informatie voor de communicatie tussen de adapter en VMware Cloud Director.
- `com.vmware.vra.vcloud.director.adapter=TRACE` - Deze logger biedt uitgebreide informatie voor de communicatie tussen de adapter en vRealize Automation.

Er zijn drie manieren om toegang te krijgen tot de logboeken:

- toegang tot het logboek door u aan te melden bij de adapterpod

```
root@host [ ~ ]# kubectl -n prelude exec -ti adapter-host-service-app-65f5c945bb-p6hpn --
bash
root [ / ]# less /var/log/adapter-host-service-app.log
```

- toegang tot het logboek met behulp van kubectl

```
root@host [ ~ ]# kubectl -n prelude get logs adapter-host-service-app-65f5c945bb-p6hpn
```

- toegang tot het logboek met behulp van het lokale exemplaar van de Kubernetes-host van de adapter

```
root@host [ ~ ]# less /services-logs/prelude/adapter-host-service-app/file-logs/adapter-
host-service-app.log
```

U kunt de configuratie van de loggers opvragen of wijzigen via het REST API-eindpunt `/patch/loggers`.

- Voorbeeld van het inschakelen van VMware Cloud Director-clientcommunicatietracing via curl:

```
curl -i -X POST -H 'Content-Type: application/json' -d '{"configuredLevel": "INFO"}'
http://{adapter-url}/actuator/loggers/org.apache.cxf.services
```

- Voorbeeld van het uitschakelen van VMware Cloud Director-clientcommunicatietracing via curl:

```
curl -i -X POST -H 'Content-Type: application/json' -d '{"configuredLevel": "OFF"}'
http://{adapter-url}/actuator/loggers/org.apache.cxf.services
```

- Voorbeeld van het verkrijgen van de huidige configuratie voor VMware Cloud Director-clientcommunicatie via curl:

```
curl http://{adapter-url}/actuator/loggers/org.apache.cxf.services
...
{"configuredLevel":"OFF","effectiveLevel":"INFO"}
```

Er zijn andere parameters die kunnen worden aangepast om de prestaties van VMware Cloud Director te wijzigen.

- `vcd.max.thread.count`: deze parameter bepaalt de maximale mate van parallelisme bij het uitvoeren van VMware Cloud Director API-aanroepen. De standaardwaarde is 128.

Opmerking Door de waarde voor deze parameter te verlagen, wordt de belasting van de VMware Cloud Director-back-end tijdens het uitvoeren van de inventarisatie verminderd, maar kunnen de inventarisatieprestaties afnemen.

- `VCD_ADAPTER_PAGINATION_SIZE_IMAGES` - Deze parameter bepaalt de paginagrootte bij het uitvoeren van de inventarisatie van images. De standaardwaarde is 50.

Opmerking Verklein deze parameter als er time-outfouten voor de adapter optreden tijdens de inventarisatie van images.

vRealize Automation integreren met andere applicaties

Met integraties kunt u externe systemen aan vRealize Automation toevoegen.

Integraties omvatten vRealize Orchestrator, configuratiebeheer en andere externe systemen zoals GitHub, Ansible, Puppet en externe IPAM-providers zoals Infoblox.

Opmerking Als u geen externe internettoegang hebt en uw integratie dit vereist, kunt u een internetserverproxy configureren. Zie [Hoe configureer ik een internetproxyserver voor vRealize Automation](#).

Hoe gebruik ik Git-integratie in Cloud Assembly

Cloud Assembly ondersteunt integratie met diverse soorten of Git-opslagplaatsen, zodat u VMware Cloud Templates en actiescripts onder broncontrole kunt beheeren. Deze functie vereenvoudigt de controle en verantwoording van processen rond implementatie.

Cloud Assembly ondersteunt verschillende soorten Git-integratie, zoals beschreven in de volgende lijst. Elk van deze opties is een afzonderlijke integratie.

- GitHub-cloud, GitHub Enterprise op locatie
- GitLab-cloud, GitLab Enterprise op locatie
- BitBucket op locatie

U moet over een geschikte lokale Git-opslagplaats beschikken die is geconfigureerd met toegang voor alle aangewezen gebruikers om een Git-integratie met Cloud Assembly in te stellen. U moet ook cloudsjablonen in een specifieke structuur opslaan, zodat ze kunnen worden gedetecteerd door Git. Om een integratie met GitLab of GitHub te maken, selecteert u **Infrastructuur > Verbindingen > Integraties** in Cloud Assembly en maakt u de juiste keuze. U hebt de URL en het token voor de doelopslagplaats nodig.

Wanneer Git-integratie is geconfigureerd met een bestaande opslagplaats, worden alle cloudsjablonen die zijn gekoppeld aan geselecteerde projecten beschikbaar voor bevoegde gebruikers. U kunt deze sjablonen gebruiken met een bestaande implementatie of als basis voor een nieuwe implementatie. Wanneer u een project toevoegt, moet u bepaalde eigenschappen selecteren die betrekking hebben op waar en hoe dit in Git wordt opgeslagen.

U kunt acties rechtstreeks vanuit Cloud Assembly opslaan in een Git-opslagplaats. U kunt versies van actiescripts direct in Git maken of u kunt versies in Cloud Assembly maken. Als u een versie van een actie in Cloud Assembly maakt, wordt deze automatisch in Git opgeslagen als een versie. Cloudsjablonen zijn iets ingewikkelder, omdat u deze niet rechtstreeks vanuit Cloud Assembly kunt toevoegen aan een Git-integratie. U moet deze rechtstreeks in een Git-instantie opslaan en vervolgens kunt u deze uit Git ophalen wanneer u met de beheerpagina voor cloudsjablonen in Cloud Assembly werkt.

Voordat u begint

U moet uw cloudsjablonen maken en opslaan in een specifieke structuur, zodat deze kunnen worden gedetecteerd door GitLab of GitHub.

- Configureer en bewaar cloudsjablonen die met GitLab moeten worden geïntegreerd op de juiste manier. Alleen geldige sjablonen worden geïmporteerd in GitLab.
 - Maak een of meer aangewezen mappen voor de cloudsjablonen.
 - Alle cloudsjablonen moeten worden opgeslagen in `blueprint.yaml`-bestanden.
 - Zorg ervoor dat de eigenschappen `name:` en `version:` bovenaan uw sjablonen staan.

- Extraheer een API-sleutel voor de betreffende opslagplaats. In uw Git-account selecteert u uw aanmeldnaam in de rechterbovenhoek en gaat u naar het menu Instellingen. Selecteer **Toegangstokens** en geef vervolgens een naam op voor uw token en stel een vervaldatum in. Selecteer vervolgens API en maak het token. Kopieer de resulterende waarde en sla deze op.

De volgende richtlijnen moeten in acht worden genomen voor alle cloudsjablonen die worden gebruikt met een Git-integratie.

- Elke cloudsjabloon moet zich in een afzonderlijke map bevinden.
- Alle cloudsjablonen moeten de naam `blueprint.yaml` krijgen.
- Alle YAML-bestanden voor cloudbestanden moeten de velden `name` en `version` gebruiken.
- Alleen geldige cloudsjablonen worden geïmporteerd.
- Als u een conceptcloudsjabloon bijwerkt die is geïmporteerd uit Git en de inhoud ervan verschilt van de inhoud in de hoofdversie, wordt het concept in de volgende synchronisaties niet bijgewerkt en wordt een nieuwe versie gemaakt. Als u een sjabloon wilt bijwerken en ook verdere synchronisaties vanuit Git wilt toestaan, moet u na de laatste wijzigingen een nieuwe versie maken.
- [Integratie van GitLab-cloudsjabloon in Cloud Assembly configureren](#)
Deze procedure demonstreert het configureren van een GitLab-integratie in Cloud Assembly, zodat u met cloudsjablonen in de opslagplaats kunt werken en opgeslagen sjablonen die zijn gekoppeld aan toegewezen projecten automatisch kunt downloaden. Als u cloudsjablonen met GitLab wilt gebruiken, moet u een verbinding met een geschikte GitLab-instantie maken en vervolgens de gewenste sjablonen opslaan in die instantie.
- [GitHub-integratie configureren in Cloud Assembly](#)
U kunt de hostingservice van de cloudgebaseerde GitHub-opslagplaats integreren in Cloud Assembly.
- [Bitbucket-integratie configureren in Cloud Assembly](#)
Cloud Assembly ondersteunt integratie met Bitbucket voor gebruik als een Git-gebaseerde opslagplaats voor ABX-actiescripts en VMware Cloud Templates.

Integratie van GitLab-cloudsjabloon in Cloud Assembly configureren

Deze procedure demonstreert het configureren van een GitLab-integratie in Cloud Assembly, zodat u met cloudsjablonen in de opslagplaats kunt werken en opgeslagen sjablonen die zijn gekoppeld aan toegewezen projecten automatisch kunt downloaden. Als u cloudsjablonen met GitLab wilt gebruiken, moet u een verbinding met een geschikte GitLab-instantie maken en vervolgens de gewenste sjablonen opslaan in die instantie.

Wanneer GitLab-integratie is geconfigureerd met een bestaande opslagplaats, worden alle cloudsjablonen die zijn gekoppeld aan geselecteerde projecten beschikbaar voor bevoegde gebruikers. U kunt deze sjablonen gebruiken met een bestaande implementatie of als basis voor een nieuwe implementatie. Wanneer u een project toevoegt, moet u bepaalde eigenschappen selecteren die betrekking hebben op waar en hoe dit in GitLab wordt opgeslagen.

Opmerking U kunt geen nieuwe of bijgewerkte cloudsjablonen naar de Git-opslagplaats pushen vanuit Cloud Assembly. U kunt evenmin nieuwe sjablonen naar de opslagplaats pushen vanuit Cloud Assembly. Om cloudsjablonen aan een opslagplaats toe te voegen, moeten ontwikkelaars de Git-interface gebruiken.

Als u een conceptcloudsjabloon bijwerkt die is geïmporteerd uit Git en de inhoud ervan verschilt van de inhoud in de hoofdversie, wordt het concept in de volgende synchronisaties niet bijgewerkt en wordt een nieuwe versie gemaakt. Als u een cloudsjabloon wilt bijwerken en ook verdere synchronisaties vanuit Git wilt toestaan, moet u na de laatste wijzigingen een nieuwe versie maken.

Nadat u uw cloudsjablonen hebt ingesteld voor gebruik met GitLab en de vereiste informatie hebt verzameld, moet u de integratie met uw GitLab-instantie instellen. Vervolgens kunt u de aangewezen cloudsjablonen importeren in GitLab. U kunt een videodemonstratie van deze procedure bekijken op <https://www.youtube.com/watch?v=h0vqo63Sdgg>.

Voorwaarden

- Extraheer een API-sleutel voor de betreffende opslagplaats. In uw GitLab-account selecteert u uw aanmeldnaam in de rechterbovenhoek en gaat u naar het menu Instellingen. Selecteer Toegangstokens en geef vervolgens een naam op voor uw token en stel een vervaldatum in. Selecteer vervolgens API en maak het token. Kopieer de resulterende waarde en sla deze op.

U moet over een geschikte lokale Git-opslagplaats beschikken die is geconfigureerd met toegang voor alle aangewezen gebruikers om een Git-integratie met Cloud Assembly in te stellen. U moet ook uw cloudsjablonen maken en opslaan in een specifieke structuur, zodat deze kunnen worden gedetecteerd door GitLab.

- Configureer en bewaar cloudsjablonen die met GitLab moeten worden geïntegreerd op de juiste manier. Alleen geldige sjablonen worden geïmporteerd in GitLab. Zie [Hoe gebruik ik Git-integratie in Cloud Assembly](#).

Procedure

- 1 Stel de integratie met uw GitLab-omgeving in Cloud Assembly in.
 - a Selecteer **Infrastructuur > Integraties > Nieuwe toevoegen** en kies GitLab.
 - b Voer de **URL** voor uw GitLab-instantie in. Voor een GitLab-instantie van Software as a Service is dit in de meeste gevallen gitlab.com.
 - c Voer het **token**, ook bekend als API-sleutel, in voor de opgegeven GitLab-instantie. Zie de bovenstaande vereisten voor informatie over het extraheren van het token van uw GitLab-instantie.

- d Voeg een passende naam en beschrijving toe.
 - e Klik op **Valideren** om de verbinding te controleren.
 - f Voeg desgewenst mogelijkheidstags toe. Zie [Capaciteitstags in Cloud Assembly gebruiken](#) voor meer informatie.
 - g Klik op **Toevoegen**.
- 2 Configureer de GitLab-verbinding om cloudsjablonen in een geschikte opslagplaats te accepteren.
- a Selecteer **Infrastructuur > Integraties** en kies de juiste GitLab-integratie.
 - b Selecteer **Projecten**.
 - c Selecteer **Nieuw project** en maak een naam voor het project.
 - d Voer het pad van de **opslagplaats** in GitLab in. Dit is doorgaans de gebruikersnaam van het hoofdaccount die is toegevoegd aan de naam van de opslagplaats.
 - e Voer de juiste GitLab-**vertakking** in die u wilt gebruiken.
 - f Voer een **Map**-naam in, indien van toepassing. Als dit veld leeg wordt gelaten, zijn alle mappen beschikbaar.
 - g Voer een geschikt **Type** in. Voer een mapnaam in, indien van toepassing. Als dit veld leeg wordt gelaten, zijn alle mappen beschikbaar.
 - h Klik op **Volgende** om het toevoegen van de opslagplaats te voltooien.

Wanneer u op **Volgende** klikt, wordt een geautomatiseerde synchronisatietask gestart die de cloudsjablonen in het platform importeert.

Wanneer de synchronisatietaken zijn voltooid, geeft een bericht aan dat de cloudsjablonen zijn geïmporteerd.

Resultaten

U kunt nu cloudsjablonen ophalen uit GitLab.

GitHub-integratie configureren in Cloud Assembly

U kunt de hostingservice van de cloudgebaseerde GitHub-opslagplaats integreren in Cloud Assembly.

U hebt een geldig GitHub-token nodig om GitHub-integratie in Cloud Assembly te configureren. Raadpleeg de GitHub-documentatie voor informatie over het maken en vinden van uw token.

Voorwaarden

- U moet toegang hebben tot GitHub.
- Configureer en bewaar cloudsjablonen die met GitHub moeten worden geïntegreerd op de juiste manier. Alleen geldige cloudsjablonen worden geïmporteerd in GitHub. Zie [Hoe gebruik ik Git-integratie in Cloud Assembly](#).

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Integraties** en klik op **Integratie toevoegen**.
- 2 Selecteer **GitHub**.
- 3 Voer de vereiste informatie in op de GitHub-configuratiepagina.
- 4 Klik op **Valideren** om de integratie te controleren.
- 5 Als u tags moet toevoegen om een tagstrategie te ondersteunen, voert u mogelijkheidstags in. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#) en [Een tagstrategie maken](#).
- 6 Klik op **Toevoegen**.
- 7 Configureer de GitHub-verbinding om cloudsjablonen in een geschikte opslagplaats te accepteren.
 - a Selecteer **Infrastructuur > Integraties** en kies de juiste GitHub-integratie.
 - b Selecteer **Projecten**.
 - c Selecteer **Nieuw project** en maak een naam voor het project.
 - d Voer het pad van de **Opslagplaats** in GitHub in. Dit is doorgaans de gebruikersnaam van het hoofdaccount die is toegevoegd aan de naam van de opslagplaats.
 - e Voer de juiste GitHub-**tak** in die u wilt gebruiken.
 - f Voer een **Map**-naam in, indien van toepassing. Als dit veld leeg wordt gelaten, zijn alle mappen beschikbaar.
 - g Voer een geschikt **Type** in.
 - h Klik op **Volgende** om het toevoegen van de opslagplaats te voltooien.

Er wordt een geautomatiseerde synchronisatietask geïnitieerd waarmee cloudsjablonen in het platform worden geïmporteerd.

Wanneer de synchronisatietaken zijn voltooid, geeft een bericht aan dat de cloudsjablonen zijn geïmporteerd.

Resultaten

GitHub kan worden gebruikt in Cloud Assembly-blueprints.

Wat nu te doen

U kunt nu cloudsjablonen ophalen uit GitHub.

Bitbucket-integratie configureren in Cloud Assembly

Cloud Assembly ondersteunt integratie met Bitbucket voor gebruik als een Git-gebaseerde opslagplaats voor ABX-actiescripts en VMware Cloud Templates.

In Cloud Assembly kunt u met twee typen opslagplaatsitems werken met behulp van Bitbucket-integratie: VMware Cloud Templates of ABX-actiescripts. U moet projecten synchroniseren waarmee u wilt werken voordat u een Bitbucket-integratie gebruikt. ABX-acties ondersteunen write-back naar de Bitbucket-opslagplaats, maar u kunt geen cloudsjablonen van de integratie wegschrijven. Als u nieuwe versies van cloudsjabloonbestanden wilt maken, moet u dit handmatig doen.

Voorwaarden

- Stel een Bitbucket-serverimplementatie op locatie in met een of meer op ABX of cloudsjablonen gebaseerde projecten die u wilt gebruiken met uw implementaties. Bitbucket-cloud wordt momenteel niet ondersteund.
- Maak of wijs een Cloud Assembly-project aan om uw Bitbucket-integratie te koppelen.
- Cloudsjabloonbestanden die moeten worden gesynchroniseerd met een Bitbucket-integratie, moeten de naam `blueprint.yaml` hebben.

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Integraties** en klik op **Integratie toevoegen**.
- 2 Selecteer Bitbucket.
- 3 Voer de samenvattingsinformatie en de Bitbucket-inloggegevens in op de pagina Samenvatting van de nieuwe Bitbucket-integratie.
- 4 Klik op **Valideren** om de integratie te controleren.
- 5 Als u labels moet toevoegen om een labelstrategie te ondersteunen, voert u capaciteitstags in. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#) en [Een tagstrategie maken](#).
- 6 Klik op **Toevoegen**.
- 7 Selecteer het tabblad Projecten op de hoofdpagina voor de Bitbucket-integratie om een project te koppelen aan deze Bitbucket-integratie.
- 8 Selecteer het Project dat u wilt koppelen aan deze Bitbucket-integratie.
- 9 Klik op **Volgende** om een Opslagplaats toe te voegen aan het Bitbucket-project en geef het type opslagplaats aan dat u toevoegt en geef vervolgens de **Opslagplaats**-naam en **Tak** op, evenals de **Map**.
- 10 Klik op **Toevoegen**.

Als u een of meer opslagplaatsen wilt toevoegen aan een project, klikt u op **Opslagplaats toevoegen**.

Resultaten

Bitbucket-integratie is geconfigureerd met de opgegeven opslagplaatsconfiguratie en u kunt ABX-acties en cloudsjablonen in geconfigureerde opslagplaatsen weergeven en bewerken. Wanneer u een project toevoegt aan een Bitbucket-integratie, wordt een synchronisatiebewerking uitgevoerd om de nieuwste versies van ABX-actiescripts en cloudsjabloonbestanden van de aangewezen opslagplaats te halen. Het tabblad Geschiedenis op de pagina Bitbucket-integratie toont de records van alle synchronisatiebewerkingen voor de integratie. Standaard worden bestanden automatisch elke 15 minuten gesynchroniseerd, maar u kunt een bestand handmatig synchroniseren door het te selecteren en op **Synchronisatie** te klikken.

Wat nu te doen

U kunt werken met ABX-acties op de pagina Cloud Assembly-uitbreidbaarheid en u kunt werken met cloudsjablonen op de ontwerppagina. Als u een gewijzigde versie van een ABX-actie opslaat op het gedeelte Uitbreidbaarheid van Cloud Assembly, wordt de nieuwe versie van het script gemaakt en naar de opslagplaats geschreven.

Een externe IPAM-integratie in vRealize Automation configureren

U kunt een providerspecifiek extern IPAM-integratiepunt maken om de IP-adressen te beheren die worden gebruikt in uw cloudsjabloonimplementaties. Wanneer u een extern IPAM-integratiepunt gebruikt worden IP-adressen verkregen van en beheerd door de aangewezen IPAM-provider in plaats van vRealize Automation.

U kunt een providerspecifiek IPAM-integratiepunt maken om IP-adressen en DNS-instellingen te beheren voor cloudsjabloonimplementaties en VM's in vRealize Automation.

Zie [Een extern IPAM-integratiepunt voor Infoblox toevoegen in vRealize Automation](#) voor informatie over het configureren van de vereisten en een voorbeeld van hoe u een provider-specifiek extern IPAM-integratiepunt maakt binnen de context van een voorbeeldwerkstroom. Houd er rekening mee dat deze werkstroom voor een Infoblox IPAM-integratie is, maar dat deze kan worden gebruikt als referentie voor elke externe IPAM-leverancier.

Zie [Hoe kan ik met de IPAM SDK een providerspecifiek extern IPAM-integratiepakket voor vRealize Automation maken](#) voor informatie over het maken van de benodigde activa om externe IPAM-partners en -leveranciers in staat te stellen hun IPAM-oplossing te integreren met vRealize Automation.

Voorwaarden

- Controleer of u over cloudbeheerdersreferenties beschikt. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Controleer of u de gebruikersrol van cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Controleer of u een account bij de externe IPAM-provider hebt, bijvoorbeeld [Infoblox](#) of [Bluecat](#), en of u de juiste toegangsgegevens hebt voor het account van uw organisatie bij de IPAM-provider.

- Controleer of u toegang hebt tot een geïmplementeerd integratiepakket voor de IPAM-provider, zoals Infoblox of BlueCat. Het geïmplementeerde pakket wordt in eerste instantie als ZIP-download verkregen van uw IPAM-provider of de [VMware Marketplace](#) en vervolgens geïmplementeerd in vRealize Automation.
- Controleer of u toegang hebt tot een geconfigureerde uitvoeringsomgeving voor de IPAM-provider.
- Als u gebruikmaakt van een op locatie geïntegreerde uitvoeringsomgeving met op acties gebaseerde uitbreidbaarheid (ABX), controleert u of u een HTTP-proxyserver in het vRealize Automation-netwerk hebt die uitgaand verkeer naar externe sites zoals gcr.io en storage.googleapis.com doorgeeft. Zie [Docker-images achter proxy verzenden in vRealize Automation 8.x \(75180\)](#) voor meer informatie.
- Controleer of u over de vereiste gebruikersreferenties beschikt om uw IPAM-leveranciersproduct te openen en te gebruiken. Raadpleeg de productdocumentatie van de integratieleverancier voor informatie over de vereiste gebruikersrechten.

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Integraties** en klik op **Integratie toevoegen**.
- 2 Klik op **IPAM**.
- 3 Selecteer een geconfigureerd IPAM-providerpakket in de vervolgkeuzelijst **Provider**.

Als de lijst leeg is, klikt u op **Providerpakket importeren**, navigeert u naar een bestaand ZIP-bestand met providerpakket en selecteert u het. Als u niet over het ZIP-bestand beschikt, kunt u het verkrijgen in de [VMware Marketplace](#).

- 4 Voer uw gebruikersnaam en wachtwoord in voor uw beheerdersaccount bij de externe IPAM-provider, samen met alle andere verplichte velden (indien aanwezig), zoals de hostnaam van uw provider.
- 5 Selecteer in de vervolgkeuzelijst **Uitvoeringsomgeving** een bestaande uitvoeringsomgeving, zoals integratiepunt op locatie voor actiegebaseerde uitbreidbaarheid.

De uitvoeringsomgeving ondersteunt communicatie tussen vRealize Automation en de IPAM-provider.

Het IPAM-framework ondersteunt alleen een ingesloten uitvoeringsomgeving op locatie voor actiegebaseerde uitbreidbaarheid (ABX).

Opmerking Als u een Amazon Web Services- of Microsoft Azure-cloudaccount gebruikt als uitvoeringsomgeving voor de integratie, moet u ervoor zorgen dat de appliance van de IPAM-provider toegankelijk is via internet en zich niet achter een NAT of firewall bevindt en dat deze een openbaar omzetbare DNS-naam heeft. Als de IPAM-provider niet toegankelijk is, kunnen de Amazon Web Services Lambda of Microsoft Azure Functions geen verbinding maken met de appliance en mislukt de integratie.

- 6 Klik op **Valideren**.

- 7 Wanneer u wordt gevraagd het zelfondertekende certificaat van de externe IPAM-provider te vertrouwen, klikt u op **Accepteren**.

Nadat u het zelfondertekende certificaat hebt geaccepteerd, kan de validatieactie verder worden voltooid.

- 8 Voer een naam in voor dit IPAM-integratiepunt en klik op **Toevoegen** om het nieuwe IPAM-integratiepunt op te slaan.

Er wordt een actie voor gegevensverzameling nagebootst. Netwerken en IP-adressen worden door gegevens verzameld van de externe IPAM-provider.

Upgraden naar een hoger extern IPAM-integratiepakket in vRealize Automation

U kunt een bestaand extern IPAM-integratiepunt upgraden naar een recentere versie van het leveranciersspecifieke IPAM-integratiepakket.

Een externe IPAM-provider of VMware kan een IPAM-bronintegratiepakket voor een bepaalde leverancier upgraden. Het externe IPAM-integratiepakket voor Infoblox is bijvoorbeeld verscheidene malen geüpgraded. Als u bestaande vRealize Automation-infrastructuurinstellingen wilt behouden die een benoemd IPAM-integratiepunt gebruiken, kunt u een IPAM-integratiepunt bewerken in de bron van het bijgewerkte IPAM-integratiepakket, in plaats van een nieuw IPAM-integratiepunt te maken.

Voorwaarden

Bij deze procedure wordt ervan uitgegaan dat u al een extern IPAM-integratiepunt hebt gemaakt en dat integratiepunt wilt upgraden om een recentere versie van het IPAM-integratiepakket van de leverancier te gebruiken.

Zie [Een extern IPAM-integratiepunt voor Infoblox toevoegen in vRealize Automation](#) voor informatie over het maken van een extern IPAM-integratiepunt.

- Controleer of u over cloudbeheerdersreferenties beschikt. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Controleer of u de gebruikersrol van cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Controleer of u een account hebt met de externe IPAM-provider en of u de juiste toegangsgegevens voor uw organisatieaccount hebt met die IPAM-provider.
- Controleer of u toegang hebt tot een geïmplementeerd integratiepakket voor uw IPAM-provider. Het geïmplementeerde pakket wordt in eerste instantie verkregen als ZIP-download van de website van uw IPAM-provider of via de [VMware Marketplace](#) en wordt vervolgens geïmplementeerd in vRealize Automation.

Zie [Een extern IPAM-providerpakket downloaden en implementeren voor gebruik in vRealize Automation](#) voor informatie over het downloaden en implementeren van het ZIP-bestand met het providerpakket en het beschikbaar maken ervan als **Provider**-waarde op de pagina IPAM-integratie.

- Controleer of u toegang hebt tot een geconfigureerde uitvoeringsomgeving voor de IPAM-provider. De uitvoeringsomgeving is doorgaans een ingesloten integratiepunt op locatie voor actiegebaseerde uitbreidbaarheid (ABX).

Zie [Een uitvoeringsomgeving voor een IPAM-integratiepunt maken in vRealize Automation](#) voor informatie over kenmerken van de uitvoeringsomgeving.

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Integraties IPAM** en open het bestaande IPAM-integratiepunt.
- 2 Klik op **Providers beheren**.
- 3 Navigeer naar het bijgewerkte IPAM-integratiepakket en importeer het.
- 4 Klik op **Valideren** en klik op **Opslaan**.

My VMware-integratie configureren in Cloud Assembly

U kunt My VMware integreren met Cloud Assembly om VMware-gerelateerde acties en mogelijkheden te ondersteunen die zijn gekoppeld aan downloadbare onderdelen waarvoor een account is vereist.

U kunt slechts één My VMware-integratie voor elke organisatie maken.

Voorwaarden

U moet over een gebruikersaccount met de juiste rechten beschikken voor My VMware.

- Zie [KB 2070555](#) voor informatie over het uitnodigen van een gebruiker voor een My VMware-account.
- Zie [KB 2006977](#) voor informatie over het toewijzen van gebruikersrechten in een My VMware-account.

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Integraties** en klik op **Integratie toevoegen**.
- 2 Selecteer My VMware.
- 3 Voer de vereiste informatie in op de My VMware-configuratiepagina.
- 4 Als u tags nodig hebt om een tagstrategie te ondersteunen, voert u capaciteitstags in. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#) en [Een tagstrategie maken](#).
- 5 Klik op **Toevoegen**.

Resultaten

My VMware is beschikbaar voor gebruik.

Wat nu te doen

Open zo nodig My VMware-onderdelen.

vRealize Orchestrator-integratie in Cloud Assembly configureren

U kunt een of meer vRealize Orchestrator-integraties configureren, zodat u werkstromen kunt gebruiken als onderdeel van uitbreidbaarheid en cloudsjablonen.

vRealize Automation bevat een vooraf geconfigureerde, ingesloten instantie van vRealize Orchestrator. U hebt toegang tot de client van de ingesloten vRealize Orchestrator vanuit de console van vRealize Automation Cloud Services.

Opmerking Om het beheercentrum van de ingesloten vRealize Orchestrator te openen, gaat u naar https://uw_vRA_FQDN/vco-controlcenter en u meldt u zich aan als **root**.

U kunt ook een externe vRealize Orchestrator-instantie integreren voor gebruik in uw vRealize Automation-uitbreidbaarheidsabonnementen en XaaS-bewerkingen (Anything as a Service) die worden gebruikt voor cloudsjablonen.

Voorwaarden

- Controleer of u over cloudbeheerdersreferenties beschikt. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Upgrade of migreer naar vRealize Orchestrator 8.3. Zie *VMware vRealize Orchestrator upgraden en migreren*.

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Integraties**.
- 2 Klik op **Integratie toevoegen**.
- 3 Selecteer **vRealize Orchestrator**.
- 4 Voer een naam in voor de vRealize Orchestrator-integratie.
- 5 (Optioneel) Voer een beschrijving in voor de vRealize Orchestrator-integratie.
- 6 Voer onder **vRealize Orchestrator URL** de volledig gekwalificeerde domeinnaam van uw externe vRealize Orchestrator-instantie in.
Bijvoorbeeld: https://my_vRO_FQDN.com:443.
- 7 Klik op **Valideren** om de integratie te valideren.
- 8 (Optioneel) Als u daarom wordt gevraagd, controleert u de certificaatgegevens en klikt u op **Accepteren**.

- 9 (Optioneel) Voeg mogelijkheidstags toe. Zie [Capaciteitstags in Cloud Assembly gebruiken](#) voor meer informatie over capaciteitstags.

Opmerking Capaciteitstags kunnen worden gebruikt om meerdere vRealize Orchestrator-integraties te beheren. Zie [Meerdere vRealize Orchestrator-integraties met projectbeperkingen beheren](#).

- 10 Klik op **Toevoegen**.

De vRealize Orchestrator-integratie wordt opgeslagen.

- 11 Selecteer **Uitbreidbaarheid > Bibliotheek > Werkstromen** om te controleren of de integratie is geconfigureerd en of de werkstromen zijn toegevoegd.

Wat nu te doen

Toegang krijgen tot de geïntegreerde externe vRealize Orchestrator-client:

- 1 Ga naar de vRealize Automation Cloud Services-console.
- 2 Selecteer **Orchestrator**.
- 3 Selecteer het bijbehorende tabblad van de geïntegreerde vRealize Orchestrator-instantie.

Opmerking Cloud Assembly-gebruikers zonder cloudbeheerdersreferenties kunnen het tabblad van de geïntegreerde vRealize Orchestrator-instantie niet zien.

vRealize Orchestrator-integraties uitschakelen of inschakelen

U kunt uw vRealize Orchestrator-integratie handmatig uitschakelen of inschakelen zodat u onderhoud kunt uitvoeren terwijl de integratie nog steeds actief is.

U kunt uw vRealize Orchestrator-integratie uitschakelen om onderhoud uit te voeren. Indien uitgeschakeld, heeft uw vRealize Orchestrator-integratie nog steeds de status **ACTIEF**, zodat u taken zoals resourcecontrole en gegevensverzameling nog steeds kunt uitvoeren.

Opmerking Naast het handmatig uitschakelen voert de vRealize Orchestrator Gateway-service periodieke gezondheidsstatuscontroles uit om te controleren of uw vRealize Orchestrator-integraties actief zijn of niet. Alle inactieve vRealize Orchestrator-integraties worden automatisch uitgeschakeld en worden ingesteld op de status **VERBINDING VERBROKEN**. U kunt geen taken zoals gegevensverzameling of resourcecontrole op niet-gekoppelde integraties uitvoeren.

Nadat een vRealize Orchestrator-integratie is uitgeschakeld of nadat de integratie is losgekoppeld door de gezondheidsstatuscontrole, worden de werkstromen alleen uitgevoerd op resterende integraties die zijn ingeschakeld. Als uw omgeving meerdere ingeschakelde vRealize Orchestrator-integraties bevat die niet worden beheerd via projectbeperkingen of capaciteitstags, wordt een willekeurige vRealize Orchestrator-integratie geselecteerd om uw werkstroom uit te voeren.

Opmerking Aangezien de vRealize Orchestrator-integratie willekeurig is geselecteerd, moet u ervoor zorgen dat informatie die vereist is om een bepaalde bewerking uit te voeren, beschikbaar is voor alle integraties. Voor inhoudsentiteiten zoals werkstromen betekent dit dat ze voor alle integraties moeten worden gesynchroniseerd. Er is voor inventarisobjecten geen garantie dat ze dezelfde object-id hebben voor alle integraties. Dus wanneer u een werkstroom probeert uit te voeren die een dergelijk inventarisobject bevat, kan een invoerparameter mislukken.

Zie [Meerdere vRealize Orchestrator-integraties met projectbeperkingen beheren](#) en [Meerdere vRealize Orchestrator-integraties beheren met capaciteitstags voor cloudaccounts](#) voor informatie over het beheren van meerdere vRealize Orchestrator-integraties met projectbeperkingen en capaciteitstags.

Voorwaarden

Configureer een of meer vRealize Orchestrator-integraties in Cloud Assembly. Zie [vRealize Orchestrator-integratie in Cloud Assembly configureren](#).

Procedure

- 1 Schakel uw vRealize Orchestrator-integratie uit.
 - a Navigeer naar **Infrastructuur > Verbindingen > Integraties**.
 - b Selecteer de vRealize Orchestrator-integratie die u wilt uitschakelen.
 - c Schakel **Eindpunt inschakelen** uit onder **Verificatiegegevens voor vRealize Orchestrator-server**.
 - d Klik op **Valideren**.
 - e Nadat de validatie is voltooid, klikt u op **Opslaan**.
- 2 Voer de nodige onderhoudstaken uit in de uitgeschakelde vRealize Orchestrator-integratie.
- 3 Schakel uw vRealize Orchestrator-integratie in.
 - a Navigeer naar **Infrastructuur > Verbindingen > Integraties**.
 - b Selecteer de eerder uitgeschakelde vRealize Orchestrator-integratie.
 - c Schakel de optie **Eindpunt inschakelen** in onder **Verificatiegegevens voor vRealize Orchestrator-server**.
 - d Klik op **Valideren**.
 - e Nadat de validatie is voltooid, klikt u op **Opslaan**.

Meerdere vRealize Orchestrator-integraties met projectbeperkingen beheren

U kunt projectbeperkingen gebruiken om te beheren welke vRealize Orchestrator-integraties worden gebruikt in werkstroomabonnementen.

Cloud Assembly ondersteunt de integratie van meerdere vRealize Orchestrator-servers die kunnen worden gebruikt in werkstroomabonnementen. U kunt bepalen welke vRealize Orchestrator-integraties worden gebruikt in cloudsjablonen die door uw project worden ingericht met zachte of harde projectbeperkingen. Zie [Cloud Assembly-projecttags en aangepaste eigenschappen gebruiken](#) voor meer informatie over projectbeperkingen.

Voorwaarden

- Controleer of u over cloudbeheerdersreferenties beschikt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Configureer twee of meer vRealize Orchestrator-integraties in Cloud Assembly. Zie [vRealize Orchestrator-integratie in Cloud Assembly configureren](#).
- Voeg capaciteitstags toe aan uw vRealize Orchestrator-integraties. Zie [Capaciteitstags in Cloud Assembly gebruiken](#).

Procedure

- 1 Navigeer naar **Infrastructuur > Beheer > Projecten** en selecteer uw project.
- 2 Selecteer het tabblad **Inrichting**.
- 3 Voer de capaciteitstags van uw vRealize Orchestrator-integraties in in het tekstvak **Uitbreidbaarheidsbeperkingen** en stel deze in als zachte of harde projectbeperkingen.
- 4 Klik op **Opslaan**.

Resultaten

Wanneer u een cloudsjabloon implementeert, gebruikt Cloud Assembly de projectbeperkingen om te bepalen welke vRealize Orchestrator-integraties worden gebruikt in werkstroomabonnementen.

Wat nu te doen

U kunt ook capaciteitstags gebruiken om meerdere vRealize Orchestrator-integraties te beheren op een niveau van het cloudaccount. Zie [Meerdere vRealize Orchestrator-integraties beheren met capaciteitstags voor cloudaccounts](#) voor meer informatie.

Meerdere vRealize Orchestrator-integraties beheren met capaciteitstags voor cloudaccounts

U kunt capaciteitstags gebruiken om te beheren welke vRealize Orchestrator-integraties worden gebruikt in werkstroomabonnementen.

Cloud Assembly ondersteunt de integratie van meerdere vRealize Orchestrator-servers die kunnen worden gebruikt in werkstroomabonnementen. U kunt beheren welke vRealize Orchestrator-integraties worden gebruikt in werkstroomabonnementen door capaciteitstags toe te voegen aan uw cloudaccount.

Voorwaarden

- Controleer of u over cloudbeheerdersreferenties beschikt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Configureer twee of meer vRealize Orchestrator-integraties in Cloud Assembly. Zie [vRealize Orchestrator-integratie in Cloud Assembly configureren](#) voor meer informatie.
- Voeg capaciteitstags toe aan uw vRealize Orchestrator-integraties. Zie [Capaciteitstags in Cloud Assembly gebruiken](#).

Procedure

- 1 Ga naar **Infrastructuur > Verbindingen > Cloudaccounts**.
- 2 Selecteer uw cloudaccount.
- 3 Voer de capaciteitstags in van de vRealize Orchestrator-integraties die u wilt gebruiken.

De capaciteitstags worden automatisch geconverteerd naar zachte beperkingen. Als u harde beperkingen wilt gebruiken bij het beheren van uw integraties, moet u projectbeperkingen gebruiken. Zie [Meerdere vRealize Orchestrator-integraties met projectbeperkingen beheren](#) voor meer informatie.
- 4 Klik op **Opslaan**.

Resultaten

Wanneer u een cloudsjabloon implementeert, gebruikt Cloud Assembly de labels in het gekoppelde cloudaccount om te beheren welke vRealize Orchestrator-integraties worden gebruikt in werkstroomabonnementen.

Gegevensverzameling voor vRealize Orchestrator-integraties

vRealize Automation voert periodiek een gegevensverzameling uit voor uw vRealize Orchestrator-integraties.

Gebeurtenissen voor gegevensverzameling voor vRealize Orchestrator-integraties worden elke 10 minuten geactiveerd. Bij de gegevensverzameling worden gegevens verzameld over de werkstromen in de bibliotheek van elke vRealize Orchestrator-integratie.

Belangrijk Zorg ervoor dat u de versie van een werkstroom verhoogt nadat u deze hebt bewerkt. Wijzigingen in werkstromen waarvan de versie niet is verhoogd, worden niet gedetecteerd door de gegevensverzamelaar.

U kunt informatie vinden over de laatste gegevensverzameling die is uitgevoerd op een vRealize Orchestrator-integratie door te navigeren naar **Infrastructuur > Verbindingen > Integraties** en de specifieke integratie te selecteren. U kunt ook een handmatige gegevensverzamelingsgebeurtenis activeren door op **Gegevensverzameling starten** te klikken.

Zie [Hoe werkt gegevensverzameling in vRealize Automation?](#) voor meer informatie over vRealize Automation-gegevensverzameling.

Hoe werk ik met Kubernetes in Cloud Assembly?

Cloud Assembly biedt verschillende opties voor het configureren, beheren en implementeren van virtuele Kubernetes-workloads.

Er zijn twee opties voor het werken met Tanzu Kubernetes-resources in Cloud Assembly. U kunt een vSphere with Tanzu Kubernetes-configuratie maken, waarvoor alleen een geschikt vCenter-cloudaccount en een clusterplan nodig zijn om toegang te krijgen tot de systeemeigen vSphere Tanzu Kubernetes-mogelijkheden. Met deze optie kunt u gebruikmaken van een vCenter-cloudaccount om toegang te krijgen tot supervisor-naamruimten om op Kubernetes gebaseerde workloads van vSphere te implementeren. U kunt ook externe Kubernetes-resources integreren in Cloud Assembly.

U kunt ook VMware Tanzu Kubernetes Grid Integrated Edition (TKGI), voorheen PKS, integreren. Voor dit type Kubernetes-implementatie is een PKS-integratie in Cloud Assembly vereist. Er is geen Cloud Assembly-clusterplan vereist.

Ten slotte kunt u ook een Red Hat OpenShift-integratie met Cloud Assembly maken om Kubernetes-resources te configureren, te beheren en te implementeren.

Werken met vSphere with Tanzu Kubernetes-clusters

vSphere 7.x bevat belangrijke verbeteringen waarmee u in het systeem met Kubernetes kunt werken om zowel virtuele machines als containers vanuit één interface te beheren. Met Cloud Assembly kunnen gebruikers gebruikmaken van de vSphere with Tanzu Kubernetes-mogelijkheden die zijn ingesloten in vSphere. U hebt toegang tot vSphere with Tanzu Kubernetes-functionaliteit via een vCenter-cloudaccount met een vSphere-implementatie die supervisorclusters bevat. Met deze implementatie kunt u zowel conventionele virtuele machines als Kubernetes-clusters van vCenter beheren.

Voor Tanzu Kubernetes-supervisor-naamruimten moeten gebruikers toegang hebben tot een toepasselijke vSphere SSO, zodat ze zich kunnen aanmelden bij een opgegeven link naar de naamruimtedetails van de supervisor. Vervolgens kunnen ze een aangepaste Kubectl met vSphere-verificatie downloaden zodat ze hun supervisor-naamruimte kunnen gebruiken.

Als u deze functionaliteit wilt gebruiken, moet u een vCenter met vSphere-cloudaccount hebben waarvoor supervisor-naamruimten zijn geconfigureerd. Nadat een gebruiker zich heeft aangemeld, kan de gebruiker aan de slag gaan met de betreffende naamruimten.

Werken met VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) of OpenShift-integraties

Voor TKGI, externe clusters of OpenShift-configuraties biedt Cloud Assembly toegang tot een Kubeconfig waarmee gebruikers toegang kunnen krijgen tot toepasselijke Kubernetes-clusters.

Nadat u een TKGI- of OpenShift-integratie hebt gemaakt, worden toepasselijke Kubernetes-clusters beschikbaar in Cloud Assembly en kunt u Kubernetes-onderdelen maken en toevoegen aan Cloud Assembly om het beheer van cluster- en containerapplicaties te ondersteunen. Deze applicaties vormen de basis van selfservice-implementaties die beschikbaar zijn in de Service Broker-catalogus.

- [VMware Tanzu Kubernetes Grid Integrated Edition-integratie configureren in Cloud Assembly](#)

U kunt een VMware Tanzu Kubernetes Grid Integrated Edition-resourceverbinding (TKGI), voorheen PKS, op locatie en in de cloud configureren om de mogelijkheden voor Kubernetes-integratie en -beheer in Cloud Assembly te ondersteunen.

- [Een vSphere with Tanzu Kubernetes-implementatie inrichten in vRealize Automation](#)

Met vRealize Automation kunt u een vSphere with Tanzu Kubernetes-implementatie van Cloud Assembly inrichten om gebruik te maken van de systeemeigen vSphere 7.x-mogelijkheden om Tanzu Kubernetes-clusters te implementeren en te beheren, zodat een infrastructuuronafhankelijke laag wordt geboden voor de inrichting en het beheer van virtuele infrastructuur.

- [De Red Hat OpenShift-integratie configureren in Cloud Assembly](#)

U kunt een Red Hat OpenShift-resourceverbinding op locatie in de cloud configureren om Kubernetes-integratie en beheermogelijkheden op bedrijfsniveau in Cloud Assembly te ondersteunen.

- [Een Kubernetes-zone in Cloud Assembly configureren](#)

Kubernetes-zones stellen cloudbeheerders in staat om op beleid gebaseerde plaatsing van Kubernetes-clusters en -naamruimten en supervisornaamruimten te definiëren die worden gebruikt in Cloud Assembly-implementaties. Een beheerder kan deze pagina gebruiken om op te geven welke clusters beschikbaar zijn voor het inrichten van Kubernetes-naamruimten en welke eigenschappen acceptabel zijn voor clusters.

- [Een clusterplan in vRealize Automation Cloud Assembly maken voor gebruik met een vSphere with Tanzu Kubernetes-implementatie](#)

U moet een clusterplan maken voor gebruik met vSphere with Tanzu Kubernetes-implementaties in vRealize Automation. Een clusterplan werkt als configuratiesjabloon voor het inrichten van Tanzu Kubernetes-clusterinstanties op een bepaalde vSphere-cloudaccountinstantie.

- [Tanzu-supervisorclusters en -naamruimten in Cloud Assembly gebruiken](#)

Beheerders kunnen supervisornaamruimten op een voor Tanzu ingeschakelde vSphere-integratie beschikbaar maken voor gebruikers, zodat ze deze naamruimten via cloudsjablonen kunnen toevoegen aan Kubernetes-implementaties of ze kunnen aanvragen via de Service Broker-catalogus.

- [Werken met Kubernetes-clusters en -naamruimten in Cloud Assembly](#)

Cloudbeheerders kunnen de configuratie van geïmplementeerde Kubernetes-clusters en -naamruimten, zowel generiek als Pacific-gebaseerd, toevoegen, weergeven en beheren in Cloud Assembly.

- [Kubernetes-onderdelen toevoegen aan cloudsjablonen in Cloud Assembly](#)

Wanneer u Kubernetes-onderdelen toevoegt aan een Cloud Assembly-cloudsjabloon, kunt u ervoor kiezen om clusters toe te voegen of gebruikers in staat te stellen om naamruimten in verschillende configuraties te maken. Deze keuze is doorgaans afhankelijk van uw vereisten voor toegangscontrole, hoe u uw Kubernetes-onderdelen hebt geconfigureerd en uw implementatievereisten.

- [Cloud Assembly-uitbreidbaarheid met Kubernetes gebruiken](#)

Cloud Assembly biedt een set gebeurtenisonderwerpen die overeenkomen met de gebruikelijke acties die zijn gerelateerd aan de implementatie van de Kubernetes-cluster en -naamruimte. Gebruikers kunnen zich desgewenst abonneren op deze onderwerpen en ze worden op het juiste moment uitgevoerd. Gebruikers ontvangen een melding wanneer een gebeurtenis voor het geabonneerde onderwerp plaatsvindt. U kunt ook vRO-werkstromen configureren om te worden uitgevoerd op basis van gebeurtenismeldingen.

VMware Tanzu Kubernetes Grid Integrated Edition-integratie configureren in Cloud Assembly

U kunt een VMware Tanzu Kubernetes Grid Integrated Edition-resourceverbinding (TKGi), voorheen PKS, op locatie en in de cloud configureren om de mogelijkheden voor Kubernetes-integratie en -beheer in Cloud Assembly te ondersteunen.

Met TKGI-integraties kunt u TKGI-instanties op locatie en in de cloud beheren, en Kubernetes-clusters die zijn ingericht op TKGI- en externe clusters. U moet een Kubernetes-profiel maken en dit koppelen aan een project ter ondersteuning van de plaatsing van resources op basis van beleid.

Voorwaarden

- U moet een geschikte geconfigureerde TKGI-server hebben ingesteld met UAA-verificatie.
- Controleer of u over cloudbeheerdersreferenties beschikt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#) voor meer informatie.

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Integraties** en klik op **Integratie toevoegen**.
- 2 Selecteer VMware Tanzu Kubernetes Grid Integrated Edition.
- 3 Voer het IP-adres of de FQDN en het TKGI-adres in voor het TKGI-cloudaccount dat u maakt.
 - Het IP-adres is de FQDN of het IP-adres van de TKGI-gebruikersverificatieserver.
 - Het TKGI-adres is de FQDN of het IP-adres voor de primaire TKGI-server.

- 4 Selecteer of deze TKGI-server lokaal is of zich in de openbare cloud of in een privécloud bevindt.
- 5 Voer een **gebruikersnaam** en **wachtwoord** voor de TKGI-server en andere gerelateerde informatie in.
- 6 Als u tags nodig hebt om een tagstrategie te ondersteunen, voert u capaciteitstags in. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#) en [Een tagstrategie maken](#).
- 7 Klik op **Toevoegen**.

Resultaten

U kunt Kubernetes-zones maken en deze toewijzen aan een project, of u kunt externe Kubernetes-clusters detecteren en deze clusters toewijzen aan projecten. Daarnaast kunt u Kubernetes-naamruimten toevoegen of maken die het beheer van clusters tussen grote groepen en organisaties mogelijk maken.

Wat nu te doen

Maak of selecteer de betreffende Kubernetes-zones, selecteer vervolgens een of meer clusters of naamruimten en wijs deze toe aan een project. Daarna kunt u cloudsjablonen maken en publiceren om gebruikers de mogelijkheid te geven om selfservice-implementaties te genereren die gebruikmaken van Kubernetes.

Een vSphere with Tanzu Kubernetes-implementatie inrichten in vRealize Automation

Met vRealize Automation kunt u een vSphere with Tanzu Kubernetes-implementatie van Cloud Assembly inrichten om gebruik te maken van de systeemeigen vSphere 7.x-mogelijkheden om Tanzu Kubernetes-clusters te implementeren en te beheren, zodat een infrastructuuronafhankelijke laag wordt geboden voor de inrichting en het beheer van virtuele infrastructuur.

De Tanzu with vSphere Kubernetes-functionaliteit maakt gebruik van de systeemeigen Kubernetes-mogelijkheid van vSphere 7.x. Er is geen vRealize Automation PKS-integratie nodig om te functioneren.

Voorwaarden

- Als u een vSphere with Tanzu Kubernetes-implementatie wilt inrichten met Cloud Assembly, moet u toegang hebben tot vSphere 7.x. In vRealize Automation is vSphere beschikbaar als onderdeel van een vCenter-cloudaccount voor Cloud Assembly. Zie [Een vCenter-cloudaccount maken in vRealize Automation](#).
- Tanzu moet zijn ingeschakeld in het vSphere-cloudaccount en moet de juiste supervisornaamruimten bevatten.

- U moet een geschikt clusterplan hebben voor gebruik met de integratie. Zie [Een clusterplan in vRealize Automation Cloud Assembly maken voor gebruik met een vSphere with Tanzu Kubernetes-implementatie](#).

Procedure

- 1 Als er nog geen geschikt vCenter-cloudaccount bestaat in Cloud Assembly, maakt u er een.
Zie [Een vCenter-cloudaccount maken in vRealize Automation](#).
- 2 Selecteer **Infrastructuur > Configureren > Kubernetes-zone** om een Kubernetes-zone in vRealize Automation Cloud Assembly te maken of te selecteren.

U kunt een bestaande Kubernetes-zone gebruiken als u een geschikte zone hebt geconfigureerd, maar een beheerder moet een of meer supervisornaamruimten aan de zone toevoegen. Deze naamruimten fungeren als computerbronnen waarop ingerichte Tanzu Kubernetes-clusters worden gemaakt in de zone. Zie [Een Kubernetes-zone in Cloud Assembly configureren](#) voor meer informatie over Kubernetes-zones.
- 3 Ga naar het tabblad Kubernetes-inrichting op de pagina **Infrastructuur > Beheer > Projecten** in Cloud Assembly en koppel de Kubernetes-zone aan het geschikte project.
- 4 Maak of selecteer een clusterplan voor een geschikt vSphere 7.x-cloudaccount.

Zie [Een clusterplan in vRealize Automation Cloud Assembly maken voor gebruik met een vSphere with Tanzu Kubernetes-implementatie](#) voor meer informatie.
- 5 Selecteer **Ontwerp > Cloudsjablonen** en maak een cloudsjabloon voor een project dat toegang heeft tot een geschikte Kubernetes-zone. Sleep vervolgens een K8s-clusteronderdeel in het cloudsjabloonschema en geef de naam en het clusterplan op.

U kunt ook het aantal werkerknooppunten opgeven.
- 6 Voer de cloudsjabloon uit en zoek vervolgens, wanneer deze is voltooid, het adres van het ingerichte Tanzu-cluster in de resource-eigenschappen op de pagina Implementaties van Cloud Assembly.
- 7 Vind en verken het Tanzu-cluster op de pagina **Infrastructuur > Configureren > Kubernetes** van Cloud Assembly.

Resultaten

Het Tanzu Kubernetes-cluster wordt ingericht zoals is opgegeven in de cloudsjabloon.

Wat nu te doen

Nadat u het Tanzu-cluster hebt geïmplementeerd, hebt u verschillende opties om hiermee te werken.

- Ga naar de pagina **Resources > Implementaties** in Cloud Assembly en zoek en download het gerelateerde Kubeconfig-bestand om toegang te krijgen tot het ingerichte Tanzu-cluster. U kunt het Kubeconfig-bestand gebruiken om het geïmplementeerde Tanzu Kubernetes-cluster te beheren zoals elk ander conform Kubernetes-cluster.

- U kunt het Tanzu-cluster vinden en verkennen op de pagina **Infrastructuur > Resources > Kubernetes** van Cloud Assembly.
- Als u een nieuwe naamruimte wilt maken, gaat u naar het tabblad Naamruimten op de pagina **Infrastructuur > Resources > Kubernetes** van Cloud Assembly en klikt u op **Nieuwe naamruimte** om een naamruimte te maken in het toepasselijke Tanzu-cluster. U kunt controleren of de naamruimte is gemaakt door te controleren of deze wordt weergegeven op het tabblad Naamruimten op de Kubernetes-pagina.

De Red Hat OpenShift-integratie configureren in Cloud Assembly

U kunt een Red Hat OpenShift-resourceverbinding op locatie in de cloud configureren om Kubernetes-integratie en beheermogelijkheden op bedrijfsniveau in Cloud Assembly te ondersteunen.

Cloud Assembly ondersteunt integratie met OpenShift-versies 3.x.

Voorwaarden

- U moet een juist geconfigureerde Red Hat OpenShift-implementatie hebben.
- Controleer of u over cloudbeheerdersreferenties beschikt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#) voor meer informatie.
- VMware biedt resources die u kunt gebruiken om een OpenShift-cluster te maken met een cloudsjabloon op de volgende locatie: <https://flings.vmware.com/enterprise-openshift-as-a-service-on-cloud-automation-services>. U kunt clusters die zijn gemaakt met deze resources gebruiken als globale clusters in de Kubernetes-zones om selfservicenaamruimten te maken.

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Integraties** en klik op **Integratie toevoegen**.
- 2 Selecteer Red Hat OpenShift.
- 3 Voer het **adres** en de **locatie** in voor de OpenShift-server.
- 4 Selecteer het juiste **type verificatiegegevens** en voer de juiste verificatiegegevens in.
OpenShift-integratie ondersteunt de verificatie met OAuth-gebruikersnaam/-wachtwoord, openbare sleutel of Bearer-token.
- 5 Voer een geschikte **naam** en **beschrijving** in voor de OpenShift-integratie.
- 6 Als u tags nodig hebt om een tagstrategie te ondersteunen, voert u de geschikte capaciteitstags in. Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#) en [Een tagstrategie maken](#).
- 7 Klik op **Toevoegen**.

Resultaten

Wanneer een integratie wordt gemaakt, worden nieuwe Kubernetes-clusters weergegeven in de relevante sectie van de Kubernetes-pagina. U kunt Kubernetes-zones maken en deze aan een project toewijzen. Daarnaast kunt u Kubernetes-naamruimten configureren die het beheer van clusters tussen grote groepen en organisaties mogelijk maken.

Wat nu te doen

Maak of selecteer de betreffende Kubernetes-zones, selecteer vervolgens een of meer clusters of naamruimten en wijs deze toe aan een project. Daarna kunt u cloudsjablonen maken en publiceren om gebruikers de mogelijkheid te geven om selfservice-implementaties te genereren die gebruikmaken van Kubernetes.

Een Kubernetes-zone in Cloud Assembly configureren

Kubernetes-zones stellen cloudbeheerders in staat om op beleid gebaseerde plaatsing van Kubernetes-clusters en -naamruimten en supervisornaamruimten te definiëren die worden gebruikt in Cloud Assembly-implementaties. Een beheerder kan deze pagina gebruiken om op te geven welke clusters beschikbaar zijn voor het inrichten van Kubernetes-naamruimten en welke eigenschappen acceptabel zijn voor clusters.

Cloudbeheerders kunnen Kubernetes-zones koppelen aan TKGI-cloudaccounts die zijn geconfigureerd voor Cloud Assembly of met externe Kubernetes-clusters die niet zijn gekoppeld aan een project.

Wanneer u een Kubernetes-zone maakt, kunt u meerdere providerspecifieke resources aan de zone toewijzen en deze resources bepalen welke eigenschappen kunnen worden ingesteld voor de nieuw ingerichte clusters in termen van het aantal werkers, masters, beschikbare CPU, geheugen en andere configuratie-instellingen. Voor TKGI-providers komen deze overeen met TKGI-plannen. Een beheerder kan ook meerdere clusters toewijzen aan een Kubernetes-zone die wordt gebruikt voor het plaatsen van nieuw ingerichte Kubernetes-naamruimten. De beheerder kan alleen clusters toewijzen waarvoor geen onboarding is voltooid, of die niet worden beheerd door CMX, en die worden ingericht via de vooraf geselecteerde clusterprovider. De beheerder kan meerdere Kubernetes-zones toewijzen aan één project, zodat ze allemaal beschikbaar zijn voor plaatsingsbewerkingen die in dit project plaatsvinden.

Een cloudbeheerder kan prioriteiten toewijzen op meerdere niveaus.

- Kubernetes-zoneprioriteit in een project.
- Resourceprioriteit binnen een Kubernetes-zone.
- Clusterprioriteit binnen een Kubernetes-zone.

De cloudbeheerder kan ook tags toewijzen op meerdere niveaus:

- Capaciteitstags per Kubernetes-zone.
- Tags per resourcetoewijzing.
- Labels per clustertoewijzing.

U kunt Kubernetes-zones maken met supervisornaamruimten op vSphere op dezelfde manier als u met generieke Kubernetes-naamruimten werkt. Om een supervisornaamruimte toe te voegen aan een Kubernetes-zone moet u de zone koppelen aan een eindpunt van vSphere 7 dat de gewenste resources van de Pacific-naamruimte bevat.

Service Broker bevat een versie van de pagina Kubernetes-zone waarmee Service Broker-beheerders toegang krijgen tot bestaande Kubernetes-zones zodat ze plaatsingsbeleidsregels kunnen maken voor Kubernetes-naamruimten en -clusters die vanuit de catalogus worden ingericht.

Voorwaarden

Configureer integratie met een geschikte VMware Tanzu Kubernetes Grid Integrated Edition-implementatie (TKGI). Zie [VMware Tanzu Kubernetes Grid Integrated Edition-integratie configureren in Cloud Assembly](#).

Procedure

- 1 Selecteer **Infrastructuur > Configureren > Kubernetes-zones** en klik op **Nieuwe Kubernetes-zone**.
- 2 Voer de naam in van het **account** voor TKGI-integratie waarop u deze zone wilt toepassen.
Hiermee wordt het cloudaccount of -eindpunt gedefinieerd dat aan de zone is gekoppeld. U kunt slechts één eindpunt aan elke zone toewijzen. Als u met de naamruimte van de supervisor op vSphere werkt, kunt u hier alleen vSphere-instanties selecteren die supervisornaamruimten bevatten.
- 3 Voeg een **naam** en **beschrijving** voor de Kubernetes-zone toe.
- 4 Voeg desgewenst capaciteitstags toe. Zie [Capaciteitstags in Cloud Assembly gebruiken](#) voor meer informatie.
- 5 Klik op **Opslaan**.
- 6 Klik op het tabblad **Op aanvraag** en voeg indien nodig TKGI-plannen toe voor de zone die u wilt gebruiken voor het inrichten van een cluster.
U kunt een of meer plannen selecteren en prioriteiten toewijzen. Lagere nummers hebben een hogere prioriteit. Prioriteitstoewijzingen zijn secundair voor op tags gebaseerde selectie.
- 7 Klik op het tabblad **Cluster** en klik vervolgens op de knop **Berekening toevoegen** om Kubernetes- of supervisorclusters aan de zone toe te voegen. Als u met een extern cluster werkt, wordt de onboarding voor Cloud Assembly automatisch voltooid wanneer u dit selecteert.
U kunt Kubernetes-naamruimten toevoegen aan het cluster op de pagina Kubernetes-clusters in Cloud Assembly.

Resultaten

Kubernetes-zones worden geconfigureerd voor gebruik met Cloud Assembly-implementaties.

Wat nu te doen

Wijs de Kubernetes-zone toe aan een project.

- 1 Selecteer **Infrastructuur > Beheer > Projecten** en selecteer vervolgens het project dat u wilt koppelen aan uw Kubernetes-zone.
- 2 Klik op het tabblad Kubernetes-inrichting op de pagina Project.
- 3 Klik op **Kubernetes-zone toevoegen** en voeg de zone toe die u zojuist hebt gemaakt. U kunt meerdere zones selecteren indien nodig en u stelt ook de prioriteit in voor de zones.
- 4 Klik op **Opslaan**.

Op het tabblad Kubernetes-inrichting van de pagina Project in Cloud Assembly kunt u limieten instellen voor het type en het aantal naamruimten dat gebruikers kunnen inrichten in een Kubernetes-zone. U kunt ook het type naamruimten selecteren dat in een zone kan worden ingericht: reguliere naamruimten of supervisornaamruimten. De tabel Kubernetes-zones op het tabblad Kubernetes-inrichting bevat kolommen met de huidige limietinstellingen. Als u limieten wilt instellen, klikt u op de betreffende zone in de tabel om een dialoogvenster te openen waarmee u limieten voor naamruimten en supervisornaamruimten kunt kiezen.

Klik in de kolom Ondersteunt in de tabel Kubernetes-zones om te selecteren welk type naamruimte kan worden ingericht voor de zone.

Nadat u een Kubernetes-zone aan een project hebt toegewezen, kunt u de pagina Cloudsjablonen op het tabblad Ontwerp in Cloud Assembly gebruiken om een implementatie in te richten op basis van de Kubernetes-zone en de projectconfiguratie. Deze pagina Cloudsjablonen bevat opties om een K8S-cluster, K8S-naamruimte en supervisornaamruimte toe te voegen. Selecteer de juiste optie voor de Kubernetes-resource waarmee u werkt.

Een clusterplan in vRealize Automation Cloud Assembly maken voor gebruik met een vSphere with Tanzu Kubernetes-implementatie

U moet een clusterplan maken voor gebruik met vSphere with Tanzu Kubernetes-implementaties in vRealize Automation. Een clusterplan werkt als configuratiesjabloon voor het inrichten van Tanzu Kubernetes-clusterinstanties op een bepaalde vSphere-cloudaccountinstantie.

In een clusterplan wordt een configuratietoewijzing gedefinieerd, vergelijkbaar met een soorttoewijzing, voor een set vSphere-cloudaccountinstanties. Over het algemeen codeert het clusterplan een betekenisvolle set configuratie-eigenschappen, zoals VM-klassen, opslagklassen, enz. die worden gebruikt bij het inrichten van Tanzu Kubernetes-clusters in een bepaald vSphere-servercloudaccount.

Eén clusterplan kan een bepaalde configuratie-eigenschapstoewijzing in één vSphere-cloudaccount en een andere configuratietoewijzing in een andere vSphere-instantie hebben. Als u bijvoorbeeld twee in aanmerking komende vSphere-cloudaccounts hebt, één met hoge resource en een andere met beperkte resources, kan het `large-clusterplan guaranteed-xlarge` specificeren voor de vSphere-server met een hoog profiel en `best-effort-medium` voor de beperkte vSphere-instantie. In het algemeen wijst de `large`-specificatie een andere configuratie-eigenschapset toe aan elke in aanmerking komende vSphere-serverinstantie.

Nadat een clusterplan is gemaakt voor een of meer vSphere-instanties, moeten alle in aanmerking komende supervisor-naamruimten die een beheerder toewijst om een Tanzu Kubernetes-cluster te hosten met behulp van een Kubernetes-zonetoewijzing worden afgestemd op de configuratie die is gedefinieerd in de specificatie van het clusterplan. Het opslagbeleid dat in het clusterplan is opgegeven, moet bijvoorbeeld als opslagklasse worden toegevoegd aan alle vSphere-supervisor-naamruimten die zijn toegewezen voor het inrichten van Tanzu-clusters.

Voorwaarden

- Als u een vSphere with Tanzu Kubernetes-implementatie in Cloud Assembly wilt maken, moet u toegang hebben tot vSphere 7.x die beschikbaar is als onderdeel van een vCenter-cloudaccount. Zie [Een vCenter-cloudaccount maken in vRealize Automation](#).
- Tanzu moet worden ingeschakeld in het vSphere-cloudaccount met een of meer supervisor-naamruimten.
- Alle supervisorclusters in het geregistreerde vSphere-cloudaccount die in aanmerking komen voor inrichting van Tanzu-clusters moeten worden toegevoegd als beheerde entiteiten op de pagina Cloud Assembly **Infrastructuur > Kubernetes > Supervisorclusters** via de optie **Supervisorcluster toevoegen**.

Procedure

- 1 Selecteer **Infrastructuur > Configureren > Clusterplan** en klik op **Nieuw clusterplan**.
- 2 Voer een **Account**, **Naam** en **Beschrijving** in voor het clusterplan. Het account definieert het cloudaccount waarop dit clusterplan van toepassing is.
- 3 Voer clusterinformatie in, waaronder **Kubernetes-versies** en **Control plane**. Deze informatie omvat toewijzingen voor knooppunten, machineklasse en opslagklasse.
 - Voer de versie van Kubernetes in die van toepassing is op dit clusterplan. Dit is de Kubernetes-versie van de ingerichte Tanzu Kubernetes-clusters: bijvoorbeeld 1.19 of 1.20.
 - Het aantal control planes definieert de specificatie voor Kubernetes API-serverknooppunten.
 - Een VM-klasse is een aanvraag voor reserveringen op de virtuele machine voor verwerkingskracht. Er zijn talloze vooraf gedefinieerde machineklassen, die verschillende niveaus van berekeningskracht hebben. Zie [VM-klassen voor Tanzu Kubernetes-clusters](#) voor meer informatie.
 - Werkers geven de Tanzu Kubernetes-werkerknooppunten op die met dit plan moeten worden geïmplementeerd.
- 4 Voer Aanvullende instellingen voor het clusterplan in en selecteer deze.
 - Voer de **Standaard PVC-opslagklasse** in om met dit cluster te gebruiken.
 - Gebruik de keuzerondjes om het gedrag aan te geven bij het gebruik van opslagklassen en netwerkinstellingen.
- 5 Klik op **Maken**.

Resultaten

Het clusterplan wordt gemaakt en is beschikbaar voor gebruik in Cloud Assembly-cloudsjablonen.

Wat nu te doen

Nadat u een clusterplan hebt gemaakt, kunt u dit gebruiken om een vSphere with Tanzu Kubernetes-implementatie in Cloud Assembly te maken. Zie [Een vSphere with Tanzu Kubernetes-implementatie inrichten in vRealize Automation](#).

Tanzu-supervisorclusters en -naamruimten in Cloud Assembly gebruiken

Beheerders kunnen supervisornaamruimten op een voor Tanzu ingeschakelde vSphere-integratie beschikbaar maken voor gebruikers, zodat ze deze naamruimten via cloudsjablonen kunnen toevoegen aan Kubernetes-implementaties of ze kunnen aanvragen via de Service Broker-catalogus.

In deze taak wordt beschreven hoe u Tanzu-supervisorclusters met Cloud Assembly toevoegt voor gebruik in implementaties en hoe u naamruimten maakt of toevoegt die bepalen welke Cloud Assembly-projecten en -gebruikers toegang hebben tot bepaalde Kubernetes-resources. Deze functionaliteit is gebaseerd op een geschikt vSphere-cloudaccount in plaats van een integratie zoals VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) of Openshift. Supervisorclusters zijn aangepaste Kubernetes-clusters die aan vSphere zijn gekoppeld. Ze tonen Kubernetes-API's aan eindgebruikers en gebruiken ESXi als platform voor werkerknooppunten in plaats van Linux. Supervisornaamruimten maken toegang tot Kubernetes-resources mogelijk, omdat het doorgaans eenvoudiger is om beleid toe te passen op naamruimten dan op afzonderlijke virtuele machines. U kunt meerdere naamruimten maken voor elk supervisorcluster.

Voor Tanzu ingeschakelde implementaties kunnen ook met vSphere gegenereerde gastclusters gebruiken. Een gastcluster is een Kubernetes-cluster dat binnen virtual machines in het supervisorcluster wordt uitgevoerd. Een gastcluster is een Kubernetes die volledig conform is met de upstream, dus u weet zeker dat het met alle Kubernetes-applicaties werkt. Gastclusters in vSphere gebruiken het opensourcecluster-API-project om Kubernetes-clusters te beheren dat de VM-operator gebruikt voor het beheer van de virtuele machines die deel uitmaken van een gast.

Wanneer Kubernetes-zones worden gebruikt met vSphere-instanties met Tanzu ingeschakeld, bepalen de Kubernetes-zones welke supervisorclusters beschikbaar zijn voor inrichting van een supervisornaamruimte. Supervisornaamruimten zijn specifiek voor voor Tanzu ingeschakelde vSphere-instanties. Het is niet mogelijk om een generieke Kubernetes-resource in te richten op voor Tanzu ingeschakelde vSphere-instanties.

Cloud Assembly-gebruikers die zijn aangewezen als projectkijkers, hebben alleen-weergavetoegang tot naamruimten, terwijl projectleden deze kunnen bewerken.

Indien gewenst kunt u de supervisorclusters die aan naamruimten zijn gekoppeld configureren.

Voorwaarden

- Als u supervisorclusters en -naamruimten met Cloud Assembly wilt gebruiken, moet u een vSphere 7.x-eindpunt hebben geconfigureerd. In vRealize Automation wordt vSphere geïnstalleerd als onderdeel van een vCenter-cloudaccount. Zie [Een vCenter-cloudaccount maken in vRealize Automation](#).
- Tanzu moet zijn ingeschakeld in het vSphere-cloudaccount en moet de juiste supervisornaamruimten bevatten.
- Zowel uw vCenter- als uw vRealize Automation-implementatie moeten dezelfde Active Directory gebruiken om gebruikers te synchroniseren. Hoewel provisioning nog steeds werkt als dit niet het geval is, krijgen vRealize Automation-gebruikers geen automatische toegang tot de naamruimte.

Procedure

- 1 Selecteer **Infrastructuur > Configureren > Kubernetes-zone** in Cloud Assembly.
Op deze pagina worden beheerde clusters weergegeven die beschikbaar zijn voor gebruik, en kunt u extra clusters toevoegen. U kunt op een van de clusters klikken om de clusterdetails weer te geven.
- 2 Selecteer **Nieuwe Kubernetes-zone**.
- 3 Geef de **accountgegevens** op voor het vSphere-doelcloudaccount.
- 4 Klik op het pictogram Zoeken in het tekstvak om alle vSphere-accounts weer te geven of zoek naar een account op naam.
- 5 Typ een **Naam** en **Beschrijving** voor de nieuwe zone.
- 6 Voeg desgewenst capaciteitstags toe. Zie [Capaciteitstags in Cloud Assembly gebruiken](#) voor meer informatie.
- 7 Klik op het tabblad Provisioning om het supervisorcluster te selecteren dat aan de naamruimten wordt gekoppeld.
- 8 Klik op **Berekening toevoegen** om de beschikbare supervisorclusters te bekijken en te selecteren.
- 9 Klik op **Toevoegen**.
- 10 Selecteer **Infrastructuur > Beheer > Projecten** en selecteer vervolgens het project dat u wilt koppelen aan uw Kubernetes-zone.
- 11 Klik op het tabblad Kubernetes-inrichting op de pagina Project.
- 12 Klik op **Kubernetes-zone toevoegen** en voeg de zone toe die u zojuist hebt gemaakt. U kunt meerdere zones selecteren indien nodig en u stelt ook de prioriteit in voor de zones.
- 13 Klik op **Opslaan**.

Wat nu te doen

Nadat u een naamruimte hebt geconfigureerd, wordt de naamruimte weergegeven op de pagina **Infrastructuur > Resources > Kubernetes** in Cloud Assembly. Gebruikers kunnen op de adreslink klikken op het tabblad Samenvatting om de vSphere Kubernetes CLI-tools te openen en de naamruimte te beheren. Gebruikers moeten een cloudbeheerder of een lid van de naamruimte voor het aangewezen project zijn om toegang te krijgen tot een link naar de naamruimtegegevens van de supervisor. Gebruikers kunnen ook een aangepaste Kubectl downloaden om de naamruimte van de supervisor te gebruiken. Gebruikers kunnen zich aanmelden bij de naamruimte van de supervisor en deze als elke andere naamruimte gebruiken, en vervolgens cloudsjablonen maken en applicaties implementeren.

Om de naamruimte aan een cloudsjabloon toe te voegen, selecteert u **Ontwerp > Cloudsjabloon** en selecteert u een bestaande cloudsjabloon of maakt u een nieuwe. Vervolgens kunt u het item supervisornaamruimte in het linkermenu selecteren en naar het canvas slepen.

U kunt opslagbeleidsregels aan een supervisornaamruimte toewijzen met tags. U kunt tags, zoals `location:local`, toevoegen om de Kubernetes-zone op te geven die u wilt gebruiken met de implementatie, evenals andere tags in uw opslagprofielen zoals `speed:fast` en `speed:slow`.

```
formatVersion: 1
resources:
  Cloud_SV_Namespace_1:
    type: Cloud.SV.Namespace
    properties:
      name: 'a'
      storage:
        -profile:
          constraints:
            - tag: 'speed:fast'
        -profile:
          limitMB:1000
          constraints:
            -tag: 'speed:slow'
```

Deze cloudsjabloon vraagt een supervisornaamruimte zonder beperkingen aan en geeft hiermee twee opslagprofielen op.

Nadat u cloudsjablonen met een supervisornaamruimte hebt geïmplementeerd, kunnen gebruikers ook supervisornaamruimten aanvragen bij de Service Broker-catalogus. U kunt ook klikken op de pagina Implementaties in Cloud Assembly om informatie over de implementatie te bekijken en toegang te krijgen tot een link die het commando bevat om de kubectl voor de naamruimte op vSphere uit te voeren.

U kunt VM-klassen voor supervisornaamruimten in een cloudsjabloon opgeven met de eigenschap `vmclasses`, zodat u een klassenaam kunt opgeven. Zie het volgende voorbeeld van een cloudsjabloon.

```
resources:
  Cloud_SV_Namespace_1:
    type: Cloud.SV.Namespace
    properties:
      name: demo-vmclass1
      vmclasses:
        - name: vmclass1
```

Werken met Kubernetes-clusters en -naamruimten in Cloud Assembly

Cloudbeheerders kunnen de configuratie van geïmplementeerde Kubernetes-clusters en -naamruimten, zowel generiek als Pacific-gebaseerd, toevoegen, weergeven en beheren in Cloud Assembly.

Gebruikers met cloudbeheerdersrechten kunnen Kubernetes-clusters en -naamruimten weergeven, toevoegen en beheren waarvoor u toegangsrechten hebt op de pagina **Infrastructuur > Resources > Kubernetes**. Deze pagina bevat tabbladen voor clusters, naamruimten, supervisorclusters en supervisornaamruimten. U kunt een van deze tabbladen selecteren om de overeenkomstige resources weer te geven en te beheren. Deze pagina vereenvoudigt het beheer van geïmplementeerde clusters en naamruimten.

- **Cluster:** een cluster is een groep Kubernetes-knooppunten die worden verdeeld over een of meer fysieke machines. Op deze pagina worden ingerichte en niet-geïmplementeerde clusters weergegeven die zijn geconfigureerd voor gebruik op uw Cloud Assembly-instantie. U kunt op een cluster klikken om informatie over de huidige status weer te geven. Wanneer u een cluster implementeert, bevat dit een link naar een Kubconfig-bestand dat alleen toegankelijk is voor cloudbeheerders. Dit bestand verleent volledige beheerdersrechten voor het cluster, inclusief een lijst met naamruimten.

Supervisorclusters zijn uniek voor vSphere-instanties en gebruiken ESXI als werkerknooppunten in plaats van Linux.

- **Naamruimten:** naamruimten zijn virtuele clusters die beheerders de mogelijkheid bieden om clusterresources te groeperen of te scheiden. Ze vereenvoudigen het beheer van resources in grote groepen gebruikers en organisaties. Een cloudbeheerder kan, in de vorm van op rollen gebaseerde toegangscontrole, gebruikers toestaan om naamruimten toe te voegen aan een project wanneer ze een implementatie aanvragen en deze naamruimten later beheren vanaf de pagina Kubernetes-clusters. Wanneer u een naamruimte implementeert, bevat deze een link naar een kubeconfig-bestand waarmee geldige gebruikers, zoals ontwikkelaars, bepaalde aspecten van die naamruimte kunnen bekijken en beheren.

Supervisorclusters en supervisornaamruimten bestaan alleen in vSphere-instanties en bieden Kubernetes-achtige toegang tot vSphere-objecten.

Een cloudbeheerder kan het project wijzigen dat is gekoppeld aan een Kubernetes-naamruimte of -cluster op deze pagina, zodat de beheerder Kubernetes-resources vanuit cloudsjablonen en Service Broker kan inrichten en deze vervolgens voor gebruik kan toewijzen aan specifieke projecten. De beheerder kan het bereik van een cluster wijzigen om het algemeen of projectspecifiek te maken. Algemene clusters worden weergegeven op het tabblad Clusters voor alle Kubernetes-zones en zijn beschikbaar voor selectie en inrichting. Als een cluster algemeen is, kan dit worden toegevoegd aan een Kubernetes-zone en vervolgens worden gebruikt om naamruimten vanuit de catalogus in te richten.

Als u een nieuw of bestaand cluster configureert, moet u selecteren of u verbinding wilt maken met een primair IP-adres of een primaire hostnaam.

Werken met generieke Kubernetes-clusters in Cloud Assembly

U kunt nieuwe, bestaande of externe clusters toevoegen aan Cloud Assembly met behulp van de opties op deze pagina.

- 1 Selecteer **Infrastructuur > Resources > Kubernetes** en bevestig dat het tabblad Clusters actief is.

Als er momenteel clusters zijn geconfigureerd voor uw Cloud Assembly-instantie, worden deze op deze pagina weergegeven.

- 2 Als u een nieuw of bestaand cluster toevoegt of een cluster implementeert, selecteert u de juiste optie volgens de volgende tabel.

Optie	Beschrijving	Details
Implementeren	Nieuwe clusters aan Cloud Assembly toevoegen	U moet het TKGI-cloudaccount opgeven waarop dit cluster wordt geïmplementeerd, evenals het gewenste plan en het aantal knooppunten.
Bestaande toevoegen	Configureer een bestaand cluster om met uw project te werken.	U moet het TKGI-cloudaccount opgeven, het cluster dat moet worden gebruikt en het geschikte project voor de doelontwikkelaar. U moet ook het bereik voor delen opgeven. Als u globaal wilt delen, moet u uw Kubernetes-zones en -naamruimten op de juiste manier configureren.
Externe toevoegen	Voeg een Vanilla Kubernetes-cluster, dat mogelijk niet aan TKGI is gekoppeld, toe aan Cloud Assembly.	U moet een project aanwijzen waaraan het cluster is gekoppeld, het IP-adres voor het gewenste cluster invoeren en een clouproxy en certificaatinformatie selecteren die nodig zijn om verbinding te maken met dit cluster.

- 3 Klik op **Toevoegen** om het cluster beschikbaar te stellen in Cloud Assembly.

Werken met Kubernetes-naamruimten in Cloud Assembly

Als u een cloudbeheerder bent, helpen naamruimten u bij het groeperen en beheren van Kubernetes-clusterresources. Als u een gebruiker bent, zijn naamruimten het gebied in Kubernetes-clusters voor uw implementaties. Beheerders en gebruikers hebben toegang tot naamruimten via het tabblad Naamruimten op de pagina **Infrastructuur > Resources > Kubernetes**.

Er zijn verschillende manieren om Kubernetes-naamruimten toe te voegen aan resources in Cloud Assembly. De volgende procedure beschrijft een typische methode.

- 1 Selecteer **Infrastructuur > Resources > Kubernetes** en klik op het tabblad Naamruimten.
- 2 Klik op **Nieuwe naamruimte** om een nieuwe naamruimte toe te voegen. Klik op **Naamruimte toevoegen** om een bestaande naamruimte toe te voegen.
- 3 Voer een **naam** en **beschrijving** in voor de naamruimte.
Op dit moment hebt u een naamruimte toegevoegd voor gebruik met Kubernetes-resources, maar deze is niet gekoppeld aan iets in het bijzonder.
- 4 Geef het **cluster** op dat u wilt koppelen aan deze naamruimte.
- 5 Klik op **Maken** om de naamruimte toe te voegen aan Cloud Assembly.

U kunt aangepaste eigenschappen op Kubernetes-naamruimten toevoegen om uitbreidbaarheid op verschillende manieren te ondersteunen. U voegt aangepaste eigenschappen toe wanneer u een naamruimte inricht door een Cloud Assembly-cloudsjabloon te maken. Wanneer u een Kubernetes-naamruimte in een cloudsjabloon opgeeft, kunt u eigenschappen aan de naamruimte toevoegen. Klik eerst met de rechtermuisknop op de eigenschappen in de sjabloon om toegang te krijgen tot de standaardeigenschappen die deel uitmaken van het schema van de cloudsjabloon. Als tweede optie kunt u door de gebruiker gedefinieerde eigenschappen toevoegen in het gedeelte met eigenschappen van de naamruimte in de cloudsjabloon.

Na de implementatie worden deze aangepaste eigenschappen weergegeven op de pagina Implementaties in Cloud Assembly voor de toepasselijke implementatie.

Ten slotte kunt u ook aangepaste eigenschappen aan een naamruimte toevoegen met acties die zijn geconfigureerd op de pagina **Uitbreidbaarheid > Acties** in Cloud Assembly.

Werken met supervisorclusters en -naamruimten

Cloudbeheerders kunnen de configuratie van de supervisorclusters en -naamruimten bekijken en wijzigen op de pagina Kubernetes in Cloud Assembly.

- 1 Selecteer **Infrastructuur > Resources > Kubernetes** in Cloud Assembly.
- 2 Selecteer **Supervisorcluster toevoegen**.
- 3 Geef de accountgegevens op voor het vSphere-doelcloudaccount.
- 4 Klik op het zoekpictogram in het tekstvak Supervisorcluster om alle supervisorclusters weer te geven of om naar een cluster te zoeken op naam.
- 5 Selecteer het gewenste cluster en klik op **Toevoegen**.

- 6 Selecteer het tabblad Supervisornaamruimten en klik op de knop **Nieuwe supervisornaamruimte** om een nieuwe naamruimte toe te voegen.
- 7 Selecteer het tabblad Supervisornaamruimten en klik op de knop **Nieuwe supervisornaamruimte** om een nieuwe naamruimte toe te voegen.
 - a Als u een nieuwe naamruimte maakt, voegt u een **naam** en **beschrijving** toe.
 - b Selecteer het juiste **cloudaccount** dat u aan de naamruimte wilt koppelen.
 - c Selecteer het **supervisorcluster** om aan deze naamruimte te koppelen.
 - d Selecteer het **project** dat u aan de naamruimte wilt koppelen.
 - e Gebruik de selectie **Beschikbare opslagbeleidsregels** om opslagbeleidsregels toe te voegen voor gebruik met de naamruimte.

U kunt alle beschikbare opslagbeleidsregels toevoegen of specifieke beleidsregels selecteren voor gebruik met de supervisornaamruimte. U kunt desgewenst ook een limiet instellen voor de beschikbare opslag grootte bij elk beschikbaar opslagbeleid.

- f Klik op **Maken**.
- 8 Controleer de relevante details voor de nieuwe naamruimte. U kunt de configuratie van het opslagbeleid indien nodig wijzigen.

Gebruikers en groepen die momenteel toegang hebben tot de naamruimte in vSphere, worden weergegeven op het tabblad Gebruikers. Als nieuwe gebruikers of groepen worden toegevoegd aan het project, klikt u op de knop **Gebruikers bijwerken** op dit tabblad om de lijst bij te werken. De lijst wordt niet automatisch bijgewerkt, dus u moet de knop gebruiken om deze bij te werken.

Opmerking Synchronisatie van gebruikers is alleen zinvol als Cloud Assembly en vCenter zijn geconfigureerd met een algemene Active Directory/LDAP-service.

Nadat een cluster of naamruimte is geconfigureerd, worden op de pagina **Infrastructuur > Resources > Kubernetes** in Cloud Assembly de clusters en naamruimten weergegeven die beschikbaar zijn voor de gebruiker. U kunt op een afzonderlijke naamruimte of afzonderlijk cluster klikken om een pagina te openen die een aantal tabbladen bevat waarop statistieken en andere informatie voor de resource worden weergegeven, en waarop u verschillende opties kunt configureren.

Met het tabblad Samenvatting voor clusters op de Kubernetes-pagina kunnen beheerders de configuratie van een cluster bekijken en in sommige gevallen bijwerken, inclusief het wijzigen van het bereik. Met de keuzerondjes Delen kunt u Algemeen (te delen via Kubernetes-zone) of Project (toegang beperkt tot één project) selecteren. Als u Project selecteert, moet u ook het betreffende project in de onderstaande projectselectie opgeven.

Opmerking Het wijzigen van de configuratie voor delen kan invloed hebben op de naamruimten die beschikbaar zijn in het cluster.

Gebruikers kunnen op de adreslink klikken op het tabblad Samenvatting om de vSphere Kubernetes CLI-tools te openen en de naamruimte te beheren. Gebruikers moeten een cloudbeheerder of een lid van de naamruimte voor het aangewezen project zijn om toegang te krijgen tot een link naar de naamruimtegegevens van de supervisor. Gebruikers kunnen ook een aangepaste Kubectl downloaden om de naamruimte van de supervisor te gebruiken. Gebruikers kunnen zich aanmelden bij de naamruimte van de supervisor en deze als elke andere naamruimte gebruiken, en vervolgens cloudsjablonen maken en applicaties implementeren.

Kubernetes-onderdelen toevoegen aan cloudsjablonen in Cloud Assembly

Wanneer u Kubernetes-onderdelen toevoegt aan een Cloud Assembly-cloudsjabloon, kunt u ervoor kiezen om clusters toe te voegen of gebruikers in staat te stellen om naamruimten in verschillende configuraties te maken. Deze keuze is doorgaans afhankelijk van uw vereisten voor toegangscontrole, hoe u uw Kubernetes-onderdelen hebt geconfigureerd en uw implementatievereisten.

Om een Kubernetes-onderdeel toe te voegen aan een cloudsjabloon in Cloud Assembly, selecteert u **Ontwerp > Cloudsjablonen**, klikt u op **Nieuw** en zoekt u de optie Kubernetes in het linkermenu en vouwt u deze uit. Vervolgens selecteert u de gewenste optie, ofwel Cluster of KBS-naamruimte, door deze naar het canvas te slepen.

Het aan een cloudsjabloon toevoegen van een Kubernetes-cluster dat aan een project is gekoppeld, is de eenvoudigste methode om Kubernetes-resources beschikbaar te maken voor geldige gebruikers. U kunt tags in clusters gebruiken om te bepalen waar deze worden geïmplementeerd, net zoals u met andere Cloud Assembly-resources werkt. U kunt tags gebruiken om een zone en een VMware Tanzu Kubernetes Grid Integrated Edition-plan (TKGI) te selecteren tijdens de toewijzingsfase van de clusterimplementatie.

Nadat u een cluster op deze manier hebt toegevoegd, is het automatisch beschikbaar voor alle geldige gebruikers.

Voorbeelden van cloudsjablonen

In het eerste cloudsjabloonvoorbeeld ziet u een sjabloon voor een eenvoudige Kubernetes-implementatie die wordt beheerd door tagging. Een Kubernetes-zone is gemaakt met twee implementatieplannen die zijn geconfigureerd op de pagina Nieuwe Kubernetes-zone. In dit geval is een tag met de naam `placement:tag` toegevoegd als mogelijkheid voor de zone en deze is gebruikt om overeen te komen met de analoge beperking in de cloudsjabloon. Als er meer dan één zone is geconfigureerd met de tag, wordt de zone met het laagste prioriteitsnummer geselecteerd.

```
formatVersion: 1
inputs: {}
resources:
  Cluster_provisioned_from_tag:
    type: Cloud.K8S.Cluster
    properties:
      hostname: 109.129.209.125
      constraints:
```



```
-tag: 'placement tag'
port: 7003
workers: 1
connectBy: hostname
```

In het tweede cloudsjabloonvoorbeeld ziet u hoe u een sjabloon instelt met een variabele met de naam `$(input.hostname)` zodat gebruikers de gewenste clusterhostnaam kunnen invoeren bij het aanvragen van een implementatie. Tags kunnen ook worden gebruikt om een zone en een TKGI-plan te selecteren tijdens de resourcetoewijzingsfase van de clusterimplementatie.

```
formatVersion: 1
inputs:
  hostname:
    type: string
    title: Cluster hostname
resources:
  Cloud_K8S_Cluster_1:
    type: Cloud.K8S.Cluster
    properties:
      hostname: ${input.hostname}
      port: 8443
      connectBy: hostname
      workers: 1
```

Als u naamruimten wilt gebruiken om het clustergebruik te beheren, kunt u een variabele instellen in de cloudsjabloon met de naam `name: ${input.name}` om de naam van de naamruimte te vervangen die een gebruiker invoert wanneer een implementatie wordt aangevraagd. Voor dit soort implementatie maakt u een sjabloon zoals in het volgende voorbeeld:

```
1 formatVersion: 1
2 inputs:
3   name:
4     type: string
5     title: "Namespace name"
6 resources:
7   Cloud_K8S_Namespace_1:
8     type: Cloud.K8S.Namespace
9     properties:
10      name: ${input.name}
```

Gebruikers kunnen geïmplementeerde clusters beheren via kubeconfig-bestanden die toegankelijk zijn via de pagina **Infrastructuur > Resources > Kubernetes-clusters**. Zoek de kaart op de pagina voor het gewenste cluster en klik op **Kubeconfig**.

Supervisornaamruimten in VMware Cloud Templates

Het volgende is het schema voor een algemene supervisor-naamruimte in een Cloud Assembly-cloudsjabloon.

```
{
  "title": "Supervisor namespace schema",
  "description": "Request schema for provisioning of Supervisor namespace resource",
```

```

"type": "object",
"properties": {
  "name": {
    "title": "Name",
    "description": "Alphabetic (a-z and 0-9) string with maximum length of 63 characters.
The character '-' is allowed anywhere except the first or last position of the identifier.",
    "type": "string",
    "pattern": "^.*\\$\\{.*\\}.*$|^((?!-)[a-z0-9-]{1,63}(?!-))$",
    "ignoreOnUpdate": true
  },
  "description": {
    "title": "Description",
    "description": "An optional description of this Supervisor namespace.",
    "type": "string",
    "ignoreOnUpdate": true
  },
  "content": {
    "title": "Content",
    "description": "Kubernetes Yaml Content",
    "type": "string",
    "maxLength": 65000
  },
  "constraints": {
    "title": "Constraints",
    "description": "To target the correct resources, blueprint constraints are matched
against infrastructure capability tags. Constraints must include the key name. Options
include value, negative [!], and hard or soft requirement.",
    "type": "array",
    "recreateOnUpdate": true,
    "items": {
      "type": "object",
      "properties": {
        "tag": {
          "title": "Tag",
          "description": "Constraint definition in syntax `[!]tag_key[:tag_value]
[:hard|:soft]` \nExamples:\n```\n!location:eu:hard\n location:us:soft\n!pci\n```,
          "type": "string",
          "recreateOnUpdate": true
        }
      }
    }
  },
  "limits": {
    "title": "Limits",
    "description": "Defines namespace resource limits such as pods, services, etc.",
    "type": "object",
    "properties": {
      "stateful_set_count": {
        "title": "stateful_set_count",
        "description": "This represents the new value for 'statefulSetCount' option which
is the maximum number of StatefulSets in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
      },
      "deployment_count": {

```

```

        "title": "deployment_count",
        "description": "This represents the new value for 'deploymentCount' option which is
the maximum number of deployments in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "cpu_limit_default": {
        "title": "cpu_limit_default",
        "description": "This represents the new value for the default CPU limit (in Mhz)
for containers in the pod. If specified, this limit should be at least 10 MHz.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "config_map_count": {
        "title": "config_map_count",
        "description": "This represents the new value for 'configMapCount' option which is
the maximum number of ConfigMaps in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "pod_count": {
        "title": "pod_count",
        "description": "This represents the new value for 'podCount' option which is the
maximum number of pods in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "job_count": {
        "title": "job_count",
        "description": "This represents the new value for 'jobCount' option which is the
maximum number of jobs in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "secret_count": {
        "title": "secret_count",
        "description": "This represents the new value for 'secretCount' option which is the
maximum number of secrets in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "cpu_limit": {
        "title": "cpu_limit",
        "description": "This represents the new value for 'limits.cpu' option which is
equivalent to the maximum CPU limit (in MHz) across all pods in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "cpu_request_default": {
        "title": "cpu_request_default",
        "description": "This represents the new value for the default CPU request (in Mhz)
for containers in the pod. If specified, this field should be at least 10 MHz.",
        "type": "integer",
        "recreateOnUpdate": false
    },

```

```

    "memory_limit_default": {
      "title": "memory_limit_default",
      "description": "This represents the new value for the default memory limit (in
mebibytes) for containers in the pod.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "memory_limit": {
      "title": "memory_limit",
      "description": "This represents the new value for 'limits.memory' option which is
equivalent to the maximum memory limit (in mebibytes) across all pods in the namespace.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "memory_request_default": {
      "title": "memory_request_default",
      "description": "This represents the new value for the default memory request (in
mebibytes) for containers in the pod.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "service_count": {
      "title": "service_count",
      "description": "This represents the new value for 'serviceCount' option which is
the maximum number of services in the namespace.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "replica_set_count": {
      "title": "replica_set_count",
      "description": "This represents the new value for 'replicaSetCount' option which is
the maximum number of ReplicaSets in the namespace.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "replication_controller_count": {
      "title": "replication_controller_count",
      "description": "This represents the new value for 'replicationControllerCount'
option which is the maximum number of ReplicationControllers in the namespace.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "storage_request_limit": {
      "title": "storage_request_limit",
      "description": "This represents the new value for 'requests.storage' which is the
limit on storage requests (in mebibytes) across all persistent volume claims from pods in the
namespace.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "persistent_volume_claim_count": {
      "title": "persistent_volume_claim_count",
      "description": "This represents the new value for 'persistentVolumeClaimCount'
option which is the maximum number of PersistentVolumeClaims in the namespace.",
      "type": "integer",

```

```

        "recreateOnUpdate": false
    },
    "daemon_set_count": {
        "title": "daemon_set_count",
        "description": "This represents the new value for 'daemonSetCount' option which is
the maximum number of DaemonSets in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    }
},
"additionalProperties": false
},
"vm_classes": {
    "title": "VM classes",
    "description": "Defines set of Virtual Machine classes to be assigned to the namespace",
    "type": "array",
    "recreateOnUpdate": false,
    "items": {
        "type": "object",
        "properties": {
            "name": {
                "title": "Name",
                "description": "Name of the Virtual Machine class.",
                "type": "string",
                "recreateOnUpdate": false
            }
        }
    }
},
"storage": {
    "title": "Storage policies",
    "description": "Defines set of storage profiles to be used to assign storage policies
to the namespace.",
    "type": "array",
    "recreateOnUpdate": false,
    "items": {
        "type": "object",
        "properties": {
            "profile": {
                "type": "object",
                "title": "Storage profile",
                "description": "Defines storage policies to be assigned to the namespace",
                "recreateOnUpdate": false,
                "properties": {
                    "constraints": {
                        "title": "Constraints",
                        "description": "To target the correct storage profiles, blueprint constraints
are matched against storage profile capability tags.",
                        "type": "array",
                        "recreateOnUpdate": false,
                        "items": {
                            "type": "object",
                            "properties": {
                                "tag": {
                                    "title": "Tag",

```

```

        "description": "Constraint definition in syntax `[!]tag_key[:tag_value]`  

        [:hard|:soft]` \nExamples:\n```\nlocation:eu:hard\n location:us:soft\n```,  

        "type": "string",  

        "recreateOnUpdate": false  

    }  

    },  

    "minItems":1  

},  

"limitMb": {  

    "title": "Limit",  

    "description": "The maximum amount of storage (in mebibytes) which can be  

utilized by the namespace for this storage policy. Optional. If unset, no limits are placed.",  

    "type": "integer"  

}  

},  

"required": [  

    "constraints"  

]  

}  

}  

}  

},  

"required": [  

    "name"  

]  

}  

}

```

VMware Cloud Templates ondersteunen het gebruik van limieten met supervisornaamruimten. Met limieten kunt u het gebruik van resources voor CPU's en geheugen beheren, evenals het maximum aantal pods dat is toegestaan in de naamruimte door geïmplementeerde machines.

```

formatVersion: 1
inputs: {}
resources:
  Cloud_SV_Namespace_1:
    type: Cloud.SV.Namespace
    properties:
      name: '${env.deploymentName}'
      limits:
        - cpu_limit: 1000
          cpu_request_default: 800
          memory_limit: 2000
          memory_limit_default: 1500
          pod_count: 200

```

In het volgende voorbeeld ziet u hoe u een opslagbeleid kunt opgeven met tags.

```

formatVersion: 1
inputs: {}
resources:
  Cloud_SV_Namespace_1:
    type: Cloud.SV.Namespace

```

```

properties:
  name: 'ns-with-storage-policy'
  description: 'sample'
  storage:
    - profile:
        limitMb: 1000
        constraints:
          - tag: 'storage:fast'
    - profile:
        constraints:
          - tag: 'storage:cheap'

```

Willekeurige YAML's gebruiken met selfservicenaamruimte of cluster-VCT's

Tijdens het maken van een cluster of naamruimte willen gebruikers vaak aanvullende aanpassingen uitvoeren. U kunt bijvoorbeeld gebruikers (rol/rolbinding) toevoegen, een podbeveiligingsbeleid maken of agents installeren. Met de YAML-eigenschap `content` kunnen gebruikers aangepaste pakketten definiëren die ze op die cluster/naamruimte/supervisornaamruimte willen inrichten.

Elk YAML-inhoudspakket dat is gekoppeld aan de eigenschap `content`, moet worden gescheiden met een drievoudig streepje (`---`). Ook de inhoudsinformatie moet een tekenreeks van meerdere regels zijn. Raadpleeg het volgende YAML-voorbeeld om te zien hoe inhoudspakketten kunnen worden geconfigureerd.

```

formatVersion: 1
inputs: {}
resources:
  Cloud_Tanzu_Cluster_1:
    type: Cloud.Tanzu.Cluster
    properties:
      name: ddonchev-tkc
      plan: small
      content: |-
        apiVersion: rbac.authorization.k8s.io/v1
        kind: ClusterRoleBinding
        metadata:
          name: psp:authenticated-from-yaml
        subjects:
          - apiGroup: rbac.authorization.k8s.io
            kind: Group
            name: system:authenticated
        roleRef:
          apiGroup: rbac.authorization.k8s.io
          kind: ClusterRole
          name: psp:vmware-system-privileged
        ---
        apiVersion: apiextensions.k8s.io/v1
        kind: CustomResourceDefinition
        metadata:
          # name must match the spec fields below, and be in the form: <plural>.<group>
          name: crontabs.stable.example.com

```

```

spec:
  # group name to use for REST API: /apis/<group>/<version>
  group: stable.example.com
  # list of versions supported by this CustomResourceDefinition
  versions:
    - name: v1
      # Each version can be enabled/disabled by Served flag.
      served: true
      # One and only one version must be marked as the storage version.
      storage: true
      schema:
        openAPIV3Schema:
          type: object
          properties:
            spec:
              type: object
              properties:
                cronSpec:
                  type: string
                image:
                  type: string
                replicas:
                  type: integer
  # either Namespaced or Cluster
  scope: Namespaced
  names:
    # plural name to be used in the URL: /apis/<group>/<version>/<plural>
    plural: crontabs
    # singular name to be used as an alias on the CLI and for display
    singular: crontab
    # kind is normally the CamelCased singular type. Your resource manifests use this.
    kind: CronTab
    # shortNames allow shorter string to match your resource on the CLI
    shortNames:
      - ct

```

De YAML die is gedefinieerd in de inhoudseigenschap wordt ook weergegeven op het tabblad Eigenschappen voor de implementatie.

Cloud Assembly kan alleen inhoudsresources maken binnen het bereik van de resource die wordt geïmplementeerd. Bijvoorbeeld: als u een Kubernetes-naamruimte inricht, kan Cloud Assembly geen implementatie binnen een andere naamruimte maken. Gebruikers hebben dezelfde rechten alsof ze de kubeconfig met kubectl gebruikten.

Nadat de virtuele machine is ingericht, begint een installatie van de Kubernetes-objecten in de eigenschap `content`. Als een van de resources waarnaar in de YAML-inhoudseigenschap wordt verwezen niet kan worden ingericht, wordt Cloud Assembly teruggedraaid en worden alle eerdere Kubernetes-objecten van de resource verwijderd en heeft de implementatie de status Mislukt. De resource is nog steeds ingericht en zichtbaar. Bovendien kunt u nog steeds acties voor dag 2 gebruiken, waaronder een poging om de inhoud opnieuw toe te passen.

U kunt de eigenschap `content` verbeteren met invoer van de cloudsjabloon, zoals in het volgende voorbeeld wordt weergegeven.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_SV_Namespace_1:
    type: Cloud.SV.Namespace
    properties:
      name: sv-namespace-with-vm-classes
      vm_classes:
        - name: best-effort-2xlarge
        - name: best-effort-4xlarge
        - name: best-effort-8xlarge
```

Daarnaast kunt u aangepaste resources zoals `TanzuKubernetesCluster` inrichten. Dit zal mislukken als een bewerking voor dag 1, omdat de supervisornaamruimte niet de vereiste VM-klassen en opslagklassen bevat. Wanneer de VM-klassen en opslagklassen aan de supervisornaamruimte zijn gebonden, kunt u `TanzuKubernetesCluster` (of een andere resource) maken met de actie voor dag 2.

Opmerking: u kunt een resource zonder inhoud inrichten en u kunt nog steeds Kubernetes-objecten als YAML toevoegen met de actie voor dag 2.

De inhoud die wordt weergegeven in de YAML-eigenschap definieert wat wordt ingericht op de resource. Wanneer u deze inhoud bewerkt, ziet u in de volgende tabel de mogelijke resultaten:

Actie	Resultaat
Als u een Kubernetes-object toevoegt en verzendt.	Het opgegeven object wordt op de resource gemaakt.
Als u een Kubernetes-object verwijdert en verzendt.	Het opgegeven object wordt van de resource verwijderd.
Als u een Kubernetes-object wijzigt en verzendt.	Er wordt een patch voor het opgegeven object op de resource toegepast.

Het is belangrijk om duidelijk te maken welke acties als wijziging in het huidige object worden beschouwd. Bijvoorbeeld: als u het naamruimteveld van een object wijzigt, wordt een nieuw object gemaakt, en wordt geen patch toegepast op het oude object.

De uniekheid van een resource wordt gedefinieerd door de volgende velden: `apiVersion`, `kind`, `metadata.name`, `metadata.namespace`

Cloud Assembly-uitbreidbaarheid met Kubernetes gebruiken

Cloud Assembly biedt een set gebeurtenisonderwerpen die overeenkomen met de gebruikelijke acties die zijn gerelateerd aan de implementatie van de Kubernetes-cluster en -naamruimte. Gebruikers kunnen zich desgewenst abonneren op deze onderwerpen en ze worden op het juiste moment uitgevoerd. Gebruikers ontvangen een melding wanneer een gebeurtenis voor het geabonneerde onderwerp plaatsvindt. U kunt ook vRO-werkstromen configureren om te worden uitgevoerd op basis van gebeurtenismeldingen.

De volgende onderwerpen zijn beschikbaar als abonnement op de pagina **Uitbreidbaarheid** > **Bibliotheek** > **Gebeurtenisonderwerpen** in Cloud Assembly. Als u deze onderwerpen wilt weergeven, zoekt u naar Kubernetes in het zoekvak Gebeurtenisonderwerpen.

- Kubernetes-clustertoewijzing
- Kubernetes-cluster na inrichting
- Kubernetes-cluster na verwijdering
- Kubernetes-clusterinrichting
- Kubernetes-clusterverwijdering
- Kubernetes-naamruimtetoewijzing
- Kubernetes-naamruimte na inrichting
- Kubernetes-naamruimte na verwijdering
- Kubernetes-naamruimteverwijdering
- Kubernetes-naamruimtetoewijzing
- Toewijzing van Kubernetes-supervisornaamruimte
- Kubernetes-supervisornaamruimte na inrichting
- Kubernetes-supervisornaamruimte na verwijdering
- Verwijdering van Kubernetes-supervisornaamruimte
- Toewijzing van Kubernetes-supervisornaamruimte

Klik op een van de onderwerpen om het schema voor dat onderwerp weer te geven, waarin alle informatie wordt getoond die wordt verzameld en verzonden. Er zijn naamruimteonderwerpen voor zowel Kubernetes-naamruimten als supervisornaamruimten. U kunt al deze schema-informatie gebruiken om verschillende meldingen en beheer- en rapportagetaken in te stellen.

U kunt actiescripts voor CMX-gerelateerde acties instellen op de pagina **Uitbreidbaarheid** > **Bibliotheek** > **Acties**. Actiescripts kunnen voor verschillende doeleinden worden gebruikt: bijvoorbeeld om een DNS-record met Kubernetes-clusterinrichting te maken. Als u een DNS-record maakt, kunt u het veld `masternodeips` gebruiken vanuit het onderwerp Kubernetes-cluster na inrichting met een REST-opdracht in een actiescript om een DNS-record te maken.

Op de pagina Abonnementen wordt de relatie tussen de gebeurtenisonderwerpen en actiescripts gedefinieerd. U kunt deze onderdelen weergeven en beheren op de pagina Abonnementen in Cloud Assembly

Zie de documentatie voor Cloud Assembly-uitbreidbaarheid op [Levenscycli van applicaties uitbreiden en automatiseren met uitbreidbaarheid](#) voor meer informatie.

Wat is configuratiebeheer in Cloud Assembly

Cloud Assembly ondersteunt integratie met Puppet Enterprise, Ansible Open Source en Ansible Tower, zodat u implementaties voor configuraties en afwijkingen kunt beheren.

Puppet-integratie

Om Puppet-gebaseerd configuratiebeheer te integreren, moet u een geldige instantie van Puppet Enterprise hebben geïnstalleerd in een publieke of privécloud met een vSphere-workload. U moet een verbinding tot stand brengen tussen dit externe systeem en uw instantie van Cloud Assembly. Vervolgens kunt u Puppet-configuratiebeheer beschikbaar maken voor Cloud Assembly door het aan de juiste blueprints toe te voegen.

De Puppet-provider van de Cloud Assembly-blueprintservice installeert, configureert en start de Puppet-agent op een geïmplementeerde berekeningsresource. De Puppet-provider ondersteunt zowel SSH- als WinRM-verbindingen met de volgende vereisten:

- SSH-verbindingen:
 - De gebruikersnaam moet een supergebruiker of een gebruiker met sudo-rechten zijn om opdrachten met NOPASSWD uit te voeren.
 - Deactiveer `requiretty` voor de opgegeven gebruiker.
 - cURL moet beschikbaar zijn op de berekeningsresource van de implementatie.
- WinRM-verbindingen:
 - PowerShell 2.0 moet beschikbaar zijn op de berekeningsresource van de implementatie.
 - Configureer de Windows-sjabloon zoals beschreven in de documentatie voor vRealize Orchestrator.

De DevOps-beheerder is verantwoordelijk voor het beheer van de verbindingen met een Puppet-master en voor het toepassen van Puppet-rollen, of configuratieregels, voor specifieke implementaties. Na de implementatie worden virtuele machines die zijn geconfigureerd om configuratiebeheer te ondersteunen, geregistreerd met de aangewezen Puppet-master.

Wanneer virtuele machines worden geïmplementeerd, kunnen gebruikers een Puppet-master als extern systeem toevoegen of verwijderen of projecten bijwerken die aan de Puppet-master zijn toegewezen. Ten slotte kunnen de juiste gebruikers de geïmplementeerde virtuele machines uit de Puppet-master verwijderen wanneer de machines buiten gebruik worden gesteld.

Ansible Open Source-integratie

Wanneer u een Ansible-integratie instelt, installeert u Ansible Open Source in overeenstemming met de installatie-instructies voor Ansible. Zie de documentatie voor Ansible voor meer informatie over de installatie.

Ansible schakelt standaard de controle van de hostsleutel in. Als een host opnieuw wordt geïnstalleerd met een andere sleutel in het bestand `known_hosts`, treedt er een fout op. Als een host niet wordt weergegeven in het bestand `known_hosts`, moet u de sleutel opgeven bij het opstarten. U kunt de controle van de hostsleutel deactiveren met de volgende instelling in het bestand `/etc/ansible/ansible.cfg` of `~/.ansible.cfg`:

```
[defaults]
host_key_checking = False
localhost_warning = False

[paramiko_connection]
record_host_keys = False

[ssh_connection]
#ssh_args = -C -o ControlMaster=auto -o ControlPersist=60s
ssh_args = -o UserKnownHostsFile=/dev/null
```

Als u fouten in de hostsleutelcontrole wilt vermijden, stelt u `host_key_checking` en `record_host_keys` u in op `False`, inclusief het toevoegen van een extra optie `UserKnownHostsFile=/dev/null` die is ingesteld in `ssh_args`. Als de inventaris in eerste instantie leeg is, waarschuwt Ansible dat de hostlijst leeg is. Dit zorgt ervoor dat de Playbook-syntaxiscontrole mislukt.

De Ansible-kluis stelt u in staat gevoelige informatie, zoals wachtwoorden of sleutels, op te slaan in versleutelde bestanden in plaats van als platte tekst. De kluis is versleuteld met een wachtwoord. In Cloud Assembly gebruikt Ansible de kluis om gegevens zoals SSH-wachtwoorden voor hostcomputers te versleutelen. Hierbij wordt ervan uitgegaan dat het pad naar het kluiswachtwoord is ingesteld.

U kunt het bestand `ansible.cfg` wijzigen om de locatie van het wachtwoordbestand op te geven in de volgende indeling.

```
vault_password_file = /path to/file.txt
```

U kunt ook de omgevingsvariabele `ANSIBLE_VAULT_PASSWORD_FILE` instellen, zodat Ansible automatisch naar het wachtwoord zoekt. Bijvoorbeeld:

```
ANSIBLE_VAULT_PASSWORD_FILE=~/.vault_pass.txt
```

Cloud Assembly beheert het inventarisbestand voor Ansible, dus u moet ervoor zorgen dat de Cloud Assembly-gebruiker `rw`-toegang tot het inventarisbestand heeft.

```
cat ~/var/tmp/vmware/provider/user_defined_script/$(ls -t ~/var/tmp/vmware/provider/
user_defined_script/ | head -1)/log.txt
```

Als u een niet-rootgebruiker met opensource-integratie van Cloud Assembly wilt gebruiken, hebben de gebruikers een set rechten nodig om de opdrachten uit te voeren die door de opensourceprovider Cloud Assembly worden gebruikt. De volgende opdrachten moeten worden ingesteld in het sudoers-bestand van de gebruiker.

```
Defaults:myuser !requiretty
```

Als de gebruiker geen deel uitmaakt van een beheerdersgroep waarvoor geen askpass-applicatie is opgegeven, stelt u de volgende opdracht in het sudoers-bestand van de gebruiker in.

```
myuser ALL=(ALL) NOPASSWD: ALL
```

Als u fouten of andere problemen ondervindt bij het instellen van de Ansible-integratie, raadpleegt u het bestand `log.txt` bij `'cat~/var/tmp/vmware/provider/user_defined_script/$(ls -t ~/var/tmp/vmware/provider/user_defined_script/ | head -1)'` op de Ansible-controlemachine.

Ansible Tower-integratie

Ondersteunde typen besturingssystemen

- Red Hat Enterprise Linux 8.0 of hoger 64-bits (x86) ondersteunt alleen Ansible Tower 3.5 en hoger.
- Red Hat Enterprise Linux 7.4 of hoger 64-bits (x86).
- CentOS 7.4 of hoger 64-bits (x86).

Het volgende is een voorbeeld van een inventarisbestand, dat wordt gegenereerd tijdens een Ansible Tower-installatie. Mogelijk moet u dit wijzigen voor het gebruik van Cloud Assembly-integratie.

```
[root@cava-env8-dev-001359 ansible-tower-setup-bundle-3.5.2-1.el8]# pwd

/root/ansible-tower-install/ansible-tower-setup-bundle-3.5.2-1.el8

[root@cava-env8-dev-001359 ansible-tower-setup-bundle-3.5.2-1.el8]# cat inventory

[tower]

localhost ansible_connection=local


[database]


[all:vars]

admin_password='VMware1!'
```

```
pg_host=''

pg_port=''


pg_database='awx'

pg_username='awx'

pg_password='VMware1!'


rabbitmq_port=5672

rabbitmq_vhost=tower

rabbitmq_username=tower

rabbitmq_password='VMware1!'

rabbitmq_cookie=cookiemonster


# Needs to be true for fqdns and ip addresses

rabbitmq_use_long_name=false


# Isolated Tower nodes automatically generate an RSA key for authentication;

# To deactivate this behavior, set this value to false

# isolated_key_generation=true
```

Puppet Enterprise-integratie configureren in Cloud Assembly

Cloud Assembly ondersteunt integratie met Puppet Enterprise-configuratiebeheer.

Wanneer u Puppet Enterprise als extern systeem aan Cloud Assembly toevoegt, is dit standaard beschikbaar voor alle projecten. U kunt het beperken tot specifieke projecten.

Om een Puppet Enterprise-integratie toe te voegen, moet u over de masternaam van de Puppet en de hostnaam of het IP-adres van de master beschikken.

U kunt Puppet-logboeken vinden op de volgende locatie voor het geval u deze moet controleren op fouten of voor informatiedoeleinden.

Beschrijving	Logboeklocatie
Logboek voor gebeurtenissen gerelateerd aan maken en installeren	Logboeken bevinden zich op de geïmplementeerde machine in <code>~/var/tmp/vmware/provider/user_defined_script/\$(ls -t ~/var/tmp/vmware/provider/user_defined_script/ head -1)/'</code> . Raadpleeg het bestand log.txt voor volledige logboekinformatie. Voor gedetailleerde Puppet Agent-logboeken verwijzen we u naar https://puppet.com/docs/puppet/4.8/services_agent_unix.html#logging
Logboek voor Puppet-taken gerelateerd aan verwijderen en uitvoeren	Logboeken bevinden zich op de PE in <code>~/var/tmp/vmware/provider/user_defined_script/\$(ls -t ~/var/tmp/vmware/provider/user_defined_script/ head -1)/'</code> . Raadpleeg het bestand log.txt voor volledige logboekinformatie.

Procedure

1 Selecteer **Infrastructuur > Verbindingen > Integraties** en klik op **Integratie toevoegen**.

2 Selecteer Puppet.

3 Voer de vereiste informatie in op de Puppet-configuratiepagina.

Voor een goede werking van Puppet-integratie moeten de opgegeven verificatiegegevens geldig zijn voor zowel het SSH- als het API-account. Ook moeten de opgegeven gebruikersaccounts voor het besturingssysteem en applicaties dezelfde gebruikersnaam en hetzelfde wachtwoord hebben.

4 Klik op **Valideren** om de integratie te controleren.

5 Klik op **Toevoegen**.

Resultaten

Puppet kan worden gebruikt met cloudsjablonen.

Wat nu te doen

Voeg Puppet-onderdelen toe aan de gewenste cloudsjablonen.

1 Selecteer, onder Cloudsjablonen in Cloud Assembly, Puppet op de canvaspagina van de cloudsjabloon onder de kop Inhoudsbeheer in het menu met cloudsjabloonopties en sleep het Puppet-onderdeel naar het canvas.

2 Geef Puppet-eigenschappen op in het deelvenster aan de rechterkant.

Eigenschap	Beschrijving
Master	Voer de naam in van de primaire Puppet-machine die wordt gebruikt met deze cloudsjabloon.
Omgeving	Selecteer de omgeving voor de primaire Puppet-machine.
Rol	Selecteer de Puppet-rol die u met deze cloudsjabloon wilt gebruiken.
Uitvoeringsinterval agent	De frequentie waarmee de Puppet-agent bij de primaire Puppet-machine de configuratiedetails moet opvragen die moeten worden toegepast op geïmplementeerde virtuele machines die aan deze cloudsjabloon zijn gekoppeld.

- Klik op het tabblad Code in het deelvenster rechts om de YAML-code voor de Puppet-configuratie-eigenschappen weer te geven.

Wanneer u een Puppet-onderdeel toevoegt aan een cloudsjabloon, kunt u de eigenschap `installMaster` toevoegen aan het YAML-bestand om te wijzen naar een Puppet-installatiemaster, ook wel compilatiemaster genoemd. De waarde van deze eigenschap kan het IP-adres of de hostnaam van de Puppet-compilatiemaster zijn. Het gebruik van deze eigenschap biedt toegang tot verbeterde mogelijkheden voor geïmplementeerde virtuele Puppet-machines en biedt ook ondersteuning voor extra acties voor dag 2.

```
Puppet_Agent:
  type: Cloud.Puppet
  properties:
    account: PEIntegrationAccount
    environment: production
    role: 'role::linux_webserver'
    host: '${CentOS-Puppet.*}'
    username: root
    password: password123!
    installMaster: my-pe-compile-master.example.com
    agentConfiguration:
      certName: '${CentOS-Puppet.address}'
    osType: linux
    count: 1
```

Opmerking Hoewel de hier gedefinieerde gebruiker root is, kan de cloudsjabloon worden geconfigureerd met elke gebruiker die is opgenomen in de lijst sudoers.

Bepaalde machinegerelateerde informatie wordt door vRealize Automation in sommige gevallen standaard als feiten doorgegeven aan virtuele Puppet-machines. Aangepaste feiten worden niet ondersteund voor Windows-machines. Op Linux-machines wordt sommige informatie standaard doorgegeven en kunnen gebruikers aanvullende informatie doorgeven met behulp van aangepaste eigenschappen.

Er gelden beperkingen voor wat wordt doorgegeven aan Puppet-machines onder Linux. Aangepaste eigenschappen op hostresources en op de Puppet-agent worden doorgegeven aan virtuele Puppet-machines. Aangepaste eigenschappen op netwerkresources worden niet doorgegeven aan de virtuele machine. Doorgegeven items omvatten eenvoudige eigenschappen, booleaanse eigenschappen, aangepaste namen en complexe typen zoals geneste kaarten met arrays.

In het volgende voorbeeld ziet u hoe verschillende aangepaste resources kunnen worden aangeroepen op hostresources:

```
resources:
  Puppet-Host:
    type: Cloud.AWS.EC2.Instance
    properties:
      customer_specified_property_on_ec2_resource: "property"

customer_specified_property_on_network_resource_that_should_also_be_a_fact_and_is_boolean:
true
  CustomerNameStuff: "zone A"
  try_map:
    key: value
    keytwo: value
  nested_array:
    - one
    - two
    - true
  try_array:
    - one
    - two
    -three:
      inner_key: value
```

Als een Puppet-purgecommando fouten oplevert, negeert vRealize Automation, in de meeste gevallen, purgefouten voor knooppunten en wordt doorgegaan met verwijderen van het knooppunt. Zelfs als er geen certificaat voor een specifiek knooppunt wordt gevonden, gaat vRealize Automation door met verwijderen. Als vRealize Automation om een of andere reden niet kan doorgaan met verwijderen van het knooppunt, kunt u op Verwijderen klikken in het menu Acties van de pagina Implementaties om een dialoogvenster te openen waarmee u kunt doorgaan met verwijderen van het knooppunt. Een soortgelijke werkstroom wordt uitgevoerd wanneer u een Puppet-integratie uit een cloudsjabloon verwijdert en vervolgens de sjabloon op de implementatie toepast. Deze werkstroom activeert een purgebewerking op het knooppunt die wordt behandeld zoals hierboven is beschreven.

Voor integratie met Puppet Enterprise is een openbaar IP-adres vereist. Als er geen openbaar IP-adres is geconfigureerd voor de Puppet Enterprise-machine, wordt het IP-adres van de eerste NIC gebruikt.

Als de NIC van een met Puppet ingerichte machine die werkt op een vSphere-machine meerdere IP-adressen heeft, kunt u de YAML-eigenschap `primaryAddress` in cloudsjablonen gebruiken om op te geven welk IP-adres moet worden gebruikt voor verbindingen. Wanneer de eigenschap `primaryAddress` is toegewezen aan een NIC, wordt het IP-adres van deze NIC gebruikt door Puppet. Er kan slechts één NIC als primair worden aangewezen. In het volgende YAML-fragment ziet u een voorbeeld van hoe de eigenschap `primaryAddress` wordt gebruikt.

```
BaseVM:
  type: Cloud.vSphere.Machine
  properties:
    image: photon
    count: 2
    customizationSpec: Linux
    cpuCount: 1
    totalMemoryMB: 1024
    networks:
      - network: '${resource.dev.id}'
        deviceIndex: 0
        primaryAddress: true
        assignment: static
      - network: '${resource.prod.id}'
        deviceIndex: 1
        assignment: static
```

Als de eigenschap `primaryAddress` niet is ingesteld voor een NIC van een virtuele machine, zal de cloudsjabloonlogica standaard het huidige gedrag voor de selectie van IP-adressen gebruiken.

Ansible Open Source-integratie configureren in Cloud Assembly

Cloud Assembly ondersteunt integratie met Ansible Open Source-configuratiebeheer. Nadat u de integratie hebt geconfigureerd, kunt u Ansible-onderdelen toevoegen aan nieuwe of bestaande implementaties.

Wanneer u Ansible Open Source integreert met Cloud Assembly, kunt u dit configureren om een of meer Ansible-playbooks in een bepaalde volgorde uit te voeren wanneer een nieuwe machine wordt ingericht om het configuratiebeheer te automatiseren. U geeft de gewenste playbooks op in de cloudsjabloon voor een implementatie.

Wanneer u een Ansible-integratie instelt, moet u de Ansible Open Source-hostmachine opgeven, evenals het pad naar het inventarisbestand dat informatie voor het beheren van resources definieert. U moet ook een naam en een wachtwoord opgeven om toegang te krijgen tot de Ansible Open Source-instantie. Wanneer u later een Ansible-onderdeel aan een implementatie toevoegt, kunt u de verbinding bijwerken voor het gebruik van verificatie op basis van sleutels.

Ansible gebruikt standaard SSH om verbinding te maken met de fysieke machines. Als u Windows-machines gebruikt zoals opgegeven in de cloudsjabloon met de Windows-eigenschap `osType`, wordt de variabele `connection_type` automatisch ingesteld op `winrm`.

In eerste instantie gebruikt Ansible-integratie de inloggegevens gebruikersnaam/wachtwoord of gebruikersnaam/sleutel die in de integratie zijn opgegeven om verbinding te maken met de Ansible-bedieningsmachine. Zodra de verbinding is gelukt, worden de opgegeven playbooks in de cloudsjabloon gevalideerd voor de syntaxis.

Als de validatie is gelukt, wordt een uitvoeringsmap gemaakt op de Ansible-bedieningsmachine bij `~/var/tmp/vmware/provider/user_defined_script/`. Dit is de locatie van waaruit scripts worden uitgevoerd om de host aan de inventaris toe te voegen, de vars-bestanden van de host te maken, inclusief de verificatiemodus in te stellen om verbinding te maken met de host, en ten slotte de playbooks uit te voeren. Op dit moment worden de verificatiegegevens in de cloudsjabloon gebruikt om verbinding te maken met de host via de Ansible-bedieningsmachine.

Ansible-integratie ondersteunt fysieke machines die geen IP-adres gebruiken. Voor machines die zijn ingericht in openbare clouds zoals AWS, Azure en GCP, wordt de adreseigenschap in de gemaakte resource alleen ingevuld met het openbare IP-adres van de machine wanneer de machine is verbonden met een openbaar netwerk. Voor machines die niet met een openbaar netwerk zijn verbonden, zoekt de Ansible-integratie naar het IP-adres van het netwerk dat aan de machine is gekoppeld. Als er meerdere netwerken zijn bijgevoegd, zoekt Ansible-integratie naar het netwerk met de minste deviceIndex. Kortom: de index van de netwerkinterfacekaart (NIC) die aan de machine is gekoppeld. Als de eigenschap deviceIndex niet is opgegeven in de blueprint, gebruikt de integratie het eerste gekoppelde netwerk.

Zie [Wat is configuratiebeheer in Cloud Assembly](#) voor meer informatie over het configureren van Ansible-opensource voor integratie in Cloud Assembly.

Voorwaarden

- De Ansible-controlemachine moet een Ansible-versie gebruiken. Zie de [vRealize Automation-ondersteuningsmatrix](#) voor informatie over ondersteunde versies.
- Uitgebreide logboekgegevens voor Ansible moet standaard worden ingesteld op nul.
- De gebruiker moet lees-/schrijftoegang hebben tot de directory waarin het Ansible-inventarisbestand zich bevindt. De gebruiker moet ook lees-/schrijftoegang hebben tot het inventarisbestand, als dit al bestaat.
- Als u een niet-rootgebruiker gebruikt met de optie sudo, moet u ervoor zorgen dat het volgende is ingesteld in het sudoers-bestand:

```
Defaults:user_name !requiretty
```

```
en
```

```
username ALL=(ALL) NOPASSWD: ALL
```

- Zorg ervoor dat de controle van de hostsleutel is uitgeschakeld door `host_key_checking = False` in te stellen op `/etc/ansible/ansible.cfg` of `~/ .ansible.cfg`.

- Zorg ervoor dat het kluiswachtwoord is ingesteld door de volgende regel toe te voegen aan het bestand `/etc/ansible/ansible.cfg` of `~/.ansible.cfg`:

```
vault_password_file = /path/to/password_file
```

Het kluiswachtwoordbestand bevat het wachtwoord in platte tekst en wordt alleen gebruikt wanneer cloudsjablonen of implementaties de combinatie van gebruikersnaam en wachtwoord opgeven voor gebruik tussen ACM en het knooppunt zoals weergegeven in het volgende voorbeeld.

```
echo 'myStr0ng9@88w0rd' > ~/.ansible_vault_password.txt
echo 'ANSIBLE_VAULT_PASSWORD_FILE=~/.ansible_vault_password.txt' > ~/.profile
# Instead of this way, you can also set it setting
'vault_password_file=~/.ansible_vault_password.txt' in either /etc/ansible/ansible.cfg or
~/.ansible.cfg
```

- Om fouten in de hostsleutel te voorkomen tijdens het uitvoeren van playbooks, is het aan te bevelen om de volgende instellingen op te nemen in `/etc/ansible/ansible config`.

```
[paramiko_connection]
record_host_keys = False

[ssh_connection]
#ssh_args = -C -o ControlMaster=auto -o ControlPersist=60s
ssh_args = -o UserKnownHostsFile=/dev/null # If you already have any
options set for ssh_args, just add the additional option shown here at the end.
```

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Integraties** en klik op **Integratie toevoegen**.
- 2 Klik op **Ansible**.
De Ansible-configuratiepagina wordt weergegeven.
- 3 Voer de hostnaam, het pad van het inventarisbestand en andere vereiste informatie voor de Ansible Open Source-instantie in.
- 4 Klik op **Valideren** om de integratie te controleren.
- 5 Klik op **Toevoegen**.

Resultaten

Ansible kan worden gebruikt met cloudsjablonen.

Wat nu te doen

Voeg Ansible-onderdelen toe aan de gewenste cloudsjablonen.

- 1 Selecteer Ansible op de canvaspagina van de cloudsjabloon onder de kop Configuratiebeheer in het menu met cloudsjabloonopties en sleep het Ansible-onderdeel naar het canvas.

- 2 Gebruik het paneel aan de rechterkant om de geschikte Ansible-eigenschappen te configureren, zoals het opgeven van de playbooks die moeten worden uitgevoerd.

In Ansible kunnen gebruikers een variabele aan één host toewijzen en deze later gebruiken in playbooks. Met Ansible Open Source-integratie kunt u deze hostvariabele in cloudsjablonen opgeven. De eigenschap `hostVariables` moet de juiste YAML-indeling hebben, zoals verwacht door de Ansible-beheermachine, en deze inhoud wordt op de volgende locatie geplaatst:

```
parent_directory_of_inventory_file/host_vars/host_ip_address/vra_user_host_vars.yml
```

De standaardlocatie van het Ansible-inventarisbestand wordt gedefinieerd in het Ansible-account dat is toegevoegd op de pagina Integraties in Cloud Assembly. De Ansible-integratie valideert de YAML-syntaxis van `hostVariable` niet in de cloudsjabloon, maar de Ansible-beheermachine zal een fout genereren wanneer u een playbook uitvoert en de indeling of syntaxis onjuist is.

Het volgende YAML-fragment van de cloudsjabloon toont een voorbeeldgebruik van de eigenschap `hostVariables`.

```
Cloud_Ansible_1:
  type: Cloud.Ansible
  properties:
    host: '${resource.AnsibleLinuxVM.*}'
    osType: linux
    account: ansible-CAVA
    username: ${input.username}
    password: ${input.password}
    maxConnectionRetries: 20
    groups:
      - linux_vms
    playbooks:
      provision:
        - /root/ansible-playbooks/install_web_server.yml
    hostVariables: |
      message: Hello ${env.requestedBy}
      project: ${env.projectName}
```

Ansible-integraties verwachten dat verificatiegegevens in een cloudsjabloon op een van de volgende manieren aanwezig moeten zijn:

- Gebruikersnaam en wachtwoord in de Ansible-resource.
- Gebruikersnaam en `privateKeyFile` in de Ansible-resource.
- Gebruikersnaam in Ansible-resource en persoonlijke sleutel in de computerbron door `remoteAccess` naar `generatedPublicPrivateKey` op te geven.

Wanneer u een Ansible Open Source-integratie maakt, moet u de aanmeldingsinformatie voor de integratiegebruiker opgeven om verbinding met de Ansible-controlemachine te maken met behulp van SSH. Als u playbooks met een integratie wilt uitvoeren, kunt u een andere gebruiker opgeven in de YAML-code van de integratie. De eigenschap `username` is verplicht en is vereist om

verbinding te maken met de virtuele machine waar Ansible wijzigingen aanbrengt. De eigenschap `playbookRunUsername` is optioneel en kan worden opgegeven om het playbook op het Ansible-knooppunt uit te voeren. De standaardwaarde van `playbookRunUsername` is de gebruikersnaam voor Ansible-eindpuntintegratie.

Als u een andere gebruiker opgeeft, moet die gebruiker schrijftoegang hebben tot het Ansible-hostbestand en moet die gebruiker rechten hebben om persoonlijke sleutelbestanden te maken.

Wanneer u een Ansible Open Source-tegel aan een cloudsjabloon toevoegt, maakt vRealize Automation de hostvermelding voor de gekoppelde virtuele machine. Standaard gebruikt vRealize Automation de resourcenaam van de virtuele machine om de hostvermelding te maken, maar u kunt elke naam opgeven met behulp van de eigenschap `hostName` in de blueprint-YAML. Om te communiceren met de machine, maakt vRealize Automation de hostvariabele `ansible_host: IP Address` voor de hostvermelding. U kunt het standaardgedrag overschrijven om communicatie met FQDN te configureren, door het trefwoord `ansible_host` onder `hostVariables` op te geven en FQDN als bijbehorende waarde op te geven. In het volgende YAML-codefragment ziet u een voorbeeld van hoe hostnaam en FQDN-communicatie kunnen worden geconfigureerd:

```
Cloud_Ansible:
  type: Cloud Ansible
  properties:
    osType: linux
    username: ubuntu
    groups:
      - sample
    hostName: resource name
    host: name of host
    account: name of account
    hostVariables:
      ansible_host:Host FQDN
```

In dit voorbeeld overschrijft u de standaardwaarde van `ansible_host` door de FQDN op te geven. Dit kan handig zijn voor gebruikers die willen dat Ansible Open Source verbinding maakt met de hostmachine met behulp van de FQDN.

De standaardwaarde van `hostVariables` in de YAML zal `ansible_host:IP_address` zijn en het IP-adres wordt gebruikt om met de server te communiceren.

Als de YAML-eigenschap `count` groter is dan 1 voor Ansible Open Source, kan de hostnaam worden toegewezen aan een van de respectieve eigenschappen van de virtuele machine. In het volgende voorbeeld ziet u de toewijzing van een VM-resource met de naam Ubuntu-VM als wij willen dat de adreseigenschap wordt toegewezen aan de hostnaam.

```
hostname: '${resource.Ubuntu-VM.address[count.index]}'
```

Controleer in cloudsjablonen of het pad naar het Ansible-playbook toegankelijk is voor de gebruiker die is opgegeven in het integratieaccount. U kunt een absoluut pad gebruiken om de playbooklocatie op te geven, maar dit is niet nodig. Een absoluut pad naar de basismap van de gebruiker wordt aanbevolen, zodat het pad geldig blijft, zelfs als de verificatiegegevens van Ansible-integratie in de loop van de tijd veranderen.

Ansible Tower-integratie configureren in Cloud Assembly

U kunt Ansible Tower met Cloud Assembly integreren om het configuratiebeheer van geïmplementeerde resources te ondersteunen. Nadat u de integratie hebt geconfigureerd, kunt u Ansible Tower-onderdelen toevoegen aan nieuwe of bestaande implementaties vanuit de cloudsjablooneditor.

Voorwaarden

- Geef gebruikers die geen beheerder zijn de juiste rechten om toegang tot Ansible Tower te krijgen. Er zijn twee opties die kunnen worden gebruikt voor de meeste configuraties. Kies de optie die het meest geschikt is voor uw configuratie.
 - Geef gebruikers de rollen Inventarisbeheerder en Taaksjabloonbeheerder op organisatieniveau.
 - Geef gebruikers Beheerdersrechten voor een bepaalde inventaris en de rol Uitvoeren voor alle taaksjablonen die worden gebruikt voor inrichting.
- U moet de juiste verificatiegegevens en sjablonen in Ansible Tower configureren voor gebruik met uw implementaties. Sjablonen kunnen opdrachtsjablonen of werkstroomsjablonen zijn. Opdrachtsjablonen definiëren de inventaris en het playbook voor gebruik met een implementatie. Er is een 1:1-toewijzing tussen een taaksjabloon en een playbook. Playbooks gebruiken een YAML-achtige syntaxis om taken te definiëren die aan de sjabloon zijn gekoppeld. Voor de meeste gangbare implementaties gebruikt u verificatiegegevens voor de machine voor verificatie.

Met werkstroomsjablonen kunnen gebruikers reeksen maken die bestaan uit een willekeurige combinatie van opdrachtsjablonen, projectsynchronisaties en inventarissynchronisaties die aan elkaar zijn gekoppeld, zodat u ze als één afzonderlijke eenheid kunt uitvoeren. De Ansible Tower Workflow Visualizer helpt gebruikers bij het ontwerpen van werkstroomsjablonen. Voor de meeste gangbare implementaties kunt u verificatiegegevens voor de machine gebruiken voor verificatie.

- a Meld u aan bij Ansible Tower en navigeer naar de sectie Sjablonen.
- b Selecteer Een nieuwe taaksjabloon toevoegen.
 - Selecteer de verificatiegegevens die u al hebt gemaakt. Dit zijn de verificatiegegevens van de machine die moet worden beheerd door Ansible Tower. Voor elke taaksjabloon kan er één verificatiegegevensobject zijn.

- Selecteer Vragen bij starten voor de limietselectie. Hiermee zorgt u ervoor dat de taaksjabloon wordt uitgevoerd op het knooppunt dat wordt ingericht of waarvan de inrichting is opgeheven vanuit Cloud Assembly. Als deze optie niet is geselecteerd, wordt er een fout Geen limiet ingesteld weergegeven wanneer de blueprint die de taaksjabloon bevat, wordt geïmplementeerd.
- c Selecteer Een nieuwe werkstroomsjabloon toevoegen.
 - Selecteer de verificatiegegevens die u al hebt gemaakt en definieer vervolgens de inventaris. Ontwerp de werkstroomsjabloon met Workflow Visualizer.

Voor het vak Limiet van werkstroom of © sjablonen kunt u doorgaans Vragen bij starten selecteren. Hiermee zorgt u ervoor dat de opdracht- of werkstroomsjabloon wordt uitgevoerd op het knooppunt dat wordt ingericht of waarvan de inrichting is opgeheven vanuit Cloud Assembly.

- U kunt de uitvoering van de opdrachtsjablonen of werkstroomsjablonen weergeven die worden aangeroepen via Cloud Assembly op het tabblad Ansible Tower-opdrachten.

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Integraties** en klik op **Integratie toevoegen**.
- 2 Klik op Ansible Tower.
De Ansible-configuratiepagina wordt weergegeven.
- 3 Voer de **Hostnaam** in, die een IP-adres kan zijn, evenals andere vereiste informatie voor de Ansible Tower-instantie.
- 4 Voer de **gebruikersnaam** en het **wachtwoord** in voor de UI-gebaseerde verificatie voor de toepasselijke Ansible Tower-instantie.
- 5 Klik op **Valideren** om de integratie te controleren.
- 6 Typ een geschikte **naam** en **beschrijving** voor de integratie.
- 7 Klik op **Toevoegen**.

Resultaten

Ansible Tower kan worden gebruikt in cloudsjablonen.

Wat nu te doen

Voeg Ansible Tower-onderdelen toe aan de gewenste cloudsjablonen. Zorg ervoor dat u de juiste opdrachtsjabloon opgeeft met uitvoeringsrechten voor de gebruiker die zijn opgegeven in het integratie-account.

- 1 Selecteer Ansible op de canvaspagina van de cloudsjabloon onder de kop Configuratiebeheer in het menu met blueprintoepies en sleep het Ansible Tower-onderdeel naar het canvas.
- 2 Gebruik het paneel aan de rechterkant om de geschikte Ansible Tower-eigenschappen zoals opdrachtsjablonen te configureren.

Wanneer u een Ansible Tower-tegel aan een cloudsjabloon toevoegt, maakt vRealize Automation de hostvermelding voor de gekoppelde virtuele machine in de Ansible Tower. Standaard gebruikt vRealize Automation de resourcenaam van de virtuele machine om de hostvermelding te maken, maar u kunt elke naam opgeven met behulp van de eigenschap `hostName` in de blueprint-YAML. Om te communiceren met de machine, maakt vRealize Automation de hostvariabele `ansible_host: IP Address` voor de hostvermelding. U kunt het standaardgedrag overschrijven om communicatie met FQDN te configureren, door het trefwoord `ansible_host` onder `hostVariables` op te geven en FQDN als bijbehorende waarde op te geven. In het volgende YAML-codefragment ziet u een voorbeeld van hoe hostnaam en FQDN-communicatie kunnen worden geconfigureerd:

```
Cloud_Ansible_Tower_1:
  type: Cloud Ansible Tower
  properties:
    host: name of host
    account: name of account
    hostName: resource name
    hostVariables:
      ansible_host:Host FQDN
```

In dit voorbeeld overschrijft u de standaardwaarde van `ansible_host` door de FQDN op te geven. Dit kan handig zijn voor gebruikers die willen dat Ansible Tower via de FQDN verbinding met de hostmachine maakt.

De standaardwaarde van `hostVariables` in de YAML zal `ansible_host:IP_address` zijn en het IP-adres wordt gebruikt om met de server te communiceren.

Als de YAML-eigenschap `count` groter is dan 1 voor Ansible Tower, kan de hostnaam worden toegewezen aan een van de respectieve eigenschappen van de virtuele machine. In het volgende voorbeeld ziet u de toewijzing van een VM-resource met de naam Ubuntu-VM als wij willen dat de adreseigenschap ervan wordt toegewezen aan de hostnaam.

```
hostname: '${resource.Ubuntu-VM.address[count.index]}'
```

Wanneer u een Ansible Tower-onderdeel toevoegt aan een cloudsjabloon, kunt u de taaksjabloon opgeven om de YAML van de cloudsjabloon aan te roepen. U kunt ook werkstroomsjablonen of een combinatie van taaksjablonen en werkstroomsjablonen opgeven. Als u het sjabloontype niet opgeeft, gaat vRealize Automation ervan uit dat u een taaksjabloon aanroept.

In het volgende YAML-fragment ziet u een voorbeeld van hoe u een combinatie van opdracht- en werkstroomsjablonen kunt aanroepen in een Ansible Tower-cloudsjabloon.

```
Cloud_Ansible_1:
  type: Cloud.Ansible.Tower
  properties:
    host: '${resource.CentOS_Machine.*}'
    account:
    maxConnectionRetries: 2
    maxJobRetries: 2
```

```
templates:
  provision:
    - name: My workflow
      type: workflow
    - name: My job template
```

We hebben de `maxConnectionsRetries` en `maxJobRetries` toegevoegd om Ansible-gerelateerde fouten te behandelen. De cloudsjablonen accepteren de aangepaste waarde en, als er geen waarde wordt opgegeven, wordt de standaardwaarde gebruikt. Voor `maxConnectionRetries` is de standaardwaarde 10 en voor `maxJobRetries` is de standaardwaarde 3.

Opmerking Eerdere versies van vRealize Automation ondersteunden de uitvoering van opdrachtsjablonen alleen met behulp van het schema `jobTemplate` in de cloudsjabloon. Het schema `jobTemplate` is nu afgeschaft en kan in toekomstige releases worden verwijderd. De eigenschap `jobTemplate` werkt momenteel nog steeds zoals verwacht. Om werkstroomsjablonen uit te voeren en aanvullende functies te gebruiken, wordt u aanbevolen het sjablonenschema te gebruiken.

Cloud Assembly-cloudsjablonen voor Ansible Tower-integraties bevatten de eigenschap `useDefaultLimit` met waarde waar of onwaar om te definiëren waar Ansible-sjablonen worden uitgevoerd. Ansible-sjablonen kunnen opdrachtsjablonen of werkstroomsjablonen zijn. Als deze waarde op waar is ingesteld, worden de opgegeven sjablonen uitgevoerd op basis van de machine die is opgegeven in het vak Limiet op de pagina Ansible-sjablonen. Als de waarde op onwaar is ingesteld, worden de sjablonen uitgevoerd op de ingerichte machine. Gebruikers moeten echter het selectievakje Vragen bij starten inschakelen op de pagina Ansible Tower-sjablonen. De standaardwaarde van deze eigenschap is onwaar. In het volgende YAML-voorbeeld ziet u hoe de eigenschap `useDefaultLimit` in cloudsjablonen wordt weergegeven.

```
templates:
  provision:
    - name: ping aws_credentials
      type: job
      useDefaultLimit: false
      extraVars: '{"rubiconSurveyJob" : "checkSurvey"}'
```

Bovendien kunt u, zoals in het vorige voorbeeld, de eigenschap `extraVars` gebruiken om extra variabelen of enquêtevariabelen op te geven. Deze mogelijkheid kan handig zijn voor het uitvoeren van sjablonen waarvoor invoer is vereist. Als een gebruiker de enquêtevariabele heeft behouden, moet u de variabele doorgeven in de sectie `extraVars` van de cloudsjabloon om fouten te voorkomen.

Een SaltStack Config-integratie maken in vRealize Automation

U kunt een SaltStack Config-integratie maken om toegang te krijgen tot de SaltStack Config-service, en SaltStack Config-objecten en -acties gebruiken in vRealize Automation.

Met vRealize Automation SaltStack Config kunt u op elke schaal software inrichten, configureren en implementeren op uw virtuele machines met behulp van gebeurtenisgestuurde automatisering. U kunt ook SaltStack Config gebruiken om optimale, conforme softwarestatussen in uw hele omgeving te definiëren en af te dwingen.

Installatie

Voordat u SaltStack Config met vRealize Automation integreert, moet u deze eerst in uw omgeving installeren. Zie [SaltStack Config installeren en configureren](#) voor meer informatie.

Overwegingen

Geïntegreerde vRealize Automation SaltStack Config is beschikbaar voor vRealize Automation met de volgende voorwaarden:

- De SaltStack Config-integratie is tijdens de installatie gekoppeld aan een specifieke host.
- vRealize Automation biedt momenteel geen ondersteuning voor multitenancy voor SaltStack Config.
- De vRealize Automation-tenant kan één SaltStack Config-integratie en één Salt-master ondersteunen. De Salt-master kan meerdere minions ondersteunen.
- Voordat u een SaltStack Config-integratie in vRealize Automation kunt verwijderen, moet u alle bestaande implementaties verwijderen die de SaltStack Config-integratie gebruiken.

Vereisten

- Controleer of u vRealize Automation-beheerdersreferenties en SaltStack Config-beheerdersreferenties (toegang op rootniveau) hebt.

U hebt vRealize Automation-beheerdersreferenties en SaltStack Config-beheerdersreferenties (toegang op rootniveau) nodig om een SaltStack Config-integratie te maken.

U hebt ook SaltStack Config-beheerdersreferenties nodig om de SaltStack Config-service te openen en met deze service te werken.

U gebruikt vRealize Automation-verificatiegegevens om toegang te krijgen tot vRealize Automation- en SaltStack Config-verificatiegegevens voor toegang tot SaltStack Config.

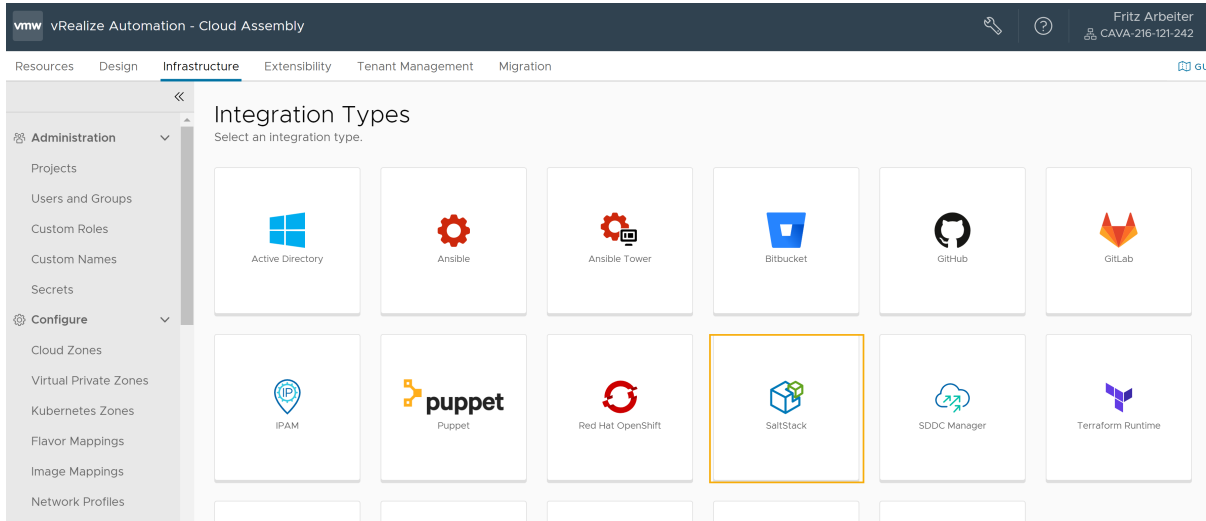
Zie de handleiding [SaltStack Config installeren en configureren](#) voor meer informatie over SaltStack Config-beheerdersreferenties.

- Controleer of de SaltStack Config-service is geïnstalleerd.
- Controleer of de Salt-master die moet worden gebruikt in de SaltStack Config-integratie de hoofdplug-in bevat.
- Controleer of u de rol van SaltStack Config-servicebeheerder in vRealize Automation hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Controleer of u de rol van Cloud Assembly-servicebeheerder in vRealize Automation hebt. Zie [Organisatie- en servicegebruikersrollen in vRealize Automation](#).

Een SaltStack Config-integratie in vRealize Automation configureren

Nadat u SaltStack Config voor vRealize Automation hebt geïnstalleerd, kunt u de integratie in Cloud Assembly configureren.

- 1 Selecteer **Infrastructuur > Verbindingen > Integraties** in Cloud Assembly en klik op **Integratie toevoegen**.
- 2 Selecteer het SaltStack Config-integratietype.



- 3 Vul het formulier in.

- a Voer een naam in voor de integratie.
- b (Optioneel) Geef een beschrijving voor de integratie op.

- c Voer de hostnaam voor de SaltStack Config-server in.
- d Geef de uitvoeringsomgeving op voor de SaltStack Config-integratie.

Als u de eigenschap `saltConfiguration` gebruikt om minions te implementeren en statusbestanden toe te passen op uw virtuele machines, hoeft u geen uitvoeringsomgeving te configureren. Het wordt echter aanbevolen dat u uw cloudsjablonen bijwerkt om de SaltStack Config-resource te gebruiken. De eigenschap `saltConfiguration` zal echter niet meer worden ondersteund in een toekomstige release.

Als u de SaltStack Config-resource gebruikt om minions te implementeren en statusbestanden toe te passen op uw virtuele machines, selecteert u de uitvoeringsomgeving **embedded-ABX-onprem**.

- e Voer de gebruikersnaam en het wachtwoord van de SaltStack Config-beheerder in die worden gebruikt om toegang te krijgen tot de opgegeven host.
- f Klik op **Valideren** om uw beheerderstoegang tot de host van de SaltStack Config-integratie te bevestigen.

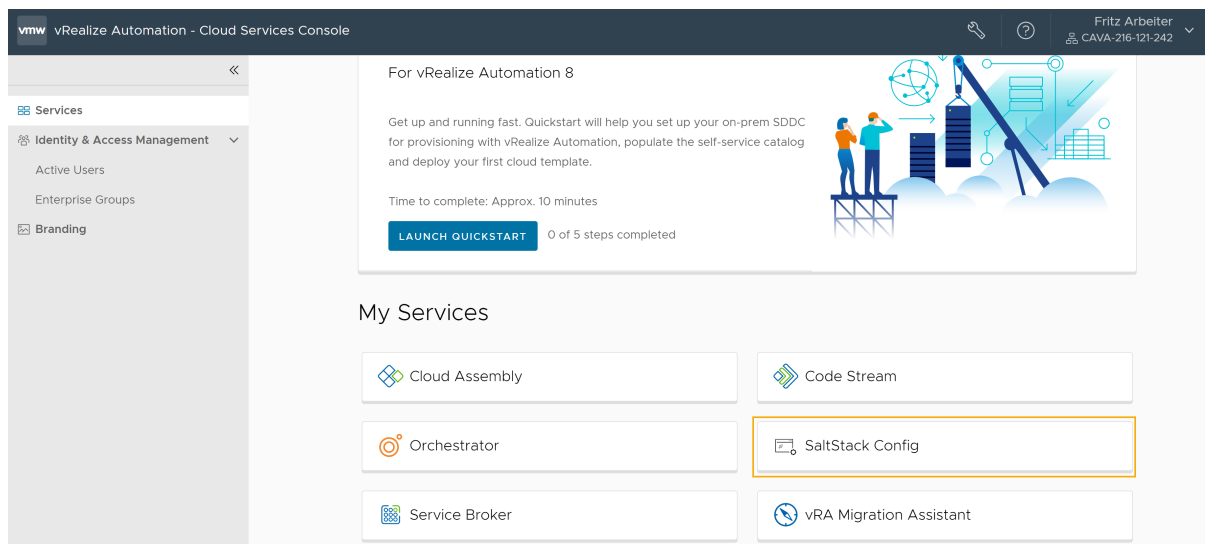
Als de validatie mislukt, controleert u of u de juiste hostnaam en gebruikersnaam en het juiste wachtwoord hebt ingevoerd.

- g Klik op **Opslaan**.

Toegang tot uw SaltStack Config-integratie

Nadat u het SaltStack Config-integratiepunt hebt opgeslagen, kunt u de SaltStack Config-integratieservice openen.

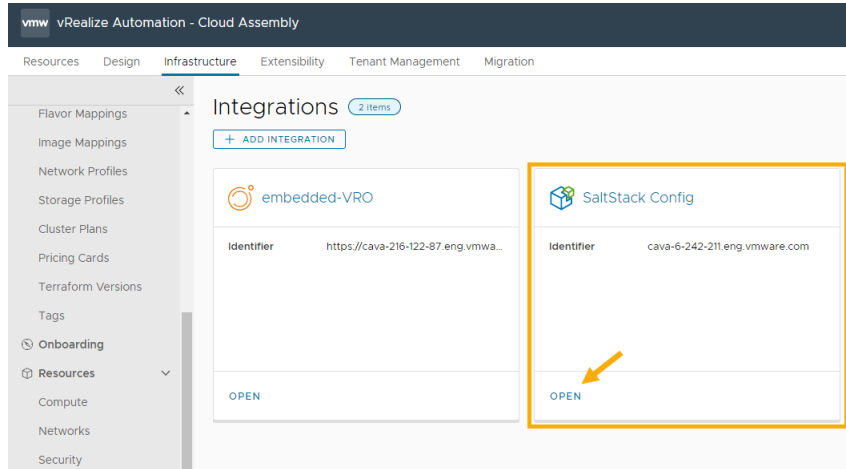
- 1 Als u SaltStack Config hebt geïmplementeerd via vRealize Suite Lifecycle Manager, kunt u op de servicetegel in de vRealize Automation-serviceconsole klikken om de integratie te openen en toegang te krijgen tot de host.



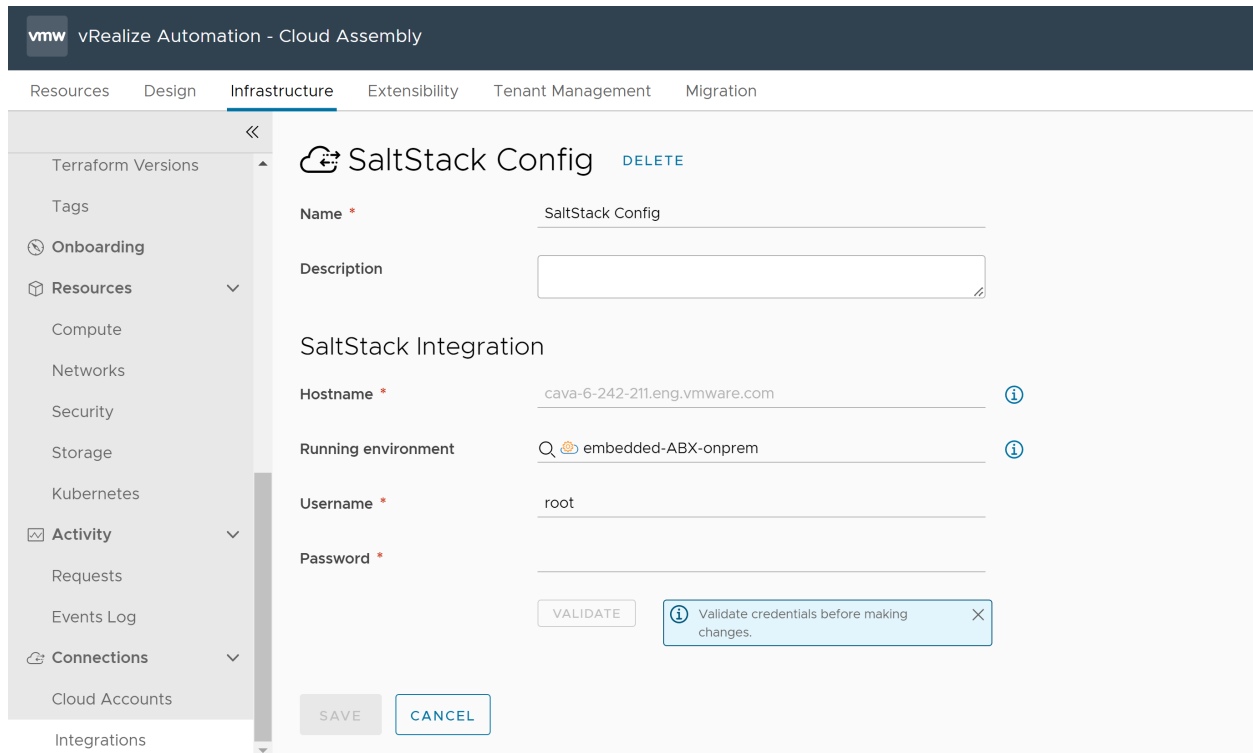
Als u een standalone installatie van SaltStack Config hebt uitgevoerd, kunt u de service openen met behulp van uw SaltStack Config-hostnaam.

- 2 Wanneer u wordt gevraagd om u aan te melden bij SaltStack Config, voert u uw gebruikersnaam en wachtwoord als SaltStack Config-beheerder in.

Als u wijzigingen in de integratie wilt aanbrengen, selecteert u **Infrastructuur > Verbindingen > Integraties**, selecteert u de beschikbare SaltStack Config-integratietegel en klikt u op **Openen**.



De hostnaam kan niet worden gewijzigd nadat u de integratie hebt geconfigureerd. U kunt alleen de naam, beschrijving, uitvoeringsomgeving en verificatiegegevens voor de integratie bewerken.



Informatie over het gebruik van SaltStack Config

SaltStack Config is een standalone product dat u kunt integreren met en gebruiken in vRealize Automation.

- Informatie over hoe u de [SaltStack Config-resource](#) toevoegt om minions te installeren op virtuele machines in uw Cloud Assembly-implementaties
- Informatie over hoe u [minions implementeert met behulp van de API \(RaaS\)](#) in een Linux- of Windows-omgeving

Hoe maak ik een Active Directory-integratie in Cloud Assembly?

Cloud Assembly ondersteunt integratie met Active Directory-servers om out-of-the-box computeraccounts te maken in een opgegeven organisatie-eenheid (OU) binnen een Active Directory-server voordat u een virtuele machine inricht. Active Directory ondersteunt een LDAP-verbinding met de Active Directory-server.

Een Active Directory-beleid dat is gekoppeld aan een project wordt toegepast op alle virtuele machines die binnen het bereik van dat project zijn ingericht. Gebruikers kunnen een of meer labels opgeven die worden gebruikt om het beleid selectief toe te passen op virtuele machines die worden ingericht in de cloudzones met overeenkomende capaciteitstags.

Bij implementaties op locatie kunt u met Active Directory-integratie een functie voor gezondheidscontrole instellen die de status van de integratie en de onderliggende ABX-integratie waarop deze berust weergeeft, inclusief de vereiste uitbreidingscloudproxy. Voordat u een Active Directory-beleid toepast, controleert Cloud Assembly de status van de onderliggende integraties. Als de integratie in orde is, gaat Cloud Assembly door met het maken van de geïmplementeerde computerobjecten in de opgegeven Active Directory. Als de integratie ongezond is, slaat de implementatiebewerking de fase Active Directory over tijdens de provisioning.

Voorwaarden

- Voor Active Directory-integratie is een LDAP-verbinding met de Active Directory-server vereist.
- Als u een Active Directory-integratie met vCenter op locatie configureert, moet u een ABX-integratie met een uitbreidingscloudproxy configureren. Selecteer **Uitbreidbaarheid > Activiteit > Integraties** en kies **Uitbreidingsacties op locatie**.
- Als u een integratie met Active Directory in de cloud configureert, moet u een Microsoft Azure- of Amazon Web Services-account hebben.
- U moet een project dat is geconfigureerd met de juiste cloudzones en image- en soorttoewijzingen hebben voor gebruik met de Active Directory-integratie.
- De gewenste organisatie-eenheid in uw Active Directory moet vooraf worden gemaakt voordat u uw Active Directory-integratie met een project koppelt.

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Integraties** en dan **Nieuwe integratie**.

2 Klik op **Active Directory**.

3 Voer op het tabblad **Samenvatting** de juiste LDAP-host- en omgevingsnamen in.

De opgegeven LDAP-host wordt gebruikt om de Active Directory-integratie te valideren en wordt ook gebruikt voor volgende implementaties als er geen alternatieve hosts worden opgegeven en aangeroepen vanwege fouten of onbeschikbaarheid.

4 Voer de gebruikersnaam en het wachtwoord voor de LDAP-server in.

5 Voer de juiste Base DN in die de root opgeeft voor de gewenste Active Directory-resources.

Opmerking U kunt slechts één DN per Active Directory-integratie opgeven.

6 Klik op **Valideren** om er zeker van te zijn dat de integratie werkt.

7 Voer een naam en een beschrijving in voor deze integratie.

8 Klik op **Opslaan**.

9 Klik op het tabblad **Project** om een project toe te voegen aan de Active Directory-integratie.

In het dialoogvenster **Projecten toevoegen** moet u een projectnaam en een gerelateerde DN selecteren. Dit is een DN die bestaat binnen de Basis-DN die is opgegeven op het tabblad Samenvatting.

10 Geef onder de selectie Uitgebreide opties een door komma's gescheiden lijst op van **alternatieve hosts** die worden gebruikt als de aanvankelijk geselecteerde server niet beschikbaar is tijdens de implementatie. De primaire server wordt altijd gebruikt voor de eerste validatie van de integratie.

Opmerking Als de primaire host een LDAP-indeling heeft, wordt LDAPS niet ondersteund voor alternatieve hosts.

11 Voer in het vak **Verbindingstime-out** de tijd in die moet worden gewacht op de reactie van de oorspronkelijke server voordat het via een alternatieve server wordt geprobeerd.

12 Klik op **Opslaan**.

Resultaten

U kunt het project met Active Directory-integratie nu aan een cloudsjabloon koppelen. Wanneer een machine wordt ingericht met deze cloudsjabloon wordt deze vooraf klaargezet in de opgegeven Active Directory en Organisatie-eenheid.

Active Directory-integraties worden in eerste instantie geïmplementeerd in een standaard-OU met weinig beperkingen voor gebruikers. Deze organisatie-eenheid wordt standaard ingesteld wanneer u een Active Directory-integratie aan een project toewijst. U kunt een eigenschap met de naam `FinalRelativeDN` toevoegen aan blueprints om de OU voor Active Directory-implementaties te wijzigen. Met deze eigenschap kunt u opgeven welke OU u wilt gebruiken voor een Active Directory-implementatie.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: CenOS8
      flavor: tiny
      activeDirectory:
        finalRelativeDN: ou=test
        securityGroup: TestSecurityGroup
```

Zoals u in het voorgaande YAML-voorbeeld ziet, kunnen gebruikers een eigenschap toevoegen aan de implementatie van een Active Directory-integratie waarmee een computeraccount aan de beveiligingsgroep wordt toegevoegd om de juiste rechten te verlenen voor de toegang tot de resources die via een netwerk worden gedeeld. De virtuele Active Directory-machine wordt in eerste instantie in een vaste organisatie-eenheid geïmplementeerd, maar zodra de machine kan worden vrijgegeven, wordt deze overgedragen naar een andere organisatie-eenheid die het juiste beleid voor de gebruikers heeft.

Als computeraccounts na implementatie naar een andere organisatie-eenheid worden verplaatst, probeert Cloud Assembly de accounts op de oorspronkelijke OU te verwijderen. Het verwijderen van computeraccounts lukt alleen als de virtuele machines naar een andere organisatie-eenheid binnen hetzelfde domein worden verplaatst.

U kunt ook als volgt een op tags gebaseerde gezondheidscontrole implementeren voor Active Directory-integraties op locatie.

- 1 Maak een Active Directory-integratie zoals beschreven in de voorgaande stappen.
- 2 Klik op het tabblad **Project** om een project toe te voegen aan de Active Directory-integratie.
- 3 Selecteer een projectnaam en een gerelateerde DN in het dialoogvenster Projecten toevoegen. De gerelateerde DN moet binnen de opgegeven Basis-DN bestaan.

Dit dialoogvenster bevat twee schakelaars waarmee u de Active Directory-configuratie op basis van cloudsjablonen kunt beheren. Beide schakelaars zijn standaard uitgeschakeld.

- **Overschrijven** - Met deze schakelaar kunt u Active Directory-eigenschappen overschrijven, in het bijzonder de relatieve DN in cloudsjablonen. Wanneer deze schakelaar is ingeschakeld, kunt u de OU wijzigen die is opgegeven in de eigenschap `relativeDN` in de cloudsjabloon. Wanneer de machine is ingericht, wordt deze toegevoegd aan de OU die is opgegeven in de eigenschap `relativeDN` in de cloudsjabloon. In het volgende voorbeeld ziet u de hiërarchie van de cloudsjablonen waarin deze eigenschap voorkomt.

```
activeDirectory:
  relativeDN: OU=ad_integration_machine_override
```

- **Negeren** - Met deze schakelaar kunt u de Active Directory-configuratie voor het project negeren. Wanneer deze schakelaar is ingeschakeld, wordt een eigenschap toegevoegd aan de cloudsjabloon met de naam `ignoreActiveDirectory` voor de gekoppelde virtuele machine. Wanneer deze eigenschap op waar is ingesteld, betekent dit dat de machine niet wordt toegevoegd aan de Active Directory wanneer deze wordt geïmplementeerd.
- 4 Voeg geschikte tags toe. Deze tags zijn van toepassing op de cloudzone waarop het Active Directory-beleid van toepassing is.
 - 5 Klik op Opslaan.

De status van de Active Directory-integratie wordt weergegeven voor elke integratie op de pagina **Infrastructuur > Verbindingen > Integraties** in Cloud Assembly.

U kunt het project met Active Directory-integratie koppelen aan een cloudsjabloon. Wanneer een machine wordt ingericht met deze sjabloon, wordt deze vooraf klaargezet in de opgegeven Active Directory en organisatie-eenheid.

Een VMware SDDC Manager-integratie configureren

U kunt een VMware SDDC Manager-integratie toevoegen aan vRealize Automation om werkloaddomeinen mogelijk te maken als onderdeel van VMware Cloud Foundation-cloudaccounts (VCF) in vRealize Automation.

Voorwaarden

- vRealize Automation ondersteunt alleen integratie met VMware SDDC Manager 4.1 en nieuwer.

Procedure

- 1 Selecteer **Infrastructuur > Verbindingen > Integraties** en klik op **Integratie toevoegen**.
- 2 Selecteer SDDC Manager.
De configuratiepagina voor de SDDC Manager-integratie wordt weergegeven.
- 3 Voer in het gedeelte Samenvatting een **naam** en **beschrijving** voor de integratie in.

- 4 Voer in het gedeelte SDDC Manager-referenties het **SDDC Mgr IP-adres/FQDN** in voor de SDDC Manager-servermachine.
- 5 Voer de gebruikersnaam en het wachtwoord in voor het beheerdersaccount dat moet worden gebruikt om verbinding te maken met de SDDC Manager. Het is aan te bevelen om verbinding te maken met het beheerdersaccount. Gebruik een ander account dat beheerdersrechten in SDDC Manager heeft om servicerollen te maken.

Deze verificatiegegevens worden gebruikt om de verbinding met de SDDC Manager te maken en vervolgens worden de servicereferenties gemaakt die moeten worden gebruikt bij het verbinden van een VCF-cloudaccount.

- 6 Klik op **Valideren** om de verbinding met de SDDC Manager te verifiëren.
- 7 Klik op **Toevoegen**.

Resultaten

Nadat de integratie is gemaakt, kunt u de workloads weergeven die zijn gekoppeld aan de SDDC op het tabblad Workloaddomein dat wordt weergegeven op de pagina met de voltooide integratie. U kunt ook workloads weergeven en selecteren die aan de integratie zijn gekoppeld en vervolgens op de knop **Cloudaccount toevoegen** klikken om een pagina te openen voor het maken van een VCF-cloudaccount dat de geselecteerde workload zal gebruiken.

Wat nu te doen

Nadat u het VCF-cloudaccount hebt geconfigureerd, wordt bovenaan de pagina de knop **Cloud instellen** weergegeven. Klik op deze knop om de instelwizard van de VCF-cloud te starten.

Integreren met vRealize Operations Manager

vRealize Automation kan samenwerken met vRealize Operations Manager om een geavanceerde verdeling van de workload uit te voeren, de status van de implementatie en statistieken van de virtuele machine te bieden en de prijzen weer te geven.

Aantal en type integraties

De integratie tussen de twee producten moet plaatsvinden van op locatie naar op locatie en niet een combinatie van op locatie en cloud.

U kunt één vRealize Automation-instantie met meerdere vRealize Operations Manager-instanties integreren, maar een vRealize Operations Manager-instantie kan slechts met één vRealize Automation-instantie worden verbonden.

U kunt geen geaggregeerd cluster van vRealize Operations Manager verbinden met vRealize Automation.

Basisvereisten voor integratie

Om te integreren met vRealize Operations Manager, gaat u naar **Infrastructuur > Verbindingen > Integraties**. Om de integratie toe te voegen, hebt u de URL van vRealize Operations Manager en de referentiegegevens nodig voor het aanmeldingsaccount dat in het volgende gedeelte wordt beschreven. Daarnaast moeten vRealize Automation en vRealize Operations Manager hetzelfde vSphere-eindpunt beheren.

Aanmeldingsaccount voor integratie

In vRealize Operations Manager hebt u een lokaal of niet-lokaal vRealize Operations Manager-aanmeldingsaccount nodig om de integratie te kunnen gebruiken. Voor het account zijn alleen-lezen rechten vereist voor de adapterinstantie van vCenter voor het vSphere-eindpunt. Houd er rekening mee dat mogelijk een niet-lokaal account moet worden geïmporteerd in vRealize Operations Manager en dat de alleen-lezen rol is toegewezen. Voor de integratie is de gebruikersnaamnotatie voor aanmelding bij niet-lokale accounts *gebruikersnaam@domein@geverifieerde-bron* zoals *jdoe@company.com@workspaceone*. Geverifieerde bronnen worden gedefinieerd tijdens de eerste installatie van de vRealize Operations Manager-server.

Zie de volgende secties voor informatie. Zie [Prijkaarten gebruiken in vRealize Automation](#) voor prijsinformatie.

Geavanceerde verdeling van workloads met vRealize Operations Manager

vRealize Automation en vRealize Operations Manager kunnen samenwerken om implementatieworkloads optimaal te verdelen.

U schakelt de verdeling van workloads in op het niveau van de op vSphere gebaseerde cloudzone. Alleen DRS-clusters (Distributed Resource Scheduler) van een cloudzone komen in aanmerking voor geavanceerde verdeling met vRealize Operations Manager.

- vRealize Automation-plaatsing — de vRealize Automation-plaatsing-engine is gebaseerd op applicatie-intenties. Deze beschouwt taggebaseerde beperkingen, projectlidmaatschap en de gekoppelde cloudzones en affiniteitsfilters die zijn gerelateerd aan netwerk, opslag en computer. De verdeling van resources is afhankelijk van al deze factoren plus de aanwezigheid van andere, gerelateerde doelresources in dezelfde implementatie.
- vRealize Operations Manager-plaatsing — vRealize Operations Manager houdt rekening met bewerkingsintentie voor een optimale plaatsing. Operationele intentie kan rekening houden met vroegere workloads en toekomstige taken, en voorwaardelijke voorspellingen.

Wanneer u geavanceerde verdeling van belasting gebruikt, moet u vRealize Automation-tagging toepassen om zakelijke intentiebeslissingen te implementeren in plaats van de zakelijke intentie-opties van vRealize Operations Manager te gebruiken.

Wanneer u integreert met vRealize Operations Manager, blijft vRealize Automation het model van de applicatie-intentie en de bijbehorende beperkingen volgen om te filteren op doelverdeling. Vervolgens gebruikt deze de vRealize Operations Manager-aanbeveling om op basis van deze resultaten de plaatsing verder te verfijnen.

Bij afwezigheid van een aanbeveling

Als u geavanceerde verdeling van workloads inschakelt en vRealize Operations Manager-analyse geen aanbevelingen heeft, kunt u vRealize Automation configureren om terug te vallen op de standaardverdeling van de applicatie-intentie.

Beperkingen op de verdeling van workloads

Er gelden bepaalde beperkingen bij het gebruik van vRealize Operations Manager om workloads te verdelen.

- vRealize Operations Manager biedt geen ondersteuning voor de verdeling van workloads over resourcepools in vCenter Server.
- Als vRealize Operations Manager inactief is, kan de time-out voor de verdeling van workloads voor het oproepen van vRealize Operations Manager verlopen.
- Plaatsing overschrijdt niet meerdere cloudzones. vRealize Automation verzendt één cloudzone naar vRealize Operations Manager voor aanbevelingen voor plaatsing in die ene cloudzone.

Verdeling van workloads inschakelen

Om de verdeling van workloads in te schakelen, zijn er stappen die u moet uitvoeren voor vSphere, vRealize Operations Manager en vRealize Automation.

- 1 Maak in Cloud Assembly verbinding met uw vCenter Server-cloudaccount.

De opties vindt u onder **Infrastructuur > Verbindingen > Cloudaccounts**.

- 2 Controleer in vCenter Server of DRS-compatibele clusters bestaan en of deze zijn ingesteld op volledig geautomatiseerd.

- 3 Controleer in vRealize Operations Manager of dezelfde vCenter Server wordt beheerd.

U hebt vRealize Operations Manager 8 of hoger nodig.

- 4 Voeg in Cloud Assembly de vRealize Operations Manager-integratie toe.

De opties vindt u onder **Infrastructuur > Verbindingen > Integraties**.

Om de integratie toe te voegen, hebt u de URL van het vRealize Operations Manager-hoofdknooppunt hieronder nodig, evenals de gebruikersnaam en het wachtwoord van de aanmelding.

`https://operations-manager-IP-address-or-FQDN/suite-api`

Nadat u de waarden hebt ingevoerd, klikt u op **VALIDEREN**.

- 5 Synchroniseer de integratie met de vCenter Server door op **SYNCHRONISEREN** te klikken.

Synchroniseer ook elke keer dat Cloud Assembly en vRealize Operations Manager beginnen met het beheer van een nieuwe vCenter Server.

- 6 Maak in Cloud Assembly een cloudzone voor het vCenter Server-account.

De opties vindt u onder **Infrastructuur > Configureren > Cloudzones**.

- 7 Op het tabblad Samenvatting van de cloudzone stelt u het plaatsingsbeleid in op GEAVANCEERD.
- 8 Selecteer onder het plaatsingsbeleid of vRealize Automation moet terugvallen op de standaardplaatsing als vRealize Operations Manager geen aanbevelingen retourneert.

Problemen met verdeling van workloads oplossen

Als vRealize Operations Manager de verdeling van workloads niet zoals verwacht aanbeveelt, controleert u de details van de implementatieaanvraag in Cloud Assembly of vRealize Automation Service Broker.

- 1 Ga naar **Infrastructuur > Activiteit > Aanvragen** en klik op de aanvraag.
- 2 Bekijk de toewijzingsfasen in de details van de aanvraag.
Zoek naar doelen die met of zonder succes zijn geïdentificeerd.
- 3 Schakel Dev-modus in in de details van de aanvraag in de rechterbovenhoek.
- 4 Volg het aanvraagpad om filterblokken te vinden.
- 5 Klik op een filterblok en bekijk de volgende sectie.

```
filterName: ComputePlacementPolicyAffinityHostFilter
  v computeLinksBefore
  v computeLinksAfter
  v filteredOutHostsReasons
```

Invoer	Beschrijving
computeLinksBefore	Lijst met mogelijke hosts voor verdeling op basis van vRealize Automation-algoritmen.
computeLinksAfter	Geselecteerde host voor verdeling.
filteredOutHostsReasons	Berichten waarin wordt uitgelegd waarom een host is geselecteerd of geweigerd. Wanneer vRealize Operations Manager de host selecteert, wordt het volgende bericht weergegeven. advance policy filter: Filtered hosts based on recommendation from vROPS.

Meer informatie over verdeling van workloads

Om de beste infrastructuur te vinden waarop een implementatie kan worden geplaatst, neemt vRealize Automation verschillende filterbeslissingen. vRealize Automation-integratie met vRealize Operations Manager kan de beslissing over de verdeling verder verfijnen.

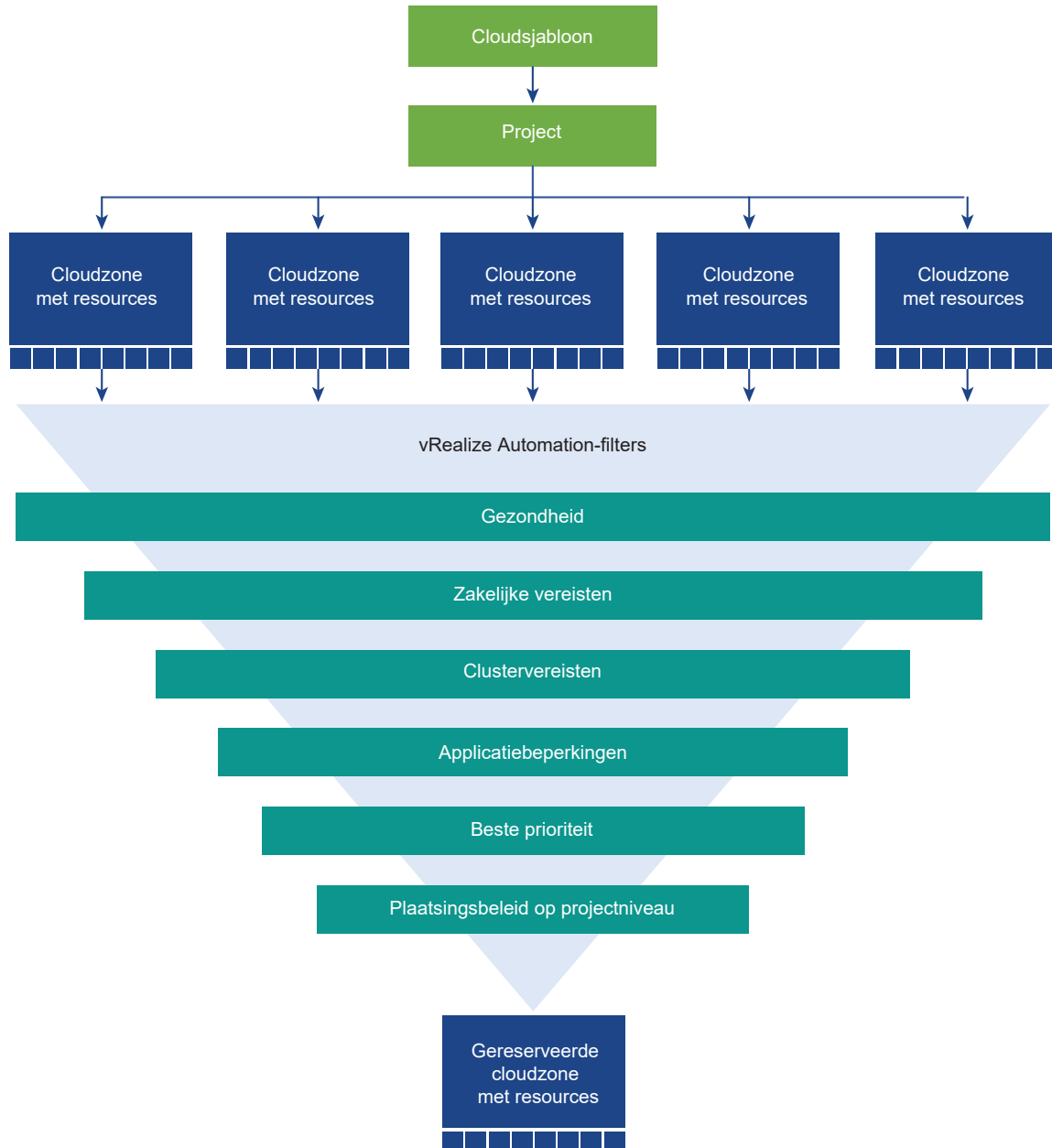
vRealize Operations Manager kan helpen bij de optimale verdeling van workloads, mits u de optie Geavanceerd plaatsingsbeleid in uw vSphere-gebaseerde cloudzones heeft ingeschakeld.

Daarnaast moeten de vSphere-cloudaccounts voor de cloudzones worden beheerd door vRealize Operations Manager.

Fase 1: Reservering

Opmerking Hoewel de naam identiek is, is de reservering niet gerelateerd aan de vRealize Automation 7-reserveringsfunctie.

De vRealize Automation-reserveringsfase is hetzelfde, ongeacht of u geavanceerde plaatsing met vRealize Operations Manager inschakelt.



- 1 Reservering begint met een cloudsjabloon die aan een project is gekoppeld. Dat project is op zijn beurt gekoppeld aan cloudzones.
- 2 De cloudzones bestaan uit computerbronhosts, pools en clusters en gekoppelde opslag.

In eerste instantie kan elke cloudzone in het project een mogelijk plaatsingsdoel zijn.

- 3 vRealize Automation filtert cloudzones die onvoldoende gezonde resources voor de implementatie hebben.

Als bijvoorbeeld te veel resources zijn uitgeschakeld of in onderhoud zijn, wordt die cloudzone gefilterd.

- 4 vRealize Automation filtert cloudzones die niet aan de bedrijfsvereisten kunnen voldoen.

De implementatie kan bijvoorbeeld een prijs- of budgetlimiet voor de zone overschrijden.

- 5 vRealize Automation filtert cloudzones die niet aan de clustervereisten kunnen voldoen.

De resources van de cloudzone kunnen bijvoorbeeld CPU- of geheugengebruikslimieten hebben die te laag zijn voor de implementatie.

- 6 vRealize Automation filtert cloudzones die geen affiniteit met applicatiebeperkingen hebben.

Affiniteit vereist dat beperkingstags voor cloudsjabloon of op projectniveau overeenkomen met capaciteitstags die ergens in de resources van de cloudzone zijn gevonden.

Als de cloudsjabloon of het project bijvoorbeeld een opslagbeperking heeft om opslag te gebruiken met de tag `pci`, wordt een cloudzone gefilterd waarin geen van de opslagresources die capaciteitstag heeft.

- 7 vRealize Automation selecteert cloudzones met de beste inrichtingsprioriteit.

- 8 Als het plaatsingsbeleid op projectniveau anders is dan Standaard, selecteert vRealize Automation een cloudzone die het niet-standaardplaatsingsbeleid ondersteunt.

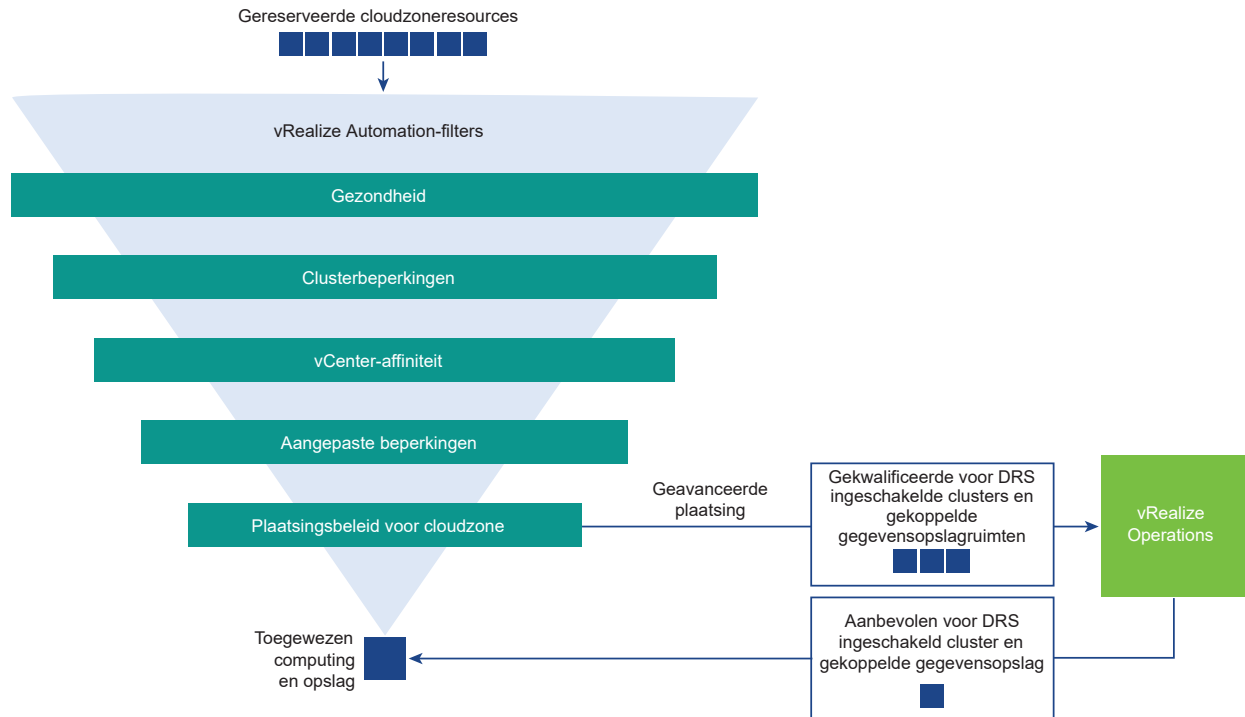
In deze release is Verspreid de enige niet-standaardwaarde. Verspreid verdeelt de workload door de cloudzone met de lagere verhouding van virtuele machines tot hosts te selecteren. Met Standaard wordt in de eerste beschikbare zone geïmplementeerd.

Het plaatsingsbeleid van een project is alleen een factor tijdens de fase van de reservering van de cloudzone. Dit heeft geen invloed op, en is niet gerelateerd aan, het plaatsingsbeleid voor cloudzones in de toewijzingsfase.

Wanneer deze is voltooid, selecteert de reserveringsfase één cloudzone en de bijbehorende resources. vRealize Automation reserveert de eerste beschikbare zone die gekwalificeerd is na het voldoen aan de voorgaande filters.

Fase 2: Toewijzing

vRealize Automation controleert de gereserveerde computerbronnen voor de cloudzone en gekoppelde opslag.



- 1 In de cloudzone filtert vRealize Automation resources die de onderhoudsstatus of uitgeschakelde status hebben.

Houd er rekening mee dat er nog steeds voldoende gezonde resources zijn voor de implementatie. Anders zou de hele cloudzone zijn gefilterd tijdens de reserveringsfase.

- 2 vRealize Automation filtert resources die niet overeenkomen met beperkingen op clusterniveau in de cloudsjabloon of het project.

Een resource in de cloudzone kan bijvoorbeeld worden getagd met `test` onder **Infrastructuur > Resources > Berekenen**.

Als de cloudsjabloon of het project een beperkingstag voor gebruik van een `dev`-resource heeft, wordt de `test`-resource gefilterd.

Daarnaast kunnen opslag- of netwerkprofielen in de cloudzone op manieren worden getagd die niet overeenkomen met opslagbeperkingen op clusterniveau of netwerkbeperkingen in de cloudsjabloon of het project.

- 3 vRealize Automation filtert resources op basis van affiniteitsinstellingen die in vCenter zijn gedefinieerd.

Er kan bijvoorbeeld een regel in vCenter zijn waarbij de aanwezigheid van een virtuele machine in één cluster kan voorkomen dat een ander cluster wordt gebruikt.

- 4 vRealize Automation filtert resources die niet overeenkomen met resterende aangepaste beperkingen in de cloudsjabloon of het project.

Als de cloudsjabloon bijvoorbeeld een beperking voor het gebruik van een met `ubuntu` getagde image bevat, wordt een cloudzone gefilterd waarin geen van de imagetoewijzingen is getagd met `ubuntu`.

- 5 vRealize Automation zoekt naar de best mogelijke computerbron en opslag in overeenstemming met het plaatsingsbeleid voor de cloudzone.

vRealize Automation schakelt vRealize Operations Manager alleen in wanneer aan de volgende twee voorwaarden wordt voldaan:

- Het plaatsingsbeleid voor de cloudzone is ingesteld op Geavanceerd.
- Na het filteren via stap 4 blijven ten minste één DRS-cluster en de opslag die hieraan is gekoppeld, gekwalificeerd.

Anders gaat vRealize Automation verder met een eigen plaatsingsalgoritme zonder invoer van vRealize Operations Manager.

Aanbeveling voor vRealize Operations Manager-plaatsing

Indien gekwalificeerd voor invoer van vRealize Operations Manager, neemt vRealize Automation contact op met vRealize Operations Manager voor een aanbeveling voor de best mogelijke computerbron en opslag voor de implementatie. vRealize Automation verzendt de volgende gegevens naar vRealize Operations Manager:

- De gekwalificeerde DRS-doelclusters en hun gekoppelde gegevensopslagruimten of gegevensopslagcluster
- Het aantal resources of de clustergrootte van de implementatie
- CPU- en geheugenvereisten voor de virtuele machines in de implementatie
- Schijfvereisten voor de virtual machines in de implementatie

Als vRealize Operations Manager vanuit de gekwalificeerde doelen een optimale plaatsing voor elk van de virtuele machines kan retourneren, wijst vRealize Automation computerbronnen en opslag toe op basis van de aanbeveling van vRealize Operations Manager.

Raadpleeg de [documentatie voor vRealize Operations](#) voor meer informatie over hoe vRealize Operations Manager workloads afhandelt.

Als vRealize Operations Manager geen aanbeveling kan vinden of vRealize Automation geen DRS-cluster en opslag kan vinden, controleert vRealize Automation de terugvalinstelling van de cloudzone:

- Met terugval
vRealize Automation wijst computerbronnen en opslag toe die nog steeds gekwalificeerd zijn, zelfs zonder aanbeveling van vRealize Operations Manager.
- Zonder terugval
vRealize Automation annuleert de aanvraag en gaat niet verder met de inrichting.

Fase 3: Inrichting

vRealize Automation implementeert de virtuele machines, de opslag en het netwerk die zijn aangevraagd via de adapter voor het plaatsingsdoel dat aan het eind van de toewijzingsfase is geselecteerd.

Het plaatsingsdoel bestaat uit computerhosts, clusters of resourcepools en gekoppelde gegevensopslag of gegevensopslagcluster.

Continue optimalisatie met behulp van vRealize Operations Manager

Wanneer u de vRealize Automation-adapter toevoegt in vRealize Operations Manager, maakt vRealize Operations Manager automatisch een nieuw aangepast datacenter (CDC) voor vRealize Automation-workloads.

Met continue optimalisatie beschikt u over de mogelijkheid om workloads anders te verdelen en te verplaatsen en kunt u vRealize Automation met vRealize Operations Manager gebruiken voor meer dan alleen de initiële verdeling van workloads. Wanneer virtualisatieresources worden verplaatst of zwaarder of lichter worden belast, kan vRealize Automation ingerichte workloads indien nodig verdelen.

- De continue optimalisatie maakt automatisch een nieuw CDC in vRealize Operations Manager. Er is één nieuw CDC voor elke vRealize Automation vSphere-cloudzone.
- Het nieuwe CDC bevat elk beheerd vRealize Automation-cluster dat is gekoppeld aan de cloudzone.

Opmerking Maak niet handmatig een gemengd CDC van vRealize Automation- en niet-vRealize Automation-clusters.

- U gebruikt vRealize Operations Manager om continue optimalisatie uit te voeren voor de nieuw gemaakte CDC op basis van vRealize Automation.
- Workloads kunnen alleen worden geherbalanceerd of verplaatst binnen dezelfde cloudzone of hetzelfde CDC.
- Bij optimalisatie wordt nooit een nieuwe vRealize Automation- of vRealize Operations Manager-verplaatsingsovertreding gemaakt.
 - Als u bestaande verplaatsingsovertredingen hebt, kan optimalisatie operationele-intentieproblemen in vRealize Operations Manager oplossen.
 - Als u bestaande verplaatsingsovertredingen hebt, kan optimalisatie geen bedrijfsintentieproblemen in vRealize Operations Manager oplossen.

Als u bijvoorbeeld vRealize Operations Manager hebt gebruikt om een virtuele machine handmatig te verplaatsen naar een cluster dat uw beperkingen niet ondersteunt, kan vRealize Operations Manager geen overtreding detecteren of het probleem niet proberen op te lossen.
- Deze release voldoet aan de operationele intentie op het niveau van het CDC. 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-CDC's, gekoppeld aan afzonderlijke vSphere-cloudzones. U kunt bijvoorbeeld verschillende test- en productieclusters instellen.

- Tijdens alle optimalisatieherbalancerings- of verplaatsingsbewerkingen wordt voldaan aan de vRealize Automation-applicatie-intentie en de beperkingen die zijn gedefinieerd in vRealize Automation.
- Plaatsingstags van vRealize Operations Manager kunnen niet worden toegepast op ingerichte vRealize Automation-workloads.

Verder wordt geplande optimalisatie met meerdere machines ondersteund. Regelmatig 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.

Continue optimalisatie inschakelen

Wanneer u de vRealize Automation-adapter toevoegt in vRealize Operations Manager, maakt vRealize Operations Manager automatisch een nieuw, apart datacenter voor vRealize Automation-gebaseerde workloads.

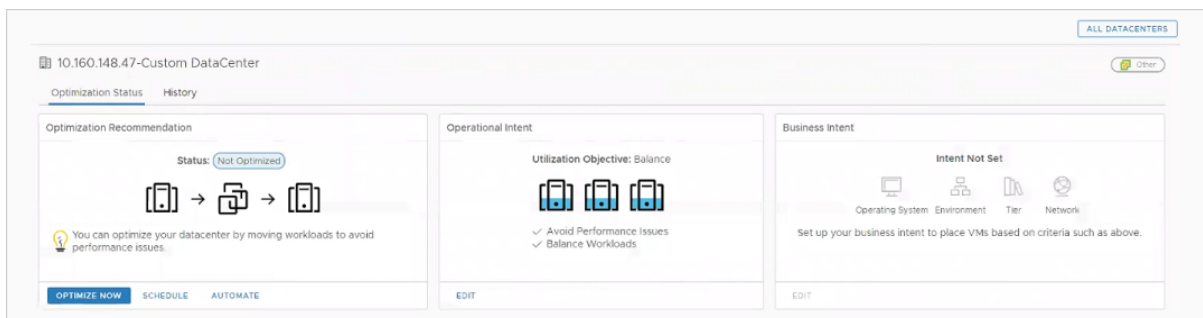
Behalve het toevoegen van de integratie in Cloud Assembly zijn geen afzonderlijke installatiestappen vereist voor continue optimalisatie. U kunt beginnen met het configureren en gebruiken van vRealize Operations Manager voor het verplaatsen van workloads in het nieuwe datacenter. Zie [Voorbeeld van continue optimalisatie](#).

Voorbeeld van continue optimalisatie

Het volgende voorbeeld toont een herbalanceringswerkstroom voor continue optimalisatie van vRealize Automation met vRealize Operations Manager.

- 1 Klik op de startpagina van vRealize Operations Manager op **Workloadoptimalisatie**.
- 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, dat wordt uitgeschakeld 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 bewerking in behandeling in vRealize Automation door op **Resources > 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 herbalancering 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.

The screenshot shows the 'Optimization Status' page in vRealize Operations Manager. The status is 'Optimized' with a green smiley face icon. Below the status, it says 'Your workloads are optimized according to your settings.' There are three buttons: 'OPTIMIZE NOW', 'SCHEDULE', and 'AUTOMATE'. To the right, there are two sections: 'Operational Intent' and 'Business Intent'. The 'Operational Intent' section shows 'Utilization Objective: Balance' with three server icons and two checkmarks: 'Avoid Performance Issues' and 'Balance Workloads'. The 'Business Intent' section shows 'Intent Not Set' with icons for Operating System, Environment, Tier, and Network, and a note: 'Set up your business intent to place VMs based on criteria such as above.' There is an 'EDIT' button at the bottom of the Business Intent section.

U kunt de bewerking in vRealize Operations Manager bekijken door te klikken op **Beheer > Geschiedenis > Recente taken**.

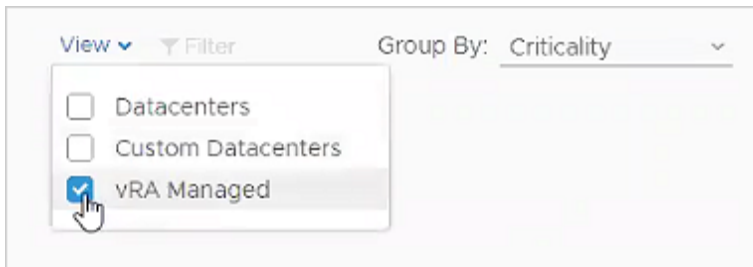
Beheerde vRealize Automation-datacenters zoeken

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 **Workloadoptimalisatie**.
- 2 Klik rechtsboven op het vervolgkeuzemenu **Weergeven**.

- 3 Selecteer alleen de beheerde vRealize Automation-datacenters.



Implementatiebewaking op basis van vRealize Operations Manager

vRealize Automation kan vRealize Operations Manager-gegevens over uw implementaties tonen.

Door de gefilterde set van statistieken direct in vRealize Automation te bekijken, bespaart u het openen en zoeken van vRealize Operations Manager. 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 vRealize Operations Manager-gegevens alleen weergeven als er specifieke integraties aanwezig zijn. Voor de integraties moet u het adres en de verificatiegegevens voor aanmelden voor vRealize Automation, vRealize Operations Manager en vCenter opgeven.

Procedure

- 1 Ga in vRealize Operations Manager naar **Gegevensbronnen > Integraties** en controleer of voeg uw vCenter-accountintegratie toe.
- 2 Ga in Cloud Assembly naar **Infrastructuur > Verbindingen > Cloudaccounts** en verifieer uw vCenter-account of voeg het toe.

vRealize Operations Manager en vRealize Automation moeten met dezelfde vCenter zijn verbonden.

- 3 Ga in vRealize Operations Manager naar **Gegevensbronnen > Integraties** en voeg de integratie van het vRealize Automation 8.x-adapteraccount toe.
- 4 Ga in Cloud Assembly naar **Infrastructuur > Verbindingen > Integraties** en voeg de vRealize Operations Manager-integratie toe.

Voer het vRealize Operations Manager-adres in de volgende vorm in:

`https://operations-manager-IP-address-or-FQDN/suite-api`

Zie [Integreren met vRealize Operations Manager](#) voor meer achtergrondinformatie.

Wat nu te doen

Klik in Cloud Assembly op **Resources > Implementaties**, selecteer een implementatie op uw vCenter en controleer of het tabblad Controleren wordt weergegeven.

Status en waarschuwingen van vRealize Operations Manager

Wanneer de controle is ingeschakeld, haalt vRealize Automation status- en bijbehorende waarschuwingen van vRealize Operations Manager over uw implementaties op.

U opent de controle door op een implementatie te klikken en het tabblad **Controleren** te selecteren. Zie [vRealize Operations Manager-gegevens inschakelen](#) als dit tabblad ontbreekt.

Markeer de implementatienaam bovenaan de onderdelenstructuur in het linkerpaneel 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 statusbadges en statuswaarschuwingen worden weergegeven. Andere typen waarschuwingen bijvoorbeeld over efficiëntie of risico's worden niet ondersteund.

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 **Controleren** te selecteren. Zie [vRealize Operations Manager-gegevens inschakelen](#) als dit tabblad ontbreekt.

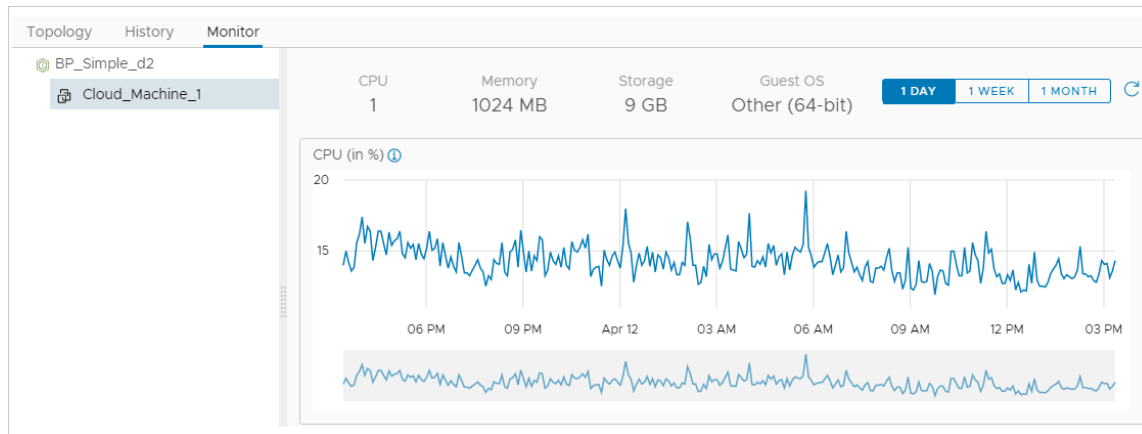
Vouw de onderdelenstructuur aan de linkerzijde uit en markeer een virtuele machine om statistieken weer te geven.

- Statistieken worden niet in de cache opgeslagen. Ze zijn rechtstreeks afkomstig van vRealize Operations Manager en het kan even duren om ze te laden.
- Alleen statistieken van virtuele machines worden weergegeven. Statistieken van andere onderdelen, zoals vCloud Director, Software of XaaS, worden niet ondersteund.
- Alleen statistieken van virtuele vSphere-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 weergegeven, klikt u op het blauwe informatiepictogram in de linkerbovenhoek van de tijdlijn.

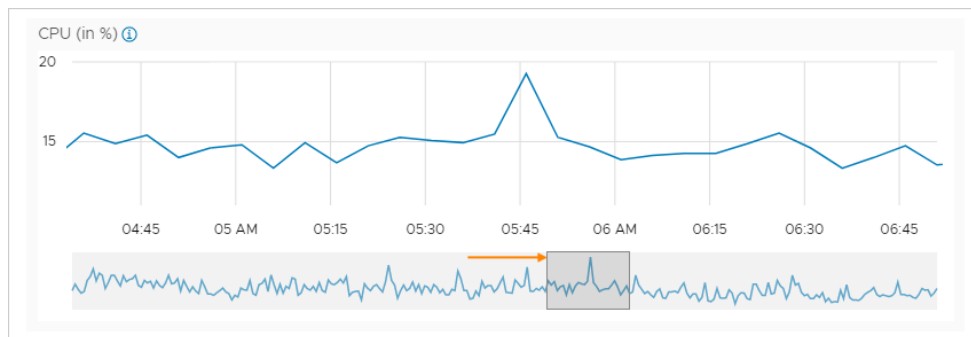


Maatregelen nemen op basis van door vRealize Operations Manager verstrekte gegevens

Wanneer de statistieken van vRealize Operations Manager een probleem onthullen, kunt u probleemgebieden direct in vRealize Automation identificeren.

Als u door vRealize Operations Manager verstrekte statistieken wilt bekijken, klikt u op een implementatie en selecteert u het tabblad **Controleren**. Zie [vRealize Operations Manager-gegevens inschakelen](#) als dit tabblad ontbreekt.

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, grijze gedeelte onder de tijdlijn van een statistiek:



Resourcebeheer en implementatieoptimalisatie met vRealize Operations Manager-statistieken in vRealize Automation

In een geïntegreerde vRealize Automation- en vRealize Operations Manager-omgeving hebt u toegang tot inzichten en waarschuwingen voor vRealize Automation-objecten die worden bewaakt door vRealize Operations Manager.

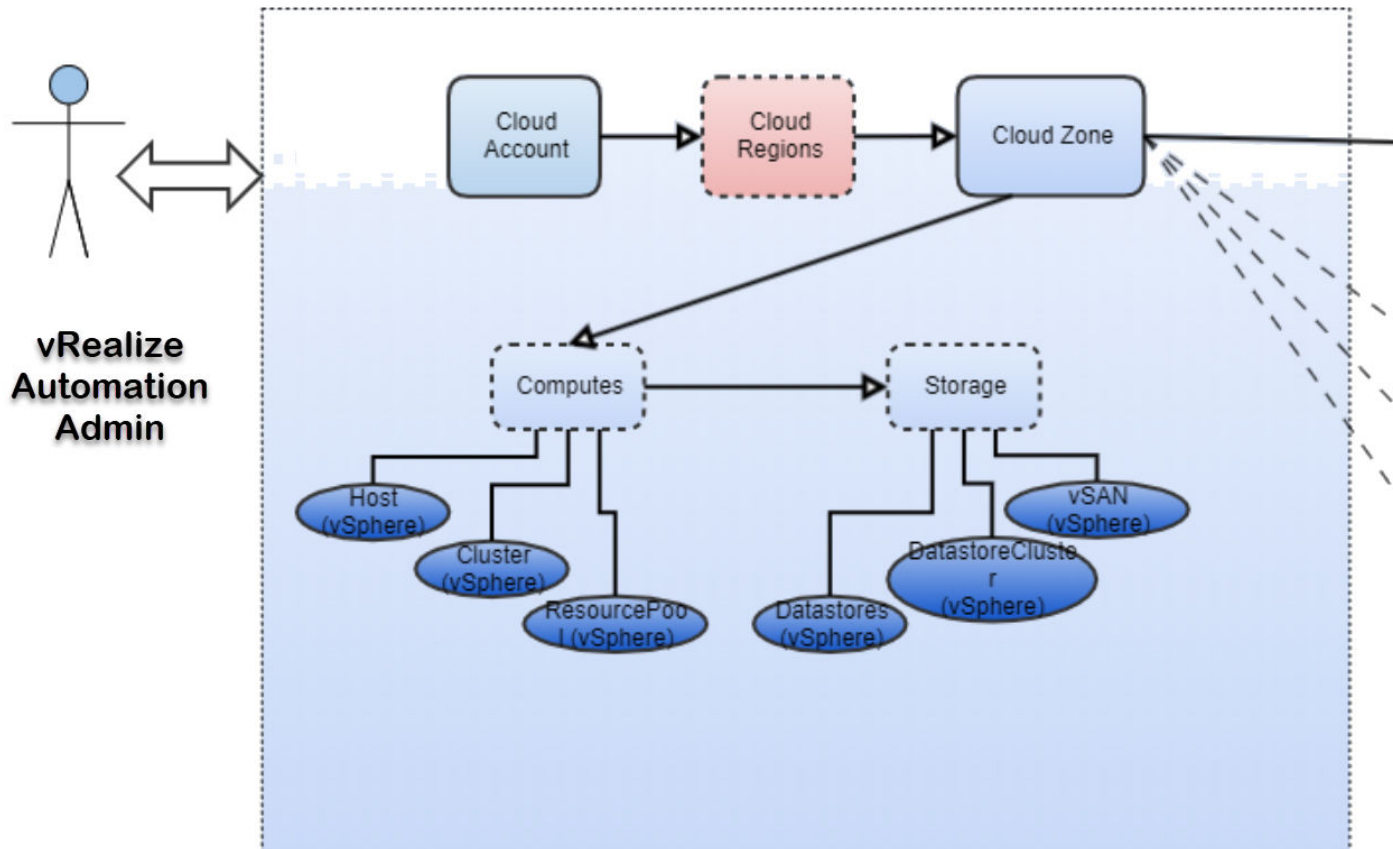
Het dashboard **Inzichten** en de tabbladen **Waarschuwingen** bieden de realtimecapaciteit en gerelateerde informatie over het feit dat u beheerbeslissingen in vRealize Automation moet nemen zonder dat u vRealize Operations Manager hoeft te openen. De informatie wordt verstrekt door de gekoppelde vRealize Operations Manager-applicatie.

Werken met het dashboard Inzichten en met resourcewaarschuwingen

Het dashboard **Inzichten** biedt informatie over capaciteitsverbruik voor alle berekeningen in de cloudzone en gegroepeerd per project. Het kan ook projectimplementaties tonen die optimalisatie nodig hebben.

De pagina's **Waarschuwingen** geven potentiële capaciteits- en prestatieproblemen weer voor objecten zoals cloudzones, projecten, implementaties en virtuele machines. Ze bevatten ook informatie voor projecteigenaren, bijvoorbeeld over welke van hun implementaties kunnen worden geoptimaliseerd. Elke implementatiekoppeling opent het tabblad **Optimaliseren** in de implementatie, waar specifieke richtlijnen worden gegeven.

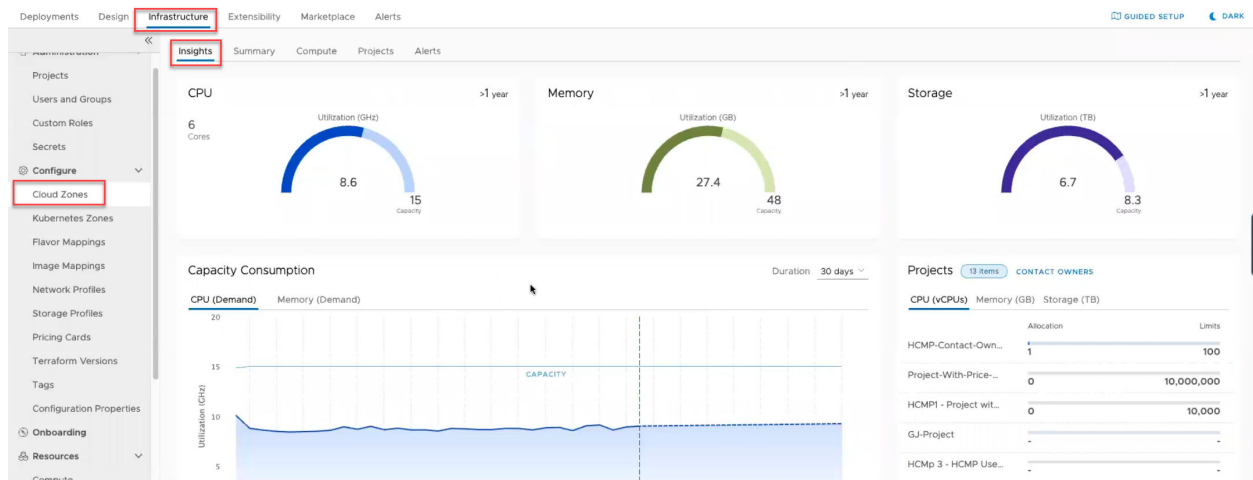
Het volgende diagram illustreert de relatie tussen uw vRealize Automation-resources en -implementaties en de gegevens die de gekoppelde vRealize Operations Manager-applicatie biedt in vRealize Automation.



Werken met het dashboard Inzichten

Het dashboard **Inzichten**, dat beschikbaar is op elke cloudzonepagina, biedt de volgende vRealize Operations Manager-statistieken:

- Gebruik van CPU, geheugen en opslag als percentage van capaciteit
- Samenvatting van capaciteitsverbruik
- De vraag- en gebruiksgeschiedenis van CPU en geheugen
- Verbruik in meerdere projecten
- Terug te winnen resourcecapaciteit, met kostenbesparingen, voor implementaties en projecten in een cloudzone



Het biedt ook een optie om projecteigenaren te waarschuwen voor implementaties die kunnen worden geoptimaliseerd.

Het dashboard **Inzichten** is beschikbaar voor vSphere- en VMware Cloud on AWS-cloudzones, op voorwaarde dat de cloudaccounts worden geconfigureerd in zowel vRealize Automation als vRealize Operations Manager en worden bewaakt in vRealize Operations Manager.

Zie [Het dashboard Inzichten gebruiken om de resourcecapaciteit te bewaken en projecteigenaren op de hoogte te stellen in vRealize Automation](#) voor meer informatie.

Werken met waarschuwingen

De pagina **Waarschuwingen** biedt de volgende filtercategorieën. Filtercategorieën worden geleverd door de bijbehorende vRealize Operations Manager-applicatie.

- Ernst
- Status
- Impact
- Type
- Subtype

■ Resource

Elk filter kan verder worden verfijnd met behulp van snelle filters. Het resourcefilter kan bijvoorbeeld verder worden verfijnd met de typen snelle filters van de cloudzone, de virtuele machine, de implementatie en de projectresource.

U kunt combinaties van filters en snelle filters gebruiken om te bepalen welke waarschuwingen beschikbaar zijn voor weergave.

Deployments Design Infrastructure Extensibility Marketplace Alerts

Resource Type Quick filters

Today

- ☒ Cloud Zone
- ☒ Virtual Machine
- ☐ Deployment
- ☒ Project

Yesterday

Virtual machine is powered off for more than 5 days 4:40 PM

Virtual Machine » Cloud_vSphere_Machine_1-mcm222450-155465769232

Virtual machine is powered off for more than 5 days

Virtual machine is powered off for more than 5 days 4:40 PM

Virtual Machine » Cloud_vSphere_Machine_2-mcm222451-155465774235

Virtual machine is powered off for more than 5 days

AlertDefinition_20571bc0-a68c-477c-bb93-118da83... 1:26 PM

Cloud Zone » sqa-vc65 / Datacenter

AlertDefinition_6b5667f5-eb02-4b2e-bcf9-40cbb2... 1:26 PM

Cloud Zone » sqa-vc67.sqa.local / Datacenter

AlertDefinition_bf5e68e4-28f1-4992-af8d-94ea214ff... 1:26 PM

Cloud Zone » sqa-vc67.sqa.local / Datacenter

Virtual machine is powered off for more than 5 days

Created: Dec 13, 2020, 4:40:46 PM | Updated: Dec 14, 2020, 7:04:47 PM

Virtual Machine » Cloud_vSphere_Machine_1-mcm222450-155465769232

Virtual machine is powered off for more than 5 days

Severity: Warning Status: Active Impact: Health Type: Infrastructure

Suggestions 2 REVIEW DEPLOYMENT

- Delete powered off machines
- Manually power on the virtual machine.

Notes

Leave a note...

ADD NOTE

Sommige **Waarschuwingen** geven informatie over, en een koppeling naar, implementaties die kunnen worden geoptimaliseerd. Een afzonderlijke waarschuwing kan de optie bieden om contact op te nemen met de projecteigenaar, een dashboard Inzichten te onderzoeken of mogelijke acties uit te voeren.

Deployments Design Infrastructure Extensibility Marketplace **Alerts** GUIDED

Severity Quick filters Status: Active X Severity: Critical X

Today

- The project has some deployments t...** 6:17 PM
Project » vc65 project
The project has some deployments that contain optimizable resources.
- Cloud Zone has less than 60 days r...** 11:46 AM
Cloud Zone » sqs-vc67.sqs.local / Datacenter
The time remaining on cloud zone is less than 60 days until capacity demand runs out.

Yesterday

- Cloud Zone has less than 60 days re...** 1:35 PM
Cloud Zone » 测试Zone-g11n
The time remaining on cloud zone is less than 60 days until capacity demand runs out.
- Cloud Zone has less than 60 days re...** 1:35 PM
Cloud Zone » vmc staging-vsphere / SDDC-Datacenter
The time remaining on cloud zone is less than 60 days until capacity demand runs out.
- AlertDefinition_ff4d3d96-fa4f-4022-...** 1:26 PM

The project has some deployments that contain optimizable resources
Created: Dec 14, 2020, 6:17:44 PM | Updated: Dec 14, 2020, 6:17:44 PM
Project » vc65 project

The project has some deployments that contain optimizable resources.

Severity: Critical Status: Active Impact: Efficiency Type: Application Subtype: Performance

Suggestions REVIEW PROJECT

- If the project is experiencing increased provisioning, you can review the project to understand the deployments and poweroff/delete the ones that are no longer in use.

Deployments to review

Name	Owner
contact-owner-test-dep-2	

Items per page 10

Notes

Investigating

ADD NOTE

Waarschuwingen zijn momenteel beschikbaar voor vSphere- en VMware Cloud on AWS-resourceobjecten.

Zie [Waarschuwingen gebruiken om de resourcecapaciteit, prestaties en beschikbaarheid in vRealize Automation te beheren](#) en [Waarschuwingen gebruiken om implementaties in vRealize Automation te optimaliseren](#) voor meer informatie over het configureren en gebruiken van geïntegreerde waarschuwingen.

Wat zijn onboardingplannen in Cloud Assembly


U gebruikt een onboardingplan voor de workload om machines te identificeren waarvoor gegevens zijn verzameld van een cloudaccounttype in een doelgebied of datacenter, maar die nog niet door een Cloud Assembly-project worden beheerd.

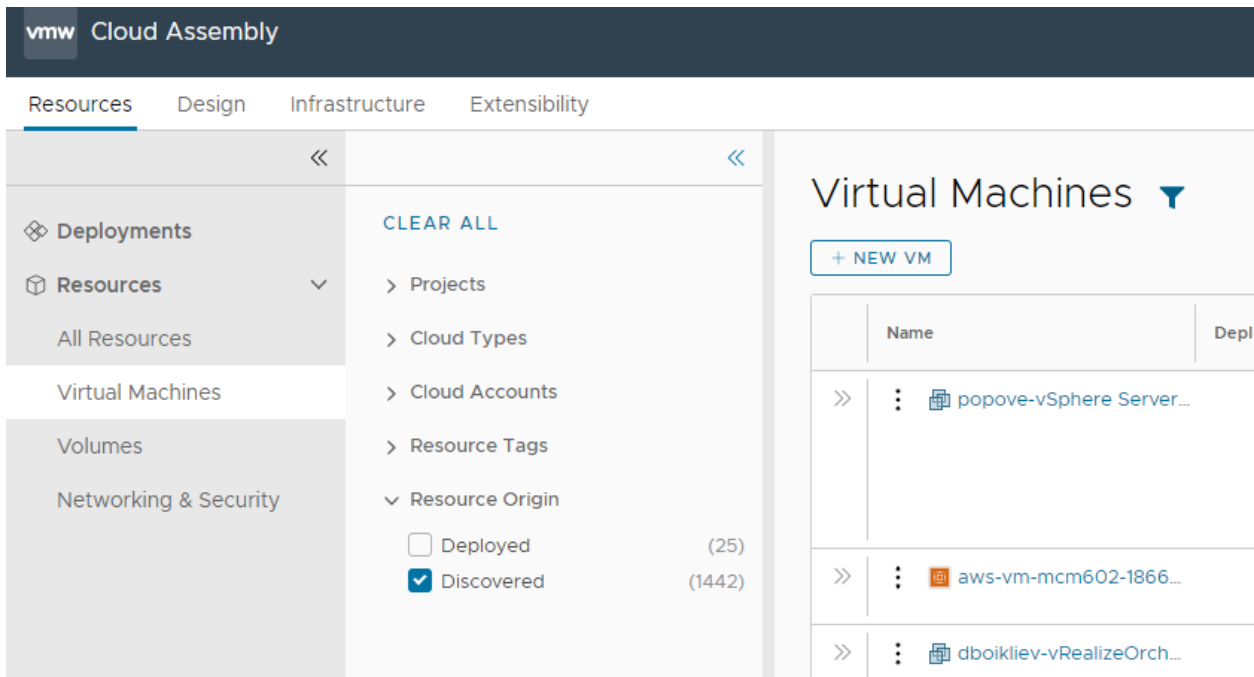
Wanneer u een cloudaccount toevoegt dat machines bevat die buiten Cloud Assembly zijn geïmplementeerd, worden de machines niet door Cloud Assembly beheerd totdat u ze onboardt. Gebruik een onboardingplan om onbeheerde machines onder beheer van Cloud Assembly te brengen. U maakt een plan, vult het met machines en voert vervolgens het plan uit om de machines te importeren. Met behulp van het onboardingplan kunt u een cloudsjabloon maken en ook een of meer implementaties maken.

U kunt een of meer onbeheerde machines op één plan onboarden door machines handmatig te selecteren.

- U kunt maximaal 3.500 onbeheerde machines in één onboarding-plan per uur onboarden.
- U kunt maximaal 17.000 onbeheerde machines gelijktijdig in meerdere onboarding-plannen per uur onboarden.

Resources die beschikbaar zijn voor onboarding van de workload, worden weergegeven op de pagina **Resources > Resource > Virtuele machines** en hebben het label *Discovered* in de kolom Afkomst. Alleen machines waarvan gegevens zijn verzameld, worden weergegeven. Nadat u de machines heeft geonboard, worden deze als *Deployed* in de kolom Afkomst weergegeven. U kunt

filteren op gedetecteerde of geïmplementeerde machines door op het filterpictogram  te klikken.



The screenshot shows the VMware Cloud Assembly interface. The top navigation bar includes 'Resources', 'Design', 'Infrastructure', and 'Extensibility'. The 'Resources' section is active, showing a list of resources. On the right, the 'Virtual Machines' section is expanded, displaying a table with columns for 'Name' and 'Depl'. The table lists three virtual machines: 'popove-vSphere Server...', 'aws-vm-mcm602-1866...', and 'dboikliev-vRealizeOrch...'. The 'Discovered' filter is selected, showing 1442 machines.

De persoon die het onboardingplan voor workloads uitvoert, wordt automatisch als eigenaar van de machine toegewezen.

Onboarding ondersteunt ook aangepaste eigenschappen voor onboarding, gekoppelde schijven, het wijzigen van implementatie-eigenaren en vSphere-netwerken.

- Aangepaste eigenschappen - U kunt aangepaste eigenschappen instellen op het plan en op de afzonderlijke machineniveaus. Een aangepaste eigenschap die op machineniveau is ingesteld, overschrijft dezelfde eigenschap op planniveau.
- Gekoppelde schijven - Als een machine niet-opstartbare schijven heeft, worden ze automatisch geonboard met de bovenliggende machine. Als u niet-opstartbare schijven wilt weergeven, klikt u op de machinenaam in het plan en navigeert u vervolgens naar het tabblad **Opslag**.

- Implementatie-eigendom - Met onboarding kunt u de standaard eigenaar voor de implementatie wijzigen. Als u de eigenaar wilt wijzigen, selecteert u een implementatie op het tabblad **Implementatie**, klikt u op **Acties > Eigenaar wijzigen**, en selecteert u de gewenste gebruiker die aan het project is gekoppeld.

Voorbeelden van onboarding

Zie [Voorbeeld: geselecteerde machines als één implementatie in Cloud Assembly onboarden](#) voor voorbeelden van onboardingstechnieken.

Abonnementen op onboardinggebeurtenissen

Er wordt een `Deployment Onboarded`-gebeurtenis gemaakt wanneer u het plan uitvoert. Via de opties op het tabblad **Uitbreidbaarheid** kunt u zich op deze implementatiegebeurtenissen abonneren en er vervolgens acties op uitvoeren.

Na onboarding kunt u een project bijwerken als actie voor dag 2 voor geonboarde implementaties. Als u de actie **Project wijzigen** wilt gebruiken, moet het doelproject dezelfde cloudzoneresources gebruiken als de implementatie. U kunt de actie **Project wijzigen** niet uitvoeren op geonboarde implementaties waarin u wijzigingen hebt aangebracht na de onboarding.

Voorbeeld: geselecteerde machines als één implementatie in Cloud Assembly onboarden

In dit voorbeeld onboordt u twee niet-beheerde machines als één implementatie van Cloud Assembly en maakt u één cloudsjabloon voor alle machines in het plan.

Wanneer u een cloudaccount maakt, worden de gegevens van alle machines die eraan zijn gekoppeld, verzameld en vervolgens weergegeven op de pagina **Resources > Resources > Virtuele machines**. Als het cloudaccount machines heeft die buiten Cloud Assembly zijn geïmplementeerd, kunt u een onboarding-plan gebruiken om Cloud Assembly de machine-implementaties te laten beheren.

Opmerking U kunt de naam van implementaties alleen wijzigen voordat ze worden geonboard. Na de onboarding wordt de optie **Naam wijzigen** uitgeschakeld.

Voorwaarden

- Controleer of u de vereiste gebruikersrol hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Bekijk [Wat zijn onboardingplannen in Cloud Assembly](#).
- Maak een Cloud Assembly-project en bereid dit voor.

Deze procedure is van toepassing op een deel van de stappen van het WordPress-basisgebruiksscenario. Zie [Tutorial: Infrastructuur en implementaties met meerdere clouds instellen en testen in Cloud Assembly](#).

- Maak een project, voeg gebruikers toe en wijs gebruikersrollen toe in het project. Zie [Deel 2: het voorbeeld van een Cloud Assembly-project maken](#).
- Maak een Amazon Web Services-cloudaccount voor het project. Zie de sectie over het cloudaccount van het [Deel 1: het voorbeeld van de Cloud Assembly-infrastructuur configureren](#).

Het Amazon Web Services-cloudaccount in deze procedure bevat machines die zijn geïmplementeerd voordat het cloudaccount aan Cloud Assembly is toegevoegd en door een andere applicatie dan Cloud Assembly.

- Controleer of de pagina **Resources > Resources > Virtuele machines** machines bevat om te onboarden. Zie [Resources beheren in Cloud Assembly](#) voor meer informatie.

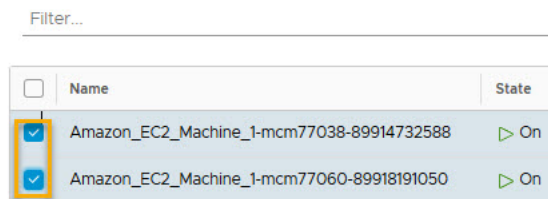
Procedure

- 1 Ga naar **Infrastructuur > Onboarding**.
- 2 Klik op **Nieuw onboardingplan** en voer voorbeeldwaarden in.

Instelling	Voorbeeldwaarde
Naam van plan	VC-sqa-deployments
Beschrijving	Voorbeeld van onboardingplan voor AWS-machine voor OurCo-AWS-cloudaccount
Cloudaccount	OurCo-AWS
Standaardproject	WordPress

- 3 Klik op **Maken**.
- 4 Klik op het tabblad **Implementaties** van het plan op **Machines selecteren**, kies een of meer machines en klik op **OK**.

Select Machines



- 5 Selecteer **Eén planimplementatie maken die alle machines bevat** en klik op **Maken**.
- 6 Klik op het selectievakje naast de nieuwe implementatienaam en klik op **Cloudsjabloon...**

- 7 Klik op **Cloudsjabloon maken in Cloud Assembly-indeling** en voer een cloudsjabloonnaam in, of klik op **Een bestaande cloudsjabloon toewijzen** en selecteer de gewenste cloudsjabloon die u wilt toewijzen.

Opmerking Het toewijzen van cloudsjablonen aan geonboarde implementaties is alleen voor visuele pariteit voor eindconsumenten. Geonboarde implementaties zijn niet compatibel met cloudsjablonen.

8 Klik op **Opslaan**.

Cloud Template Configuration

Mapping of Cloud Templates to onboarded deployments is only for visual parity for end consumers. Onboarded deployments are not compatible with Cloud Templates.

Deployment: Demo

☐ None (use runtime snapshot)
☐ Create Cloud Template in Cloud Assembly format
☒ Assign an existing Cloud Template

	Name	Project	Last Updated
<input checked="" type="radio"/>	Demo	onboarding	Oct 21, 2021, 1:36:15 PM
<input type="radio"/>	171	onboarding	Jun 10, 2021, 8:21:55 AM
<input type="radio"/>	asdf	onboarding	May 25, 2021, 9:24:07 AM
<input type="radio"/>	asdf	onboarding	Dec 7, 2020, 3:03:53 PM

CANCEL SAVE

Opmerking Wanneer uw onboardingplan een vSphere-machine gebruikt, moet u de cloudsjabloon bewerken nadat het onboardingproces is voltooid. Het onboardingproces kan de vSphere-bronmachine en de bijbehorende machinesjabloon niet koppelen en de resulterende cloudsjabloon bevat de `imageRef: "no image available"`-vermelding in de cloudsjablooncode. De cloudsjabloon kan niet worden geïmplementeerd totdat u de juiste sjabloonnaam opgeeft in het veld `imageRef:`. Om het gemakkelijker te maken de blueprint te vinden en bij te werken nadat het onboardingproces is voltooid, gebruikt u de optie **Naam van cloudsjabloon** op de pagina **Configuratie van cloudsjabloon** van de implementatie. Registreer de automatisch gegenereerde cloudsjabloonnaam of voer een cloudsjabloonnaam van uw keuze in en noteer deze. Wanneer het onboardingproces is voltooid, zoekt en opent u de cloudsjabloon en vervangt u de vermelding `"no image available"` in het veld `imageRef:` door de juiste sjabloonnaam.

9 Klik op het selectievakje voor Implementatienaam, klik op **Uitvoeren** en klik vervolgens opnieuw op **Uitvoeren** op de pagina **Plan uitvoeren**.

De geselecteerde machines worden als één implementatie geonboard, met een bijbehorende cloudsjabloon.

- 10 Open en onderzoek de cloudsjabloon door op de pagina **Ontwerp > Cloudsjablonen** te klikken en vervolgens op de naam van de cloudsjabloon te klikken.
- 11 Open en onderzoek de implementatie door op de pagina **Resources > Implementaties** te klikken en vervolgens op de naam van de implementatie te klikken.

Geavanceerde configuratie voor Cloud Assembly-omgeving

U kunt uw Cloud Assembly-omgeving configureren voor verdere ondersteuning van de projectconfiguratie, integratie en implementatie.

Voor gerelateerde en aanvullende informatie over beheermethoden, zoals het gebruik van gebruikers en logboeken en het toevoegen of verlaten van het programma voor klantenervaring, raadpleegt u de Help-documentatie [vRealize Automation beheren](#).

Hoe configureer ik een internetproxyserver voor vRealize Automation

Voor vRealize Automation-installaties in geïsoleerde netwerken zonder directe internettoegang kunt u een internetproxyserver gebruiken om de functionaliteit Internet via proxy toe te staan. De internetproxyserver ondersteunt HTTP en HTTPS.

Als u openbare cloudproviders zoals Amazon Web Services (AWS), Microsoft Azure en Google Cloud Platform (GCP) evenals externe integratiepunten, zoals IPAM, Ansible en Puppet, met vRealize Automation wilt configureren en gebruiken, moet u een internetproxyserver configureren om toegang te krijgen tot de interne vRealize Automation-internetproxyserver.

vRealize Automation bevat een interne proxyserver die communiceert met uw internetproxyserver. Deze server communiceert met uw proxyserver als deze is geconfigureerd met de opdracht `vracli proxy set` Als u geen internetproxyserver hebt geconfigureerd voor uw organisatie, probeert de interne vRealize Automation-proxyserver direct verbinding te maken met internet.

U kunt vRealize Automation instellen om een internetproxyserver te gebruiken door het meegeleverde opdrachtregelprogramma `vracli` te gebruiken. Informatie over het gebruik van de `vracli` API is beschikbaar door het argument `--help` op de opdrachtregel `vracli`, bijvoorbeeld `vracli proxy --help`, te gebruiken.

Voor toegang tot de internetproxyserver is gebruik van de ingesloten besturingselementen op locatie voor actiegebaseerde uitbreidbaarheid (ABX) vereist die zijn ingebouwd in vRealize Automation.

Opmerking Toegang tot Workspace ONE Access (eerder VMware Identity Manager genoemd) wordt niet ondersteund door de internetproxy. U kunt de opdracht `vracli set vidm` niet gebruiken om toegang te krijgen tot Workspace ONE Access via de internetproxyserver.

Voor de interne proxyserver is IPv4 als standaard-IP-indeling vereist. Hiervoor zijn geen internetprotocolbeperkingen, verificatie of man-in-the-middle-acties op TLS-certificaatverkeer (HTTPS) vereist.

Voorwaarden

- Controleer of u een bestaande HTTP- of HTTPS-server hebt, die u kunt gebruiken als internetproxyserver, in het vRealize Automation-netwerk waarmee uitgaand verkeer naar externe sites kan worden doorgegeven. De verbinding moet worden geconfigureerd voor IPv4.
- Controleer of de doelinternetproxyserver is geconfigureerd om IPv4 als standaard-IP-indeling te ondersteunen en niet IPv6.
- Als de internetproxyserver gebruikmaakt van TLS en een HTTPS-verbinding met clients vereist, moet u het servercertificaat importeren met een van de volgende opdrachten, voordat u de proxyconfiguratie instelt.

```
■ vracli certificate proxy --set path_to_proxy_certificate.pem
```

```
■ vracli certificate proxy --set stdin
```

Gebruik de `stdin`-parameter voor interactieve invoer.

Procedure

- 1 Maak een proxyconfiguratie voor de pods of containers die worden gebruikt door Kubernetes. In dit voorbeeld is de proxyserver toegankelijk via het HTTP-schema.

```
vracli proxy set --host http://proxy.vmware.com:3128
```

- 2 Geef de proxyconfiguratie weer.

```
vracli proxy show
```

Het resultaat is vergelijkbaar met:

```
{
  "enabled": true,
  "host": "10.244.4.51",
  "java-proxy-exclude": ".*local|*.localdomain|localhost|10.244.*|
192.168.*|172.16.*|kubernetes|sc2-rdops-vm06-dhcp-198-120.eng.vmware.com|10.192.204.9|
*.eng.vmware.com|sc2-rdops-vm06-dhcp-204-9.eng.vmware.com|10.192.213.146|sc2-rdops-vm06-
dhcp-213-146.eng.vmware.com|10.192.213.151|sc2-rdops-vm06-dhcp-213-151.eng.vmware.com",
  "java-user": null,
  "password": null,
  "port": 3128,
  "proxy-
exclude": ".local,.localdomain,localhost,10.244.,192.168.,172.16.,kubernetes,sc2-
rdops-vm06-dhcp-198-120.eng.vmware.com,10.192.204.9,.eng.vmware.com,sc2-
rdops-vm06-dhcp-204-9.eng.vmware.com,10.192.213.146,sc2-rdops-vm06-
dhcp-213-146.eng.vmware.com,10.192.213.151,sc2-rdops-vm06-dhcp-213-151.eng.vmware.com",
  "scheme": "http",
  "upstream_proxy_host": null,
  "upstream_proxy_password_encoded": "",
```

```

    "upstream_proxy_port": null,
    "upstream_proxy_user_encoded": "",
    "user": null,
    "internal.proxy.config": "dns_v4_first on \nhttp_port
0.0.0.0:3128\nlogformat squid %ts.%03tu %6tr %>a %Ss/%03>Hs
%<st %rm %ru %[un %Sh/%<a %mt\naccess_log stdio:/tmp/logger squid\ncoredump_dir /\ncache
deny all \nappend_domain .prelude.svc.cluster.local\nacl mylan src 10.0.0.0/8\nacl mylan
src 127.0.0.0/8\nacl mylan src 192.168.3.0/24\nacl proxy-exclude dstdomain .local\nacl
proxy-exclude dstdomain .localdomain\nacl proxy-exclude dstdomain localhost\nacl
proxy-exclude dstdomain 10.244.\n\nacl proxy-exclude dstdomain 192.168.\n\nacl proxy-exclude
dstdomain 172.16.\n\nacl proxy-exclude dstdomain kubernetes\nacl proxy-exclude dstdomain
10.192.204.9\nacl proxy-exclude dstdomain .eng.vmware.com\nacl proxy-exclude dstdomain
10.192.213.146\nacl proxy-exclude dstdomain 10.192.213.151\nalways_direct allow proxy-
exclude\nhttp_access allow mylan\nhttp_access deny all\n# End autogen configuration\n",
    "internal.proxy.config.type": "default"
}

```

Opmerking Als u een internetproxyserver voor uw organisatie hebt geconfigureerd, wordt "internal.proxy.config.type": "non-default" in het bovenstaande voorbeeld weergegeven in plaats van 'default'. Om veiligheidsredenen wordt het wachtwoord niet weergegeven.

Opmerking Als u de parameter `-proxy-exclude` gebruikt, moet u de standaardwaarden bewerken. Als u bijvoorbeeld `acme.com` wilt toevoegen als domein dat niet toegankelijk is via de internetproxyserver, gebruikt u de volgende stappen:

- a Voer `vracli proxy default-no-proxy` in om de standaarduitsluitingsinstellingen voor proxy's te krijgen. Dit is een lijst met automatisch gegenereerde domeinen en netwerken.
 - b Bewerk de waarde om `.acme.com` toe te voegen.
 - c Voer `vracli proxy set --proxy-exclude ...` in om de configuratie-instellingen bij te werken.
 - d Voer de opdracht `/opt/scripts/deploy.sh` uit om de omgeving opnieuw te implementeren.
-

- 3 (Optioneel) U kunt geen DNS-domeinen, FQDN's en IP-adressen uitsluiten van toegang door de internetproxyserver.

Wijzig altijd de standaardwaarden van de variabele `proxy-exclude` met parameter `--proxy-exclude`. Als u het domein `exclude.vmware.com` wilt toevoegen, gebruikt u eerst de opdracht `vrali proxy show`, kopieert u de variabele `proxy-exclude` en voegt u de domeinwaarde toe met de opdracht `vracli proxy set ...`, zoals u hieronder ziet:

```
vracli proxy set --host http://
proxy.vmware.com:3128 --proxy-exclude "exclude.vmware.com,docker-
registry.prelude.svc.cluster.local,localhost,.local,.cluster.local,10.244.,192.,172.16.,sc-
rdops-vm11-dhcp-75-38.eng.vmware.com,10.161.75.38,.eng.vmware.com"
```

Opmerking Voeg elementen toe aan `proxy-exclude` in plaats van waarden te vervangen. Als u standaardwaarden voor `proxy-exclude` verwijdert, werkt vRealize Automation niet goed. Als dit gebeurt, verwijdert u de proxyconfiguratie en begint u opnieuw.

- 4 Nadat u de internetproxyserver met de opdracht `vracli proxy set ...` hebt ingesteld, kunt u de opdracht `vracli proxy apply` gebruiken om de configuratie van de internetproxyserver bij te werken en de meest recente proxyinstellingen te activeren.
- 5 Als u dit nog niet hebt gedaan, activeert u de scriptwijzigingen door de volgende opdracht uit te voeren:

```
/opt/scripts/deploy.sh
```

- 6 (Optioneel) Configureer zo nodig de proxyserver om externe toegang op poort 22 te ondersteunen.

Om integraties zoals Puppet en Ansible te ondersteunen, moet de proxyserver poort 22 toestaan om toegang te krijgen tot de relevante hosts.

Voorbeeld: Voorbeeld van Squid-configuratie

Als u een Squid-proxy instelt, kunt u (gerelateerd aan stap 1) uw configuratie in `/etc/squid/squid.conf` verfijnen door deze aan het volgende voorbeeld aan te passen:

```
acl localnet src 192.168.11.0/24

acl SSL_ports port 443

acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
```

```

http_access allow !Safe_ports
http_access allow CONNECT !SSL_ports
http_access allow localnet

http_port 0.0.0.0:3128

maximum_object_size 5 GB
cache_dir ufs /var/spool/squid 20000 16 256
coredump_dir /var/spool/squid
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern (Release|Packages(.gz)*)$ 0 20% 2880
refresh_pattern . 0 20% 4320

client_persistent_connections on
server_persistent_connections on

```

Wat kan ik doen met NSX-T-toewijzing aan meerdere vCenters in vRealize Automation

U kunt een NSX-T-cloudaccount koppelen aan een of meer vCenter-cloudaccounts om verschillende implementatiedoelstellingen te ondersteunen.

U kunt hetzelfde bestaande NSX-T-netwerk koppelen aan netwerkprofielen voor verschillende vCenter's en een implementatie inrichten in een vCenter op basis van beperkingen. Hieronder staan enkele voorbeelden:

- Cloudsjablonen die één machine bevatten met meerdere NIC's die hetzelfde netwerkprofiel gebruiken, waarbij dat netwerkprofiel een NSX-T-netwerk bevat dat meerdere vCenter's omvat.
- Cloudsjablonen die een machine bevatten op een *privé*netwerk dat een netwerkprofiel gebruikt met isolatie op basis van subnetten en die een *bestaand* netwerk van NSX-T gebruikt dat meerdere vCenter's omvat.
- Cloudsjablonen die een enkele machine bevatten op een *privé*netwerk dat een netwerkprofiel gebruikt met isolatie op basis van de beveiligingsgroep en dat een NSX-T-netwerk gebruikt dat vCenter's omvat.
- Cloudsjablonen die een enkele machine bevatten op een *geleid* netwerk dat gebruikmaakt van een netwerkprofiel dat een NSX-T-netwerk bevat dat meerdere vCenter's omvat.
- Cloudsjablonen die een load balancer op aanvraag bevatten die is gedefinieerd in een netwerkprofiel waarop de load balancer wordt toegepast op alle vCenter-machines in het netwerk.
- Cloudsjablonen die een netwerk op aanvraag bevatten dat is gedefinieerd in een netwerkprofiel waarop het netwerk op aanvraag wordt gebruikt door alle vCenter's die gebruikmaken van het netwerkprofiel.

- Cloudsjablonen die een beveiligingsgroep op aanvraag bevatten die optioneel firewallregels bevat en waarbij de beveiligingsgroep is gekoppeld aan alle vCenter's op het netwerk.

U kunt de interne of externe vRealize Automation-IPAM configureren op het NSX-T-netwerk en hetzelfde IP-adres delen voor machines die zijn ingericht in verschillende vCenter's.

Als er geen netwerkprofiel in uw systeem is gedefinieerd, kunt u een cloudsjabloon inrichten die meerdere machines bevat op verschillende vCenter's die één *bestaand* NSX-T-netwerk delen.

Wat gebeurt er als ik een NSX-cloudaccountassociatie in vRealize Automation verwijder

Als u een associatie tussen een NSX-cloudaccount en een vCenter-cloudaccount verwijderd, moet u ook de gerelateerde netwerkprofielen bijwerken om de gekoppelde NSX-objecten te verwijderen.

Als u een associatie tussen een NSX-cloudaccount en een vCenter-cloudaccount verwijderd, worden de infrastructuurelementen niet automatisch bijgewerkt door vRealize Automation. U moet uw bestaande netwerkprofielen bijwerken om de gekoppelde NSX-objecten te verwijderen.

De gebruikersinterface bevat informatie om de elementen van het netwerkprofiel als volgt te markeren:

- Als het netwerkprofiel een bestaand netwerk van NSX geselecteerd heeft:
 - Het object is gemarkeerd als *ongeldig* en het bericht *Sommige netwerkobjecten ontbreken of zijn ongeldig* wordt weergegeven.
 - De objecten worden verwijderd wanneer u het netwerkprofiel opslaat.
- Als het netwerkprofiel app-isolatie heeft geconfigureerd, moet u de instellingen voor het Isolatiebeleid bijwerken voordat het netwerkprofiel kan worden opgeslagen.
- Als het netwerkprofiel beveiligingsgroepen of load balancers heeft geselecteerd, worden de objecten verwijderd wanneer u het netwerkprofiel opslaat.

Bestaande implementaties blijven werken zoals ontworpen voor bestaande onderdelen, maar zullen mislukken bij het maken van nieuwe onderdelen, bijvoorbeeld in een uitschaalbewerking.

Als u de associatie opnieuw tot stand brengt, wordt het netwerkprofiel opnieuw ingevuld en functioneren bestaande implementaties zoals ontworpen.

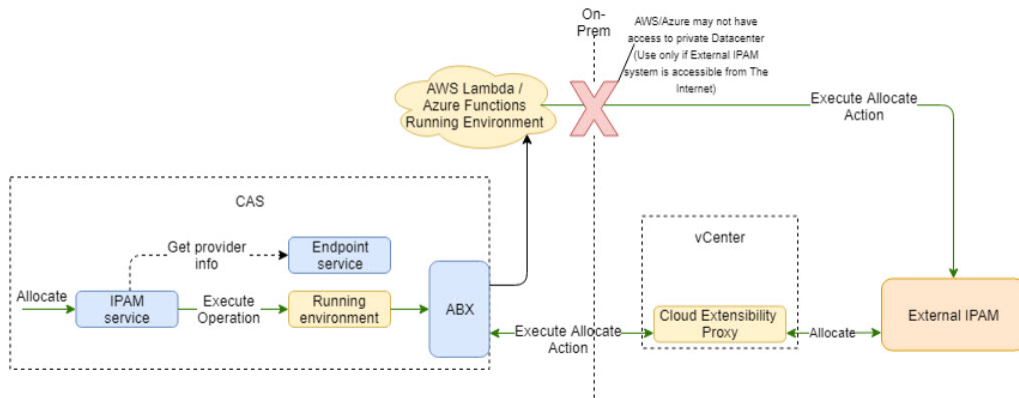
Als u het NSX-cloudaccount verwijderd, is het bovenstaande gedrag hetzelfde, maar worden de netwerkobjecten gemarkeerd als *ontbreekt* in plaats van *ongeldig*.

Hoe kan ik met de IPAM SDK een providerspecifiek extern IPAM-integratiepakket voor vRealize Automation maken

Externe IPAM-leveranciers en -partners kunnen de IPAM SDK downloaden en gebruiken om een IPAM-integratiepakket te maken waarmee vRealize Automation de providerspecifieke IPAM-oplossing kan ondersteunen.

Het proces voor het maken en implementeren van een aangepast IPAM-integratiepakket voor vRealize Automation met behulp van de meegeleverde IPAM SDK wordt beschreven in het document [Creating and Deploying a Provider-specific IPAM Integration Package for VMware Cloud Assembly](#). Zoals beschreven in het document, kunt u de meest recente *VMware vRealize Automation Third-Party IPAM SDK* downloaden van de site [VMware Code](#). De volgende IPAM SDK-pakketten zijn beschikbaar:

- [VMware vRealize Automation Third-Party IPAM SDK 1.1.0](#)
- [VMware vRealize Automation Third-Party IPAM SDK 1.0.0](#)



Voordat u de tijd neemt om een leverancierspecifiek IPAM-integratiepakket te maken met de IPAM SDK, controleert u of er al één bestaat voor vRealize Automation. U kunt zoeken naar een providerspecifiek IPM-integratiepakket op de website van uw IPAM-provider of in de [VMware Marketplace](#).

Hoewel het voorbeeld [Tutorial: Een providerspecifieke externe IPAM-integratie voor vRealize Automation configureren](#) leverancierspecifiek is, bevat het ook nuttige naslaginformatie.

vRealize Automation gebruiken met VMware-oplossing in Azure

Deze procedure beschrijft hoe u vRealize Automation instelt voor gebruik met een hybride selfservicecloudomgeving met een VMware-oplossing in Microsoft Azure, zodat u vRealize Automation-workloads in deze omgeving kunt gebruiken.

vRealize Automation ondersteunt verbindingen met de Azure-VMware-oplossing (AVS) om VMware-workloads te verplaatsen en uit te voeren in een Azure-cloudomgeving. AVS is door Microsoft gemaakt om de interface met VMware-omgevingen te ondersteunen.

Het gebruik van AVS is goed gedocumenteerd door Microsoft. U vindt de documentatie hier:

- Azure VMware Solution - <https://docs.microsoft.com/en-us/azure/azure-vmware/>

Als u AVS in vRealize Automation wilt gebruiken, moet u zowel vCenter- als NSX-T-cloudaccounts instellen. Zie de volgende documentatie voor het instellen van deze cloudaccounts:

- vCenter-cloudaccount instellen - [Een vCenter-cloudaccount maken in vRealize Automation](#)
- Een NSX-T-cloudaccount maken - [Een NSX-T-cloudaccount maken in vRealize Automation](#)

In de volgende procedure worden de stappen op hoog niveau uiteengezet om uw omgeving zo te configureren dat u vRealize Automation-workloads in AVS kunt implementeren.

- 1 Installeer en configureer een VMware-oplossing in Azure op basis van de instructies van de leverancier, zoals gepast voor uw omgeving.
- 2 Maak vCenter- en NSX-T-cloudaccounts in uw vRealize Automation-implementatie.

vRealize Automation gebruiken met Google Cloud VMware Engine

Deze procedure beschrijft hoe u vRealize Automation instelt voor gebruik met een hybride selfservicecloudomgeving met een VMware-oplossing in de Google Cloud, zodat u vRealize Automation-workloads in deze omgevingen kunt gebruiken.

vRealize Automation ondersteunt verbindingen met Google Cloud VMware Engine (GCVE) om VMware-workloads te verplaatsen en in de Google Cloud uit te voeren. GCVE is door Google gemaakt om de interface met VMware-omgevingen te ondersteunen.

Het gebruik van GCVE is goed gedocumenteerd door Google. U vindt de documentatie hier:

- Google Cloud VMware Engine - <https://cloud.google.com/vmware-engine/docs>

Als u GCVE met vRealize Automation wilt gebruiken, moet u zowel vCenter- als NSX-T-cloudaccounts instellen in vRealize Automation. Zie de volgende documentatie voor het instellen van deze cloudaccounts:

- vCenter-cloudaccount instellen - [Een vCenter-cloudaccount maken in vRealize Automation](#)
- Een NSX-T-cloudaccount maken - [Een NSX-T-cloudaccount maken in vRealize Automation](#)

In de volgende procedure worden de stappen op hoog niveau uiteengezet om uw omgeving zo te configureren dat u vRealize Automation-workloads in GCVE kunt implementeren.

- 1 Installeer en configureer Google Cloud VMware Engine op basis van de instructies van de leverancier, zoals gepast voor uw omgeving.
- 2 Maak vCenter- en NSX-T-cloudaccounts in uw vRealize Automation-implementatie.

vRealize Automation gebruiken met de VMware-oplossing in de Oracle Cloud

Deze procedure beschrijft hoe u vRealize Automation instelt voor gebruik met een hybride selfservicecloudomgeving met een VMware-oplossing in de Oracle Cloud, zodat u vRealize Automation-workloads in deze omgevingen kunt gebruiken.

vRealize Automation ondersteunt een verbinding met de VMware-oplossing in de Oracle Cloud (OCVS) om VMware-workloads te verplaatsen en in de Oracle Cloud uit te voeren. OCVS is door Google gemaakt om de interface met VMware-omgevingen te ondersteunen.

Het gebruik van OCVS is goed gedocumenteerd door Google. U vindt de documentatie hier:

- VMware-oplossing in Oracle Cloud - <https://docs.oracle.com/en-us/iaas/Content/VMware/Concepts/ocvsoverview.htm>

Als u OCVS wilt gebruiken, moet u zowel vCenter- als NSX-T-cloudaccounts instellen. Zie de volgende documentatie voor het instellen van deze cloudaccounts:

- vCenter-cloudaccount instellen - [Een vCenter-cloudaccount maken in vRealize Automation](#)
- Een NSX-T-cloudaccount maken - [Een NSX-T-cloudaccount maken in vRealize Automation](#)

In de volgende procedure worden de stappen op hoog niveau uiteengezet om uw omgeving zo te configureren dat u vRealize Automation-workloads in OCVS kunt implementeren.

- 1 Installeer en configureer een VMware-oplossing in de Oracle Cloud op basis van de instructies van de leverancier, zoals gepast voor uw omgeving.
- 2 Maak vCenter- en NSX-T-cloudaccounts in uw vRealize Automation-implementatie.

vRealize Automation gebruiken met VMware Cloud on Dell EMC

Deze procedure beschrijft hoe u vRealize Automation instelt voor gebruik met een hybride selfservicecloudomgeving met VMware Cloud on Dell EMC, zodat u vRealize Automation-workloads in deze omgevingen kunt gebruiken.

vRealize Automation ondersteunt verbinding met VMware Cloud on Dell EMC om VMware-workloads te verplaatsen en uit te voeren.

Raadpleeg de documentatie voor VMware Cloud on Dell EMC op <https://docs.vmware.com/nl/VMware-Cloud-on-Dell-EMC/index.html> voor meer informatie.

Als u vRealize Automation met VMware Cloud on Dell EMC wilt gebruiken, moet u een vCenter-cloudaccount instellen. Zie de volgende documentatie voor het instellen van dit cloudaccount:

- vCenter-cloudaccount instellen - [Een vCenter-cloudaccount maken in vRealize Automation](#)

In de volgende procedure worden de stappen op hoog niveau uiteengezet om uw omgeving zo te configureren dat u vRealize Automation-workloads op VMware Cloud on Dell EMC kunt implementeren.

- 1 Installeer en configureer VMware Cloud on Dell EMC op basis van de instructies van de leverancier, zoals gepast voor uw omgeving.
- 2 Maak een vCenter-cloudaccount in uw vRealize Automation-implementatie.

Uw Cloud Assembly-resource-infrastructuur maken

4

De Cloud Assembly-resource-infrastructuur is de locatie waar u cloudaccountregio's definieert als zones waarin cloudsjablonen en hun workloads kunnen worden geïmplementeerd.

Daarnaast omvat de resource-infrastructuur de aanmaak van algemene toewijzingen van images en machinegrootten, en profielen die netwerk- en opslagmogelijkheden definiëren in cloudaccountregio's of datacenters.

Dit hoofdstuk omvat de volgende onderwerpen:

- Cloudzones toevoegen die doelplaatsingsregio's of datacenters van Cloud Assembly definiëren
- Soorttoewijzingen in vRealize Automation toevoegen om algemene machinegrootten op te geven
- Imagetoewijzingen toevoegen aan vRealize Automation voor toegang tot veelgebruikte besturingssystemen
- Netwerkprofielen toevoegen in vRealize Automation
- Cloud Assembly-opslagprofielen toevoegen die aan verschillende vereisten voldoen
- Prijskaarten gebruiken in vRealize Automation
- Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren
- Werken met resources in vRealize Automation
- Tenantresources voor meerdere providers configureren met vRealize Automation

Cloudzones toevoegen die doelplaatsingsregio's of datacenters van Cloud Assembly definiëren

Een Cloud Assembly-cloudzone is een reeks resources in een cloudaccounttype zoals AWS of vSphere.

Cloudzones in een specifieke accountregio is waar uw cloudsjablonen workloads implementeren. Elke cloudzone is gekoppeld aan een Cloud Assembly-project.

Selecteer **Infrastructuur > Configureren > Cloudzones** en klik op **Nieuwe zone toevoegen**.

Meer informatie over Cloud Assembly-cloudzones

Cloud Assembly-cloudzones zijn secties van computerresources die specifiek zijn voor uw cloudaccounttype, zoals AWS of vSphere.

Cloudzones zijn specifiek voor een regio. U moet deze toewijzen aan een project. Er is een veel-op-veel-relatie tussen cloudzones en projecten. Cloud Assembly ondersteunt de implementatie naar de populairste publieke clouds, waaronder Azure, AWS en GCP, evenals naar vSphere. Zie [Cloudaccounts aan Cloud Assembly toevoegen](#).

Aanvullende plaatsingsbesturingselementen zijn onder meer plaatsingsbeleidsopties, mogelijkheidtags en computertags.

■ Plaatsingsbeleid

Plaatsingsbeleid bepaalt hostselectie voor implementaties binnen de opgegeven cloudzone.

- standaard - Hiermee worden computerresources over clusters en host machines gedistribueerd op basis van beschikbaarheid. Alle machines in een bepaalde implementatie worden bijvoorbeeld op de eerste relevante host ingericht.
- binpack - Plaatst computerresources op de meest belaste host die voldoende beschikbare resources heeft om de gegeven berekening uit te voeren.
- spread - Richt Resources berekenen in, op implementatieniveau, voor de cluster of host met het kleinste aantal virtuele machines. Voor vSphere distribueert Distributed Resource Scheduler (DRS) de virtuele machines over de hosts. Alle aangevraagde machines in een implementatie worden bijvoorbeeld op hetzelfde cluster geplaatst, maar de volgende implementatie kan een ander vSphere-cluster kiezen, afhankelijk van de huidige belasting.

Stel dat u de volgende configuratie hebt:

- DRS-cluster 1 met 5 virtuele machines
- DRS-cluster 2 met 9 virtuele machines
- DRS-cluster 3 met 6 virtuele machines

Als u een cluster van 3 virtuele machines aanvraagt en een Spread-beleid selecteert, moeten deze allemaal op cluster 1 worden geplaatst. De bijgewerkte loads worden 8 virtuele machines voor cluster 1, terwijl de loads voor clusters 2 en 3 op 9 en 6 hetzelfde blijven.

Als u vervolgens 2 extra virtuele machines aanvraagt, worden deze op DRS-cluster 3 geplaatst, die nu 8 virtuele machines heeft. De last voor clusters 1 en 3 blijft op 8 en 9 hetzelfde.

Als twee cloudzones beide voldoen aan alle criteria die nodig zijn voor de inrichting selecteert de plaatsingslogica de locatie met de hoogste prioriteit.

■ Mogelijkheidtags

Blueprints bevatten beperkingstags om de plaatsing van de implementatie te helpen bepalen. Tijdens de implementatie worden de beperkingstags van de blueprint toegewezen aan de overeenkomstige mogelijkheidstags in cloudzones en computerbronnen om te bepalen welke cloudzones beschikbaar zijn voor de plaatsing van VM-resources.

■ Computerbronnen

U kunt de computerresources bekijken en beheren die beschikbaar zijn voor het inrichten van werklasten, zoals AWS-beschikbaarheidszones en vCenter-clusters, op deze cloudzone.

Opmerking Vanaf release vRealize Automation 8.3 delen cloudzones niet langer computerbronnen. Oude cloudzones die gebruikmaken van gedeelde computerbronnen worden nog wel ondersteund, maar gebruikers wordt gevraagd om ze bij te werken zodat ze voldoen aan de huidige standaarden.

Cloudzones die automatisch worden gegenereerd tijdens het maken van het cloudaccount, worden na gegevensverzameling gekoppeld aan de onderliggende computerbronnen.

Als een vCenter-berekeningscluster is ingeschakeld met DRS wordt in de cloudzone alleen het cluster in de lijst met berekeningen weergegeven en worden de onderliggende hosts niet weergegeven. Als een vCenter-computercluster niet voor DRS is ingeschakeld, worden in de cloudzone alleen standalone ESXi-hosts weergegeven, indien aanwezig.

Voeg indien nodig computerresources toe voor de cloudzone. Het tabblad Berekenen bevat een filtermechanisme waarmee u kunt bepalen hoe computerbronnen worden opgenomen in cloudzones. In eerste instantie worden alle beschikbare computerbronnen in de filterselectie opgenomen en in de onderstaande lijst worden alle beschikbare computerbronnen weergegeven die allemaal beschikbaar zijn voor gebruik in implementaties. Er zijn twee extra opties voor het toevoegen van computerresources aan een cloudzone.

- Berekenen handmatig selecteren - Selecteer deze optie als u computerresources handmatig in de lijst wilt selecteren. Nadat u deze heeft geselecteerd, klikt u op Berekening toevoegen om de resources aan de zone toe te voegen. De geselecteerde resources zijn beschikbaar voor gebruik in implementaties.
- Berekeningen dynamisch opnemen op basis van tags - Selecteer deze optie als u computerbronnen wilt insluiten of uitsluiten voor de zone op basis van tags. Alle computerbronnen worden weergegeven totdat u de juiste tags toevoegt die overeenkomen met bestaande tags op computerbronnen. Nadat u een of meer tags hebt toegevoegd, worden computerbronnen met tags die overeenkomen met het filter, opgenomen in de zone en zijn deze beschikbaar voor gebruik in implementaties, terwijl computerbronnen die niet overeenkomen, worden uitgesloten.

Voor beide berekeningsopties kunt u een of meer computerresources verwijderen die op de pagina worden weergegeven door het vakje aan de rechterkant te selecteren en op Verwijderen te klikken.

Computertags helpen om de plaatsing verder te besturen. U kunt tags gebruiken om beschikbare computerbronnen te filteren op alleen die bronnen die overeenkomen met één of meer tags, zoals getoond in de volgende voorbeelden.

- Computerbronnen bevatten geen tags en er wordt geen filter gebruikt.

New Cloud Zone

Summary **Compute** Projects

All compute resources listed apply to this cloud zone. Use the filter to add or remove resources from the list.

Filter tags Enter tags to filter resources ⓘ

⌵ TAGS

<input type="checkbox"/>	Name	Account / region	Type	Tags
<input type="checkbox"/>	us-east-1a	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1b	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1c	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1d	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1e	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1f	Amazon / us-east-1	Availability Zone	

6 computes

- Twee computerbronnen bevatten dezelfde tag, maar er wordt geen filter gebruikt.

New Cloud Zone

Summary **Compute** Projects

All compute resources listed apply to this cloud zone. Use the filter to add or remove resources from the list.

Filter tags Enter tags to filter resources ⓘ

⌵ TAGS

<input type="checkbox"/>	Name	Account / region	Type	Tags
<input type="checkbox"/>	us-east-1a	Amazon / us-east-1	Availability Zone	test.case42
<input type="checkbox"/>	us-east-1b	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1c	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1d	Amazon / us-east-1	Availability Zone	test.case42
<input type="checkbox"/>	us-east-1e	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1f	Amazon / us-east-1	Availability Zone	

6 computes

- Twee computerbronnen bevatten dezelfde tag en het tagfilter komt overeen met de tag die wordt gebruikt op de twee computerbronnen.

New Cloud Zone

Summary **Compute** Projects

All compute resources listed apply to this cloud zone. Use the filter to add or remove resources from the list.

Filter tags: test:case42 X
Enter tags to filter resources

TAGS

<input type="checkbox"/>	Name	Account / region	Type	Tags
<input type="checkbox"/>	us-east-1a	Amazon / us-east-1	Availability Zone	test:case42
<input type="checkbox"/>	us-east-1d	Amazon / us-east-1	Availability Zone	test:case42

2 computes

■ Projecten

U kunt zien welke projecten zijn geconfigureerd om de werklastinrichting in deze cloudzone te ondersteunen.

Na het maken van een cloudzone kunt u de configuratie ervan valideren.

Dashbord Inzichten

Als u een gekoppelde vRealize Operations Manager-applicatie hebt die u hebt geconfigureerd om met vRealize Automation te werken, kunt u toegang krijgen tot een dashboard **Inzichten** in de cloudzone. Het dashboard geeft capaciteitsgerelateerde informatie weer over resources en implementaties voor de vSphere- of VMware Cloud on AWS-cloudzone, op voorwaarde dat de cloudaccounts worden geconfigureerd in zowel vRealize Automation als vRealize Operations Manager en worden gecontroleerd in vRealize Operations Manager. Zie [Resourcebeheer en implementatieoptimalisatie met vRealize Operations Manager-statistieken in vRealize Automation](#) voor meer informatie over het dashboard **Inzichten**.

Soorttoewijzingen in vRealize Automation toevoegen om algemene machinegrootten op te geven

Een vRealize Automation-soorttoewijzing is de stap waar u in natuurlijke taal doelimplementatiegrootten voor een specifiek(e) cloudaccount/-regio definieert.

Met soorttoewijzingen geeft u de implementatiegrootten van uw omgeving aan. Een voorbeeld is *small* voor 1 CPU en 2 GB geheugen en *large* voor 2 CPU's en 8 GB geheugen voor een vCenter-account in een benoemd datacenter en t2.nano voor een Amazon Web Services-account in een benoemde regio.

Selecteer **Tenantbeheer > Soorttoewijzingen of Infrastructuur > Soorttoewijzingen** en klik op **Nieuwe soorttoewijzing**.

Meer informatie over soorttoewijzingen in vRealize Automation

Een soorttoewijzing groepeeret een set doelimplementatiegrootten voor een specifiek(e) cloudaccount/-regio in vRealize Automation met behulp van namen in natuurlijke taal.

Met soorttoewijzing kunt u een benoemde toewijzing maken die vergelijkbare soortgrootten in uw accountregio's bevat. Een soorttoewijzing met de naam `standard_small` kan bijvoorbeeld een vergelijkbare soortgrootte (zoals 1 CPU, 2 GB RAM) hebben voor sommige of alle beschikbare accounts/regio's in uw project. Wanneer u een cloudsjabloon bouwt, selecteert u een beschikbare soort die aan uw behoeften voldoet.

Deel de soorttoewijzingen voor uw project in op basis van de opzet van de implementatie.

Om het maken van cloudsjablonen te vereenvoudigen, kunt u een preconfiguratieoptie selecteren wanneer u een nieuw cloudaccount toevoegt. Wanneer u de preconfiguratieoptie selecteert, worden de meest populaire soorttoewijzing en imageroewijzing van uw organisatie voor de opgegeven regio geselecteerd.

Met betrekking tot imageroewijzingen in cloudsjablonen die vSphere-resources bevatten, kunt u onbeperkt geheugen en CPU configureren met vSphere-specifieke instellingen in de cloudsjabloon als er geen soorttoewijzingen zijn gedefinieerd voor een vSphere-cloudzone. Als er soorttoewijzingen zijn gedefinieerd voor een vSphere-cloudzone, fungeert de soorttoewijzing als limiet voor vSphere-specifieke configuraties in de cloudsjabloon.

Imageroewijzingen toevoegen aan vRealize Automation voor toegang tot veelgebruikte besturingssystemen

Een vRealize Automation-imageroewijzing is de plaats waar u natuurlijke taal gebruikt om besturingssystemen voor doelimplementaties te definiëren voor een specifiek(e) cloudaccount/-regio.

Selecteer **Tenantbeheer > Imageroewijzingen** en klik op **Nieuwe imageroewijzing**.

Create Image Mapping

Account / region *

Image name *

Image *

Constraints

Tenant *

Cloud configuration

1	
---	--

Meer informatie over imagoetoewijzingen in vRealize Automation

Een imagoetoewijzing groepeerde een reeks vooraf gedefinieerde specificaties voor het doelbesturingssysteem voor een specifiek cloudaccount of specifieke regio in vRealize Automation met behulp van natuurlijke taalbenaming.

Accounts van cloudleveranciers zoals Microsoft Azure en Amazon Web Services gebruiken images om een set doelimplementatievoorwaarden te groeperen, waaronder het besturingssysteem en gerelateerde configuratie-instellingen. vCenter en op NSX gebaseerde omgevingen, inclusief VMware Cloud on AWS, gebruiken een vergelijkbaar groepsmechanisme om een set implementatievoorwaarden voor besturingssystemen te definiëren. Wanneer u een cloudsjabloon bouwt en uiteindelijk implementeert en itereert, kunt u een beschikbare image kiezen die het beste bij uw behoeften past.

Deel imagoetoewijzingen voor een project in op basis vergelijkbare instellingen voor het besturingssysteem, de tagstrategie en de functionele opzet van de implementatie.

Om het maken van cloudsjablonen te vereenvoudigen, kunt u een preconfiguratieoptie selecteren wanneer u een nieuw cloudaccount toevoegt. Wanneer u de preconfiguratieoptie selecteert, worden de meest populaire soorttoewijzing en imagoetoewijzing van uw organisatie voor de opgegeven regio geselecteerd.

Wanneer u image-informatie aan een cloudsjabloon toevoegt, gebruikt u de vermelding `image` of `imageRef` in het gedeelte `properties` van een machineonderdeel. Als u bijvoorbeeld een momentopname wilt klonen, gebruikt u de eigenschap `imageRef`.

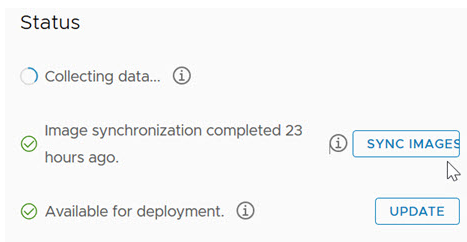
Zie [Hoofdstuk 6 Uw Cloud Assembly-implementaties ontwerpen](#) voor voorbeelden van `image`- en `imageRef`-vermeldingen in de cloudsjablooncode.

Als u rechten wilt toewijzen aan een contentbibliotheek, moet een beheerder de rechten aan de gebruiker toekennen als algemene rechten. Zie [Hiërarchische overname van rechten voor contentbibliotheeken](#) in *vSphere-beheer van virtuele machines* in *VMware vSphere-documentatie* voor gerelateerde informatie.

Images voor cloudaccount/regio synchroniseren

U kunt imagesynchronisatie uitvoeren om ervoor te zorgen dat de afbeeldingen die u toevoegt of verwijderd voor een bepaald cloudaccount/bepaalde regio op de pagina **Infrastructuur > Configureren > Imagoetoewijzing** zijn bijgewerkt.

- 1 Open het/de gekoppelde **Cloudaccount/regio** door **Infrastructuur > Verbindingen > Cloudaccounts** te selecteren. Selecteer het/de bestaande cloudaccount/regio.
- 2 Klik op de knop **Images synchroniseren** om de actie te voltooien.



- 3 Wanneer de actie is voltooid, klikt u op **Infrastructuur > Configureren > Imagoetoewijzing**. Definieer een nieuwe of bewerk een bestaande imagoetoewijzing en selecteer het cloudaccount/de regio in stap 1.
- 4 Klik op het pictogram voor Imagesynchronisatie op de pagina **Imagoetoewijzing**.



- 5 Configureer instellingen voor Imagoetoewijzingen voor het/de opgegeven cloudaccount/regio op de pagina **Imagoetoewijzing**.

OVF-details weergeven

U kunt OVF-specificaties opnemen in Cloud Assembly-cloudsjabloonobjecten, zoals vCenter-machineonderdelen en -imagoetoewijzingen. Als uw image een OVF-bestand bevat, kunt u de inhoud ervan verkennen zonder het bestand te openen. Wijs het OVF-bestand aan om OVF-details waaronder de naam en de locatie weer te geven. Zie [vcenter ovf: property](#) voor meer informatie over de OVF-bestandsindeling. Als u de OVF-gegevens wilt weergeven, moet de imagoetoewijzing zich op de webserver bevinden.



Raadpleeg het externe artikel [Cloud-sjabloon van een OVA](#) voor gerelateerde informatie over het weergeven van OVF-gegevens met behulp van een OVF-koppeling in het toewijzingsveld.

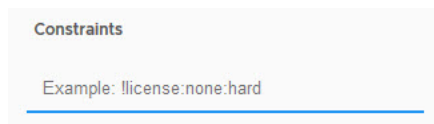
Gedeelde en meest recente images uit een Microsoft Azure-imagegalerie gebruiken

Wanneer u imagedoewijzingen voor Microsoft Azure maakt, kunt u images uit een gedeelde Azure-imagegalerie in het abonnement selecteren. De images in het vervolgkeuzemenu met gegevensverzameling worden beschikbaar gesteld op basis van uw geselecteerde regio.

Hoewel gedeelde imagegaleries voor meerdere abonnementen kunnen worden gebruikt, kunnen ze niet worden weergegeven in het vervolgkeuzemenu voor imagedoewijzing voor meerdere abonnementen. Alleen de images van een bepaald abonnement worden via gegevens verzameld en weergegeven in de lijst met imagedoewijzingen. Als u een image uit een imagegalerie in een ander abonnement wilt gebruiken, geeft u de image-id in de imagedoewijzing op en gebruikt u die imagedoewijzing in de cloudsjabloon.

Beperkingen en tags gebruiken om de selectie van images te verfijnen

Om de imageselectie in een cloudsjabloon verder te verfijnen, kunt u een of meer beperkingen toevoegen om op tags gebaseerde beperkingen op te geven voor het type image dat kan worden geïmplementeerd. Het opgegeven voorbeeld **Beperkingen** dat wordt weergegeven wanneer u een imagedoewijzingsconfiguratie maakt of bewerkt, is `!license:none:hard`. Het voorbeeld illustreert een tagbeperking waarbij de image alleen kan worden gebruikt als de `license:none`-tag *niet* aanwezig is in de cloudsjabloon. Als u tags toevoegt zoals `license:88` en `license:92`, kan de opgegeven image alleen worden gebruikt als de `license:88` en de `license:92`-tags aanwezig *zijn* in de cloudsjabloon.



Een cloudconfiguratiescript gebruiken om implementatie te beheren

U kunt een cloudconfiguratiescript in een imagedoewijzing, cloudsjabloon of beide gebruiken om aangepaste besturingssysteemkenmerken te definiëren voor gebruik in een Cloud Assembly-implementatie. Bijvoorbeeld: afhankelijk van uw keuze om een cloudsjabloon in een publieke of privécloud te implementeren, kunt u specifieke gebruikersrechten, rechten voor het besturingssysteem of andere voorwaarden voor de image toepassen. Een cloudconfiguratiescript voldoet aan een `cloud-init`-indeling voor op Linux gebaseerde images of een `cloudbase-init`-indeling voor op Windows gebaseerde images. Cloud Assembly ondersteunt de tool [cloud-init](#) voor Linux-systemen en de tool [cloudbare-init](#) voor Windows.

Voor Windows-machines kunt u elke indeling voor cloudconfiguratiescripts gebruiken die door `cloudbase-init` wordt ondersteund.

De machineresource in het volgende voorbeeld van cloudsjablooncode gebruikt een image die een cloudconfiguratiescript bevat, waarvan de inhoud bij de `image`-vermelding wordt weergegeven.

```
resources:
  demo-machine:
    type: Cloud.vSphere.Machine
    properties:
      flavor: small
      image: MyUbuntu16
      https://cloud-images.ubuntu.com/releases/16.04/release-20170307/ami-ubuntu-16.04-1.10.3-00-15269239.ova
      cloudConfig: |
        ssh_pwauth: yes
        chpasswd:
          list: |
            ${input.username}:${input.password}
          expire: false
        users:
          - default
          - name: ${input.username}
            lock_passwd: false
            sudo: ['ALL=(ALL) NOPASSWD:ALL']
            groups: [wheel, sudo, admin]
            shell: '/bin/bash'
      runcmd:
        - echo "Defaults:${input.username} !requiretty" >> /etc/sudoers.d/${input.username}
```

De dynamische eigenschapsevaluatie werkt wanneer u cloudConfig rechtstreeks in een cloudsjabloon gebruikt, maar wordt niet ondersteund voor cloudConfig in een imageroewijzing.

In de cloudsjablooncode gebruikt u de instelling `image` om te verwijzen naar een image die als imageroewijzing is gedefinieerd. U gebruikt de instelling `imageRef` om een sjabloon te identificeren die een momentopname (voor gekoppelde klonen), een imagesjabloon of een OVF-sjabloon voor een inhoudsbibliotheek bevat.

Wat gebeurt er als een imageroewijzing en een cloudsjabloon een cloudconfiguratiescript bevatten?

Wanneer een cloudsjabloon die een cloudconfiguratiescript bevat, gebruikmaakt van een imageroewijzing die een cloudconfiguratiescript bevat, worden beide scripts gecombineerd. De samenvoegactie verwerkt de inhoud van het imageroewijzingsscript en de inhoud van het tweede cloudsjabloonscript, waarbij rekening wordt gehouden met het feit of de scripts de `#cloud-config`-indeling hebben of niet.

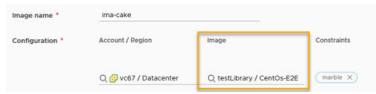
- Voor scripts die de `#cloud-config`-indeling hebben, combineert de samenvoeging de inhoud van elke module (bijvoorbeeld `runcmd`, `users` en `write_files`) als volgt:
 - Voor modules waarvan de inhoud een lijst is, worden de lijsten met opdrachten uit de imageroewijzing en de cloudsjablonen samengevoegd, met uitzondering van opdrachten die identiek zijn in beide lijsten.

- Voor modules waarvan de inhoud een woordenboek is, worden de opdrachten samengevoegd en wordt het resultaat een combinatie van beide woordenboeken. Als dezelfde sleutel in beide woordenboeken bestaat, blijft de sleutel uit het woordenboek voor imagoetoewijzing behouden en wordt de sleutel uit de woordenlijst voor de cloudsjabloon genegeerd.
- Voor modules waarvan de inhoud een tekenreeks is, worden de inhoudswaarden van het imagoetoewijzingsscript behouden en worden de inhoudswaarden van het cloudsjabloonscript genegeerd.
- Voor scripts met een andere indeling dan `#cloud-config`, of wanneer één script in `#cloud-config`-indeling is en de andere niet, worden beide scripts gecombineerd op een manier waarbij het imagoetoewijzingsscript eerst wordt uitgevoerd en het cloudsjabloonscript wordt uitgevoerd wanneer het imagoetoewijzingsscript is voltooid.

Zie [Gebruikersgegevenssecties samenvoegen](#) voor gerelateerde informatie.

Een image uit een vCenter-inhoudsbibliotheek toevoegen

Wanneer een lokale inhoudsbibliotheek of een inhoudsbibliotheek van een uitgever zich bevindt in een vCenter dat door uw vRealize Automation-organisatie wordt beheerd, worden sjabloonimages uit een inhoudsbibliotheek weergegeven in het vervolgkeuzemenu met images. De images in de lijst zijn onder andere OVF- en VM-sjabloonimages in lokale bibliotheken of vCenter-inhoudsbibliotheken van uitgevers. Images in inhoudsbibliotheken van abonnees worden niet weergegeven in het vervolgkeuzemenu. De sjabloon van waaruit een VM is gekloond, wordt weergegeven in de sectie met machinegegevens van de gebruikersinterface voor machine-implementaties.



Opmerking Als de vCenter uit de inhoudsbibliotheek van de uitgever door vRealize Automation wordt beheerd, wordt de uitgeverinformatie in het raster met de selectie van de imago-toewijzingen in de volgende indeling weergegeven: *publisher_content_library_name / content_item_name*

Als u rechten wilt toewijzen aan een contentbibliotheek, moet een beheerder de rechten aan de gebruiker toekennen als algemene rechten. Zie [Hiërarchische overname van rechten voor contentbibliotheek](#) in *vSphere-beheer van virtuele machines* in [VMware vSphere-documentatie](#) voor gerelateerde informatie.

Als de vCenter uit de inhoudsbibliotheek van de uitgever niet wordt beheerd door vRealize Automation, wordt de informatie van de abonnee in het raster met de selectie van imago-toewijzingen weergegeven in de volgende indeling: *subscriber_content_library_name / content_item_name*

In het volgende scenario zijn bijvoorbeeld alleen de inhoudsbibliotheekitems van de abonnee zichtbaar in de vRealize Automation-lijst met imago-toewijzingen:

- Voor een vCenter met de naam VC-1 is er een inhoudsbibliotheek voor een abonnee in het VC en wordt er een cloudaccount gemaakt in vRealize Automation dat is gekoppeld aan VC-1.
- Voor een vCenter met de naam VC-2 is er een inhoudsbibliotheek voor een uitgever in de VC waarop de inhoudsbibliotheek voor een abonnee van VC-1 is geabonneerd. Er is echter geen cloudaccount in vRealize Automation dat is gekoppeld aan VC-2.

Omdat VC-1 is gekoppeld aan een vRealize Automation-cloudaccount, is de inhoudsbibliotheek van de abonnee beschikbaar in vRealize Automation. De inhoud wordt verzameld en weergegeven in de vRealize Automation-lijst met imago-toewijzingen. Maar omdat VC-2 niet aan een cloudaccount is gekoppeld, heeft vRealize Automation geen kennis van de inhoudsbibliotheek van de uitgever. Als u de inhoudsbibliotheekitems van de uitgever wilt weergeven in de lijst met imago-toewijzingen, moet u een cloudaccount koppelen aan het vCenter VC-2.

Wanneer u een cloudsjabloon implementeert die een imago-toewijzing voor een VM-sjabloon bevat, probeert vRealize Automation toegang te krijgen tot de toegewezen image in de inhoudsbibliotheek die het dichtst bij de gegevensopslag is en vervolgens het dichtst bij de host van de machine is die moet worden ingericht. Dit kan bestaan uit een lokale inhoudsbibliotheek en een inhoudsbibliotheek van een uitgever of abonnee.

Wanneer u een cloudsjabloon implementeert die een OVF-sjabloonimage bevat, zijn OVF-images toegankelijk zoals is opgegeven in de imago-toewijzingsrij, als de image zich in een lokale inhoudsbibliotheek of een lokale inhoudsbibliotheek van een abonnee of een opgegeven externe inhoudsbibliotheek van een uitgever bevindt.

Voor gerelateerde informatie over het maken en gebruiken van vCenter-inhoudsbibliotheken raadpleegt u [Inhoudsbibliotheken gebruiken](#) in de [productdocumentatie voor vSphere](#) en het [blogartikel](#) over het gebruik van inhoudsbibliotheken in vRealize Automation 8 en vRealize Automation Cloud.

Meer informatie over het configureren en gebruiken van cloudconfiguratiescripts

Zie [Machine-initialisatie in Cloud Assembly](#) voor meer informatie over het gebruik van cloudconfiguratiescripts in cloudsjablonen.

Zie ook de VMware-blogartikelen [vSphere Customization with Cloud-init While Using vRealize Automation 8 or vCloud](#) en [Customizing Cloud Assembly Deployments with Cloud-Init](#).

Netwerkprofielen toevoegen in vRealize Automation

Een netwerkprofiel van vRealize Automation beschrijft het gedrag van het netwerk dat moet worden geïmplementeerd.

Een netwerk kan bijvoorbeeld internetgericht zijn in plaats van alleen intern.

Netwerken en netwerkprofielen zijn clouds specifiek.

Selecteer **Infrastructuur > Configureren > Netwerkprofielen** en klik op **Nieuw netwerkprofiel**.

Meer informatie over netwerkprofielen in vRealize Automation

Een netwerkprofiel definieert een groep netwerken en netwerkinstellingen die beschikbaar zijn voor een cloudaccount in een bepaalde regio of een bepaald datacenter in vRealize Automation.

U definieert doorgaans netwerkprofielen om een doelimplementatieomgeving te ondersteunen, bijvoorbeeld een kleine testomgeving waar een bestaand netwerk alleen uitgaande toegang heeft, of een grote productieomgeving met gelijke taakverdeling waarvoor een reeks beveiligingsbeleidsregels nodig is. Beschouw een netwerkprofiel als een verzameling van netwerkkenmerken die specifiek zijn voor de workload.

Inhoud van een netwerkprofiel

Een netwerkprofiel bevat specifieke informatie voor een bepaald type cloudaccount en een regio in vRealize Automation, waaronder de volgende instellingen:

- Benoemde cloudaccount/regio en optionele capaciteitstags voor het netwerkprofiel.
- Benoemde bestaande netwerken en hun instellingen.
- Netwerkbeleidsregels die op aanvraag definiëren en andere aspecten van het netwerkprofiel.
- Optionele opname van bestaande load balancers.
- Optionele opname van bestaande beveiligingsgroepen.

U bepaalt de netwerk-IP-beheerfunctionaliteit op basis van het netwerkprofiel.

Capaciteitstags voor netwerkprofielen worden gekoppeld aan de beperkingstags in cloudsjablonen om de netwerkselectie te helpen beheren. Verder worden alle tags die zijn toegewezen aan de netwerken die worden verzameld door het netwerkprofiel ook gekoppeld aan tags in de cloudsjabloon om de netwerkselectie te helpen beheren wanneer de cloudsjabloon wordt geïmplementeerd.

Capaciteitstags zijn optioneel. Capaciteitstags worden toegepast op alle netwerken in het netwerkprofiel, maar alleen wanneer de netwerken worden gebruikt als onderdeel van dat netwerkprofiel. Voor netwerkprofielen die geen capaciteitstags bevatten, vindt tagafstemming alleen plaats voor netwerktags. De netwerk- en beveiligingsinstellingen die in het gekoppelde netwerkprofiel zijn gedefinieerd, worden toegepast wanneer de cloudsjabloon wordt geïmplementeerd.

Wanneer u statische IP gebruikt, wordt het adresbereik beheerd door vRealize Automation. Voor DHCP worden de begin- en eindadressen van de IP beheerd door de onafhankelijke DHCP-server en niet door vRealize Automation. Wanneer u DHCP of een gemengde netwerkadrestoewijzing gebruikt, wordt de waarde van het netwerkverbruik ingesteld op nul. Het toegewezen bereik van een netwerk op aanvraag is gebaseerd op de CIDR en de subnetgrootte die is opgegeven in het netwerkprofiel. Om zowel een statische als dynamische toewijzing in de implementatie te ondersteunen, wordt het toegewezen bereik verdeeld in twee bereiken: een voor statische toewijzing en een andere voor dynamische toewijzing.

Netwerken

Netwerken, ook wel subnetten genoemd, zijn logische onderverdelingen van een IP-netwerk. Een netwerk groepeerd een cloudaccount, IP-adres of -bereik en netwerktags om te bepalen hoe en waar een cloudsjabloonimplementatie moet worden ingericht. Netwerkparameters in het profiel definiëren hoe machines in de implementatie met elkaar kunnen communiceren via IP-laag 3. Netwerken kunnen tags hebben.

U kunt netwerken aan het netwerkprofiel toevoegen, aspecten van netwerken bewerken die worden gebruikt door het netwerkprofiel en netwerken uit het netwerkprofiel verwijderen.

Wanneer u een netwerk toevoegt aan het netwerkprofiel, kunt u beschikbare netwerken selecteren in een gefilterde lijst met vSphere- en NSX-netwerken. Als het netwerktype wordt ondersteund voor het cloudaccounttype, kunt u het toevoegen aan het netwerkprofiel.

In een VCF-gebaseerde implementatie worden de NSX-netwerksegmenten lokaal in het NSX-T-netwerk gemaakt en worden ze niet gemaakt als algemene netwerken.

■ Netwerkdomein of Transportzone

Een netwerkdomein of transportzone is de gedistribueerde virtuele switch (dvSwitch) voor de vSphere-vNetwork Distributed PortGroups (dvPortGroup). Een *transportzone* is een bestaand NSX-concept dat vergelijkbaar is met termen zoals *dvSwitch* of *dvPortGroup*.

Wanneer u een NSX-cloudaccount gebruikt, is de elementnaam op de pagina **Transportzone**, anders is de naam **Netwerkdomein**.

Voor standaardswitches is het netwerkdomein of de transportzone gelijk aan de switch zelf. Het netwerkdomein of de transportzone definieert de grenzen van de subnetwerken binnen vCenter.

Een transportzone regelt het bereik van een logische NSX-switch. Het kan een of meer vSphere-clusters omvatten. Transportzones bepalen welke clusters en welke virtuele machines kunnen deelnemen aan het gebruik van een bepaald netwerk. Subnetwerken die tot dezelfde NSX-transportzone behoren, kunnen voor dezelfde machinehosts worden gebruikt.

- **Domein**

Vertegenwoordigt de domeinnaam van de machine. De domeinnaam wordt doorgegeven aan de aanpassingsspecificatie van de vSphere-machine.

- **IPv4 CIDR en IPv4-standaardgateway**

vSphere-machineonderdelen in de cloudsjabloon ondersteunen IPv4-, IPv6- en dual stack IP-toewijzing voor netwerkinterfaces. Bijvoorbeeld: 192.168.100.14/24 staat voor het IPv4-adres 192.168.100.14 en het bijbehorende routeringsvoorvoegsel 192.168.100.0, of het equivalente subnetmasker 255.255.255.0, dat 24 1-voorloopbits heeft. Het IPv4-blok 192.168.100.0/22 staat voor de 1024 IP-adressen van 192.168.100.0 tot 192.168.103.255.

- **IPv6 CIDR en IPv6-standaardgateway**

vSphere-machineonderdelen in de cloudsjabloon ondersteunen IPv4-, IPv6- en dual stack IP-toewijzing voor netwerkinterfaces. Bijvoorbeeld: 2001:db8::/48 staat voor het blok met IPv6-adressen van 2001:db8:0:0:0:0:0:0 t/m 2001:db8:0:ffff:ffff:ffff:ffff:ffff.

De IPv6-indeling wordt niet ondersteund voor netwerken op aanvraag.

- **DNS-servers en DNS-zoekdomeinen**

- **Ondersteuning openbare IP**

Selecteer deze optie om het netwerk als openbaar te markeren. Netwerkonderdelen in een cloudsjabloon met de eigenschap `network type: public` worden gekoppeld aan netwerken die zijn gemarkeerd als openbaar. Verdere aanpassing vindt plaats tijdens de cloudsjabloonimplementatie om de netwerkselectie te bepalen.

- **Standaard voor zone**

Selecteer deze optie om het netwerk als standaard te markeren voor de cloudzone. Tijdens de implementatie van cloudsjablonen krijgen standaardnetwerken de voorkeur boven andere netwerken.

- **Bron**

Identificeert de netwerkbron.

- **Tags**

Geeft een of meer tags op die aan het netwerk zijn toegewezen. Tags zijn optioneel. Het koppelen van tags is van invloed op welke netwerken beschikbaar zijn voor uw cloudsjabloonimplementaties.

Netwerktags bestaan voor het netwerkitem zelf, ongeacht het netwerkprofiel. Netwerktags zijn van toepassing op elk exemplaar van het netwerk waaraan ze zijn toegevoegd en op alle netwerkprofielen die dat netwerk bevatten. Van netwerken kan een instantie worden gemaakt in een onbeperkt aantal netwerkprofielen. Ongeacht de locatie van het netwerkprofiel is er een netwerktag gekoppeld aan dat netwerk waar het netwerk ook wordt gebruikt.

Wanneer u een cloudsjabloon implementeert, worden beperkingstags in de netwerkonderdelen van een cloudsjabloon gekoppeld aan netwerktags, inclusief capaciteitstags voor netwerkprofielen. Voor netwerkprofielen die capaciteitstags bevatten, worden de capaciteitstags toegepast op alle netwerken die beschikbaar zijn voor dat netwerkprofiel. De netwerk- en beveiligingsinstellingen die in het gekoppelde netwerkprofiel zijn gedefinieerd, worden toegepast wanneer de cloudsjabloon wordt geïmplementeerd.

Netwerkbeleid

Met behulp van netwerkprofielen kunt u subnetwerken definiëren voor bestaande netwerkdomeinen die statische, DHCP- of een combinatie van statische en DHCP-IP-adresinstellingen bevatten. U kunt subnetwerken definiëren en IP-adresinstellingen opgeven met behulp van het tabblad **Netwerkbeleid**.

Wanneer u NSX-V, NSX-T of VMware Cloud on AWS gebruikt, worden netwerkbeleidsinstellingen toegepast wanneer een cloudsjabloon `networkType: outbound` of `networkType: private` vereist of wanneer een NSX-netwerk `networkType: routed` vereist.

Afhankelijk van het bijbehorende cloudaccount kunt u netwerkbeleidsregels gebruiken om instellingen te definiëren voor de netwerktypen `outbound`, `private` en `routed` en voor beveiligingsgroepen op aanvraag. U kunt ook netwerkbeleidsregels gebruiken om `existing` netwerken te beheren wanneer er een load balancer is gekoppeld aan dat netwerk.

In uitgaande netwerken is eenrichtingstoegang tot upstream netwerken mogelijk. In privénetwerken is geen externe toegang mogelijk. Gerouteerde netwerken staan Oost/West-verkeer toe tussen de gerouteerde netwerken. De bestaande en openbare netwerken in het profiel worden gebruikt als onderliggende of upstreamnetwerken.

Opties voor de volgende selecties op aanvraag worden beschreven in de **Netwerkprofielen**-hulp op het scherm en worden hieronder samengevat.

- **Maak geen netwerk op aanvraag of een beveiligingsgroep op aanvraag**

U kunt deze optie gebruiken bij het specificeren van een `existing` netwerk of een netwerk van het type `public`. Cloudsjablonen waarvoor een `outbound`-, `private`- of `routed`-netwerk nodig is, zijn niet gekoppeld aan dit profiel.

- **Maak een netwerk op aanvraag**

U kunt deze optie gebruiken bij het specificeren van een `outbound`-, `private`- of `routed`-netwerktype.

Amazon Web Services, Microsoft Azure, NSX, vSphere en VMware Cloud on AWS ondersteunen deze optie.

■ Maak een beveiligingsgroep op aanvraag

U kunt deze optie gebruiken bij het specificeren van een `outbound` netwerk of een netwerk van het type `private`.

Er wordt een nieuwe beveiligingsgroep gemaakt voor overeenkomende cloudsjablonen als het netwerktype `outbound` of `private` is.

Amazon Web Services, Microsoft Azure, NSX en VMware Cloud on AWS ondersteunen deze optie.

Netwerkbeleidsinstellingen kunnen voor een specifiek type cloudaccount gelden. Deze instellingen worden beschreven in de wegwijzerhulp op het scherm en worden hieronder samengevat:

■ Netwerkdomein of Transportzone

Een netwerkdomein of transportzone is de gedistribueerde virtuele switch (dvSwitch) voor de vSphere-vNetwork Distributed PortGroups (dvPortGroup). Een *transportzone* is een bestaand NSX-concept dat vergelijkbaar is met termen zoals *dvSwitch* of *dvPortGroup*.

Wanneer u een NSX-cloudaccount gebruikt, is de elementnaam op de pagina **Transportzone**, anders is de naam **Netwerkdomein**.

Voor standaardswitches is het netwerkdomein of de transportzone gelijk aan de switch zelf. Het netwerkdomein of de transportzone definieert de grenzen van de subnetwerken binnen vCenter.

Een transportzone regelt het bereik van een logische NSX-switch. Het kan een of meer vSphere-clusters omvatten. Transportzones bepalen welke clusters en welke virtuele machines kunnen deelnemen aan het gebruik van een bepaald netwerk. Subnetwerken die tot dezelfde NSX-transportzone behoren, kunnen voor dezelfde machinehosts worden gebruikt.

■ Extern subnet

Een netwerk op aanvraag met uitgaande toegang vereist een extern subnet met uitgaande toegang. Het externe subnet wordt gebruikt om uitgaande toegang te bieden indien hierom wordt gevraagd in de cloudsjabloon. Het bepaalt niet de netwerkplaatsing. Het externe subnet heeft bijvoorbeeld geen invloed op het plaatsen van een privénetwerk.

■ CIDR

CIDR-notatie is een compacte weergave van een IP-adres en het bijbehorende routeringsvoorvoegsel. De CIDR-waarde geeft het adresbereik van het netwerk op dat moet worden gebruikt tijdens de inrichting om subnetwerken te maken. Deze CIDR-instelling op het tabblad **Netwerkbeleid** accepteert een IPv4-notatie die eindigt op /nn en die waarden bevat tussen 0-32.

■ Subnetgrootte

Deze optie bepaalt de grootte van het netwerk op aanvraag, met behulp van de IPv4-notatie, voor elk geïsoleerd netwerk in een implementatie die dit netwerkprofiel gebruikt. De instelling voor subnetgrootte is beschikbaar voor intern of extern IP-adresbeheer.

De IPv6-indeling wordt niet ondersteund voor netwerken op aanvraag.

■ **Gedistribueerde logische router**

Voor een gerouteerd netwerk op aanvraag moet u een gedistribueerd logisch netwerk specificeren wanneer u een NSX-V-cloudaccount gebruikt.

Een gedistribueerde logische router (DLR) wordt gebruikt om oost/westverkeer tussen op aanvraag gerouteerde netwerken op NSX-V te routeren. Deze optie is alleen zichtbaar als de waarde account/regio voor het netwerkprofiel is gekoppeld aan een NSX-V-cloudaccount.

■ **IP-bereik toewijzen**

Deze optie is beschikbaar voor cloudaccounts die NSX of VMware Cloud on AWS ondersteunen, inclusief vSphere.

De instelling IP-bereik is beschikbaar wanneer u een bestaand netwerk met een extern IPAM-integratiepunt gebruikt.

U kunt een van de volgende drie opties selecteren om een toewijzingstype voor IP-bereiken op te geven voor het implementatienetwerk:

■ **Statisch en DHCP**

Standaard en aanbevolen. Deze gemengde optie gebruikt de toegewezen instellingen **CIDR** en **Subnetbereik** om de DHCP-serverpool te configureren om de helft van de adresruimtetoewijzing te ondersteunen met behulp van de (dynamische) DHCP-methode en de helft van de IP-adresruimtetoewijzing met behulp van de statische methode. Gebruik deze optie wanneer er voor sommige machines die zijn verbonden met een netwerk op aanvraag toegewezen statische IP-adressen nodig zijn en voor andere dynamische IP-adressen. Er worden twee IP-bereiken gemaakt.

Deze optie is vooral effectief in implementaties met machines die zijn verbonden met een netwerk op aanvraag, waarbij aan sommige machines statische IP's worden toegewezen en aan andere machines dynamische IP-adressen worden toegewezen door een NSX-DHCP-server en -implementaties waarbij de load balancer-VIP statisch is.

■ **DHCP (dynamisch)**

Deze optie gebruikt de toegewezen CIDR om een IP-pool op een DHCP-server te configureren. Alle IP-adressen voor dit netwerk worden dynamisch toegewezen. Er wordt één IP-bereik gemaakt voor elke toegewezen CIDR.

■ **Statisch**

Deze optie gebruikt de toegewezen CIDR om statisch IP-adressen toe te wijzen. Gebruik deze optie wanneer een DHCP-server niet hoeft te worden geconfigureerd voor dit netwerk. Er wordt één IP-bereik gemaakt voor elke toegewezen CIDR.

■ **IP-blokken**

De instelling IP-blokken is beschikbaar bij gebruik van een netwerk op aanvraag met een extern IPAM-integratiepunt.

Als u de IP-blokinstelling gebruikt, kunt u een benoemd IP-blok of bereik toevoegen aan het netwerkprofiel van uw geïntegreerde externe IPAM-provider. U kunt ook een toegevoegd IP-blok uit het netwerkprofiel verwijderen. Zie [Een extern IPAM-integratiepunt voor Infoblox toevoegen in vRealize Automation](#) voor informatie over het maken van een externe IPAM-integratie.

Externe IPAM is beschikbaar voor de volgende typen cloudaccount/regio:

- vSphere
- vSphere met NSX-T
- vSphere met NSX-V
- **Netwerkresources - Extern netwerk**

Externe netwerken worden ook wel bestaande netwerken genoemd. Van deze netwerken worden gegevens verzameld en ze zijn beschikbaar voor selectie.

- **Netwerkresources - logische Tier-O-router**

NSX-T gebruikt de logische tier-O-router als gateway naar netwerken die buiten de NSX-implementatie vallen. De logische router van tier O configureert uitgaande toegang voor netwerken op aanvraag.

- **Netwerkresources - Edge-cluster**

Het opgegeven edge-cluster biedt routingservices. Het edge-cluster wordt gebruikt om uitgaande toegang te configureren voor netwerken op aanvraag en load balancers. Het identificeert het edge-cluster of de resourcepool waar het edge-apparaat moet worden geïmplementeerd.

- **Netwerkresources - Edge-datastore**

De opgegeven edge-datastore wordt gebruikt om het edge-apparaat in te richten. Deze instelling is alleen van toepassing op NSX-V.

Tags kunnen worden gebruikt om te bepalen welke netwerken beschikbaar zijn voor de cloudsjabloon.

Load balancers

U kunt load balancers toevoegen aan het netwerkprofiel. Vermelde load balancers zijn beschikbaar op basis van informatie die is verzameld uit het broncloudaccount.

Als een tag op een van de load balancers in het netwerkprofiel overeenkomt met een tag die wordt gebruikt in een load-balanceronderdeel in de cloudsjabloon, wordt de load balancer in aanmerking genomen tijdens de implementatie. Load balancers in een overeenkomend netwerkprofiel worden gebruikt wanneer een cloudsjabloon wordt geïmplementeerd.

Zie [Instellingen voor load balancers in netwerkprofielen gebruiken in vRealize Automation](#) en [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#) voor meer informatie.

Beveiligingsgroepen

Wanneer een cloudsjabloon wordt geïmplementeerd, worden de beveiligingsgroepen in het netwerkprofiel toegepast op de machine-NIC's die worden ingericht. Voor een Amazon Web Services-specifiek netwerkprofiel zijn de beveiligingsgroepen in het netwerkprofiel beschikbaar in hetzelfde netwerkdomein (VPC) als de netwerken die worden weergegeven op het tabblad Netwerken. Als voor het netwerkprofiel geen netwerken worden weergegeven op het tabblad Netwerken, worden alle beschikbare beveiligingsgroepen weergegeven.

U kunt een beveiligingsgroep gebruiken om de isolatie-instellingen voor een `private-` of `outbound-`netwerk op aanvraag verder te definiëren. Beveiligingsgroepen worden ook toegepast op `existing-`netwerken. U kunt ook algemene beveiligingsgroepen toewijzen.

De vermelde beveiligingsgroepen zijn beschikbaar op basis van informatie die is verzameld van het broncloudaccount of die is toegevoegd als een beveiligingsgroep op aanvraag in een projectcloudsjabloon. Zie [Beveiligingsresources in vRealize Automation](#) voor meer informatie.

Beveiligingsgroepen worden toegepast op alle machines in de implementatie die zijn verbonden met het netwerk dat overeenkomt met het netwerkprofiel. Omdat er mogelijk meerdere netwerken in een cloudsjabloon zijn, waarbij elk netwerk overeenkomt met een ander netwerkprofiel, kunt u verschillende beveiligingsgroepen voor verschillende netwerken gebruiken.

Opmerking Naast het opgeven van een beveiligingsgroep kunt u ook NSX-netwerken (standaard), vSphere-netwerken of beide selecteren. Wanneer u een cloudsjabloon implementeert, voegt vRealize Automation de toegewezen of opgegeven beveiligingsgroep toe aan de machine-NIC's die zijn verbonden met het toegewezen NSX-netwerk. Alleen machine-NIC's die zijn verbonden met een NSX-netwerk, kunnen worden toegevoegd aan een NSX-beveiligingsgroep. Als de machine-NIC is verbonden met een vSphere-netwerk, mislukt de sjabloonimplementatie.

Door een tag aan een bestaande beveiligingsgroep toe te voegen, kunt u de beveiligingsgroep in een `Cloud.SecurityGroup`-cloudsjabloononderdeel gebruiken. Een beveiligingsgroep moet ten minste één tag hebben, anders kan deze niet worden gebruikt in een cloudsjabloon. Zie [Beveiligingsresources in vRealize Automation](#) en [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#) voor meer informatie.

Meer informatie over netwerkprofielen, netwerken, cloudsjablonen en tags

Zie [Netwerkresources in vRealize Automation](#) voor meer informatie over netwerken.

Zie [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#) voor voorbeelden van de code van een voorbeeldnetwerkonderdeel in een cloudsjabloon.

Zie [Network Automation with Cloud Assembly and NSX](#) voor voorbeelden van werkstromen voor netwerkautomatisering.

Zie [Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren](#) voor meer informatie over tags en tagstrategie.

Zie [Hoe kan ik de naam van een netwerkinterfacecontroller configureren met behulp van uitbreidbaarheidsacties](#) voor informatie over hoe u de machine-NIC's een naam geeft.

Netwerkinstellingen gebruiken in netwerkprofielen en cloudsjablonen in vRealize Automation

U gebruikt netwerken en netwerkprofielen in vRealize Automation om te helpen bij het definiëren van het gedrag van de netwerkinrichting voor uw implementaties.

In vRealize Automation kunt u cloudspecifieke netwerkprofielen definiëren. Zie [Meer informatie over netwerkprofielen in vRealize Automation](#).

Met behulp van netwerk- en netwerkprofielinstellingen kunt u bepalen hoe netwerk-IP-adressen worden gebruikt in vRealize Automation-cloudsjablonen en -implementaties.

Ondersteuning voor IPv4 en IPv6 in vRealize Automation-netwerken

vRealize Automation-netwerken ondersteunen stack IPv4, single stack IPv6 of dual stack IPv4 en IPv6.

IPv6 wordt ondersteund voor bestaande vSphere-netwerken en bestaande NSX-netwerken.

IPv6 wordt niet ondersteund voor load balancers, NSX-netwerken op aanvraag of externe IPAM-providers zoals Infoblox.

Ondersteuning externe IPAM-providers

Naast de geleverde interne IPAM-ondersteuning kunt u een externe IPAM-provider gebruiken om IP-adressen voor netwerken dynamisch of statisch toe te wijzen als IP-bereiken voor bestaande netwerken in uw cloudsjabloonontwerpen en -implementaties en IP-blokken voor netwerken op aanvraag in uw cloudsjabloonontwerpen en -implementaties.

Ondersteuning voor externe IPAM-providers, zoals Infoblox, is beschikbaar voor leveranciers-specifieke IPAM-integratiepunten die u kunt maken met behulp van de menuvolgorde **Infrastructuur > Verbindingen > Integratie toevoegen > IPAM**.

Opties voor het definiëren van adresinformatie van een externe IPAM-provider zijn beschikbaar via de optie **IPAM IP-bereik toevoegen** op de pagina **Netwerkbeleid > IPAM IP-bereik toevoegen**.

Zie [Een externe IPAM-integratie in vRealize Automation configureren](#) voor informatie over het maken van een extern IPAM-integratiepunt. Zie [Tutorial: Een providerspecifieke externe IPAM-integratie voor vRealize Automation configureren](#) voor een voorbeeld van hoe u een IPAM-integratiepunt maakt voor een specifieke IPAM-leverancier.

Netwerktypen

Een netwerkonderdeel in een cloudsjabloon wordt als een van de volgende `networkType`-typen gedefinieerd.

Netwerktipe	Definitie
existing	<p>Selecteert een bestaand netwerk dat is geconfigureerd in de onderliggende cloudprovider, zoals vCenter, Amazon Web Services en Microsoft Azure. Een bestaand netwerk is vereist door het <code>outbound</code>-netwerk op aanvraag.</p> <p>U kunt een bereik van statische IP-adressen in een bestaand netwerk definiëren.</p>
public	<p>Machines op een openbaar netwerk zijn toegankelijk via internet. Een IT-beheerder definieert deze netwerken. De definitie van een <code>public</code>-netwerk is identiek aan die van een <code>existing</code>-netwerk voor netwerken die netwerkverkeer langs openbare netwerken mogelijk maken.</p>
private	<p>Een netwerktipe op aanvraag.</p> <p>Beperkt netwerkverkeer zodat dit alleen plaatsvindt tussen resources in het geïmplementeerde netwerk. Hierdoor wordt inkomend en uitgaand verkeer voorkomen. In NSX kan dit worden gelijkgesteld aan een on-demand één-op-veel-NAT.</p>
outbound	<p>Een netwerktipe op aanvraag.</p> <p>Beperkt het netwerkverkeer tussen de berekeningsresources in de implementatie, maar maakt ook uitgaand netwerkverkeer in één richting mogelijk. In NSX kan dit worden gelijkgesteld aan een on-demand één-op-veel-NAT met extern IP.</p>
routed	<p>Een netwerktipe op aanvraag.</p> <p>Gerouteerde netwerken bevatten een routeerbare IP-ruimte die is verdeeld over beschikbare subnetwerken die aan elkaar zijn gekoppeld. De virtual machines die zijn ingericht met geleide netwerken en die hetzelfde geleide netwerkprofiel hebben, kunnen met elkaar en het externe netwerk communiceren.</p> <p>Geleide netwerken zijn een on-demand netwerktipe dat beschikbaar is voor NSX-V- en NSX-T-netwerken. Microsoft Azure en Amazon Web Services bieden deze connectiviteit standaard.</p> <p>Een <code>routed</code>-netwerk is alleen beschikbaar voor cloudsjabloonspecificatie in een <code>Cloud.NSX.Network-</code>netwerkonderdeel.</p>

Zie [Meer informatie over netwerkresources in vRealize Automation-cloudsjablonen](#) voor meer informatie.

Zie [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#) voor voorbeelden van ingevulde cloudsjablonen die netwerkonderdeelgegevens bevatten.

Voorbeeld van netwerkscenario's

U kunt het volgende gedrag verwachten wanneer u een cloudsjabloon implementeert die de volgende netwerkprofielconfiguratie gebruikt.

Netwerkttype of -scenario	Geen netwerkprofielen beschikbaar voor de cloudzone	Netwerkprofielen die beschikbaar zijn voor de cloudzone
Geen netwerk	<p>Als er geen netwerk in de cloudsjabloon is opgegeven, wordt een willekeurig netwerk uit dezelfde inrichtingsregio als de berekening geselecteerd.</p> <p>De voorkeur wordt gegeven aan netwerken die als standaard worden aangeduid.</p> <p>Als er geen netwerken in een beschikbare inrichtingsregio bestaan, mislukt de inrichting.</p>	<p>Er wordt een netwerk uit een overeenkomend netwerkprofiel geselecteerd.</p> <p>De voorkeur wordt gegeven aan netwerken die als standaard worden aangeduid.</p> <p>Als geen van de netwerkprofielen aan de criteria voldoet, mislukt de inrichting.</p>
Bestaand netwerk	<p>Als het netwerkonderdeel in de cloudsjabloon beperkingstags bevat, worden deze beperkingen gebruikt om de lijst met beschikbare netwerken te filteren. Beperkingstags in het netwerkonderdeel van de cloudsjabloon worden in overeenstemming gebracht met netwerktags en, indien beschikbaar, beperkingstags van het netwerkprofiel.</p> <p>In de gefilterde lijst met netwerken wordt één netwerk uit dezelfde inrichtingsregio als berekeningsresource geselecteerd.</p> <p>De voorkeur wordt gegeven aan netwerken die als standaard worden aangeduid.</p> <p>Als na het filteren op beperkingen geen netwerken in de inrichtingsregio bestaan, mislukt de inrichting.</p>	<p>Er wordt een netwerk uit een overeenkomend netwerkprofiel geselecteerd.</p> <p>De voorkeur wordt gegeven aan netwerken die als standaard worden aangeduid.</p> <p>Als geen van de netwerkprofielen aan de criteria voldoet, mislukt de inrichting.</p> <p>Netwerkbeperkingen kunnen worden gebruikt voor het filteren van bestaande netwerken in het profiel op basis van de vooraf toegewezen tags.</p>
Openbaar netwerk	<p>Als het netwerk beperkingen heeft, worden deze beperkingen gebruikt om de lijst met beschikbare netwerken te filteren waarvoor het kenmerk <code>supports public IP</code> is ingesteld.</p> <p>In de gefilterde lijst met netwerken wordt een willekeurig netwerk uit dezelfde inrichtingsregio als de berekeningsresource geselecteerd.</p> <p>De voorkeur wordt gegeven aan netwerken die als standaard worden aangeduid.</p> <p>Als na het filteren op beperkingen geen openbare netwerken in de inrichtingsregio bestaan, mislukt de inrichting.</p>	<p>Er is een netwerk met het kenmerk <code>supports public IP</code> uit een overeenkomend netwerkprofiel geselecteerd.</p> <p>De voorkeur wordt gegeven aan netwerken die als standaard worden aangeduid.</p> <p>Netwerkbeperkingen kunnen worden gebruikt voor het filteren van bestaande openbare netwerken in het profiel op basis van de vooraf toegewezen tags.</p>

Netwerkttype of -scenario	Geen netwerkprofielen beschikbaar voor de cloudzone	Netwerkprofielen die beschikbaar zijn voor de cloudzone
Privénetwerk	De inrichting mislukt omdat privénetwerken informatie van een netwerkprofiel nodig hebben.	Er wordt een nieuw netwerk of een nieuwe beveiligingsgroep gemaakt op basis van instellingen in het overeenkomstige netwerkprofiel. Netwerkbeperingstags kunnen worden gebruikt om netwerkprofielen en netwerken te filteren.
Uitgaand netwerk	Inrichting mislukt omdat voor uitgaande netwerken informatie van een netwerkprofiel is vereist.	Er wordt een nieuw netwerk of een nieuwe beveiligingsgroep gemaakt op basis van instellingen in het overeenkomstige netwerkprofiel. Netwerkbeperingstags kunnen worden gebruikt om netwerkprofielen en netwerken te filteren.
Geleid on-demand netwerk	De inrichting mislukt omdat voor geleide netwerken informatie van een netwerkprofiel is vereist.	Voor NSX-V is een DLR-selectie (Distributed Logical router) nodig. Voor NSX-T en VMware Cloud on AWS hebben we soortgelijke on-demand instellingen nodig als voor privé en uitgaand.
WordPress-gebruiksscenario met bestaande of openbare netwerken	De inrichting vindt plaats zoals voor een bestaand netwerk of een openbaar netwerk is beschreven.	Zie de bovenstaande beschrijvingen voor het gedrag van bestaande netwerken en openbare netwerken. Zie Tutorial: Infrastructuur en implementaties met meerdere clouds instellen en testen in Cloud Assembly.
WordPress-gebruiksscenario met bestaande of openbare netwerken en privé- of uitgaande netwerken	De inrichting mislukt omdat voor het netwerk informatie van een netwerkprofiel is vereist.	Zie de bovenstaande beschrijvingen voor een privénetwerk en een uitgaand netwerk. Zie Tutorial: Infrastructuur en implementaties met meerdere clouds instellen en testen in Cloud Assembly.
WordPress-gebruiksscenario met load balancer	De inrichting mislukt omdat voor een load balancer informatie van een netwerkprofiel is vereist. De inrichting kan plaatsvinden wanneer bestaande load balancers aanwezig zijn.	Er wordt een nieuwe load balancer gemaakt op basis van de configuratie van het netwerkprofiel. U kunt een bestaande load balancer opgeven die in het netwerkprofiel is ingeschakeld. De inrichting mislukt wanneer u een bestaande load balancer aanvraagt, maar er geen enkele aan de beperkingen in het netwerkprofiel voldoet. Zie Tutorial: Infrastructuur en implementaties met meerdere clouds instellen en testen in Cloud Assembly.

Instellingen voor beveiligingsgroepen gebruiken in netwerkprofielen en cloudsjabloonontwerpen in vRealize Automation

U kunt instellingen voor beveiligingsgroepen definiëren en wijzigen in netwerkprofielen en in cloudsjabloonontwerpen.

U kunt de mogelijkheden van de beveiligingsgroep op verschillende manieren gebruiken:

- Bestaande beveiligingsgroep die is opgegeven in een netwerkprofiel

U kunt een bestaande beveiligingsgroep toevoegen aan een netwerkprofiel. Wanneer een cloudsjabloonontwerp dat netwerkprofiel gebruikt, worden de machines gegroepeerd als leden van de beveiligingsgroep. Bij deze methode hoeft u geen resource van een beveiligingsgroep aan een cloudsjabloonontwerp toe te voegen. U kunt ook een load balancer in deze configuratie gebruiken. Voor gerelateerde informatie raadpleegt u [Meer informatie over load-balancerresources in vRealize Automation-cloudsjablonen](#).

- Beveiligingsgroepsonderdeel dat is gekoppeld aan machineresource in een cloudsjabloonontwerp

U kunt een resource van een beveiligingsgroep slepen en neerzetten in een cloudsjabloonontwerp en de resource van de beveiligingsgroep binden aan een machine-NIC met behulp van beperkingstags voor de bestaande beveiligingsgroep in het cloudsjabloonontwerp en op de bestaande beveiligingsgroep in de met gegevens verzamelde resource. U kunt deze koppeling ook maken door de objecten te verbinden met een verbindinglijn op het cloudsjabloonontwerpcanvas, vergelijkbaar met het koppelen van netwerken aan machines op het ontwerpcanvas.

Wanneer u een resource van een beveiligingsgroep naar het ontwerpcanvas voor cloudsjablonen sleept en neerzet, kan het type `existing` of `new` zijn. Als het een beveiligingsgroep van het type `existing` is, moet u een tagbeperkingswaarde toevoegen wanneer dit wordt gevraagd. Als het een beveiligingsgroep van het type `new` is, kunt u firewall-regels configureren.

- Een bestaande beveiligingsgroep die is toegewezen met tagbeperkingen en gekoppeld aan een machine-NIC in de cloudsjabloon

U kunt bijvoorbeeld een resource van een beveiligingsgroep koppelen aan een machine-NIC (in een machineresource) in het cloudsjabloonontwerp door tags tussen de twee resources te vergelijken.

Als voorbeeld voor NSX-T wanneer tags zijn opgegeven in het broneindpunt, kunt u NSX-T-tags gebruiken die zijn opgegeven in uw NSX-T-applicatie. U kunt dan een NSX-T-tag gebruiken die is opgegeven als een beperking op een netwerkresource in een cloudsjabloonontwerp, waarbij de netwerkresource is verbonden met een machine-NIC in het cloudsjabloonontwerp. Met NSX-T-tags kunt u machines dynamisch groeperen met behulp van een vooraf gedefinieerde NSX-T-tag met gegevensverzameling vanaf het NSX-T-broneindpunt. Gebruik een logische poort wanneer u de NSX-T-tag in NSX-T maakt.

- Firewallregels in een resource van een beveiligingsgroep op aanvraag in een cloudsjabloonontwerp

U kunt in het cloudsjabloonontwerp firewallregels toevoegen aan een beveiligingsgroep op aanvraag.

Zie [Meer informatie over beveiligingsgroep- en tagresources in vRealize Automation-cloudsjablonen](#) voor informatie over beschikbare firewall-regels.

Meer informatie

Zie [Meer informatie over netwerkprofielen in vRealize Automation](#) voor informatie over het definiëren van beveiligingsgroepen in netwerkprofielen.

Zie [Beveiligingsresources in vRealize Automation](#) voor informatie over het weergeven en wijzigen van instellingen voor beveiligingsgroepen op infrastructuurresourcepagina's.

Zie [Meer informatie over beveiligingsgroep- en tagresources in vRealize Automation-cloudsjablonen](#) voor informatie over het definiëren van beveiligingsgroepen in cloudsjabloonontwerpen.

Zie [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#) voor voorbeelden van beveiligingsgroepresources in cloudsjabloonontwerpen.

Instellingen voor load balancers in netwerkprofielen gebruiken in vRealize Automation

U kunt de load balancer-instellingen in uw netwerkprofielconfiguratie configureren.

U kunt een bestaande load balancer aan een netwerkprofiel toevoegen met behulp van het tabblad **Load Balancer**.

U kunt een load balancer toevoegen aan een cloudsjabloonontwerp door deze te koppelen aan een netwerkprofiel dat een of meer load balancers bevat of direct met behulp van een load-balancerresource in het ontwerpcanvas van de cloudsjabloon of de code.

Voorbeelden van het gebruik van een load balancer-VIP op basis van een beveiligingsgroep in een netwerkprofiel

Er zijn twee typen beveiligingsgroepen die u kunt gebruiken in een netwerkprofiel: een bestaande beveiligingsgroep die u selecteert op het tabblad **Beveiligingsgroepen** en een beveiligingsgroep op aanvraag die u maakt met behulp van een isolatiebeleid op het tabblad **Netwerkbeleid**.

Wanneer een load balancer-VIP is gekoppeld aan een beveiligingsgroep op basis van de instellingen van het netwerkprofiel, wordt de configuratie van de beveiligingsgroep geleverd door het netwerkprofiel.

In de volgende tabel ziet u enkele voorbeeldscenario's.

Cloudsjabloonontwerptopologie - gekoppelde resources	Netwerkprofielconfiguratie	Lidmaatschap beveiligingsgroep
Eenarmige load balancer met VIP op privénetwerk en een machine op hetzelfde privénetwerk.	Het geselecteerde netwerkprofiel gebruikt een isolatiebeleid dat is gedefinieerd als een beveiligingsgroep op aanvraag.	De machine-NIC en de load balancer-VIP worden toegevoegd aan de isolatiebeveiligingsgroep.
Eenarmige load balancer met VIP op privénetwerk en een machine op hetzelfde privénetwerk.	Het geselecteerde netwerkprofiel gebruikt een bestaande beveiligingsgroep en gebruikt een isolatiebeleid dat is gedefinieerd als een beveiligingsgroep op aanvraag.	De machine-NIC en de load balancer-VIP worden toegevoegd aan de isolatiebeveiligingsgroep en de bestaande beveiligingsgroep.
Tweearmige load balancer met VIP op een openbaar netwerk en machine op een privénetwerk.	Het geselecteerde netwerkprofiel gebruikt een bestaande beveiligingsgroep en gebruikt een isolatiebeleid dat is gedefinieerd als een beveiligingsgroep op aanvraag.	De machine-NIC en de load balancer-VIP worden toegevoegd aan de isolatiebeveiligingsgroep en de bestaande beveiligingsgroep.
Tweearmige load balancer met VIP op een openbaar netwerk en een machine op een privénetwerk.	Het geselecteerde netwerkprofiel gebruikt een bestaande beveiligingsgroep.	De machine-NIC en de load balancer-VIP worden toegevoegd aan de bestaande beveiligingsgroep.
Tweearmige load balancer, VIP bevindt zich op netwerk 1 en de machine bevindt zich op netwerk 2.	Twee netwerkprofielen: <ul style="list-style-type: none"> ■ Netwerkprofiel 1: gebruikt een bestaande beveiligingsgroep 1. ■ Netwerkprofiel 2: gebruikt een bestaande beveiligingsgroep 2. 	De load balancer belandt op netwerkprofiel 1 en de machine belandt op netwerkprofiel 2. De load balancer-VIP wordt toegevoegd aan beveiligingsgroep 1 en de machine-NIC wordt toegevoegd aan beveiligingsgroep 2.

Meer informatie

Zie [Meer informatie over load-balancerresources in vRealize Automation-cloudsjablonen](#) voor informatie over het toevoegen van load-balancerresources aan een cloudsjabloonontwerp.

Zie [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#) voor voorbeelden van cloudsjabloonontwerpen die load balancers bevatten.

Hoe configureer ik een netwerkprofiel om een netwerk op aanvraag te ondersteunen voor een externe IPAM-integratie in vRealize Automation

U kunt een netwerkprofiel configureren om blokken IP-adressen voor een netwerk op aanvraag te ondersteunen wanneer dat netwerkprofiel wordt gebruikt in een vRealize Automation-cloudsjabloon die gebruikmaakt van externe IPAM-integratie.

Door een bestaande integratie voor een bepaalde externe IPAM-provider te gebruiken, kunt u een netwerk op aanvraag inrichten om een nieuw netwerk in het externe IPAM-systeem te maken.

Met dit proces configureert u een blok met IP-adressen in plaats van een bovenliggende CIDR op te geven (zoals wordt gedaan bij het gebruik van de interne IPAM van vRealize Automation). Het IP-adresblok wordt gebruikt tijdens de provisioning van het netwerk op aanvraag om het nieuwe netwerk te segmenteren. De IP-blokken worden verzameld van de externe IPAM-provider, vooropgesteld dat de integratie netwerken op aanvraag ondersteunt. Als u bijvoorbeeld een Infoblox IPAM-integratie gebruikt, vertegenwoordigen IP-blokken Infoblox-netwerkcontainers.

Wanneer u een profiel van een netwerk op aanvraag en een externe IPAM-integratie in een cloudsjabloon gebruikt, treden de volgende gebeurtenissen op wanneer de cloudsjabloon wordt geïmplementeerd:

- Er wordt een netwerk gemaakt in de externe IPAM-provider.
- Er wordt ook een netwerk gemaakt in vRealize Automation, waarbij de nieuwe netwerkconfiguratie van de IPAM-provider wordt weergegeven, inclusief instellingen zoals CIDR- en gateway-eigenschappen.
- Het IP-adres van de geïmplementeerde virtuele machine wordt opgehaald van het nieuw gemaakte netwerk.

In dit voorbeeld van het netwerk op aanvraag configureert u een netwerkprofiel om een cloudsjabloonimplementatie toe te staan een machine in te richten op een netwerk op aanvraag in vSphere door Infoblox als externe IPAM-provider te gebruiken.

Zie [Hoe configureer ik een netwerkprofiel om een bestaand netwerk te ondersteunen voor een externe IPAM-integratie in vRealize Automation](#) voor gerelateerde informatie. De voorbeelden van de netwerkconfiguratie passen binnen de algemene werkstroom van de leverancier voor externe IPAM-integratie op [Tutorial: VMware Cloud on AWS voor vRealize Automation configureren](#).

Voorwaarden

Hoewel de volgende vereisten van toepassing zijn op de persoon die het netwerkprofiel maakt of bewerkt, is het netwerkprofiel zelf van toepassing wanneer het wordt gebruikt door een cloudsjabloonimplementatie die een IPAM-integratie bevat. Zie [Een externe IPAM-integratie in vRealize Automation configureren](#) voor meer informatie over leverancierspecifieke IPAM-integratiepunten.

Deze reeks stappen wordt weergegeven in de context van een integratiewerkstroom van de IPAM-provider. Zie [Tutorial: Een providerspecifieke externe IPAM-integratie voor vRealize Automation configureren](#).

- Controleer of u over cloudbeheerdersreferenties beschikt. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Controleer of u de gebruikersrol van cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Controleer of u een account bij de externe IPAM-provider hebt, bijvoorbeeld [Infoblox](#) of [Bluecat](#), en of u de juiste toegangsgegevens hebt voor het account van uw organisatie bij de IPAM-provider. In deze voorbeeldwerkstroom is Infoblox de IPAM-provider.

- Controleer of u over een IPAM-integratiepunt voor de IPAM-provider beschikt en dat het IPAM-pakket dat wordt gebruikt om de IPAM-integratie te maken netwerken op aanvraag ondersteunt. Zie [Een extern IPAM-integratiepunt voor Infoblox toevoegen in vRealize Automation](#).

Hoewel het Infoblox IPAM-pakket netwerken op aanvraag ondersteunt, moet u, als u een externe IPAM-integratie voor een andere provider gebruikt, controleren of hun IPAM-integratiepakket ondersteuning biedt voor netwerken op aanvraag.

Procedure

- 1 Als u een netwerkprofiel wilt configureren, klikt u op **Infrastructuur > Configureren > Netwerkprofielen**.
- 2 Klik op **Nieuw netwerkprofiel**.
- 3 Klik op het tabblad **Samenvatting** en geef de volgende voorbeeldinstellingen op:
 - Geef een vSphere-cloudaccount/-regio op, bijvoorbeeld **vSphere-IPAM-OnDemandA/Datacenter**.

In dit voorbeeld wordt uitgegaan van het gebruik van een vSphere-cloudaccount dat niet is gekoppeld aan een NSX-cloudaccount.
 - Geef het netwerkprofiel een naam, bijvoorbeeld **Infoblox-OnDemandNP**.
 - Voeg een capaciteitstag toe voor het netwerkprofiel, bijvoorbeeld **infoblox_ondemandA**.

Noteer de capaciteitstagwaarde, aangezien u deze ook moet gebruiken als een beperkingstag voor de cloudsjabloon om de netwerkprofielassociatie te maken die moet worden gebruikt bij het inrichten van de cloudsjabloon.
- 4 Klik op het tabblad **Netwerkbeleid** en geef de volgende voorbeeldinstellingen op:
 - Selecteer **Netwerk op aanvraag** in het vervolgkeuzemenu **Isolatiebeleid**.

Met deze optie kunt u externe IPAM IP-blokken gebruiken. Afhankelijk van het cloudaccount worden nieuwe opties weergegeven. De volgende opties worden bijvoorbeeld weergegeven wanneer u een vSphere-cloudaccount gebruikt dat is gekoppeld aan een NSX-cloudaccount:
 - Transportzone
 - Logische laag-0-router
 - Edge-cluster
In dit voorbeeld is het vSphere-cloudaccount niet gekoppeld aan NSX, zodat de menuoptie **Netwerkdomein** wordt weergegeven.
 - Laat de optie **Netwerkdomein** leeg.
- 5 Klik op **Extern** als adresbeheer **Bron**.
- 6 Klik op **IP-blok toevoegen** om de pagina **IPAM-IP-blok toevoegen** te openen.

- 7 Selecteer een bestaande externe IPAM-integratie in het menu **Provider** op de pagina **IPAM-IP-blok toevoegen**. Selecteer bijvoorbeeld het *Infoblox_Integration*-integratiepunt vanaf [Een extern IPAM-integratiepunt voor Infoblox toevoegen in vRealize Automation](#) in de voorbeeldwerkstroom.

- 8 Selecteer in het menu **Adresruimten** een van de beschikbare en vermelde IP-blokken, bijvoorbeeld **10.23.118.0/24** en voeg deze toe.

Als de IPAM-provider adresruimten ondersteunt, wordt het menu **Adresruimten** geopend. Voor een Infoblox-integratie worden adresruimten vertegenwoordigd door Infoblox-netwerkweergaven.

- 9 Selecteer een **Subnetgrootte**, zoals **/29 (-6 IP-adressen)**.

- 10 Klik op **Maken**.

Resultaten

Er wordt een netwerkprofiel gemaakt dat kan worden gebruikt om een netwerk op aanvraag in te richten met behulp van de opgegeven externe IPAM-integratie. De volgende voorbeeldcloudsjabloon toont één machine die wordt geïmplementeerd op een netwerk dat is gedefinieerd door dit nieuwe netwerkprofiel.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: ubuntu
      flavor: small
      networks:
        - network: '${resource.Cloud_Network_1.id}'
          assignment: static
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: private
```



```
constraints:
  - tag: infoblox_ondemanda
```

Opmerking Wanneer de cloudsjabloon is geïmplementeerd, wordt het eerste beschikbare netwerk in het opgegeven IP-blok opgehaald en als de netwerk-CIDR beschouwd. Als u een NSX-netwerk in het cloudsjabloon gebruikt, kunt u in plaats daarvan de CIDR van het netwerk handmatig instellen met behulp van de netwerkeigenschap `networkCidr`, zoals hieronder aangegeven, om handmatig een CIDR in te stellen en de instellingen voor IP-blokken en de grootte van het subnet te overschrijven die zijn opgegeven in het gekoppelde netwerkprofiel.

```
Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkCidr: 10.10.0.0/16
```

Hoe configureer ik een netwerkprofiel om een bestaand netwerk te ondersteunen voor een externe IPAM-integratie in vRealize Automation

U kunt een netwerkprofiel configureren om IP-adresbereiken voor een bestaand netwerk te ondersteunen wanneer dat netwerkprofiel wordt gebruikt in een vRealize Automation-blueprint die externe IPAM-integratie gebruikt.

Er wordt een voorbeeld gegeven binnen de context van een leverancierspecifieke voorbeeldwerkstroom op [Configureer een netwerk en netwerkprofiel voor het gebruik van externe IPAM voor een bestaand netwerk in vRealize Automation](#). De algemene leverancierspecifieke werkstroom voor externe IPAM-integratie is op [Tutorial: VMware Cloud on AWS voor vRealize Automation configureren](#).

Zie [Hoe configureer ik een netwerkprofiel om een netwerk op aanvraag te ondersteunen voor een externe IPAM-integratie in vRealize Automation](#) voor gerelateerde informatie.

Cloud Assembly-opslagprofielen toevoegen die aan verschillende vereisten voldoen

Een opslagprofiel van Cloud Assembly beschrijft het type opslag dat moet worden geïmplementeerd.

Voor opslag worden profielen doorgaans gemaakt aan de hand van kenmerken zoals het serviceniveau of de kosten, prestaties of het doel, zoals een back-up.

Selecteer **Infrastructuur > Configureren > Opslagprofielen** en klik op **Nieuw opslagprofiel**.

Meer informatie over opslagprofielen in vRealize Automation

Een cloudaccountregio bevat opslagprofielen waarmee de cloudbeheerder opslag voor de regio in vRealize Automation kan definiëren.

Wat doet een opslagprofiel

Opslagprofielen bevatten schijfaanpassingen en een manier om het type opslag te identificeren via capaciteitstags. Tags worden vervolgens afgestemd op beperkingen voor de inrichtingsserviceaanvraag om de gewenste opslagruimte te maken tijdens het implementeren.

Opslagprofielen worden ingedeeld onder clouds specifieke regio's. Eén cloudaccount kan meerdere regio's hebben, met verschillende opslagprofielen onder elke regio.

Leverancieronafhankelijke plaatsing is mogelijk. Stel bijvoorbeeld dat u drie verschillende leveranciersaccounts en een regio voor elk account hebt. Elke regio bevat een opslagprofiel dat voor capaciteit is getagd als *fast*. Tijdens het inrichten zoekt een aanvraag met een harde beperkingstag *fast* naar een overeenkomende capaciteit *fast*, ongeacht welke leverancierscloud de resources levert. Bij een overeenkomst worden de instellingen voor het gekoppelde opslagprofiel toegepast tijdens het maken van het geïmplementeerde opslagitem.

Opmerking Een andere cloudopslag kan verschillende prestatiekenmerken hebben, maar zal nog steeds worden beschouwd als het *fast* aanbod door de beheerder die deze heeft getagd.

Capaciteitstags die u aan opslagprofielen toevoegt, mogen geen werkelijke resourcedoelen identificeren. In plaats daarvan beschrijven ze typen opslag. Zie [Opslagresources in vRealize Automation](#) voor meer informatie over het inschakelen van werkelijke resources.

Standaardinrichtingstype

Het inrichtingstype van het opslagprofiel bepaalt alleen een standaardgedrag. De instelling heeft niet noodzakelijk invloed op de plaatsing en kan worden overschreven door een eigenschap in de cloudsjabloon.

U kunt bijvoorbeeld het opslagprofiel voor thin provisioning instellen. In de meeste gevallen maken aanvragen standaard opslag met thin provisioning. Als de eigenschap `provisioningType` voor de cloudsjabloon op eager-zero is ingesteld, overschrijft de cloudsjabloon echter de standaardoptie thin.

Opmerking Wanneer u exacte controle wilt, is het beter om capaciteits- en beperkingstags toe te voegen die zijn gelabeld voor het gewenste inrichtingstype.

Voor de inrichtingstypestandaard overschrijft een cloudsjablooneigenschap een opslagprofielstandaard en overschrijft een opslagprofielstandaard een standaard van een vCenter-opslagbeleid.

Schijftoewijzing met machines

In een project met meerdere cloudzones die tot verschillende cloudaccounts behoren, volgt een schijf de machine, zelfs als de schijf niet aan de machine is gekoppeld. Dit gedrag houdt de resources bij elkaar om fouten te voorkomen wanneer u ervoor kiest de schijf later te koppelen.

Het volgende ontwerp werkt bijvoorbeeld niet. De cloudsjabloon probeert locatiebeperkingen te gebruiken om de schijf te scheiden, maar de implementatie retourneert in plaats daarvan de fout `No matching placement`.

Als u een schijf in een ander cloudaccount moet plaatsen, gebruikt u een afzonderlijke implementatie om de schijf te implementeren.

```
resources:
  Machine1:
    type: Cloud.vSphere.Machine
    properties:
      image: ubuntu
      flavor: small
      constraints:
        - tag: 'location:siteA'
  Disk1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
      constraints:
        - tag: 'location:siteB'
```

Eersteklasschijven en standaardschijven

Met behulp van de optie **Schijftype** op de pagina Opslagprofiel of de vRealize Automation-API kunt u een opslagprofiel maken ter ondersteuning van FCD- (eersteklasschijf) of standaardschijfopslag. De FCD-optie maakt een vSphere-opslagprofiel.

■ Eersteklasschijf

Eersteklasschijven kunnen onafhankelijk van een virtuele vSphere-machine bestaan. Een eersteklasschijf heeft ook levenscyclusbeheermogelijkheden die onafhankelijk van een virtuele machine kunnen werken. Eersteklasschijven zijn beschikbaar voor vSphere 6.7 Update 2 en hoger, en worden momenteel in vRealize Automation geïmplementeerd als alleen-API-functie.

Zie [Wat kan ik doen met de eersteklasschijfopslag in vRealize Automation](#) voor informatie over de FCD-opslag, inclusief de mogelijkheden die beschikbaar zijn in de vRealize Automation-API, en voor koppelingen naar de API-documentatie zelf.

■ Standaardschijf

Standaardschijfopslag wordt gemaakt en beheerd als geïntegreerd onderdeel van een virtuele machine.

Zie [Wat kan ik doen met standaardschijfopslag in vRealize Automation](#) en [Wat kan ik doen met persistente schijfopslag in vRealize Automation](#) voor meer informatie over standaardschijfopslag.

Schijfversleuteling aan Azure-serverzijde

Als u voor Azure-resources versleuteling in een opslagprofiel voor een beheerde schijf wilt ondersteunen, selecteert u ook schijfversleuteling met een gekoppelde sleutel. De beschikbare versleuteling en sleutels komen overeen met de schijfversleutelingssets die in Azure zijn geconfigureerd voor de locatie.

Microsoft Azure

Search resources, services, and docs (G+)

Home >

Disk Encryption Sets

+ Add Manage view Refresh Export to CSV Open query Assign tags Feedback

Filter for any field... Subscription == R&D Resource group == all Location == all Add filter

Showing 1 to 100 of 305 records.

Name	Resource group	Location	Key
MyDES	DiskEncryptionSets	West US	WestUSKey...
MyDES1	DiskEncryptionSets	West US	WestUSKey...
MyDES10	DiskEncryptionSets	West US	WestUSKey...
MyDES100	DiskEncryptionSets	West US	WestUSKey...
MyDES101	DiskEncryptionSets	West US	WestUSKey...

Account / region * AzureAcc / West US

Name * SP-with-des

Description

Storage type * Managed disks

Disk type * Standard HDD

OS disk caching * Read only

Data disk caching * Read only

Supports encryption ☒

Encryption set Search for encryption set

Capability tags

CREATE CANCEL

MyDES

WestUSKeyForDisk

MyDES1

WestUSKeyForDisk

MyDES10

WestUSKeyForDisk

MyDES100

WestUSKeyForDisk

MyDES101

WestUSKeyForDisk

EncryptDiskWestUS

EncryptDiskWestUS

EncryptDiskWestUS

EncryptDiskWestUS

EncryptDiskWestUS

Prijskaarten gebruiken in vRealize Automation

Cloud Assembly-prijskaarten helpen cloudbeheerders om het prijsbeleid te definiëren en toe te wijzen voor de financiële impact van uw individuele implementaties om u te helpen bij het beheren van resources.

Opmerking Voor de goede werking van prijzen in omgevingen met meerdere tenants moet u een afzonderlijke vRealize Operations Manager-instantie hebben voor elke vRealize Automation-tenant.

Prijskaarten bepalen de tarieven voor een prijsbeleid. Het prijsbeleid kan vervolgens aan specifieke projecten worden toegewezen om een totaalprijs te definiëren. Nadat u een vRealize Operations Manager- of CloudHealth-eindpunt heeft gemaakt, is er een vooraf gedefinieerde standaardtariefkaart beschikbaar met kosten die overeenkomen met de prijsconfiguratie op het tabblad **Infrastructuur > Prijskaarten**. U kunt prijskaarten maken die van toepassing zijn op alleen projecten of op cloudzones. Alle nieuwe prijskaarten worden standaard toegepast op projecten.

Opmerking Als u de instelling **Alle prijskaarten worden toegepast op** wijzigt, worden alle bestaande prijskaarttoewijzingen verwijderd. Als het vRealize Operations Manager-eindpunt wordt verwijderd uit Cloud Assembly, worden ook alle prijskaarten en toewijzingen verwijderd.

De prijs van een implementatie in de loop van de tijd wordt op zowel de implementatiekaart als op het project weergegeven als de prijs van maand tot heden, die aan het begin van elke maand opnieuw wordt ingesteld op nul. De kostenspecificaties van het onderdeel zijn beschikbaar in de implementatiedetails. Als u deze informatie op het niveau van de implementatie opgeeft, informeert u de cloudbeheerder, maar helpt u ook leden meer inzicht te krijgen in de impact van hun werk op budgetten en ontwikkeling op lange termijn.

U kunt ervoor kiezen de prijsinformatie van gebruikers in Cloud Assembly en Service Broker weer te geven door de knop **Prijsinformatie weergeven** te selecteren. Als deze optie is uitgeschakeld, wordt de prijsinformatie verborgen voor Cloud Assembly- en Service Broker-gebruikers.

Hoe wordt de prijs berekend?

De oorspronkelijke prijs die u ziet op het niveau van de implementatie voor uw berekenings- en opslagresources, zijn gebaseerd op standaardbenchmarktarieven uit de sector en worden vervolgens berekend in de loop van de tijd. Het tarief wordt op hosts toegepast en de service berekent de CPU- en geheugentarieven. De server berekent de prijs elke 6 uur opnieuw.

Nieuwe beleidsregels, toewijzingen en prijzen vooraf worden vastgesteld tijdens de volgende gegevensverzamelingscyclus. De gegevensverzamelingscyclus wordt standaard elke 5 minuten uitgevoerd. Het kan 6 uur duren voordat nieuwe beleidsregels of wijzigingen in projecten en implementaties zijn bijgewerkt.

Hoe schat ik de prijs van al mijn implementaties en projecten?

Voordat u een catalogusitem implementeert, kunt u de 'prijs vooraf' als prijsraming voor uw implementatie gebruiken. Als u de prijs in Cloud Assembly wilt weergeven, moet u een vRealize Operations Manager-integratie-eindpunt hebben geconfigureerd met prijscalculatie ingeschakeld en valuta vooraf ingesteld.

Daily Price Estimate



Guest OS and one time prices are excluded in this estimate.



price-service-f309c00

\$0.54



Cloud_vSphere_Machine_1

\$0.53

Compute

\$0.39

Storage

\$0.03

Additional charges

\$0.11



Cloud_vSphere_Disk_1

\$0.01

Storage

\$0.01

CLOSE

Voor een prijsschatting vooraf is de grootte van de opstartschijf per VM altijd 8 GB.

De 'prijs vooraf' van een implementatie is een dagelijkse prijsschatting, gebaseerd op de toewijzing van een resource, voor een bepaald catalogusitem voordat het wordt geïmplementeerd. Nadat een catalogusitem is geïmplementeerd, kunt u de maand-tot-datum-prijs weergeven als een samenvoeging van de 'prijs vooraf' op de tabbladen **Implementatie** en **Infrastructuur > Projecten**. Prijscalculatie vooraf wordt ondersteund voor privécloudresources zoals vSphere-machine en vSphere-schijf, Cloud Assembly-catalogusitems en cloudonafhankelijke items met vCenter geconfigureerd voor privécloud.

Opmerking Prijscalculatie vooraf wordt niet ondersteund voor publieke cloudresources, of privécloudresources van niet-vSphere-machines of -schijven.

Om de kosten van uw implementatie te schatten, selecteert u in de catalogus een catalogusitem en klikt u **Aanvragen > Berekenen**. Als de prijs acceptabel is, klikt u op **Verzenden**.

U kunt de prijskaarten voor projecten gebruiken om de totale prijs van al uw projecten te schatten.

Om de kosten van een project te schatten, klikt u op de pagina **Infrastructuur > Prijskaart** naast **Alle prijskaarten worden toegepast op** op **Bewerken** en selecteert u **Projecten**.

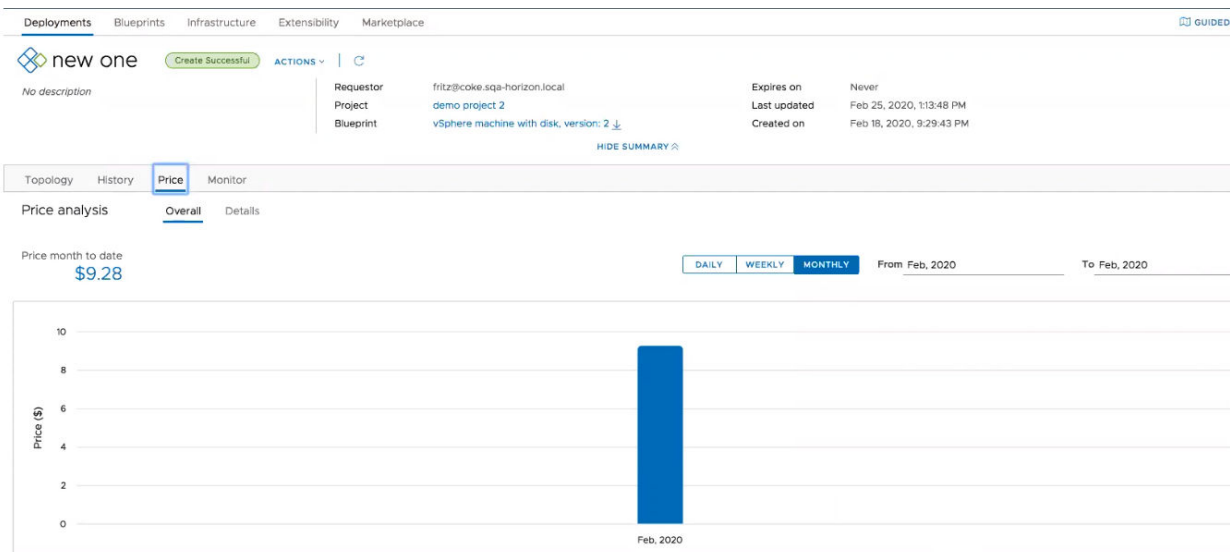
Als u de instelling **Alle prijskaarten worden toegepast op** wijzigt, worden alle bestaande prijskaarttoewijzingen verwijderd. Maak prijskaarten en -toewijzingen met behulp van een op kosten gebaseerde benadering.

Prijskaarten voor vSphere en VMC maken

U kunt een prijskaart maken en toewijzen aan projecten of cloudzones, afhankelijk van de strategie voor prijzen die door de cloudbeheerder is bepaald voor privécloudimplementaties.

Prijskaarten kunnen worden aangepast op basis van door gebruikers geselecteerde parameters. Nadat u een prijskaart heeft geconfigureerd, kunt u deze toewijzen aan een of meer projecten en cloudzones die worden bepaald door de prijsstrategie.

U kunt de prijsserver op elk gewenst moment handmatig vernieuwen op de vROps-eindpuntpagina: **Infrastructuur > Integraties > vROps-eindpunt > .** Klik in de sectie vCenter-servers op **Synchronisatie**. Wanneer u de prijsserver handmatig vernieuwt met behulp van de optie **Synchronisatie**, wordt de prijs opnieuw berekend voor alle projecten in de organisatie. Afhankelijk van het aantal projecten dat uw organisatie heeft, kan dit proces intensief zijn en tijd in beslag nemen.



Na het maken en toewijzen van een prijskaart kunt u de prijsgeschiedenis van uw implementaties en projecten bekijken. Om de prijsgeschiedenis weer te geven, navigeert u naar uw implementatie en klikt u op **Prijs**. De prijsanalyse biedt een overzicht en gedetailleerde weergave van de implementatieprijs samen met de prijswaarde van maand tot heden. U kunt de grafische weergave wijzigen om de implementatieprijs weer te geven als dagelijkse, wekelijkse of maandelijkse waarden. U kunt ook een exact datumbereik of exacte maand opgeven voor de prijsgeschiedenis.

Als u de prijsspecificaties per kostonderdeel wilt weergeven, klikt u op **Details**.

Prijzen worden bepaald door typen geprijsde onderdelen.

Tabel 4-1. Typen geprijsde onderdelen

Type blueprintonderdeel	Servicenaam/objecttype	Type blueprintresource	Opmerkingen
Cloudonafhankelijke	machine	Cloud.Machine	Als een cloudonafhankelijke machine is geconfigureerd met vSphere, kunt u de implementatiekosten bekijken.
	Schijf	Cloud.Volume	Als een cloudonafhankelijke schijf is gekoppeld aan een virtuele machine die is geconfigureerd met vSphere, kunt u de implementatiekosten bekijken.
vSphere	vSphere-machine	Cloud.vSphere.Machine	Geïmplementeerd met een clouds specifieke blueprint.
	vSphere-schijf	Cloud.vSphere.Disk	Geïmplementeerd met een clouds specifieke blueprint die is gekoppeld aan een virtuele machine.
VMware Managed Cloud (VMC)	vSphere-machine	Cloud.vSphere.Machine	VMC ondersteunt alleen op tarieven gebaseerde prijskaarten (op kosten gebaseerde prijskaarten worden niet ondersteund).
	vSphere-schijf	Cloud.vSphere.Disk	

Voorwaarden

Voordat u prijskaarten kunt maken of toewijzen, moet u prijscalculatie configureren en inschakelen en valuta in vRealize Operations configureren om met vRealize Automation te werken. Wanneer u vRealize Operations met vRealize Automation configureert, moet u ervoor zorgen dat beide applicaties op dezelfde tijdzone zijn ingesteld. Als u de tijdzone in vRealize Operations wilt configureren, schakelt u SSH in en meldt u zich aan bij elk vRealize Operations-knooppunt, bewerkt u het bestand `$ALIVE_Base/user/conf/analytics/advanced.properties` en voegt u `timeZoneUsedInMeteringCalculation =<time zone> toe`.

Voor de goede werking van prijzen in omgevingen met meerdere tenants moet u een afzonderlijke vROps-instantie hebben voor elke vRA-tenant.

U moet een vRealize Operations-eindpunt configureren voordat u prijskaarten kunt configureren. Om het vRealize Operations-eindpunt te configureren, navigeert u naar **Infrastructuur > Verbindingen > Integraties > Integratie toevoegen**.

Opmerking Wanneer meerdere vRealize Operations-eindpunten worden toegevoegd, mogen ze niet hetzelfde vCenter volgen.

Procedure

- 1 Navigeer naar **Infrastructuur > Prijskaart > Nieuwe prijskaart**.
- 2 Voer op het tabblad Samenvatting een naam en beschrijving in voor de prijskaart. Nadat het beleid is gedefinieerd op het tabblad Prijzen, wordt de overzichtstabel ingevuld met tarieven voor de prijskaart.

Opmerking De valuta-eenheid wordt bepaald door de waarde die is geselecteerd in vRealize Operations.

- 3 Optioneel. Schakel het selectievakje **Standaardinstelling voor niet-toegewezen projecten?** in om deze prijskaart standaard toe te wijzen aan alle niet-toegewezen projecten.

4 Klik op **Prijs** en configureer de details van uw prijsbeleid.

Tabel 4-2. Configuratie van prijsbeleid

Parameter	Beschrijving
Basistoelagen	<p>Voer een naam en een beschrijving in voor uw beleid. Selecteer op basis van kosten of tarief.</p> <ul style="list-style-type: none"> ■ Kosten - De kosten worden gedefinieerd in vRealize Operations. Indien geselecteerd, is een vermenigvuldigingsfactor vereist. Als u bijvoorbeeld 1,1 als factor selecteert, worden de kosten vermenigvuldigd met 1,1, wat resulteert in een stijging van 10% ten opzichte van de berekende kosten. De prijsvergelijking met kosten is: $\text{<kosten>} \times \text{<vermenigvuldigingsfactor>} = \text{prijs}$ ■ Tarief - Als dit is geselecteerd, moet u absolute waarden gebruiken om de kosten te bepalen. De prijsvergelijking met tarief is: $\text{<Tarief>} = \text{prijs}$. Selecteer een tariefinterval in de vervolgkeuzelijst om op te geven hoe dit tarief in rekening moet worden gebracht. <p>In de sectie met basiskosten definieert u de kosten of het tarief voor CPU, geheugen, opslag en aanvullende diverse kosten.</p>
Gastbesturingssystemen	<p>U kunt de toeslag van een gastbesturingssysteem definiëren door op Toeslag toevoegen te klikken. Voer de naam van het gastbesturingssysteem in en definieer de toeslagmethode en het basistarief.</p> <ul style="list-style-type: none"> ■ Terugkerend - Voer een basistarief in en definieer een terugkerend interval als toeslagperiode. De absolute tariefwaarde is vereist en wordt toegevoegd aan de totale prijs. ■ Eenmalig - Definieer de eenmalige toeslag van het basistarief. De absolute waarde is vereist en wordt toegevoegd als eenmalige prijs. ■ Tariefactor - Er is een vermenigvuldigingsfactor vereist die wordt toegepast op de geselecteerde toeslagcategorie. Bijvoorbeeld: als u CPU-toeslag en tariefactor 2 selecteert. De CPU van het gastbesturingssysteem wordt als 2 keer de standaardkosten in rekening gebracht. <p>U kunt meerdere gastbesturingssystemen met verschillende tarieven toevoegen door op Toeslag toevoegen te klikken en een extra toeslagbeleid te configureren.</p> <hr/> <p>Opmerking Er worden geen 'toeslagen vooraf' voor gastbesturingssystemen weergegeven op de samenvattingspagina, hoewel ze deel uitmaken van het beleid.</p>

Tabel 4-2. Configuratie van prijsbeleid (vervolg)

Parameter	Beschrijving
Tags	<p>U kunt een tagtoeslag definiëren door op Toeslag toevoegen te klikken.</p> <p>Selecteer de tagnaam en definieer de toeslagmethode en het basistarief.</p> <ul style="list-style-type: none"> ■ Terugkerend - Voer een basistarief in en definieer een terugkerend interval als toeslagperiode. De absolute tariefwaarde is vereist en wordt toegevoegd aan de totale prijs. ■ Eenmalig - Definieer de eenmalige toeslag van het basistarief. De absolute waarde is vereist en wordt toegevoegd als eenmalige prijs. ■ Tarieffactor - Er is een vermenigvuldigingsfactor vereist die wordt toegepast op de geselecteerde toeslagcategorie. <p>Selecteer hoe u de tag in rekening wilt brengen op basis van de ingeschakelde status.</p> <p>U kunt meerdere tags met verschillende tarieven toevoegen door te klikken op Toeslag toevoegen en een extra toeslagbeleid te configureren.</p> <hr/> <p>Opmerking Extra toeslagen in de berekende uiteindelijke prijs zijn inbegrepen in tags op VM's en bevatten geen tags op schijven en netwerken.</p>
Aangepaste eigenschappen	<p>U kunt een aangepaste eigenschapstoeslag definiëren door op Toeslag toevoegen te klikken.</p> <p>Voer de eigenschapsnaam en -waarde in en definieer de toeslagmethode en het basistarief.</p> <ul style="list-style-type: none"> ■ Terugkerend - Voer een basistarief in en definieer een terugkerend interval als toeslagperiode. De absolute tariefwaarde is vereist en wordt toegevoegd aan de totale prijs. ■ Eenmalig - Definieer de eenmalige toeslag van het basistarief. De absolute waarde is vereist en wordt toegevoegd als eenmalige prijs. ■ Tarieffactor - Er is een vermenigvuldigingsfactor vereist die wordt toegepast op de geselecteerde toeslagcategorie. <p>Selecteer hoe u de aangepaste eigenschap in rekening wilt brengen op basis van de ingeschakelde status.</p> <p>U kunt meerdere aangepaste eigenschappen met verschillende tarieven toevoegen door op Toeslag toevoegen te klikken en een extra toeslagbeleid te configureren.</p>
Algemene toeslagen	<p>Definieer een extra toeslag die u aan het prijsbeleid wilt toevoegen. U kunt zowel eenmalige als terugkerende toeslagen toevoegen.</p>

Eenmalige toeslagen worden niet weergegeven in de prijsraming van een catalogusitem of op het tabblad Samenvatting. Alleen de raming van de dagprijs voor een bepaald catalogusitem wordt weergegeven.

- 5 Klik op het tabblad **Toewijzingen** en klik vervolgens op **Projecten toewijzen**. Selecteer een of meer projecten waaraan u de prijskaart wilt toewijzen.

Opmerking Standaardprij斯卡arten worden toegepast op projecten. Op het tabblad **Infrastructuur > Prij斯卡arten** kunt u selecteren om prij斯卡arten toe te passen op de cloudzones. Als u cloudzones heeft geselecteerd, klikt u op **Cloudzones toewijzen** op het tabblad Toewijzingen.

- 6 Klik op **Maken** om uw prijsbeleid te maken en op te slaan.

Resultaten

Uw nieuwe prijsbeleid wordt weergegeven op de pagina Prij斯卡arten. Klik op **Openen** om de details en de configuratie van het beleid weer te geven of te bewerken.

Tags gebruiken om Cloud Assembly-resources en -implementaties te beheren

Tags zijn een essentieel onderdeel van Cloud Assembly en sturen de plaatsing van implementaties via het afstemmen van mogelijkheden en beperkingen. U moet tags begrijpen en effectief implementeren om optimaal gebruik te maken van Cloud Assembly.

Tags zijn labels die u aan Cloud Assembly items toevoegt. U kunt elke tag maken die geschikt is voor uw organisatie en implementatie. Tags fungeren als meer dan alleen labels, omdat tags bepalen hoe en waar Cloud Assemblyresources en infrastructuur gebruikt om implementeerbare services te bouwen. Tags ondersteunen ook governance in Cloud Assembly.

Tagstructuur

Tags moeten de conventie van het paar `name:value` volgen, maar voor het overige heeft hun constructie grotendeels een vrije vorm. In Cloud Assembly worden alle tags op dezelfde manier weergegeven en wordt de tagfunctionaliteit bepaald door de context.

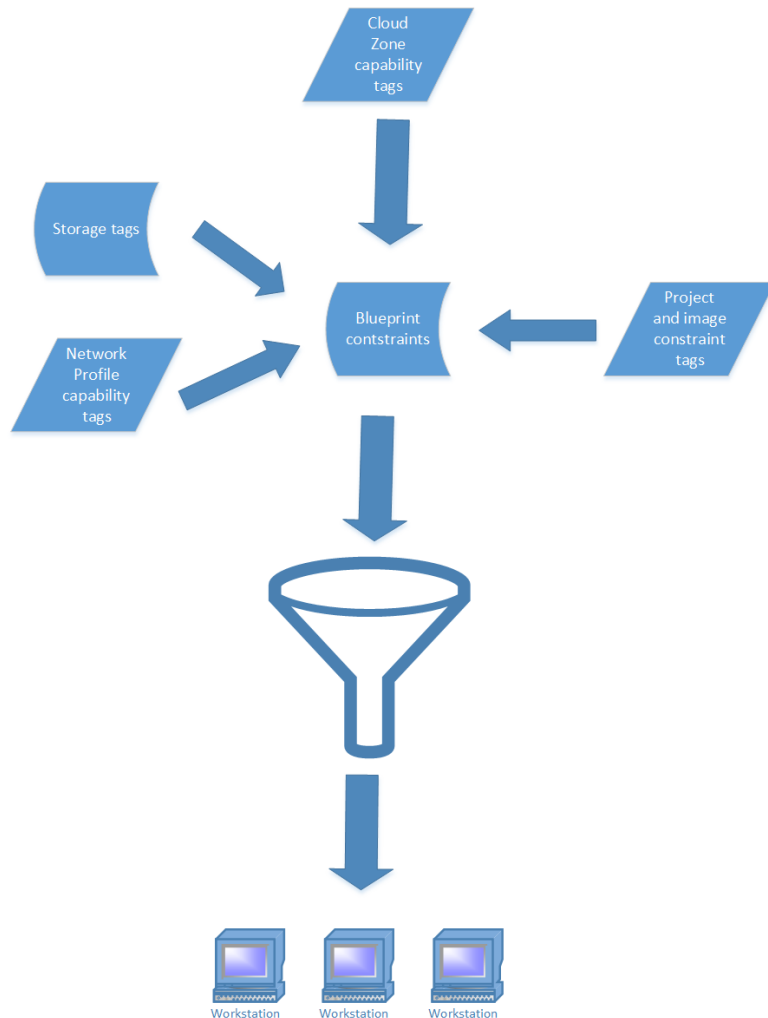
Tags in infrastructuurresources werken bijvoorbeeld hoofdzakelijk als capaciteitstags omdat Cloud Assembly deze gebruikt om resources af te stemmen op implementaties. Ze kunnen ook de resources identificeren.

Tagfunctie

De primaire functie van tags is om de mogelijkheden en beperkingen uit te drukken die Cloud Assembly gebruiken om implementaties te definiëren. Context bepaalt de functie van tags. Tags die in cloudzones, netwerk- en opslagprofielen zijn geplaatst, en individuele infrastructuurresources functioneren als capaciteitstags en definiëren de gewenste capaciteiten voor infrastructuur die wordt gebruikt in implementaties. Tags die op de cloudsjabloonfunctie

worden geplaatst, fungeren als beperkingen die resources voor implementaties definiëren. Daarnaast kunnen cloudbeheerders beperkingstags op projecten plaatsen om een vorm van governance voor die projecten toe te passen. Deze beperkingstags worden toegevoegd aan andere beperkingen die in cloudsjablonen worden gebruikt.

Tijdens het inrichten stemt Cloud Assembly deze capaciteiten af op beperkingen, die ook als tags worden uitgedrukt, in cloudsjablonen voor het definiëren van de implementatieconfiguratie. Deze taggebaseerde capaciteits- en beperkingsfunctionaliteit legt de basis voor implementatieconfiguratie in Cloud Assembly. U kunt bijvoorbeeld tags gebruiken om de infrastructuur alleen voor PCI-resources in een bepaalde regio beschikbaar te maken.



Op een secundair niveau kunnen tags ook nuttig zijn bij het zoeken en identificeren van opslag- en netwerkitems en andere infrastructuurresources.

Stel bijvoorbeeld dat u cloudzones instelt en dat er veel berekeningsresources beschikbaar zijn. Als u uw berekeningsresources op de juiste wijze hebt getagd, kunt u de zoekfunctie op het tabblad Berekenen van de pagina Cloudzone gebruiken om de resources te filteren die aan die specifieke cloudzone zijn gekoppeld.

De pagina Tagbeheer van Cloud Assembly en de configuratiepagina's voor resources bevatten bovendien zoekfuncties waarmee u items kunt zoeken op tagnamen. Het gebruik van logische en leesbare tags voor deze items is essentieel om deze zoek- en identificatiefunctie mogelijk te maken.

Bekijk de volgende YouTube-video voor meer informatie en voorbeelden van taggebruik: <https://youtu.be/4zNQ33RyQio>

Externe tags

Cloud Assembly kan ook externe tags bevatten. Deze tags worden automatisch geïmporteerd van cloudaccounts die u aan een instantie van Cloud Assembly koppelt. Deze tags kunnen vanuit vSphere, AWS, Azure of andere externe softwareproducten worden geïmporteerd. Nadat de tags zijn geïmporteerd, zijn deze op dezelfde manier als door gebruikers gemaakte tags beschikbaar voor gebruik.

Tags beheren

U kunt de pagina Tagbeheer in Cloud Assembly gebruiken om uw tagbibliotheek bij te houden en te beheren. U kunt op deze pagina ook tags maken. Daarnaast is de pagina Tagbeheer de enige pagina waarop u externe tags kunt weergeven en identificeren.

The screenshot displays the 'Tag Management' page in the vRealize Automation Cloud Assembly interface. The left sidebar shows a navigation menu with sections like 'Configure', 'Resources', and 'Activity'. The main content area is titled 'Tag Management' and includes a 'Tags' tab. Below the tab, there are buttons for '+ NEW TAG', 'FIND TAG USAGE', and 'DELETE'. A search filter is also present. The central part of the page features a table with two columns: 'Key' and 'Value'. The table contains the following entries:

Key	Value
a	
AAA	sofiaaaa
aktag1	val1
alex	kris
AppID	ABC
AppID	XYZ
applicationtier	tango-machine
Application Tier	tango-machine
Application Tier	
astoyanov-rp	
Atos-Tagging-Category	Atos-Storage-Tag
AutomaticCleanExpirationTime	2019-01-08T08:45:33.127Z

At the bottom right of the table, it indicates '215 tags'.

Tagstrategie

Om verwarring te minimaliseren, moet u een geschikte codestrategie en coderingsconventies ontwerpen voordat u tags in Cloud Assembly maakt, zodat alle gebruikers die tags maken en gebruiken, begrijpen wat deze betekenen en hoe deze moeten worden gebruikt. Zie [Een tagstrategie maken](#).

Een tagstrategie maken

U moet zorgvuldig een geschikte tagstrategie plannen en implementeren op basis van de IT-structuur en doelstellingen van uw organisatie om het maximum te halen uit de Cloud Assembly-functionaliteit en mogelijke verwarring tot een minimum te beperken.

Terwijl tags verschillende algemene doelen dienen, moet uw tagstrategie zijn afgestemd op de behoeften, structuur en doelstellingen van uw implementatie.

Aanbevolen procedures voor het gebruik van tags

Enkele algemene kenmerken van een effectieve tagstrategie:

- Ontwerp en implementeer een samenhangende tagstrategie die bij de structuur van uw bedrijf past en maak deze strategie bekend aan alle betrokken gebruikers. Een strategie moet uw implementatiebehoeften ondersteunen, duidelijke mensentaal gebruiken en begrijpelijk zijn voor alle betrokken gebruikers.
- Gebruik eenvoudige, duidelijke en herkenbare namen en waarden voor tags. Tagnamen voor opslag- en netwerkitems, bijvoorbeeld, moeten duidelijk en samenhangend zijn zodat gebruikers de toegewezen tags die ze selecteren of bekijken voor een geïmplementeerde bron direct begrijpen.
- U kunt tags maken met een naam zonder waarde, maar het is beter om een toepasselijke waarde te maken voor elke tagnaam, omdat dit het taggebruik duidelijk maakt voor andere gebruikers.
- Vermijd het maken van dubbele of externe tags. Maak bijvoorbeeld alleen tags voor opslagitems die zijn gerelateerd aan opslagproblemen.

Implementatie van tags

Bepaal uw voornaamste overwegingen voor een standaard tagstrategie. Hierna volgen enkele algemene overwegingen om rekening mee te houden bij het bepalen van uw strategie. Houd er rekening mee dat deze overwegingen eerder representatief dan definitief zijn. Mogelijk zijn er andere overwegingen die zeer relevant zijn voor uw gebruikssituaties. Uw specifieke strategie moet geschikt zijn voor uw specifieke gebruikssituaties.

- In hoeveel verschillende omgevingen gaat u implementeren? Doorgaans maakt u tags die elke omgeving voorstellen.
- Hoe zijn uw computerbronnen gestructureerd en hoe gebruikt u ze om implementaties te ondersteunen.
- In hoeveel verschillende regio's of locaties implementeert u? Doorgaans maakt u tags op profielniveau die deze verschillende regio's of locaties voorstellen.
- Hoeveel verschillende opslagopties zijn er beschikbaar voor implementaties en welke kenmerken wilt u ze geven? Deze opties moeten worden voorgesteld door tags.
- Categoriseer uw netwerkopties en maak tags voor alle toepasselijke opties.

- Typische implementatievariabelen. Bijvoorbeeld: in hoeveel verschillende omgevingen gaat u implementeren? De meeste organisaties hebben minimaal een test-, ontwikkelings- en productieomgeving. U doet er goed aan overeenkomende beperkingstags en capaciteitstags voor cloudzones te maken en te coördineren, zodat u eenvoudig implementaties kunt instellen in een of meer van deze omgevingen.
- Coördineer tags voor netwerk- en opslagbronnen zodat ze logisch zijn in de context van de netwerk- en opslagprofielen waarin ze worden gebruikt. De brontags kunnen dienen om de implementatie van de bronnen nauwkeuriger te beheren.
- Zorg dat capaciteitstags voor cloudzones en netwerkprofielen, en andere capaciteitstags, worden gecoördineerd met beperkingstags. Doorgaans maakt uw beheerder eerst capaciteitstags voor cloudzones en netwerkprofielen en vervolgens kunnen andere gebruikers cloudsjablonen ontwerpen met beperkingen die overeenkomen met deze capaciteitstags.

Nadat u inzicht hebt gekregen in de belangrijke overwegingen voor uw organisatie, kunt u geschikte tagnamen plannen die op een logische manier rekening houden met deze overwegingen. Maak vervolgens een overzicht van uw strategie en maak dit beschikbaar voor alle gebruikers met rechten om tags te maken of bewerken.

Als handige implementatiebenadering kunt u beginnen met het afzonderlijk taggen van al uw computerinfrastructuurbronnen. Zoals gezegd gebruikt u het beste logische categorieën voor tagnamen die verband houden met de specifieke bron. U kunt bijvoorbeeld de tags tier1, tier2, etc. gebruiken voor opslagbronnen. Ook kunt u zich bij het taggen van computerbronnen baseren op hun besturingssysteem, zoals Windows, Linux, etc.

Na het taggen van bronnen kunt u vervolgens overwegen om tags te maken voor cloudzones en opslag- en netwerkprofielen die het beste aan uw behoeften voldoen.

Capaciteitstags in Cloud Assembly gebruiken

In Cloud Assembly kunt u met capaciteitstags implementatiecapaciteiten definiëren voor infrastructuuronderdelen. Samen met de beperkingen werken ze als basis voor plaatsingslogica in vRealize Automation.

U kunt capaciteitscodes voor berekeningsresources, cloudzones, images en imageroewijzingen en netwerken en netwerkprofielen maken. De pagina's voor het maken van deze resources bevatten opties voor het maken van capaciteitstags. U kunt ook de pagina Tagbeheer in Cloud Assembly gebruiken om capaciteitstags te maken. Capaciteitstags in cloudzones en netwerkprofielen zijn van invloed op alle resources in die zones of profielen. Capaciteitstags in opslag- of netwerkoonderdelen zijn alleen van invloed op de onderdelen waarop ze worden toegepast.

Doorgaans kunnen capaciteitstags kenmerken zoals locatie voor een computerbron, adaptertype voor een netwerk of laagniveau voor een opslagresource definiëren. Deze kunnen ook omgevingslocatie of -type en andere zakelijke overwegingen definiëren. Net als bij uw algemene tagstrategie moet u uw capaciteitstags op een logische manier indelen voor uw bedrijfsbehoeften.

Cloud Assembly komt overeen met capaciteitstags in cloudzones met beperkingen voor cloudsjablonen tijdens de implementatie. Dus wanneer u capaciteitstags maakt en gebruikt, moet u dit begrijpen en plannen om de juiste cloudsjabloonbeperkingen te maken zodat afstemming verloopt zoals verwacht.

Bijvoorbeeld: in de sectie over cloudzone in het [Deel 1: het voorbeeld van de Cloud Assembly-infrastructuur configureren](#) die in de documentatie is opgenomen, wordt beschreven hoe u dev- en testtags voor de cloudzones OurCo-AWS-US-East en OurCo AWS-US-West kunt maken. In deze tutorial geven deze tags aan dat de zone OurCo-AWS-US-East een ontwikkelingsomgeving is en dat de zone OurCo-AWS-US_West een testomgeving is. Als u analoge beperkingstags in cloudsjablonen maakt, kunt u met deze capaciteitstags implementaties naar de gewenste omgevingen leiden.

Tagovername

Cloud Assembly gebruikt tagovername om selectief tags voor cloudaccounts toe te voegen aan andere gerelateerde resources. In het bijzonder wanneer u tags maakt op een cloudaccount, worden deze ook effectief voor alle opslagprofielen computerbronnen die overeenkomen met dat cloudaccount.

Opmerking Het gedrag voor doorvoering van tags is niet van toepassing op opslagprofielen. vRealize Automation selecteert niet automatisch de beperking voor opslagprofielen. Daarom moeten gebruikers handmatig de vereiste beperkingstag toevoegen om deze te selecteren en toe te passen op opslagprofielen.

In het volgende voorbeeld ziet u hoe tagovername werkt.

Berekeningsresources

- Cluster1 met tagcluster-1
- Cluster2 met tagcluster-2
- Cluster3 met tagcluster-3

```
Vm resource:
  properties:
    constraints:
      - tag: 'cluster-01'
```

Opslagprofielen

- Profiel 1 voor Datastorecluster1 met tagopslag-01
- Profiel 2 voor Datastorecluster2 met tagopslag-02
- Profiel 3 voor Datastorecluster3 met tagopslag-03

```
vm-resource:
  properties:
    storage:
```

```
constraints:
  - tag: 'storage-01'
```

Cloudaccount

vSphere-cloudaccount met alle drie de tags: cluster-1, cluster-2 en cluster-3

Tijdens het samenvoegen van tags voor opslagprofielen en computerbronnen houdt Cloud Assembly ook rekening met de tags op cloudaccountniveau. Daarom zijn de effectieve tags op alle opslagprofielen en computers cluster-1, cluster-2 en cluster-3. Daarom komen alle opslagprofielen en computers beschikbaar voor plaatsing op elk van de computerhosts en de machine kan op elk van de computerhosts terecht komen, zoals in het voorgaande voorbeeld wordt weergegeven.

Om onverwachte resultaten te minimaliseren en tags overzichtelijk te houden, gaat u een bepaalde tag alleen toepassen op het niveau van het cloudaccount als die tag de juiste capaciteit is voor alle ondergeschikte computerbronnen en opslagresources.

Beperkingstags in Cloud Assembly gebruiken

Tags die zijn toegevoegd aan projecten en cloudsjablonen, functioneren als beperkingstags wanneer ze worden gebruikt voor het afstemmen van capaciteitstags op infrastructuurresources, profielen en cloudzones. In het geval van cloudsjablonen gebruikt Cloud Assembly deze overeenkomende functionaliteit om resources toe te wijzen voor implementaties.

Cloud Assembly stelt u in staat om beperkingstags op twee voornaamste manieren te gebruiken. De eerste manier is tijdens het configureren van projecten en images. U kunt tags gebruiken als beperkingen om resources te koppelen aan het project of de image. De tweede manier is in cloudsjablonen waar tags die zijn opgegeven als beperkingen, worden gebruikt om resources voor implementaties te selecteren. Beperkingen die op beide manieren worden toegepast, worden samengevoegd in cloudsjablonen om een set implementatievereisten op te stellen waarmee resources worden gedefinieerd die beschikbaar zijn voor een implementatie.

Hoe beperkingstags werken voor projecten

Wanneer u Cloud Assembly-resources configureert, kunnen cloudbeheerders beperkingstags toepassen op projecten. Op deze manier kunnen beheerders governancebeperkingen rechtstreeks op projectniveau toepassen. Alle beperkingen die op dit niveau worden toegevoegd, worden toegepast op elke cloudsjabloon die voor het betreffende project is aangevraagd, en deze beperkingstags hebben voorrang op andere tags.

Als beperkingstags voor het project conflicteren met beperkingstags voor de cloudsjabloon, hebben de projecttags voorrang, waardoor de cloudbeheerder de governance-regels kan afdwingen. Als de cloudbeheerders bijvoorbeeld een tag `location:london` voor het project maken, maar een ontwikkelaar een tag `location:boston` op de cloudsjabloon plaatst, krijgt de eerst voorrang en wordt de resource geïmplementeerd in de infrastructuur met de tag `location:london`.

Er zijn drie typen beperkingstags die gebruikers kunnen toepassen op projecten: netwerk, opslag en uitbreidbaarheid. U kunt zoveel instanties van elk tagtype als nodig toepassen. Projectbeperkingen kunnen hard of zacht zijn. Deze zijn standaard hard. Met harde beperkingen kunt u implementatiebeperkingen strikt afdwingen. Als er niet aan een of meer harde beperkingen wordt voldaan, mislukt de implementatie. Zachte beperkingen bieden een manier om voorkeuren aan te geven die worden geselecteerd als ze beschikbaar zijn, maar de implementatie mislukt niet als er niet aan de zachte beperkingen wordt voldaan.

Hoe beperkingstags werken in cloudsjablonen

In cloudsjablonen voegt u beperkingstags als YAML-code toe aan resources, zodat deze overeenkomen met de juiste capaciteitstags die uw cloudbeheerder voor resources, cloudzones en opslag- en netwerkprofielen heeft gemaakt. Daarnaast zijn er nog andere complexere opties voor het implementeren van beperkingstags. U kunt bijvoorbeeld een variabele gebruiken om een of meer tags op een aanvraag in te vullen. Zo kunt u een of meer tags opgeven op het moment van de aanvraag.

Maak beperkingstags met behulp van het label `tag` onder een beperkingskop in de YAML-code van de cloudsjabloon. Beperkingstags van projecten worden toegevoegd aan de beperkingstags die in cloudsjablonen zijn gemaakt.

Cloud Assembly ondersteunt een eenvoudige tekenreeksnotatie om gemakkelijker beperkingen in YAML-bestanden te maken:

```
[!]tag_key[:tag_value][:hard|:soft]
```

Cloud Assembly maakt standaard een positieve beperking met harde afdwinging. De tagwaarde is optioneel, maar wordt aanbevolen, zoals in de rest van de applicatie.

In het volgende voorbeeld van WordPress met MySQL worden YAML-beperkingstags weergegeven die locatiegegevens voor berekeningsresources opgeven.

```
name: "wordpressWithMySQL"
components:
  mysql:
    type: "Compute"
    data:
      name: "mysql"
      # ... skipped lines ...
  wordpress:
    type: "Compute"
    data:
      name: "wordpress"
      instanceType: small
      imageType: "ubuntu-server-1604"
      constraints:
        - tag: "!location:eu:hard"
        - tag: "location:us:soft"
        - tag: "!pci"
      # ... skipped lines ...
```

Zie [Deel 3: het voorbeeld van een Cloud Assembly-sjabloon ontwerpen en implementeren](#) voor meer informatie over werken met cloudsjablonen.

Hoe harde en zachte beperkingen in projecten en cloudsjablonen werken

Beperkingen in zowel projecten als cloudsjablonen kunnen hard of zacht zijn. Het vorige codefragment bevat voorbeelden van harde en zachte beperkingen. Alle beperkingen zijn standaard hard. Met harde beperkingen kunt u implementatiebeperkingen strikt afdwingen. Als er niet aan een of meer harde beperkingen wordt voldaan, mislukt de implementatie. Zachte beperkingen geven voorkeuren aan die indien beschikbaar van toepassing zijn, maar ze zorgen er niet voor dat ze mislukken als er niet aan wordt voldaan.

Als u een reeks harde en zachte beperkingen voor een specifiek resourcetype hebt, kunnen de zachte beperkingen mogelijk doorslaggevend zijn. Dat wil zeggen, als meerdere resources aan een harde beperking voldoen, worden de zachte beperkingen gebruikt om de werkelijke resource te selecteren die in de implementatie wordt gebruikt.

Stel bijvoorbeeld dat u een harde opslagbeperking maakt met de tag `location:boston`. Als geen enkele opslag in het project met deze beperking overeenkomt, mislukt elke gerelateerde implementatie.

Standaardtags

Cloud Assembly past standaardtags op sommige implementaties toe om analyse, controle en groepering van geïmplementeerde resources te ondersteunen.

Standaardtags zijn uniek in Cloud Assembly. In tegenstelling tot andere tags werken gebruikers er niet mee tijdens de configuratie van de implementatie en worden er geen beperkingen toegepast. Deze tags worden automatisch toegepast tijdens het inrichten op AWS-, Azure- en vSphere-implementaties. Deze tags worden opgeslagen als aangepaste systeemeigenschappen en worden na het inrichten aan implementaties toegevoegd.

De lijst met standaardtags wordt hieronder weergegeven.

Tabel 4-3. Standaardtags

Beschrijving	Tag
Organisatie	<code>org:orgID</code>
Project	<code>project:projectID</code>
Aanvrager	<code>aanvrager:username</code>
Implementatie	<code>implementatie:deploymentID</code>
Cloudsjabloonreferentie (indien van toepassing)	<code>blueprint:blueprintID</code>
Onderdeelnaam in blueprint	<code>blueprintResourceName:CloudMachine_1</code>
Plaatsingsbeperkingen: toegepast in blueprint, aanvraagparameters of via IT-beleid	<code>beperkingen:key:value:soft</code>

Tabel 4-3. Standaardtags (vervolg)

Beschrijving	Tag
Cloudaccount	cloudAccount:accountID
Zone of profiel, indien van toepassing	zone:zoneID, networkProfile:profileID, storageProfile:profileID

Hoe Cloud Assembly tags verwerkt

In Cloud Assembly bieden tags snelle capaciteiten en beperkingen die bepalen hoe en waar resources tijdens het inrichtingsproces aan ingerichte implementaties worden toegewezen.

Cloud Assembly gebruikt een specifieke volgorde en hiërarchie van bewerkingen bij het omzetten van tags om ingerichte implementaties te maken. Door inzicht te krijgen in de basisprincipes van dit proces, kunt u tags efficiënt implementeren om voorspelbare implementaties te maken.

In de volgende lijst vindt u een overzicht van de bewerkingen op hoog niveau en de volgorde die Cloud Assembly gebruikt om tags om te zetten en een implementatie te definiëren:

- Cloudzones worden gefilterd op verschillende criteria, waaronder beschikbaarheid en profielen. Tags in profielen voor de regio waarvan de zone deel uitmaakt, worden hier afgestemd.
- Capaciteitstags voor zones en berekeningen worden gebruikt om de resterende cloudzones te filteren op harde beperkingen.
- Uit de gefilterde zones wordt prioriteit gebruikt om een cloudzone te selecteren. Als er verschillende cloudzones met dezelfde prioriteit zijn, worden ze gesorteerd door zachte beperkingen af te stemmen, met behulp van een combinatie van de cloudzone- en berekeningsmogelijkheden.
- Nadat een cloudzone is geselecteerd, wordt een host geselecteerd door een reeks filters af te stemmen, waaronder harde en zachte beperkingen, zoals uitgedrukt in cloudsjablonen.

Hoe kan ik een eenvoudige tagstructuur instellen?

Dit onderwerp beschrijft een eenvoudige benadering en opties voor een logische Cloud Assembly-tagstrategie. U kunt deze voorbeelden gebruiken als beginpunt voor een echte implementatie, of u kunt een andere strategie uitwerken die beter aan uw behoeften tegemoetkomt.

Doorgaans is de cloudbeheerder de primaire persoon die verantwoordelijk is voor het maken en onderhouden van tags.

In dit onderwerp wordt verwezen naar het WordPress-gebruiksscenario elders in de documentatie voor Cloud Assembly om te illustreren hoe tags aan sommige belangrijke items kunnen worden toegevoegd. Ook worden mogelijke alternatieven en uitbreidingen beschreven voor de tagvoorbeelden die in het WordPress-gebruiksscenario worden weergegeven.

Zie [Tutorial: Infrastructuur en implementaties met meerdere clouds instellen en testen in Cloud Assembly](#) voor meer informatie over het WordPress-gebruiksscenario.

In het WordPress-gebruiksscenario wordt beschreven hoe u tags in cloudzones en opslag- en netwerkprofielen plaatst. Deze profielen zijn net als georganiseerde pakketten resources. Tags die in profielen worden geplaatst, zijn van toepassing op alle items in het profiel. U kunt ook tags maken en op opslagresources en individuele netwerk items, maar ook op berekeningsresources plaatsen, maar deze tags zijn alleen van toepassing op de specifieke resources waarop deze worden geplaatst. Wanneer u tags instelt, is het doorgaans het beste om te beginnen met het taggen van berekeningsresources en vervolgens kunt u later tags aan profielen en cloudzones toevoegen. U gebruikt deze tags ook om de lijst met berekeningsresources voor een cloudzone te filteren.

Terwijl u bijvoorbeeld tags in opslagprofielen kunt plaatsen, zoals in dit gebruiksscenario wordt weergegeven, kunt u ook tags in individuele opslagbeleidsregels, gegevensopslagruimten en opslagaccounts plaatsen. Met tags in deze resources kunt u een betere controle uitoefenen over de manier waarop opslagresources worden geïmplementeerd. Tijdens de verwerking als voorbereiding op de implementatie worden deze tags omgezet als volgend niveau van verwerking na de profieltags.

Als voorbeeld van hoe u een typisch klantscenario kunt configureren, kunt u de tag `region: eastern` op een netwerkprofiel plaatsen. Deze tag is van toepassing op alle resources in dat profiel. Vervolgens kunt u de tag `networktype:pci` op een PCI-netwerkrecursoe in het profiel plaatsen. Een cloudsjabloon met de beperkingen `eastern` en `pci` maakt implementaties die dit PCI-netwerk voor de oostelijke regio gebruiken.

Procedure

1 Tag uw resources voor berekeningsinfrastructuren op een logische en geschikte manier.

Het is vooral belangrijk dat u berekeningsresources op een logische manier tagt, zodat u deze kunt vinden met behulp van de zoekfunctie op het tabblad Berekenen van de pagina Cloudzone maken. Met behulp van deze zoekfunctie kunt u snel de berekeningsresources filteren die aan een cloudzone zijn gekoppeld. Als u de opslag en netwerken op profielniveau tagt, hoeft u mogelijk geen individuele opslag- en netwerkresources te taggen.

- a Selecteer **Resources > Berekenen** om de berekeningsresources weer te geven die voor uw Cloud Assembly-instantie zijn geïmporteerd.
- b Selecteer elke berekeningsresource die u nodig hebt en klik op **Tags** om een tag aan de resource toe te voegen. U kunt indien nodig meer dan één tag aan elke resource toevoegen.
- c Herhaal zo nodig de vorige stap voor de opslag- en netwerkresources.

2 Maak capaciteitstags voor cloudzones en netwerkprofielen.

U kunt dezelfde tags gebruiken voor zowel cloudzones als netwerkprofielen of u kunt unieke tags maken voor elk item, als dat zinvoller is voor uw implementatie.

In netwerkprofielen kunt u tags op het hele profiel plaatsen en op subnetten in het profiel. Tags die op profielniveau worden toegepast, zijn van toepassing op alle onderdelen, zoals subnetten, binnen dat profiel. Tags op subnetten zijn alleen van toepassing op het specifieke subnet waarop deze zijn geplaatst. Tijdens het verwerken van tags hebben de tags op profielniveau voorrang op de tags op subnetniveau.

Zie de cloudzone- en netwerksecties van het [Deel 1: het voorbeeld van de Cloud Assembly-infrastructuur configureren](#) voor informatie over het toevoegen van tags aan cloudzones of netwerkprofielen.

In dit voorbeeld maken we drie eenvoudige tags die doorheen de documentatie voor het gebruiksscenario voor cloudzone- en netwerkprofieltags van Cloud Assembly worden gebruikt. Deze tags identificeren de omgeving voor de profielonderdelen.

- `zone:test`
- `zone:dev`
- `zone:prod`

3 Maak opslagprofieltags voor uw opslagonderdelen.

Opslagtags identificeren doorgaans het prestatieniveau van opslagitems, zoals laag1 of laag2, of deze identificeren de aard van opslagitems, zoals PCI.

Zie de sectie over opslag van het [Deel 1: het voorbeeld van de Cloud Assembly-infrastructuur configureren](#) voor informatie over het toevoegen van tags aan opslagprofielen.

- `usage:general`
- `usage:fast`

Resultaten

Nadat u een basistagstructuur hebt gemaakt, kunt u hieraan gaan werken en zo nodig tags toevoegen of bewerken om uw tagcapaciteiten te verfijnen en uit te breiden.

Werken met resources in vRealize Automation

Een cloudbeheerder kan vRealize Automation-resources controleren die via gegevensverzameling beschikbaar worden gesteld.

De cloudbeheerder kan resources met capaciteitstags labelen om te bepalen waar vRealize Automation-cloudsjablonen worden geïmplementeerd.

Naast de weergaven die hier worden geboden kunt u met het tabblad Resources ook verschillende resources beheren. Zie [Resources beheren in Cloud Assembly](#).

Computerbronnen in vRealize Automation

Een cloudbeheerder kan berekeningsresources controleren die beschikbaar worden gesteld via gegevensverzameling.

De cloudbeheerder kan ervoor kiezen tags direct op de resources toe te passen om de capaciteiten voor afstemmingsdoeleinden bij het inrichten met vRealize Automation te labelen.

Netwerkresources in vRealize Automation

In vRealize Automation kunnen cloudbeheerders de netwerkresources bekijken en bewerken waarvan de gegevens zijn verzameld uit de cloudaccounts en integraties die zijn toegewezen aan uw project.

Nadat u een cloudaccount hebt toegevoegd aan uw Cloud Assembly-infrastructuur, bijvoorbeeld door gebruik te maken van de menuopties **Infrastructuur > Verbindingen > Cloudaccounts**, worden gegevens van de netwerk- en beveiligingsinformatie van het cloudaccount ontdekt door gegevensverzameling. Deze informatie is dan beschikbaar voor gebruik in netwerken, netwerkprofielen en andere definities.

Netwerken zijn de IP-specifieke onderdelen van een beschikbaar netwerkdomein of beschikbare transportzone. Als u een Amazon Web Services- of Microsoft Azure-gebruiker bent, beschouwt u netwerken als subnetten.

U kunt informatie over de netwerken in uw project weergeven met behulp van de pagina **Infrastructuur > Resources > Netwerken**.

De pagina **Netwerken** in Cloud Assembly bevat informatie zoals:

- Netwerken en load balancers die extern in het netwerkdomein van uw cloudaccount zijn gedefinieerd, bijvoorbeeld in vCenter, NSX-T of Amazon Web Services.
- Netwerken en load balancers die door de cloudbeheerder zijn geïmplementeerd.
- IP-bereiken en andere netwerkkenmerken die door uw cloudbeheerder zijn gedefinieerd of gewijzigd.
- Externe IP-bereiken van de IPAM-provider voor een bepaalde adresruimte in een externe IPAM-integratie van een provider.

Voor meer informatie over netwerken verwijzen we u naar de volgende informatie, wegwijzerhulp voor verschillende instellingen op de pagina **Netwerken** en [Meer informatie over netwerkprofielen in vRealize Automation](#).

Netwerken

U kunt netwerken en hun kenmerken weergeven en bewerken, bijvoorbeeld om tags toe te voegen of ondersteuning voor openbare IP-toegang te verwijderen. U kunt ook netwerkinstellingen beheren, zoals DNS, CIDR, gateway en tagwaarden. U kunt ook nieuwe IP-bereiken definiëren en bestaande IP-bereiken in een netwerk beheren.

Voor bestaande netwerken kunt u het IP-bereik en de taginstellingen wijzigen door het selectievakje van het netwerk in te schakelen en **IP-bereiken beheren** of **Tags** te selecteren. Anders kunt u het netwerk zelf selecteren om de informatie te bewerken.

Tags bieden een manier om geschikte netwerken, en optioneel ook netwerkprofielen, af te stemmen op netwerkonderdelen in cloudsjablonen. Netwerktags worden op elke instantie van dat netwerk toegepast, ongeacht de netwerkprofielen waarin het netwerk zich bevindt. Van netwerken kan een instantie worden gemaakt in een onbeperkt aantal netwerkprofielen. Ongeacht de locatie van het netwerkprofiel is er een netwerktag gekoppeld aan dat netwerk waar het netwerk ook wordt gebruikt. Het afstemmen van netwerktags vindt plaats met andere onderdelen in de cloudsjabloon nadat de cloudsjabloon is afgestemd op een of meer netwerkprofielen.

Voor algemene netwerken kunt u gebruikmaken van bestaande en openbare netwerken voor de NSX-T-cloudaccounts van algemene beheerders en lokale beheerders en de vCenter-cloudaccounts die zijn gekoppeld aan de lokale beheerders. De weergave van lokale beheerders van uitgerekte netwerken wordt gedefinieerd in een transportzone. Een transportzone is een constructie voor lokale NSX-T-beheerders die de reikwijdte bepaalt van NSX-T-netwerken voor vCenter Server-hosts en -clusters.

Cloud Assembly maakt een inventarisatie of gegevensverzameling van bestaande en openbare netwerken. U kunt een algemeen netwerk maken door een bestaand of openbaar netwerk toe te voegen aan een algemene NSX-T-beheerder. Het algemene netwerk kan vervolgens worden gebruikt door alle bijbehorende lokale beheerders. Algemene netwerken kunnen zich richten op een specifieke lokale beheerder, alle bijbehorende lokale beheerders of een subset daarvan.

Om een machine in te richten voor een algemeen netwerk maakt u gebruik van een statische IP-toewijzing. DHCP wordt niet ondersteund.

U kunt de volgende typen algemene netwerken maken voor een algemene beheerder:

- 1 Overlay: een overlaynetwerk is gekoppeld aan een lokale beheerder van laag-0/laag-1 en bestrijkt automatisch alle sites die zijn verbonden met de lokale beheerder van laag-0/laag-1. Voor elke lokale beheerder wordt de standaardtransportzone van de overlay gebruikt.
- 2 VLAN: een VLAN-netwerk is van toepassing op één lokale beheerder waarbij de transportzone handmatig kan worden geselecteerd.

Algemene netwerken worden weergegeven op de pagina **Infrastructuur > Resources** met alle cloudaccounts waarop ze van toepassing zijn.

De volgende bewerkingen voor dag 2 worden ondersteund voor algemene netwerken:

- Een algemeen netwerk in een cloudsjabloondefinitie omzetten naar een lokaal netwerk en omgekeerd.
- Uit- en inschalen van machines in algemene netwerken.

Zie [Meer informatie over netwerkresources in vRealize Automation-cloudsjablonen](#) voor meer informatie over het gebruik van netwerken in cloudsjablonen.

Zie [Netwerkresources in vRealize Automation bijwerken na migratie van N-VDS naar C-VDS in NSX-T](#) voor informatie over het bijwerken van vSphere-netwerken in vRealize Automation na de NSX-T-migratie van N-VDS naar C-VDS.

IP-bereiken

Gebruik een IP-bereik om het begin- en eind-IP-adres van een bepaald netwerk in uw organisatie te definiëren of te wijzigen. U kunt IP-bereiken weergeven en beheren voor vermelde netwerken. Als het netwerk wordt beheerd door een externe IPAM-provider, kunt u IP-bereiken in verband met het bijbehorende IPAM-integratiepunt beheren.

Klik op **Nieuw IP-bereik** om een extra IP-bereik toe te voegen aan het netwerk. U kunt een **intern IP-bereik** opgeven, of als er een geldige IPAM-integratie beschikbaar is, kunt u een **extern IP-bereik** opgeven.

U kunt de standaardgateway niet opnemen in een IP-bereik. Het IP-bereik van het subnet kan de waarde van de subnetgateway niet bevatten.

Als u een externe IPAM-integratie voor een bepaalde IPAM-provider gebruikt, kunt u het **externe IP-bereik gebruiken** om een IP-bereik te selecteren uit een beschikbaar extern IPAM-integratiepunt. Dit proces wordt beschreven in de context van een algemene externe IPAM-integratiestroom op [Configureer een netwerk en netwerkprofiel voor het gebruik van externe IPAM voor een bestaand netwerk in vRealize Automation](#).

Opmerking Wanneer een IP-bereik van een externe IPAM-provider wordt verwijderd in de externe IPAM-applicatie, wordt het IP-bereik automatisch verwijderd tijdens de inventarisatie in vRealize Automation. Het verwijderde IP-bereik is niet langer zichtbaar of beschikbaar voor netwerkkoppeling in vRealize Automation, waardoor zwevende IP-adresbereiken worden voorkomen.

Met vRealize Automation kunt u een IP-adresbereik toepassen en beheren in meerdere vSphere- en NSX-netwerken. Ondersteuning voor gedeelde IP-bereiken wordt geboden voor zowel interne als externe IPAM. U kunt één IP-bereik instellen op een uitgerekt NSX-netwerk zodat machines in dat netwerk IP-adressen kunnen gebruiken die vanuit dat ene IP-bereik zijn toegewezen, zelfs als ze in verschillende vCenters zijn geïmplementeerd.

IP-adressen

U kunt de IP-adressen zien die momenteel door uw organisatie worden gebruikt en hun status weergeven, bijvoorbeeld `available` of `allocated`. De IP-adressen die worden weergegeven, zijn ofwel IP-adressen die intern worden beheerd door vRealize Automation of IP-adressen die zijn toegewezen voor implementaties die een externe IPAM-providerintegratie bevatten. Externe IPAM-providers beheren hun eigen toewijzing van IP-adressen.

Als het netwerk intern wordt beheerd door vRealize Automation en niet door een externe IPAM-provider, kunt u ook IP-adressen vrijgeven.

Wanneer u interne IPAM gebruikt en IP-adressen vrijgeeft, nadat u bijvoorbeeld een machine hebt verwijderd die de IP-adressen gebruikte of op **IP-adres vrijgeven** hebt geklikt voor een specifiek netwerk, is er een wachttijd tussen het moment van vrijgave van de ongebruikte adressen en het moment van beschikbaarheid voor hergebruik. Door deze wachttijd, of time-

outperiode voor vrijgave, kan de DNS-cache worden gewist. De IP-adressen kunnen vervolgens aan een nieuwe machine worden toegewezen. De wachttijd voor de vrijgave van IP-adressen is standaard 30 minuten. U kunt de wachttijd wijzigen door op de optie **Instellingen** te klikken in de rechterbovenhoek van de pagina **Netwerken** en de waarde bij **Time-out vrijgave** te wijzigen.

- Tijdens de time-outperiode voor vrijgave worden relevante IP-adressen weergegeven als vrijgegeven. Wanneer de time-outperiode voor de vrijgave is verstreken, worden deze IP-adressen weergegeven als beschikbaar.
- Het systeem controleert elke vijf minuten op nieuw vrijgegeven IP-adressen. Dus afhankelijk van wanneer de laatste controle is uitgevoerd, kan het zelfs bij een time-outwaarde van één minuut, één tot zes minuten duren voordat de vrijgegeven IP-adressen beschikbaar zijn. Het interval voor controle van vijf minuten is van toepassing op alle waarden die groter zijn dan nul.
- Als u de time-outwaarde voor vrijgave instelt op 0, worden IP-adressen onmiddellijk vrijgegeven en dus onmiddellijk beschikbaar.
- De time-outwaarde voor vrijgave is van toepassing op alle cloudaccounts in de organisatie.

Load balancers

U kunt informatie over beschikbare load balancers voor het account en regiocloudaccounts in uw organisatie beheren. U kunt de geconfigureerde instellingen voor elke beschikbare load balancer openen en weergeven. U kunt ook tags voor een load balancer toevoegen en verwijderen.

Zie [Meer informatie over load-balancerresources in vRealize Automation-cloudsjablonen](#) voor meer informatie over het gebruik van load balancers in cloudsjablonen.

Netwerkdomeinen

De lijst met netwerkdomeinen bevat gerelateerde en niet-overlappende netwerken.

Beveiligingsresources in vRealize Automation

Nadat u een cloudaccount in Cloud Assembly hebt toegevoegd, detecteert gegevensverzameling de netwerk- en beveiligingsinformatie van het cloudaccount en maakt deze de informatie beschikbaar voor gebruik in netwerkprofielen en andere opties.

Beveiligingsgroepen en firewallregels ondersteunen netwerkisolatie. Gegevens van beveiligingsgroepen worden verzameld. Er worden geen gegevens van firewallregels verzameld.

Via **Infrastructuur > Resources > Beveiliging** kunt u beveiligingsgroepen op aanvraag weergeven die zijn gemaakt in Cloud Assembly-cloudsjabloonontwerpen en bestaande beveiligingsgroepen die zijn gemaakt in bronapplicaties, zoals NSX-T en Amazon Web Services. De beschikbare beveiligingsgroepen worden weergegeven door het gegevensverzamelingsproces.

U kunt een tag gebruiken om de machine-interface (NIC) te koppelen aan een beveiligingsgroep in een gedefinieerde cloudsjabloon of in een netwerkprofiel. U kunt de beschikbare beveiligingsgroepen bekijken en tags voor geselecteerde beveiligingsgroepen toevoegen of verwijderen. Een auteur van een cloudsjabloon kan een of meer beveiligingsgroepen toewijzen aan een machine-NIC om de beveiliging voor de implementatie te beheren.

In het cloudsjabloonontwerp wordt de parameter `securityGroupType` in de beveiligingsgroepresource opgegeven als `existing` voor een bestaande beveiligingsgroep of `new` voor een beveiligingsgroep op aanvraag.

Bestaande beveiligingsgroepen

Bestaande beveiligingsgroepen worden in de kolom **Afkomst** weergegeven en ingedeeld als *Discovered*.

Bestaande beveiligingsgroepen van het eindpunt van het onderliggende cloudaccount, zoals NSX-V, NSX-T of Amazon Web Services-applicaties, zijn beschikbaar voor gebruik.

Een cloudbeheerder kan een of meer tags toewijzen aan een bestaande beveiligingsgroep zodat deze kan worden gebruikt in een cloudsjabloon. Een auteur van cloudsjablonen kan een `Cloud.SecurityGroup`-resource in een cloudsjabloonontwerp gebruiken om een bestaande beveiligingsgroep toe te wijzen met behulp van tagbeperkingen. Voor een bestaande beveiligingsgroep moet ten minste één beperkingstag worden opgegeven in de beveiligingsresource in het cloudsjabloonontwerp.

Als u een bestaande beveiligingsgroep rechtstreeks in de bronapplicatie bewerkt, zoals in de NSX-bronapplicatie in plaats van in Cloud Assembly, zijn de updates niet zichtbaar in Cloud Assembly totdat u de gegevensverzameling uitvoert en gegevens voor het gekoppelde cloudaccount of integratiepunt worden verzameld vanuit Cloud Assembly. Gegevensverzameling wordt automatisch om de 10 minuten uitgevoerd.

Bestaande beveiligingsgroepen kunnen worden gebruikt voor de NSX-T-cloudaccounts van algemene beheerders en lokale beheerders en de vCenter-cloudaccounts die zijn gekoppeld aan de lokale beheerders. Cloud Assembly maakt een inventarisatie of gegevensverzameling van bestaande beveiligingsgroepen en koppelt deze aan de netwerkinterfaces (NIC's) van een machine. U kunt een algemene beveiligingsgroep maken door een bestaande beveiligingsgroep toe te voegen voor een algemene NSX-T-beheerder. De algemene beveiligingsgroep kan vervolgens worden gebruikt door de bijbehorende lokale beheerders. Algemene beveiligingsgroepen kunnen zich richten op een specifieke lokale beheerder, alle bijbehorende lokale beheerders of een subset daarvan.

- Bestaande algemene beveiligingsgroepen worden ondersteund en geïnventariseerd voor alle gedefinieerde regio's.
- Algemene beveiligingsgroepen worden weergegeven op de pagina **Infrastructuur > Resources** met alle cloudaccounts waarop ze van toepassing zijn.
- U kunt een machine-interface (NIC) direct koppelen aan een bestaande algemene beveiligingsgroep in een cloudsjabloon of in het geselecteerde netwerkprofiel.

- De volgende bewerkingen voor dag 2 worden ondersteund voor algemene beveiligingsgroepen:
 - De omzetting van een beveiligingsgroep in een cloudsjabloon van een algemene naar een lokale beveiligingsgroep, en omgekeerd.
 - Uit- en inschalen van machines die aan algemene beveiligingsgroepen zijn gekoppeld.

Beveiligingsgroepen op aanvraag

Beveiligingsgroepen op aanvraag die u maakt in Cloud Assembly (in een cloudsjabloon of in een netwerkprofiel) worden in de kolom **Afkomst** weergegeven en ingedeeld als `Managed by Cloud Assembly`. Beveiligingsgroepen op aanvraag die u maakt als onderdeel van een netwerkprofiel, worden intern geclassificeerd als isolatiebeveiligingsgroep met vooraf ingestelde firewallregels en worden niet aan een cloudsjabloonontwerp toegevoegd als beveiligingsgroepresource. Beveiligingsgroepen op aanvraag die u in een cloudsjabloonontwerp maakt, en die snelle firewallregels kunnen bevatten, worden toegevoegd als onderdeel van een beveiligingsgroepresource die als `new` is geclassificeerd.

Opmerking U kunt firewallregels voor beveiligingsgroepen op aanvraag voor NSX-V en NSX-T rechtstreeks in een beveiligingsgroepresource in de cloudsjabloonontwerpcodes maken. De kolom **Toegepast op** bevat geen beveiligingsgroepen die zijn geclassificeerd of worden beheerd door een gedistribueerde firewall van NSX (DFW). Firewallregels die van toepassing zijn op applicaties, zijn voor oost-westverkeer in de DFW. Sommige firewallregels kunnen alleen in de bronapplicatie worden beheerd en kunnen niet worden bewerkt in Cloud Assembly. Bijvoorbeeld: ethernet-, nood-, infrastructuur- en omgevingsregels worden in NSX-T beheerd.

Er is momenteel geen ondersteuning voor beveiligingsgroepen op aanvraag voor NSX-T-cloudaccounts voor algemene beheerders.

Meer informatie

Zie [Meer informatie over netwerkprofielen in vRealize Automation](#) voor meer informatie over het gebruik van beveiligingsgroepen in netwerkprofielen.

Voor informatie over het definiëren van firewallregels, zie [Instellingen voor beveiligingsgroepen gebruiken in netwerkprofielen en cloudsjabloonontwerpen in vRealize Automation](#).

Zie [Meer informatie over beveiligingsgroep- en tagresources in vRealize Automation-cloudsjablonen](#) voor meer informatie over het gebruik van beveiligingsgroepen in een cloudsjabloon.

Zie [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#) voor voorbeelden van cloudsjabloonontwerpcodes die beveiligingsgroepen bevatten.

Opslagresources in vRealize Automation

Een cloudbeheerder kan werken met opslagresources en hun capaciteiten, die worden gedetecteerd via vRealize Automation-gegevensverzameling uit gekoppelde cloudaccounts.

Capaciteiten van opslagresources zijn beschikbaar via tags die doorgaans afkomstig zijn van het broncloudaccount. Een cloudbeheerder kan ervoor kiezen om aanvullende tags direct op opslagresources toe te passen met behulp van Cloud Assembly. De aanvullende tags kunnen tijdens het inrichten een specifieke capaciteit voor afstemmingsdoeleinden labelen.

vRealize Automation ondersteunt standaardschijf- en eersteklasschijfmogelijkheden. Eersteklasschijf is alleen beschikbaar voor vSphere.

- [Wat kan ik doen met standaardschijfopslag in vRealize Automation](#)
- [Wat kan ik doen met de eersteklasschijfopslag in vRealize Automation](#)

Capaciteiten voor opslagresources worden zichtbaar als onderdeel van de definitie van een Cloud Assembly-opslagprofiel. Zie [Meer informatie over opslagprofielen in vRealize Automation](#).

Eersteklasschijven waarvoor gegevens zijn verzameld, verschijnen in de weergave **Resources > Resources > Volumes**.

Meer informatie over resources in Cloud Assembly

Cloud Assembly kan aanvullende informatie weergeven over resources met verzamelde gegevens, zoals prijskaarten.

Hoe werkt gegevensverzameling in vRealize Automation?

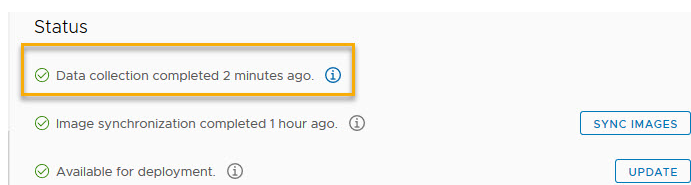
Na de initiële gegevensverzameling wordt resourcegegevensverzameling automatisch elke 10 minuten uitgevoerd. Het interval voor gegevensverzameling kan niet worden geconfigureerd en u kunt gegevensverzameling niet handmatig starten.

U kunt informatie over resourcegegevensverzameling en imagesynchronisatie voor een bestaand cloudaccount vinden in de sectie Status van de betreffende pagina. Selecteer hiertoe **Infrastructuur > Verbindingen > Cloudaccounts** en klik vervolgens op **Openen** in het bestaande cloudaccount van uw keuze.

U kunt een bestaand cloudaccount openen en de bijbehorende eindpuntversie bekijken in de sectie **Status** van de betreffende pagina. Als het gekoppelde eindpunt is geüpgraded, wordt de nieuwe eindpuntversie gedetecteerd tijdens gegevensverzameling en weergegeven in de sectie **Status** op de pagina van het cloudaccount.

Resourcegegevensverzameling

Gegevensverzameling wordt om de 10 minuten uitgevoerd. Elk cloudaccount wordt weergegeven wanneer de gegevensverzameling voor het laatst is voltooid.

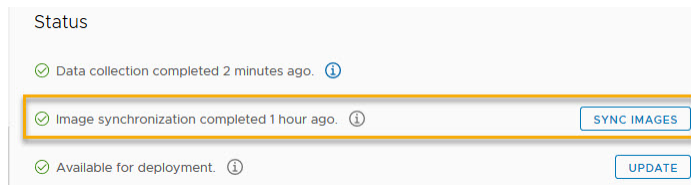


Imagegegevensverzameling

Imagesynchronisatie vindt elke 24 uur plaats. U kunt de synchronisatie van images voor sommige cloudaccounttypen starten. Om een imagesynchronisatie te starten, opent u het cloudaccount (**Infrastructuur > Cloudaccounts** en vervolgens selecteert en opent u het bestaande cloudaccount) en klikt u op de knop **Images synchroniseren**. Er is geen optie voor het synchroniseren van images voor NSX-cloudaccounts.

Opmerking Images worden intern ingedeeld als openbaar of privé. Openbare images worden gedeeld en zijn niet specifiek voor een bepaald cloudabonnement of een organisatie. Privé-images worden niet gedeeld en zijn specifiek voor een specifiek abonnement. Openbare en persoonlijke images worden automatisch elke 24 uur gesynchroniseerd. Met een optie op de pagina van het cloudaccount kunt u synchronisatie voor privé-images activeren.

De pagina van het cloudaccount wordt weergegeven wanneer imagesynchronisatie voor het laatst is voltooid.



Om fouttolerantie en hoge beschikbaarheid in implementaties mogelijk te maken, vertegenwoordigt elk NSX-T-datacentereindpunt een cluster van drie NSX-managers. Zie [Een NSX-T-cloudaccount maken in vRealize Automation](#) voor gerelateerde informatie.

Cloudaccounts en onboardingplannen

Wanneer u een cloudaccount maakt, worden de gegevens van alle machines die eraan zijn gekoppeld, verzameld en vervolgens weergegeven op de pagina **Resources > Resources > Virtuele machines**. Als het cloudaccount machines heeft die buiten Cloud Assembly zijn geïmplementeerd, kunt u een onboarding-plan gebruiken om Cloud Assembly de machine-implementaties te laten beheeren.

Zie [Cloudaccounts aan Cloud Assembly toevoegen](#) voor informatie over het toevoegen van cloudaccounts.

Zie [Wat zijn onboardingplannen in Cloud Assembly](#) voor informatie over het onboarden van niet-beheerde machines.

Netwerkrecursoes in vRealize Automation bijwerken na migratie van N-VDS naar C-VDS in NSX-T

Na de NSX-T-migratie van NSX Virtual Distributed Switch (N-VDS) naar geconvergeerde VDS (C-VDS) moet u betrokken vSphere-netwerkrecursoes in vRealize Automation bijwerken om deze resources te blijven gebruiken in nieuwe en bestaande cloudsjablonen en implementaties.

Na de migratie van N-VDS naar C-VDS ontbreken uw vSphere-netwerken mogelijk in vRealize Automation-netwerkprofielen waarvan ze lid zijn. Om te voorkomen dat u deze vSphere-netwerken verliest en deze te kunnen toewijzen in bestaande en nieuwe implementaties, moet u alle vermelde C-VDS-netwerken in vRealize Automation Cloud Assembly handmatig bijwerken.

Opmerking Deze procedure is specifiek voor acties die nodig zijn in vRealize Automation om vSphere-netwerken bij te werken nadat de migratie van N-VDS naar C-VDS is uitgevoerd in NSX-T. Er is geen actie nodig in vRealize Automation op NSX-netwerken na de migratie van N-VDS naar C-VDS. NSX-netwerken vereisen geen handmatige interventie na de migratie van N-VDS naar C-VDS.

Terwijl een NSX-T-beheerder NSX-T op VDS-netwerktypen (N-VDS) kan migreren naar geconvergeerde VDS-netwerktypen (C-VDS) in NSX, heeft deze actie gevolgen voor bestaande vSphere-netwerkresources in vRealize Automation. De vRealize Automation-beheerder kan acties na migratie uitvoeren om die resources in vRealize Automation te combineren met de bijbehorende wijzigingen in NSX-T en vCenter Server. Houd er rekening mee dat naar C-VDS, of VDS, elders ook wordt verwezen als vSphere 7 Virtual Distributed Switch (VDS).

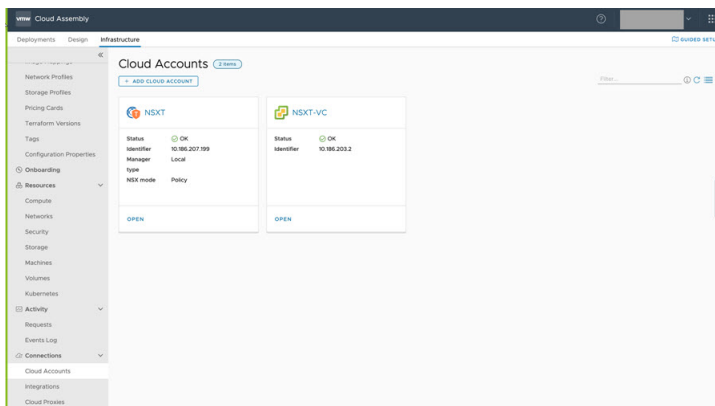
Voor gerelateerde informatie over geconvergeerde VDS van NSX-T raadpleegt u het VMware Knowledge Base-artikel [NSX-T on VDS \(79872\)](#) en [VMware Cloud on AWS \(VMConAWS\)](#) en [VMware Cloud on Dell EMC-migratie van N-VDS naar VDS \(82487\)](#).

Opmerking Dit voorbeeldscenario illustreert de stappen die nodig zijn om resources in een vRealize Automation-omgeving te combineren na de migratie van N-VDS naar C-VDS. U kunt dit voorbeeld en de procedure in vRealize Automation 8.5 en hoger gebruiken om wijzigingen die in vCenter Server zijn aangebracht, af te stemmen na de migratie van N-VDS naar C-VDS in NSX-T.

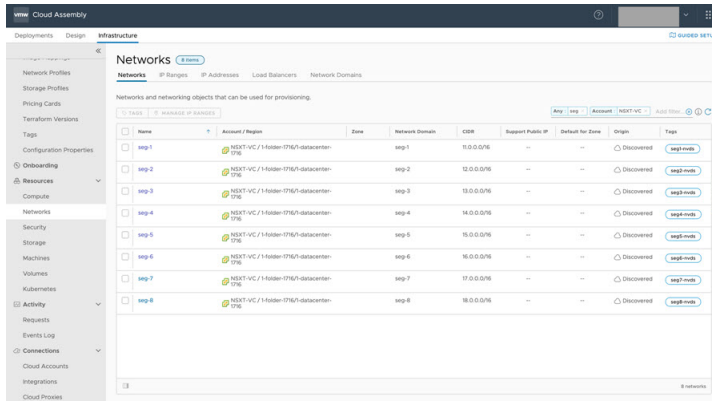
Bijvoorbeeld: vRealize Automation-resources vóór de migratie

In dit voorbeeld ziet u voorbeeldresources van NSX-T in een voorbeeldomgeving van vRealize Automation voorafgaand aan de migratie van N-VDS naar C-VDS.

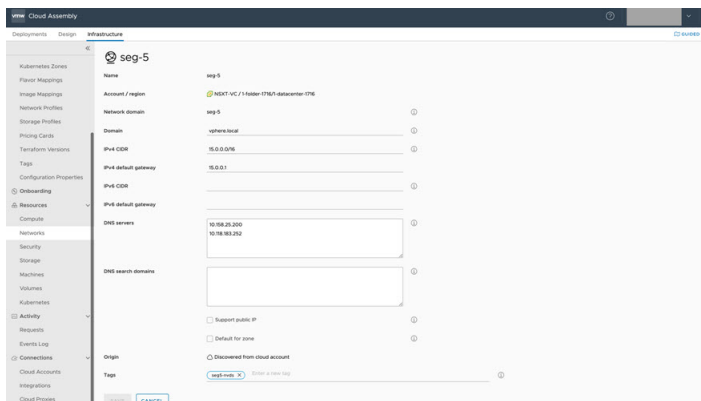
- Het voorbeeld bevat NSX-T- en vCenter-cloudaccounts, zoals hieronder wordt weergegeven.



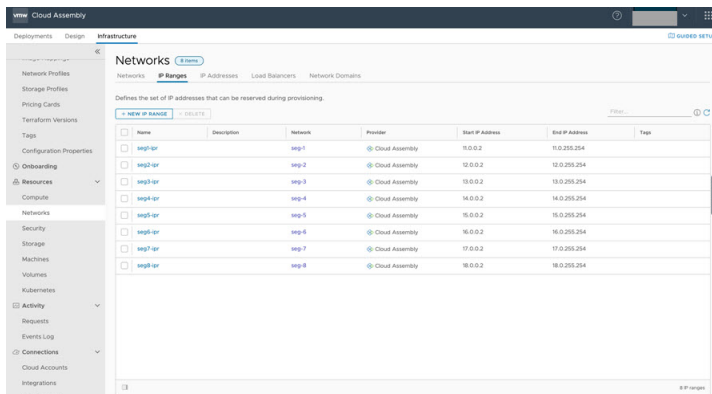
- Het voorbeeld bevat diverse vSphere-netwerken, zoals hieronder wordt weergegeven.



- De voorbeeldnetwerkconfiguratie bevat CIDR- en DNS-instellingen, zoals hieronder wordt weergegeven.



- Het voorbeeld bevat ook bestaande IP-bereiken, zoals hieronder wordt weergegeven.



- Het voorbeeld bevat een netwerkprofiel (**ex-np**) dat verschillende N-VDS-netwerken (N-VDS) bevat, inclusief **seg-5**, zoals hieronder wordt

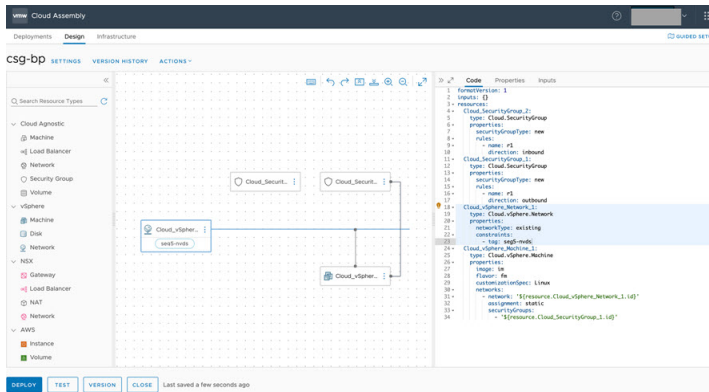
The screenshot shows the AWS IAM console's 'Network Profiles' page. The page title is 'Network Profiles' and it includes a search bar and a 'Filter' button. The main content area displays a table of network profiles. The table has columns for Name, VPC, Amazon EC2 Instance Profile, Zone, Network Boundary, CIDR, Subnet Policy ID, Default for Zone, Status, and Tags. There are 8 profiles listed, all with a status of 'Discontinued'. The 'ex-np' profile is highlighted. The left sidebar shows the navigation menu with 'Network Profiles' selected. The top bar shows the 'IAM' logo and 'Network Profiles' title.

Name	VPC	Amazon EC2 Instance Profile	Zone	Network Boundary	CIDR	Subnet Policy ID	Default for Zone	Status	Tags
exp-1	us-east-1-vpc	us-east-1-ec2-instance-profile	us-east-1a	us-east-1	10.0.0.0/16	us-east-1-subnet-policy	Default	Discontinued	exp-1
exp-2	us-east-1-vpc	us-east-1-ec2-instance-profile	us-east-1b	us-east-1	10.0.0.0/16	us-east-1-subnet-policy	Default	Discontinued	exp-2
exp-3	us-east-1-vpc	us-east-1-ec2-instance-profile	us-east-1c	us-east-1	10.0.0.0/16	us-east-1-subnet-policy	Default	Discontinued	exp-3
exp-4	us-east-1-vpc	us-east-1-ec2-instance-profile	us-east-1d	us-east-1	10.0.0.0/16	us-east-1-subnet-policy	Default	Discontinued	exp-4
exp-5	us-east-1-vpc	us-east-1-ec2-instance-profile	us-east-1e	us-east-1	10.0.0.0/16	us-east-1-subnet-policy	Default	Discontinued	exp-5
exp-6	us-east-1-vpc	us-east-1-ec2-instance-profile	us-east-1f	us-east-1	10.0.0.0/16	us-east-1-subnet-policy	Default	Discontinued	exp-6
exp-7	us-east-1-vpc	us-east-1-ec2-instance-profile	us-east-1g	us-east-1	10.0.0.0/16	us-east-1-subnet-policy	Default	Discontinued	exp-7
exp-8	us-east-1-vpc	us-east-1-ec2-instance-profile	us-east-1h	us-east-1	10.0.0.0/16	us-east-1-subnet-policy	Default	Discontinued	exp-8

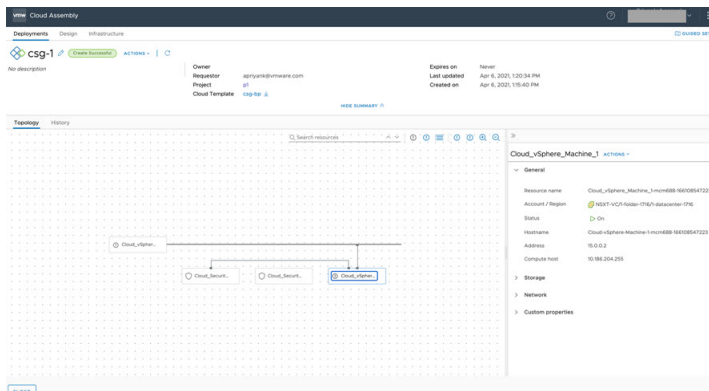
At the bottom of the page, there are buttons for 'Filter', 'Cancel', and 'Apply'. The page number '13' is shown at the bottom left, and the text '1 of 13 items' is at the bottom right.

weergegeven.

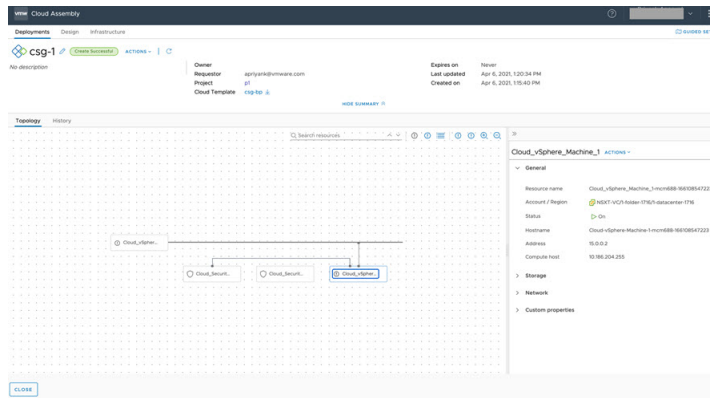
- In dit voorbeeld wordt het bestaande **seg5**-netwerkonderdeel weergegeven in de volgende voorbeeldsyntax voor cloudsjablonen. Het netwerk is getagd als N-VDS-netwerk. We illustreren de benodigde updates na migratie voor het **seg5**-netwerk later in dit voorbeeld.



- Het voorbeeld van de cloudsjabloon genereert de implementatie, zoals hieronder wordt weergegeven.



- IP-adressen van de voorbeeldmachine worden weergegeven in de voorbeeldimplementatie, zoals hieronder wordt weergegeven.

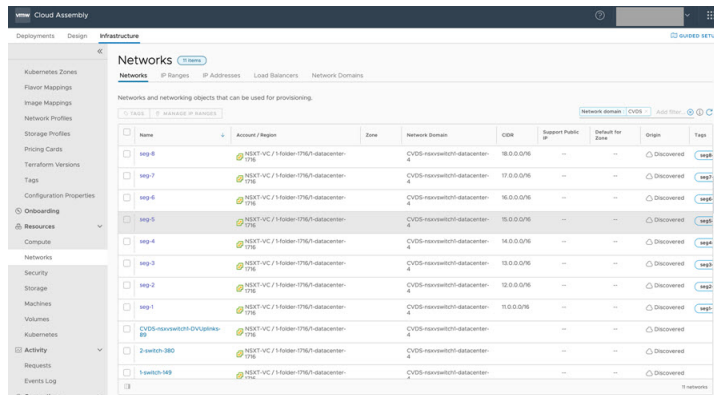


Voorbeeld: stap 1 na migratie - Voer gegevensverzameling uit na migratie van N-VDS- naar C-VDS en inventarisatie

In de bovenstaande sectie zijn schermafbeeldingen gebruikt om de infrastructuur te illustreren die wordt gebruikt in een voorbeeldomgeving van vRealize Automation. Daarna is gekeken naar de cloudsjabloon voor uitvoer en de implementatie.

Als u of een andere beheerder de migratie van N-VDS naar C-VDS in NSX-T heeft uitgevoerd, moet u minstens 10 minuten wachten zodat vRealize Automation het periodieke proces voor gegevensverzameling en inventarisatie kan uitvoeren om beïnvloede resources in vRealize Automation op te halen en weer te geven.

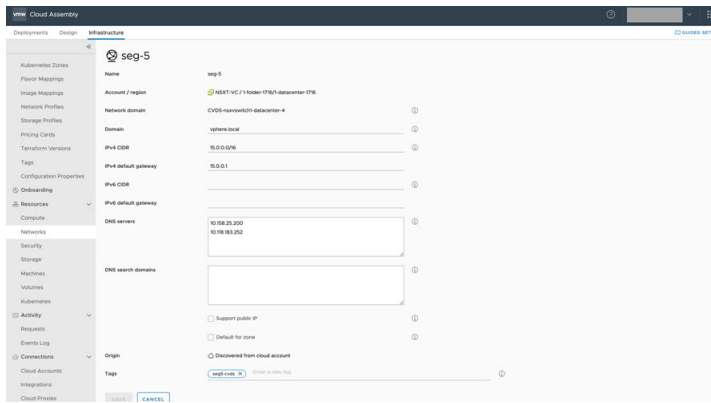
Nadat vRealize Automation-gegevensverzameling is voltooid, klikt u op **Infrastructuur > Netwerken** om de beschikbare C-VDS-netwerken weer te geven en te openen. Hieronder ziet u een **seg5**-netwerk.



Voorbeeld: stap 2 na migratie - Voeg eerder gedefinieerde CIDR en DNS toe aan gemigreerde C-VDS-netwerken

Bewerk een gemigreerd C-VDS-netwerk om CIDR- en DNS-gegevens toe te voegen die zijn opgegeven in de definitie van N-VDS voor migratie en wijzig de netwerktag.

- 1 Voeg CIDR- en DNS-gegevens toe die zijn gedefinieerd in de definitie van N-VDS voor migratie
- 2 Voeg een nieuwe tag toe voor het voorbeeld van het C-VDS-netwerksegment **seg-5**, zoals *seg5-cvds*.



Het oorspronkelijke N-VDS-netwerk **seg-5** is getagd als *seg5-nvds*, zoals weergegeven in eerdere schermen. De wijziging in de details van resourcetags is vereist voor netwerkherconfiguratie. vRealize Automation vereist dat u een andere tagnaam in de cloudsjabloon voor het C-VDS-netwerk opneemt dan de tag die wordt gebruikt in het oorspronkelijke N-VDS-netwerk. De gewijzigde tag identificeert een wijziging in de cloudsjabloon wanneer u een geldige herimplementatie genereert.

Voorbeeld: stap 3 na migratie - Voeg bijgewerkte informatie over het IP-bereik toe

U kunt IP-bereiken voor het netwerk bewerken tot IP-bereikdetails die zijn opgegeven in de definitie van N-VDS vóór de migratie, met behulp van een commandoregel-API of door een menureeks in vRealize Automation te gebruiken.

- Optie 1: Gebruik de API om de gegevens van het IP-bereik bij te werken, zoals in het volgende voorbeeldscherm wordt weergegeven.

PATCH : `{{host}}/iaas/api/network-ip-ranges/{{subnet-range-id}}`

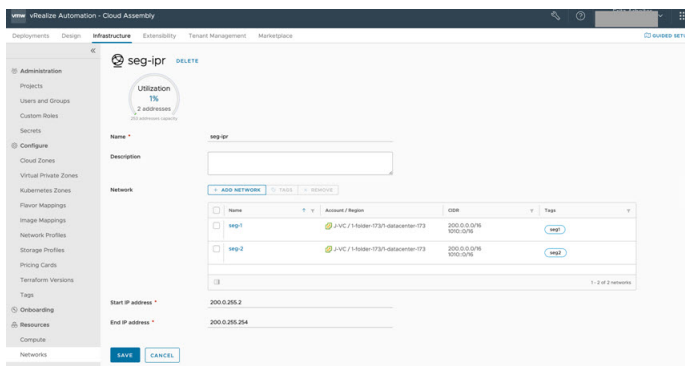
Headers :

- **Authorization :** `Bearer {{token}}`

Payload :

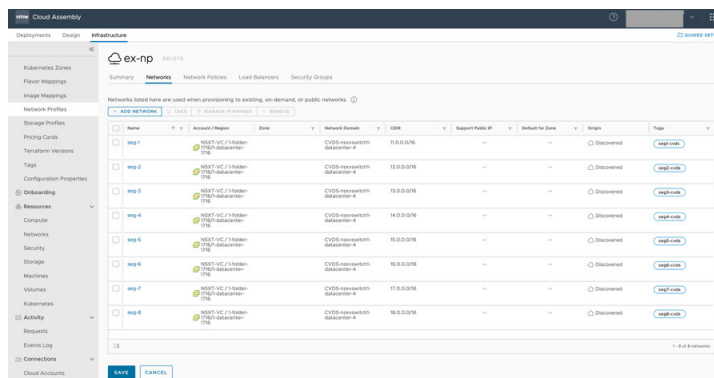
```
{
  "fabricNetworkIds": ["{{subnet-id}}"]
}
```

- Optie 2: Gebruik de gebruikersinterface om de gegevens van het IP-bereik bij te werken, zoals in het volgende voorbeeldscherm wordt weergegeven.



Voorbeeld: stap 4 na migratie - Werk netwerkprofielen bij om ontbrekende netwerken te corrigeren

Na de migratie worden N-VDS-netwerken na gegevensverzameling en inventarisatie afgestemd en uit vRealize Automation Cloud Assembly verwijderd. Beïnvloede netwerkprofielen (zoals het voorbeeld **ex-np**) hebben ontbrekende netwerken. Als u het probleem met ontbrekende netwerken wilt oplossen, moet u elk N-VDS-netwerk bijwerken als C-VDS-netwerk, zoals hieronder wordt weergegeven.

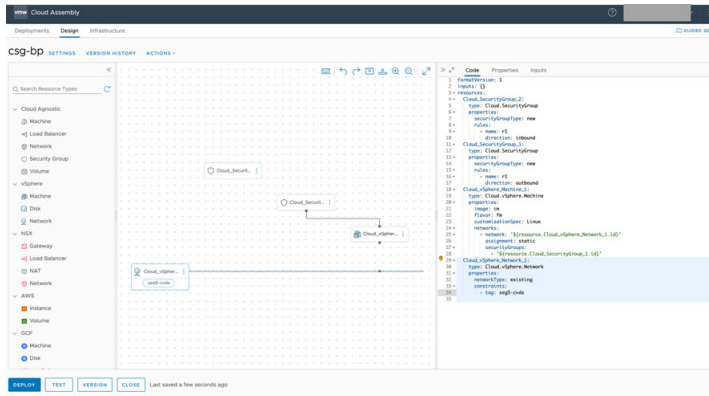


Voorbeeld: stap 5 na migratie - Werk netwerkbeperkingen bij in cloudsjablonen

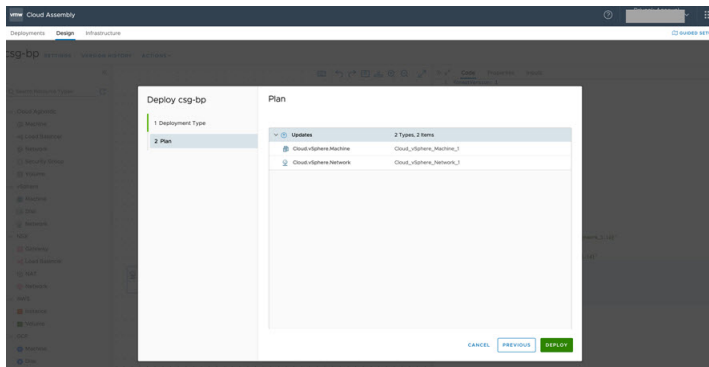
Voor bestaande implementaties moet u netwerkbeperkingen in de cloudsjabloon bijwerken, zodat deze overeenkomen met de nieuwe C-VDS-netwerken in de bijgewerkte netwerkprofielen. Bijgewerkte netwerkbeperkingen zijn ook vereist om iteratieve implementaties uit te voeren en om netwerken van de oorspronkelijke vSphere N-VDS-weergave opnieuw te configureren naar vSphere C-VDS-weergave.

Voor nieuwe implementaties worden de opgegeven C-VDS-resources gebruikt, waardoor deze stap niet is vereist. Iteratieve implementaties en netwerkherconfiguratie werken zoals ze zijn ontworpen.

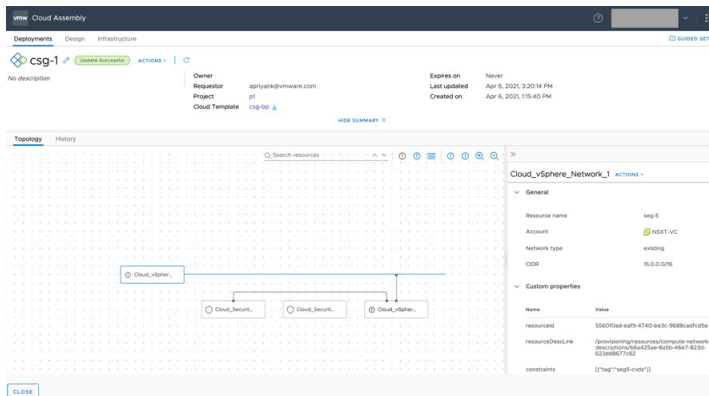
- 1 Wijzig voor dit voorbeeld de netwerkbeperkingen in de cloudsjabloon van *seg5-nvds* in *seg5-cvds*, zoals hieronder wordt weergegeven.



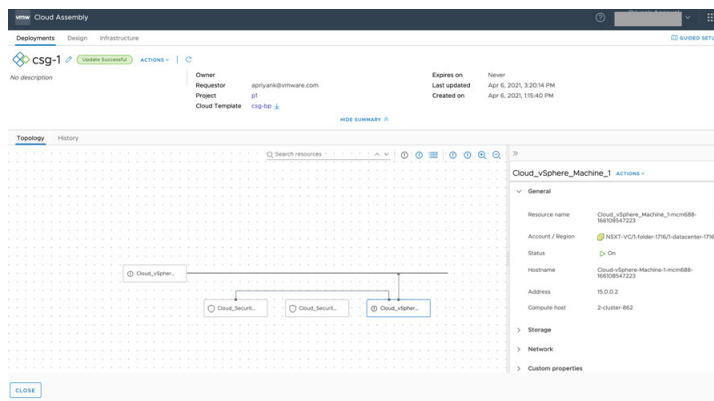
- 2 Voer een iteratieve implementatie uit om het netwerk opnieuw te configureren, zoals hieronder wordt weergegeven.



- 3 Na een geslaagde herimplementatie ziet u dat de aangepaste netwerkeigenschappen de bijgewerkte beperkingen weergeven, zoals hieronder wordt weergegeven.



Omdat het IP-bereik eerder is bijgewerkt met de nieuwe C-VDS-gegevens, wordt het IP-adres van de machine niet correct aangepast in de herimplementatie, zoals hieronder wordt weergegeven.



Het dashboard Inzichten gebruiken om de resourcecapaciteit te bewaken en projecteigenaren op de hoogte te stellen in vRealize Automation

Een cloudbeheerder kan infrastructuurresources en implementatieoptimalisaties in elke cloudzone controleren en beheren. Door realtime-inzichten te visualiseren en voorgestelde acties te bekijken voor de resources die u ondersteunt, kunt u projecteigenaren proactief helpen bij het beheren van de broncapaciteit en hun implementaties optimaliseren.

U kunt het dashboard **Inzichten** gebruiken om statistiekgegevens voor de resources en implementaties in cloudzones te bekijken in de projecten die u beheert. Gebruik deze informatie, verkregen van een combinatie van vRealize Automation en uw geïntegreerde vRealize Operations Manager-applicatie, om eventuele vereiste aanpassingen in het geheugen, CPU's, enzovoort aan te brengen of om deze informatie met uw team te delen, zodat ze beter kunnen worden geïnformeerd en breng alle nodige aanpassingen aan.

Op het dashboard Inzichten kunt u contact opnemen met sommige of alle projecteigenaren die implementaties hebben in de cloudzone die terug te winnen resourcecapaciteit bevatten. De inzichten in de cloudzone geven terug te winnen capaciteit voor projecten en implementaties weer.

Projecteigenaren waarmee contact is opgenomen zien op de pagina **Waarschuwingen** een melding van hun implementatie. De melding bevat hun naam en de naam van (en de koppeling naar) elke implementatie die kan worden geoptimaliseerd.

Het dashboard **Inzichten** is beschikbaar voor vSphere- en VMware Cloud on AWS-cloudzones, op voorwaarde dat de cloudaccounts worden geconfigureerd in zowel vRealize Automation als vRealize Operations Manager en worden bewaakt in vRealize Operations Manager.

Vereisten

- Bekijk [Resourcebeheer en implementatieoptimalisatie met vRealize Operations Manager-statistieken in vRealize Automation](#).
- Controleer of u over de vereiste beheerdersreferenties voor de vRealize Automation-cloud beschikt en HTTPS-toegang hebt ingeschakeld op poort 443. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).

- Controleer of u de gebruikersrol van vRealize Automation-cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Configureer een vRealize Automation-integratie met vRealize Operations Manager.
- Configureer de vRealize Automation-adapter in vRealize Operations Manager.

Over vRealize Operations Manager en de verzamelde capaciteitsstatistieken van de resources

vRealize Operations Manager verzamelt capaciteitsstatistieken voor dezelfde infrastructuurresources die u en de teams die u ondersteunt, in vRealize Automation gebruiken. Door vRealize Automation met vRealize Operations Manager te integreren, worden de vRealize Operations Manager-statistiekgegevens beschikbaar gemaakt en weergegeven voor elk beheerd project in een dashboard **Inzichten** binnen elke cloudzone.

Projectgegevens worden geparseerd naar het vRealize Automation-dashboard van de geïntegreerde vRealize Operations Manager-applicatie. Het dashboard Inzichten bevat de volgende informatie:

- Percentage van CPU-verbruik ten opzichte van capaciteit
- Percentage van geheugenverbruik ten opzichte van capaciteit
- Percentage van opslagverbruik ten opzichte van capaciteit
- Geschiedenis van berekende CPU- en geheugenvraag en verwachte vraag
- Optie om contact op te nemen met eigenaren van sommige of alle implementaties in een cloudzone die kunnen worden geoptimaliseerd door resources vrij te maken, bijvoorbeeld door de grootte van machines te wijzigen of machines te verwijderen. Optimalisatiegegevens worden berekend in volgorde van dagen.

Het dashboard Inzichten is beschikbaar voor vSphere-resources.

Een trendwidget bevat de computeronderdelen van een cloudzone (zoals clusters en hosts), hun CPU-gebruik in GHz ten opzichte van de CPU-capaciteit en hun geheugengebruik in GB ten opzichte van de geheugencapaciteit.

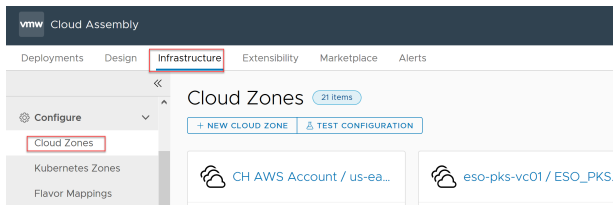
Informatie over de rollen die zijn vereist voor het gebruik van waarschuwingen, is beschikbaar op [Custom gebruikersrollen in vRealize Automation](#).

Zie [Resourcebeheer en implementatieoptimalisatie met vRealize Operations Manager-statistieken in vRealize Automation](#) voor gerelateerde informatie.

Procedure

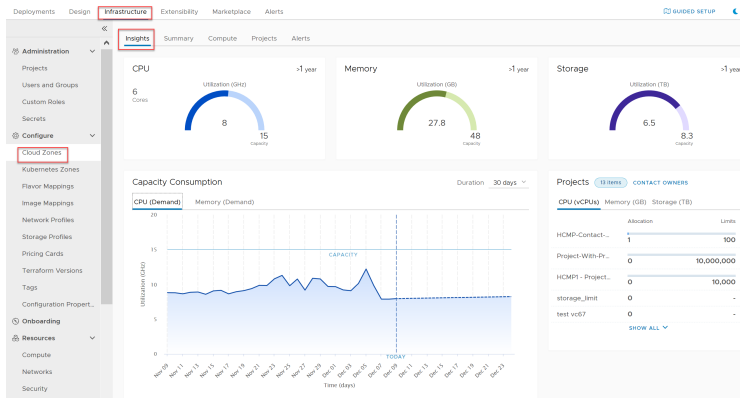
Open een cloudzone om de capaciteitsstatistieken te ontdekken en optioneel informatie op te halen over projectimplementaties die kunnen worden geoptimaliseerd. De gegevens worden verzameld en geleverd door de bijbehorende vRealize Operations Manager-applicatie.

- 1 Klik in Cloud Assembly op **Infrastructuur > Configureren > Cloudzones** en selecteer een cloudzone.

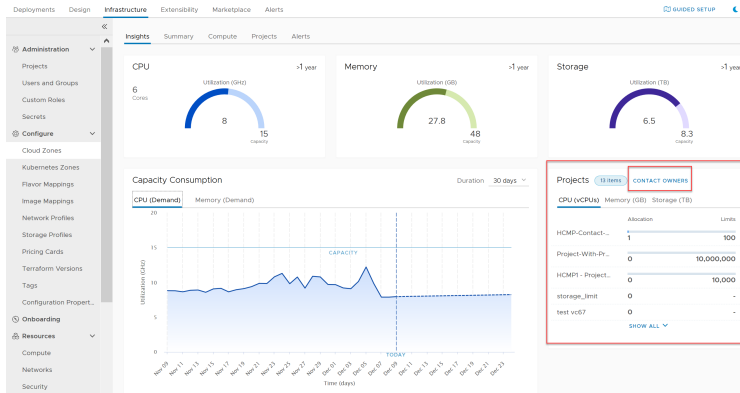


- Klik op het tabblad **Inzichten** en bekijk het dashboard Inzichten.

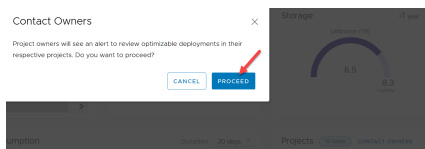
In het volgende voorbeeld wordt informatie over de CPU, het geheugen en de opslagcapaciteit weergegeven voor de resources die door projecten in de cloudzone worden gebruikt.



- Als u de eigenaar van het project wilt informeren over implementaties die kunnen worden geoptimaliseerd, klikt u op **Contact opnemen met eigenaren** in de sectie **Projecten**. Meldingen worden weergegeven op het tabblad **Waarschuwingen**.

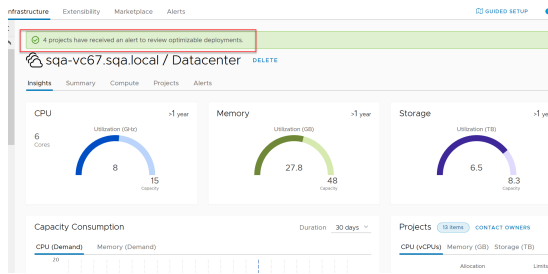


- Als u optimalisatie-informatie over elke implementatie voor het project wilt ophalen, klikt u op **Doorgaan**.



Als het project implementaties bevat die kunnen worden geoptimaliseerd, wordt die informatie aan de projecteigenaar verstrekt op het tabblad **Waarschuwingen** in Cloud Assembly.

- 5 Er wordt een bericht weergegeven met het aantal implementaties dat kan worden geoptimaliseerd.



Meldingsinformatie over deze resources en implementaties is beschikbaar voor de projecteigenaar op het tabblad **Waarschuwingen** in Cloud Assembly. Voor dit voorbeeld bevat meldingsinformatie de naam van, en een link naar, elke implementatie die kan worden geoptimaliseerd, zoals in het volgende voorbeeld wordt weergegeven:

The screenshot shows the 'Alerts' tab in the Cloud Assembly interface. A list of alerts is displayed on the left, with one alert selected: 'The project has some deployments that contain optimizable resources'. The right pane shows the details of this alert, including a 'Deployments to review' table with columns 'Name' and 'Owner'. The table lists 'DND-Deployment-Genie' as a deployment that can be optimized. A red arrow points to the 'DND-Deployment-Genie' entry in the table. The 'Notes' section contains a text area with the note 'Leave a note...'.

Volgende stappen

Gebruik de informatie die u hebt verkregen van het dashboard **Inzichten** om de nodige aanpassingen aan te brengen in de resources die u beheert. Open de pagina **Waarschuwingen** om aanvullende informatie, voorgestelde acties en links naar implementaties te verkrijgen die kunnen worden geoptimaliseerd. Zie [Waarschuwingen gebruiken om de resourcecapaciteit, prestaties en beschikbaarheid in vRealize Automation te beheren](#).

Waarschuwingen gebruiken om de resourcecapaciteit, prestaties en beschikbaarheid in vRealize Automation te beheren

Als cloudbeheerder moet u weten wanneer capaciteit, prestaties en beschikbaarheid in vRealize Automation problematisch worden, zodat u proactief kunt reageren voordat gebruikers onvoldoende resources hebben.

U kunt een reeks waarschuwingen weergeven die door de betreffende vRealize Operations Manager-applicatie zijn opgegeven. Waarschuwingen zijn momenteel beschikbaar voor vSphere- en VMware Cloud on AWS-resourceobjecten. Gebruik informatie in waarschuwingen om de resources en implementaties die u beheert, te wijzigen of om die informatie met uw team te delen, zodat het objecten kan wijzigen die het beheert.

Opmerking Zie [Waarschuwingen gebruiken om implementaties in vRealize Automation te optimaliseren](#) om projectimplementaties te onderzoeken en de nodige acties uit te voeren voor projectimplementaties die u mogelijk kunt optimaliseren.

Waarschuwingen zijn momenteel alleen beschikbaar voor vSphere- en VMware Cloud on AWS-resourceobjecten. Het tabblad **Waarschuwingen** is alleen beschikbaar als toegang tot vRealize Operations Manager is geconfigureerd.

De drempelwaarden voor vRealize Automation-waarschuwingen worden ingesteld in vRealize Operations Manager. Sommige vRealize Automation-waarschuwingen zijn momenteel vooraf gedefinieerd. Meldingen voor waarschuwingen worden ook in vRealize Operations Manager ingesteld. Zie de [productdocumentatie](#) voor vRealize Operations Manager voor informatie over het instellen van waarschuwingsdefinities en het configureren van meldingen.

Vereisten

- Bekijk [Resourcebeheer en implementatieoptimalisatie met vRealize Operations Manager-statistieken in vRealize Automation](#).
- Controleer of u over de vereiste beheerdersreferenties voor de vRealize Automation-cloud beschikt en HTTPS-toegang hebt ingeschakeld op poort 443. Zie [Inloggegevens die vereist zijn voor het werken met cloudaccounts in vRealize Automation](#).
- Controleer of u de gebruikersrol van vRealize Automation-cloudbeheerder hebt. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Configureer een vRealize Automation-integratie met vRealize Operations Manager.
- Configureer de vRealize Automation-adapter in vRealize Operations Manager.
- Configureer de rollen die nodig zijn om waarschuwingen te beheren. Zie [Custom gebruikersrollen in vRealize Automation](#).

Rolmogelijkheden zijn onder meer:

- Cloudbeheerders kunnen cloudzonewaarschuwingen beheren.
- Projectbeheerders kunnen projectwaarschuwingen beheren.
- Service Broker-beheerders kunnen implementatiewaarschuwingen beheren.

Over vRealize Operations Manager en resourcewaarschuwingen

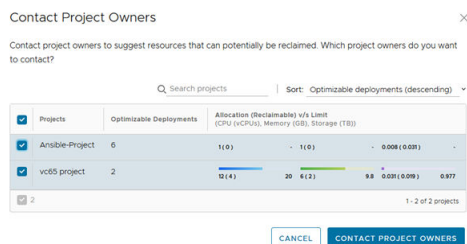
vRealize Operations Manager verzamelt status-, gebruiks- en andere statistieken voor dezelfde infrastructuurresources en -implementaties die u in vRealize Automation beheert. Door vRealize Automation te integreren met vRealize Operations Manager, worden de gecontroleerde gegevens ter beschikking gesteld in vRealize Automation via het tabblad **Waarschuwingen** in het hoofdmenu van Cloud Assembly.

De waarschuwingsgegevens van vRealize Operations Manager omvatten status- en risicodrempels voor cloudsjablonen, implementaties, organisaties en projecten. Ze bevatten ook informatie over implementaties die kunnen worden geoptimaliseerd, op basis van de eigenaar die wordt benaderd door een actie die is ondernomen op het tabblad **Inzichten** van de cloudzone. Zie [Het dashboard Inzichten gebruiken om de resourcecapaciteit te bewaken en projecteigenaren op de hoogte te stellen in vRealize Automation](#).

Waarschuwingdetails voor elke implementatie zijn onder meer:

- Projectnaam
- Implementatienaam (en link naar de implementatie) die resources bevat die kunnen worden geoptimaliseerd
- Voorgestelde acties
- Mogelijke kostenbesparingen door terugwinning en optimalisatie
- Totaal aantal virtuele CPU's die door de implementatie wordt gebruikt
- Totale hoeveelheid RAM-geheugen dat door de implementatie wordt gebruikt
- Totale hoeveelheid opslagruimte die door de implementatie wordt gebruikt
- Virtuele machines in de implementatie die worden aanbevolen voor terugwinning en optimalisatie, inclusief resourcenaam, niet-actieve machines, uitgeschakelde machines, te grote en te kleine machines, onderbenutte machines en machinemomentopnamen

Door de optie **Contact opnemen met projecteigenaren** te gebruiken op het dashboard Inzichten van de cloudzone, kunt u een samenvatting bekijken van alle projecten die terug te winnen capaciteit (CPU, geheugen en opslag) in de cloudzone hebben en een waarschuwing verstrekken aan sommige of alle projecteigenaren.



Procedure

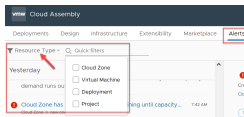
U kunt waarschuwingsdrempelinformatie weergeven over de resources die u beheert met behulp van filteropties op de pagina **Waarschuwingen**. Waarschuwingsgegevens worden verstrekt door uw gekoppelde vRealize Operations Manager-applicatie. Voor elke waarschuwing worden aanbevolen acties gegeven.

U kunt ook een implementatie selecteren in de sectie **Te controleren implementaties** om die implementatie te openen en te optimaliseren. Zie [Waarschuwingen gebruiken om implementaties in vRealize Automation te optimaliseren](#).

- 1 Klik in de Cloud Assembly-service op het tabblad **Waarschuwingen** in het hoofdmenu.

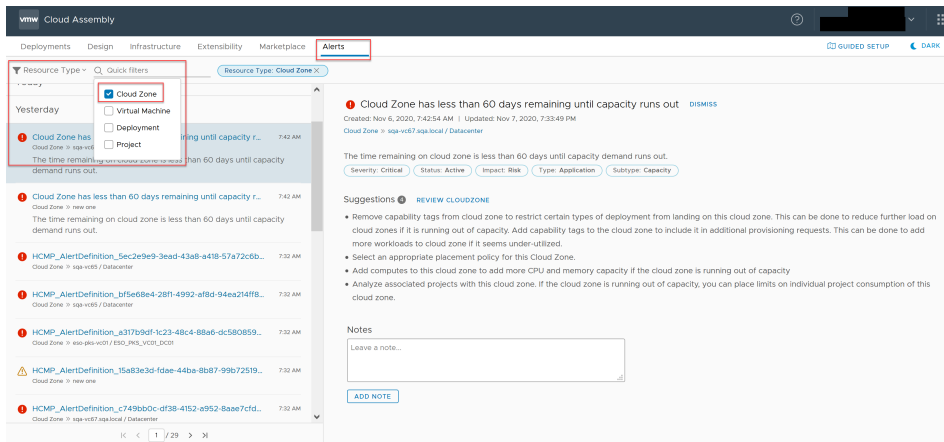


- 2 Als u wilt bepalen hoe waarschuwingen worden weergegeven, experimenteert u met de beschikbare filters. Bijvoorbeeld: selecteer de optie **Resources** in het vervolgkeuzemenu Filters.



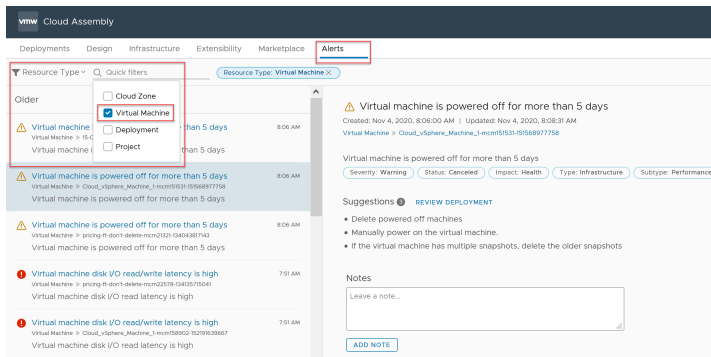
- 3 Gebruik snelfilteropties in het selectiepaneel om waarschuwingen en voorgestelde acties voor die waarschuwingen weer te geven.

- Geef waarschuwingen over cloudzonerresources weer.



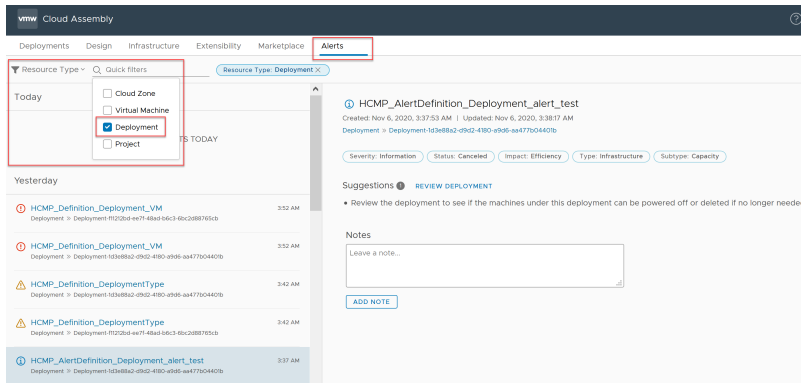
vRealize Operations Manager kan de resterende tijdsduur, de resterende capaciteit, terug te winnen capaciteit, enzovoort bewaken.

- Geef waarschuwingen over resources van virtuele machines weer.



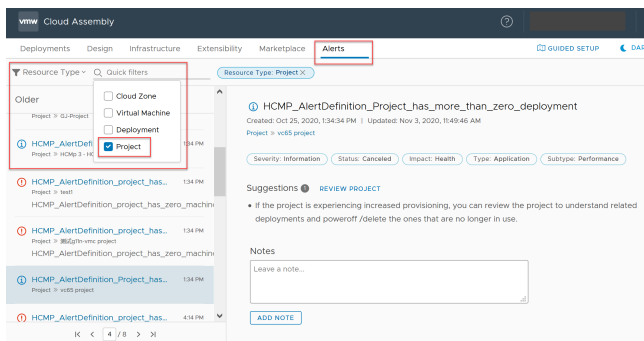
De meeste waarschuwingen voor de virtuele machine hebben betrekking op aan-uitstatus, vertraging, enzovoort.

- Geef waarschuwingen over implementatieresources weer.



De implementatiewaarschuwingen hebben betrekking op terug te winnen resources en het optimaliseren van de grootte.

- Geef waarschuwingen over projectresources weer.



De projectwaarschuwingen hebben betrekking op terug te winnen resources en toewijzingslimieten.

- 4 Bekijk andere filtertypen en hun snelle filteropties om de lijst met waarschuwingen verder te beheren.

- Gebruik de snelle filters **Impact** voor status, risico en efficiëntie.
- Gebruik de snelle filters **Ernst** voor kritiek, onmiddellijk, waarschuwing en informatie.

- Gebruik de snelle filters **Status** voor actief, geannuleerd en gesloten.
- Gebruik de filters **Subtype** voor beschikbaarheid, prestaties en capaciteit.
- Gebruik de snelle filters **Type** voor applicatie, hardware, infrastructuur, opslag en netwerk.

5 Voer de nodige acties uit op basis van waarschuwingsgegevens en suggesties.

Volgende stappen

Zie [Waarschuwingen gebruiken om implementaties in vRealize Automation te optimaliseren](#) voor meer informatie over andere beschikbare acties.

U kunt ook **capaciteitsinzichten** weergeven voor resources op basis van cloudzones in projecten die u beheert. Zie [Het dashboard Inzichten gebruiken om de resourcecapaciteit te bewaken en projecteigenaren op de hoogte te stellen in vRealize Automation](#) voor informatie over het gebruik van gegevens in door vRealize Operations Manager geleverde **inzichten** in vRealize Automation.

Waarschuwingen gebruiken om implementaties in vRealize Automation te optimaliseren

Als cloudbeheerder of projecteigenaar kunt u machineresources zo goed mogelijk controleren en beheren met behulp van gegevens die zijn verkregen van vRealize Operations Manager en worden weergegeven in vRealize Automation.

Wanneer u vRealize Automation verbindt met vRealize Operations Manager, hebt u toegang tot informatie op basis van gegevensverzameling over resources in de projecten die u beheert. Gegevens van waarschuwingen en inzichten worden geboden om u te informeren over verschillende problemen met de projecten die u beheert, en bieden een eenvoudige manier om optimalisatiesuggesties en ondersteunende gegevens die worden verzameld in vRealize Operations Manager, eenvoudig te communiceren aan projecteigenaren zonder de vRealize Automation-applicatie te verlaten. U kunt bijvoorbeeld terug te winnen resourcecapaciteit zien, met specifieke kostenbesparingen, voor elke implementatie in een cloudzone. Waar een cloudzone meerdere implementaties bevat die kunnen worden geoptimaliseerd, kunt u sommige of alle project- en implementatie-eigenaren op de hoogte stellen.

Waarschuwingen voor implementatieoptimalisatie kunnen worden gegenereerd vanaf het dashboard Inzichten. Zie [Het dashboard Inzichten gebruiken om de resourcecapaciteit te bewaken en projecteigenaren op de hoogte te stellen in vRealize Automation](#) . U kunt contact opnemen met projecteigenaren zodat zij een benoemde implementatie kunnen openen om te worden geoptimaliseerd via een koppeling op de pagina **Waarschuwingen**. Projecteigenaren kunnen ook hun implementaties rechtstreeks openen en het tabblad **Optimaliseren** gebruiken om beschikbare optimalisatietaken uit te voeren. Acties die een projecteigenaar kan uitvoeren, zijn onder andere het vrijmaken van resources door niet-kritieke implementaties te verwijderen en het stoppen van verdere inrichting binnen een cloudzone.

Opmerking Zie [Waarschuwingen gebruiken om de resourcecapaciteit, prestaties en beschikbaarheid in vRealize Automation te beheren](#) voor meer informatie over andere herstelacties voor resources die u kunt uitvoeren.

Vereisten

Zie [Waarschuwingen gebruiken om de resourcecapaciteit, prestaties en beschikbaarheid in vRealize Automation te beheren](#) voor de benodigde verificatiegegevens en configuratiegegevens voor toegang tot vRealize Operations Manager-gegevens in vRealize Automation.

Zie [Het dashboard Inzichten gebruiken om de resourcecapaciteit te bewaken en projecteigenaren op de hoogte te stellen in vRealize Automation](#) om aan te vragen dat projecteigenaren worden gewaarschuwd voor implementaties die kunnen worden geoptimaliseerd.

Info

Elke implementatie bevat een tabblad **Optimaliseren**. De volgende optimalisatieparameters zijn beschikbaar:

- Machines die de juiste grootte kunnen krijgen - Geeft informatie en acties weer voor te grote en te kleine machines in de implementatie, samen met kostenbesparingen voor optimalisatie.
- Machines die onderbenut zijn - Geeft informatie en acties weer voor inactieve of uitgeschakelde machines in de implementatie, samen met kostenbesparingen voor optimalisatie.
- Momentopnamen van machines - Geeft informatie en acties weer voor machinemomentopnamen als machines in de implementatie momentopnamen bevatten, samen met kostenbesparingen voor optimalisatie.

Als beheerder kunt u projecteigenaren informeren dat ze implementaties hebben die kunnen worden geoptimaliseerd. Meldingen worden weergegeven op het tabblad **Waarschuwingen** in Cloud Assembly.

Het tabblad **Waarschuwingen** is alleen beschikbaar als toegang tot vRealize Operations Manager is geconfigureerd. Projecteigenaren kunnen hun implementaties openen en optimaliseren om op waarschuwingen te reageren.

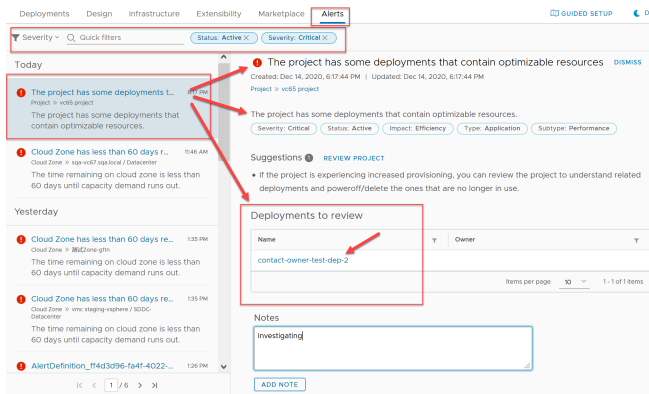
Procedure

U kunt waarschuwingsdrempelinformatie weergeven over de resources die u beheert met behulp van filteropties op de pagina **Waarschuwingen**. Waarschuwingsgegevens worden verstrekt door uw gekoppelde vRealize Operations Manager-applicatie. Voor elke waarschuwing worden aanbevolen acties gegeven. In dit voorbeeld opent de projecteigenaar de implementatie via een link die wordt geleverd in een waarschuwing melding. Op het tabblad **Optimaliseren** van de implementatie worden beschikbare machineparameters weergegeven om deze te optimaliseren.

- 1 Als projecteigenaar of beheerder klikt u op het tabblad **Waarschuwingen** in het hoofdmenu.



- 2 Zoek een waarschuwing die informatie bevat over een implementatie die kan worden geoptimaliseerd en klik op de implementatiennaam in **Te controleren implementaties** om die implementatie te openen en het tabblad **Optimaliseren** weer te geven.



3 Wanneer de implementatie wordt geopend, klikt u op **Optimaliseren**.



- Als er onbenutte machines zijn, onderzoekt u inactieve en uitgeschakelde machines en voert u de nodige acties uit. U kunt een te kleine implementatie uitschakelen of verwijderen.
- Als er machines zijn die de juiste grootte kunnen krijgen, onderzoekt u eventuele te grote en te kleine machines in de implementatie en voert u de nodige acties uit.
- Als een of meer machines in de implementatie een momentopname bevatten, kunt u elke momentopname verwijderen of exporteren.
- Wanneer u klaar bent, bevestigt u dat de implementatie is geoptimaliseerd zoals u wilt en sluit u de implementatie.

Volgende stappen

Zie [Waarschuwingen gebruiken om de resourcecapaciteit, prestaties en beschikbaarheid in vRealize Automation te beheren](#) voor meer informatie over andere beschikbare acties.

U kunt ook **capaciteitsinzichten** weergeven voor resources op basis van cloudzones in projecten die u beheert. Zie [Het dashboard Inzichten gebruiken om de resourcecapaciteit te bewaken en projecteigenaren op de hoogte te stellen in vRealize Automation](#) voor informatie over het gebruik van gegevens in door vRealize Operations Manager geleverde **inzichten** in vRealize Automation.

Wat kan ik doen met standaardschijfopslag in vRealize Automation

Standaardschijven kunnen persistent of niet-persistent zijn.

vRealize Automation ondersteunt twee categorieën opslagruimte: standaardschijf en de eersteklasschijf. De eersteklasschijf is alleen beschikbaar voor vSphere.

■ vSphere

vSphere ondersteunt afhankelijke (standaard), onafhankelijke permanente en onafhankelijke niet-permanente standardschijven. Zie [Wat kan ik doen met persistente schijfopslag in vRealize Automation](#) voor gerelateerde informatie.

Wanneer u een virtuele machine verwijdert, worden de afhankelijke en onafhankelijke niet-persistente schijven ook verwijderd.

Wanneer u een virtuele machine verwijdert, worden de onafhankelijke persistente schijven ervan niet verwijderd.

U kunt een momentopname maken van afhankelijke en onafhankelijke niet-persistente schijven. U kunt geen momentopname maken van een onafhankelijke persistente schijf.

- Amazon Web Services (AWS) EBS

U kunt een EBS-volume koppelen aan een AWS-berekeningsinstantie of een EBS-volume loskoppelen van een AWS-berekeningsinstantie.

Wanneer u een virtuele machine verwijdert, wordt het gekoppelde EBS-volume losgekoppeld, maar niet verwijderd.

- Microsoft Azure VHD

Gekoppelde schijven zijn altijd persistent.

Wanneer u een virtuele machine verwijdert, geeft u op of de gekoppelde opslagschijven moeten worden verwijderd.

- Google Cloud Platform (GCP)

Gekoppelde schijven zijn altijd persistent.

Persistente schijven bevinden zich op een onafhankelijke locatie van uw VM-instanties. U kunt persistente schijven dus loskoppelen of verplaatsen met behoud van uw gegevens, zelfs als u uw VM-instanties hebt verwijderd.

Wanneer u een virtuele machine verwijdert, wordt de gekoppelde schijf losgekoppeld, maar niet verwijderd.

Zie [Meer informatie over opslagprofielen in vRealize Automation](#) voor gerelateerde informatie.

Wat kan ik doen met persistente schijfopslag in vRealize Automation

Persistente schijven beschermen waardevolle gegevens tegen onopzettelijk verwijderen.

In een cloudsjabloon onder een volume kunt u de eigenschap `persistent: true` toevoegen om de schijf het verwijderen van Cloud Assembly of Service Broker te laten overleven. Persistente schijven worden niet verwijderd tijdens het verwijderen van de implementatie, noch met verwijderbewerkingen voor de schijf voor dag 2.

Hierdoor kunnen persistente schijven in uw infrastructuur blijven bestaan, zelfs na het verwijderen van een implementatie of schijf. Om deze te verwijderen, kunt u de volgende technieken gebruiken.

- De opschoningsvlag expliciet doorgeven als queryparameter met behulp van API VERWIJDEREN.
- Ze direct uit het cloudeindpunt verwijderen.

Houd er rekening mee dat er geen Cloud Assembly- of Service Broker-gebruikersinterface is om deze te verwijderen.

Wat kan ik doen met de eersteklasschijfopslag in vRealize Automation

Een FCD-schijf (Eersteklassschijf) biedt opslaglevenscyclusbeheer op virtuele schijven als een schijfservice of als EBS-achtige schijfopslag waarmee u schijven onafhankelijk van virtuele machines van vSphere kunt maken en beheren.

vRealize Automation ondersteunt twee categorieën opslagschijven: standaardschijf en de eersteklassschijf. Eersteklassschijf-functionaliteit wordt alleen ondersteund voor vSphere. vRealize Automation biedt momenteel eersteklassschijffunctionaliteit als een alleen-API-mogelijkheid.

Een eersteklassschijf heeft eigen levenscyclusbeheerfuncties die onafhankelijk van een VM werken. Eén manier waarop een eersteklassschijf verschilt van een onafhankelijke persistente schijf is dat u een eersteklassschijf kunt gebruiken om momentopnamen onafhankelijk van een VM te maken en beheren.

U kunt een nieuw opslagprofiel voor vRealize Automation maken om de mogelijkheden van de eersteklassschijf of standaardschijf te ondersteunen. Zie [Meer informatie over opslagprofielen in vRealize Automation](#) en [Opslagresources in vRealize Automation](#).

U kunt ook een `Cloud.vSphere.Disk`-eersteklassschijfelement in uw vRealize Automation-cloudsjablonen en -implementaties toevoegen om vSphere-eersteklassschijven te ondersteunen. De eersteklassschijven waarvoor gegevens zijn verzameld, verschijnen op de pagina **Resources > Resources > Volumes**.

In vCenter worden de eersteklassschijven ook wel *Verbeterde virtuele schijven (IVD)* of *beheerde virtuele schijven* genoemd.

Capaciteiten

Met vRealize Automation-API-mogelijkheden kunt u:

- Een eersteklassschijf maken, in een lijst zetten en verwijderen.
- De grootte van een eersteklassschijf wijzigen.
- Een eersteklassschijf koppelen en ontkoppelen.
- De momentopnamen van de eersteklassschijf maken en beheren.
- Een bestaande standaardschijf converteren naar een eersteklassschijf

De volgende scenario's worden ook ondersteund:

- VM's inrichten op basis van momentopnamen in een gegevensopslagcluster.
- Het bezitten en delen van apparaatgebaseerde opslagblokken door gebruikers en tenants.
- VM-momentopnamen maken en herstellen.
- Opslag koppelen op meerdere VM's en tussen clusters.

Gerelateerde API-informatie over het maken en beheren van FCD-opslag (Eersteklasschijf) met behulp van de vRealize Automation-API, inclusief hoe u een opslagprofiel definieert voor het gebruik van de mogelijkheden van de eersteklasschijf, is beschikbaar op code.vmware.com bij [Wat zijn de vRealize Automation Cloud-API's en hoe gebruik ik ze](#) of door te navigeren vanaf de volgende locaties:

- API-documentatie voor FCD is beschikbaar in de [Eersteklasschijf \(FCD\)](#)-sectie van de [Virtual Disk Development Kit-programmeerhandleiding](#).
- Links naar de API-gebruiksscenario-documentatie voor FCD in vRealize Automation zijn beschikbaar op de pagina [vRealize Automation API-documentatie](#) voor uw vRealize Automation-release.

Overwegingen en beperkingen

Overwegingen en beperkingen voor de eersteklasschijf omvatten momenteel:

- De eersteklasschijf is alleen beschikbaar voor vSphere-VM's.
- vSphere 6.7 update 2 of hoger is vereist voor het gebruik van eersteklasschijven.
- Het inrichten van eersteklasschijven op gegevensopslagclusters wordt niet ondersteund.
- De optie voor meervoudig koppelen volume wordt niet ondersteund voor eersteklasschijven.
- De grootte van eersteklasschijven met momentopnamen kan niet worden gewijzigd.
- Eersteklasschijven met momentopnamen kunnen niet worden verwijderd.
- De momentopnamehiërarchie van eersteklasschijven kan alleen worden gemaakt met behulp van de optie `createdAt`-API.
- De minimale versie van VM-hardware die is vereist voor het koppelen van eersteklasschijven is vmx-13 (ESX 6.5-compatibel).

Tenantresources voor meerdere providers configureren met vRealize Automation

In multitenancy omgevingen kunnen klanten de toewijzing van resources per tenant beheren met behulp van virtuele privézones (VPZ's).

In vRealize Automation 8.x kunnen klanten multitenancy omgevingen configureren met behulp van VMware Lifecycle Manager en Workspace ONE Access. Met deze tools kunnen gebruikers multitenancy instellen en tenants maken en configureren. Nadat tenants zijn geconfigureerd, kunnen providerbeheerders virtuele privézones in Cloud Assembly maken en kunnen ze vervolgens zones aan tenants toewijzen via de Cloud Assembly-functionaliteit Tenants beheren.

Multitenancy is gebaseerd op de hieronder beschreven coördinatie en configuratie van drie verschillende VMware-producten:

- **Workspace ONE Access:** dit product biedt de infrastructurele ondersteuning voor multitenancy en de Active Directory-domeinverbindingen waarmee het gebruikers- en groepsbeheer binnen tenantorganisaties wordt geregeld.
- **vRealize Suite Lifecycle Manager:** met dit product kunt u tenants maken en configureren voor ondersteunde producten, zoals vRealize Automation. Daarnaast hebt u hiermee een beperkt aantal mogelijkheden voor certificaatbeheer.
- **vRealize Automation:** providers en gebruikers melden zich aan bij vRealize Automation om toegang te krijgen tot tenants waarin ze implementaties maken en beheren.

Wanneer u multitenancy configureert, moeten gebruikers bekend zijn met alle drie de producten en bijbehorende documentatie.

Zie het volgende voor meer informatie over het werken met vRealize Suite Lifecycle Manager en Workspace ONE Access.

Hoe maak ik een Virtuele privézone voor vRealize Automation

Providerbeheerders kunnen een Virtuele privézone (VPZ) creëren om infrastructuurresources toe te wijzen aan tenants in een vRealize Automation-omgeving met meerdere organisaties. Beheerders kunnen ook VPZ's gebruiken om de toewijzing van resources te beheren in implementaties met één tenant.

U kunt virtuele privézones gebruiken om resources zoals images, netwerken en opslagresources toe te wijzen. Virtuele privézones functioneren grotendeels als cloudzone per tenant, maar ze zijn specifiek ontworpen voor gebruik met implementaties met meerdere tenants. Voor elk project kunt u cloudzones of VPZ's gebruiken, maar niet beide. Daarnaast bestaat er een één-op-één-relatie tussen VPZ's en tenants. Dat wil zeggen dat een VPZ slechts aan één tenant tegelijk kan worden toegewezen.

Opmerking U configureert image- en soorttoewijzingen voor een VPZ op de pagina Tenantbeheer.

U kunt een VPZ maken met of zonder NSX. Als u een zone maakt zonder NSX zijn er beperkingen ten aanzien van NSX-gerelateerde functionaliteit op vSphere-eindpunten.

- Beveiliging (groepen, firewall)
- Netwerkonderdelen (NAT)

Voorwaarden

- U kunt multitenancy op uw vRealize Automation-implementatie inschakelen en configureren met behulp van VMware Lifecycle Manager en VMware Workspace ONE Access.
- Maak indien nodig tenantbeheerders voor uw tenantconfiguratie.
- Als u NSX wilt gebruiken, moet u een geschikt NSX-cloudaccount maken in de organisatie van uw provider.

Procedure

- 1 Selecteer **Infrastructuur > Configureren > Virtuele privézones**

De pagina VPZ toont alle bestaande zones en stelt u in staat om zones te maken.

- 2 Klik op **Nieuwe virtuele privézone**.

New Virtual Private Zone

Er zijn vier selecties aan de linkerkant van de pagina die u kunt gebruiken om samenvattingsinformatie en infrastructuuronderdelen voor de zone te configureren.

3 Voer samenvattingsinformatie voor de nieuwe zone in.

- a Voer een naam en een beschrijving in.
- b Selecteer een account waarop de zone van toepassing is.
- c Schakel het Plaatsingsbeleid in.

Plaatsingsbeleid bepaalt hostselectie voor implementaties binnen de opgegeven cloudzone.

- **Standaard** - Hiermee worden computerresources over clusters en willekeurige hosts gedistribueerd. Deze selectie werkt op een individueel machineniveau. Alle machines in een bepaalde implementatie worden bijvoorbeeld willekeurig verdeeld over de beschikbare clusters en hosts die voldoen aan de vereisten.
- **binpack** - Plaatst computerresources op de meest belaste host die voldoende beschikbare resources heeft om de gegeven berekening uit te voeren.
- **spread** - Geeft implementatieberekenningsresources aan het cluster of de host met het minste aantal virtuele machines. Voor vSphere distribueert Distributed Resource Scheduler (DRS) de virtuele machines over de hosts. Alle aangevraagde machines in een implementatie worden bijvoorbeeld op hetzelfde cluster geplaatst, maar de volgende implementatie kan een ander vSphere-cluster selecteren, afhankelijk van de huidige belasting.

4 Selecteer Resource berekenen voor de zone.

Voeg indien nodig computerresources toe voor de cloudzone. In eerste instantie omvat de filterselectie inclusief Alle berekeningen opnemen is en de volgende lijst alle beschikbare computerresources toont en die worden toegewezen aan de relevante zone. Er zijn twee extra opties voor het toevoegen van computerresources aan een cloudzone.

- **Selecteer handmatig Berekenen** - Selecteer dit menu-item als u computerresources handmatig wilt selecteren in de lijst hieronder. Nadat u deze heeft geselecteerd, klikt u op Berekening toevoegen om de resources aan de zone toe te voegen.
- **Dynamisch opnemen op basis van labels** - Selecteer dit menu-item als u een rekenresource wilt selecteren die aan de zone moet worden toegevoegd op basis van labels. Alle computerresources worden weergegeven totdat u de juiste labels toevoegt. U kunt een of meer labels selecteren of invoeren in de optie Berekening opnemen met deze labels.

Voor beide rekenselecties kunt u een of meer rekenresources verwijderen die op de pagina worden weergegeven door het vak aan de rechterkant te selecteren en op Verwijderen te klikken.

- 5 Voer de gewenste labels in of selecteer deze.
- 6 Selecteer Opslag in het linkermenu en selecteer het opslagbeleid en andere opslagconfiguraties voor de zone.

- 7 In het linkermenu selecteert u **Netwerk** en definieert u de netwerken en optioneel een netwerkbeleid dat u met deze zone wilt gebruiken. U kunt ook load balancers en beveiligingsgroepen configureren voor de geselecteerde netwerkbeleidsregels.

Netwerk	<ul style="list-style-type: none"> ■ Alle bestaande netwerken die aan deze VPZ zijn gekoppeld, worden weergegeven in de tabel op het tabblad Netwerken. ■ Klik op Netwerk toevoegen om alle netwerken te zien die aan de geselecteerde regio zijn gekoppeld. Voeg een netwerk toe voor gebruik met deze zone. ■ Selecteer een netwerk en klik op Labels om een of meer labels toe te voegen aan het gespecificeerde netwerk. ■ Selecteer IP-bereiken beheren om het IP-bereik op te geven waarmee gebruikers toegang hebben tot dit netwerk. ■ Indien van toepassing klikt u op het tabblad Netwerkbeleid en selecteert u een isolatiebeleid.
Netwerkbeleid	<p>Indien geconfigureerd, selecteert u een netwerkbeleid dat u wilt gebruiken met deze zone om een isolatiebeleid af te dwingen voor uitgaande en privénetwerken.</p> <ul style="list-style-type: none"> ■ Selecteer indien gewenst een isolatiebeleid. ■ Selecteer een logische router van Tier 0 en een Edge-cluster indien gewenst.
Load balancers	Klik op Load Balancer toevoegen om load balancers voor de account- en regio-cloudaccounts te configureren.
Beveiligingsgroepen	Klik op Beveiligingsgroep toevoegen om beveiligingsgroepen te gebruiken om firewallregels toe te passen op ingerichte machines.

Resultaten

De Virtuele privézone wordt gemaakt met de opgegeven resourcetoewijzingen.

Wat nu te doen

Cloudbeheerders kunnen de VPZ koppelen aan een project.

- 1 Selecteer in Cloud Assembly **Beheer > Projecten**
- 2 Selecteer het tabblad Provisioning.
- 3 Klik op **Zone toevoegen** en kies de optie Virtuele privézone toevoegen.
- 4 Selecteer de gewenste VPZ uit de lijst.
- 5 U kunt de inrichtingsprioriteit en -limieten instellen voor het aantal instanties, de hoeveelheid beschikbaar geheugen en het aantal beschikbare CPU's.
- 6 Klik op **Toevoegen**.

Configuratie van virtuele privézone beheren voor vRealize Automation-tenants

Providerbeheerders kunnen virtuele privézones (VPZ) in Cloud Assembly beheren om de toewijzing van infrastructuurresources per tenant te beheren. Op de pagina Tenantbeheer kunnen beheerders tenants en VPZ-zones weergeven en VPZ's voor tenants in- of uitschakelen.

Virtuele privézones worden standaard niet toegewezen aan tenants. U moet de VPZ's op deze pagina toewijzen om deze met uw tenants te kunnen gebruiken.

VPZ's die worden gemaakt, zijn standaard ingeschakeld. Een ingeschakelde VPZ is klaar om te worden toegewezen en gebruikt met de opgegeven tenant. Wanneer VPZ's zijn uitgeschakeld, kunnen deze niet worden gebruikt voor het inrichten of toewijzen aan een tenant. Een VPZ kan worden uitgeschakeld, maar nog steeds worden toegewezen aan een tenant.

Wanneer een providerbeheerder naar de pagina Tenantbeheer navigeert, worden op de pagina alle beschikbare tenants weergegeven en kan de beheerder er een selecteren. Nadat een tenant is geselecteerd, worden op de pagina VPZ's weergegeven die momenteel zijn toegewezen voor die tenant. De beheerder kan deze pagina gebruiken om VPZ's toe te wijzen aan de geselecteerde tenant.

Wanneer een VPZ is toegewezen, kunnen tenantbeheerders deze toevoegen aan hun projecten en wordt deze beschikbaar voor inrichting door tenantgebruikers. Nadat een VPZ is toegewezen aan één tenant, kan deze aan een andere tenant worden toegewezen.

Nadat een VPZ is ingeschakeld, is deze klaar voor gebruik binnen de opgegeven tenant. Providerbeheerders kunnen VPZ's uitschakelen om onderhouds- of tenantherconfiguratie mogelijk te maken, en zij kunnen gebruikers meldingen geven over de uitschakeling. Als u een VPZ niet meer permanent beschikbaar wilt maken voor een tenant, kunt u de toewijzing ervan opheffen. Als de toewijzing van een bestaande VPZ aan een tenant om een bepaalde reden niet kan worden opgeheven, kan deze niet worden gebruikt om implementaties van die tenant te maken.

Voorwaarden

- Stel multitenancy in en maak zo nodig virtuele privézones zoals geschikt voor uw implementatie.
- Configureer algemene image- en soorttoewijzingen voor de VPZ- en tenantconfiguratie met behulp van de menuselecties voor imageroewijzing en soorttoewijzing aan de linkerkant van de pagina Tenantbeheer in Cloud Assembly. Zie [Algemene image- en soorttoewijzing voor vRealize Automation-tenants maken](#).

U kunt deze algemene toewijzingen nu of later overschrijven met de tenantspecifieke selecties voor image- en soorttoewijzing bovenaan de pagina Tenantbeheer. Zie [Tenantspecifieke image- en soorttoewijzingen voor vRealize Automation configureren](#).

Procedure

1 Selecteer Tenants beheren in Cloud Assembly.

Op de pagina Tenantbeheer worden alle tenants weergegeven die zijn geconfigureerd voor de organisatie van de beheerder in een kaartweergave.

2 Klik op een tenant om deze te selecteren.

3 Klik op het tabblad Infrastructuurbeheer om alle toegewezen VPZ's voor de tenant weer te geven.

4 Selecteer **Virtuele privézone toewijzen** om een dialoogvenster te openen waarin alle zones worden weergegeven die momenteel niet aan tenants zijn toegewezen. Wijs de zone toe aan een tenant.

5 Selecteer een of meer zones in het dialoogvenster en klik op **Toewijzen aan tenant**.

Wat nu te doen

Nadat VPZ's zijn toegewezen, kunnen tenantbeheerders deze toewijzen aan projecten.

Providerbeheerders kunnen de kaartweergave van tenants gebruiken om de status van VPZ's te controleren en te beheren.

- Als u een tenant wilt uitschakelen, klikt u op **Uitschakelen** op de kaart voor de tenant.
- Als u een tenant wilt inschakelen, klikt u op **Inschakelen** op de kaart voor de tenant.
- Als u de toewijzing voor een tenant ongedaan wilt maken, klikt u op **Toewijzing ongedaan maken** op de kaart voor die tenant.

Algemene image- en soorttoewijzing voor vRealize Automation-tenants maken

Providerbeheerders kunnen algemene image- en soorttoewijzingen selecteren of maken die aan vRealize Automation-tenants kunnen worden toegewezen.

Met algemene image- en soorttoewijzing kunt u snel toewijzingen instellen die van toepassing zijn op meerdere tenants. U kunt deze toewijzingen ook snel bijwerken. Op de pagina Tenantbeheer kunt u ook specifieke image- en soorttoewijzingen voor de tenant maken die de standaardconfiguraties kunnen overschrijven.

Opmerking Image- en soorttoewijzingen die zijn geconfigureerd op de pagina Tenantbeheer, zijn alleen van toepassing op tenants zoals geconfigureerd en zijn niet van toepassing op de bredere organisatie van de provider.

Voorwaarden

Procedure

- 1 Selecteer Tenants beheren in Cloud Assembly.

Op de pagina Tenantbeheer worden alle tenants weergegeven die zijn geconfigureerd voor de organisatie van de beheerder in een kaartweergave.

- 2 Selecteer Imagetoewijzing in het linkermenu van de pagina Tenantbeheer.

Op de pagina Imagetoewijzing worden alle images weergegeven die momenteel zijn geconfigureerd voor tenants in Cloud Assembly en wordt aangegeven of de toewijzingen algemeen zijn of aan een specifieke tenant zijn gekoppeld.

Create Image Mapping ×

Account / region *

Q

Search for regions

Image Name *

Image *

Q

Search for images

Constraints

Example: !license:none:hard

Scope *

Q

All tenants

Cloud Configuration

1	
---	--

CANCEL

CREATE

3 Selecteer **Imagetoewijzing toevoegen** om een imagetoewijzing toe te voegen voor gebruik met tenants.

- a Selecteer een Account/regio waarop de imagetoewijzing moet worden toegepast.
- b Voer een naam voor de imagetoewijzing in en selecteer de specifieke instantie of versie van de image waarop deze betrekking heeft.
- c Voer de gewenste beperkingstags in.
- d Selecteer het bereik voor de imagetoewijzing. Het bereik kan Alle tenants of algemeen zijn, of u kunt een specifieke tenant selecteren waarop de imagetoewijzing wordt toegepast.

4 Indien gewenst kunt u een cloudconfiguratiescript gebruiken om aangepaste besturingssysteemkenmerken voor implementaties te definiëren.

Bijvoorbeeld: afhankelijk van uw keuze om een cloudsjabloon in een publieke of privécloud te implementeren, kunt u specifieke gebruikersrechten, rechten voor het besturingssysteem of andere voorwaarden voor de image toepassen. Een cloudconfiguratiescript voldoet aan een `cloud-init`-indeling voor op Linux gebaseerde images of een `cloudbase-init`-indeling voor op Windows gebaseerde images. Zie [Meer informatie over imagetoewijzingen in vRealize Automation](#) voor meer informatie.

5 Klik op **Maken** om de imagetoewijzing te maken.

- 6 Selecteer **Soorttoewijzing toevoegen** om een soorttoewijzing toe te voegen voor gebruik met tenants.

- Selecteer een Account/regio waarop de soorttoewijzing van toepassing is.
- Voer een naam in voor de soorttoewijzing die u maakt.
- Selecteer de grootteparameters voor de soorttoewijzing die u maakt.
U kunt het aantal processoren en de hoeveelheid geheugen voor deze soort opgeven.
- Selecteer het bereik voor de soorttoewijzing. Het bereik kan Alle tenants of algemeen zijn, of u kunt een specifieke tenant selecteren waarop de soorttoewijzing van toepassing is. Alle tenants is van toepassing op alle tenants in de organisatie van de providerbeheerder.

- 7 Klik op **Maken** om de soorttoewijzing te maken.

Resultaten

Nadat u algemene toewijzingen hebt gemaakt, worden deze toewijzingen weergegeven op de tabbladen Soorttoewijzing of Tenanttoewijzing op de pagina Tenantbeheer voor toepasselijke tenants.

Wat nu te doen

U kunt algemene image- en soorttoewijzingen op deze pagina bewerken of verwijderen. Als u een toewijzing wilt bewerken, selecteert u deze en brengt u de gewenste wijzigingen aan.

Tenantspecifieke image- en soorttoewijzingen voor vRealize Automation configureren

Met Cloud Assembly kunt u algemene image- en soorttoewijzingen configureren die beschikbaar zijn voor alle virtuele privézones (VPZ's) binnen uw organisatie. U kunt ook de algemene instellingen overschrijven en tenantspecifieke image- en soorttoewijzingen configureren voor uw implementaties.

Doorgaans configureert een cloudbeheerder algemene image- en soorttoewijzingen met de linkernavigatielinks op de pagina Tenantbeheer. Deze toewijzingen zijn van toepassing voor al uw tenants. In sommige gevallen wilt u mogelijk aangepaste, tenantspecifieke image- en soorttoewijzingen maken voor specifieke tenants. Deze optie wordt ondersteund op de pagina Tenantbeheer.

Image- en soorttoewijzingen worden weergegeven op hun respectieve tabbladen op de pagina Tenantbeheer. Klik op een van de bestaande image- en soorttoewijzingen om deze te bewerken. Als u een image- of soorttoewijzing wilt verwijderen, selecteert u de toewijzing en klikt u op **Verwijderen**.

Voorwaarden

- Schakel multitenancy in en configureer tenants voor uw implementatie.
- Maak geschikte VPZ's.

Procedure

- 1 Selecteer Tenantbeheer in het hoofdmenu van Cloud Assembly.
- 2 Selecteer de tenant waarvoor u een aangepaste image- of soorttoewijzing wilt configureren.
- 3 Selecteer de link Imageroewijzing bovenaan de pagina en klik vervolgens op **Imageroewijzing toevoegen**.
Het dialoogvenster Imageroewijzing maken wordt weergegeven.
- 4 Zorg ervoor dat Account/regio correct is ingevuld en voeg een naam voor de toewijzing toe in het tekstvak **Imageroewijzingnaam**.
- 5 Selecteer de onderliggende machine-image die u wilt gebruiken in het vervolgkeuzemenu **Image**.
- 6 Voeg beperkingstags toe indien van toepassing op uw imagegebruik.
- 7 Selecteer het juiste **Bereik** voor de image.
 - Klik op het keuzerondje Alleen beschikbaar voor deze tenant als u wilt dat deze imageroewijzing alleen beschikbaar is voor gebruik door de geselecteerde tenant.
 - Klik op het keuzerondje Gedeeld tussen projecten als u wilt dat deze imageroewijzing beschikbaar is voor gebruik door andere tenants.
- 8 Klik op **Maken** om de imageroewijzing op te slaan zoals geconfigureerd.

- 9 Selecteer de link Soorttoewijzing bovenaan de pagina en klik vervolgens op **Soorttoewijzing toevoegen** om een soorttoewijzing te maken.
Het dialoogvenster Soorttoewijzing maken wordt weergegeven.
- 10 Zorg ervoor dat Account/regio correct is ingevuld en voeg een naam voor de toewijzing toe in het tekstvak **Naam**.
- 11 Geef de CPU- en geheugeninstellingen van de soort op in het veld **Waarde**.
- 12 Selecteer het juiste **Bereik** voor de image.
 - Klik op het keuzerondje Alleen beschikbaar voor deze tenant als u wilt dat deze imago-toewijzing alleen beschikbaar is voor gebruik door de geselecteerde tenant.
 - Klik op het keuzerondje Gedeeld tussen projecten als u wilt dat deze imago-toewijzing beschikbaar is voor gebruik door andere tenants.
- 13 Klik op **Maken** om de soorttoewijzing op te slaan zoals geconfigureerd.

Resultaten

Tenantspecifieke image- en soorttoewijzingen worden geconfigureerd zoals opgegeven.

Uitbreidbaarheidsabonnementen voor providers of tenants maken

Provider- en tenantbeheerders kunnen uitbreidbaarheidsabonnementen maken om toegang te krijgen tot vRealize Orchestrator-werkstromen. vRealize Orchestrator-werkstromen worden geactiveerd op basis van gebeurtenissen als er een abonnement is voor bepaalde gebeurtenisonderwerpen die overeenkomen met een bepaalde levenscyclusfase van de applicatie.

De kenmerken van een uitbreidbaarheidsabonnement verschillen afhankelijk van de maker van het abonnement: de providerbeheerder of de tenantbeheerder.

- De tenantbeheerder kan een abonnement maken, maar kan het organisatiebereik niet opgeven. Dat abonnement wordt alleen geactiveerd voor gebeurtenissen die worden geactiveerd door de tenant.
- De providerbeheerder kan een abonnement maken en het providerbereik opgeven. Het abonnement gedraagt zich net als een tenantabonnement of een omgeving die niet meerdere tenants bevat. Het wordt geactiveerd op basis van gebeurtenissen die afkomstig zijn van de provider.
- De provider kan een abonnement maken en het tenantbereik opgeven. Het abonnement wordt geactiveerd op basis van gebeurtenissen die afkomstig zijn van elke tenant. Het wordt niet geactiveerd door gebeurtenissen die afkomstig zijn van de provider.

Abonnementen activeren vRealize Orchestrator-werkstromen op basis van specifieke gebeurtenissen. Ze roepen geen uitbreidbaarheidsacties aan. Momenteel wordt slechts één vRealize Orchestrator-instantie ondersteund voor een bepaalde providerorganisatie. Zie [Uitbreidbaarheidsterminologie](#) voor meer informatie over gebeurtenissen, gebeurtenisonderwerpen en abonnementen.

Voorwaarden

Configureer tenants en virtuele privézones zoals gepast is voor uw implementatie.

Procedure

- 1 Ga in vRealize Automation vervolgens naar de pagina Abonnementen en klik op **Nieuw abonnement**.

- 2 Voer een **naam** en **beschrijving** in voor de naamruimte.

- 3 Zorg ervoor dat het keuzerondje Abonnement inschakelen is geselecteerd.

U kunt deze knop op de uitpositie laten staan als u niet wilt dat het abonnement direct actief wordt.

- 4 Als u een providerbeheerder bent, selecteert u het geschikte **Organisatiebereik**.

De opties voor het organisatiebereik zijn provider en tenant. Als u tenant selecteert, is het projectbereik een project en kan dit niet worden gewijzigd. Als u een provider selecteert, kunt u het projectbereik opgeven met behulp van de selectie onderaan de pagina Abonnementen.

- 5 Selecteer het **Gebeurtenisonderwerp** waarop u zich wilt abonneren.

- 6 Selecteer een of meer werkstromen.

Resultaten

Providers en tenants kunnen de geretourneerde gebeurtenissen voor een specifieke implementatie bekijken op de pagina Gebeurtenissen in Cloud Assembly. De weergegeven resultaten zijn afhankelijk van uw rol en het organisatiebereik.

- Als Provider is geselecteerd als organisatiebereik, zien providers gebeurtenissen op basis van hun acties in dezelfde providerorganisatie.
- Als Tenant is geselecteerd als organisatiebereik, zien tenants de gebeurtenissen, maar kan de provider ze niet zien. Gebeurtenissen leven altijd in de organisatie van de uitgever.

- 1 Selecteer **Uitbreidbaarheid > Gebeurtenissen** in Cloud Assembly.

- 2 Voer in het zoekvak op de pagina Gebeurtenissen de implementatie-id in waarvoor u gebeurtenissen wilt bekijken.

Op de pagina worden gebeurtenissen weergegeven die overeenkomen met de zoekcriteria.

Werken met oude virtuele privézones in nieuwere versies van vRealize Automation

De configuratieopties voor VPZ's zijn gewijzigd in Cloud Assembly. U kunt oudere virtuele privézones bijwerken of ermee werken in huidige versies van vRealize Automation.

In vRealize Automation 8.2 geconfigureerde gebruikers image- en soorttoewijzingen binnen VPZ's. In nieuwere versies van vRealize Automation maken gebruikers image- en soorttoewijzingen per tenant, waardoor de efficiëntie en configuratieflexibiliteit worden vergroot met name in implementaties met een groot aantal tenants. Hoewel het niet mogelijk is om deze oudere VPZ's die zijn gemaakt in vRealize Automation 8.2 te migreren, zijn er verschillende opties om ze te gebruiken met nieuwere versies van vRealize Automation.

De eerste en meest flexibele optie is om de oude image- en soorttoewijzingen te verwijderen uit de oudere VPZ's en ze opnieuw te configureren met nieuwe toewijzingen die zijn gemaakt op de pagina Tenantbeheer.

- 1 Selecteer **Infrastructuur > Configureren > Virtuele privézones** om de VPZ-pagina te openen.
- 2 Selecteer Imagetoewijzing om de bestaande toewijzing weer te geven.
- 3 Selecteer toewijzingen en klik om ze te verwijderen.
- 4 Selecteer Imagetoewijzing om de bestaande toewijzing weer te geven.
- 5 Selecteer toewijzingen en klik om ze te verwijderen.
- 6 Sluit de VPZ-pagina.
- 7 Selecteer Tenanttoewijzing en maak een algemene toewijzing voor de toepasselijke tenants of maak een tenantspecifieke toewijzing.

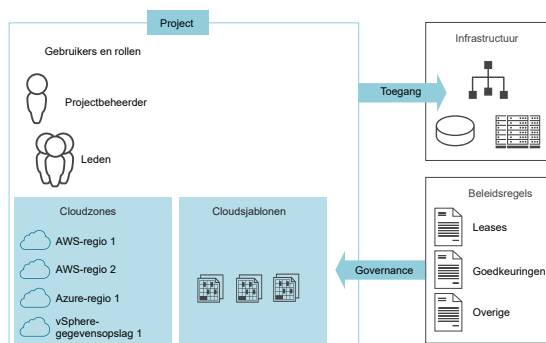
U kunt ook oudere VPZ's gebruiken met nieuwere versies van vRA in hun bestaande configuratie. De oude image- en soorttoewijzingen werken nog steeds zoals geconfigureerd, maar hun configuratieopties zijn alleen-lezen op de VPZ-pagina. Deze opties bieden minder flexibiliteit dan de eerste optie.

Cloud Assembly-projecten toevoegen en beheren

5

Projecten bepalen wie toegang tot Cloud Assembly-cloudsjablonen heeft en waar de sjablonen worden geïmplementeerd. U gebruikt projecten om te organiseren en te bepalen wat uw gebruikers kunnen doen en naar welke cloudzones cloudsjablonen in uw zij cloudinfrastructuur kunnen implementeren.

Cloudbeheerders stellen de projecten in, waaraan zij gebruikers en cloudzones kunnen toevoegen. Iedereen die cloudsjablonen maakt en implementeert, moet lid zijn van ten minste één project.



Dit hoofdstuk omvat de volgende onderwerpen:

- [Hoe voeg ik een project toe voor mijn Cloud Assembly-ontwikkelingsteam](#)
- [Meer informatie over Cloud Assembly-projecten](#)

Hoe voeg ik een project toe voor mijn Cloud Assembly-ontwikkelingsteam

U maakt een project waaraan u leden en cloudzones toevoegt, zodat de projectleden hun cloudsjablonen kunnen implementeren in de gekoppelde zones. Als Cloud Assembly-beheerder maakt u een project voor een ontwikkelingsteam. U kunt vervolgens een projectbeheerder toewijzen of u kunt bewerkingen uitvoeren als projectbeheerder.

Wanneer u een cloudsjabloon maakt, selecteert u het project waaraan u het wilt koppelen. Het project moet bestaan voordat u de cloudsjabloon kunt maken.

Zorg ervoor dat uw projecten de zakelijke behoeften van het ontwikkelingsteam ondersteunen.

- Biedt het project de resources die de doelstellingen van het team ondersteunen? Zie [Tutorial: Infrastructuur en implementaties met meerdere clouds instellen en testen in Cloud Assembly](#) voor een voorbeeld van hoe de infrastructuurresources en een project een cloudsjabloon ondersteunen.
- Hebben uw projectleden vereist of verwacht dat hun implementaties gedeeld of privé zijn? Gedeelde implementaties zijn beschikbaar voor alle projectleden op de pagina Implementaties en niet alleen het implementerende lid. U kunt de status van de delen van de implementatie wijzigen op elk gewenst moment.

Wanneer u de implementatie met projectleden deelt, kunnen de leden dezelfde dag 2-actie uitvoeren. Om de mogelijkheid te beheren van leden om acties van dag 2 uit te voeren, kunt u dag 2-beleidsregels maken in Service Broker. De beleidsregels zijn van toepassing op Cloud Assembly- en Service Broker-implementaties.

Voor meer informatie over de dag 2-beleidsregels raadpleegt u [Hoe kan ik aan implementatiegebruikers rechten verlenen voor dag 2-acties via beleidsregels?](#).

Deze procedure is gebaseerd op het maken van een eerste project dat alleen de basisconfiguraties bevat. Terwijl uw ontwikkelingsteam cloudsjablonen maakt en implementeert, kunt u wijzigingen aanbrengen in het project. U kunt beperkingen, aangepaste eigenschappen en andere opties toevoegen om de implementatie efficiënter te laten werken. Zie de artikelen die beschikbaar zijn in [Meer informatie over Cloud Assembly-projecten](#).

Voorwaarden

- Controleer of u de cloudzones hebt geconfigureerd. Zie [Hoofdstuk 4 Uw Cloud Assembly-resource-infrastructuur maken](#).
- Controleer of u de toewijzingen en profielen hebt geconfigureerd voor de regio's die als cloudzones voor dit project zijn opgenomen. Zie [Hoofdstuk 4 Uw Cloud Assembly-resource-infrastructuur maken](#).
- Controleer of u de nodige rechten hebt om deze taak uit te voeren. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#).
- Bepaal wie u als projectbeheerder wilt aanduiden. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#) voor informatie over wat de projectbeheerder in Cloud Assembly kan doen.
- Als u Active Directory-groepen toevoegt aan projecten, controleert u of u Active Directory-groepen voor uw organisatie hebt geconfigureerd. Zie [Roltoewijzingen voor groepen bewerken in vRealize Automation](#) in *vRealize Automation beheren*. Als de groepen niet zijn gesynchroniseerd, zijn ze niet beschikbaar wanneer u ze probeert toe te voegen aan een project.

Procedure

- 1 Selecteer **Infrastructuur > Beheer > Projecten** en klik op **Nieuw project**.
- 2 Voer de projectnaam in.

3 Klik op het tabblad **Gebruikers**.

- a Om implementaties door projectleden alleen toegankelijk te maken voor de aanvragende gebruiker, schakelt u **Implementatie delen** uit. Om ervoor te zorgen dat u het eigendom van een implementatie kunt toewijzen aan een ander lid van het project, controleert u of **Delen van implementaties** is ingeschakeld.
- b Voeg gebruikers met toegewezen rollen toe.

4 Klik op het tabblad **Inrichting** en voeg een of meer cloudzones toe.

Voeg eventuele cloudzones en virtuele privézones toe die de resources bevatten die de cloudsjablonen ondersteunen die door de projectgebruikers zijn geïmplementeerd.

Voor elke zone kunt u een zoneprioriteit instellen en de hoeveelheid resources beperken die het project kan gebruiken. De mogelijke limieten zijn het aantal instanties, geheugen en CPU's. Alleen voor vSphere-cloudzones kunt u opslaglimieten configureren voor geïmplementeerde resources die zijn gebaseerd op vSphere VM-sjablonen. De opslaglimieten worden geëvalueerd wanneer u een implementatie aanvraagt en wanneer u wijzigingen aanbrengt met behulp van de acties voor het wijzigen van de schijfgrootte, het wijzigen van de opstartschijfgrootte, het verwijderen van de schijf en het bijwerken van het aantal. Deze opslaglimieten zijn niet van toepassing op andere resourcetypen zoals AWS, Microsoft Azure of Google Cloud Platform.

Terwijl u elke zone toevoegt en beperkingen toepast, moet u de projectresources niet zo strikt beperken dat de leden hun cloudsjablonen niet kunnen implementeren.

Wanneer uw gebruikers een implementatieaanvraag indienen, worden de zones geëvalueerd om te bepalen welke zones de resources hebben om de implementatie te ondersteunen. Als meer dan één zone de implementatie ondersteunt, wordt de prioriteit geëvalueerd en wordt de belasting op de toepassing geplaatst met de hoogste prioriteit. Dit is het laagste gehele getal.

5 Als het implementeren van de gevraagde workloads voor dit project langer duurt dan twee uur, voert u een hogere waarde in voor de **time-out**.

De standaardwaarde is twee uur.

6 Klik op **Maken**.

7 Als u uw project wilt testen met de cloudzones van het project, klikt u op **Testconfiguratie** op de pagina Projecten.

De simulatie voert een gestandaardiseerde hypothetische implementatietest uit op de resources voor de cloudzones van het project. Als dit mislukt, kunt u de details controleren en uw resourceconfiguratie corrigeren.

Wat nu te doen

Ga aan de slag met cloudsjablonen. Zie [Hoofdstuk 6 Uw Cloud Assembly-implementaties ontwerpen](#).

Meer informatie over Cloud Assembly-projecten

Projecten zijn de connector tussen cloudsjablonen en resources. Hoe meer u begrijpt over hoe deze werken en hoe u deze voor u kunt laten werken, hoe doeltreffender uw ontwikkelings- en implementatieproces met Cloud Assembly is.

Cloud Assembly-projecttags en aangepaste eigenschappen gebruiken

Als beheerder kunt u governancebeperkingen op projectniveau of aangepaste eigenschappen toevoegen wanneer de vereisten van het project verschillen van de Cloud Assembly-cloudsjablonen. Naast de beperkingstags kunt u ook resourcetags toevoegen die worden toegevoegd aan geïmplementeerde resources tijdens het inrichtingsproces, zodat u de resources kunt beheren.

Wat zijn projectresourcetags?

Een resourcetag voor een project fungeert als een gestandaardiseerde identificatietag die u kunt gebruiken om de geïmplementeerde resources te beheren en om de naleving te waarborgen.

De resourcetags die zijn gedefinieerd in een project worden toegevoegd aan alle onderdeelresources die worden geïmplementeerd als onderdeel van dat project. U kunt dan de standaardtagging gebruiken om de resources te beheren met andere applicaties, bijvoorbeeld om de kosten bij te houden met CloudHealth, en, belangrijk, om naleving van het beleid te garanderen.

Als cloudbeheerder wilt u bijvoorbeeld een applicatie als CloudHealth gebruiken om kosten te beheren. U voegt de tag `costCenter:eu-cc-1234` toe aan een project dat speciaal is bedoeld voor het ontwikkelen van een tool voor personeelszaken van de Europese Unie. Wanneer het projectteam vanuit dit project implementeert, wordt de tag toegevoegd aan de geïmplementeerde resources. Vervolgens configureert u de kostenbeheertool om de resources te identificeren en te beheren die deze tag bevatten. Andere projecten met andere kostencenters zouden alternatieve waarden moeten hebben voor de sleutel.

Wat zijn projectbeperkingstags?

Een projectbeperking fungeert als governance definitie. Het is een `key:value`-tag die definieert welke resources de implementatieaanvraag verbruikt of vermijdt in de cloudzones van het project.

Het implementatieproces zoekt naar tags voor de netwerken en opslag die overeenkomen met de projectbeperkingen, en implementeert op basis van overeenkomstige tags.

De uitbreidbaarheidsbeperking wordt gebruikt om op te geven welke met vRealize Orchestrator geïntegreerde instantie moet worden gebruikt voor uitbreidbaarheidswerkstromen.

Houd rekening met de volgende indelingen wanneer u projectbeperkingen configureert.

- **key:value** en **key:value:hard**. Gebruik deze tag, in een van beide indelingen, wanneer de cloudsjabloon moet worden ingericht op resources met de overeenkomende capaciteitstag. Het implementatieproces mislukt wanneer er geen overeenkomende tag wordt gevonden.

Een cloudsjabloon die door de leden van een project is geïmplementeerd, moet bijvoorbeeld worden ingericht op een netwerk dat PCI-conform is. U gebruikt `security:pci`. Als er geen netwerken worden gevonden in de cloudzones van het project, mislukt de implementatie en worden er geen onveilige implementaties uitgevoerd.

- **key:value:soft**. Gebruik deze tag wanneer u de voorkeur geeft aan een overeenkomende resource, maar u wilt dat het implementatieproces zonder storing wordt voortgezet en de resources kan accepteren waarvan de tag niet overeenkomt. U wilt bijvoorbeeld dat de projectleden hun cloudsjablonen naar een minder dure opslag implementeren, maar u wilt niet dat de opslagbeschikbaarheid de mogelijkheid om te implementeren verstoort. U gebruikt `tier:silver:soft`. Als er geen opslag met de tag `tier:silver` in de cloudzones van het project is, wordt de cloudsjabloon nog steeds op andere opslagresources geïmplementeerd.
- **!key:value**. Gebruik deze tag, met hard of zacht, wanneer u het implementeren op resources met een overeenkomende tag wilt vermijden.

Belangrijk: de beperkingstags van het project hebben een hogere prioriteit dan de beperkingstags van de cloudsjabloon en overschrijven deze tijdens het implementeren. Als u een cloudsjabloon hebt waar dit nooit mag gebeuren, kunt u de `failOnConstraintMergeConflict:true` in de sjabloon gebruiken. Als uw project bijvoorbeeld een netwerkbepkering `loc:london` heeft terwijl de cloudsjabloon `loc:mumbai` is, en niet wilt dat de projectlocatie voorrang heeft, maar wilt dat de implementatie mislukt met een beperkingsconflictbericht, voegt u een eigenschap toe die lijkt op het volgende voorbeeld.

```
constraints:
  - tag: 'loc:mumbai'
failOnConstraintMergeConflict:true
```

Hoe kan ik aangepaste eigenschappen voor het project gebruiken

U kunt een aangepaste projecteigenschap voor rapportage gebruiken om uitbreidbaarheidsacties en werkstromen te activeren en in te vullen, en om de eigenschappen voor het cloudsjabloonniveau te overschrijven.

Door een aangepaste eigenschap aan een implementatie toe te voegen, kunt u de waarde in de gebruikersinterface gebruiken of deze ophalen met behulp van de API, zodat u rapporten kunt genereren.

Uitbreidbaarheid kan ook een aangepaste eigenschap voor een uitbreidbaarheidsabonnement gebruiken. Zie [Levenscycli van applicaties uitbreiden en automatiseren met uitbreidbaarheid](#) voor meer informatie over uitbreidbaarheid.

Een cloudsjabloon kan een bepaalde eigenschapswaarde hebben die u voor een project wilt wijzigen. U kunt een alternatieve naam en waarde opgeven als aangepaste eigenschap.

U kunt ook de eigenschapswaarde versleutelen zodat u en uw gebruikers de waarde die in de implementatie is opgenomen, niet kunnen zien. U kunt bijvoorbeeld een wachtwoord versleutelen dat alle gebruikers in het project gebruiken, maar dat u niet zichtbaar wilt maken. Nadat u de waarde hebt versleuteld en het project hebt opgeslagen, kunt u de waarde niet meer zichtbaar maken of vervangen. Als u het selectievakje **Versleuteld** uitschakelt, wordt de waarde verwijderd. U moet een waarde opnieuw invoeren.

Hoe beïnvloedt het plaatsingsbeleid op projectniveau de toewijzing van resources in vRealize Automation

Als beheerder kunt u plaatsingsbeleid definiëren voor projecten waarbij meerdere cloudzones in aanmerking komen als doelzone van de implementatie. U kunt bijvoorbeeld een project hebben waarin u cloudsjablonen wilt implementeren op basis van de prioriteit die u instelt. Of mogelijk wilt u de geïmplementeerde resources verdelen over meerdere zones op basis van de beste verhouding tussen VM en host.

Overwegingen bij toewijzingen

Voor een standaard- of verspreid plaatsingsbeleid.

- Als de implementerende gebruiker rechten heeft om cloudaccounts te beheren die zich in de onderhoudsmodus bevinden, kan het toewijzingsproces een cloudaccount selecteren dat zich in de onderhoudsmodus bevindt omdat de gebruiker mogelijk een testimplementatie moet uitvoeren voordat het onderhoudsvenster wordt gesloten.
- Als de gebruiker geen rechten heeft om cloudaccounts te beheren, worden de cloudaccounts die zich in de onderhoudsmodus bevinden, uit het toewijzingsproces gefilterd.
- Hosts die zich in de onderhoudsmodus bevinden, worden meegeteld in de verspreide verhouding. Om een host in onderhoud uit te sluiten van de verhoudingsberekening, moet u de energiestatus instellen op uit.

Voor een verspreid beleid.

- Verhoudingen worden berekend op basis van hosts. De hosts kunnen standalone zijn of deel uitmaken van een cluster.
- Als een standalone host wordt uitgeschakeld, wordt deze niet meegeteld in de verhouding.
- Als een host die deel uitmaakt van een cluster wordt uitgeschakeld, wordt de uitgeschakelde status niet doorgevoerd in het cluster en wordt de host nog steeds beschouwd bij het berekenen van de verhouding.

Het plaatsingsbeleid instellen

Als er voor een project meerdere gelijkwaardige cloudzones in aanmerking komen als doel voor een implementatie, wordt de plaatsing tijdens de implementatieaanvraag vastgesteld op basis van het **plaatsingsbeleid** dat u hebt geconfigureerd.

- 1 Selecteer **Infrastructuur > Projecten** en maak of selecteer een project.
- 2 Klik in het project op het tabblad **Inrichting**.

3 Selecteer een beleid.

Plaatsingsbeleid	Beschrijving
Standaard	<p>Implementeert de aangevraagde resources in de eerste cloudzone die voldoet aan de vereisten.</p> <p>Selecteer Standaard wanneer u de workloads op volgorde van prioriteit wilt implementeren en u het geen probleem vindt dat alle resources op een host worden gebruikt.</p> <p>Als deze optie is geselecteerd, worden er geen waarden voor VM en Hosts opgehaald.</p>
Verspreid	<p>Implementeert de aangevraagde resources in de cloudzone met het kleinste aantal virtuele machines per host.</p> <p>Selecteer Verspreid wanneer u de workloads over hosts wilt distribueren en resources algemeen over hosts wilt verdelen.</p> <p>Als deze optie is geselecteerd, wordt het aantal VM's en hosts opgehaald uit de resources van de cloudzone en vervolgens geëvalueerd.</p>

4 Klik op **Opslaan**.**Controleren hoe het beleid wordt toegepast**

Nadat u het plaatsingsbeleid op projectniveau hebt geconfigureerd, kunt u in een inrichtingsdiagram zien waar het systeem de cloudsjabloon wil implementeren.

- 1 Selecteer **Ontwerp > Cloudsjablonen** en selecteer of configureer een sjabloon die het project gebruikt waarvoor u een beleid hebt geselecteerd.
- 2 Klik op **Test**.
- 3 Wanneer de test is voltooid, klikt u op **Inrichtingsdiagram** in de testresultaten.

4 Het diagram ziet er ongeveer uit zoals in de volgende twee voorbeelden.

Beleidstype

Inrichtingsdiagram

Standaard



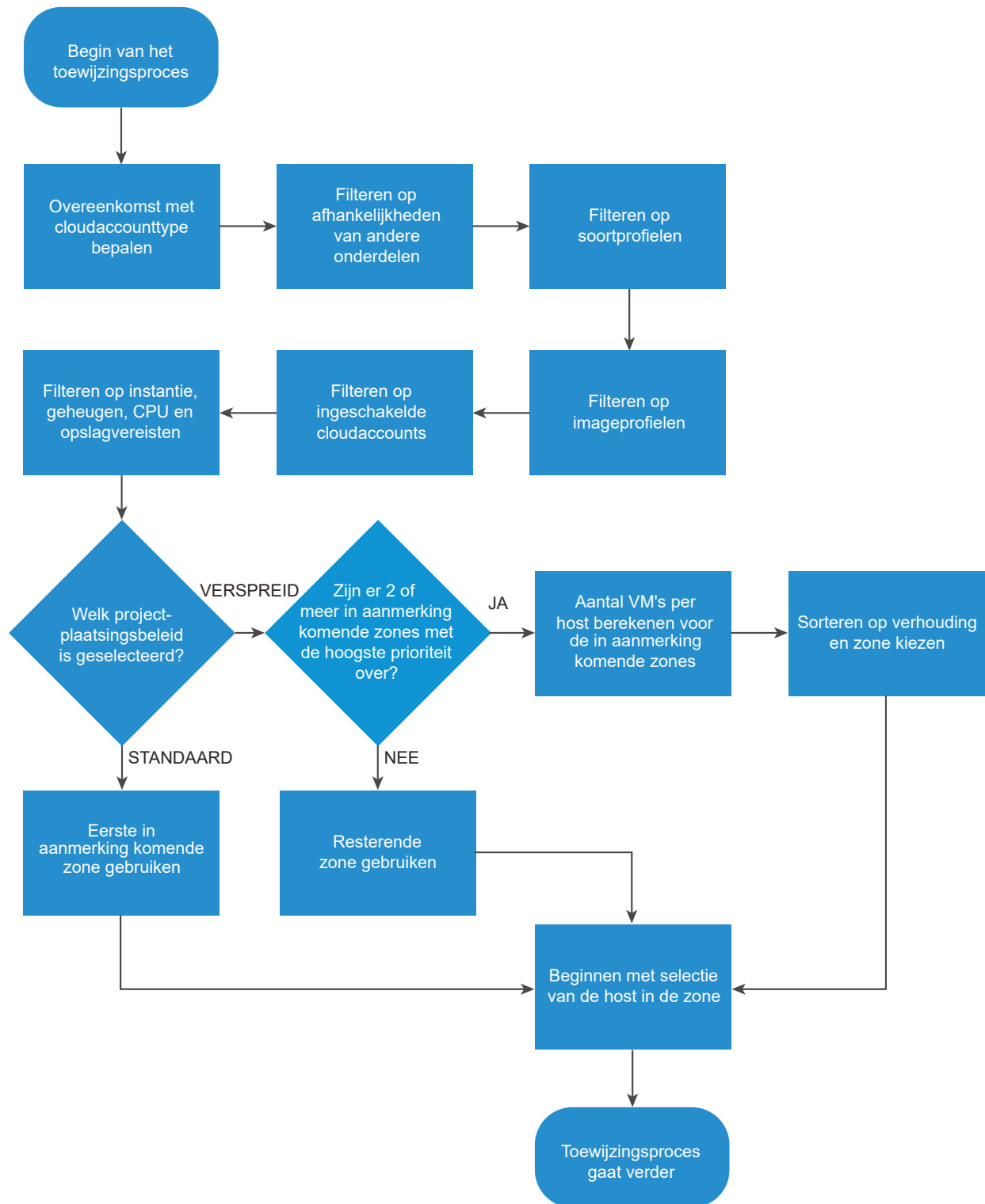
Verspreid



- 5 Als u klaar bent om te implementeren, gaat u terug naar de cloudsjabloon en klikt u op **Implementeren**.

Evaluatie van het plaatsingsbeleid tijdens het toewijzingsproces

Het volgende diagram laat zien wanneer het beleid wordt geëvalueerd tijdens het toewijzingsproces en wanneer de doelzone en host worden geïdentificeerd.



Wat zijn de projectkosten in Cloud Assembly

De kosten die beschikbaar zijn in uw Cloud Assembly-projecten, helpen u bij het beheren van de resourcekosten die aan volledige projecten zijn verbonden. Het project bevat ook de afzonderlijke implementatiekosten.

Ansible-Project DELETE

Summary Users Provisioning Kubernetes Provisioning **Price** Integrations

Price Analysis **\$10.81**
Month to date (private cloud only)

Deployment Name	Description	Requestor	Created On	Expiring In	Price
AnsibleTower-Demo		skuradmutti@vmware.com	Jan 26, 2021	Never expires	\$3.07
Check-Delete		krishanw@vmware.com	Jan 18, 2021	Never expires	\$3.04
Ansible vSphere		skuradmutti@vmware.com	Jan 19, 2021	Never expires	\$3.01
WT with 2 machines		gsumonv@vmware.com	Feb 14, 2021	Never expires	\$0.61
Create with templates		gsumonv@vmware.com	Feb 14, 2021	Never expires	\$0.32
Ansible		skuradmutti@vmware.com	Jan 07, 2021	Never expires	\$0.31
Create with job templates		gsumonv@vmware.com	Feb 14, 2021	Never expires	\$0.31

7 deployments

SAVE CANCEL

De kosteninformatie die u voor een project en voor de afzonderlijke implementaties ziet, wordt weergegeven nadat ten minste één implementatie is ingericht die aan het project is gekoppeld. De kosten worden dagelijks berekend en bijgewerkt, zodat u de kosten van een implementatie in de loop van de tijd kunt bijhouden. De initiële waarden zijn gebaseerd op benchmarks uit de sector.

Cloudbeheerders kunnen de waarden aanpassen om de werkelijke kosten weer te geven.

Zie [Prijskaarten gebruiken in vRealize Automation](#) voor meer informatie.

Hoe werken Cloud Assembly-projecten tijdens het implementeren

Projecten regelen de toegang van gebruikers tot de cloudzones en gebruikerseigendom van de ingerichte resources. Of u een cloudbeheerder of een cloudsjabloonontwikkelaar bent, u moet begrijpen hoe de projecten tijdens het implementeren werken, zodat u uw implementaties kunt beheren en eventuele problemen kunt oplossen.

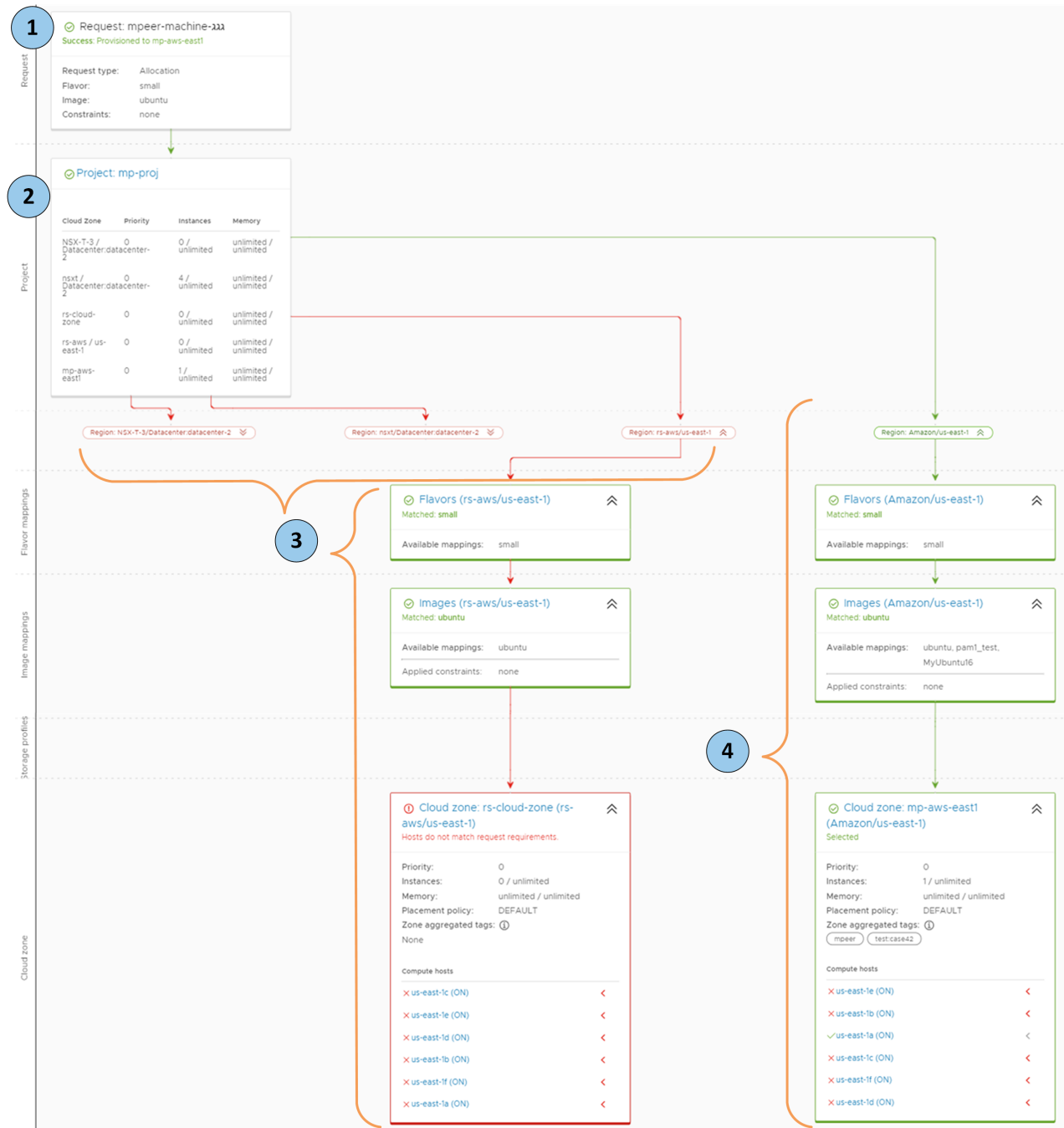
Als cloudbeheerder die projecten voor verschillende teams instelt, moet u begrijpen hoe projecten bepalen waar cloudsjabloononderdelen worden geïmplementeerd. Dit inzicht helpt u bij het maken van projecten die cloudsjabloonontwikkelaars ondersteunen, en bij het oplossen van mislukte implementaties.

Wanneer u een cloudsjabloon maakt, koppelt u deze eerst aan een project. Tijdens het implementeren worden de vereisten voor de cloudsjabloon geëvalueerd ten opzichte van de cloudzones van het project om de beste locatie voor de implementatie te vinden.

In de volgende werkstroom wordt het proces geïllustreerd.

- 1 U moet een implementatieaanvraag voor een cloudsjabloon verzenden.
- 2 Het project evalueert de sjabloon- en projectvereisten, zoals soort, image en beperkingstags. De vereisten worden vergeleken met de cloudzones van het project om een zone te zoeken die de vereisten ondersteunt.
- 3 Deze zones hadden geen resources om de aanvraag te ondersteunen.

- 4 Deze cloudzone ondersteunt de aanvraagvereisten en de sjabloon wordt in deze accountregio van de cloudzone geïmplementeerd.



Uw Cloud Assembly- implementaties ontwerpen

6

Cloudsjablonen (voorheen blueprints genoemd) vormen het beginpunt van een implementatie en bestaan uit versleutelde specificaties die de machines, applicaties en services definiëren die u in cloudresources maakt met Cloud Assembly.

Hoe cloudsjablonen werken

Sjablonen kunnen gericht zijn op specifieke cloudleveranciers maar ook cloudonafhankelijk zijn. De cloudzones die aan uw project worden toegewezen, bepalen welke aanpak u volgt. Neem contact op met uw cloudbeheerder om er zeker van te zijn dat u weet uit welk type resources uw cloudzones zijn samengesteld.

Het maken van Cloud Assembly-sjablonen is een proces van programmeerbare infrastructuur. U begint met het toevoegen van resources aan het ontwerpcanvas. Vervolgens gebruikt u de code-editor om de details in te vullen. Met de code-editor kunt u direct code typen of waarden in een formulier invoeren.

Voordat u een cloudsjabloon maakt

U kunt op elk gewenst moment een Cloud Assembly-sjabloon maken. Om de sjabloon te implementeren, moet u echter eerst de infrastructuur van uw cloudresource [Hoofdstuk 4 Uw Cloud Assembly-resource-infrastructuur maken](#) en [Hoofdstuk 5 Cloud Assembly-projecten toevoegen en beheren](#) dat die infrastructuur bevat.

Klaar om te ontwerpen?

Bekijk het navigatiemenu aan de linkerkant of ga rechtstreeks naar onderwerpen in de volgende tabel.

Aan de slag	Meer informatie over cloudsjabloonontwerpen en bijbehorende functies		Meer voorbeelden
Aan de slag met Cloud Assembly-ontwerpen	Gebruikersinvoer in vRealize Automation-aanvragen	Cloud Assembly-resourcevlaggen voor aanvragen	Voorbeeld van een gedocumenteerde Cloud Assembly-sjabloon
Bindingen en afhankelijkheden maken tussen resources in Cloud Assembly	Aangepaste naamgeving voor geïmplementeerde resources in Cloud Assembly	Cloud Assembly-expressies	Voorbeelden van vSphere-resources in Cloud Assembly
Versies van uw Cloud Assembly-sjablonen maken	Een groep eigenschappen in Cloud Assembly hergebruiken	Geheime Cloud Assembly-eigenschappen	Meer informatie over netwerkresources in vRealize Automation-cloudsjablonen
Andere manieren om Cloud Assembly-sjablonen te maken	Externe toegang tot een Cloud Assembly-implementatie	Machine-initialisatie in Cloud Assembly	Meer informatie over beveiligingsgroep- en tagresources in vRealize Automation-cloudsjablonen
Hulp bij het voltooien van code in Cloud Assembly	Statische IP-adressen van vSphere in Cloud Assembly	Terraform-configuraties in Cloud Assembly	Meer informatie over load-balancerresources in vRealize Automation-cloudsjablonen
	Machine- en schijfclusters in Cloud Assembly	SCSI-schijfplaatsing met Cloud Assembly	Voorbeelden van cloudsjabloon voor vCenter Puppet-configuratie
	Typen aangepaste resources voor Cloud Assembly-cloudsjablonen	Levenscycli van applicaties uitbreiden en automatiseren met uitbreidbaarheid	

Dit hoofdstuk omvat de volgende onderwerpen:

- [Aan de slag met Cloud Assembly-ontwerpen](#)
- [Hulp bij het voltooien van code in Cloud Assembly](#)
- [Bindingen en afhankelijkheden maken tussen resources in Cloud Assembly](#)
- [Versies van uw Cloud Assembly-sjablonen maken](#)
- [Gebruikersinvoer in vRealize Automation-aanvragen](#)
- [Een groep eigenschappen in Cloud Assembly hergebruiken](#)
- [Cloud Assembly-resourcevlaggen voor aanvragen](#)
- [Cloud Assembly-expressies](#)
- [Geheime Cloud Assembly-eigenschappen](#)
- [Externe toegang tot een Cloud Assembly-implementatie](#)
- [SCSI-schijfplaatsing met Cloud Assembly](#)
- [Machine-initialisatie in Cloud Assembly](#)

- Machine- en schijfclusters in Cloud Assembly
- Aangepaste naamgeving voor geïmplementeerde resources in Cloud Assembly
- De SaltStack Config-resource toevoegen aan Cloud Assembly-ontwerpen
- Terraform-configuraties in Cloud Assembly
- Typen aangepaste resources voor Cloud Assembly-cloudsjablonen
- Cloud Assembly-ontwerpen als voorbereiding op wijzigingen voor dag 2
- Meer voorbeelden van Cloud Assembly-code
- vRealize Automation-schema met eigenschappen voor aangepaste resources
- Andere manieren om Cloud Assembly-sjablonen te maken
- Levenscycli van applicaties uitbreiden en automatiseren met uitbreidbaarheid

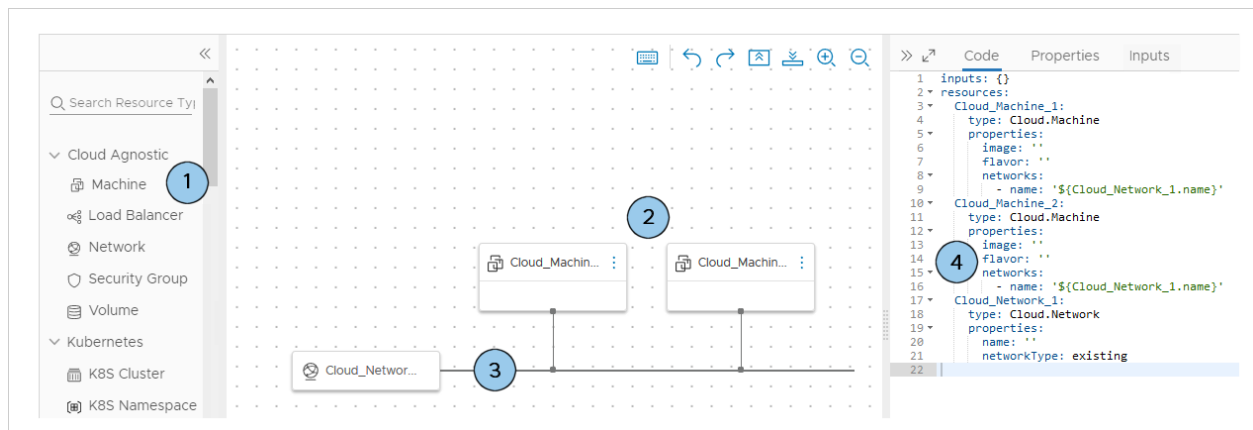
Aan de slag met Cloud Assembly-ontwerpen

U gebruikt de ontwerppagina om Cloud Assembly-sjabloonspecificaties te maken voor de machines en toepassingen die u wilt inrichten.

De ontwerppagina gebruiken

Als u een nieuwe cloudsjabloon wilt maken, gaat u naar **Ontwerp > Cloudsjablonen**. Klik vervolgens op **Nieuw van > Leeg canvas**.

- 1 Zoek resources.
- 2 Sleep resources naar het canvas.
- 3 Verbind resources.
- 4 Configureer resources door de cloudsjablooncode te bewerken.



Selecteer de gewenste resources en sleep deze naar het canvas.

De beschikbare resources worden links op de ontwerppagina weergegeven.

Cloudfanafhankelijke resources	U kunt cloudfanafhankelijke resources naar elke cloudfleverancier implementeren. Tijdens het inrichten worden in de implementatie cloudfspecifieke resources gebruikt die overeenkomen. Als u bijvoorbeeld verwacht dat een cloudfjabloon voor zowel AWS- als vSphere-cloudfzones wordt geïmplementeerd, gebruikt u cloudfanafhankelijke resources.
Cloudfleveranciersresources	Leveranciersresources, zoals specifieke resources voor Amazon Web Services, Microsoft Azure, Google Cloud Platform of VMware vSphere, kunnen alleen worden geïmplementeerd in overeenkomende AWS-, Azure-, GCP- of vSphere-cloudfzones. U kunt cloudfanafhankelijke resources toevoegen aan een cloudfjabloon die cloudfspecifieke resources voor een bepaalde leverancier bevat. Houd er rekening mee wat de cloudfzones van het project in termen van de leverancier ondersteunen.
Resources voor configuratiebeheer	Resources voor configuratiebeheer zijn afhankelijk van uw geïntegreerde applicaties. Een Puppet-resource kan bijvoorbeeld de configuratie van de andere resources controleren en afdwingen.

Resources verbinden

Gebruik de grafische besturingselementen van het Cloud Assembly-ontwerpcanvas om de resources met elkaar te verbinden.

Alleen compatibele resources kunnen met elkaar worden verbonden. Bijvoorbeeld:

- Een load balancer verbinden met een cluster van machines.
- Een machine verbinden met een netwerk.
- Externe opslag verbinden met een machine.

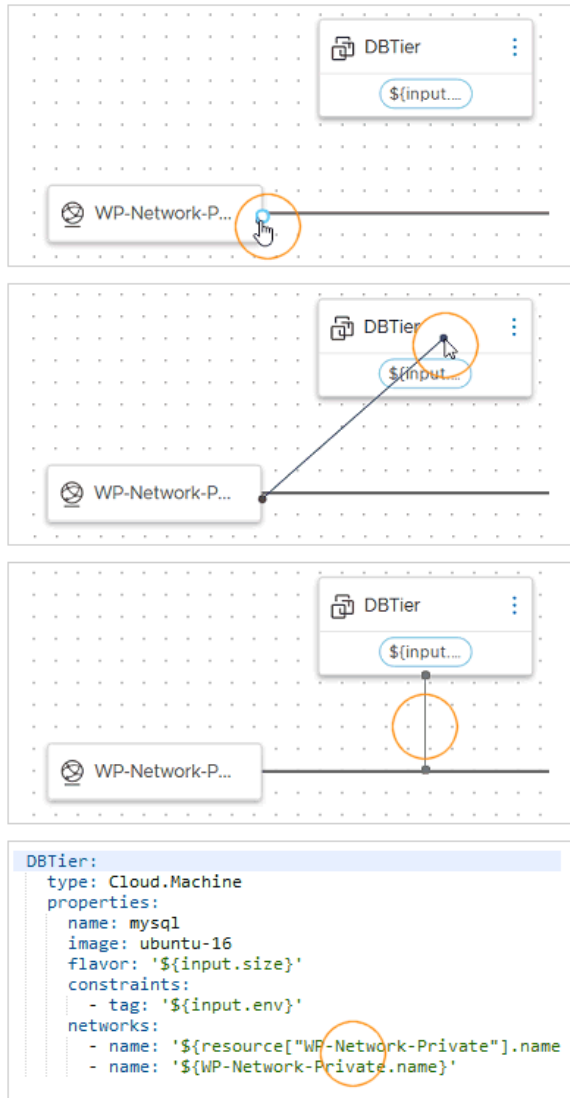
Belangrijk Voor een connector met ononderbroken lijn moeten de twee resources in dezelfde cloudfzone zijn geïmplementeerd. Als u conflicterende beperkingen aan de resources toevoegt, kan de implementatie mislukken.

U kunt bijvoorbeeld geen verbonden resources implementeren waar beperkingstags de plaatsing van één resource in een zone in us-west-1 en de andere resource in een zone in us-east-1 afdwingen.

Ononderbroken of onderbroken pijlen geven alleen een afhankelijkheid aan, geen verbinding. Zie [Bindingen en afhankelijkheden maken tussen resources in Cloud Assembly](#) voor meer informatie over afhankelijkheden.

Als u een verbinding wilt maken, moet u de rand van een resource aanwijzen om de verbindingsballon weer te geven. Klik vervolgens op de ballon, sleep deze naar de doelresource en laat deze vervolgens los.

In de code-editor wordt extra code voor de bronresource weergegeven in de doelresourcecode.



In de afbeelding zijn de SQL-machine en het privénetwerk verbonden en dus moeten ze in dezelfde cloudzone zijn geïmplementeerd.

Cloudsjablooncode bewerken

Met de code-editor kunt u code direct typen, knippen, kopiëren en plakken. Als u zich niet prettig voelt bij het bewerken van code, selecteert u een resource in het ontwerpcanvas, klikt u op het tabblad **Eigenschappen** van de code-editor en voert u daar waarden in. De eigenschapswaarden die u invoert, worden in de code weergegeven, alsof u ze direct heeft ingevoerd.

The screenshot displays the vRealize Automation Cloud Assembly interface. On the left is a code editor showing a JSON-like configuration for a 'WebTier' resource. On the right is a 'Properties' form with tabs for 'Code', 'Properties', and 'Inputs'. The 'Properties' tab is active, showing various configuration fields.

Code Editor (Left):

```
WebTier:
  type: Cloud.Machine
  properties:
    name: wordpress
    flavor: '${input.size}'
    image: ubuntu
    count: '${input.count}'
    constraints:
      - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
        assignPublicIpAddress: true
    storage:
      disks:
        - capacityGb: '${input.archiveDiskSize}'
          name: ArchiveDisk
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all

  packages:
    - apache2
    - php
    - php-mysql
    - libapache2-mod-php
```

Properties Form (Right):

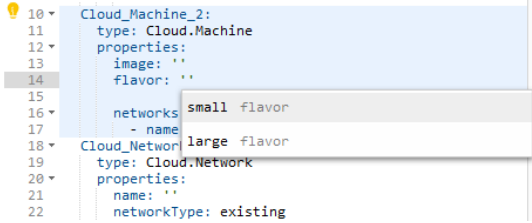
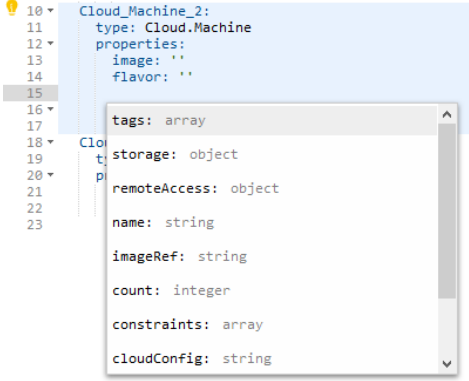
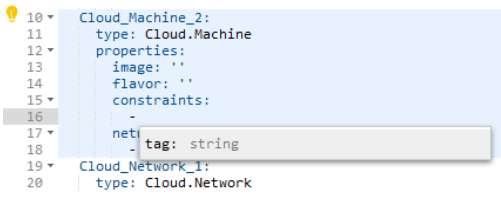
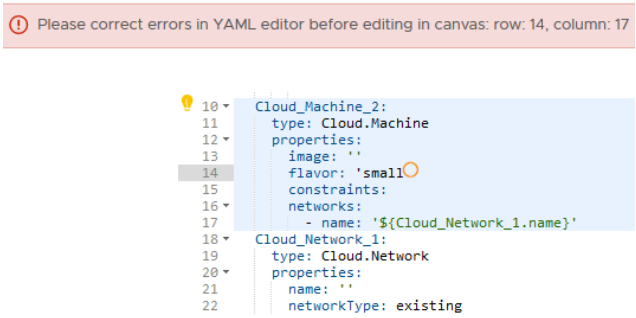
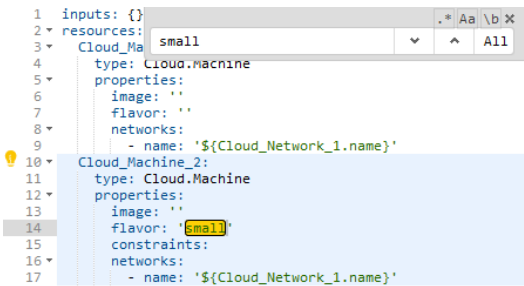
- Count:** "\${input.count}"
- Image Type:** ubuntu
- Flavor *:** \${input.size}
- Storage:**
- Constraints:**
 - Tag: []
- Maximum Capacity of the disk in GB:** 1
- Size of boot disk in GB:** 1
- Networks:**

Merk op dat u code uit een cloudsjabloon kunt kopiëren en in een andere kunt plakken.

Hulp bij het voltooien van code in Cloud Assembly

Door Cloud Assembly-resources toe te voegen en deze op het canvas te verbinden, wordt alleen een startcode gemaakt. Als u deze volledig wilt configureren, moet u de code bewerken.

Met de code-editor kunt u direct code typen of eigenschapswaarden in een formulier invoeren. De Cloud Assembly-editor biedt syntaxisvoltooiings- en foutcontrolefuncties om u te helpen bij het direct maken van code.

Hints voor editor	Voorbeeld
Beschikbare waarden	
Toegestane eigenschappen	
Onderliggende eigenschappen	
Syntaxfouten	
Ctrl+F om te zoeken	

Hints voor editor	Voorbeeld
Optionele parameter s	<pre> 1 inputs: {} 2 resources: 3 Cloud_Machine_1: 4 type: Cloud.Machine 5 properties: 6 image: '' 7 flavor: '' 8 networks: 9 - name: '\${Cloud_Network_1.name}' 10 Cloud_Machine_2: 11 type: Cloud.Machine 12 properties: 13 image: '' 14 flavor: 'small' 15 constraints: 16 networks: 17 - name: '\${Cloud_Network_1.name}' </pre>

Help bij
schema

Voor alle aangepaste eigenschappen kunt u ook [vRealize Automation Resource Type Schema op VMware {code}](#) raadplegen.

```

cloudConfig
Type string

When provisioning an instance, machine
cloud-init startup instructions from user data
fields. Sample cloud config instructions:

#cloud-config
repo_update: true
repo_upgrade: all
packages:
- httpd
- db-server

runcmd:
- [ sh, -c, "amazon-linux-extras insta
- systemctl start httpd
- sudo systemctl enable httpd

cloudConfig:
  repo_update: true
  repo_upgrade: all

  packages:
    - mysql-server

  runcmd:
    - sed -e '/bind-address/ s/^#/#/' -i
    - service mysql restart
    - mysql -e "GRANT ALL PRIVILEGES ON *.
    - mysql -e "FLUSH PRIVILEGES;"

attachedDisks: []

```

Bindingen en afhankelijkheden maken tussen resources in Cloud Assembly

Wanneer u een Cloud Assembly-sjabloon implementeert, vereist een resource mogelijk dat eerst een andere resource beschikbaar is.

Belangrijk Pijlen geven alleen een afhankelijkheid aan, geen verbinding. Zie [Aan de slag met Cloud Assembly-ontwerpen](#) om resources te verbinden zodat ze communiceren.

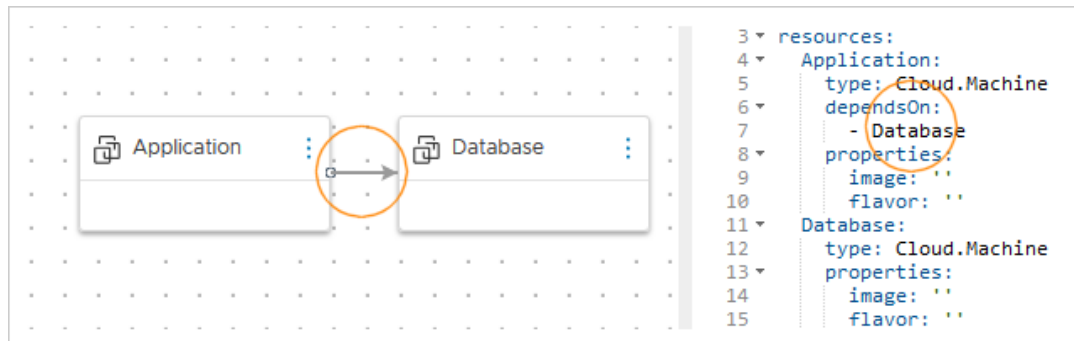
Expliciete afhankelijkheden

Soms vereist een resource dat een andere resource eerder wordt geïmplementeerd. Er moet bijvoorbeeld eerst een databaseserver bestaan, voordat een applicatieserver kan worden gemaakt en geconfigureerd om er toegang toe te krijgen.

Met een expliciete afhankelijkheid wordt de samenstellingsvolgorde tijdens het implementeren ingesteld, of voor de acties voor in- of uitschalen. U kunt een expliciete afhankelijkheid toevoegen met behulp van het grafische ontwerpcanvas of de code-editor.

- Ontwerpcanvasoptie — teken een verbinding die begint bij de afhankelijke resource en eindigt bij de resource die eerst moet worden geïmplementeerd.
- Code-editoroptie — voeg de eigenschap `dependsOn` toe aan de afhankelijke resource en identificeer de resource die eerst moet worden geïmplementeerd.

Een expliciete afhankelijkheid maakt een ononderbroken pijl in het canvas.



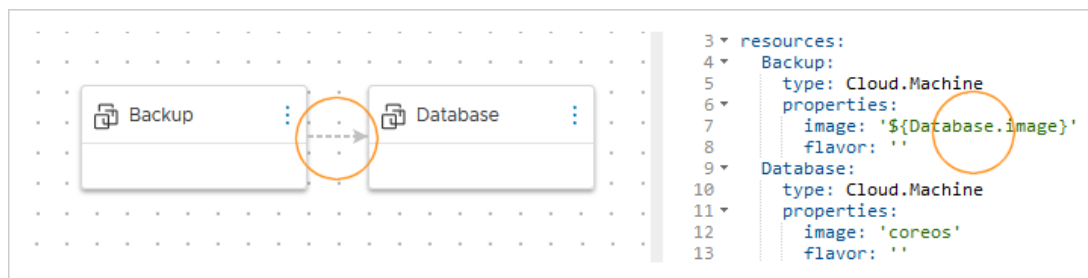
Eigenschapsbindingen

Soms heeft een resource-eigenschap een waarde nodig die in de eigenschap van een andere resource kan worden gevonden. Een back-upserver heeft bijvoorbeeld mogelijk de besturingssysteemimage van de databaseserver nodig waarvan een back-up wordt gemaakt. Dus moet de databaseserver eerst bestaan.

Een eigenschapsbinding of impliciete afhankelijkheid bepaalt de aanmaakvolgorde door te wachten tot de vereiste eigenschap beschikbaar is voordat de afhankelijke resource wordt geïmplementeerd. U voegt een eigenschapsbinding toe met behulp van de code-editor.

- Bewerk de afhankelijke resource en voeg een eigenschap toe die de resource en de eigenschap identificeert die eerst moeten bestaan.

Een eigenschapsbinding is te herkennen aan een onderbroken pijl in het canvas.



Versies van uw Cloud Assembly-sjablonen maken

Als cloudsjabloonontwikkelaar kunt u veilig een momentopname van een werkend ontwerp vastleggen voordat verdere wijzigingen worden aangebracht.

Tijdens het implementeren kunt u elk van uw versies selecteren om te implementeren.

Een versie van een cloudsjabloon vastleggen

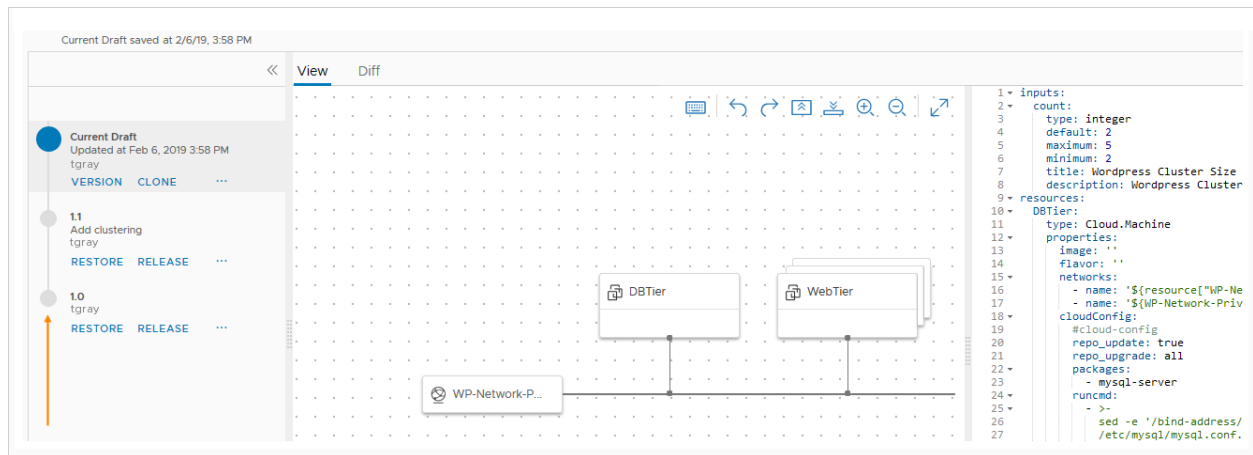
Klik op de ontwerppagina op **Versie** en geef een naam op.

De naam moet alfanumeriek zijn, zonder spaties, en alleen punten, afbreekstreepjes en onderstrepingstekens zijn als speciale tekens toegestaan.

Een oudere versie herstellen

Klik op de ontwerppagina op **Versiegeschiedenis**.

Selecteer aan de linkerkant een oudere versie om deze te controleren op het canvas en in de code-editor. Wanneer u de gewenste versie hebt gevonden, klikt u op **Herstellen**. Bij het herstellen wordt het huidige concept overschreven zonder dat er benoemde versies worden verwijderd.



Een versie vrijgeven aan Service Broker

Klik op de ontwerppagina op **Versiegeschiedenis**.

Selecteer aan de linkerkant een versie en geef deze vrij.

U kunt het huidige concept pas vrijgeven nadat u er een versie van hebt gemaakt.

De versie opnieuw importeren in Service Broker

Als u de nieuwe versie voor catalogusgebruikers wilt inschakelen, moet u deze opnieuw importeren.

Ga in Service Broker naar **Inhoud en beleidsregels > Inhoudsbronnen**.

Klik in de lijst met bronnen op de bron voor het project dat de cloudsjabloon met de nieuwe vrijgegeven versie bevat.

Klik op **Opslaan en importeren**.

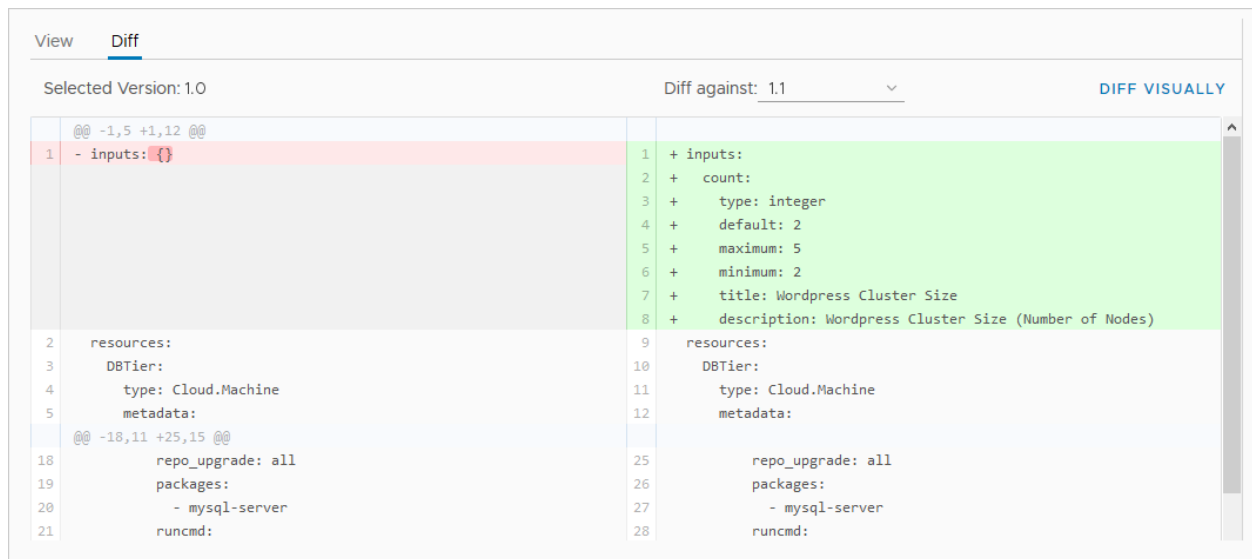
Cloudsjabloonversies vergelijken

Wanneer er wijzigingen en versies worden verzameld, wilt u mogelijk de verschillen tussen de items identificeren.

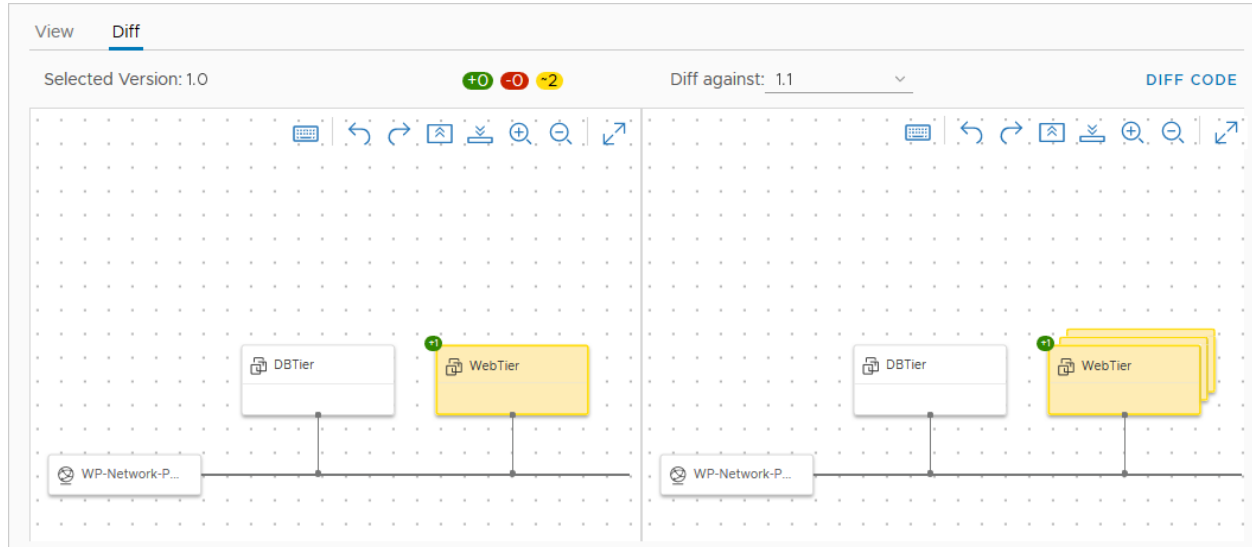
Selecteer in de weergave Versiegeschiedenis van Cloud Assembly een versie en klik op **Diff**. Selecteer vervolgens in de vervolgkeuzelijst **Diff met** een andere versie om mee te vergelijken.

U kunt schakelen tussen het bekijken van codeverschillen of visuele topologieverschillen.

Figuur 6-1. Codeverschillen



Figuur 6-2. Visuele topologieverschillen



Een cloudsjabloon klonen

Hoewel het niet hetzelfde is als het opslaan van een versie, kunt u op de ontwerppagina **Acties** > **Klonen** selecteren om een kopie van de huidige sjabloon voor alternatieve ontwikkeling te maken.

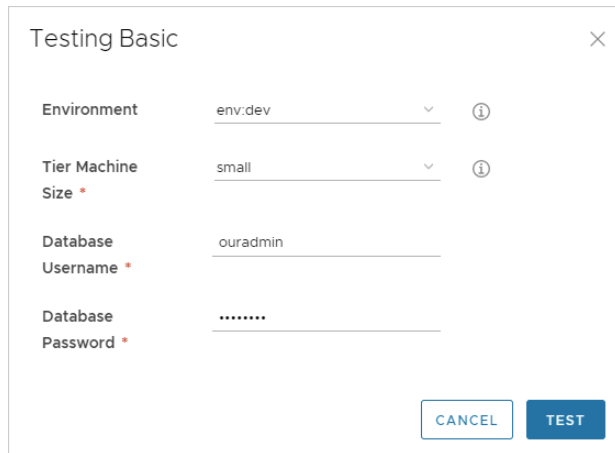
Gebruikersinvoer in vRealize Automation-aanvragen

Als cloudsjabloonontwikkelaar gebruikt u invoerparameters zodat gebruikers aangepaste keuzes kunnen maken op het moment van de aanvraag.

Hoe invoer werkt

Wanneer gebruikers invoer opgeven, hoeft u niet langer meerdere kopieën van sjablonen op te slaan die slechts een beetje verschillen. Daarnaast kunt u met invoer een sjabloon voorbereiden voor bewerkingen voor dag 2. Zie [Cloudsjablooninvoer voor vRealize Automation-updates voor dag 2 gebruiken](#).

De volgende invoer toont hoe u één cloudsjabloon voor een MySQL-databaseserver maakt, waarbij gebruikers die ene sjabloon in verschillende cloudresourceomgevingen kunnen implementeren en elke keer een andere capaciteit en andere verificatiegegevens toepassen.



The image shows a 'Testing Basic' dialog box with a close button (X) in the top right corner. It contains four input fields: 'Environment' with a dropdown menu showing 'env:dev', 'Tier Machine Size' with a dropdown menu showing 'small', 'Database Username' with a text field containing 'ouradmin', and 'Database Password' with a masked text field showing seven dots. Each dropdown menu has an information icon (i) to its right. At the bottom right, there are two buttons: 'CANCEL' and 'TEST'.

Invoerparameters toevoegen

Voeg het gedeelte `inputs` toe aan uw sjablooncode, waar u de gewenste waarden instelt.

In het volgende voorbeeld kunnen de machinegrootte, het besturingssysteem en het aantal geclusterde servers worden geselecteerd.

```
inputs:
  wp-size:
    type: string
    enum:
      - small
      - medium
    description: Size of Nodes
    title: Node Size
  wp-image:
    type: string
    enum:
      - coreos
      - ubuntu
    title: Select Image/OS
  wp-count:
    type: integer
    default: 2
    maximum: 5
    minimum: 2
    title: Wordpress Cluster Size
    description: Wordpress Cluster Size (Number of nodes)
```

Als u niet voldoende vertrouwd bent om uw code te bewerken, klikt u op het tabblad **Invoer** van de code-editor en voert u daar instellingen in. Het volgende voorbeeld toont invoer voor de MySQL-database die eerder is vermeld.

Cloud Template Inputs

+ NEW EDIT DELETE

<input type="checkbox"/>	Name	Title	Type	Default Value
<input type="checkbox"/>	size	Tier Machine Size	string	
<input type="checkbox"/>	username	Database Username	string	
<input type="checkbox"/>	userpassword	Database Password	string	****
<input type="checkbox"/>	databaseDiskSize	MySQL Data Disk Size	number	4

Edit Cloud Template Input: size

Name *

Title

Description

Type

Encrypted ☐

Verwijzen naar invoerparameters

Vervolgens verwijst u in de sectie `resources` naar een invoerparameter met de syntaxis `${input.property-name}`.

Als de naam van een eigenschap een spatie bevat, moet u deze markeren met vierkante haakjes en dubbele aanhalingstekens in plaats van de puntnotatie te gebruiken: `${input["property name"]}`

Belangrijk In de cloudsjablooncode kunt u het woord `input` niet gebruiken om een invoerparameter aan te duiden.

```
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      flavor: '${input.wp-size}'
      image: '${input.wp-image}'
      count: '${input.wp-count}'
```

Optionele invoer

Invoer is doorgaans vereist en gemarkeerd met een asterisk. Als u invoer optioneel wilt maken, stelt u een lege standaardwaarde in, zoals weergegeven.

```
owner:
  type: string
  minLength: 0
  maxLength: 30
  title: Owner Name
  description: Account Owner
  default: ''
```

The screenshot shows a 'Testing Basic' dialog box with the following fields and values:

- Environment:** env:dev
- Tier Machine Size:** small
- Owner Name:** (empty, highlighted with an orange arrow)
- Database Username:** ouradmin
- Database Password:** (masked with dots)

Buttons at the bottom: CANCEL, TEST.

Lijst met invoereigenschappen

Eigenschap	Beschrijving
const	Wordt gebruikt met oneOf. De werkelijke waarde die aan de beschrijvende titel is gekoppeld.
default	Vooraf ingevulde waarde voor de invoer. De standaardwaarde moet van het juiste type zijn. Voer niet een woord in als standaardwaarde voor een geheel getal.
description	Helptekst voor de gebruiker voor de invoer.
encrypted	Of de invoer van de gebruiker moet worden versleuteld, waar of onwaar. Wachtwoorden worden doorgaans versleuteld. U kunt ook versleutelde eigenschappen maken die herbruikbaar zijn in meerdere cloudsjablonen. Zie Geheime Cloud Assembly-eigenschappen .

Eigenschap	Beschrijving
enum	<p>Een vervolgkeuzelijst met toegestane waarden.</p> <p>Gebruik het volgende voorbeeld als richtlijn voor de opmaak.</p> <pre>enum: - value 1 - value 2</pre>
format	<p>Stelt de verwachte notatie voor de invoer in. Bijvoorbeeld: (25/04/19) ondersteunt datum/tijd.</p> <p>Staat het gebruik van de datumkiezer in aangepaste formulieren van Service Broker toe.</p>
items	Geeft items in een array aan. Ondersteunt getal, geheel getal, tekenreeks, Booleaans of object.
maxItems	Maximum aantal selecteerbare items in een array.
maxLength	<p>Maximum aantal tekens dat is toegestaan voor een tekenreeks.</p> <p>Als u bijvoorbeeld een veld wilt beperken tot 25 tekens, voert u <code>maxLength: 25</code> in.</p>
maximum	De grootste toegestane waarde voor een getal of geheel getal.
minItems	Minimum aantal items dat in een array kan worden geselecteerd.
minLength	Minimum aantal tekens dat voor een tekenreeks is toegestaan.
minimum	De kleinste toegestane waarde voor een getal of geheel getal.
oneOf	<p>Staat toe dat het formulier voor gebruikersinvoer een beschrijvende naam (titel) voor een minder gebruiksvriendelijke waarde (const) weergeeft. Als u een standaardwaarde instelt, stelt u <code>const</code> in, niet de titel.</p> <p>Geldig voor gebruik met de typen tekenreeks, geheel getal en getal.</p>
pattern	<p>Toegestane tekens voor invoer van een tekenreeks, in de syntax van reguliere expressies.</p> <p>Bijvoorbeeld: <code>'[a-z]+'</code> of <code>'[a-z0-9A-Z@#]+\$'</code>.</p>
properties	Geeft het eigenschappenblok <code>key:value</code> aan voor objecten.
readOnly	Wordt gebruikt om alleen een formulierlabel op te geven.
title	Wordt gebruikt met <code>oneOf</code> . De beschrijvende naam voor een <code>const</code> -waarde. De titel wordt tijdens het implementeren weergegeven op het formulier voor gebruikersinvoer.

Eigenschap	Beschrijving
type	<p>Het gegevenstype getal, geheel getal, tekenreeks, Booleaans of object.</p> <hr/> <p>Belangrijk Het type Booleaans voegt een leeg selectievakje toe aan het aanvraagformulier. Als u het vak niet bewerkt, wordt de invoer niet False.</p> <p>Om de invoer in te stellen op False, moeten gebruikers het vakje inschakelen en vervolgens uitschakelen.</p>
writeOnly	<p>Verbergt toetsaanslagen in het formulier achter sterretjes. Kan niet met enum worden gebruikt. Wordt als wachtwoordveld weergegeven in aangepaste formulieren van Service Broker.</p>

Aanvullende voorbeelden

Tekenreeks met inventarisatie

```
image:
  type: string
  title: Operating System
  description: The operating system version to use.
  enum:
    - ubuntu 16.04
    - ubuntu 18.04
  default: ubuntu 16.04

shell:
  type: string
  title: Default shell
  description: The default shell that will be configured for the created user.
  enum:
    - /bin/bash
    - /bin/sh
```

Geheel getal met minimum en maximum

```
count:
  type: integer
  title: Machine Count
  description: The number of machines that you want to deploy.
  maximum: 5
  minimum: 1
  default: 1
```

Array van objecten

```
tags:
  type: array
  title: Tags
  description: Tags that you want applied to the machines.
  items:
```

```

type: object
properties:
  key:
    type: string
    title: Key
  value:
    type: string
    title: Value

```

Tekenreeks met beschrijvende namen

```

platform:
  type: string
  oneOf:
    - title: AWS
      const: platform:aws
    - title: Azure
      const: platform:azure
    - title: vSphere
      const: platform:vsphere
  default: platform:aws

```

Tekenreeks met patroonvalidatie

```

username:
  type: string
  title: Username
  description: The name for the user that will be created when the machine is provisioned.
  pattern: ^[a-zA-Z]+$

```

Tekenreeks als wachtwoord

```

password:
  type: string
  title: Password
  description: The initial password that will be required to logon to the machine.
  Configured to reset on first login.
  encrypted: true
  writeOnly: true

```

Tekenreeks als tekstgebied

```

ssh_public_key:
  type: string
  title: SSH public key
  maxLength: 256

```


Booleaans

```
public_ip:
  type: boolean
  title: Assign public IP address
  description: Choose whether your machine should be internet facing.
  default: false
```

Agendakiezer voor datum en tijd

```
leaseDate:
  type: string
  title: Lease Date
  format: date-time
```

vRealize Orchestrator-acties als invoer

U kunt in een Cloud Assembly-sjabloon vRealize Orchestrator-acties opnemen als cloudsjablooninvoer.

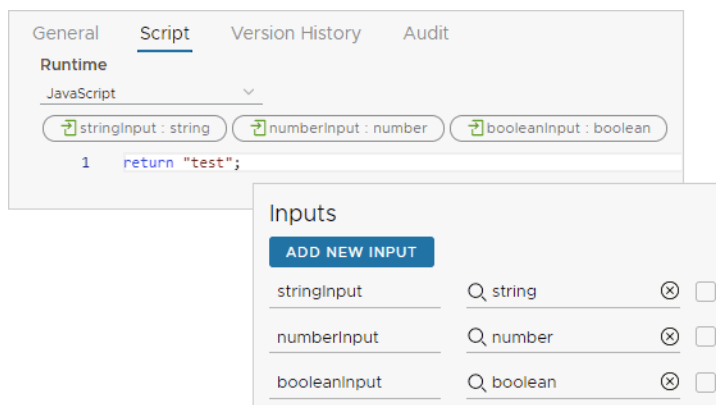
Een vRealize Orchestrator-actie toevoegen als invoer voor cloudsjablonen

Volg deze richtlijnen als u vRealize Orchestrator-acties wilt gebruiken als invoer voor cloudsjablonen.

- 1 Maak in de vRealize Orchestrator-instantie die is ingesloten in vRealize Automation, een actie die doet wat u wilt.

De vRealize Orchestrator-actie mag alleen de typen primitieve tekenreeks, geheel getal, getal en booleaans bevatten. vRealize Orchestrator-typen worden niet ondersteund.

In dit eenvoudige voorbeeld verzamelt de vRealize Orchestrator-actie drie invoerwaarden en wordt een hardgecodeerde tekenreeks geretourneerd.



- 2 Maak of bewerk een cloudsjabloon in Cloud Assembly.
- 3 Klik in de code-editor op het tabblad **Invoer** en **Nieuwe cloudsjablooninvoer**.
- 4 Om de invoer van de vRealize Orchestrator-actie toe te voegen, klikt u op het type en vervolgens op **Constante**.

Voeg elke invoer van de vRealize Orchestrator-actie afzonderlijk toe als nieuwe cloudsjablooninvoer.

New Cloud Template Input

Name *

Display Name

Description

Type

STRING INTEGER **NUMBER** BOOLEAN OBJECT ARRAY

Default value source ☒ Constant ☐ External source

Default value

- 5 Nadat u de actie-invoer hebt toegevoegd, maakt u een nieuwe cloudsjablooninvoer en klikt u achtereenvolgens op het type, **Externe bron** en op **Selecteren**.

New Cloud Template Input

Name *

Display Name

Description

Type

STRING INTEGER NUMBER BOOLEAN OBJECT ARRAY

Default value source ☐ Constant ☒ External source

Action

- 6 Zoek in **Actie** naar de door u gemaakte vRealize Orchestrator-actie en klik vervolgens op **Opslaan**.

Dialog box titled "Add an existing action". The "Action" field is highlighted with an orange arrow. The search bar contains "returnSimpleAction" and "com.form.service.test". Below the search bar are "CANCEL" and "SAVE" buttons.

Wanneer u de cloudsjabloon implementeert, worden de instellingen van de vRealize Orchestrator-actie weergegeven in het invoerformulier van de aanvragende gebruiker.

Form titled "Values for VRO". It contains the following fields:

- String for VRO: _____
- VRO Action: test
- Number for VRO: _____
- On-Off for VRO: ☐

Configureerbare standaardwaarden

Als u het invoerformulier wilt invullen met standaardwaarden, voert u een van de volgende handelingen uit wanneer u de vRealize Orchestrator-actie als externe bron toevoegt.

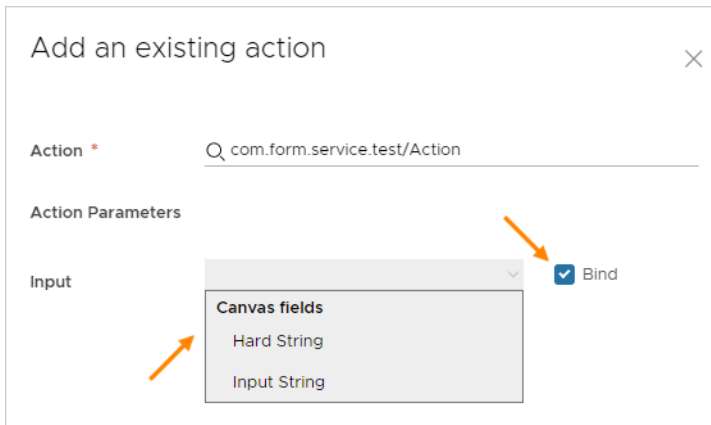
- Geef de standaardwaarde voor de eigenschap handmatig op.

Wis de optie **Binden** en voer de waarde in.

Dialog box titled "Add an existing action". The "Action" field is filled with "com.form.service.test/Action". The "Input" field is filled with "Readme". The "Bind" checkbox is unchecked. Orange arrows point to the "Readme" field and the "Bind" checkbox.

- Gebruik een andere eigenschapswaarde van de aanwezige invoer in de cloudsjabloon.

Selecteer de optie **Binden** en selecteer een eigenschap in het vervolgkeuzelijst.

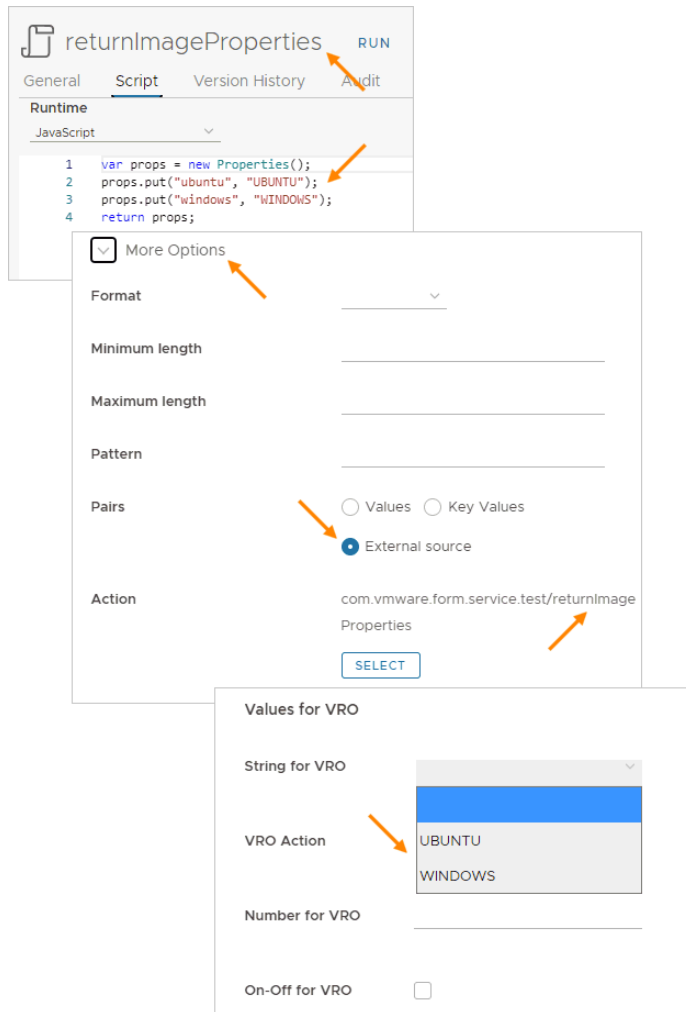


Geïntegreerde invoerselecties van vRealize Orchestrator toevoegen

Als u een op vRealize Orchestrator gebaseerde selectielijst in een invoerformulier wilt maken, doet u het volgende wanneer u deze aan cloudsjablooninvoer toevoegt.

- 1 Maak in vRealize Orchestrator een actie die de waarden toewijst die u in de lijst wilt gebruiken.
- 2 Vouw bij het toevoegen van de cloudsjablooninvoer **Meer opties** uit in Cloud Assembly.
- 3 Klik voor **Paren** op **Externe bron**, klik op **Selecteren** en voeg de vRealize Orchestrator-actie toe die u hebt gemaakt.

Opmerking Als u ook een standaardwaarde maakt bij het toevoegen van de eigenschap, moet die standaardwaarde exact overeenkomen met een van de geïntegreerde waarden van de vRealize Orchestrator-actie.



Een groep eigenschappen in Cloud Assembly hergebruiken

Wanneer u meerdere Cloud Assembly-eigenschappen hebt die altijd samen worden weergegeven, kunt u deze samenvoegen in een eigenschapsgroep.

U kunt snel een eigenschapsgroep aan andere Cloud Assembly-ontwerpen toevoegen, zodat u tijd bespaart bij het een voor een toevoegen van dezelfde meerdere eigenschappen. Daarnaast hebt u één plek om de eigenschappenset te onderhouden of te wijzigen, wat zorgt voor een consistente toepassing.

Alleen gebruikers met de Cloud Assembly-beheerdersrol kunnen een eigenschapsgroep maken, bijwerken of verwijderen. De beheerder kan een eigenschapsgroep delen met een hele organisatie of het gebruik ervan beperken tot alleen in een project.

Voorzichtig Een eigenschapsgroep kan in veel cloudsjablonen worden opgenomen, inclusief de eigenschapsgroepen die al in de catalogus zijn vrijgegeven. Wijzigingen in een eigenschapsgroep kunnen andere gebruikers beïnvloeden.

Er zijn twee typen eigenschapsgroepen.

- **Invoereigenschapsgroepen in Cloud Assembly**

Eigenschapsgroepen voor invoer worden verzameld en toegepast op het moment dat de gebruiker een consistente set eigenschappen invoert. Eigenschapsgroepen voor invoer kunnen vermeldingen bevatten die de gebruiker kan toevoegen of selecteren, of ze kunnen alleen-lezen waarden bevatten die nodig zijn voor het ontwerp.

Eigenschappen die de gebruiker kan bewerken of selecteren, kunnen leesbaar of versleuteld zijn. Alleen-lezen eigenschappen worden weergegeven op het aanvraagformulier, maar kunnen niet worden bewerkt. Als u wilt dat alleen-lezen waarden verborgen blijven, gebruikt u in plaats daarvan een constante eigenschapsgroep.

- **Constance eigenschapsgroepen in Cloud Assembly**

Constance eigenschapsgroepen passen bekende eigenschappen op de achtergrond toe. In feite zijn constante eigenschapsgroepen onzichtbare metagegevens. Ze bieden waarden aan uw Cloud Assembly-ontwerpen op een manier die voorkomt dat een aanvragende gebruiker deze waarden kan lezen of zelfs kan weten dat ze aanwezig zijn. Voorbeelden hiervan zijn licentiesleutels of verificatiegegevens voor het domeinaccount.

De twee typen eigenschapsgroep worden zeer verschillend behandeld door Cloud Assembly. Wanneer u een eigenschapsgroep maakt, moet u eerst selecteren of u invoer of constanten wilt maken. U kunt geen gemengde eigenschapsgroep maken en een bestaande set eigenschappen en hun eigenschapsgroep niet converteren van één type naar het andere.

Invoereigenschapsgroepen in Cloud Assembly

Invoereigenschapsgroepen van Cloud Assembly bevatten doorgaans gerelateerde instellingen die de gebruiker moet invoeren of selecteren. Ze kunnen ook alleen-lezen waarden bevatten die nodig zijn voor het ontwerp van de cloudsjabloon.

De invoereigenschapsgroep maken

- 1 Ga naar **Ontwerp > Eigenschapsgroepen** en klik op **Nieuwe eigenschapsgroep**.
- 2 Selecteer **Invoerwaarden**.
- 3 Geef een naam en beschrijving op voor de nieuwe eigenschapsgroep.

Naam	Eigenschapsgroepsnamen moeten uniek zijn binnen een bepaalde organisatie. Alleen letters, cijfers en onderstrepingstekens zijn toegestaan.
Schermnaam	Voeg een kop toe voor de hele groep eigenschappen, die wordt weergegeven op het aanvraagformulier.
Beschrijving	Leg uit waarvoor deze set eigenschappen is bedoeld.

Scope	Bepaal of een beheerder de eigenschapsgroep mag delen met de hele organisatie. Anders krijgt slechts één project toegang tot de eigenschapsgroep. Hoewel u altijd eigenschappen in de groep kunt toevoegen of aanpassen, is het bereik permanent en kan het later niet worden gewijzigd.
Project	Wanneer het bereik uitsluitend dit project is, krijgt dit project toegang tot de eigenschapsgroep.

4 Klik op **Nieuwe eigenschap** om een eigenschap aan de groep toe te voegen.

Het paneel voor het toevoegen van een nieuwe eigenschap lijkt erg op het tabblad Invoer van de code-editor op de Cloud Assembly-ontwerppagina.

Naam	Vrije naam voor de individuele eigenschap. Alleen letters, cijfers en onderstrepingstekens zijn toegestaan.
Schermnaam	Voeg de naam van een individuele eigenschap toe die op het aanvraagformulier moet worden weergegeven.
Type	Tekenreeks, geheel getal, cijfer, booleaans (waar/onwaar), object of array.
Standaardwaarde	Vooraf ingestelde waarde-invoer die wordt weergegeven in het aanvraagformulier. Voor alle typen behalve Boole is de gebruikersvermelding standaard optioneel. Om ervoor te zorgen dat alle invoer vermeldingen heeft, voert u een van de volgende handelingen uit: <ul style="list-style-type: none"> ■ Stel een standaardwaarde in. ■ Vereist gebruikersinvoer door de volgende cloudsjablooneigenschap toe te voegen aan de voltooide code. <pre>populateRequiredOnNonDefaultProperties: true</pre>
Versleuteld	Indien geselecteerd, wordt de waarde verborgen tijdens het invoeren ervan in het aanvraagformulier en in de volgende implementatie. Versleutelde eigenschappen kunnen geen standaardwaarde hebben.
Alleen-lezen	Een onbewerkbare, maar zichtbare waarde in het aanvraagformulier. Vereist een standaardwaarde.
Meer opties	Opties die variëren afhankelijk van het eigenschapstype. Vouw de vervolgkeuzelijst uit, voeg eventuele aanvullende instellingen toe en klik op Maken .

In het volgende voorbeeld vertegenwoordigt de eigenschap die wordt toegevoegd, de image van het besturingssysteem en kan de aanvragende gebruiker er uit twee kiezen.

Opmerking De besturingssystemen die in de voorbeeldafbeelding worden weergegeven, moeten al deel uitmaken van de geconfigureerde Cloud Assembly-infrastructuur.

New Property

Name * image

Display Name Machine Image

Description

Type

STRING INTEGER NUMBER BOOLEAN OBJECT ARRAY

Default value coreos

Encrypted ☐

Read-only ☐ ⓘ

▼ More Options

Format ▼

Minimum length

Maximum length

Pattern

Pairs ☒ Values ☐ Key Values

Enum

Value

coreos -

ubuntu - +

- 5 Voeg meer eigenschappen aan de groep toe en klik op **Opslaan** wanneer u klaar bent.

Properties 2 items

Add at least one property in order to create a property group

[+ NEW PROPERTY](#) [x DELETE](#)

<input type="checkbox"/>	Name	Display Name	Type	Default Value
<input type="checkbox"/>	image	Machine Image	string	coreos
<input type="checkbox"/>	flavor	Machine Flavor	string	small

De eigenschapsgroep toevoegen aan invoer voor cloudsjablonen

Zelfs voor een lange lijst met eigenschapsinvoer hoeft u alleen de eigenschapsgroep toe te voegen om deze volledig onderdeel te maken van het aanvraagformulier.

- 1 Klik op de ontwerppagina van de cloudsjabloon rechts boven het bewerkingsgebied op het tabblad **Invoer**.
- 2 Klik op **Nieuwe cloudsjablooninvoer**.
- 3 Geef een naam en beschrijving op voor de eigenschapsgroep.

Naam	Voer iets in zoals de naam van de eigenschapsgroep die u eerder hebt gemaakt.
Schermnaam	Voer dezelfde kop in die u eerder hebt gemaakt voor de hele groep eigenschappen, die wordt weergegeven op het aanvraagformulier.
Type	Selecteer Object .
Objecttype	Selecteer Eigenschapsgroep .
Lijst met eigenschapsgroepen	Selecteer de gewenste eigenschapsgroep. Alleen eigenschapsgroepen die zijn gemaakt en beschikbaar zijn voor uw project, worden weergegeven. Constante eigenschapsgroepen worden niet weergegeven.

New Cloud Template Input [X]

Name * pgmachine

Display Name Machine Properties

Description

Type

STRING INTEGER NUMBER BOOLEAN **OBJECT** ARRAY

Select Object Type ☐ Properties ☒ Property Groups

Select from the existing property groups

Q

Name	Description
<input checked="" type="radio"/> machine	

- 4 Klik op **Maken**.

Het proces maakt invoercode voor een cloudsjabloon, vergelijkbaar met het volgende voorbeeld.

```
inputs:
  pgmachine:
    type: object
    title: Machine Properties
    $ref: /ref/property-groups/machine
  pgrequester:
    type: object
    title: Requester Details
    $ref: /ref/property-groups/requesterDetails
```

U kunt code ook rechtstreeks op de Cloud Assembly-ontwerppagina invoeren en gebruikmaken van de automatische prompts wanneer u `$ref: /ref/p...` in de code-editor typt.

Resources van een cloudsjabloon binden aan de eigenschapsgroep

Om gebruik te maken van invoerwaarden voor de eigenschapsgroep, voegt u bindingen toe onder de resource.

Afhankelijk van het type waarden in een eigenschapsgroep wilt u er mogelijk afzonderlijk naar verwijzen. U kunt ze afzonderlijk invoeren op eigenschapsgroepsnaam en eigenschapsnaam.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: '${input.pgmachine.image}'
      flavor: '${input.pgmachine.flavor}'
```

U kunt ook snel een hele set waarden aan een resource toevoegen door te verwijzen naar een hele eigenschapsgroep.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      requester: '${input.pgrequester}'
```

Voltooide code

Wanneer u klaar bent met de invoer en resources, ziet de voltooide code er als volgt uit.

```

>> Code Properties Inputs
1 formatVersion: 1
2 inputs:
3   pgmachine:
4     type: object
5     title: Machine Properties
6     $ref: /ref/property-groups/machine
7   pgrequester:
8     type: object
9     title: Requester Details
10    $ref: /ref/property-groups/requesterDetails
11  count:
12    type: integer
13    title: 'Machine Count'
14  resources:
15    Cloud_Machine_1:
16      type: Cloud.Machine
17      properties:
18        image: '${input.pgmachine.image}'
19        flavor: '${input.pgmachine.flavor}'
20        count: '${input.count}'
21        requester: '${input.pgrequester}'
22

```

Na de implementatieaanvraag worden uw eigenschapsgroepen weergegeven om door de aanvragende gebruiker te worden voltooid.

Deployment Inputs

Machine Properties

Machine Image

coreos

Machine Flavor

small

Requester Details

Email
Mobile
Internal account?

☐

PIN
Account Type

User

Machine Count *

Eigenschapsgroepen in de Service Broker-editor voor aangepaste formulieren

Invoereigenschapsgroepen worden weergegeven in de Service Broker-interface voor aangepaste formulieren en zijn daar beschikbaar voor aanpassing. Er zijn geen bijzondere overwegingen alleen voor eigenschapsgroepen wanneer u ze aanpast. Service Broker gebruikers hoeven niet eens te weten dat de bron van de vermeldingen een eigenschapsgroep is in plaats van afzonderlijk gemaakte eigenschappen.

The screenshot shows the 'General' tab of a form in vRealize Automation Cloud Assembly. The form has a grid background and includes the following fields:

- Project**: A text input field with a dropdown arrow.
- Deployment Name**: A text input field.
- Machine Count**: A text input field.
- Machine Properties**: A dashed orange box containing:
 - Machine Image**: A text input field with a dropdown arrow.
 - Machine Flavor**: A text input field with a dropdown arrow.
- Requester Details**: A dashed orange box containing:
 - Email**: A text input field.
 - Mobile**: A text input field.
 - Internal account?**: A checkbox.
 - PIN**: A text input field.
 - Account Type**: A text input field.

Zie [Een Service Broker-pictogram en aanvraagformulier aanpassen](#) voor meer informatie.

vRealize Orchestrator-acties in een invoereigenschapsgroep

In een invoereigenschapsgroep in Cloud Assembly kunt u dynamische interactie met vRealize Orchestrator toevoegen.

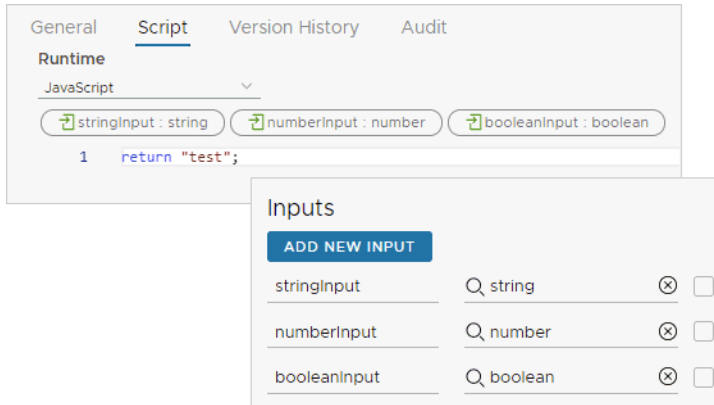
Een vRealize Orchestrator-actie toevoegen aan een invoereigenschapsgroep

Volg deze richtlijnen als u dynamische interactie met vRealize Orchestrator wilt toevoegen aan een invoereigenschapsgroep.

- 1 Maak in de vRealize Orchestrator-instantie die is ingesloten in vRealize Automation, een actie die doet wat u wilt.

De vRealize Orchestrator-actie mag alleen de typen primitieve tekenreeks, geheel getal, getal en booleaans bevatten. vRealize Orchestrator-typen worden niet ondersteund.

In dit eenvoudige voorbeeld verzamelt de vRealize Orchestrator-actie drie invoerwaarden en wordt een hardgecodeerde tekenreeks geretourneerd.



- In Cloud Assembly start u het proces voor het maken of bewerken van een invoereigenschapsgroep. Zie [Invoereigenschapsgroepen in Cloud Assembly](#) indien nodig.
- Om de invoerwaarden van de vRealize Orchestrator-actie toe te voegen aan een eigenschapsgroep, voegt u nieuwe eigenschappen toe, klikt u op het type en klikt u op **Constante**.

Voeg elke invoer voor de vRealize Orchestrator-actie afzonderlijk toe.

The 'New Property' dialog box is shown. It has fields for 'Name' (numberInput), 'Display Name' (Number for VRO), and 'Description'. Below these is a 'Type' section with buttons for STRING, INTEGER, NUMBER, BOOLEAN, OBJECT, and ARRAY. The 'NUMBER' button is selected, indicated by an orange arrow. Below the type buttons is a 'Default value source' section with radio buttons for 'Constant' (selected) and 'External source'. An orange arrow points to the 'Constant' radio button. At the bottom is a 'Default value' field.

- Nadat u de invoer hebt toegevoegd, voegt u een nieuwe eigenschap toe, klikt u op het type, klikt u op **Externe bron** en klikt u op **Selecteren**.

New Property

Name *

Display Name

Description

Type

STRING INTEGER NUMBER BOOLEAN OBJECT ARRAY

Default value source ☐ Constant ☒ External source

Action

- 5 Zoek in **Actie** naar de door u gemaakte vRealize Orchestrator-actie en klik vervolgens op **Opslaan**.

Add an existing action

Action *

com.form.service.test

- 6 Sla de eigenschapsgroep op en voeg deze toe aan uw cloudsjabloon. Zie [Invoereigenschapsgroepen in Cloud Assembly](#) indien nodig.

Wanneer u de cloudsjabloon implementeert, wordt de eigenschapsgroep van de vRealize Orchestrator-actie in het invoerformulier weergegeven voor de aanvragende gebruiker.

Values for VRO

String for VRO

VRO Action

Number for VRO

On-Off for VRO

test

☐

Configureerbare standaardwaarden

Als u het invoerformulier wilt invullen met standaardwaarden, voert u een van de volgende handelingen uit wanneer u de vRealize Orchestrator-actie als externe bron toevoegt.

- Geef de standaardwaarde voor de eigenschap handmatig op.

Wis de optie **Binden** en voer de waarde in.

Add an existing action

Action *

Action Parameters

Input

Readme

☐ Bind

- Gebruik een andere eigenschapswaarde uit dezelfde eigenschapsgroep.

Selecteer de optie **Binden** en selecteer een eigenschap in het vervolgkeuzelijst.

Add an existing action

Action *

Action Parameters

Input

Canvas fields

Hard String

Input String

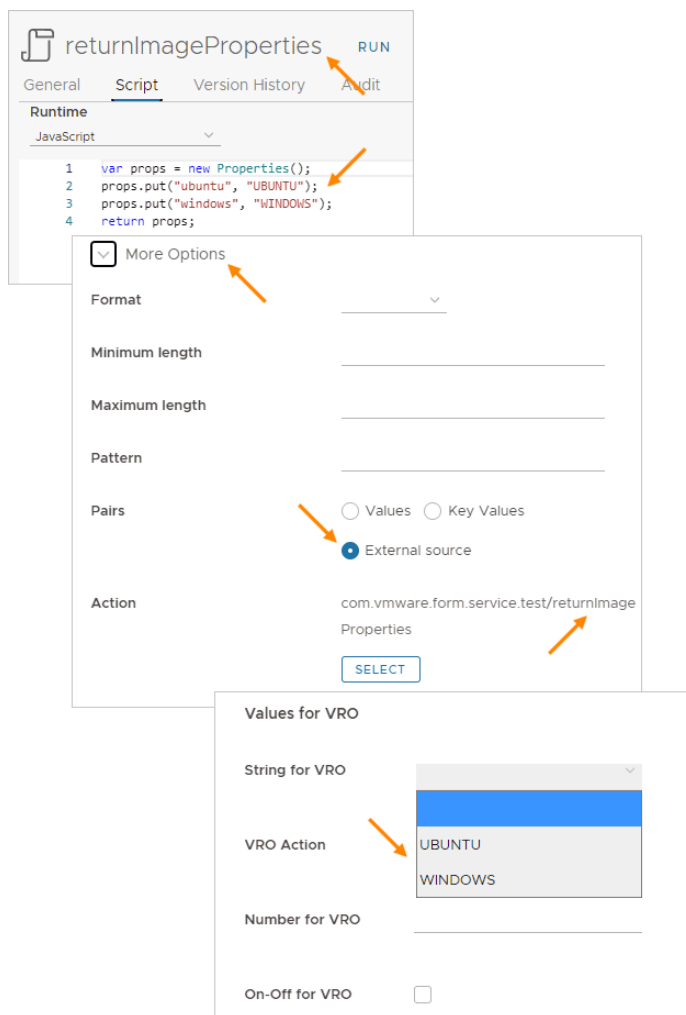
☒ Bind

Geïntegreerde invoerselecties van vRealize Orchestrator toevoegen

Als u een op vRealize Orchestrator gebaseerde selectielijst in een invoerformulier wilt maken, doet u het volgende wanneer u deze aan een eigenschapsgroep toevoegt.

- 1 Maak in vRealize Orchestrator een actie die de waarden toewijst die u in de lijst wilt gebruiken.
- 2 Vouw **Meer opties** uit in Cloud Assembly wanneer u een eigenschap toevoegt aan de groep.
- 3 Klik voor **Paren** op **Externe bron**, klik op **Selecteren** en voeg de vRealize Orchestrator-actie toe die u hebt gemaakt.

Opmerking Als u ook een standaardwaarde maakt bij het toevoegen van de eigenschap, moet die standaardwaarde exact overeenkomen met een van de geïntegreerde waarden van de vRealize Orchestrator-actie.



Constance eigenschapsgroepen in Cloud Assembly

Met Cloud Assembly-constanten kunt u bekende sleutelwaardeparen op de achtergrond op uw ontwerpen toepassen.

Hoe constanten werken

De sleutel wordt weergegeven in de code van de cloudsjabloon en de waarde wordt onderdeel van implementaties die zijn gebaseerd op die cloudsjabloon. Voor 'constanten' is de binding `propgroup` vereist onder de resource.

De binding `propgroup` wordt alleen gebruikt met constante eigenschapsgroepen, geen eigenschapsgroepen voor invoer.

Geheime eigenschappen

Als u verwacht dat u een geheime eigenschap aan een eigenschapsgroep gaat toevoegen, maakt u de geheime eigenschap voordat u doorgaat. Zie [Geheime Cloud Assembly-eigenschappen](#).

De constante eigenschapsgroep maken

- 1 Ga naar **Ontwerp > Eigenschapsgroepen** en klik op **Nieuwe eigenschapsgroep**.
- 2 Selecteer **Constante waarden**.
- 3 Geef een naam en beschrijving op voor de nieuwe eigenschapsgroep.

Naam	Eigenschapsgroepsnamen moeten uniek zijn binnen een bepaalde organisatie. Alleen letters, cijfers en onderstrepingstekens zijn toegestaan.
Schermnaam	Laat het veld leeg. Er wordt geen kop weergegeven op het aanvraagformulier.
Beschrijving	Leg uit waarvoor deze set constanten is bedoeld.
Scope	<p>Bepaal of een beheerder de eigenschapsgroep mag delen met de hele organisatie. Anders krijgt slechts één project toegang tot de eigenschapsgroep.</p> <p>Hoewel u altijd eigenschappen in de groep kunt toevoegen of aanpassen, is het bereik permanent en kan het later niet worden gewijzigd.</p> <p>Geheimen—Als u verwacht dat u een geheime eigenschap gaat toevoegen aan de eigenschapsgroep, moet u één projectbereik gebruiken. Geheime eigenschappen worden alleen op projectniveau opgeslagen.</p>
Project	Wanneer het bereik uitsluitend dit project is, krijgt dit project toegang tot de eigenschapsgroep.

- 4 Als u een constante eigenschap wilt toevoegen aan de groep, klikt u op **Nieuwe eigenschap**.
- 5 Voer een naam in die als sleutel fungeert, evenals een beschrijving.
- 6 Selecteer een eigenschapstype.
- 7 Voer de gewenste constante waarde in en klik op **Maken**.
 - Voor de typen tekenreeks, geheel getal en getal wordt directe invoer gebruikt.

- Voor een geheime tekenreekswaarde selecteert u uit de lijst met geheime eigenschappen voor het project.
- Het booleaanse type gebruikt een selectievakje om true aan te geven.
- Voor het object- of arraytype vervangt u `null` door de gewenste tekst.

The left screenshot shows the 'New Property' dialog with the 'Constant value' tab selected. The 'Name' field contains 'payerAccountNumber' and the 'Constant value' field contains '123456'. The 'Type' dropdown is set to 'STRING'. The 'Select Type' section has 'Constant value' selected.

The right screenshot shows the 'New Property' dialog with the 'Secret' tab selected. The 'Name' field contains 'payerAccountNumber'. The 'Type' dropdown is set to 'STRING'. The 'Select Type' section has 'Secret' selected. Below the 'Select Type' section is a search bar and a list of secret properties. The list has columns 'Name' and 'Description'. The first item is 'AccountNumber', which is selected with a radio button. Below it are 'password' and 'RemoteAccessKey1'. At the bottom right of the list, it says '7 secrets'.

- 8 Voeg meer constanten aan de groep toe en klik op **Opslaan** wanneer u klaar bent.

Properties 3 items

Add at least one property in order to create a property group

[+ NEW PROPERTY](#) [X DELETE](#)

<input type="checkbox"/>	Name	Display Name	Type	Constant Value
<input type="checkbox"/>	payerFederal		boolean	true
<input type="checkbox"/>	payerCostCenter		integer	7890
<input type="checkbox"/>	payerAccountNumber		string	123456

Resources van een cloudsjabloon binden aan de eigenschapsgroep

Als u constante waarden in een resource op de achtergrond wilt gebruiken, voegt u `propgroup`-bindingen toe onder de resource.

U kunt snel een hele set constanten aan een resource toevoegen door naar de eigenschapsgroep zelf te verwijzen.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      payerInfo: '${propgroup.payerDetails}'
```

U kunt ook individuele constanten uit de eigenschapsgroep toevoegen aan geselecteerde onderdelen van uw ontwerp.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      payerAccount: '${propgroup.payerDetails.payerAccountNumber}'
      payerCost: '${propgroup.payerDetails.payerCostCenter}'
      payerFed: '${propgroup.payerDetails.payerFederal}'
```

Meer informatie over Cloud Assembly-eigenschapsgroepen

Een Cloud Assembly-eigenschapsgroep kan zijn opgenomen in veel cloudsjablonen, wat van invloed is op de manier waarop u eigenschapsgroepen moet beheren.

Een eigenschapsgroep wijzigen

Wijzigingen in een Cloud Assembly-eigenschapsgroep zijn van invloed op elke cloudsjabloon die deze gebruikt. Bovendien zijn die wijzigingen nu van invloed op Service Broker-catalogusgebruikers wanneer de gewijzigde versie van de cloudsjabloon wordt vrijgegeven.

In de lijst met eigenschapsgroepen en de bewerkingspagina's voor eigenschapsgroepen wordt het aantal cloudsjablonen weergegeven die de eigenschapsgroep bevatten. Klik op het aantal om te zien welke cloudsjabloon door een wijziging wordt beïnvloed.

The screenshot displays the 'Property Groups' management interface. At the top, there's a header 'Property Groups' with a count of '61 items' and a filter icon. Below this are buttons for '+ NEW PROPERTY GROUP' and 'x DELETE', along with a search bar labeled 'Filter...'. A table lists the property groups:

	Name	Type	Properties	Cloud Templates	Last Updated
<input type="radio"/>	machine	Input	2	2 ←	Apr 29, 2021, 4:26:18 PM
<input type="radio"/>	mh_const	Constant	5	1	Apr 27, 2021, 5:29:33 PM

Below the table, a modal window titled 'Cloud Templates' is open, showing a count of '2' with an orange arrow pointing to the 'Cloud Templates' column of the 'machine' group. This modal contains a 'Properties' section with '2 items' and a message: 'Add at least one property in order to create a property group'. It includes buttons for '+ NEW PROPERTY' and 'x DELETE', and a table of properties:

<input type="checkbox"/>	Name	Display Name	Type	Default Value
<input type="checkbox"/>	image	Machine Image	string	coreos
<input type="checkbox"/>	flavor	Machine Flavor	string	small

Voordat u een eigenschapsgroep wijzigt, moet u ervoor zorgen dat de wijziging acceptabel is voor iedereen die implementaties maakt of bijwerkt op basis van de weergegeven cloudsjablonen.

Een eigenschapsgroep verwijderen

Het verwijderen van een eigenschapsgroep zou fouten veroorzaken in elke cloudsjabloon die deze gebruikt.

U kunt een eigenschapsgroep pas verwijderen als u deze handmatig verwijdert uit alle cloudsjablonen waarin deze is opgenomen. Als u een eigenschapsgroep uit een cloudsjabloon wilt verwijderen, opent u de cloudsjabloon in het ontwerpcanvas.

■ Eigenschapsgroepen invoeren

Selecteer en verwijder de eigenschapsgroep op het tabblad Invoer. U kunt ook de code-editor gebruiken om de bijbehorende eigenschapsgroep te verwijderen in het gedeelte `inputs` van de code.

■ Constante eigenschapsgroepen

Gebruik de code-editor om de bijbehorende `propgroup`-invoer of -vermeldingen in het gedeelte `resources` van de code te verwijderen.

Opmerking U kunt een eigenschapsgroep niet verwijderen als deze is opgenomen in een cloudsjabloon met versie. Cloudsjablonen met versie zijn alleen-lezen.

Cloud Assembly-resourcevlaggen voor aanvragen

Cloud Assembly bevat verschillende instellingen voor cloudsjablonen die bepalen hoe een resource op het moment van de aanvraag wordt verwerkt.

Instellingen voor resourcevlaggen maken geen deel uit van het eigenschappenschema van het resourceobject. Voor een bepaalde resource voegt u de markeringsinstellingen buiten de sectie met eigenschappen toe, zoals getoond.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    preventDelete: true
    properties:
      image: coreos
      flavor: small
      attachedDisks:
        - source: '${resource.Cloud_Volume_1.id}'
  Cloud_Volume_1:
    type: Cloud.Volume
    properties:
      capacityGb: 1
```

Resourcevlag	Beschrijving
allocatePerInstance	<p>Indien ingesteld op waar, kan de resourcetoewijzing voor elke machine in een cluster worden aangepast. Als u uitbreidbaarheid gebruikt, kan het gebeurtenisonderwerp voor <code>compute.allocation.pre</code>-uitbreidbaarheid meerdere keren worden uitgevoerd bij het implementeren van meer dan één cloudmachine.</p> <p>De standaardwaarde is onwaar, waarmee resources gelijkmatig over het cluster worden toegewezen, wat resulteert in dezelfde configuratie voor elke machine. Bovendien zijn acties voor dag 2 mogelijk niet afzonderlijk mogelijk voor afzonderlijke resources.</p> <p>Met de toewijzing per instantie kan <code>count.index</code> de configuratie voor afzonderlijke machines correct toepassen. Zie Machine- en schijfclusters in Cloud Assembly voor meer codevoorbeelden.</p>
createBeforeDelete	<p>Voor sommige updateacties moet de bestaande resource worden verwijderd en moet er een nieuwe worden gemaakt. Standaard wordt eerst de resource verwijderd, wat kan leiden tot situaties waarin de oude resource is verdwenen, maar er om een of andere reden nog geen nieuwe is gemaakt.</p> <p>Stel deze vlag in op waar als u er zeker van wilt zijn dat de nieuwe resource is gemaakt voordat u de vorige verwijdert.</p>

Resourcevlag	Beschrijving
createTimeout	<p>De standaardtime-out van Cloud Assembly voor aanvragen om resources toe te wijzen, te maken en te plannen is 2 uur (2h). Daarnaast kan een projectbeheerder een aangepaste standaardtime-out voor deze aanvragen instellen, die van toepassing is op het hele project.</p> <p>Met deze vlag kunt u de standaardinstellingen overschrijven en de individuele time-out instellen voor een specifieke resourcebewerking. Zie ook <code>updateTimeout</code> en <code>deleteTimeout</code>.</p>
deleteTimeout	<p>De standaardtime-out van Cloud Assembly voor verwijderingsaanvragen is 2 uur (2h). Daarnaast kan een projectbeheerder een andere standaardtime-out voor verwijderingsaanvragen instellen, die van toepassing is op het hele project.</p> <p>Met deze vlag kunt u de standaardinstellingen overschrijven en de individuele time-out instellen voor een specifieke resourceverwijdering. Zie ook <code>updateTimeout</code> en <code>createTimeout</code>.</p>
dependsOn	<p>Deze vlag identificeert een expliciete afhankelijkheid tussen resources, waarbij één resource moet bestaan voordat de volgende wordt gemaakt. Zie Bindingen en afhankelijkheden maken tussen resources in Cloud Assembly voor meer informatie.</p>
dependsOnPreviousInstances	<p>Indien ingesteld op waar, maakt u sequentieel clusterresources. De standaardwaarde is onwaar, waarmee alle resources gelijktijdig in een cluster worden gemaakt.</p> <p>Sequentiële aanmaak is bijvoorbeeld handig voor databaseclusters waarbij primaire en secundaire knooppunten moeten worden gemaakt, maar voor het maken van secundaire knooppunten configuratie-instellingen nodig zijn die het knooppunt verbinden met een bestaand, primair knooppunt.</p>
forceRecreate	<p>Het verwijderen van de bestaande resource en het maken van een nieuwe is niet voor alle updateacties vereist. Als u wilt dat een update de oude resource verwijdert en een nieuwe maakt, ongeacht of de update dit standaard zou hebben gedaan, moet u deze vlag instellen op waar.</p>
ignoreChanges	<p>Gebruikers van een resource kunnen deze opnieuw configureren en de resource vanuit de geïmplementeerde status wijzigen.</p> <p>Als u een implementatie-update wilt uitvoeren, maar de gewijzigde resource niet wilt overschrijven met de configuratie van de cloudsjabloon, stelt u deze vlag in op waar.</p>

Resourcevlag	Beschrijving
ignorePropertiesOnUpdate	<p>Gebruikers van een resource kunnen bepaalde eigenschappen aanpassen en deze eigenschappen worden tijdens een updateactie mogelijk opnieuw ingesteld op de oorspronkelijke status van de cloudsjabloon.</p> <p>Als u wilt voorkomen dat de eigenschappen opnieuw worden ingesteld door een updateactie, stelt u deze vlag in op waar.</p>
preventDelete	<p>Als u een gemaakte resource wilt beveiligen tegen onopzettelijke verwijdering, stelt u deze vlag in op true. Als een gebruiker de implementatie echter verwijdert, wordt de resource verwijderd.</p>
recreatePropertiesOnUpdate	<p>Gebruikers van een resource kunnen deze eigenschappen opnieuw configureren en de resource vanuit de geïmplementeerde status wijzigen. Tijdens een update kan een resource wel of niet opnieuw worden gemaakt. Resources die niet opnieuw worden gemaakt, blijven mogelijk behouden met eigenschappen in een gewijzigde staat.</p> <p>Als u wilt dat een resource en de bijbehorende eigenschappen opnieuw worden gemaakt, ongeacht of dit tijdens de update standaard wordt gedaan, stelt u deze vlag in op waar.</p>
updateTimeout	<p>De standaardtime-out van Cloud Assembly voor updateaanvragen is 2 uur (2h). Daarnaast kan een projectbeheerder een andere standaardtime-out voor updateaanvragen instellen, die van toepassing is op het hele project.</p> <p>Met deze vlag kunt u de standaardinstellingen overschrijven en de individuele time-out instellen voor een specifieke resource-update. Zie ook deleteTimeout en createTimeout.</p>

Cloud Assembly-expressies

Voor meer flexibiliteit kunt u expressies aan cloudsjablooncode toevoegen in Cloud Assembly.

Hoe expressies werken

Cloud Assembly-expressies gebruiken de construct `${expressie}`, zoals in de volgende voorbeelden wordt weergegeven.

Opmerking Cloud Assembly-expressies zijn anders dan reguliere expressies. Zie de [Syntaxis voor Cloud Assembly-expressie](#) voor Cloud Assembly.

De volgende codevoorbeelden zijn ingekort tot de belangrijkste regels. De volledige, niet-bewerkte cloudsjabloon wordt aan het einde weergegeven.

Voorbeelden

Tijdens de implementatie kan de gebruiker de versleutelde sleutel plakken die nodig is voor externe toegang:

```
inputs:
  sshKey:
    type: string
    maxLength: 500
resources:
  frontend:
    type: Cloud.Machine
    properties:
      remoteAccess:
        authentication: publicPrivateKey
        sshKey: '${input.sshKey}'
```

Voor het implementeren in VMware Cloud on AWS de mapnaam instellen op de vereiste naam van *Workload*:

```
inputs:
  environment:
    type: string
    enum:
      - AWS
      - vSphere
      - Azure
      - VMC
      - GCP
    default: vSphere
resources:
  frontend:
    type: Cloud.Machine
    properties:
      folderName: '${input.environment == "VMC" ? "Workload" : ""}'
```

Tijdens het implementeren tagt u de machine met de tag *env* (in kleine letters) die overeenkomt met de geselecteerde omgeving:

```
inputs:
  environment:
    type: string
    enum:
      - AWS
      - vSphere
      - Azure
      - VMC
      - GCP
    default: vSphere
resources:
  frontend:
```



```

type: Cloud.Machine
properties:
  constraints:
    - tag: '${"env:" + to_lower(input.environment)}'

```

Stel het aantal machines in het front-endcluster in op één (klein) of twee (groot). Houd er rekening mee dat het grote cluster wordt ingesteld op basis van eliminatie:

```

inputs:
  envsize:
    type: string
    enum:
      - Small
      - Large
resources:
  frontend:
    type: Cloud.Machine
    properties:
      count: '${input.envsize == "Small" ? 1 : 2}'

```

Machines aan hetzelfde *standaardnetwerk* koppelen door te binden aan de eigenschap die is gevonden in de netwerkresource:

```

resources:
  frontend:
    type: Cloud.Machine
    properties:
      networks:
        - network: '${resource.Cloud_Network_1.name}'
  apitier:
    type: Cloud.Machine
    properties:
      networks:
        - network: '${resource.Cloud_Network_1.name}'
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      name: Default
      networkType: existing

```

Toegangsreferenties versleutelen die zijn verzonden naar de API:

```

resources:
  apitier:
    type: Cloud.Machine
    properties:
      cloudConfig: |
        #cloud-config
      runcmd:
        - export apikey=${base64_encode(input.username:input.password)}
        - curl -i -H 'Accept:application/json' -H 'Authorization:Basic :$apikey' http://
example.com

```

Het adres van de API-machine detecteren:

```
resources:
  frontend:
    type: Cloud.Machine
    properties:
      cloudConfig: |
        runcmd:
          - echo ${resource.apitier.networks[0].address}
  apitier:
    type: Cloud.Machine
    properties:
      networks:
        - network: '${resource.Cloud_Network_1.name}'
```

Cloudsjabloon voltooien

```
inputs:
  environment:
    type: string
    enum:
      - AWS
      - vSphere
      - Azure
      - VMC
      - GCP
    default: vSphere
  sshKey:
    type: string
    maxLength: 500
  envsize:
    type: string
    enum:
      - Small
      - Large
resources:
  frontend:
    type: Cloud.Machine
    properties:
      folderName: '${input.environment == "VMC" ? "Workload" : ""}'
      image: ubuntu
      flavor: medium
      count: '${input.envsize == "Small" ? 1 : 2}'
      remoteAccess:
        authentication: publicPrivateKey
        sshKey: '${input.sshKey}'
      cloudConfig: |
        packages:
          - nginx
        runcmd:
          - echo ${resource.apitier.networks[0].address}
      constraints:
        - tag: '${"env:" + to_lower(input.environment)}'
    networks:
```

```

    - network: '${resource.Cloud_Network_1.name}'
  apitier:
    type: Cloud.Machine
    properties:
      folderName: '${input.environment == "VMC" ? "Workload" : ""}'
      image: ubuntu
      flavor: small
      cloudConfig: |
        #cloud-config
        runcmd:
          - export apikey=${base64_encode(input.username:input.password)}
          - curl -i -H 'Accept:application/json' -H 'Authorization:Basic :$apikey' http://
example.com
      remoteAccess:
        authentication: publicPrivateKey
        sshKey: '${input.sshKey}'
      constraints:
        - tag: '${"env:" + to_lower(input.environment)}'
    networks:
      - network: '${resource.Cloud_Network_1.name}'
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      name: Default
      networkType: existing
    constraints:
      - tag: '${"env:" + to_lower(input.environment)}'

```

Syntaxis voor Cloud Assembly-expressie

De expressiesyntaxis geeft alle beschikbare mogelijkheden van expressies in Cloud Assembly-sjablonen weer.

Opmerking Cloud Assembly-expressies zijn anders dan reguliere expressies.

De volgende syntaxis wordt slechts gedeeltelijk weergegeven in de voorbeelden die u ziet in [Cloud Assembly-expressies](#).

Literals

De volgende literals worden ondersteund:

- Booleaans (waar of onwaar)
- Geheel getal
- Drijvende komma
- Tekenreeks

Backslash wordt gebruikt om dubbele aanhalingstekens, enkele aanhalingstekens en een backslash zelf aan te geven:

" wordt met escapeteken aangegeven als \"

' wordt met escapeteken aangegeven als \'

\ wordt met escapeteken aangegeven als \\

De aanhalingstekens hoeven alleen met een escapeteken te worden aangegeven in een tekenreeks die is ingesloten tussen aanhalingstekens van hetzelfde type, zoals hieronder wordt weergegeven.

```
"I am a \"double quoted\" string inside \"double quotes\"."
```

- Null

Omgevingsvariabelen

Omgevingsnamen:

- orgId
- projectId
- projectName
- deploymentId
- deploymentName
- blueprintId
- blueprintVersion
- blueprintName
- requestedBy (gebruiker)
- requestedAt (tijd)

Syntaxis:

```
env.ENV_NAME
```

Voorbeeld:

```
${env.blueprintId}
```

Resourcevariabelen

Met resourcevariabelen kunt u vanuit andere resources binden aan resource-eigenschappen.

Syntaxis:

```
resource.RESOURCE_NAME.PROPERTY_NAME
```

Resourcenamen mogen geen dashjes of punten bevatten. Onderstrepingstekens zijn toegestaan.

Voorbeelden:

- \${resource.db.id}

- `${resource.db.networks[0].address}`
- `${resource.app.id}` (De tekenreeks voor niet-geclusterde resources retourneren, waarbij aantal niet is opgegeven. De array voor geclusterde resources retourneren.)
- `${resource.app[0].id}` (De eerste invoer voor geclusterde resources retourneren.)

Self-variabelen voor resource

Self-variabelen voor resources zijn alleen toegestaan voor resources die de toewijzingsfase ondersteunen. Self-variabelen voor resources zijn alleen beschikbaar (of hebben alleen een ingestelde waarde) nadat de toewijzingsfase is voltooid.

Syntaxis:

```
self.property_name
```

Voorbeeld:

```
${self.address} (Retourneren het adres dat is toegewezen tijdens de toewijzingsfase.)
```

Voor een resource met de naam `resource_x` zijn `self.property_name` en `resource.resource_x.property_name` hetzelfde en beide worden beschouwd als zelfverwijzingen.

Voorwaarden

Syntaxis:

- Gelijkheidsoperators zijn `==` en `!=`.
- Relationale operators zijn `<` `>` `<=` en `>=`.
- Logische operators zijn `&&` `||` en `!`.
- Conditionals gebruiken het patroon:
condition-expression ? true-expression : false-expression

Voorbeelden:

```
${input.count < 5 && input.size == 'small'}
```

```
${input.count < 2 ? "small":"large"}
```

Clustertellerindex

Syntaxis:

```
count.index
```

Voorbeelden:

- Het knooppunttype voor geclusterde resources retourneren:

```
${count.index == 0 ? "primary":"secondary"}
```

- De grootte van elke schijf tijdens de toewijzing instellen:

```
inputs:
  disks:
    type: array
    minItems: 0
    maxItems: 12
    items:
      type: object
      properties:
        size:
          type: integer
          title: Size (GB)
          minSize: 1
          maxSize: 2048
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    allocatePerInstance: true
    properties:
      capacityGb: '${input.disks[count.index].size}'
      count: '${length(input.disks)}'
```

- Zie [Machine- en schijfclusters in Cloud Assembly](#) voor meer voorbeelden.

Rekenkundige operators

Syntaxis:

Operators zijn + - / * en %.

Voorbeeld:

```
${(input.count + 5) * 2}
```

Samenvoeging van tekenreeks

Syntaxis:

```
${'ABC' + 'DEF'} resulteert in ABCDEF.
```

Operators [] en .

De expressie volgt het ECMAScript om de verwerking van de operators [] en . gelijk te schakelen.

Dus is `expr.identifiek` gelijk aan `expr["identifiek"]`. De id wordt gebruikt om een literal te maken waarvan de waarde de id is en vervolgens wordt de operator [] met die waarde gebruikt.

Voorbeeld:

```
${resource.app.networks[0].address}
```

Als een eigenschap een spatie bevat, moet u deze bovendien markeren met vierkante haakjes en dubbele aanhalingstekens in plaats van de puntnotatie te gebruiken.

Onjuist:

```
input.operating system
```

Juist:

```
input["operating system"]
```

Constructie van kaart

Syntaxis:

```
${{'key1':'value1', 'key2':input.key2}}
```

Constructie van array

Syntaxis:

```
${['key1','key2']}
```

Voorbeeld:

```
${[1,2,3]}
```

Functies

Syntaxis:

```
${functie(argumenten...)}
```

Voorbeeld:

```
${to_lower(resource.app.name)}
```

Tabel 6-1. Functies

Functie	Beschrijving
abs(getal)	Absolute getalwaarde
avg(array)	Het gemiddelde van alle waarden van een array met getallen retourneren
base64_decode(tekenreeks)	Gedecodeerde Base64-waarde retourneren
base64_encode(tekenreeks)	Base64-gecodeerde waarde retourneren
ceil(getal)	Retourneert de kleinste waarde (die negatieve oneindigheid het dichtst benadert) die groter is dan of gelijk is aan het argument en gelijk is aan een wiskundig geheel getal
contains(array, waarde)	Controleren of de array een waarde bevat
contains(tekenreeks, waarde)	Controleren of de tekenreeks een waarde bevat
digest(waarde, type)	Samenvatting van waarde met ondersteund type (md5, sha1, sha256, sha384, sha512) retourneren
ends_with(onderwerp, achtervoegsel)	Controleren of de onderwerptekenreeks eindigt op de achtervoegseltekenreeks

Tabel 6-1. Functies (vervolg)

Functie	Beschrijving
<code>filter_by(array, filter)</code>	<p>Retourneert alleen de arrayvermeldingen die slagen voor de filterbewerking</p> <pre>filter_by([1,2,3,4], x => x >= 2 && x <= 3)</pre> <p>retourneert <code>[2, 3]</code></p> <pre>filter_by({'key1':1, 'key2':2}, (k,v) => v != 1)</pre> <p>retourneert <code>[{"key2": 2}]</code></p>
<code>floor(getal)</code>	Retourneert de grootste waarde (die positieve oneindigheid het dichtst benadert) die kleiner is dan of gelijk is aan het argument en gelijk is aan een wiskundig geheel getal
<code>format(notatie, waarden...)</code>	Een opgemaakte tekenreeks met behulp van Java Class Formatter -notatie en -waarden retourneren.
<code>from_json(tekenreeks)</code>	JSON-tekenreeks parseren
<code>join(array, scheidingsteken)</code>	Array van tekenreeksen met een scheidingsteken samenvoegen en een tekenreeks retourneren
<code>json_path(waarde, pad)</code>	Het pad ten opzichte van de waarde evalueren met behulp van XPath voor JSON .
<code>keys(toewijzing)</code>	Sleutels van toewijzing retourneren
<code>length(array)</code>	Lengte van array retourneren
<code>length(tekenreeks)</code>	Lengte van tekenreeks retourneren
<code>map_by(array, bewerking)</code>	<p>Retourneert elke arrayvermelding met een bewerking die op deze vermelding is toegepast</p> <pre>map_by([1,2], x => x * 10)</pre> <p>retourneert <code>[10, 20]</code></p> <pre>map_by([1,2], x => to_string(x))</pre> <p>retourneert <code>["1", "2"]</code></p> <pre>map_by({'key1':1, 'key2':2}, (k,v) => {k:v*10})</pre> <p>retourneert <code>[{"key1":10}, {"key2":20}]</code></p>
<code>map_to_object(array, sleutelnaam)</code>	<p>Retourneert een array met sleutelwaardeparen van de opgegeven sleutelnaam die zijn gekoppeld aan waarden uit een andere array</p> <pre>map_to_object(resource.Disk[*].id, "source")</pre> <p>Retourneert een array met sleutelwaardeparen die een sleutelveld heeft, bron genoemd, gekoppeld aan schijf-id-tekenreeksen</p> <p>Opmerking</p> <pre>map_by(resource.Disk[*].id, id => {'source':id})</pre> <p>retourneert hetzelfde resultaat</p>
<code>matches(tekenreeks, regex)</code>	Controleren of de tekenreeks overeenkomt met een regex-expressie
<code>max(array)</code>	Maximumwaarde van array met getallen retourneren
<code>merge(toewijzing, toewijzing)</code>	Een samengevoegde toewijzing retourneren
<code>min(array)</code>	Minimumwaarde uit array met getallen retourneren
<code>not_null(array)</code>	De eerste vermelding retourneren die niet leeg is

Tabel 6-1. Functies (vervolg)

Functie	Beschrijving
now()	Huidige tijd in ISO-8601-indeling retourneren
range(start, stop)	Retourneert een reeks getallen in stappen van 1 die beginnen met het beginnummer en eindigen net vóór het stopnummer
replace(tekenreeks, doel, vervanging)	Tekenreeks door doeltekenreeks vervangen
reverse(array)	Vermeldingen in array omkeren
slice(array, begin, einde)	Segment van array retourneren van beginindex tot eindindex
split(tekenreeks, scheidingsteken)	Tekenreeks met scheidingsteken splitsen en array met tekenreeksen retourneren
starts_with(onderwerp, voorvoegsel)	Controleren of de onderwerptekenreeks begint met de voorvoegseltekenreeks
substring(tekenreeks, begin, einde)	Subtekenreeks van tekenreeks vanaf de beginindex tot de eindindex retourneren
sum(array)	De som van alle waarden van de array met getallen retourneren
to_json(waarde)	Waarde als JSON-tekenreeks serialiseren
to_lower(tekenreeks)	Tekenreeks converteren naar kleine letters
to_number(tekenreeks)	Tekenreeks als getal parseren
to_string(waarde)	Tekenreeksweergave van de waarde retourneren
to_upper(tekenreeks)	Tekenreeks converteren naar hoofdletters
trim(tekenreeks)	Voorloop- en volgspaties verwijderen
url_encode(tekenreeks)	Tekenreeks coderen met behulp van URL-coderingsspecificatie
uuid()	Willekeurig gegenereerde UUID retourneren
values(toewijzing)	Waarden van toewijzing retourneren

Problemen oplossen

In de YAML-taal wordt een dubbele punt en spatie (': ') gebruikt als scheidingsteken tussen sleutel en waarde in sleutelwaardeparen. De expressiesyntax is afhankelijk van YAML, zodat een spatie na een dubbele punt er soms voor kan zorgen dat een expressie mislukt.

De spatie tussen "win" : en "lin" in de volgende expressie veroorzaakt bijvoorbeeld een fout.

```
${contains(input.image,"(Windows)" == true ? "win" : "lin")}
```

De werkende expressie laat de spatie weg.

```
${contains(input.image,"(Windows)" == true ? "win" : "lin")}
```

Als een expressie blijft mislukken, probeert u de volledige expressie binnen vinkjes te plaatsen, zoals weergegeven.

```
ezOS: '${contains(input.image,"(Windows)" == true ? "win" : "lin"}'
```

Geheime Cloud Assembly-eigenschappen

Een geheime Cloud Assembly-eigenschap is een herbruikbare, versleutelde waarde die projectgebruikers aan hun cloudsjabloonontwerpen kunnen toevoegen.

Beveiligde toegangssleutels en -verificatiegegevens zijn typische voorbeelden van geheime eigenschappen. Wanneer een geheime eigenschapswaarde is gemaakt en opgeslagen, kan deze nooit meer worden versleuteld of gelezen.

Een geheime eigenschap maken

- 1 Meld u aan bij Cloud Assembly met rechten voor de rol van projectbeheerder.
- 2 Ga naar **Infrastructuur > Beheer > Geheimen** en klik op **Nieuw geheim**.
- 3 Selecteer het project.
- 4 Voer een unieke eigenschapsnaam voor het geheim in, zonder spaties of speciale tekens.

De naam is de zichtbare id voor het geheim.

- 5 Voer de geheime waarde in.

Tijdens het typen wordt de waarde standaard verborgen. Zo is deze beschermt wanneer het scherm wordt gedeeld.

Indien nodig kunt u op het oogsymbool klikken om een waarde weer te geven en te controleren. Nadat een geheime waarde is opgeslagen, wordt deze versleuteld in de database en kan deze nooit opnieuw worden bekendgemaakt.

- 6 Geef eventueel een langere beschrijving van de geheime eigenschap op.
- 7 Klik op **Maken**.

The screenshot shows a 'Create Secret' dialog box. It includes a 'Project' dropdown menu set to 'admin-project', a 'Name' field containing 'ourPublicKey', a 'Value' field with a masked input (dots) and a toggle icon, and a 'Description' text area. At the bottom right, there are 'CANCEL' and 'CREATE' buttons.

Een geheime eigenschap toevoegen aan een cloudsjabloon

Projectgebruikers kunnen een geheime eigenschap toevoegen als binding in de cloudsjablooncode.

Wanneer u begint met het typen van de tekens voor `'${secret.'`, wordt een selectielijst met geheimen getoond die voor het project zijn gemaakt.

```
type: Cloud.Machine
properties:
  name: ourvm
  image: mint20
  flavor: small
  remoteAccess:
    authentication: publicPrivateKey
    sshKey: '${secret.ourPublicKey}'
    username: root
```

Zie [Een geheime Cloud Assembly-eigenschap in een Terraform-configuratie gebruiken](#) als u een geheime eigenschap wilt toevoegen aan een Terraform-configuratie.

Externe toegang tot een Cloud Assembly-implementatie

Om extern toegang te krijgen tot een machine die door Cloud Assembly is geïmplementeerd, voegt u eigenschappen vóór implementatie toe aan de cloudsjabloon voor die machine.

Voor externe toegang kunt u een van de volgende verificatieopties configureren.

Opmerking In gevallen waar sleutels moeten worden gekopieerd, kunt u ook een `cloudConfig`-gedeelte in de cloudsjabloon maken om de sleutels bij het inrichten automatisch te kopiëren. De details worden hier niet vermeld, maar [Machine-initialisatie in Cloud Assembly](#) biedt algemene informatie over `cloudConfig`.

Een sleutelpaar genereren tijdens het inrichten

Als u geen eigen openbare/persoonlijke sleutelpaar voor verificatie van externe toegang hebt, kunt u Cloud Assembly een sleutelpaar laten genereren.

Gebruik de volgende code als richtlijn.

- 1 Voeg voordat u begint met de inrichting in Cloud Assembly `remoteAccess`-eigenschappen toe aan de cloudsjabloon, zoals weergegeven in het voorbeeld.

De gebruikersnaam is optioneel. Als u deze weglaat, genereert het systeem een willekeurige id als gebruikersnaam.

Voorbeeld:

```
type: Cloud.Machine
properties:
  name: our-vm2
  image: Linux18
```

```

flavor: small
remoteAccess:
  authentication: generatedPublicPrivatekey
  username: testuser

```

- 2 In Cloud Assembly richt u de machine in vanaf de cloudsjabloon en brengt u deze naar de opgestarte status.

Het inrichtingsproces genereert de sleutels.

- 3 Zoek de sleutelnaam in de eigenschappen via **Resources > Implementaties > Topologie**.
- 4 Gebruik de cloudproviderinterface, zoals de vSphere-client, om toegang te krijgen tot de commandoregel voor de ingerichte machine.
- 5 Verleen leesrechten aan de persoonlijke sleutel.

```
chmod 600 key-name
```

- 6 Ga naar de Cloud Assembly-implementatie, selecteer de machine en klik op **Acties > Persoonlijke sleutel ophalen**.
- 7 Kopieer het bestand met de persoonlijke sleutel naar uw lokale machine.

Een typisch lokaal bestandspad is `/home/username/.ssh/ key-name`.

- 8 Open een externe SSH-sessie en maak verbinding met de ingerichte machine.

```
ssh -i key-name user-name@machine-ip
```

Uw eigen openbaar/persoonlijk sleutelpaar opgeven

Veel bedrijven maken en verdelen hun eigen openbare/persoonlijke sleutelparen voor verificatie.

Gebruik de volgende code als richtlijn.

- 1 Verkrijg of genereer uw openbaar/persoonlijk sleutelpaar in uw lokale omgeving.
Genereer nu alleen de sleutels en sla deze lokaal op.
- 2 Voeg voordat u begint met de inrichting in Cloud Assembly `remoteAccess`-eigenschappen toe aan de cloudsjabloon, zoals weergegeven in het voorbeeld.

De `sshKey` bevat de lange alfanumerieke tekens die worden gevonden in het bestand met de openbare sleutel `key-name.pub`.

De gebruikersnaam is optioneel en wordt voor u gemaakt om u aan te melden. Als u deze weglaat, genereert het systeem een willekeurige id als gebruikersnaam.

Voorbeeld:

```

type: Cloud.Machine
properties:
  name: our-vm1
  image: Linux18
  flavor: small
  remoteAccess:

```

```

authentication: publicPrivateKey
sshKey: ssh-rsa Iq+5aQgBP3ZNT4o1baP5Ii+dstIcowRRkyobbfpA1mj9tslf
qGxvU66PX9IeZax5hZvNWFgjw6ag+Z1zndOLhVdVoW49f274/mIRild7Uuw...
username: testuser

```

- 3 In Cloud Assembly richt u de machine in vanaf de cloudsjabloon en brengt u deze naar de opgestarte status.
- 4 Open de ingerichte machine met de client van de cloudleverancier.
- 5 Voeg het bestand met de openbare sleutel toe aan de basismap van de machine. Gebruik de sleutel die u in `remoteAccess.sshKey` hebt opgegeven.
- 6 Controleer of het overeenkomende bestand met de persoonlijke sleutel op uw lokale machine aanwezig is.

De sleutel is doorgaans `/home/username/.ssh/key-name` zonder `.pub`-extensie.

- 7 Open een externe SSH-sessie en maak verbinding met de ingerichte machine.

```
ssh -i key-name user-name@machine-ip
```

Een AWS-sleutelpaar opgeven

Door een AWS-sleutelpaarnaam aan de cloudsjabloon toe te voegen, kunt u op afstand toegang krijgen tot een machine die Cloud Assembly in AWS implementeert.

Houd er rekening mee dat AWS-sleutelparen specifiek zijn voor elke regio. Als u workloads in `us-east-1` inricht, moet het sleutelpaar in `us-east-1` bestaan.

Gebruik de volgende code als richtlijn. Deze optie werkt alleen voor AWS-cloudzones.

```

type: Cloud.Machine
properties:
  image: Ubuntu
  flavor: small
  remoteAccess:
    authentication: keyPairName
    keyPair: cas-test
constraints:
  - tag: 'cloud:aws'

```

Een gebruikersnaam en wachtwoord opgeven

Door een gebruikersnaam en wachtwoord aan de cloudsjabloon toe te voegen, kunt u op afstand eenvoudig toegang krijgen tot een machine die Cloud Assembly implementeert.

Hoewel het minder veilig is, is het voor uw situatie mogelijk voldoende dat u zich op afstand met een gebruikersnaam en wachtwoord aanmeldt. Houd er rekening mee dat sommige cloudleveranciers of -configuraties deze minder veilige optie mogelijk niet ondersteunen.

- 1 Voeg voordat u begint met de inrichting in Cloud Assembly `remoteAccess`-eigenschappen toe aan de cloudsjabloon, zoals weergegeven in het voorbeeld.

Stel de gebruikersnaam en het wachtwoord in op het account waarmee u wilt inloggen.

Voorbeeld:

```
type: Cloud.Machine
properties:
  name: our-vm3
  image: Linux18
  flavor: small
  remoteAccess:
    authentication: usernamePassword
    username: testuser
    password: admin123
```

- 2 In Cloud Assembly richt u de machine in vanaf de cloudsjabloon en brengt u deze naar de opgestarte status.
- 3 Ga naar de interface van uw cloudleverancier en open de ingerichte machine.
- 4 Maak het account of schakel het account in op de ingerichte machine.
- 5 Open vanaf uw lokale machine een externe sessie op het IP-adres van de ingerichte machine of FQDN en meld u op de gebruikelijke wijze aan met de gebruikersnaam en het wachtwoord.

SCSI-schijfplaatsing met Cloud Assembly

Als u een SCSI-schijf wilt beheren, moet u de SCSI-controller en het LUN-nummer (Logical Unit Number) opgeven en weten. Voor een vSphere-schijfobject kunt u Cloud Assembly gebruiken om beide waarden in de cloudsjabloon toe te wijzen.

De mogelijkheid om verschillende SCSI-controllers te gebruiken is belangrijk voor de prestaties. Dit is vereist voor sommige implementatietypen, zoals Oracle Real Application Clusters (RAC).

Eigenschappen voor SCSI-controller en LUN-schijf

Als u een SCSI-controller en LUN wilt toewijzen, voegt u de volgende eigenschappen voor een cloudsjabloon toe:

SCSIController

unitNumber

U hebt ook de optie om de eigenschappen weg te laten, waarbij de toewijzing een voorspelbare standaard volgt. Cloud Assembly implementeert SCSI-schijven niet langer in willekeurige volgorde, waardoor ze moeilijk te beheren waren.

SCSI-controllers en -schijven worden in volgorde genummerd, beginnend vanaf nul. Elke SCSI-controller kan SCSI-schijven met eenheidsnummers van 0 t/m 15 ondersteunen.

Optie 1: zowel SCSI-controller als eenheidsnummer instellen

U kunt beide eigenschappen volledig opgeven, zoals in het volgende voorbeeld wordt weergegeven. Zo ja, dan komen de toewijzing van de SCSI-controller en het eenheidsnummer overeen met de waarden die u invoert.

```
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      cpuCount: 1
      totalMemoryMB: 1024
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
        - source: '${resource.Cloud_vSphere_Disk_2.id}'
        - source: '${resource.Cloud_vSphere_Disk_3.id}'
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
      SCSIController: SCSI_Controller_2
      unitNumber: 0
  Cloud_vSphere_Disk_2:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
      SCSIController: SCSI_Controller_2
      unitNumber: 1
  Cloud_vSphere_Disk_3:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
      SCSIController: SCSI_Controller_3
      unitNumber: 4
```

Optie 2: alleen de SCSI-controller instellen

U kunt de SCSI-controller opgeven en het eenheidsnummer weglaten. In dit geval komt de toewijzing van de SCSI-controller overeen met de waarde die u invoert. Het eenheidsnummer wordt ingesteld op het eerste beschikbare eenheidsnummer onder die controller.

```
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      cpuCount: 1
      totalMemoryMB: 1024
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
        - source: '${resource.Cloud_vSphere_Disk_2.id}'
        - source: '${resource.Cloud_vSphere_Disk_3.id}'
```

```

Cloud_vSphere_Disk_1:
  type: Cloud.vSphere.Disk
  properties:
    capacityGb: 1
    SCSIController: SCSI_Controller_0
Cloud_vSphere_Disk_2:
  type: Cloud.vSphere.Disk
  properties:
    capacityGb: 1
    SCSIController: SCSI_Controller_0
Cloud_vSphere_Disk_3:
  type: Cloud.vSphere.Disk
  properties:
    capacityGb: 1
    SCSIController: SCSI_Controller_1

```

Optie 3: beide eigenschappen weglaten

U kunt de SCSI-controller en het eenheidsnummer weglaten. In dit geval wordt de toewijzing ingesteld op de eerste beschikbare SCSI-controller en het eerste beschikbare eenheidsnummer onder die controller.

```

resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      cpuCount: 1
      totalMemoryMB: 1024
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
        - source: '${resource.Cloud_vSphere_Disk_2.id}'
        - source: '${resource.Cloud_vSphere_Disk_3.id}'
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Disk_2:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Disk_3:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1

```

Geen optie: alleen LUN

U kunt de SCSI-controller niet weglaten en alleen een eenheidsnummer opgeven. Als u dit doet, kan dit resulteren in een implementatie waarbij meerdere SCSI-controllers een schijf met dat nummer hebben, maar waarbij u voor beheerdoeleinden niet weet welke schijf dewelke is.

Invoer gebruiken om de SCSI-controller en het LUN in te stellen

Om het ontwerp dynamischer te maken, gebruikt u invoer, zodat de gebruiker tijdens de aanvraag of update het SCSI-controller en eenheidsnummer kan opgeven.

```
inputs:
  diskProperties:
    type: array
    minItems: 1
    maxItems: 10
    items:
      type: object
      properties:
        size:
          type: integer
        SCSIController:
          type: string
          title: SCSI Controller
          enum:
            - SCSI_Controller_0
            - SCSI_Controller_1
            - SCSI_Controller_2
            - SCSI_Controller_3
        unitNumber:
          type: integer
          title: Unit Number

resources:
  app:
    type: Cloud.vSphere.Machine
    allocatePerInstance: true
    properties:
      flavor: small
      image: centos
      attachedDisks: '${map_to_object(slice(resource.disk[*].id, 0, 4), 'source')}'
  disk:
    type: Cloud.vSphere.Disk
    allocatePerInstance: true
    properties:
      capacityGb: '${input.diskProperties[count.index].size}'
      SCSIController: '${input.diskProperties[count.index].SCSIController}'
      unitNumber: '${input.diskProperties[count.index].unitNumber}'
      count: ${length(input.diskProperties)}
```

size	<input type="text" value="1"/>
SCSI Controller	<input type="text" value="SCSI_Controller_0"/> ▼
Unit Number	<input type="text" value="2"/>

Machine-initialisatie in Cloud Assembly

U kunt machine-initialisatie toepassen in Cloud Assembly door opdrachten rechtstreeks uit te voeren of, via aanpassingsspecificaties bij een implementatie in vSphere-gebaseerde cloudzones.

Hoe werken opdrachten en aanpassingsspecificaties

- **Commando's (Commands)**

Een cloudConfig-sectie in uw cloudsjablooncode bevat de opdrachten die u wilt uitvoeren.

- **Aanpassingsspecificaties**

Een eigenschap in uw cloudsjablooncode verwijst naar een vSphere-aanpassingsspecificatie op naam.

Opdrachten en aanpassingsspecificaties kunnen mogelijk niet door elkaar worden gebruikt

Wanneer u in vSphere implementeert, moet u goed opletten als u probeert de initialisatie van cloudConfig en aanpassingsspecificaties te combineren. Deze zijn niet formeel compatibel en kunnen inconsistente of ongewenste resultaten opleveren wanneer deze samen worden gebruikt.

Zie [Statische IP-adressen van vSphere in Cloud Assembly](#) voor een voorbeeld van interactie tussen opdrachten en aanpassingsspecificaties.

vSphere-aanpassingsspecificaties in Cloud Assembly-sjablonen

Als u implementeert op vSphere-gebaseerde cloudzones in Cloud Assembly, kunnen tijdens de implementatie aanpassingsspecificaties worden gebruikt om instellingen voor het gastbesturingssysteem toe te passen.

De aanpassingsspecificatie inschakelen

De aanpassingsspecificatie moet in vSphere bestaan, op het doel waarop u implementeert.

Bewerk de cloudsjablooncode direct. In het volgende voorbeeld wordt verwezen naar een `cloud-assembly-linux-aanpassingsspecificatie` voor een WordPress-host in vSphere.

```
resources:
  WebTier:
    type: Cloud.vSphere.Machine
    properties:
      name: wordpress
      cpuCount: 2
      totalMemoryMB: 1024
      imageRef: 'Template: ubuntu-18.04'
      customizationSpec: 'cloud-assembly-linux'
      folderName: '/Datacenters/Datacenter/vm/deployments'
```

Of u aanpassingsspecificaties of cloudConfig-opdrachten moet gebruiken

Als u wilt dat het inrichtingsproces overeenkomt met wat u momenteel in vSphere doet, blijft het gebruik van aanpassingsspecificaties de beste benadering. Als u het proces echter wilt uitbreiden naar hybride of meervoudige cloudinrichting, is het gebruik van cloudConfig-initialisatieopdrachten een meer neutrale benadering.

Zie [Configuratieopdrachten in Cloud Assembly-sjablonen](#) voor meer informatie over cloudConfig-secties in cloudsjablonen.

Opdrachten en aanpassingsspecificaties kunnen mogelijk niet door elkaar worden gebruikt

Wanneer u in vSphere implementeert, moet u goed opletten als u initialisatie van de ingesloten opdrachten en aanpassingsspecificaties probeert te combineren. Deze zijn niet formeel compatibel en kunnen inconsistente of ongewenste resultaten opleveren wanneer deze samen worden gebruikt.

Zie [Statische IP-adressen van vSphere in Cloud Assembly](#) voor een voorbeeld van interactie tussen opdrachten en aanpassingsspecificaties.

Configuratieopdrachten in Cloud Assembly-sjablonen

U kunt een cloudConfig-sectie toevoegen aan de code van een Cloud Assembly-sjabloon, waarin u machine-initialisatieopdrachten toevoegt die worden uitgevoerd tijdens de implementatie.

cloudConfig-opdrachtnotaties

- Linux — initialisatieopdrachten volgen de open [cloud-init](#)-standaard.
- Windows — initialisatieopdrachten maken gebruik van [Cloudbase-init](#).

[cloud-init](#) voor Linux en [cloudbase-init](#) voor Windows hebben niet dezelfde syntaxis. Een sectie cloudConfig voor één besturingssysteem werkt niet in een machine-image van het andere besturingssysteem.

Wat cloudConfig-opdrachten kunnen doen

U gebruikt initialisatieopdrachten om de applicatie van gegevens of instellingen te automatiseren tijdens het maken van een instantie, waarmee gebruikers, rechten, installaties of andere bewerkingen op basis van opdrachten kunnen worden aangepast. Voorbeelden zijn:

- Een hostnaam instellen
- Persoonlijke SSH-sleutels genereren en instellen
- Pakketten installeren

Waar cloudConfig-opdrachten kunnen worden toegevoegd

U kunt een cloudConfig-sectie toevoegen aan de code van een cloudsjabloon, maar u kunt er vooraf ook een aan een machine-image toevoegen bij het configureren van de infrastructuur. Alle cloudsjablonen die naar de bronimage verwijzen, krijgen dan dezelfde initialisatie.

Mogelijk hebt u een imageroewijzing en een cloudsjabloon die allebei initialisatieopdrachten bevatten. Tijdens de implementatie worden de opdrachten samengevoegd en voert Cloud Assembly de geconsolideerde opdrachten uit.

Wanneer dezelfde opdracht op beide plaatsen wordt weergegeven maar andere parameters bevat, wordt alleen de opdracht van de imageroewijzing uitgevoerd.

Zie [Meer informatie over imageroewijzingen in vRealize Automation](#) voor meer informatie.

Voorbeeld van cloudConfig-opdrachten

Het volgende voorbeeld van een cloudConfig-sectie komt uit de cloudsjablooncode van [Een basiscloudsjabloon maken](#) voor de op Linux gebaseerde MySQL-server.

Opmerking Om de juiste interpretatie van commando's te garanderen, moet u altijd het sluitsteken `cloudConfig: |` toevoegen, zoals getoond.

```
cloudConfig: |
#cloud-config
repo_update: true
repo_upgrade: all
packages:
- apache2
- php
- php-mysql
- libapache2-mod-php
- php-mcrypt
- mysql-client
runcmd:
- mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
mywordpresssite --strip-components 1
- i=0; while [ $i -le 5 ]; do mysql --connect-timeout=3 -h $
{DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;
i=$((i+1)); done
```

```

- mysql -u root -pmysqlpassword -h ${DBTier.networks[0].address} -e "create database
wordpress_blog;"
- mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/
mywordpresssite/wp-config.php
- sed -i -e s/"define( 'DB_NAME', 'database_name_here' );"/"define( 'DB_NAME',
'wordpress_blog' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_USER', 'username_here' );"/"define( 'DB_USER',
'root' );"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
-e s/"define( 'DB_PASSWORD', 'password_here' );"/"define( 'DB_PASSWORD',
'mysqlpassword' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_HOST', 'localhost' );"/"define( 'DB_HOST', '$
${DBTier.networks[0].address}' );"/ /var/www/html/mywordpresssite/wp-config.php
- service apache2 reload

```

Als een cloud-init-script zich onverwacht gedraagt, controleert u de vastgelegde console-uitvoer in `/var/log/cloud-init-output.log` bij het oplossen van problemen. Zie de [documentatie voor cloud-init](#) voor meer informatie over cloud-init.

Opdrachten en aanpassingsspecificaties kunnen mogelijk niet door elkaar worden gebruikt

Wanneer u in vSphere implementeert, moet u goed opletten als u initialisatie van de ingesloten opdrachten en aanpassingsspecificaties probeert te combineren. Deze zijn niet formeel compatibel en kunnen inconsistente of ongewenste resultaten opleveren wanneer deze samen worden gebruikt.

Zie [Statische IP-adressen van vSphere in Cloud Assembly](#) voor een voorbeeld van interactie tussen opdrachten en aanpassingsspecificaties.

vSphere-sjablonen voor initialisatie in Cloud Assembly

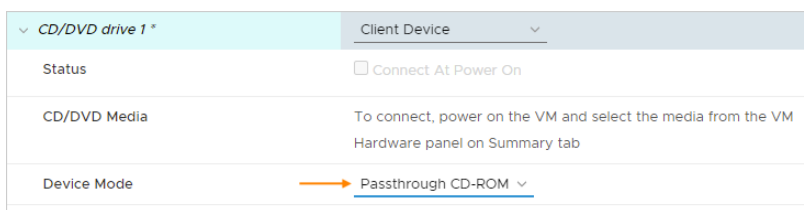
Wanneer uw Cloud Assembly-sjabloon een image implementeert op basis van een vSphere-sjabloon, moet de vSphere-sjabloon vooraf worden geconfigureerd om cloud-init te ondersteunen.

Als u een vSphere-sjabloon wilt configureren om cloud-init te ondersteunen, voert u de volgende stappen uit.

- 1 Installeer cloud-init op de virtuele machine die de sjabloon wordt.

Gebruik bijvoorbeeld `yum` om cloud-init in CentOS te installeren of `apt-get` om in Ubuntu te installeren.

- 2 Stel de cd-rom van de virtuele machine in op passthroughmodus.



- 3 Voer `cloud-init clean` uit op de commandoregel van het gastbesturingssysteem.

Opmerking Als `cloud-init clean` is voltooid, mag u de virtuele machine niet verder aanpassen.

- 4 Sluit de virtuele machine af en converteer deze naar een sjabloon.

Statische IP-adressen van vSphere in Cloud Assembly

Wanneer u vanuit Cloud Assembly implementeert in vSphere, kunt u een statisch IP-adres toewijzen, maar moet u ervoor zorgen dat er geen conflicten ontstaan tussen de cloudConfig-initialisatieopdrachten en aanpassingsspecificaties.

Voorbeeldontwerpen

De volgende ontwerpen passen op veilige wijze een statisch IP-adres toe zonder conflicten tussen initialisatieopdrachten voor cloudsjablonen en aanpassingsspecificaties. Ze bevatten allemaal de netwerkinstelling `assignment: static`.

Ontwerp	Voorbeeld van een cloudsjablooncode
<p>Een statisch IP-adres toewijzen aan een Linux-machine zonder cloud-init-code</p>	<pre>resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: linux-template networks: - name: '\${wpnet.name}' assignment: static network: '\${resource.wpnet.id}'</pre>
<p>Wijz een statisch IP-adres toe aan een Linux-machine met cloud-init-code die geen opdrachten voor netwerktoewijzing bevat.</p> <p>OPMERKING: de vSphere-aanpassingsspecificatie wordt toegepast, ongeacht of u de eigenschap customizeGuestOs op waar instelt of de eigenschap customizeGuestOs weglaat.</p>	<p>Ubuntu-voorbeeld</p> <pre>resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu-template customizeGuestOs: true cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: root:Pa\$\$w0rd expire: false write_files: - path: /tmpFile.txt content: \${resource.wpnet.dns} runcmd: - hostnamectl set-hostname --pretty \$ {self.resourceName} - touch /etc/cloud/cloud-init.disabled networks: - name: '\${wpnet.name}' assignment: static network: '\${resource.wpnet.id}'</pre> <p>CentOS-voorbeeld</p> <pre>resources: wpnet: type: Cloud.Network properties:</pre>

Ontwerp**Voorbeeld van een cloudsjablooncode**

```
name: wpnet
networkType: public
constraints:
  - tag: sqa
DBTier:
type: Cloud.vSphere.Machine
properties:
  flavor: small
  image: centos-template
  customizeGuestOs: true
  cloudConfig: |
    #cloud-config
    write_files:
      - path: /test.txt
        content: |
          deploying in power off.
          then rebooting.
networks:
  - name: '${wpnet.name}'
    assignment: static
    network: '${resource.wpnet.id}'
```


Ontwerp	Voorbeeld van een cloudsjablooncode
<p>Wijs een statisch IP-adres toe aan een Linux-machine met cloud-init-code die netwerktoewijzingsopdrachten bevat. De eigenschap <code>customizeGuestOs</code> moet onwaar zijn.</p>	<p>Ubuntu-voorbeeld</p> <pre> resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu-template customizeGuestOs: false cloudConfig: #cloud-config write_files: - path: /etc/netplan/99-installer- config.yaml content: network: version: 2 renderer: networkd ethernet: ens160: addresses: - \${resource.DBTier.networks[0].address}/\${ {resource.wpnet.prefixLength} gateway4: \$ {resource.wpnet.gateway} nameservers: search: \$ {resource.wpnet.dnsSearchDomains} addresses: \${resource.wpnet.dns} runcmd: - netplan apply - hostnamectl set-hostname --pretty \$ {self.resourceName} - touch /etc/cloud/cloud-init.disabled networks: - name: '\${wpnet.name}' assignment: static network: '\${resource.wpnet.id}' </pre> <p>CentOS-voorbeeld</p> <pre> resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: centos-template </pre>

Ontwerp**Voorbeeld van een cloudsjablooncode**

```

customizeGuestOs: false
cloudConfig: |
  #cloud-config
  ssh_pwauth: yes
  chpasswd:
    list: |
      root:VMware1!
    expire: false
  runcmd:
    - nmcli con add type
ethernet con-name 'custom ens192'
ifname ens192 ip4 ${self.networks[0].address}/
${resource.wpnet.prefixLength} gw4 $
{resource.wpnet.gateway}
  - nmcli con mod 'custom ens192' ipv4.dns "$
{join(resource.wpnet.dns, ' ')}"
  - nmcli con mod 'custom ens192' ipv4.dns-
search "${join(resource.wpnet.dnsSearchDomains, ',')}"
  - nmcli con down 'System ens192' ; nmcli
con up 'custom ens192'
  - nmcli con del 'System ens192'
  - hostnamectl set-hostname --static `dig -x
${self.networks[0].address} +short | cut -d "." -f 1`
  - hostnamectl set-hostname --pretty $
{self.resourceName}
  - touch /etc/cloud/cloud-init.disabled
networks:
  - name: '${wpnet.name}'
    assignment: static
    network: '${resource.wpnet.id}'

```

Wanneer u de implementatie baseert op een verwezen image, wijst u een statisch IP-adres toe aan een Linux-machine met cloud-init-code die netwerktoewijzingsopdrachten bevat.

De eigenschap `customizeGuestOs` moet onwaar zijn. Bovendien mag de cloudsjabloon de eigenschap `ovfProperties` niet bevatten, omdat deze aanpassing blokkeert.

```

resources:
  wpnet:
    type: Cloud.Network
    properties:
      name: wpnet
      networkType: public
      constraints:
        - tag: sqa
  DBTier:
    type: Cloud.vSphere.Machine
    properties:
      flavor: small

imageRef: 'https://cloud-images.ubuntu.com/releases/focal/release/ubuntu-20.04-server-cloudimg-amd64.ova'
customizeGuestOs: false
cloudConfig: |
  #cloud-config
  ssh_pwauth: yes
  chpasswd:
    list: |
      root:Pa$$w0rd
      ubuntu:Pa$$w0rd
    expire: false
  write_files:
    - path: /etc/netplan/99-netcfg-vrac.yaml
      content: |
        network:
          version: 2
          renderer: networkd

```

Ontwerp	Voorbeeld van een cloudsjablooncode
	<pre> ethernets: ens192: dhcp4: no dhcp6: no addresses: - \${resource.DBTier.networks[0].address}/\${ {resource.wpnet.prefixLength} gateway4: \$ {resource.wpnet.gateway} nameservers: search: \$ {resource.wpnet.dnsSearchDomains} addresses: \${resource.wpnet.dns} runcmd: - netplan apply - hostnamectl set-hostname --pretty \$ {self.resourceName} - touch /etc/cloud/cloud-init.disabled networks: - name: '\${wpnet.name}' assignment: static network: '\${resource.wpnet.id}' </pre>

Ontwerpen die niet werken of ongewenste resultaten kunnen opleveren

- De cloud-init-code bevat geen netwerktoewijzingsopdrachten en de eigenschap `customizeGuestOs` is onwaar.
Er zijn geen initialisatieopdrachten en aanpassingsspecificaties aanwezig om de netwerkinstellingen te configureren.
- De cloud-init-code bevat geen netwerktoewijzingsopdrachten en de eigenschap `ovfProperties` is ingesteld.
Initialisatieopdrachten zijn niet aanwezig, maar `ovfProperties` heeft de aanpassingsspecificatie geblokkeerd.
- De cloud-init-code bevat netwerktoewijzingsopdrachten en de eigenschap `customizeGuestOs` ontbreekt of is ingesteld op waar.
Toepassing van de aanpassingsspecificatie is in strijd met initialisatieopdrachten.

Andere tijdelijke oplossingen voor cloud-init en aanpassingsspecificaties

Wanneer u implementeert op vSphere, kunt u ook een image aanpassen om conflicten met cloud-init en aanpassingsspecificaties te vermijden. Zie de volgende externe opslagplaats voor meer informatie.

- [vSphere-imagevoorbereidingsscripts](#)

Vertraagde implementatie in Cloud Assembly

Mogelijk moet een virtuele machine volledig worden geïnitieerd voordat verder kan worden gegaan met de Cloud Assembly-implementatie.

Bijvoorbeeld: als u een machine implementeert waarvoor nog steeds pakketten worden geïnstalleerd en het starten van een webserver kan leiden tot situaties waarin een snelle gebruiker probeert de applicatie te bereiken voordat deze beschikbaar is.

Houd rekening met de volgende overwegingen wanneer u deze functie gebruikt.

- De functie gebruikt de module `phone_home` van [cloud-init](#) en is beschikbaar tijdens het implementeren van Linux-machines.
- Phone home is niet beschikbaar voor Windows vanwege beperkingen van [Cloudbase-init](#).
- Phone home kan invloed hebben op de implementatievolgorde zoals een expliciete afhankelijkheid, maar heeft meer flexibiliteit voor timing- en verwerkingsopties.
Zie [Bindingen en afhankelijkheden maken tussen resources in Cloud Assembly](#).
- Voor phone home is een `cloudConfig`-sectie in de cloudsjabloon vereist.
- Uw creativiteit is een factor. Initialisatieopdrachten kunnen een ingesloten wachttijd tussen bewerkingen bevatten, die in combinatie met phone home kan worden gebruikt.
- Phone home op basis van cloudsjablonen werkt niet als de machinesjabloon al instellingen voor de module `phone_home` bevat.
- De machine moet uitgaande communicatietoegang tot Cloud Assembly hebben.

Om een vertraagde implementatie in Cloud Assembly mogelijk te maken, voegt u een `cloudConfigSettings`-sectie toe aan de cloudsjabloon:

```
cloudConfigSettings:
  phoneHomeShouldWait: true
  phoneHomeTimeoutSeconds: 600
  phoneHomeFailOnTimeout: true
```

Eigenschap	Beschrijving
<code>phoneHomeShouldWait</code>	Of wordt gewacht op de initialisatie, waar of onwaar.
<code>phoneHomeTimeoutSeconds</code>	Wanneer moet worden beslist om door te gaan met de implementatie, zelfs als de initialisatie nog steeds wordt uitgevoerd. De standaardwaarde is 10 minuten.
<code>phoneHomeFailOnTimeout</code>	Of moet worden doorgedaan met de implementatie na een time-out, waar of onwaar. Houd er rekening mee dat de implementatie ook wanneer deze wordt voortgezet, alsnog om andere redenen kan mislukken.

Windows-gast aanpassen in Cloud Assembly

Als u wilt dat Cloud Assembly een Windows-machine automatisch initialiseert tijdens de implementatie, bereidt u een image voor die cloudbase-init ondersteunt en vervolgens een cloudsjabloon die de juiste opdrachten bevat.

Het proces voor het maken van images varieert afhankelijk van de cloudleverancier. Het voorbeeld dat hier wordt weergegeven, is voor vSphere.

Windows Cloud Assembly-image voor vSphere

Als u wilt dat Cloud Assembly een Windows-machine initialiseert die is geïmplementeerd op vSphere, moet de image zijn gebaseerd op een vSphere-sjabloon met cloudbase-init geïnstalleerd en geconfigureerd.

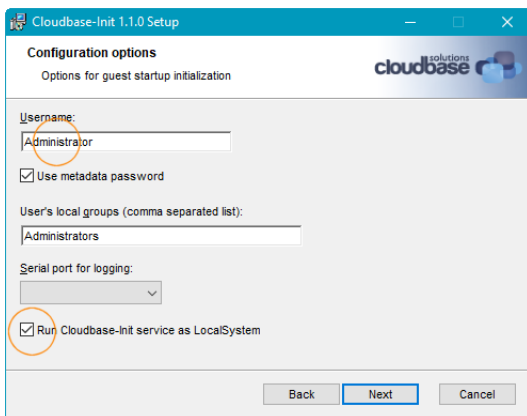
De image maken

- 1 Gebruik vSphere om een virtuele Windows-machine te maken en in te schakelen.
- 2 Meld u op de virtuele machine aan bij Windows.
- 3 Download Cloudbase-Init.

<https://cloudbase.it/cloudbase-init/#download>

- 4 Start het .msi-bestand voor de installatie van cloudbase-init.

Tijdens de installatie voert u **Administrator** in als gebruikersnaam en selecteert u de optie om als LocalSystem uit te voeren.



Andere instelselecties kunnen als standaardwaarden behouden blijven.

- 5 Voer de installatie uit, maar sluit de laatste pagina Voltooid van de instelwizard niet.

Belangrijk Sluit de laatste pagina van de instelwizard niet.

- 6 Ga, met de pagina Voltooid van de instelwizard nog steeds geopend, in Windows naar het installatiepad voor cloudbase-init en open het volgende bestand in een teksteditor.

```
conf\cloudbase-init-unattend.conf
```

- 7 Stel `metadata_services` in op `OvfService` zoals weergegeven. Voeg de instelling toe als deze nog niet bestaat.

```
metadata_services=cloudbaseinit.metadata.services.ovfservice.OvfService
```

- 8 Sla op en sluit `cloudbase-init-unattend.conf`.
- 9 Open het volgende bestand in dezelfde map in een teksteditor.

```
conf\cloudbase-init.conf
```

- 10 Stel `first_logon_behaviour`, `metadata_services` en `plugins` in zoals weergegeven. Voeg de instellingen toe als ze nog niet bestaan.

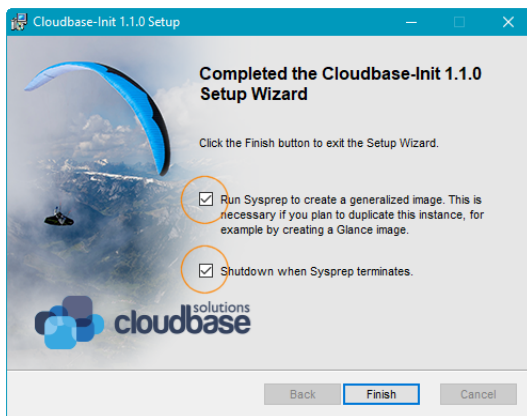
```
first_logon_behaviour=always
. . .
metadata_services=cloudbaseinit.metadata.services.ovfservice.OvfService
. . .
plugins=cloudbaseinit.plugins.windows.createuser.CreateUserPlugin,cloudbaseinit.plugins.win
dows.setuserpassword.SetUserPasswordPlugin,cloudbaseinit.plugins.common.sshpublickeys.SetUs
erSSHPublicKeysPlugin,cloudbaseinit.plugins.common.userdata.UserDataPlugin
. . .
```

- 11 Sla op en sluit `cloudbase-init.conf`.
- 12 Selecteer op de pagina Voltooid van de instelwizard de opties om Sysprep uit te voeren en af te sluiten na Sysprep en klik vervolgens op **Voltooien**.

Opmerking VMware heeft situaties gezien waarbij het uitvoeren van Sysprep voorkomt dat implementaties van de image werken.

Bij de implementatie past Cloud Assembly een dynamisch gegenereerde aanpassingsspecificatie toe, waardoor de netwerkiterface wordt losgekoppeld. De in behandeling zijnde Sysprep-status in de image kan ertoe leiden dat de aanpassingsspecificatie mislukt en de implementatie niet wordt verbonden.

Als u vermoedt dat dit gebeurt in uw omgeving, probeert u de Sysprep-opties uitgeschakeld te houden tijdens het maken van de image.



- 13 Nadat de virtuele machine is afgesloten, gebruikt u vSphere om er een sjabloon van te maken.

Extra details

De volgende tabel wordt uitgevouwen bij de configuratievermeldingen die tijdens het instellen zijn gemaakt.

Configuratie-instelling	Doel
Gebruikersnaam, CreateUserPlugin en SetUserPasswordPlugin	Na Sysprep gebruikt de eerste opstartprocedure CreateUserPlugin om het account met de gebruikersnaam Administrator te maken met een leeg wachtwoord. SetUserPasswordPlugin staat cloudbase-init toe om het lege wachtwoord te wijzigen in het externe toegangswachtwoord dat wordt opgenomen in de cloudsjabloon.
Gedrag bij eerste aanmelding	Deze instelling vraagt de gebruiker om het wachtwoord te wijzigen bij de eerste aanmelding.
Metagegevensservices	Door alleen OvfService weer te geven, zal cloudbase-init niet proberen andere metagegevensservices te vinden die niet worden ondersteund in vCenter. Dit resulteert in overzichtelijkere logboekbestanden, omdat de logboeken anders vol zouden staan met vermeldingen over mislukte pogingen om deze andere services te vinden.
Plug-ins	Door alleen plug-ins met door OvfService ondersteunde mogelijkheden weer te geven, zijn logboeken opnieuw overzichtelijker. Cloudbase-init voert invoegtoepassingen uit in de opgegeven volgorde.
Uitvoeren als LocalSystem	Deze instelling ondersteunt geavanceerde initialisatieopdrachten die mogelijk vereisen dat cloudbase-init wordt uitgevoerd onder een specifiek beheerdersaccount.

Cloudbase-init-opdrachten voor Windows in Cloud Assembly

Om een Windows machine-initialisatie uit te voeren tijdens het implementeren, voegt u cloudbase-init-opdrachten toe aan de Cloud Assembly-sjablooncode.

Het voorbeeld dat hier wordt weergegeven, is gebaseerd op vSphere, maar andere cloudleveranciers zijn vergelijkbaar.

Vereisten

- Maak infrastructuur. Voeg in Cloud Assembly uw vSphere-cloudaccount en een gekoppelde cloudzone toe.
- Voeg soort- en imageroewijzingen toe en voeg netwerk- en opslagprofielen toe.

In uw infrastructuur moet een imageroewijzing verwijzen naar een Windows-sjabloon die u hebt gemaakt om cloudbase-init te ondersteunen. Zie [Windows Cloud Assembly-image voor vSphere](#).

Als de sjabloon niet wordt weergegeven, gaat u naar cloudaccounts en synchroniseert u images. Anders wordt automatische synchronisatie elke 24 uur uitgevoerd.

- Voeg een project toe, voeg gebruikers toe en zorg ervoor dat de gebruikers in uw cloudzone kunnen inrichten.

Zie de voorbeelden in het [Tutorial: Infrastructuur en implementaties met meerdere clouds instellen en testen in Cloud Assembly](#) voor meer informatie over het maken van infrastructuur en projecten.

Procedure

- 1 Ga in Cloud Assembly naar het tabblad **Ontwerp** en maak een nieuwe cloudsjabloon.
- 2 Voeg een sectie `cloudConfig` toe met de cloudbase-init-opdrachten die u wilt.

In de volgende opdrachtvoorbeelden wordt een nieuw bestand gemaakt op het `C:`-station in Windows en wordt de hostnaam ingesteld.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: cloudbase-init-win-2016
      flavor: small
      remoteAccess:
        authentication: usernamePassword
        username: Administrator
        password: Password1234@$
      cloudConfig: |
        #cloud-config
        write_files:
          content: Cloudbase-Init test
          path: C:\test.txt
          set_hostname: testname
```

Zie de [documentatie voor Cloudbase-init](#) voor meer informatie.

- 3 Voeg `remoteAccess`-eigenschappen toe zodat u de machine kunt configureren voor de eerste aanmelding bij Windows.

Zoals vermeld bij het maken van de sjabloon worden door de metagegevensservice de verificatiegegevens opgehaald en worden deze beschikbaar gemaakt voor `CreateUserPlugin` en `SetUserPasswordPlugin`. Het wachtwoord moet voldoen aan de vereisten voor Windows-wachtwoorden.

- 4 Test en implementeer de cloudsjabloon vanaf Cloud Assembly.
- 5 Na het implementeren gebruikt u Windows RDP en de verificatiegegevens in de sjabloon om u aan te melden bij de nieuwe Windows-machine en de aanpassing te verifiëren.

In het vorige voorbeeld moet u het `C:\test.txt`-bestand opzoeken en de systeemeigenschappen voor de hostnaam controleren.

Machine- en schijfclusters in Cloud Assembly

Cloud Assembly-sjabloonontwerpen kunnen een cluster van machines implementeren en een cluster van schijven koppelen.

Als u clusters van machines en schijven wilt implementeren, maakt u gebruik van de [Cloud Assembly-resourcevlaggen voor aanvragen](#) `allocatePerInstance`, en `count.index` en [Syntaxis voor Cloud Assembly-expressie](#) `map_to_object` in uw cloudsjablonen.

De volgende voorbeelden van cloudsjablooncode kunnen fungeren als richtlijnen voor ontwerpen die clusters implementeren.

Twee machines die een schijfcluster delen

```
resources:
  app0:
    type: Cloud.Machine
    allocatePerInstance: true
    properties:
      image: ubuntu
      flavor: small
      attachedDisks: '${map_to_object(slice(resource.disk[*].id, 0,2), "source")}'
  appl:
    type: Cloud.Machine
    allocatePerInstance: true
    properties:
      image: ubuntu
      flavor: small
      attachedDisks: '${map_to_object(slice(resource.disk[*].id, 2,4), "source")}'
  disk:
    type: Cloud.Volume
    allocatePerInstance: true
    properties:
      count: 4
      capacityGb: 5
```

Variabel aantal machines met elk één schijf

```
inputs:
  count:
    type: integer
    default: 2
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    allocatePerInstance: true
    properties:
      image: ubuntu
      flavor: small
      count: '${input.count}'
      attachedDisks: '${map_to_object(slice(resource.disk[*].id, count.index, count.index + 1), "source")}'
```

```

disk:
  type: Cloud.Volume
  allocatePerInstance: true
  properties:
    count: '${input.count}'
    capacityGb: 5

```

Variabel aantal machines met elk twee schijven

```

inputs:
  count:
    type: integer
    default: 2
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    allocatePerInstance: true
    properties:
      image: ubuntu
      flavor: small
      count: ${input.count}
      attachedDisks: '${map_to_object(slice(resource.disk[*].id, 2*count.index,
2*(count.index + 1)), "source")}'
    disk:
      type: Cloud.Volume
      allocatePerInstance: true
      properties:
        count: ${2*input.count}
        capacityGb: 5

```

Schijfgrootte instellen op het moment van de aanvraag

```

inputs:
  disksize:
    type: array
    minItems: 2
    maxItems: 2
    items:
      type: object
      properties:
        size:
          type: integer
resources:
  app:
    type: Cloud.Machine
    allocatePerInstance: true
    properties:
      flavor: small
      image: ubuntu
      attachedDisks: ${map_to_object(slice(resource.disk[*].id, 0, 2), 'source')}
    disk:
      type: Cloud.Volume

```

```
allocatePerInstance: true
properties:
  count: 2
  capacityGb: ${input.disksize[count.index].size}
```

Aangepaste naamgeving voor geïmplementeerde resources in Cloud Assembly

Als cloud- of projectbeheerder hebt u een voorgeschreven naamgevingsconventie voor resources in uw omgeving en u wilt dat de geïmplementeerde resource deze conventies zonder gebruikersinteractie volgt. U kunt een naamgevingssjabloon maken voor alle implementaties van een Cloud Assembly-project.

Uw naamgevingsconventie voor hosts bestaat er bijvoorbeeld in om als volgt het voorvoegsel te gebruiken bij een resource *projectname-sitecode-costcenter-whereDeployed-identifier*. U configureert de sjabloon voor de aangepaste naamgeving voor de machines voor elk project. Sommige sjabloonvariabelen worden opgehaald uit het systeem wanneer het wordt geïmplementeerd, andere zijn gebaseerd op aangepaste projecteigenschappen. De aangepaste naamgevingssjabloon voor bovenstaand voorvoegsel ziet er ongeveer uit zoals in het volgende voorbeeld.

```
${project.name}-${resource.siteCode}-${resource.costCenter}-${endpoint.name}-${#####}
```

De identificatie, die in de sjabloon wordt weergegeven als `${#####}`, toont een ID van zes cijfers. De identificatie is een teller die de uniekheid waarborgt. De teller is algemeen voor de organisatie en stijgt voor alle projecten, niet alleen voor het huidige project. Wanneer u meerdere projecten hebt, verwacht dan geen opeenvolgende identificaties, zoals 000123 en 000124, voor implementaties in het huidige project. U mag bijvoorbeeld verwachten dat de identificatie van 000123 springt naar 000127.

Alle resourcenames moeten uniek zijn. Gebruik de eigenschap voor oplopende getallen om de uniekheid te garanderen. De nummering wordt opgehoogd voor alle implementaties, inclusief implementaties die hun naam krijgen via Cloud Assembly. Naarmate uw systeem robuuster wordt en er steeds meer soorten resources een aangepaste naam krijgen, kan de nummering weliswaar willekeurig lijken, maar zal elke waarde steeds uniek blijven. De cijfers stijgen ook wanneer u een testimplementatie uitvoert.

De volgende lijst geeft voorbeelden van de soorten resources waarop de aangepaste namen worden toegepast. De lijst is niet definitief bedoeld.

Tabel 6-2. Voorbeeldlijst met resources waarop aangepaste namen worden toegepast

Resourcegroep	Resourcetypen
Virtual machines	<ul style="list-style-type: none"> ■ Cloud.Machine ■ Cloud.vSphere.Machine ■ Cloud.AWS.EC2.Instance ■ Cloud.GCP.Machine ■ Cloud.Azure.Machine
Load balancers	<ul style="list-style-type: none"> ■ Cloud.LoadBalancer ■ Cloud.NSX.LoadBalancer
Netwerken	<ul style="list-style-type: none"> ■ Cloud.Network ■ Cloud.vSphere.Network ■ Cloud.NSX.Network
Beveiligingsgroepen	<ul style="list-style-type: none"> ■ Cloud.SecurityGroup
Schijven	<ul style="list-style-type: none"> ■ Cloud.Volume ■ Cloud.vSphere.Disk ■ Cloud.AWS.Volume ■ Cloud.GCP.Disk ■ Cloud.Azure.Disk
NSX	<ul style="list-style-type: none"> ■ Cloud.NSX.Gateway ■ Cloud.NSX.NAT
Microsoft Azure	<ul style="list-style-type: none"> ■ Cloud.Azure.ResourceGroup

Naast de voorbeelden die hier worden vermeld, kunt u ook de gebruikersnaam, de afbeelding die wordt gebruikt, andere ingebouwde opties en eenvoudige tekenreeksen toevoegen. Wanneer u de sjabloon bouwt, worden er hints met betrekking tot mogelijke opties weergegeven.

Houd er rekening mee dat sommige waarden die u ziet alleen voorbeelden zijn. U kunt deze waarden niet letterlijk overnemen in uw omgeving. Denk er dus goed over na waar u uw eigen vervangingen zou maken, of leid dit af uit de voorbeeldwaarden, om te voldoen aan uw eigen cloudinfrastructuur- en implementatiebeheerbehoefte.

Voorwaarden

- Controleer of u de naamgevingsconventie weet die u wilt gebruiken voor implementaties van een project.
- Bij deze procedure wordt ervan uitgegaan dat u een eenvoudige cloudsjabloon hebt of kunt maken die u gebruikt om de naamgeving van uw aangepaste hostvoorvoegsels te testen.

Procedure

- 1 Selecteer **Infrastructuur > Projecten**.
- 2 Selecteer een bestaand project of maak een nieuw.

- 3 Ga op het tabblad **Inrichting** naar de sectie Aangepaste eigenschappen en maak de eigenschappen voor de sitecode en kostenplaatswaarden.

Hier vervangt u de waarden die u hier ziet door de waarden voor uw omgeving.

Custom Properties

Specify the custom properties that should be added to all requests in this project. ⓘ

Define custom properties	Name	Value
	siteCode	BGL
	costCenter	IT-research

Custom Naming

Specify the naming template to be used for machines provisioned in this project.

Template `${project.name}-${resource.siteCode}-${resource.costCenter}` ⓘ

- a Maak een aangepaste eigenschap met de naam **siteCode** en de waarde **BGL**.
 - b Voeg een andere aangepaste eigenschap toe met de naam **costCenter** en de waarde **IT-onderzoek**.
- 4 Zoek de aangepaste naamgevingssectie en voeg de volgende sjabloon toe.

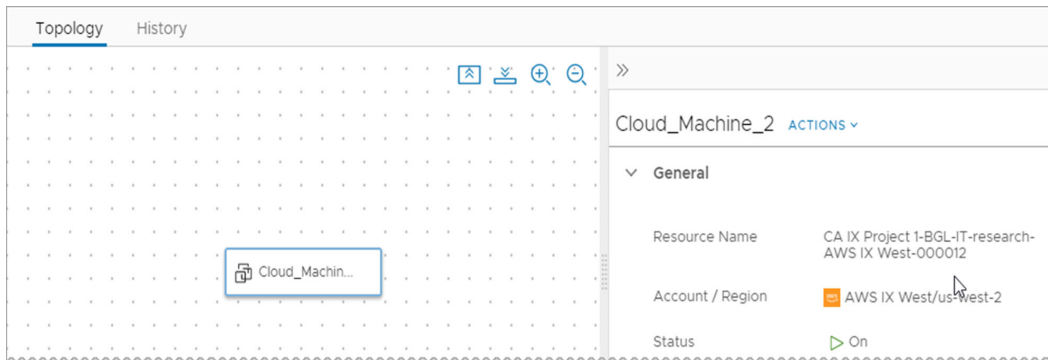
```
${project.name}-${resource.siteCode}-${resource.costCenter}-${endpoint.name}-${#####}
```

U kunt de tekenreeks kopiëren, maar als dit uw eerste naamgevingssjabloon is, overweeg dan om de hinttekst te gebruiken en snel te selecteren wanneer u de sjabloon bouwt.

- 5 Implementeer een cloudsjabloon die is gekoppeld aan het project om te controleren of de aangepaste naam op de resource is toegepast.
 - a Klik op het tabblad **Ontwerp** en klik vervolgens op een cloudsjabloon die aan het project is gekoppeld.
 - b Implementeer de cloudsjabloon.

De pagina **Implementaties** wordt geopend en toont uw implementatie in behandeling.

- c Wanneer de implementatie is voltooid, klikt u op de implementatienaam.
- d Op het tabblad **Topologie** ziet u dat uw aangepaste naam de naam van de resource in het rechterdeelvenster is.



- 6 Als u een testcloudsjabloon hebt geïmplementeerd om de naamgevingsconventie te controleren, kunt u de implementatie verwijderen.

Wat nu te doen

Maak aangepaste naamgevingssjablonen voor uw andere projecten.

De SaltStack Config-resource toevoegen aan Cloud Assembly-ontwerpen

Als u SaltStack Config met vRealize Automation heeft geïntegreerd, kunt u de SaltStack Config-resource toepassen om de minions op virtuele machines in uw implementaties te installeren. Nadat de minion is geïmplementeerd, kunt u gebruikmaken van het krachtige configuratiebeheer, de correctie van afwijkingen en het statusbeheer van SaltStack Config om uw resources te beheren.

Minions zijn agents die de Salt-minionservice uitvoeren. De service abonneert zich op opdrachten die door een Salt-master worden gepubliceerd. Dit is een server die de Salt-masterservice uitvoert. Als een specifieke opdracht van toepassing is op een minion, voert de minion de opdracht uit.

U kunt de SaltStack Config-resource gebruiken om minions te implementeren en statusbestanden toe te passen wanneer u Linux- en Windows-machines implementeert. Om minions en statusbestanden op bestaande implementaties toe te voegen of bij te werken, kunt u de actie **Salt-configuratie toepassen** voor dag 2 uitvoeren. Deze actie gebruikt de eigenschap `saltConfiguration`. Zie [Welke acties kan ik op Cloud Assembly-implementaties uitvoeren](#) voor meer informatie over de actie voor dag 2.

Als u de eigenschap `saltConfiguration` heeft gebruikt om minions en statusbestanden als actie voor dag 0 te implementeren, kunt u overwegen uw cloudsjablonen bij te werken om de SaltStack Config-resource te gebruiken. De eigenschap `saltConfiguration` zal in een toekomstige release worden afgeschaft en zal worden vervangen door de SaltStack Config-resource, samen met een alternatieve actie voor dag 2.

Opmerking Zowel de eigenschap `saltConfiguration` als de SaltStack Config-resource worden in dezelfde cloudsjabloon ondersteund, maar niet voor dezelfde resource.

U kunt bijvoorbeeld een cloudsjabloon met twee machines maken. De eerste machine wordt gekoppeld aan een SaltStack Config-resource. De tweede machine wordt niet gekoppeld aan een SaltStack Config-resource en er wordt ook geen Salt-configuratie op toegepast. Nadat u de cloudsjabloon heeft geïmplementeerd, kunt u alleen een bewerking voor dag 2 uitvoeren op de tweede machine om een Salt-configuratie toe te passen. De actie voor dag 2 voor de machine met de SaltStack Config-resource wordt uitgeschakeld

Voordat u aan de slag gaat

- 1 Controleer of u SaltStack Config hebt geïnstalleerd en de integratie hebt geconfigureerd. Zie [Een SaltStack Config-integratie maken in vRealize Automation](#).
- 2 Controleer in SaltStack Config of de FQDN-naamomzetting van minion naar master werkt.
 - a Om de FQDN op de Salt-master in SaltStack Config te verifiëren, selecteert u **Minions > Alle minions**.
 - b Filter de kolom **Minion-id** op de waarde **saltmaster**.
 - c Klik op **saltmaster** om de details weer te geven.
 - d Controleer of de FQDN-waarde klopt.
- 3 Als u minions implementeert op een Linux-machine, controleert u of voor de images in vSphere die u van plan bent te implementeren met een Salt-minion, SSH-mogelijkheden zijn ingeschakeld. SSH wordt gebruikt om op afstand toegang te krijgen tot de machine en de minion te implementeren.
- 4 Als u minions implementeert op een Windows-machine, raadpleegt u [Hoe implementeer ik minions met behulp van de API in een Windows-omgeving](#).
- 5 Controleer of u IP-adressen kunt toewijzen aan de machines die u implementeert.
SaltStack Config vereist dat de machines IP-adressen hebben. Gebruik de IP-adressen van het openbare IP CIDR-bereik voor het SDDC (software-defined datacenter) waar uw Salt-master zich bevindt.
- 6 Controleer of de cloudsjabloon waaraan u de minion toevoegt, kan worden geïmplementeerd voordat u de SaltStack Config-resource-eigenschappen toevoegt.
- 7 Controleer of u over de volgende servicerollen beschikt:
 - a Cloud Assembly-beheerder

- b Cloud Assembly-gebruiker
- c Service Broker-beheerder

Deze servicerollen zijn vereist voor het gebruik van de SaltStack Config-resource.

De SaltStack Config-resource toevoegen aan de cloudsjabloon

Als ontwikkelaar van cloudsjablonen kunt u eigenschappen toevoegen aan de YAML om de SaltStack Config-minion te installeren wanneer u de sjabloon implementeert.

De kerneigenschappen die u toevoegt aan de sjabloon, omvatten externe toegang voor de machine die u wilt implementeren en configuratie-eigenschappen voor de SaltStack Config-resource. Het gaat in deze procedure alleen over geselecteerde eigenschappen. De YAML biedt ook andere SaltStack Config-resource-eigenschappen die niet in dit voorbeeld worden gebruikt. Bekijk het schema voor meer informatie.

In dit voorbeeld ziet u hoe u een gebruikersnaam en wachtwoord toevoegt voor de eigenschappen voor externe toegang, maar u kunt ook een geheime eigenschap configureren en deze toevoegen aan de sjabloon. Zie [Geheime Cloud Assembly-eigenschappen](#) voor een voorbeeld.

Procedure

- 1 Selecteer **Ontwerp > Cloudsjablonen** in Cloud Assembly.
- 2 Open een bestaande sjabloon.
- 3 Zoek de **SaltStack Config**-resource en sleep deze naar het canvas.
- 4 Koppel de **SaltStack Config**-resource aan de machine waarop de minion wordt geïnstalleerd.
- 5 Voeg eigenschappen toe aan de `Cloud_SaltStack_1`-resource in het codevenster.

Het is niet vereist om alle mogelijke eigenschappen toe te voegen. De gebruikte waarden in dit voorbeeld worden uitgelegd in de tabel.

```
Cloud_SaltStack_1:
  type: Cloud.SaltStack
  properties:
    masterId: saltstack_enterprise_installer
    hosts:
      - ${resource.Cloud_vSphere_Machine_1.id}
    saltEnvironment: sse
    stateFiles:
      - /doe.sls
    variables:
      user: joe
```

Beschrijving van de `Cloud_SaltStack_1`-eigenschappen die in dit voorbeeld worden gebruikt.

Eigenschap	Beschrijving
masterId	In het voorbeeldschema is <code>saltstack_enterprise_installer</code> de waarde voor <code>masterId</code> . Mogelijk hebt u al master-id's in SaltStack Config gedefinieerd via Beheer > Mastersleutels .
hosts	<p>De waarde voor <code>hosts</code> is de id van de machine of het cluster met machines waarop u de minion wilt installeren. Standaard wordt de naam van de machine doorgegeven als minion-id in SaltStack Config.</p> <p>Het wordt aanbevolen dat u machinenamen van 15 tekens of minder kiest, in het bijzonder als u minions in Windows implementeert. Windows staat geen hostnamen van meer dan 15 tekens toe.</p> <p>Als u een aangepaste naamgevingsconventie wilt definiëren voor de machines die u wilt implementeren, raadpleegt u Aangepaste naamgeving voor geïmplementeerde resources in Cloud Assembly.</p>
saltEnvironment	In dit voorbeeld is <code>sse</code> een bestandslocatie voor de statusbestanden. Mogelijk staan uw statusbestanden op andere bestandsserverlocaties in SaltStack Config in Configuratie > Bestandsserver .
stateFiles	In dit voorbeeld is <code>doe.sls</code> een statusbestand in de bestandsserverdirectory die is opgegeven als <code>saltEnvironment</code> .
variables	De variabelen zijn de waarden die in het statusbestand worden gebruikt. In dit voorbeeld accepteert <code>doe.sls</code> een <code>user</code> -waarde als invoer.

- 6 Voeg `remoteAccess`-eigenschappen toe aan de machine die als host fungeert voor de Salt-minion.

De waarde voor de sleutel `authentication` moet `usernamePassword` of `generatedPublicPrivateKey` zijn. `publicPrivateKey` wordt niet ondersteund.

```
remoteAccess:
  authentication: usernamePassword
  username: adminUser
  password: adminPassword
```

- 7 Controleer of uw YAML vergelijkbare eigenschappen bevat als in het onderstaande voorbeeld.

```
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: ubuntu
      flavor: small
      remoteAccess:
        authentication: usernamePassword
```

```

username: adminUser
password: adminPassword
Cloud_SaltStack_1:
  type: Cloud.SaltStack
  properties:
    masterId: saltstack_enterprise_installer
    hosts:
      - ${resource.Cloud_vSphere_Machine_1.id}
    saltEnvironment: sse
    stateFiles:
      - /doe.sls
    variables:
      user: joe

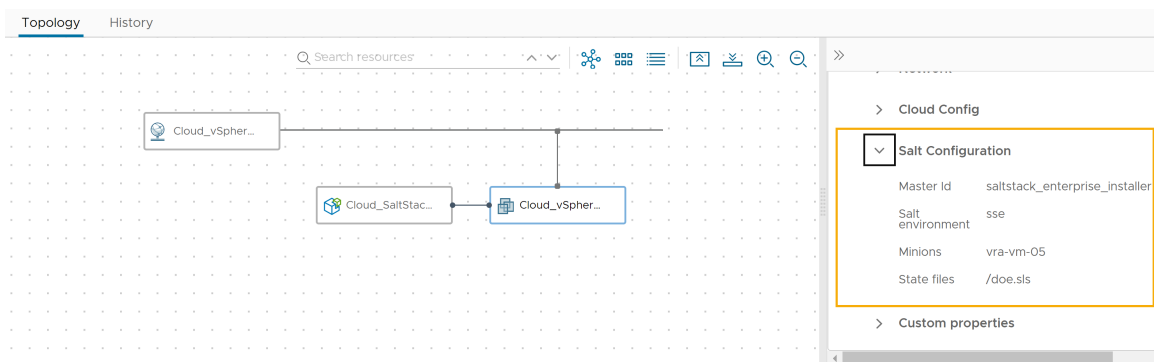
```

8 Test en implementeer de cloudsjabloon.

Zie [Problemen oplossen met minionimplementaties](#) als uw minionimplementatie mislukt.

9 Controleer de Salt-configuratie-eigenschappen voor de geïmplementeerde machine.

- Selecteer **Implementaties > Implementaties** en open de implementatiedetails.
- Klik op het tabblad **Topologie** op de machine en vouw de eigenschappen in het rechtervenster uit.



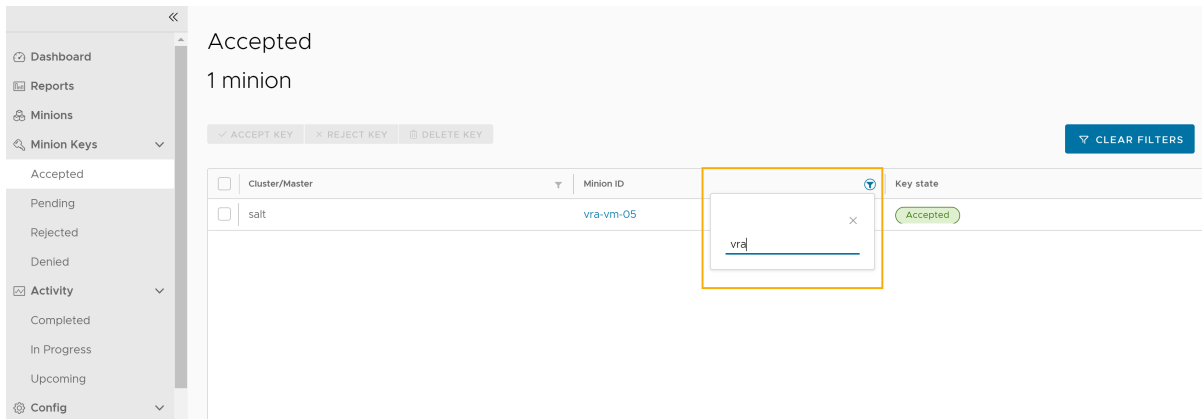
De minion controleren in SaltStack Config

Nadat u de minion op de virtual machine hebt geïnstalleerd, zoekt u de minion en voert u taken of opdrachten uit voor de resource.

Procedure

- Om SaltStack Config te openen, klikt u in de rechterbovenhoek op het menu **Applicaties** en klikt u op **Cloud Services-console**.
- Klik op de servicetegel **SaltStack Config**.
- Vouw **Minionsleutels** uit in SaltStack Config en klik op **Geaccepteerd**.
- Klik in de kolom **Minion-id** op het filterpictogram en voer de naam van de minion in.

De naam van de minion wordt standaard ingesteld op de hostnaam van de virtuele machine. In dit voorbeeld is vra-vm-05 de minion-id.



- 5 Als u de details wilt weergeven, klikt u op de naam van de minion.

U kunt taken of opdrachten uitvoeren voor de minion. Bijvoorbeeld: inzage in schijfgebruik. Deze taak retourneert statistieken over het schijfgebruik voor een minion.

vra-vm-05

Presence: Present

Key state: Accepted

Master: salt

Targets: [All Minions](#) , [Linux](#) , [Ubuntu](#)

IPv4: 10.196.194.192, 127.0.0.1

OS: Ubuntu16.04

Salt Version: 3002.7

[RUN JOB](#) [RUN COMMAND](#)

Grains Activity

biosreleasedate	12/12/2018
biosversion	6.00
> cpu_flags	--
cpu_model	Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz
cpuarch	x86_64
cwd	/
> disks	--

Problemen oplossen met minionimplementaties

Lees over enkele veelvoorkomende fouten die gebruikers ervaren tijdens het implementeren van Salt-minions met behulp van de SaltStack Config-resource of de eigenschap `saltConfiguration`.

Vertraagd opstarten van host

Wanneer Windows- of Linux-services op de host niet gereed zijn nadat u uw cloudsjabloon heeft geïmplementeerd, ontvangt u mogelijk de fout 'Minionimplementatie en/of uitvoeren van statusbestand mislukt' in Cloud Assembly.

Upgrade de masterplug-in naar de nieuwste stabiele versie om deze fout op te lossen. Na het upgraden kunt u een configuratie-instelling inschakelen in `/etc/salt/master.d/raas.conf` waardoor Windows- en Linux-services de tijd krijgen om actief te worden voordat u de Salt-minion implementeert.

Nadat u de upgrade naar de nieuwste versie van de masterplug-in heeft voltooid, voltooit u deze stappen om het opstarten van de host uit te stellen:

- 1 Controleer het tabblad **Geschiedenis** op de pagina met implementatiegegevens.
- 2 Als er in het foutbericht wordt gemeld dat de uitvoering van de minionimplementatie en/of het statusbestand is mislukt, kopieert u de opdracht-ID (JID) en opent u SaltStack Config.
- 3 Selecteer **Activiteit > Voltooid** in SaltStack Config om voltooide opdrachten te openen.
- 4 Klik in de kolom **JID** op het filterpictogram en typ de JID.
- 5 Klik op de JID om de pagina met opdrachtresultaten te bekijken.
- 6 Klik op het tabblad **Raw** om de onbewerkte uitvoer voor de opdracht te zien.

Windows

Als de laatste regel in de onbewerkte uitvoer voor de opdracht 'Kan geen verbinding maken met host: time-out opgetreden' bevat, moet u deze configuratie-instelling toevoegen aan `/etc/salt/master.d/raas.conf` om het opstarten met 180 seconden te vertragen:

```
sseapi_win_minion_deploy_delay: 180
```

Linux

Als de laatste regel in de onbewerkte uitvoer voor de opdracht 'Externe host is niet toegankelijk met opgegeven verificatiegegevens', moet u deze configuratie-instelling toevoegen aan `/etc/salt/master.d/raas.conf` om het opstarten met 90 seconden te vertragen:

```
sseapi_linux_minion_deploy_delay: 90
```

- 7 Herstart de Salt-masterservice:

```
systemctl restart salt-master
```

- 8 Implementeer uw cloudsjabloon opnieuw.

Als de implementatie niet is gelukt, kunt u de vertragingparameter verhogen en de sjabloon opnieuw implementeren.

Wat moet u nu doen

Raadpleeg de [documentatie voor SaltStack Config](#) als u de SaltStack Config-mogelijkheden wilt gebruiken om uw resources te beheren.

Terraform-configuraties in Cloud Assembly

U kunt Terraform-configuraties insluiten als resource in cloudsjablonen in Cloud Assembly.

Een Terraform runtimeomgeving voor Cloud Assembly voorbereiden

Ontwerpen die Terraform-configuraties bevatten, vereisen toegang tot een Terraform-runtimeomgeving die u integreert met het Cloud Assembly-product op locatie.

Een Terraform-runtime toevoegen

De runtimeomgeving bestaat uit een Kubernetes-cluster dat Terraform CLI-opdrachten uitvoert om aangevraagde bewerkingen uit te voeren. Daarnaast verzamelt de runtime logboeken en worden de resultaten van Terraform CLI-opdrachten geretourneerd.


Het vRealize Automation-product op locatie vereist dat gebruikers hun eigen Kubernetes-cluster van de Terraform-runtime configureren. Er wordt slechts één Terraform-runtime per organisatie ondersteund. Alle Terraform-implementaties voor die organisatie gebruiken dezelfde runtime.

- 1 Controleer of u over een Kubernetes-cluster beschikt waarop de Terraform CLI moet worden uitgevoerd.
 - Alle gebruikers kunnen een kubeconfig-bestand leveren om de Terraform CLI uit te voeren op een niet-beheerd Kubernetes-cluster.
 - Gebruikers met een Enterprise-licentie kunnen ervoor kiezen om de Terraform CLI uit te voeren op een Kubernetes-cluster dat wordt beheerd door vRealize Automation.

Ga in Cloud Assembly naar **Infrastructuur > Resources > Kubernetes** en controleer of u een Kubernetes-cluster hebt. Raadpleeg [Hoe werk ik met Kubernetes in Cloud Assembly?](#) als u er een moet toevoegen.
- 2 Als het Kubernetes-cluster nieuw is toegevoegd of gewijzigd, wacht u tot het verzamelen van gegevens is voltooid.

Gegevensverzameling haalt de lijst met naamruimten en andere informatie op en kan tot 5 minuten duren, afhankelijk van de provider.
- 3 Nadat de gegevensverzameling is voltooid, gaat u naar **Infrastructuur > Verbindingen > Integraties > Integratie toevoegen** en selecteert u de kaart **Terraform-runtime**.
- 4 Voer de instellingen in.

Figuur 6-3. Voorbeeld van Terraform-runtime-integratie



New Integration

Name *

OurOrg TF Runtime

Description

Terraform Runtime Integration

Runtime type *

☒ Managed kubernetes cluster
 ☐ External kubeconfig

Kubernetes cluster *

?

Kubernetes namespace *

?

Runtime Container Settings

Image

?

CPU request (Millicores)

CPU limit (Millicores)

Memory request (MB)

Memory limit (MB)

VALIDATE

Instelling	Beschrijving
Naam	Geef de runtime-integratie een unieke naam.
Beschrijving	Leg uit waar de integratie voor is.
Terraform-runtime-integratie:	
Runtime type (alleen Enterprise)	Gebruikers met een Enterprise-licentie kunnen aangeven of de Terraform CLI moet worden uitgevoerd op een Kubernetes-cluster dat wordt beheerd door vRealize Automation of op een niet-beheerd cluster.
Kubernetes kubeconfig (alle gebruikers)	<p>Voor een niet-beheerd Kubernetes-cluster plakt u de volledige inhoud van het kubeconfig-bestand voor het externe cluster.</p> <p>Zie Proxyondersteuning toevoegen als u een externe Kubernetes-runtime wilt gebruiken met een proxyserver. Deze optie is beschikbaar voor alle gebruikers.</p>

Instelling	Beschrijving
Kubernetes-cluster (alleen Enterprise)	Voor Kubernetes, beheerd door vRealize Automation, selecteert u het cluster waarin u de Terraform CLI moet worden uitgevoerd. Het cluster en het kubeconfig-bestand moeten bereikbaar zijn. U kunt toegang tot kubeconfig valideren met een GET op /cmx/api/resources/k8s/clusters/{clusterId}/kube-config. Deze optie is alleen beschikbaar voor Enterprise-licenties.
Kubernetes-naamruimte	Selecteer de naamruimte die u in het cluster wilt gebruiken, voor het maken van pods die de Terraform CLI uitvoert.
Instellingen voor runtimecontainer:	
Image	Voer het pad in naar de containerimage van de Terraform-versie die u wilt uitvoeren. Opmerking De knop VALIDEREN controleert niet op containerimage.
CPU-aanvraag	Voer de hoeveelheid CPU in voor het uitvoeren van containers. Standaard is 250 millicores.
CPU-limiet	Voer het maximum aantal toegestane CPU's in voor het uitvoeren van containers. Standaard is 250 millicores.
Geheugenaanvraag	Voer de hoeveelheid geheugen in voor het uitvoeren van containers. Standaardwaarde is 512 MB.
Geheugenlimiet	Voer het maximaal toegestane geheugen in voor het uitvoeren van containers. Standaardwaarde is 512 MB.

5 Klik op **VALIDEREN** en pas de instellingen indien nodig aan.

6 Klik op **TOEVOEGEN**.

Instellingen worden in de cache opgeslagen. Nadat u de integratie hebt toegevoegd, kunt u instellingen zoals het cluster of de naamruimte wijzigen, maar het kan tot 5 minuten duren voordat een wijziging wordt gedetecteerd en de Terraform CLI wordt uitgevoerd met de nieuwe instellingen.

Problemen met de Terraform-runtime oplossen

Sommige problemen met de implementatie van de Terraform-configuratie zijn mogelijk gerelateerd aan de runtime-integratie.

Probleem	Oorzaak	Oplossing
Validatie mislukt met een fout met de mededeling dat de naamruimte ongeldig is.	U heeft het cluster gewijzigd, maar hebt de vorige naamruimte in de gebruikersinterface verlaten.	Selecteer een naamruimte altijd opnieuw nadat u de clusterselectie hebt gewijzigd.
De vervolgkeuzelijst Naamruimte is leeg of vermeldt geen nieuwe toegevoegde naamruimten.	Gegevensverzameling voor het cluster is niet voltooid. Het verzamelen van gegevens neemt 5 minuten in beslag na het invoeren of wijzigen van het cluster en tot 10 minuten bij het invoeren of wijzigen van de naamruimte.	Voor een nieuw cluster met bestaande naamruimten moet u maximaal 5 minuten wachten tot het verzamelen van gegevens is voltooid. Voor een nieuwe naamruimte in een bestaand cluster moet u maximaal 10 minuten wachten tot het verzamelen van gegevens is voltooid. Als het probleem zich blijft voordoen, verwijdert u het cluster en voegt u het opnieuw toe onder Infrastructuur > Resources > Kubernetes .
Terraform CLI-containers worden gemaakt in een vorig cluster, vorige naamruimte of met eerdere runtime-instellingen, zelfs nadat het integratieaccount is bijgewerkt.	De Kubernetes API-client die door vRealize Automation wordt gebruikt, wordt gedurende 5 minuten in de cache opgeslagen.	Het kan tot 5 minuten duren voordat wijzigingen van kracht worden.
Validatie of een Terraform-implementatiebewerking mislukt met een foutmelding dat kubeconfig niet beschikbaar is.	Soms treden deze fouten op omdat het cluster niet bereikbaar is vanaf vRealize Automation. In andere gevallen zijn gebruikersreferenties, tokens of certificaten ongeldig.	De kubeconfiguratiefout kan een aantal redenen hebben en vereist mogelijk dat u contact opneemt technische ondersteuning om het probleem op te lossen.

Proxyondersteuning toevoegen

Als u uw externe Kubernetes-runtimecluster wilt verbinden via een proxyserver, volgt u deze stappen.

- 1 Meld u aan bij uw externe Kubernetes-clusterserver.
- 2 Maak een lege map.
- 3 Voeg de volgende regels toe aan een nieuw bestand met de naam Dockerfile in de nieuwe map.

```
FROM projects.registry.vmware.com/vra/terraform:latest as final
ENV https_proxy=protocol://username:password@proxy_host:proxy_port
ENV http_proxy=protocol://username:password@proxy_host:proxy_port
ENV no_proxy=.local,.localdomain,localhost
```

- 4 Pas de tijdelijke waarden aan zodat de omgevingsvariabelen `https_proxy` en `http_proxy` de proxyserverinstellingen bevatten die u gebruikt om toegang te krijgen tot internet.

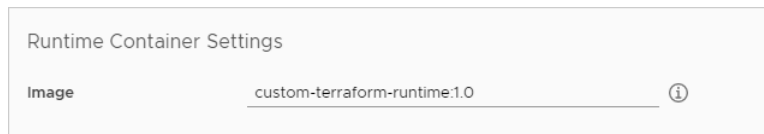
Het *protocol* is http of https afhankelijk van wat uw proxyserver gebruikt, wat mogelijk niet overeenkomt met de naam van de omgevingsvariabele van `https_proxy` of `http_proxy`.

- 5 Sla Dockerfile op en sluit het.
- 6 Voer de volgende opdracht uit in de lege map. Afhankelijk van uw accountrechten moet u de opdracht mogelijk uitvoeren in de sudo-modus.

```
docker build --file Dockerfile --tag custom-terraform-runtime:1.0 .
```

De opdracht maakt een lokale custom-terraform-runtime:1.0 Docker-image.

- 7 Ga in Cloud Assembly onder **Infrastructuur > Verbindingen > Integraties** naar uw Terraform-runtime-integratie.
- 8 Maak of bewerk de instellingen voor de runtimecontainer om de custom-terraform-runtime:1.0-image te gebruiken:



Cloud Assembly Terraform-runtime zonder internettoegang

Cloud Assembly-gebruikers die Terraform-integraties moeten ontwerpen en uitvoeren indien niet verbonden met internet, kunnen hun runtime-omgeving instellen door dit voorbeeld te volgen.

Opmerking Voor het verkrijgen van een bron voor het maken van images moet voor de setup kort verbinding worden gemaakt met internet. Mogelijk moet u deze stappen buiten uw niet-verbonden site uitvoeren als een tijdelijke verbinding niet mogelijk is.

Bij dit proces wordt ervan uitgegaan dat u [uw eigen Docker-register](#) hebt en dat u zonder internetverbinding toegang hebt tot de opslagplaatsen.

De aangepaste containerimage maken

- 1 Maak een aangepaste containerimage die de binaire bestanden van de Terraform-providerinvoegtoepassing bevat.

In het volgende Docker-bestand ziet u een voorbeeld van het maken van een aangepaste image met de Terraform GCP-provider.

Voor de download van de basisimage `projects.registry.vmware.com/vra/terraform:latest` in het Docker-bestand is internettoegang vereist tot het VMware Harbor-register op `projects.registry.vmware.com`.

Firewallinstellingen of proxyinstellingen kunnen ertoe leiden dat de imagebuild mislukt. Mogelijk heeft u toegang nodig tot releases.hashicorp.com om de binaire bestanden van de Terraform-providerinvoegtoepassing te downloaden. U kunt echter uw privéregister gebruiken om de binaire bestanden van de invoegtoepassing als optie te leveren.

```
FROM projects.registry.vmware.com/vra/terraform:latest as final

# Create provider plug-in directory
ARG plugins=/tmp/terraform.d/plugin-cache/linux_amd64
RUN mkdir -m 777 -p $plugins

# Download and unzip all required provider plug-ins from hashicorp to provider directory
RUN cd $plugins \
    && wget -q https://releases.hashicorp.com/terraform-provider-google/3.58.0/terraform-provider-google_3.58.0_linux_amd64.zip \
    && unzip *.zip \
    && rm *.zip

# For "terraform init" configure terraform CLI to use provider plug-in directory and not
download from internet
ENV TF_CLI_ARGS_init="-plugin-dir=$plugins -get-plugins=false"
```

- 2 Bouw, tag en push de aangepaste containerimage naar uw eigen Docker-opslagplaats op uw locatie zonder verbinding.
- 3 Ga in Cloud Assembly op uw locatie zonder verbinding onder **Infrastructuur > Verbindingen > Integraties** naar uw Terraform-runtime-integratie.
- 4 Maak of bewerk de runtimecontainerinstellingen om uw opslagplaats toe te voegen voor de aangepaste containerimage. De naam van het voorbeeld van de ingebouwde aangepaste containerimage is `registry.ourcompany.com/project1/image1:latest`.

Runtime Container Settings

Image

[registry.ourcompany.com/project1/image1:latest](#) ⓘ

De Terraform CLI lokaal hosten

- 1 Download de binaire bestanden voor de Terraform CLI.
- 2 Upload de binaire bestanden voor de Terraform CLI naar uw lokale webserver of FTP-server.
- 3 Ga in Cloud Assembly naar **Infrastructuur > Configureren > Terraform-versies**.
- 4 Maak of bewerk de Terraform-versie zodat deze de URL naar de binaire bestanden voor de Terraform CLI bevat die op uw lokale server worden gehost.
- 5 Als voor uw lokale web- of FTP-server aanmeldingsverificatie is vereist, selecteert u **Basisverificatie** en voert u de verificatiegegevens voor gebruikersnaam en wachtwoord in die toegang geven tot de server.

Als u het verificatietype wilt wijzigen, moet u de rol van cloudbeheerder in Cloud Assembly hebben.

0.12.29 DELETE

Version * 0.12.29 ⓘ

Description

Enabled ☒ ⓘ

URL * http://host1.ourcompany.com:8080/tf/0.12.29/terraform_0.12.29_linux_amd64.zip ⓘ

Authentication type * ☒ No authentication ☐ Basic authentication ⓘ

SHA256 Checksum * 872245d9c6302b24dc0d98a1e010aef1e4ef60865a2d1f60102c8ad03e9d5a1d ⓘ

Terraform-configuraties ontwerpen en implementeren

Als de runtime is geïmplementeerd, kunt u Terraform-configuratiebestanden aan git toevoegen, cloudsjablonen voor die bestanden ontwerpen en implementeren.

Zie [Terraform-configuraties in Cloud Assembly voorbereiden](#) om aan de slag te gaan.

Problemen oplossen

Open de implementatie in Cloud Assembly tijdens het implementeren. Zoek op het tabblad Geschiedenis naar Terraform-gebeurtenissen en klik op **Logboeken weergeven** aan de rechterkant. Wanneer uw lokale Terraform-provider werkt, worden de volgende berichten in het logboek weergegeven.

```
Initializing provider plugins
```

```
Terraform has been successfully initialized
```

Voor een meer robuust logboek kunt u de cloudsjablooncode handmatig bewerken om `TF_LOG:` `DEBUG` toe te voegen, zoals in het volgende voorbeeld wordt weergegeven.

```
resources:
  terraform:
    type: Cloud.Terraform.Configuration
    properties:
      providers:
        - name: google
          # List of available cloud zones: gcp/us-west1
          cloudZone: gcp/us-west1
      environment:
        # Configure terraform CLI debug log settings
        TF_LOG: DEBUG
      terraformVersion: 0.12.29
```

```
configurationSource:
  repositoryId: fc569ef7-f013-4489-9673-6909a2791071
  commitId: 3e00279a843a6711f7857929144164ef399c7421
  sourceDirectory: gcp-simple
```

Uw eigen basisimage maken

Hoewel VMware de basisimage bij `projects.registry.vmware.com/vra/terraform:latest` af en toe bijwerkt, kan die image verouderd zijn en kwetsbaarheden bevatten.

Als u uw eigen basisimage wilt bouwen, gebruikt u in plaats daarvan het volgende Docker-bestand.

```
FROM alpine:latest as final
RUN apk add --no-cache git wget curl openssh
```

Terraform-configuraties in Cloud Assembly voorbereiden

Voordat u een Terraform-configuratie aan een Cloud Assembly-sjabloon toevoegt, moet u uw opslagplaats voor versiebeheer instellen en integreren.

- 1 [Vereisten](#)
- 2 [Terraform-configuratiebestanden opslaan in een opslagplaats voor versiebeheer](#)
- 3 [Cloudzonetoe wijzing inschakelen](#)
- 4 [Integreer uw opslagplaats met Cloud Assembly](#)

Vereisten

Om Terraform-bewerkingen uit te voeren met het vRealize Automation-product op locatie hebt u de Terraform-runtime-integratie nodig. Zie [Een Terraform runtimeomgeving voor Cloud Assembly voorbereiden](#).

Terraform-configuratiebestanden opslaan in een opslagplaats voor versiebeheer

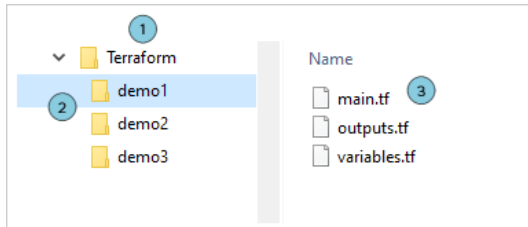
Cloud Assembly ondersteunt de volgende opslagplaatsen voor versiebeheer voor Terraform-configuraties.

- GitHub-cloud, GitHub Enterprise op locatie
- GitLab-cloud, GitLab Enterprise op locatie
- Bitbucket op locatie

Maak in uw opslagplaats voor versiebeheer een standaarddirectory met één laag subdirectory's, elk met Terraform-configuratiebestanden. Maak één subdirectory per Terraform-configuratie.

- 1 Standaarddirectory
- 2 Laag met één subdirectory
- 3 Terraform-configuratiebestanden die klaar zijn voor implementatie

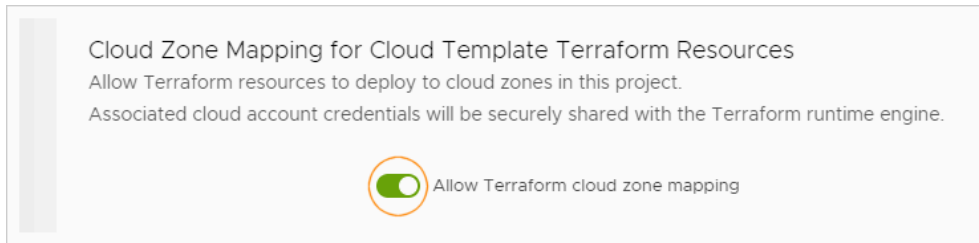
Neem geen Terraform-statusbestand op in configuratiebestanden. Als `terraform.tfstate` aanwezig is, treden er fouten op tijdens de implementatie.



Cloudzonetoewijzing inschakelen

Als u gaat implementeren naar een publieke cloud, heeft de Terraform-runtime-engine de verificatiegegevens van de cloudzone nodig.

In het tabblad **Provisioning** van het project schakelt u **Terraform-cloudzonetoewijzing toestaan** in.



Hoewel verificatiegegevens veilig worden verzonden, moet u voor extra beveiliging de optie gedeactiveerd laten als projectgebruikers geen implementatie hoeven uit te voeren in een cloudaccount.

Integreer uw opslagplaats met Cloud Assembly

Ga in Cloud Assembly naar **Infrastructuur > Verbindingen > Integraties**.

Voeg een integratie toe aan het aanbodtype voor de opslagplaats waar u de Terraform-configuraties hebt opgeslagen: GitHub, GitLab of Bitbucket.

Wanneer u uw project aan de integratie toevoegt, selecteert u het type **Terraform-configuraties** en identificeert u de opslagplaats en de vertakking.

Map is de standaarddirectory van uw eerdere structuur.

Add Repository: testProject

Configure a repository to be used for this project.

Type *

Terraform Configurations

Repository *

parnassusdemo/repository1

Branch *

master

Folder

/Terraform

Ontwerpen voor Terraform-configuraties in Cloud Assembly

Met uw opslagplaats- en Terraform-configuratiebestanden op locatie kunt u er een Cloud Assembly-sjabloon voor ontwerpen.

- 1 [Vereisten](#)
- 2 [Terraform-runtimeversies inschakelen](#)
- 3 [Terraform-resources aan het ontwerp toevoegen](#)
- 4 [De cloudsjabloon implementeren](#)

Vereisten

Uw opslagplaats voor versiebeheer instellen en integreren. Zie [Terraform-configuraties in Cloud Assembly voorbereiden](#).

Terraform-runtimeversies inschakelen

U kunt de Terraform-runtimeversies die beschikbaar zijn voor gebruikers definiëren tijdens het implementeren van Terraform-configuraties. Houd er rekening mee dat Terraform-configuraties ook interne gecodeerde versiebeperkingen kunnen bevatten.

Om de lijst met toegestane versies te maken, gaat u naar **Infrastructuur > Configureren > Terraform-versies**.

Terraform-resources aan het ontwerp toevoegen

Maak uw cloudsjabloon die Terraform-configuraties bevat.

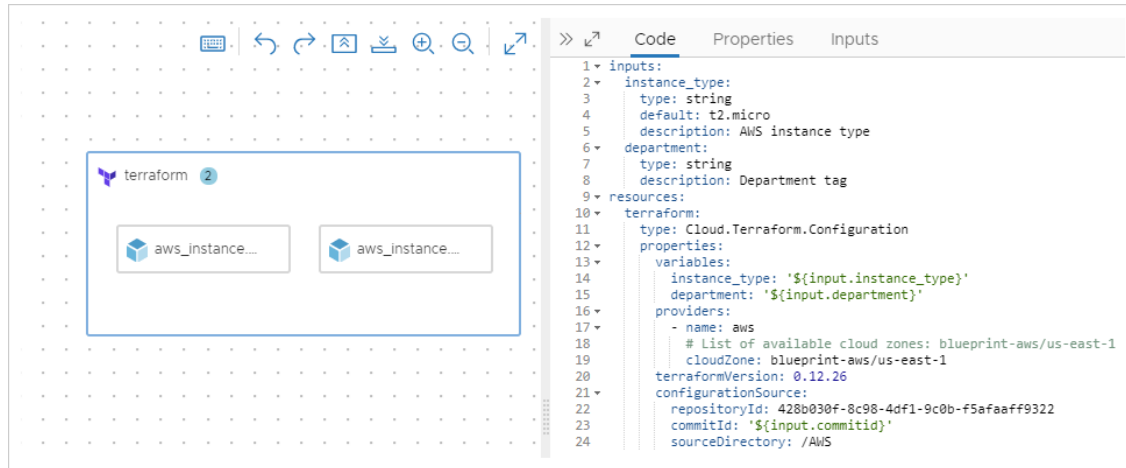
- 1 Ga in Cloud Assembly naar **Ontwerp > Cloudsjablonen** en klik op **Nieuw van > Terraform**.
De Terraform-configuratiewizard wordt weergegeven.
- 2 Volg de aanwijzingen.

Wizard-pagina	Instelling	Waarde
Nieuwe cloudsjabloon	Naam	Geef het ontwerp een identificerende naam.
	Beschrijving	Leg uit waar het ontwerp voor is.

Wizard-pagina	Instelling	Waarde
Configuratiebron	Project	Selecteer het project dat de opslagplaatsintegratie bevat waar de Terraform-configuratie is opgeslagen.
	Opslagplaats	Selecteer de geïntegreerde opslagplaats waar u de Terraform-configuratie hebt opgeslagen.
	Commit	Selecteer een opslagplaats-commit of laat het veld leeg om de Terraform-configuratie van de opslagplaatskop te gebruiken. Bitbucket-beperking - Het aantal selecteerbare commits kan worden ingekort vanwege de configuratie van de Bitbucket-opslagplaatsserver.
Configuratie voltooien	Brondirectory	Selecteer een subdirectory uit de opslagplaatsstructuur die u hebt gemaakt. De eerder vermelde voorbeelden van subdirectory's in de eerdere configuratie zijn demo1, demo2 en demo3.
	Opslagplaats	Controleer de selectie van de juiste opslagplaats.
	Brondirectory	Controleer de selectie van de juiste directory.
	Terraform-versie	Selecteer de Terraform-runtimeversie die moet worden uitgevoerd bij het implementeren van de Terraform-configuratie.
	Providers	Als de Terraform-configuratie een providerblok bevat, controleert u de provider en de cloudzone waar deze cloudsjabloon naar zal worden geïmplementeerd. Het is geen probleem als er geen provider is. Nadat u de wizard hebt voltooid, bewerkt u de provider en de cloudzone in de sjablooneigenschappen om het implementatiedoel toe te voegen of te wijzigen.
	Variabelen	Selecteer gevoelige waarden voor versleuteling, zoals wachtwoorden.
	Outputs	Controleer de outputs van de Terraform-configuratie die converteren naar expressies die uw ontwerpcode kan raadplegen.

3 Klik op **Maken**.

De Terraform-resource wordt weergegeven op het cloudsjablooncanvas met Cloud Assembly-code die de te implementeren Terraform-configuratie weergeeft.



Indien gewenst kunt u andere Cloud Assembly-resources aan de cloudsjabloon toevoegen om Terraform- en niet-Terraform-code in een hybride ontwerp te combineren.

Opmerking Door Terraform-configuraties in de opslagplaats bij te werken, worden de wijzigingen niet gesynchroniseerd in uw cloudsjabloon. Automatische synchronisatie kan beveiligingsrisico's met zich meebrengen, zoals nieuw toegevoegde gevoelige variabelen.

Om Terraform-configuratiewijzigingen vast te leggen, voert u de wizard opnieuw uit, kiest u de nieuwe commit en identificeert u eventuele nieuwe gevoelige variabelen.

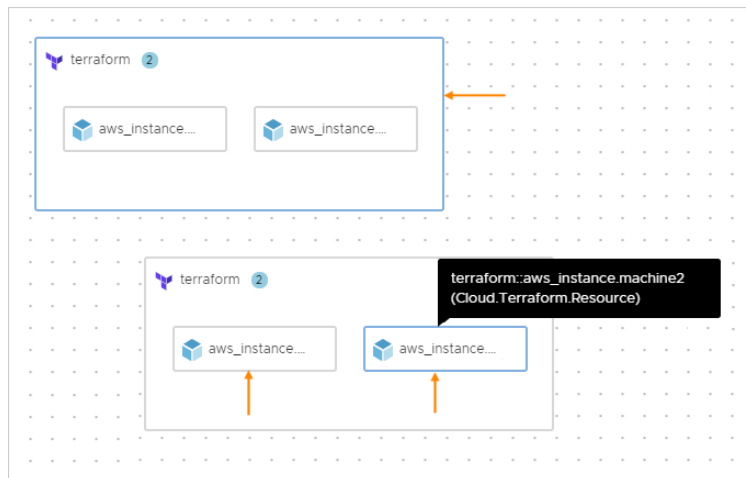
De cloudsjabloon implementeren

Wanneer u de cloudsjabloon implementeert, kunt u op het tabblad **Geschiedenis** van de implementatie een gebeurtenis zoals een toewijzings- of aanmaakfase uitvouwen om een logboek met berichten van de Terraform-CLI te controleren.

Goedkeuringen — Naast de verwachte Terraform-fasen zoals PLANNEN, TOEWIJZEN of MAKEN, introduceert Cloud Assembly governance door middel van een goedkeuringsfase. Zie [Hoe configureer ik Service Broker-goedkeuringsbeleidsregels](#) voor meer informatie over goedkeuringen van aanvragen.

Timestamp	Status	Resource type	Resource name	Details
Aug 3, 202...	PLAN_FINISHED	Cloud.Terraform.Configurati...	terraform	Creating 2 Terraform resources, updating 0 Terraform resources, deleting 0 Terraform resources
Aug 3, 202...	PLAN_IN_PROGRESS	Cloud.Terraform.Configurati...	terraform	Hide Logs <pre> 2:24:23 PM * provider.random: version = "~> 2.3" 2:24:23 PM 2:24:23 PM Terraform has been successfully initialized! 2:24:28 PM Refreshing Terraform state in-memory prior to plan... 2:24:28 PM The refreshed state will be used to calculate this plan, but will not be 2:24:28 PM persisted to local or remote state storage. </pre> View as plain text
Aug 3, 202...	INITIALIZATION_FINISH...			
Aug 3, 202...	INITIALIZATION_IN_PRO...			

Na de implementatie ziet u een buitenste bron die het algemene Terraform-onderdeel vertegenwoordigt, met onderliggende bronnen voor de afzonderlijke onderdelen die door Terraform zijn gemaakt. De bovenliggende Terraform-resource bepaalt de levenscyclus van de onderliggende resources.



Een geheime Cloud Assembly-eigenschap in een Terraform-configuratie gebruiken

U kunt geheime, versleutelde waarden toepassen op Terraform-configuraties die u toevoegt aan Cloud Assembly-cloudsjabloonontwerpen.

- 1 Voeg in uw Git-opslagplaats een Terraform-configuratiebronbestand toe dat naar de geheime eigenschappen verwijst als variabelen.

In dit voorbeeld van een Terraform-configuratiebron zijn API- en applicatiesleutels de geheime variabelen.

```
variable "datadog_api_key" {
  description = "Datadog API Key"
}

variable "datadog_app_key" {
  description = "Datadog App Key"
}

provider "datadog" {
  api_key = "${var.datadog_api_key}"
  app_key = "${var.datadog_app_key}"
}

# Create a new monitor
resource "datadog_monitor" "default" {
  # ...
}

# Create a new timeboard
resource "datadog_timeboard" "default" {
  # ...
}
```

- 2 Ga in Cloud Assembly naar **Infrastructuur > Beheer > Geheimen** en voer de waarden van uw geheime eigenschap in.

Voeg geheime namen en bijbehorende waarden toe. Voor de namen is het het gemakkelijkst om gewoon dezelfde naam als de naam van de variabele uit uw Terraform-bron in te voeren.

Zie zo nodig [Geheime Cloud Assembly-eigenschappen](#) voor meer informatie.

Secrets			
+ NEW SECRET			
	Name	Project	Value
⋮	datadog_api_key	Terraform	*****
⋮	datadog_app_key	Terraform	*****

- 3 Importeer in Cloud Assembly de Terraform-configuratie voor gebruik in een cloudsjabloon.

Ga naar **Ontwerp > Cloudsjablonen** en klik op **Nieuw van > Terraform**.

Opmerking Hoewel de variabelen op de laatste pagina van de wizard kunnen worden geselecteerd, hoeft u de geheime variabelen niet als gevoelig in te stellen. Geheime Cloud Assembly-variabelen zijn al versleuteld en hebben de versleuteling nodig die de wizard toepast.

Zie zo nodig [Ontwerpen voor Terraform-configuraties in Cloud Assembly](#) voor meer informatie.

De cloudsjabloon zou op de volgende code moeten lijken:

```
inputs:
  datadog_api_key:
    type: string
    description: Datadog API Key
  datadog_app_key:
    type: string
    description: Datadog App Key
resources:
  terraform:
    type: Cloud.Terraform.Configuration
    properties:
      variables:
        datadog_api_key: '${input.datadog_api_key}'
        datadog_app_key: '${input.datadog_app_key}'
      providers: []
      terraformVersion: 0.12.29
      configurationSource:
        repositoryId: 0fbf8f5e-54e1-4da3-9508-2b701gf25f51
        commitId: ed12424b249aa50439kr1c268942a4616bd751b6
        sourceDirectory: datadog
```

- 4 In de code-editor wijzigt u voor de geheime waarden handmatig de waarde `input` in `secret` zoals weergegeven.

```
terraform:
  type: Cloud.Terraform.Configuration
  properties:
    variables:
      datadog_api_key: '${secret.datadog_api_key}'
      datadog_app_key: '${secret.datadog_app_key}'
```

- 5 Verwijder in de sectie `inputs`: van de code de invoervermeldingen die zijn vervangen door de bindingen met geheime eigenschappen.

Meer informatie over Terraform-configuraties in vRealize Automation

Houd rekening met bepaalde beperkingen en probleemoplossingen bij het insluiten van Terraform-configuraties als resource in vRealize Automation.

Beperkingen voor Terraform-configuraties

- Bij het valideren van een ontwerp met Terraform-configuraties controleert de knop TEST Cloud Assembly-syntaxis, maar niet de syntaxis van de native Terraform-code.

Daarnaast valideert de knop TEST niet de commit-id's die zijn gekoppeld aan Terraform-configuraties.

- Voor een cloudsjabloon die Terraform-configuraties bevat, is de volgende tijdelijke oplossing vereist voor het klonen van de sjabloon voor een ander project.
 - a In het nieuwe project kopieert u op het tabblad **Integraties** de `repositoryId` voor uw integratie.
 - b Open de kloonsjabloon. In de code-editor vervangt u de `repositoryId` door de id die u heeft gekopieerd.
- Neem in de opslagplaats voor versiecontrole geen Terraform-statusbestand op met configuratiebestanden. Als `terraform.tfstate` aanwezig is, treden er fouten op tijdens de implementatie.

Ondersteunde acties voor dag 2 voor de bovenliggende Terraform-resource

Voor de bovenliggende Terraform-resource kunt u het Terraform-statusbestand weergeven of vernieuwen. Zie de volledige lijst met acties op [Welke acties kan ik op Cloud Assembly-implementaties uitvoeren](#) voor meer informatie over de acties van het statusbestand.

Ondersteunde acties voor dag 2 voor onderliggende resources

Nadat Terraform-configuraties zijn geïmplementeerd, kan het tot 20 minuten duren voordat een actie voor dag 2 beschikbaar komt op onderliggende resources.

Voor onderliggende resources in een Terraform-configuratie wordt alleen de volgende subset van acties voor dag 2 ondersteund. Voor meer informatie over de acties kunt u deze opzoeken in de volledige lijst met acties op [Welke acties kan ik op Cloud Assembly-implementaties uitvoeren](#).

Provider	Type Terraform-resource	Ondersteunde acties voor dag 2
AWS	aws_instance	Inschakelen
		Uitschakelen
		Opnieuw opstarten
		Opnieuw instellen
Azure	azurerm_virtual_machine	Inschakelen
		Uitschakelen
		Opnieuw opstarten
		Opheffen
vSphere	vsphere_virtual_machine	Inschakelen
		Uitschakelen
		Opnieuw opstarten
		Opnieuw instellen
		Afsluiten

Provider	Type Terraform-resource	Ondersteunde acties voor dag 2
GCP	google_compute_instance	Opheffen
		Momentopname maken
		Momentopname verwijderen
		Momentopname terugzetten
		Inschakelen
		Uitschakelen
		Momentopname maken
		Momentopname verwijderen

Problemen oplossen met beschikbaarheid van acties voor dag 2

Out-of-the-box-acties (OOTB) voor dag 2 die ontbreken of zijn gedeactiveerd, kunnen probleemoplossing nodig hebben.

Probleem	Oorzaak	Oplossing
Een Terraform-resource heeft geen verwachte OOTB-actie voor dag 2 in het actiemenu.	De actie wordt mogelijk niet ondersteund voor de provider en het resourcetype zoals vermeld in de vorige lijst. Het kan ook zijn dat de actie 20 minuten moet worden weergegeven vanwege de timing van resourcedetectie en resourcecache.	Controleer de provider en het resourcetype in het ontwerp. Wacht maximaal 20 minuten tot het verzamelen van gegevens is voltooid.
Een Terraform-resource heeft geen verwachte actie voor dag 2, zelfs na de 20 minuten, voor het verzamelen van gegevens.	Een probleem met resourcedetectie voorkomt dat de actie wordt weergegeven. Een manier waarop dat gebeurt is wanneer de resource per ongeluk in een cloudzone buiten het project wordt gemaakt. Uw project bevat bijvoorbeeld alleen een cloudaccount en cloudzone us-east-1, maar de Terraform-configuratie bevat een providerblok voor us-west-1 en u heeft deze niet gewijzigd tijdens het ontwerpen. Een andere mogelijkheid is dat het verzamelen van gegevens niet werkt.	Controleer de cloudzones van het project met betrekking tot de cloudzones in het ontwerp. Ga naar Infrastructuur > Verbindingen > Cloudaccounts en controleer de status van het verzamelen van gegevens en de tijd van wanneer het verzamelen van gegevens voor het cloudaccount is voltooid.

Probleem	Oorzaak	Oplossing
Hoewel er geen duidelijke problemen zijn met de resourcestatus en het verzamelen van gegevens, is een actie voor dag 2 gedeactiveerd (grijs).	Het is bekend dat incidenteel periodieke timingproblemen en fouten bij het verzamelen van gegevens optreden.	Het probleem moet binnen 20 minuten worden opgelost.
De verkeerde actie voor dag 2 is gedeactiveerd, een die op basis van de resourcestatus actief moet zijn. Uitschakelen (Power Off) is bijvoorbeeld ingeschakeld en Inschakelen (Power On) is gedeactiveerd, zelfs als de resource is uitgeschakeld met behulp van de providerinterface.	Timing van gegevensverzameling kan een tijdelijk conflict veroorzaken. Als u de energiestatus van buiten vRealize Automation wijzigt, kan het even duren voordat de wijziging van kracht wordt.	Wacht maximaal 20 minuten.

Aangepaste Terraform-providers gebruiken in vRealize Automation

Als u een aangepaste Terraform-provider wilt gebruiken, voert u de volgende stappen uit.

Voeg in uw opslagplaats voor Git-versiebeheer onder de Terraform-directory die main.tf bevat, de volgende subdirectorystructuur en het zip-bestand van uw aangepaste Terraform-provider toe.

```
terraform.d/plugins/<HOSTNAME>/<NAMESPACE>/<TYPE>/terraform-provider-
<TYPE_VERSION_TARGET>.zip
```

Als u bijvoorbeeld [azurerm version 3.12.0](#) heeft gedownload, maakt u de volgende structuur.

```
terraform.d/plugins/registry.terraform.io/hashicorp/azurerm/terraform-provider-
azurerm_3.12.0_linux_amd64.zip
```

Typen aangepaste resources voor Cloud Assembly-cloudsjablonen

Wanneer u een cloudsjabloon maakt in Cloud Assembly bevat het resourcetypepalet voor de ondersteunde cloudaccount- en integratie-eindpunten. Mogelijk hebt u gebruiksscenario's waarin u cloudsjablonen wilt maken op basis van een uitgebreide lijst met resourcetypen. U kunt typen aangepaste resources maken, deze toevoegen aan het ontwerpcanvas en cloudsjablonen maken die uw ontwerp- en implementatiebehoeften ondersteunen.

Aangepaste resourcenaam en resourcetype

De aangepaste resourcenaam identificeert uw aangepaste resource binnen het palet met resourcetypen van de cloudsjabloon.

Het resourcetype van een aangepaste resource moet beginnen met **Custom.** en elk resourcetype moeten uniek zijn. U kunt bijvoorbeeld `Custom.ADUser` instellen als resourcetype voor een aangepaste resource die Active Directory-gebruikers toevoegt. Hoewel de opname van **Custom.** niet is gevalideerd in het veld, wordt de tekenreeks automatisch toegevoegd als u deze verwijdert.

Aangepaste resources voor uitbreidbaarheidsacties

Met typen aangepaste resources kunt u uitbreidbaarheidsacties in cloudsjablonen gebruiken om complexe applicaties te bouwen. U kunt bijvoorbeeld de native integratie van uitbreidbaarheidsacties met Amazon Web Services en Microsoft Azure gebruiken om eenvoudig te integreren met hun respectieve services. U kunt aangepaste resources voor de uitbreidbaarheidsactie maken door op de optie **Gebaseerd op** te klikken in de editor voor aangepaste resources en **Door gebruiker gedefinieerd ABX-schema** te selecteren.

Levenscyclusacties voor aangepaste resources voor uitbreidbaarheidsacties

Wanneer u een uitbreidbaarheidsactie voor uw aangepaste resource gebruikt, kunt u de volgende levenscyclusacties definiëren:

- **Maken:** Deze uitbreidbaarheidsactie wordt aangeroepen wanneer een implementatie wordt gestart.
- **Lezen:** Deze uitbreidbaarheidsactie wordt gebruikt om de laatste status van de geïmplementeerde resource op te halen.
- **Bijwerken:** Deze uitbreidbaarheidsactie wordt aangeroepen wanneer een cloudsjablooneigenschap wordt bijgewerkt. Deze actie wordt alleen geactiveerd wanneer een eigenschap niet is gemarkeerd met `recreateOnUpdate`.
- **Vernietigen:** Deze uitbreidbaarheidsactie wordt aangeroepen wanneer een implementatie wordt verwijderd.

Deze levenscyclusacties kunnen handmatig uit uw bestaande uitbreidbaarheidsacties worden geselecteerd of automatisch worden gegenereerd door **Acties genereren** te selecteren. Wanneer u **Acties genereren** selecteert, moet u het project opgeven waarin de nieuwe uitbreidbaarheidsactie wordt gegenereerd.

Opmerking U kunt de uitbreidbaarheidsacties bewerken die zijn gekoppeld aan uw levenscyclusacties door op de optie **Openen** naast de specifieke actie te klikken.

Aangepaste resources van vRealize Orchestrator

Elke aangepaste resource van vRealize Orchestrator is gebaseerd op een SDK-inventaristype en wordt gemaakt door een vRealize Orchestrator-werkstroom met een uitvoer die een instantie is van het gewenste SDK-type. Primitieve typen, zoals `Properties`, `Date`, `string` en `number`, worden niet ondersteund voor het maken van typen aangepaste resources.

Opmerking SDK-objecttypen kunnen worden onderscheiden van andere eigenschapstypen door de dubbele punt (:) die wordt gebruikt om de naam van de invoegtoepassing en de naam van het type te scheiden. `AD:UserGroup` is bijvoorbeeld een SDK-objecttype dat wordt gebruikt om Active Directory-gebruikersgroepen te beheren.

U kunt de ingebouwde werkstromen gebruiken in vRealize Orchestrator of u kunt uw eigen werkstromen maken. Als u vRealize Orchestrator gebruikt om XaaS-werkstromen op een willekeurige manier te maken, kunt u een cloudsjabloon maken die een Active Directory-gebruiker toevoegt aan machines tijdens de implementatie of een custom F5 load balancer toevoegen aan een implementatie. U kunt aangepaste resources voor vRealize Orchestrator maken door op de optie **Gebaseerd op** te klikken in de editor voor aangepaste resources en **vRO-inventaris** te selecteren.

Extern type aangepaste resource voor vRealize Orchestrator

De eigenschap extern type bepaalt het type van uw aangepaste resource van vRealize Orchestrator. Wanneer u een werkstroom Maken in uw type aangepaste resource in Cloud Assembly selecteert, wordt daaronder het vervolgkeuzemenu voor extern type weergegeven. Het vervolgkeuzemenu bevat eigenschappen voor extern type die zijn geselecteerd in de uitvoerparameters van de vRealize Orchestrator-werkstroom. De eigenschappen voor de geselecteerde werkstroom in het vervolgkeuzemenu moeten niet-array-SDK-objecttypen zijn, zoals `VC:VirtualMachine` of `AD:UserGroup`.

Opmerking Wanneer u aangepaste werkstromen maakt die gebruikmaken van de dynamische type-invoegtoepassing, controleert u of hun variabelen worden gemaakt met behulp van de `DynamicTypesManager.GetObject()`-methode.

Wanneer u uw typen aangepaste resources definieert, definieert u ook het bereik van de beschikbaarheid van het geselecteerde externe type. Het geselecteerde externe type kan:

- Tussen projecten worden gedeeld.
- Alleen beschikbaar zijn voor het geselecteerde project.

U kunt slechts één type aangepaste resource met een specifieke waarde voor extern type per gedefinieerd bereik hebben. Als u bijvoorbeeld een aangepaste resource in uw project maakt, die gebruikmaakt van `VC:VirtualMachine` als extern type, kunt u geen andere aangepaste resource maken voor hetzelfde project dat hetzelfde externe type gebruikt. U kunt ook geen twee gedeelde aangepaste resources maken die hetzelfde externe type gebruiken.

Validatie van levenscyclusactie voor vRealize Orchestrator

Wanneer u werkstromen Maken, Verwijderen en Bijwerken als levenscyclusacties toevoegt aan uw aangepaste resource, valideert Cloud Assembly dat de geselecteerde werkstromen de juiste invoer- en uitvoereigenschapsdefinities hebben.

- De werkstroom Maken moet een uitvoerparameter hebben die een SDK-objecttype is, zoals `SSH:Host` of `SQL:Database`. Als de geselecteerde werkstroom de validatie niet doorgeeft, kunt u geen werkstromen Bijwerken of Verwijderen toevoegen of uw wijzigingen niet opslaan in de aangepaste resource.
- De werkstroom Verwijderen moet een invoerparameter hebben die een SDK-objecttype is dat overeenkomt met het externe type van de aangepaste resource.
- De werkstroom Bijwerken moet zowel een invoer- als uitvoerparameter hebben die een SDK-objecttype is dat overeenkomt met het externe type van de aangepaste resource.

Schema met eigenschappen voor aangepaste resource

U kunt het schema met eigenschappen voor aangepaste resource-eigenschappen weergeven en bewerken door het tabblad **Eigenschappen** te selecteren. Het schema bevat de naam, het gegevenstype, het eigenschapstype en, indien beschikbaar, de beschrijving van een bepaalde eigenschap. Het schema definieert ook of een bepaalde eigenschap vereist of optioneel is in de cloudsjabloon.

Opmerking Voor het schema met eigenschappen van aangepaste resources voor uitbreidbaarheidsacties zijn alle eigenschappen vereist in de cloudsjabloon.

Wanneer u vRealize Orchestrator-werkstromen toevoegt aan uw aangepaste resource, worden de invoer- en uitvoerparameters toegevoegd als eigenschappen. Voor aangepaste resources voor uitbreidbaarheidsacties moet u het schema met eigenschappen van aangepaste resources voor de uitbreidbaarheidsacties handmatig maken op het tabblad **Eigenschappen**. Op dit tabblad kunt u ook de eigenschappen van uw vRealize Orchestrator of aangepaste resources op basis van uitbreidbaarheidsacties wijzigen en opmaken. U kunt bijvoorbeeld de schermnaam van een bepaalde eigenschap wijzigen of beperkingen toevoegen.

Opmerking Wanneer u beperkingen toevoegt aan de itemsectie van arrayvelden of de eigenschappensectie van objectenvelden in het eigenschappenschema, controleert u of u deze beperkingen heeft gevalideerd omdat onjuist toegepaste beperkingen problemen met de aangepaste resource kunnen veroorzaken. Wanneer u bijvoorbeeld een maximumbeperking toevoegt aan een array met getallen, moet u controleren of deze beperking de standaardwaarde van de eigenschap niet breekt.

U kunt het eigenschappenschema voor aangepaste resources bewerken door naar het tabblad **Eigenschappen** te gaan en het tabblad **Code** of **Formulier** te gebruiken.

- **Code:** bewerk het eigenschappenschema met behulp van YAML-inhoud.

- **Formulier:** door op **Nieuwe eigenschap** te klikken, maakt u een nieuwe eigenschap door naam, schermnaam, beschrijving, eigenschapstype en standaardwaarde te configureren. U kunt ook niet-vereiste en niet-berekende eigenschappen in het schema verbergen door op **Eigenschap verwijderen** te klikken.

Aangepaste aanvraagformulieren voor bewerkingen voor dag 2

U kunt het aanvraagformulier voor bewerkingen voor dag 2 die in uw aangepaste resource zijn opgenomen, stroomlijnen door verschillende typen resource-eigenschappen toe te voegen en aan te passen.

U kunt bijvoorbeeld de waarde van een invoerparameter in uw aanvraagformulier binden aan een externe bron, zoals een vRealize Orchestrator-actie die een implementatienaam of projectnaam ophaalt. U kunt ook de waarde van een specifieke invoerparameter binden aan de berekende waarde van twee andere tekstvakken die in hetzelfde aanvraagformulier zijn opgenomen.

Opmerking Deze functionaliteit is beschikbaar voor zowel aangepaste resources als resourceacties. U kunt de waarde van de invoereigenschappen van uw aanvraagformulier aanpassen via het tabblad **Waarden** van de pagina **Aanvraagparameters** van de editor voor de aangepaste resource of resourceactie.

Validatie van aanvraagformulieren voor bewerking voor dag 2

U kunt het aanvraagformulier voor uw bewerkingen voor dag 2 valideren door een externe validatie toe te voegen. Door een externe validatie te gebruiken, voorkomt u dat de gebruiker het aanvraagformulier indient totdat aan de validatieparameters is voldaan. U kunt externe validatie toevoegen vanuit het tabblad **Validaties** van de pagina **Aanvraagparameters** van de editor voor een aangepaste resource of resourceactie. Nadat u het tabblad heeft geselecteerd, kunt u een element voor **Orchestrator-validatie** naar het canvas slepen en een vRealize Orchestrator-actie toevoegen die u wilt gebruiken voor validatie.

U kunt bijvoorbeeld een aangepaste resource maken die een bewerking voor dag 2 bevat voor het wijzigen van een gebruikerswachtwoord. Voor een dergelijk gebruiksscenario kunt u een vRealize Orchestrator-actie toevoegen met de invoerparameters `newPassword` en `confirmPassword` die gebruikmaken van het type `SecureString`.

Opmerking Dit is een voorbeeldscript voor het valideren van een gebruikerswachtwoord. Voor uw eigen gebruiksscenario kunt u ervoor kiezen om een ander script te gebruiken.

```
if (newPassword != confirmPassword) {
    return 'passwords are different';
}
if (newPassword.length < 7) {
    return 'password must be at least 10 symbols';
}
return null;
```

Hoe maak ik een Cloud Assembly-cloudsjabloon waarmee gebruikers aan Active Directory worden toegevoegd

Naast de Cloud Assembly-cloudsjabloonresources die u gebruikt bij het maken van cloudsjablonen, kunt u ook uw eigen aangepaste resources maken.

Aangepaste resources zijn vRealize Orchestrator of uitbreidbaarheidsactieobjecten die u via vRealize Automation beheert met de levenscyclusacties die in de aangepaste resource zijn gedefinieerd. De cloudsjabloonservice roept automatisch de geschikte vRealize Orchestrator-werkstromen of -uitbreidbaarheidsacties op wanneer de bewerking wordt geactiveerd die is gekoppeld aan een specifieke levenscyclusactie. U kunt de functionaliteit van het resourcetype uitbreiden door ook vRealize Orchestrator-werkstromen of -uitbreidbaarheidsacties te selecteren die kunnen worden gebruikt als bewerkingen voor dag 2.

Dit gebruiksscenario gebruikt ingebouwde werkstromen die in de vRealize Orchestrator-bibliotheek zijn opgegeven. Het bevat beschrijvende waarden of tekenreeksen die aantonen hoe het proces moet worden uitgevoerd. U kunt deze aanpassen aan uw omgeving.

Voor referentiedoeleinden gebruikt dit scenario een project met de naam **DevOpsTesting**. U kunt dit voorbeeldproject vervangen door elk project in uw omgeving.

Voorwaarden

- Controleer of u een vRealize Orchestrator-integratie hebt geconfigureerd. Zie [vRealize Orchestrator-integratie in Cloud Assembly configureren](#).
- Controleer of de werkstromen die u gebruikt voor de acties voor maken, bijwerken, vernietigen en dag 2 bestaan in vRealize Orchestrator en dat ze correct worden uitgevoerd.
- Zoek in vRealize Orchestrator het resourcetype dat door de werkstromen wordt gebruikt. De werkstromen die zijn opgenomen in deze aangepaste resource moeten allemaal hetzelfde resourcetype gebruiken. In dit gebruiksscenario is het resourcetype `AD:User`. Zie [Typen aangepaste resources voor Cloud Assembly-cloudsjablonen](#) voor meer informatie over validatie van het resourcetype.
- Met behulp van de ingebouwde Active Directory-werkstromen in uw vRealize Orchestrator-integratie configureert u een Active Directory-server.
- Controleer of u weet hoe u een machinecloudsjabloon kunt configureren en implementeren.

Procedure

- 1 Maak een aangepaste Active Directory-resource voor het toevoegen van een gebruiker in een groep.

Deze stap voegt de aangepaste resource toe aan het ontwerpcanvas voor cloudsjablonen als resourcetype.

- a Selecteer **Ontwerp > Aangepaste resources** in Cloud Assembly en klik op **Nieuwe aangepaste resource**.
- b Geef de volgende waarden op.

Onthoud dat dit, met uitzondering van de werkstroomnamen, voorbeeldwaarden zijn.

Instelling	Voorbeeldwaarde
Naam	AD-gebruiker Dit is de naam die wordt weergegeven in het palet van het resourcetype voor de cloudsjabloon.
Resourcetype	Custom.ADUser Het resourcetype moet beginnen met Custom. en elk resourcetype moeten uniek zijn. Hoewel de opname van Custom. niet is gevalideerd in het veld, wordt de tekenreeks automatisch toegevoegd als u deze verwijdert. Dit resourcetype wordt toegevoegd aan het resourcetypepalet zodat u het in de cloudsjabloon kunt gebruiken.

- c Als u dit resourcetype wilt inschakelen in de lijst met resourcetypen van de cloudsjabloon, controleert u of de optie **Activeren** is ingeschakeld.
- d Selecteer de instelling **Bereik** die het resourcetype beschikbaar maakt voor elk project.
- e Controleer onder **Gebaseerd op** of **vRO-inventaris** is geselecteerd als provider voor levenscyclusacties.

- f Selecteer de werkstromen die de resource en de acties voor dag 2 definiëren.

Opmerking De geselecteerde werkstromen voor dag 2 moeten een invoerparameter hebben die van hetzelfde type is als het externe type. De invoer van het externe type wordt niet weergegeven op het door de gebruiker aangevraagde aangepaste formulier voor dag 2, omdat het automatisch aan de aangepaste resource is gebonden.

Instelling	Voorbeeldwaarde
Levenscyclusacties - Maken	<p>Selecteer de werkstroom Een gebruiker met een wachtwoord in een organisatie-eenheid maken.</p> <p>Als u meerdere vRealize Orchestrator-integraties hebt, selecteert u de werkstroom voor de integratie-instantie die u gebruikt om deze aangepaste resources uit te voeren.</p> <p>Nadat u de werkstroom hebt geselecteerd, komt het vervolgkeuzemenu Extern type beschikbaar en wordt het automatisch ingesteld op <code>AD:User</code>.</p> <hr/> <p>Opmerking Een extern brontype kan slechts één keer worden gebruikt als het wordt gedeeld en eenmaal per project. In dit geval biedt u dezelfde custom resource voor alle projecten. Het betekent echter dat u <code>AD:User</code> niet kunt gebruiken voor andere resourcetypen voor alle projecten. Als u andere werkstromen hebt waarvoor het type <code>AD:User</code> is vereist, moet u voor elk project individuele aangepaste resources maken.</p>
Levenscyclusacties - Vernietigen	Selecteer de werkstroom Een gebruiker vernietigen .
Aanvullende acties	<p>Selecteer de werkstroom Een gebruikerswachtwoord wijzigen.</p> <p>Voeg in het venster Actie toevoegen een naam voor de actie toe, zoals <code>password_change</code> en klik op Toevoegen.</p> <p>Als u het aanvraagformulier voor acties wilt wijzigen dat de gebruiker beantwoordt wanneer deze de actie aanvraagt, klikt u op het pictogram in de kolom Aanvraagparameters.</p> <hr/> <p>Opmerking Controleer voor aanvullende actiewerkstromen of de werkstroom een invoerparameter heeft van hetzelfde type als het externe type.</p>

In dit voorbeeld is er geen geschikte applicatie voor een updatewerkstroom. Een bekend voorbeeld van een updatewerkstroom, die wijzigingen aanbrengt op de ingerichte aangepaste resource, is het in- of uitschalen van een implementatie.

- g Controleer de schemasleutel en typewaarden in het tabblad **Eigenschappen**, zodat u de werkstroominvoer begrijpt en de invoer in de cloudsjabloon kunt configureren.

Het schema geeft de vereiste en optionele invoerwaarden weer die in de werkstroom zijn gedefinieerd. De vereiste invoerwaarden zijn opgenomen in de cloudsjabloon-YAML.

In de werkstroom Een gebruiker maken zijn `accountName`, `displayName` en `ouContainer` vereiste invoerwaarden. De andere schema-eigenschappen zijn niet vereist. U kunt het schema ook gebruiken om te bepalen waar u bindingen met andere veldwaarden, werkstromen of acties wilt maken. Bindingen zijn niet opgenomen in dit gebruiksscenario.

- h Om het maken van uw aangepaste resource te voltooien, klikt u op **Maken**.

2 Maak een cloudsjabloon die de gebruiker toevoegt aan een machine wanneer u deze implementeert.

- a Selecteer **Ontwerp > Cloudsjablonen** en klik op **Nieuw van > Leeg canvas**.
- b Geef de cloudsjabloon de naam **Machine met een AD-gebruiker**.
- c Selecteer het project **DevOpsTesting** en klik op **Maken**.
- d Voeg een vSphere-machine toe en configureer deze.
- e Sleep in de lijst met aangepaste resources aan de linkerkant van de ontwerppagina voor cloudsjablonen het resourcetype **AD-gebruiker** naar het canvas.

Opmerking U kunt de aangepaste resource selecteren door naar beneden te scrollen en deze te selecteren in het linkerdeelvenster, of ernaar te zoeken in het tekstvak **Resourcetypen zoeken**. Als de aangepaste resource niet wordt weergegeven, klikt u op de knop Vernieuwen naast het tekstvak **Resourcetypen zoeken**.

- f Bewerk aan de rechterkant de YAML-code om de verplichte invoerwaarden en het wachtwoord toe te voegen.

Voeg een `inputs`-sectie in de code toe zodat gebruikers de naam kunnen opgeven van de gebruikers die ze toevoegen. In het volgende voorbeeld zijn enkele van deze waarden voorbeeldgegevens. Uw waarden kunnen hiervan verschillen.

```
inputs:
  accountName:
    type: string
    title: Account name
    encrypted: true
  displayName:
    type: string
    title: Display name
  password:
    type: string
    title: Password
    encrypted: true
  confirmPassword:
    type: string
    title: Password
    encrypted: true
  ouContainer:
    type: object
    title: AD OU container
    $data: 'vro/data/inventory/AD:OrganizationalUnit'
    properties:
      id:
        type: string
      type:
        type: string
```

- g Voeg de code `${input.input-name}` toe in de sectie `resources` om gebruikers naar hun selectie te vragen.

```
resources:
  Custom_ADUser_1:
    type: Custom.ADUser
    properties:
      accountName: '${input.accountName}'
      displayName: '${input.displayName}'
      ouContainer: '${input.ouContainer}'
      password: '${input.password}'
      confirmPassword: '${input.confirmPassword}'
```

3 Implementeer de cloudsjabloon.

- a Klik op **Implementeren** op de ontwerppagina voor cloudsjablonen.
- b Voer de **implementatienaam AD-gebruiker Scott** in.

- c Selecteer de **Versie van cloudsjabloon** en klik op **Volgende**.
 - d Voltooi de implementatie-invoer.
 - e Klik op **Implementeren**.
- 4 Controleer de inrichtingsaanvraag op de pagina **Implementaties** om ervoor te zorgen dat de gebruiker wordt toegevoegd aan Active Directory en dat de implementatie wordt voltooid.

Wat nu te doen

Wanneer uw geteste cloudsjabloon werkt, kunt u vervolgens de aangepaste resource **AD-gebruiker** met andere cloudsjablonen gebruiken.

Een Cloud Assembly-sjabloon met SSH maken

U kunt aangepaste resources maken die u kunt gebruiken om cloudsjablonen te bouwen met behulp van vRealize Orchestrator-werkstromen. In dit gebruiksscenario voegt u een custom resource toe die een Secure Shell-host toevoegt. Vervolgens kunt u de resource opnemen in cloudsjablonen. Deze procedure voegt ook een updatewerkstroom toe zodat gebruikers wijzigingen in de Secure Shell-configuratie kunnen aanbrengen na de implementatie in plaats van individuele acties voor dag 2 uit te voeren.

Aangepaste resources zijn vRealize Orchestrator of uitbreidbaarheidsactieobjecten die u via vRealize Automation beheert met de levenscyclusacties die in de aangepaste resource zijn gedefinieerd. De cloudsjabloonservice roept automatisch de geschikte vRealize Orchestrator-werkstromen of -uitbreidbaarheidsacties op wanneer de bewerking wordt geactiveerd die is gekoppeld aan een specifieke levenscyclusactie. U kunt de functionaliteit van het resourcetype uitbreiden door ook vRealize Orchestrator-werkstromen of -uitbreidbaarheidsacties te selecteren die kunnen worden gebruikt als bewerkingen voor dag 2.

Dit gebruiksscenario gebruikt ingebouwde werkstromen die in de vRealize Orchestrator-bibliotheek zijn opgegeven. Het bevat beschrijvende waarden of tekenreeksen die aantonen hoe het proces moet worden uitgevoerd. U kunt deze aanpassen aan uw omgeving.

Voor referentiedoeleinden gebruikt dit scenario een project met de naam **DevOpsTesting**. U kunt het project vervangen door een van de bestaande projecten.

Voorwaarden

- Controleer of u een vRealize Orchestrator-integratie hebt geconfigureerd. Zie [vRealize Orchestrator-integratie in Cloud Assembly configureren](#).
- Controleer of de werkstromen die u gebruikt voor de acties voor maken, bijwerken, vernietigen en dag 2 bestaan in vRealize Orchestrator en dat ze correct worden uitgevoerd.
- Zoek in vRealize Orchestrator het resourcetype dat door de werkstromen wordt gebruikt. De werkstromen die zijn opgenomen in deze aangepaste resource moeten allemaal hetzelfde resourcetype gebruiken. In dit gebruiksscenario is het resourcetype `SSH:Host`. Zie [Typen aangepaste resources voor Cloud Assembly-cloudsjablonen](#) voor meer informatie over validatie van het resourcetype.

- Controleer of u weet hoe u een machinecloudsjabloon kunt configureren en implementeren.

Procedure

- 1 Maak een aangepaste Secure Shell-hostresource om Secure Shell toe te voegen aan een cloudsjabloon.

Deze stap voegt de aangepaste resource toe aan het cloudsjabloonontwerpcanvas als resourcetype.

- a Selecteer **Ontwerp > Aangepaste resources** in Cloud Assembly en klik op **Nieuwe aangepaste resource**.
- b Geef de volgende waarden op.

Onthoud dat dit, met uitzondering van de werkstroomnamen, voorbeeldwaarden zijn.

Tabel 6-3.

Instelling	Voorbeeldwaarde
Naam	Secure Shell-host - DevOpsTesting-project Dit is de naam die wordt weergegeven in het palet van het resourcetype voor de cloudsjabloon.
Resourcetype	Custom.SSHHost Het resourcetype moet beginnen met Custom. en elk resourcetype moeten uniek zijn. Hoewel de opname van Custom. niet is gevalideerd in het veld, wordt de tekenreeks automatisch toegevoegd als u deze verwijdt. Dit resourcetype wordt toegevoegd aan het ontwerpcanvas zodat u het in de cloudsjabloon kunt gebruiken.

- c Als u dit resourcetype wilt inschakelen in de lijst met resourcetypes van de cloudsjabloon, controleert u of de optie **Activeren** is ingeschakeld.
- d Selecteer de instelling **Bereik** die het resourcetype beschikbaar maakt voor het **DevOpsTesting**-project.
- e Controleer onder **Gebaseerd op** of **vRO-inventaris** is geselecteerd als provider voor levenscyclusacties.

- f Selecteer de werkstromen die de resource definiëren.

Instelling	Instelling
Levenscyclusacties - Maken	<p>Selecteer de werkstroom Secure Shell-host toevoegen.</p> <p>Als u meerdere vRealize Orchestrator-integraties hebt, selecteert u de werkstroom voor de integratie-instantie die u gebruikt om deze aangepaste resources uit te voeren.</p> <p>Nadat u de werkstroom hebt geselecteerd, komt het vervolgkeuzemenu Extern type beschikbaar en wordt het automatisch ingesteld op <code>SSH:Host</code>. Een extern brontype kan slechts één keer worden gebruikt als het wordt gedeeld en eenmaal per project. In dit scenario geeft u de aangepaste resource alleen op voor het DevOpsTesting-project. Als u andere werkstromen had waarvoor het type <code>SSH:Host</code> is vereist, moet u voor elk project individuele aangepaste resources maken.</p>
Levenscyclusacties - Update	Selecteer de werkstroom Secure Shell-host bijwerken .
Levenscyclusacties - Vernietigen	Selecteer de werkstroom Secure Shell-host verwijderen .

- g Controleer de schemasleutel en typewaarden in het tabblad **Eigenschappen**, zodat u de werkstroominvoer begrijpt en de invoer in de cloudsjabloon kunt configureren.

Het schema geeft de vereiste en optionele invoerwaarden weer die in de werkstroom zijn gedefinieerd. De vereiste invoerwaarden zijn opgenomen in de cloudsjabloon-YAML.

In de werkstroom **Secure Shell-host toevoegen** zijn `hostname`, `port` en `username` vereiste invoerwaarden. De andere schema-eigenschappen zijn niet vereist. U kunt het schema ook gebruiken om te bepalen waar u bindingen met andere veldwaarden, werkstromen of acties wilt maken. Bindingen zijn niet opgenomen in dit gebruiksscenario.

- h Om het maken van uw aangepaste resource te voltooien, klikt u op **Maken**.

- 2 Maak een cloudsjabloon die de Secure Shell-host toevoegt wanneer u deze implementeert.
 - a Selecteer **Ontwerp > Cloudsjablonen** en klik op **Nieuw van > Leeg canvas**.
 - b Geef de cloudsjabloon de naam **Machine met Secure Shell-host**.
 - c Selecteer het project **DevOpsTesting** en klik op **Maken**.
 - d Voeg een vSphere-machine toe en configureer deze.

- e Sleep in de lijst met aangepaste resources aan de linkerkant van de ontwerppagina voor cloudsjablonen het resourcetype **Secure Shell-host - DevOpsTesting-project** naar het canvas.

Opmerking U kunt de aangepaste resource selecteren door naar beneden te scrollen en deze te selecteren in het linkerdeelvenster, of ernaar te zoeken in het tekstvak **Resourcotypen zoeken**. Als de aangepaste resource niet wordt weergegeven, klikt u op de knop Vernieuwen naast het tekstvak **Resourcotypen zoeken**.

Ter herinnering: het resourcetype is beschikbaar omdat het is geconfigureerd voor het project. Als u een cloudsjabloon voor een ander project aan het maken was, kunt u het resourcetype niet zien.

- f Bewerk aan de rechterkant de YAML-code om de verplichte invoerwaarden toe te voegen.

Voeg een sectie `inputs` toe aan de code zodat gebruikers de gebruikersnaam en de hostnaam kunnen opgeven op het moment van de implementatie. In dit voorbeeld is de standaardpoort 22. In het volgende voorbeeld zijn enkele van deze waarden voorbeeldgegevens. Uw waarden kunnen hiervan verschillen.

```
inputs:
  hostname:
    type: string
    title: The hostname of the SSH Host
  username:
    type: string
    title: Username
```

- g Voeg de code `${input.input-name}` toe in de sectie `resources` om gebruikers naar hun selectie te vragen.

```
resources:
  Custom_SSHHost_1:
    type: Custom.SSHHost
    properties:
      port: 22
      hostname: '${input.hostname}'
      username: '${input.username}'
```

3 Implementeer de cloudsjabloon.

- a Klik op **Implementeren** op de ontwerppagina voor cloudsjablonen.
- b Voer de **Implementatienaam** **Secure Shell-hosttest** in.
- c Selecteer de **Versie van cloudsjabloon** en klik op **Volgende**.
- d Voltooi de implementatie-invoer.
- e Klik op **Implementeren**.

- 4 Controleer de inrichtingsaanvraag op de pagina **Implementaties** om ervoor te zorgen dat de SSH-host is opgenomen in de implementatie en dat de implementatie is gelukt.

Wat nu te doen

Wanneer uw geteste cloudsjabloon werkt, kunt u vervolgens de aangepaste resource `SSH Host` met andere cloudsjablonen gebruiken.

Cloud Assembly-ontwerpen als voorbereiding op wijzigingen voor dag 2

Naast de acties voor dag 2 die al zijn gekoppeld aan Cloud Assembly-resourcetypes, hebt u ontwerpopties waarmee u zich vooraf kunt voorbereiden op aangepaste updates die gebruikers mogelijk moeten uitvoeren.

Voorzichtig Als u een implementatie wilt wijzigen, kunt u de cloudsjabloon bewerken en opnieuw toepassen of kunt u acties voor dag 2 gebruiken. In de meeste gevallen is het echter beter om het gebruik van twee manieren door elkaar te vermijden.

Wijzigingen in levenscyclus voor dag 2, zoals in- en uitschakelen, zijn doorgaans veilig, maar voor andere is voorzichtigheid vereist, bijvoorbeeld bij het toevoegen van schijven.

Als u bijvoorbeeld schijven met een actie voor dag 2 toevoegt en vervolgens een gemengde benadering volgt door de cloudsjabloon opnieuw toe te passen, kan de cloudsjabloon de wijziging voor dag 2 overschrijven, waardoor mogelijk schijven worden verwijderd en gegevens verloren gaan.

De voorbereiding voor dag 2 kan direct gebruik van ofwel de cloudsjablooncode ofwel de Cloud Assembly-ontwerpinterface inhouden.

- U kunt invoer in cloudsjablooncode gebruiken zodat de interface bij het bijwerken van de implementatie of geïmplementeerde resource om nieuwe waarden vraagt.
- U kunt Cloud Assembly gebruiken om een aangepaste actie op basis van een vRealize Orchestrator-werkstroom of een uitbreidbaarheidsactie te ontwerpen. Het uitvoeren van de aangepaste actie zorgt ervoor dat workflow of uitbreidbaarheidsactie wijzigingen aanbrengt in de implementatie of geïmplementeerde resource.

Cloudsjablooninvoer voor vRealize Automation-updates voor dag 2 gebruiken

Wanneer u cloudsjablonen ontwerpt, geven vRealize Automation-invoerparameters gebruikers voor dag 2 toestemming om selecties opnieuw in te voeren vanuit de eerste implementatieaanvraag.

Voorzichtig Sommige eigenschapswijzigingen kunnen ervoor zorgen dat een resource opnieuw wordt gemaakt. Als u bijvoorbeeld de `connection_string.name` wijzigt onder een `Cloud.Service.Azure.App.Service` wordt de bestaande resource verwijderd en wordt er een nieuwe gemaakt.

Bij het ontwerpen van invoer ter ondersteuning van wijzigingen voor dag 2, helpt het schema [Gehoste modellen op code.vmware.com](#) u de eigenschappen te vinden die resources verwijderen en opnieuw maken.

Zie [Gebruikersinvoer in vRealize Automation-aanvragen](#) voor informatie over het maken van invoer.

Zie de volgende sectie voor een specifiek voorbeeld voor dag 2.

Een geïmplementeerde machine naar een ander netwerk verplaatsen

Terwijl u implementaties en netwerken onderhoudt, moet u mogelijk de mogelijkheid hebben om machines te verplaatsen die u met Cloud Assembly hebt geïmplementeerd.

U kunt een machine bijvoorbeeld eerst implementeren in een testnetwerk en vervolgens verplaatsen naar een productienetwerk. De techniek die hier wordt beschreven, stelt u in staat om een cloudsjabloon vooraf te ontwerpen en dergelijke acties voor dag 2 voor te bereiden. Houd er rekening mee dat de machine wordt verplaatst. Deze wordt niet verwijderd en opnieuw geïmplementeerd.

Deze procedure is alleen van toepassing op `Cloud.vSphere.Machine`-resources. Deze werkt niet voor cloudfanafhangelijke machines die zijn geïmplementeerd in vSphere.

Voorwaarden

- Het Cloud Assembly-netwerkprofiel moet alle subnetten bevatten waarmee de machine verbinding maakt. In Cloud Assembly kunt u netwerken controleren door naar **Infrastructuur > Configureren > Netwerkprofielen** te gaan.

Het netwerkprofiel moet zich bevinden in een account en regio die deel uitmaken van het juiste Cloud Assembly-project voor uw gebruikers.

- Tag de twee subnetten met verschillende tags. In het volgende voorbeeld wordt ervan uitgegaan dat **test** en **prod** de tagnamen zijn.
- De geïmplementeerde machine moet hetzelfde IP-toewijzingstype behouden. De machine kan niet worden gewijzigd van statisch in DHCP of andersom, terwijl u deze naar een ander netwerk verplaatst.

Procedure

- 1 Ga in Cloud Assembly naar **Ontwerp** en maak een cloudsjabloon voor de implementatie.
- 2 In de invoersectie van de code voegt u een vermelding toe waarmee de gebruiker een netwerk kan selecteren.

```
inputs:
  net-tagging:
    type: string
    enum:
      - test
      - prod
    title: Select a network
```

- 3 Voeg in de resourcesectie van de code **Cloud.Network** toe en verbind de vSphere-machine.
- 4 Maak onder **Cloud.Network** een beperking die verwijst naar de selectie vanuit de invoer.

```
resources:
  ABCServer:
    type: Cloud.vSphere.Machine
    properties:
      name: abc-server
      . . .
    networks:
      - network: '${resource["ABCNet"].id}'
  ABCNet:
    type: Cloud.Network
    properties:
      name: abc-network
      . . .
    constraints:
      - tag: '${input.net-tagging}'
```

- 5 Ga door met uw ontwerp en implementeer het op de gebruikelijke manier. Tijdens de implementatie wordt u gevraagd om het **test**- of **prod**-netwerk te selecteren.
- 6 Wanneer u een wijziging voor dag 2 wilt aanbrengen, gaat u naar **Resources > Implementaties** en zoekt u de implementatie die aan de cloudsjabloon is gekoppeld.
- 7 Klik rechts van de implementatie op **Acties > Bijwerken**.
- 8 In het paneel Bijwerken vraagt de interface u op dezelfde manier om het **test**- of **prod**-netwerk te selecteren.
- 9 Als u netwerken wilt wijzigen, selecteert u de gewenste optie, klikt u op **Volgende** en klikt u op **Verzenden**.

Een aangepaste Cloud Assembly-resourceactie maken voor een virtuele machine met vMotion

Nadat u een cloudsjabloon hebt geïmplementeerd, kunt u acties voor dag 2 uitvoeren die de implementatie wijzigen. Cloud Assembly omvat veel acties voor dag 2, maar u kunt er ook andere

opgeven. U kunt aangepaste resourceacties maken en deze voor gebruikers beschikbaar maken als acties voor dag 2.

De aangepaste resourceacties zijn gebaseerd op vRealize Orchestrator-werkstromen.

Dit voorbeeld van een aangepaste resourceactie voor dag 2 is bedoeld om u te introduceren in het aanmaakproces. Als u resourceacties effectief wilt gebruiken, moet u vRealize Orchestrator-werkstromen en -acties kunnen maken die de taken uitvoeren die u nodig hebt.

Voorwaarden

- Controleer of u een vRealize Orchestrator-integratie hebt geconfigureerd. Zie [vRealize Orchestrator-integratie in Cloud Assembly configureren](#).
- Controleer of de werkstroom die u gebruikt voor de actie voor dag 2 zich in vRealize Orchestrator bevindt en of deze correct wordt uitgevoerd.

Procedure

- 1 Maak een aangepaste resourceactie die vMotion gebruikt om een virtuele vSphere-machine van de ene naar de andere host te verplaatsen.
 - a Selecteer in Cloud Assembly **Ontwerp > Resourceacties** en klik op **Nieuwe resourceactie**.
 - b Geef de volgende waarden op.

Onthoud dat dit, met uitzondering van de werkstroomnamen, voorbeeldwaarden zijn.

Instelling	Voorbeeldwaarde
Naam	vSphere_VM_vMotion Dit is de naam die wordt weergegeven in de lijst met resourceacties.
Scherмнаam	VM verplaatsen Dit is de naam die gebruikers zien in het menu met implementatieacties.

- c Klik op de optie **Activeren** om deze actie in te schakelen in het menu met acties voor dag 2 voor resources die overeenkomen met het resourcetype.
- d Selecteer het resourcetype en de werkstroom die de actie voor dag 2 definiëren.

Instelling	Voorbeeldwaarde
Resourcetype	<p>Selecteer het resourcetype Cloud.vSphere.Machine. Dit is het resourcetype dat wordt geïmplementeerd als cloudsjabloononderdeel, niet noodzakelijkerwijs wat zich in de cloudsjabloon bevindt. U kunt bijvoorbeeld een cloudfonafhankelijke machine in uw cloudsjabloon hebben, maar wanneer deze wordt geïmplementeerd op een vCenter Server, is de machine Cloud.vSphere.Machine. Omdat de actie van toepassing is op het geïmplementeerde type, gebruikt u geen cloudfonafhankelijke typen wanneer u uw aangepaste resourceacties definieert.</p> <p>In dit voorbeeld werkt vMotion alleen voor vSphere-machines, maar u hebt mogelijk andere acties die u wilt uitvoeren op meerdere resourcetypes. U moet een actie maken voor elk resourcetype.</p>
Werkstroom	<p>Selecteer de werkstroom Virtuele machine met vMotion migreren.</p> <p>Als u meerdere vRealize Orchestrator-integraties hebt, selecteert u de werkstroom voor de integratie-instantie die u gebruikt om deze aangepaste resourceacties uit te voeren.</p>

- 2 Maak een binding voor de vRealize Orchestrator-eigenschappen aan de Cloud Assembly-schema-eigenschappen. Cloud Assembly-acties voor dag 2 ondersteunen drie typen bindingen.

Bindingstype	Beschrijving
in aanvraag	Het bindingstype voor de standaardwaarde. Wanneer dit is geselecteerd, wordt de invoereigenschap weergegeven in het aanvraagformulier en moet de waarde ervan tijdens de aanvraag worden opgegeven door de gebruiker.
met bindingactie	<p>Deze optie is alleen beschikbaar voor invoer van verwijzingstypen zoals:</p> <ul style="list-style-type: none"> ■ VC:VirtualMachine ■ VC:Folder <p>De gebruiker selecteert een actie die de binding uitvoert. De geselecteerde actie moet hetzelfde type retourneren als de invoerparameter. De juiste eigenschapsdefinitie is <code>\${properties.someProperty}</code>.</p>
direct	Deze optie is beschikbaar voor invoereigenschappen die primitieve gegevenstypen gebruiken. Indien geselecteerd, wordt de eigenschap met het geschikte type direct toegewezen vanuit het schema van de invoereigenschap. De gebruiker selecteert de eigenschap in de schemastructuur. Eigenschappen met verschillende typen zijn uitgeschakeld.

In dit scenario is de binding een vRealize Orchestrator-actie die de verbinding maakt tussen het vRealize Orchestrator `VC:VirtualMachine`-invoertype dat wordt gebruikt in de werkstroom en het Cloud Assembly `Cloud.vSphere.Machine`-resourcetype. Door de binding in te stellen, maakt u de actie voor dag 2 naadloos voor de gebruiker die de actie `vMotion` aanvraagt op een virtuele vSphere-machine. Het systeem geeft de naam in de werkstroom zodat de gebruiker dit niet hoeft te doen.

- a Nadat u de werkstroom **Virtuele machine met vMotion migreren** hebt geselecteerd, navigeert u naar het deelvenster **Eigenschapsbinding**.

- b Selecteer de binding van de `vm`-invoereigenschap.

- c Selecteer **met bindingactie** onder **Binding**.

De actie **findVcVmByVcAndVmUuid** wordt automatisch geselecteerd. Deze actie wordt vooraf geconfigureerd met uw vRealize Orchestrator-integratie in Cloud Assembly.

- d Klik op **Opslaan**.

- 3 Als u de wijzigingen in de actie voor dag 2 wilt opslaan, klikt u op **Maken**.

- 4 Als u de andere invoerparameters in de werkstroom wilt gebruiken, kunt u het aanvraagformulier aanpassen dat gebruikers zien wanneer ze de actie aanvragen.

- a Selecteer in **Resourceacties** de laatst gemaakte actie voor dag 2.
- b Klik op **Aanvraagparameters bewerken**.

U kunt aanpassen hoe de aanvraagpagina wordt weergegeven voor gebruikers.

Standaardveldnaam	Vormgeving	Waarden	Beperkingen
Bestemmingsresourcepool voor de virtuele machine. Standaard is de huidige resourcepool.	<ul style="list-style-type: none"> ■ Label = bestemmingsresourcepool ■ Weergavetype = waardekiezer 		
Doelhost waarnaar de virtuele machine moet worden gemigreerd	<ul style="list-style-type: none"> ■ Label = doelhost ■ Weergavetype = waardekiezer 		Vereist = Ja
Prioriteit van de migratietaak	Label = prioriteit van de taak	Waardeopties <ul style="list-style-type: none"> ■ Waardebron = Constante In het tekstvak voert u een door komma's gescheiden lijst in. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> lowPriority Low,defaultPriority Default,highPriority High </div>	Vereist = Ja
(Optioneel) Migreer de virtuele machine alleen als de aan-status overeenkomt met de opgegeven status	Verwijder dit tekstvak. vMotion kan machines met elke energiestatus verplaatsen.		

- c Klik op **Opslaan**.

- 5 Als u wilt beperken wanneer de actie beschikbaar is, kunt u de voorwaarden configureren.

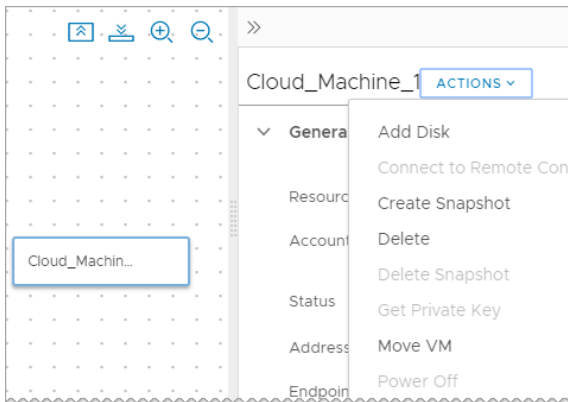
U wilt bijvoorbeeld alleen de actie vMotion beschikbaar maken wanneer de machine vier of minder CPU's heeft.

- a Schakel **Voorwaarde is vereist** in.
- b Voer de voorwaarde in.

Key	Operator	Waarde
\${properties.cpuCount}	lessThan	4

Zie [Geavanceerde voorwaarden voor aangepaste Cloud Assembly-acties bouwen](#) als u complexe voorwaarden nodig hebt.

- c Klik op **Bijwerken**.
- 6 Controleer of de actie VM verplaatsen beschikbaar is voor geïmplementeerde machines die aan de criteria voldoen.
- a Selecteer **Implementaties**.
 - b Zoek een implementatie die een geïmplementeerde machine bevat die voldoet aan de gedefinieerde criteria.
 - c Open de implementatie en selecteer de machine.
 - d Klik op acties in het rechterdeelvenster en controleer of de actie *Move VM* bestaat.

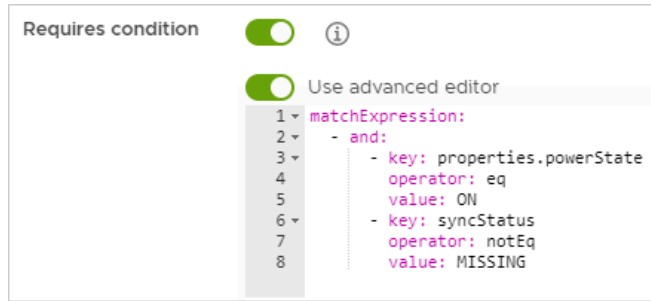


- e Voer de actie uit.

Geavanceerde voorwaarden voor aangepaste Cloud Assembly-acties bouwen

Als alternatief voor de lijst met eenvoudige voorwaarden in Cloud Assembly kunt u met de geavanceerde editor complexere criteria-expressies samenstellen om te bepalen wanneer de actie beschikbaar is.

Wanneer u een nieuwe resourceactie maakt, selecteert u **Voorwaarde is vereist** en **Geavanceerde editor gebruiken**. Voer vervolgens de gewenste criteria-expressie in.



De expressie is een component of lijst met componenten, die elk de indeling sleutel-operator-waarde hebben. De voorgaande afbeelding toont criteria waar het doel moet worden ingeschakeld en aanwezig moet zijn.

Componenten

Component	Beschrijving	Voorbeeld
en	Alle subcomponenten moeten waar zijn zodat het expressieresultaat waar is.	Resulteert alleen in waar wanneer zowel properties.powerState AAN is en syncStatus niet ONTBREEKT. <pre>matchExpression: - and: - key: properties.powerState operator: eq value: ON - key: syncStatus operator: notEq value: MISSING</pre>
of	Een of meer subcomponenten moeten waar zijn zodat het expressieresultaat waar kan zijn.	Resulteert in waar wanneer properties.powerState AAN of UIT is. <pre>matchExpression: - or: - key: properties.powerState operator: eq value: ON - key: properties.powerState operator: eq value: OFF</pre>

Operatoren

Operator	Beschrijving	Voorbeeld
eq	Gelijk aan. Zoek naar een exacte overeenkomst.	<p>Resulteert in waar wanneer properties.powerState AAN is.</p> <pre>matchExpression: - and: - key: properties.powerState operator: eq value: ON</pre>
notEq	Niet gelijk aan. Voorkom een exacte overeenkomst.	<p>Resulteert in waar wanneer properties.powerState niet UIT is.</p> <pre>matchExpression: - and: - key: properties.powerState operator: notEq value: OFF</pre>
hasAny	Zoek naar een overeenkomst in een verzameling van objecten.	<p>Resulteert in waar wanneer de array storage.disks een 100 IOPS EBS-object bevat.</p> <pre>matchExpression: - key: storage.disks operator: hasAny value: matchExpression: - and: - key: iops operator: eq value: 100 - key: service operator: eq value: ebs</pre>
in	Zoek naar een overeenkomst in een waardenset.	<p>Resulteert in waar wanneer properties.powerState UIT of OPHEFFEN is.</p> <pre>matchExpression: - and: - key: properties.powerState operator: in value: OFF, SUSPEND</pre>
notIn	Voorkom dat een waardenset overeenkomt.	<p>Resulteert in waar wanneer properties.powerState niet UIT of OPHEFFEN is.</p> <pre>matchExpression: - and: - key: properties.powerState operator: notIn value: OFF, SUSPEND</pre>

Operator	Beschrijving	Voorbeeld
greaterThan	Zoek naar een overeenkomst boven een bepaalde drempelwaarde. Alleen van toepassing op numerieke waarden.	Resulteert in waar wanneer het eerste object in de array storage.disks meer dan 50 IOPS heeft. <pre>matchExpression: - and: - key: storage.disks[0].iops operator: greaterThan value: 50</pre>
lessThan	Zoek naar een overeenkomst onder een bepaalde drempelwaarde. Alleen van toepassing op numerieke waarden.	Resulteert in waar wanneer het eerste object in de array storage.disks minder dan 200 IOPS heeft. <pre>matchExpression: - and: - key: storage.disks[0].iops operator: lessThan value: 200</pre>
greaterThanEquals	Zoek naar een overeenkomst op of boven een bepaalde drempelwaarde. Alleen van toepassing op numerieke waarden.	Resulteert in waar wanneer het eerste object in de array storage.disks 100 of meer IOPS heeft. <pre>matchExpression: - and: - key: storage.disks[0].iops operator: greaterThanEquals value: 100</pre>
lessThanEquals	Zoek naar een overeenkomst op of onder een bepaalde drempelwaarde. Alleen van toepassing op numerieke waarden.	Resulteert in waar wanneer het eerste object in de array storage.disks 100 of minder IOPS heeft. <pre>matchExpression: - and: - key: storage.disks[0].iops operator: lessThanEquals value: 100</pre>
matchesRegex	Gebruik een reguliere expressie om te zoeken naar een overeenkomst.	Resulteert in waar wanneer properties.zone us-east-1a of us-east-1c is. <pre>matchExpression: - and: - key: properties.zone operator: matchesRegex value: (us-east-1)+(a c) {1,2}</pre>

Voorbeelden

De volgende criteria-expressie resulteert in waar wanneer properties.tags een tag met sleutel `key1` en waarde `value1` bevat.

De buitenste expressie gebruikt `hasAny` omdat `properties.tags` een array is en u wilt dat deze resulteert in waar wanneer `key1=value1` wordt weergegeven in een van de sleutelwaardenparen in de array.

In de binnenste expressie staan twee componenten: één voor het sleutelveld en één voor het waardeveld. De array `properties.tags` bevat tagparen met sleutelwaarde en zowel de sleutel- als waardeelden moeten overeenkomen.

```
matchExpression:
  - key: properties.tags
    operator: hasAny
    value:
      matchExpression:
        - and:
            - key: key
              operator: eq
              value: key1
            - key: value
              operator: eq
              value: value1
```

De volgende criteria-expressie lijkt op het vorige voorbeeld, maar resulteert nu in waar wanneer `properties.tags` een tag met `key1=value1` of `key2=value2` bevat.

```
matchExpression:
  - or:
      - key: properties.tags
        operator: hasAny
        value:
          matchExpression:
            - and:
                - key: key
                  operator: eq
                  value: key1
                - key: value
                  operator: eq
                  value: value1
      - key: properties.tags
        operator: hasAny
        value:
          matchExpression:
            - and:
                - key: key
                  operator: eq
                  value: key2
                - key: value
                  operator: eq
                  value: value2
```

Meer voorbeelden van Cloud Assembly-code

De cloudsjablooncode in Cloud Assembly is bijna onbeperkt in combinatie en toepassing.

Vaak is een voorbeeld van succesvolle code uw beste beginpunt voor verdere ontwikkeling. Wanneer u een voorbeeld volgt, kunt u vervangingen uitvoeren om uw site-instellingen toe te passen in termen van resourcenames, waarden, enzovoort.

Voorbeeld van een gedocumenteerde Cloud Assembly-sjabloon

Dankzij een uitgebreide set opmerkingen kunt u in dit voorbeeld de structuur en het doel van de secties in een Cloud Assembly-sjabloon, voorheen een blueprint genoemd, bekijken.

```
# *****
#
# This WordPress cloud template is enhanced with comments to explain its
# parameters.
#
# Try cloning it and experimenting with its YAML code. If you're new to
# YAML, visit yaml.org for general information.
#
# The cloud template deploys a minimum of 3 virtual machines and runs scripts
# to install packages.
#
# *****
#
# -----
# Templates need a descriptive name and version if
# source controlled in git.
# -----
name: WordPress Template with Comments
formatVersion: 1
version: 1
#
# -----
# Inputs create user selections that appear at deployment time. Inputs
# can set placement decisions and configurations, and are referenced
# later, by the resources section.
# -----
inputs:
#
# -----
# Choose a cloud endpoint. 'Title' is the visible
# option text (oneOf allows for the friendly title). 'Const' is the
# tag that identifies the endpoint, which was set up earlier, under the
# Cloud Assembly Infrastructure tab.
# -----
platform:
  type: string
  title: Deploy to
  oneOf:
    - title: AWS
      const: aws
    - title: Azure
      const: azure
    - title: vSphere
      const: vsphere
  default: vsphere
```



```

#
# -----
# Choose the operating system. Note that the Cloud Assembly
# Infrastructure must also have an AWS, Azure, and vSphere Ubuntu image
# mapped. In this case, enum sets the option that you see, meaning there's
# no friendly title feature this time. Also, only Ubuntu is available
# here, but having this input stubbed in lets you add more operating
# systems later.
# -----
osimage:
  type: string
  title: Operating System
  description: Which OS to use
  enum:
    - Ubuntu
#
# -----
# Set the number of machines in the database cluster. Small and large
# correspond to 1 or 2 machines, respectively, which you see later,
# down in the resources section.
# -----
dbenvsize:
  type: string
  title: Database cluster size
  enum:
    - Small
    - Large
#
# -----
# Dynamically tag the machines that will be created. The
# 'array' of objects means you can create as many key-value pairs as
# needed. To see how array input looks when it's collected,
# open the cloud template and click TEST.
# -----
Mtags:
  type: array
  title: Tags
  description: Tags to apply to machines
  items:
    type: object
    properties:
      key:
        type: string
        title: Key
      value:
        type: string
        title: Value
#
# -----
# Create machine credentials. These credentials are needed in
# remote access configuration later, in the resources section.
# -----
username:
  type: string
  minLength: 4

```

```

    maxLength: 20
    pattern: '[a-z]+'
    title: Database Username
    description: Database Username
  userpassword:
    type: string
    pattern: '[a-z0-9A-Z@#\$]+'
    encrypted: true
    title: Database Password
    description: Database Password
#
# -----
# Set the database storage disk size.
# -----
databaseDiskSize:
  type: number
  default: 4
  maximum: 10
  title: MySQL Data Disk Size
  description: Size of database disk
#
# -----
# Set the number of machines in the web cluster. Small, medium, and large
# correspond to 2, 3, and 4 machines, respectively, which you see later,
# in the WebTier part of the resources section.
# -----
clusterSize:
  type: string
  enum:
    - small
    - medium
    - large
  title: Wordpress Cluster Size
  description: Wordpress Cluster Size
#
# -----
# Set the archive storage disk size.
# -----
archiveDiskSize:
  type: number
  default: 4
  maximum: 10
  title: Wordpress Archive Disk Size
  description: Size of Wordpress archive disk
#
# -----
# The resources section configures the deployment of machines, disks,
# networks, and other objects. In several places, the code pulls from
# the preceding interactive user inputs.
# -----
resources:
#
# -----
# Create the database server. Choose a cloud agnostic machine 'type' so
# that it can deploy to AWS, Azure, or vSphere. Then enter its property

```

```

# settings.
# -----
DBTier:
  type: Cloud.Machine
  properties:
#
# -----
# Descriptive name for the virtual machine. Does not become the hostname
# upon deployment.
# -----
    name: mysql
#
# -----
# Hard-coded operating system image to use. To pull from user input above,
# enter the following instead.
# image: '${input.osimage}'
# -----
    image: Ubuntu
#
# -----
# Hard-coded capacity to use. Note that the Cloud Assembly
# Infrastructure must also have AWS, Azure, and vSphere flavors
# such as small, medium, and large mapped.
# -----
    flavor: small
#
# -----
# Tag the database machine to deploy to the cloud vendor chosen from the
# user input. Tags are case-sensitive, so 'to_lower' forces the tag to
# lowercase to ensure a match with a site's tagging convention. It's
# important if platform input were to contain any upper case characters.
# -----
    constraints:
      - tag: '${"env:" + to_lower(input.platform)}'
#
# -----
# Also tag the database machine with any free-form tags that were created
# during user input.
# -----
    tags: '${input.Mtags}'
#
# -----
# Set the database cluster size by referencing the dbenvsize user
# input. Small is one machine, and large defaults to two.
# -----
    count: '${input.dbenvsize == "Small" ? 1 : 2}'
#
# -----
# Add a variable to connect the machine to a network resource based on
# a property binding to another resource. In this case, it's the
# 'WP_Network' network that gets defined further below.
# -----
    networks:
      - network: '${resource.WP_Network.id}'
#

```

```

# -----
# Enable remote access to the database server. Reference the credentials
# from the user input.
# -----
    remoteAccess:
      authentication: usernamePassword
      username: '${input.username}'
      password: '${input.userpassword}'
#
# -----
# You are free to add custom properties, which might be used to initiate
# an extensibility subscription, for example.
# -----
    ABC-Company-ID: 9393
#
# -----
# Run OS commands or scripts to further configure the database machine,
# via operations such as setting a hostname, generating SSH private keys,
# or installing packages.
# -----
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
      packages:
        - mysql-server
      runcmd:
        - sed -e '/bind-address/ s/^#*\/#/' -i /etc/mysql/mysql.conf.d/mysqld.cnf
        - service mysql restart
        - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'mysqlpassword';"
        - mysql -e "FLUSH PRIVILEGES;"
    attachedDisks: []
#
# -----
# Create the web server. Choose a cloud agnostic machine 'type' so that it
# can deploy to AWS, Azure, or vSphere. Then enter its property settings.
# -----
    WebTier:
      type: Cloud.Machine
      properties:
#
# -----
# Descriptive name for the virtual machine. Does not become the hostname
# upon deployment.
# -----
    name: wordpress
#
# -----
# Hard-coded operating system image to use. To pull from user input above,
# enter the following instead:
# image: '${input.osimage}'
# -----
    image: Ubuntu
#
# -----

```

```

# Hard-coded capacity to use. Note that the Cloud Assembly
# Infrastructure must also have AWS, Azure, and vSphere flavors
# such as small, medium, and large mapped.
# -----
#     flavor: small
#
# -----
# Set the web server cluster size by referencing the clusterSize user
# input. Small is 2 machines, medium is 3, and large defaults to 4.
# -----
#     count: '${input.clusterSize== "small" ? 2 : (input.clusterSize == "medium" ? 3 : 4)}'
#
# -----
# Set an environment variable to display object information under the
# Properties tab, post-deployment. Another example might be
# {env.blueprintID}
# -----
#     tags:
#       - key: cas.requestedBy
#         value: '${env.requestedBy}'
#
# -----
# You are free to add custom properties, which might be used to initiate
# an extensibility subscription, for example.
# -----
#     ABC-Company-ID: 9393
#
# -----
# Tag the web server to deploy to the cloud vendor chosen from the
# user input. Tags are case-sensitive, so 'to_lower' forces the tag to
# lowercase to ensure a match with your site's tagging convention. It's
# important if platform input were to contain any upper case characters.
# -----
#     constraints:
#       - tag: '${"env:" + to_lower(input.platform)}'
#
# -----
# Add a variable to connect the machine to a network resource based on
# a property binding to another resource. In this case, it's the
# 'WP_Network' network that gets defined further below.
# -----
#     networks:
#       - network: '${resource.WP_Network.id}'
#
# -----
# Run OS commands or scripts to further configure the web server,
# with operations such as setting a hostname, generating SSH private keys,
# or installing packages.
# -----
#     cloudConfig: |
#       #cloud-config
#       repo_update: true
#       repo_upgrade: all
#       packages:
#         - apache2

```

```

- php
- php-mysql
- libapache2-mod-php
- php-mcrypt
- mysql-client
runcmd:
  - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
mywordpresssite --strip-components 1
  - i=0; while [ $i -le 5 ]; do mysql --connect-timeout=3 -h $
{DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;
i=$((i+1)); done
  - mysql -u root -pmysqlpassword -h ${resource.DBTier.networks[0].address} -e
"create database wordpress_blog;"
  - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/
mywordpresssite/wp-config.php
  - sed -i -e s/"define('DB_NAME', 'database_name_here');"/"define('DB_NAME',
'wordpress_blog');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
-e s/"define('DB_USER', 'username_here');"/"define('DB_USER', 'root');"/ /var/www/html/
mywordpresssite/wp-config.php && sed -i -e s/"define('DB_PASSWORD',
'password_here');"/"define('DB_PASSWORD', 'mysqlpassword');"/ /var/www/html/mywordpresssite/
wp-config.php && sed -i -e s/"define('DB_HOST', 'localhost');"/"define('DB_HOST', '$
{resource.DBTier.networks[0].address}');"/ /var/www/html/mywordpresssite/wp-config.php
  - service apache2 reload
#
# -----
# Create the network that the database and web servers connect to.
# Choose a cloud agnostic network 'type' so that it can deploy to AWS,
# Azure, or vSphere. Then enter its property settings.
# -----
WP_Network:
  type: Cloud.Network
  properties:
#
# -----
# Descriptive name for the network. Does not become the network name
# upon deployment.
# -----
    name: WP_Network
#
# -----
# Set the networkType to an existing network. You could also use a
# constraint tag to target a specific, like-tagged network.
# The other network types are private or public.
# -----
    networkType: existing
#
# *****
#
# VMware hopes that you found this commented template useful. Note that
# you can also access an API to create templates, or query for input
# schema that you intend to request. See the following Swagger
# documentation.

```

```
#
# www.mgmt.cloud.vmware.com/blueprint/api/swagger/swagger-ui.html
#
# *****
```

Voorbeelden van vSphere-resources in Cloud Assembly

In deze codevoorbeelden worden vSphere-machineresources in Cloud Assembly-cloudsjablonen gedefinieerd.

Resource	Voorbeeld van cloudsjabloon
Virtuele vSphere-machine met CPU, geheugen en besturingssysteem	<pre>resources: demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine cpuCount: 1 totalMemoryMB: 1024 image: ubuntu</pre>
vSphere-machine met een gegevensopslagresource	<pre>resources: demo-vsphere-disk-001: type: Cloud.vSphere.Disk properties: name: DISK_001 type: 'HDD' capacityGb: 10 dataStore: 'datastore-01' provisioningType: thick</pre>
vSphere-machine met gekoppelde schijf	<pre>resources: demo-vsphere-disk-001: type: Cloud.vSphere.Disk properties: name: DISK_001 type: HDD capacityGb: 10 dataStore: 'datastore-01' provisioningType: thin demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine cpuCount: 2 totalMemoryMB: 2048 imageRef: >- https://packages.vmware.com/photon/4.0/ Rev1/ova/photon-ova-4.0-ca7c9e9330.ova attachedDisks: - source: '\${demo-vsphere-disk-001.id}'</pre>

Resource	Voorbeeld van cloudsjabloon
vSphere-machine met een dynamisch aantal schijven	<pre> inputs: disks: type: array title: disks items: title: disks type: integer maxItems: 15 resources: Cloud_Machine_1: type: Cloud.vSphere.Machine properties: image: Centos flavor: small attachedDisks: '\$ {map_to_object(resource.Cloud_Volume_1[*].id, "source")}' Cloud_Volume_1: type: Cloud.Volume allocatePerInstance: true properties: capacityGb: '\${input.disks[count.index]}' count: '\${length(input.disks)}' </pre>
vSphere-machine op basis van een image van een momentopname Voeg een slash en de naam van de momentopname toe. De image van de momentopname kan een gekoppelde kloon zijn.	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: imageRef: 'demo-machine/snapshot-01' cpuCount: 1 totalMemoryMB: 1024 </pre>
vSphere-machine in een specifieke map in vCenter	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine cpuCount: 2 totalMemoryMB: 1024 imageRef: ubuntu resourceGroupName: 'myFolder' </pre>

Resource	Voorbeeld van cloudsjabloon
vSphere-machine met meerdere NIC's	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: image: ubuntu flavor: small networks: - network: '\${network-01.name}' deviceIndex: 0 - network: '\${network-02.name}' deviceIndex: 1 network-01: type: Cloud.vSphere.Network properties: name: network-01 network-02: type: Cloud.vSphere.Network properties: name: network-02 </pre>
vSphere-machine met een gekoppelde tag in vCenter	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu tags: - key: env value: demo </pre>

Resource	Voorbeeld van cloudsjabloon
vSphere-machine met een aanpassingsspecificatie	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine image: ubuntu flavor: small customizationSpec: Linux </pre>
vSphere-machine met externe toegang	<pre> inputs: username: type: string title: Username description: Username default: testUser password: type: string title: Password default: VMware@123 encrypted: true description: Password for the given username resources: demo-machine: type: Cloud.vSphere.Machine properties: flavor: small imageRef: >- https://cloud-images.ubuntu.com/releases/ 16.04/release-20170307/ubuntu-16.04-server-cloudimg- amd64.ova cloudConfig: ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' runcmd: - echo "Defaults:\${input.username} ! requiretty" >> /etc/sudoers.d/\${input.username} </pre>

Kernen per socket en aantal CPU's in Cloud Assembly

Met Cloud Assembly-sjablooncode kunt u een aantal kernen per socket voor een vSphere-machineresource opgeven.

U kunt het aantal kernen per virtuele socket of het totale aantal sockets opgeven. In uw licentievoorwaarden wordt bijvoorbeeld vermeld dat software die per socket is gelicentieerd wordt beperkt, of dat beschikbare besturingssystemen mogelijk slechts een bepaald aantal sockets herkennen zodat extra CPU's moeten worden ingericht als extra kernen.

Voeg de eigenschap `coreCount` toe aan een cloudsjabloon in de vSphere-machineresource.

De waarde voor `coreCount` moet kleiner zijn dan of gelijk zijn aan de waarde voor het aantal CPU's (`cpuCount`) die is opgegeven in de soorttoewijzing of in de resourcecode van de vSphere-machine in de cloudsjabloon. Zie [Setting the number of cores per CPU in a virtual machine \(1010184\)](#) voor gerelateerde informatie.

De eigenschap `coreCount` is optioneel en is alleen beschikbaar voor vSphere-machineresources.

Een voorbeeldfragment van een vSphere-machineresource wordt hieronder weergegeven.

```
Cloud_vSphere_Machine_1:
  type: Cloud.vSphere.Machine
  properties:
    cpuCount: 8
    coreCount: 4
```

Aanvullende informatie over sockets en instellingen voor kernen per socket is beschikbaar in het blogartikel [Virtual Machine vCPU and vNUMA Rightsizing – Guidelines](#).

Netwerken, beveiligingsgroepen en load balancers in vRealize Automation

U kunt resources en instellingen voor netwerken, beveiliging en load balancers gebruiken in cloudsjabloonontwerpen en -implementaties.

Zie [vRealize Automation Resource Type Schema](#) voor een samenvatting van de opties voor cloudsjabloonontwerpcodes.

Voor gerelateerde informatie zie:

- [Meer informatie over netwerkresources in vRealize Automation-cloudsjablonen](#)
- [Meer informatie over beveiligingsgroep- en tagresources in vRealize Automation-cloudsjablonen](#)
- [Meer informatie over load-balancerresources in vRealize Automation-cloudsjablonen](#)

Deze voorbeelden tonen de resources voor netwerk, beveiliging en load balancer in een standaardontwerp van cloudsjablonen.

Netwerken

Resource scenario	Voorbeeldontwerpcodes voor cloudsjabloon
vSphere-machine met meerdere NIC's die zijn verbonden met vSphere- en NSX-netwerken met DHCP IP-toewijzing	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: image: ubuntu flavor: small networks: - network: \${resource["demo-vSphere- Network"].id} deviceIndex: 0 - network: \${resource["demo-NSX- Network"].id} deviceIndex: 1 demo-vSphere-Network: type: Cloud.vSphere.Network properties: networkType: existing demo-NSX-Network: type: Cloud.NSX.Network properties: networkType: outbound </pre>
Een privénetwerk met een statisch IP-adres voor een Azure VM-implementatie toevoegen	<pre> formatVersion: 1 inputs: {} resources: Cloud_Azure_Machine_1: type: Cloud.Azure.Machine properties: image: photon flavor: Standard_B1ls networks: - network: '\${ {resource.Cloud_Network_1.id}' assignment: static address: 10.0.0.45 assignPublicIpAddress: false Cloud_Network_1: type: Cloud.Network properties: networkType: existing </pre>

Resource scenario	Voorbeeldontwerpcode voor cloudsjabloon
<p>U kunt een vast toegewezen IP-adres gebruiken met vRealize IPAM (intern zoals geleverd door vRealize Automation of extern op basis van de vRA IPAM SDK, zoals voor een van de Infoblox-invoegtoepassingen die beschikbaar zijn in de VMware Marketplace). Andere gebruiken van <code>assignment: static</code> worden niet ondersteund, zoals beschreven in de sectie <i>Restricties</i> van Meer informatie over netwerkresources in vRealize Automation-cloudsjablonen.</p>	<pre>resources: demo_vm: type: Cloud.vSphere.Machine properties: image: 'photon' cpuCount: 1 totalMemoryMB: 1024 networks: - network: \${resource.demo_nw.id} assignment: static demo_nw: type: Cloud.vSphere.Network properties: networkType: existing</pre>

Resource scenario	Voorbeeldontwerpcodes voor cloudsjabloon
<p>Voeg regels voor NAT en DNAT port mapping toe of bewerk deze in een Cloud.NSX.NAT-resource voor een bestaande implementatie.</p>	<pre> resources: gw: type: Cloud.NSX.Gateway properties: networks: - \${resource.akout.id} nat: type: Cloud.NSX.Nat properties: networks: - \${resource.akout.id} natRules: - translatedInstance: \$ {resource.centos.networks[0].id} index: 0 protocol: TCP kind: NAT44 type: DNAT sourceIPs: any sourcePorts: 80 translatedPorts: 8080 destinationPorts: 8080 description: edit - translatedInstance: \$ {resource.centos.networks[0].id} index: 1 protocol: TCP kind: NAT44 type: DNAT sourceIPs: any sourcePorts: 90 translatedPorts: 9090 destinationPorts: 9090 description: add gateway: \${resource.gw.id} centos: type: Cloud.vSphere.Machine properties: image: WebTinyCentOS65x86 flavor: small customizationSpec: Linux networks: - network: \${resource.akout.id} assignment: static akout: type: Cloud.NSX.Network properties: networkType: outbound constraints: - tag: nsxt-nat-1-M2 </pre>

Resource scenario	Voorbeeldontwerpcodes voor cloudsjabloon
<p>Publieke cloudmachine gebruikt een intern IP-adres in plaats van een openbaar IP. In dit voorbeeld wordt een specifieke netwerk-ID gebruikt.</p> <p>N.b: de optie <code>network:</code> wordt gebruikt in de instelling <code>networks:</code> om een doelnetwerk-ID op te geven. De optie <code>name:</code> in de instelling <code>networks:</code> is verouderd en mag niet worden gebruikt.</p>	<pre>resources: wf_proxy: type: Cloud.Machine properties: image: ubuntu 16.04 flavor: small constraints: - tag: 'platform:vsphere' networks: - network: '\${resource.wf_net.id}' assignPublicIpAddress: false</pre>
<p>Gerouteerd netwerk voor NSX-V of NSX-T met behulp van het NSX-netwerkrecursoetype.</p>	<pre>Cloud_NSX_Network_1: type: Cloud.NSX.Network properties: networkType: routed</pre>
<p>Voeg een tag toe aan een machine-NIC-resource in de cloudsjabloon.</p>	<pre>formatVersion: 1 inputs: {} resources: Cloud_Machine_1: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu networks: - name: '\${resource.Cloud_Network_1.name}' deviceIndex: 0 tags: - key: 'nic0' value: null - key: internal value: true - name: '\${resource.Cloud_Network_2.name}' deviceIndex: 1 tags: - key: 'nic1' value: null - key: internal value: false</pre>
<p>Tag logische schakelopties van NSX-T voor een uitgaand netwerk.</p> <p>Taggen wordt ondersteund voor NSX-T en VMware Cloud on AWS.</p> <p>Voor meer informatie over dit scenario verwijzen we u naar het blogbericht Creating Tags in NSX with Cloud Assembly in de community.</p>	<pre>Cloud_NSX_Network_1: type: Cloud.NSX.Network properties: networkType: outbound tags: - key: app value: opencart</pre>

Beveiligingsgroepen

Resource scenario	Voorbeeldontwerpcodes voor cloudsjabloon
<p>Bestaande beveiligingsgroep met een beperkingstag die wordt toegepast op een machine-NIC.</p> <p>Als u een bestaande beveiligingsgroep wilt gebruiken, voert u <i>bestaand</i> in voor de eigenschap <code>securityGroupType</code>.</p> <p>U kunt tags toewijzen aan een <code>Cloud.SecurityGroup</code>-resource om bestaande beveiligingsgroepen toe te wijzen met behulp van tagbeperkingen. Beveiligingsgroepen die geen tags bevatten, kunnen niet worden gebruikt in het cloudsjabloonontwerp.</p> <p>Beperkingstags moeten worden ingesteld voor <code>securityGroupType: existing-beveiligingsgroepresources</code>. Deze beperkingen moeten overeenstemmen met de tags die zijn ingesteld voor de bestaande beveiligingsgroepen. Beperkingstags kunnen niet worden ingesteld voor <code>securityGroupType: new-beveiligingsgroepresources</code>.</p>	<pre>formatVersion: 1 inputs: {} resources: allowSsh_sg: type: Cloud.SecurityGroup properties: securityGroupType: existing constraints: - tag: allowSsh compute: type: Cloud.Machine properties: image: centos flavor: small networks: - network: '\${resource.prod-net.id}' securityGroups: - '\${resource.allowSsh_sg.id}' prod-net: type: Cloud.Network properties: networkType: existing</pre>
<p>Beveiligingsgroep op aanvraag met twee firewallregels die de Allow- en Deny-toegangsopties illustreren.</p>	<pre>resources: Cloud_SecurityGroup_1: type: Cloud.SecurityGroup properties: securityGroupType: new rules: - ports: 5000 source: 'fc00:10:000:000:000:56ff:fe89:48b4' access: Allow direction: inbound name: allow_5000 protocol: TCP - ports: 7000 source: 'fc00:10:000:000:000:56ff:fe89:48b4' access: Deny direction: inbound name: deny_7000</pre>

Resource scenario	Voorbeeldontwerpcodes voor cloudsjabloon
	<pre> protocol: TCP Cloud_vSphere_Machine_1: type: Cloud_vSphere.Machine properties: image: photon cpuCount: 1 totalMemoryMB: 256 networks: - network: '\$ {resource.Cloud_Network_1.id}' assignIPv6Address: true assignment: static securityGroups: - '\$ {resource.Cloud_SecurityGroup_1.id}' Cloud_Network_1: type: Cloud.Network properties: networkType: existing </pre>
<p>Complexe cloudsjabloon met 2 beveiligingsgroepen, waaronder:</p> <ul style="list-style-type: none"> ■ 1 bestaande beveiligingsgroep ■ 1 beveiligingsgroep op aanvraag met meerdere voorbeelden van firewallregels ■ 1 vSphere-machine ■ 1 bestaand netwerk <p>In dit voorbeeld ziet u verschillende combinaties van protocollen en poorten, services, IP CIDR als bron en doel, IP-bereik als bron of bestemming, en de opties voor alle, IPv6 en (::/0).</p> <p>Voor machine-NIC's kunt u het verbonden netwerk en de beveiligingsgroep(en) opgeven. U kunt ook de NIC-index of een IP-adres opgeven.</p>	<pre> formatVersion: 1 inputs: {} resources: DEMO_ESG : <i>existing security group - security group 1)</i> type: Cloud.SecurityGroup properties: constraints: - tag: BlockAll securityGroupType: existing (<i>designation of existing for security group 1)</i> DEMO_ODSG: (<i>on-demand security group - security group 2)</i>) type: Cloud.SecurityGroup properties: rules: (<i>multiple firewall rules in this section</i>) - name: IN-ANY (<i>rule 1</i>) source: any service: any direction: inbound access: Deny - name: IN-SSH (<i>rule 2</i>) source: any service: SSH direction: inbound access: Allow - name: IN-SSH-IP (<i>rule 3</i>) source: 33.33.33.1-33.33.33.250 protocol: TCP ports: 223 direction: inbound access: Allow - name: IPv-6-ANY-SOURCE (<i>rule 4</i>) source: '::/0' protocol: TCP ports: 223 direction: inbound access: Allow - name: IN-SSH-IP (<i>rule 5</i>) source: 44.44.44.1/24 protocol: UDP </pre>

Resource scenario	Voorbeeldontwerpcodes voor cloudsjabloon
	<pre> ports: 22-25 direction: inbound access: Allow - name: IN-EXISTING-SG (rule 6) source: '\${resource["DEMO_ESG"].id}' protocol: ICMPv6 direction: inbound access: Allow - name: OUT-ANY (rule 7) destination: any service: any direction: outbound access: Deny - name: OUT-TCP-IPv6 (rule 8) destination: '2001:0db8:85a3::8a2e:0370:7334/64' protocol: TCP ports: 22 direction: outbound access: Allow - name: IPv6-ANY-DESTINATION (rule 9) destination: '::/0' protocol: UDP ports: 23 direction: outbound access: Allow - name: OUT-UDP-SERVICE (rule 10) destination: any service: NTP direction: outbound access: Allow securityGroupType: new (designation of on- demand for security group 2) DEMO_VC_MACHINE: (machine resource) type: Cloud.vSphere.Machine properties: image: PHOTON cpuCount: 1 totalMemoryMB: 1024 networks: (Machine network NICs) - network: '\${resource.DEMO_NW.id}' securityGroups: - '\${resource.DEMO_ODSG.id}' - '\${resource.DEMO_ESG.id}' DEMO_NETWORK: (network resource) type: Cloud.vSphere.Network properties: networkType: existing constraints: - tag: nsx62 </pre>

Load balancers

Resource scenario	Voorbeeldontwerpcodes voor cloudsjabloon
Geef een logboekregistratieniveau, algoritme en grootte op voor de load balancer.	<p>Een voorbeeld van een NSX-load balancer met het gebruik van het logboekregistratieniveau, het algoritme en de grootte:</p> <pre>resources: Cloud_LoadBalancer_1: type: Cloud.NSX.LoadBalancer properties: name: myapp-lb network: '\${appnet-public.name}' instances: '\${wordpress.id}' routes: - protocol: HTTP port: '80' loggingLevel: CRITICAL algorithm: LEAST_CONNECTION type: MEDIUM</pre>
<p>Koppel een load balancer aan een benoemde machine of een benoemde machine-NIC. U kunt <code>machine ID</code> of <code>machine network ID</code> opgeven om de machine toe te voegen aan de pool met load balancers. De eigenschap van de instantie ondersteunt zowel machines (<code>machine by ID</code>) als NIC's (<code>machine by network ID</code>).</p> <p>In het eerste voorbeeld gebruikt de implementatie de <code>machine by ID</code>-instelling om de machine te verdelen wanneer deze op een netwerk wordt geïmplementeerd.</p> <p>In het tweede voorbeeld gebruikt de implementatie de <code>machine by network ID</code>-instelling om de machine alleen te verdelen wanneer de machine wordt geïmplementeerd op de genoemde machine-NIC.</p> <p>Het derde voorbeeld toont beide instellingen die worden gebruikt in dezelfde <code>instances</code>-optie.</p>	<p>U kunt de eigenschap <code>instances</code> gebruiken om een machine-ID of een machinenetwerk-ID te definiëren:</p> <p>■ Machine-ID</p> <pre>Cloud_LoadBalancer_1: type: Cloud.LoadBalancer properties: network: '\${resource.Cloud_Network_1.id}' instances: '\$ {resource.Cloud_Machine_1.id}'</pre> <p>■ Machinenetwerk-ID</p> <pre>Cloud_LoadBalancer_1: type: Cloud.LoadBalancer properties: network: '\${resource.Cloud_Network_1.id}' instances: '\$ {resource.Cloud_Machine_1.networks[0].id}'</pre> <p>■ Er is één machine opgegeven voor het opnemen van de load balancer en een andere machine-NIC die is opgegeven voor het opnemen van de load balancer:</p> <pre>instances: - resource.Cloud_Machine_1.id - resource.Cloud_Machine_2.networks[2].id</pre>

Resource scenario	Voorbeeldontwerpcodes voor cloudsjabloon
<p>Voeg instellingen voor statuscontrole toe aan een NSX load balancer. Aanvullende opties zijn <code>httpMethod</code>, <code>requestBody</code> en <code>responseBody</code>.</p>	<pre>myapp-lb: type: Cloud.NSX.LoadBalancer properties: name: myapp-lb network: '\${appnet-public.name}' instances: '\${wordpress.id}' routes: - protocol: HTTP port: '80' algorithm: ROUND_ROBIN instanceProtocol: HTTP instancePort: '80' healthCheckConfiguration: protocol: HTTP port: '80' urlPath: /mywordpresssite/wp-admin/ install.php intervalSeconds: 60 timeoutSeconds: 10 unhealthyThreshold: 10 healthyThreshold: 2 connectionLimit: '50' connectionRateLimit: '50' maxConnections: '500' minConnections: '' internetFacing: true{code}</pre>

Resource scenario	Voorbeeldontwerpcodes voor cloudsjabloon
Netwerk op aanvraag met een load balancer met 1 arm.	<pre> inputs: {} resources: mp-existing: type: Cloud.Network properties: name: mp-existing networkType: existing mp-wordpress: type: Cloud.vSphere.Machine properties: name: wordpress count: 2 flavor: small image: tiny customizationSpec: Linux networks: - network: '\${resource["mp-private"].id}' mp-private: type: Cloud.NSX.Network properties: name: mp-private networkType: private constraints: - tag: nsxt mp-wordpress-lb: type: Cloud.LoadBalancer properties: name: wordpress-lb internetFacing: false network: '\${resource.mp-existing.id}' instances: '\${resource["mp-wordpress"].id}' routes: - protocol: HTTP port: '80' instanceProtocol: HTTP instancePort: '80' healthCheckConfiguration: protocol: HTTP port: '80' urlPath: /index.pl intervalSeconds: 60 timeoutSeconds: 30 unhealthyThreshold: 5 healthyThreshold: 2 </pre>
Bestaand netwerk met een load balancer.	<pre> formatVersion: 1 inputs: count: type: integer default: 1 resources: ubuntu-vm: type: Cloud.Machine properties: name: ubuntu flavor: small image: tiny count: '\${input.count}' networks: </pre>

Resource scenario	Voorbeeldontwerpcodes voor cloudsjabloon
	<pre> - network: '\$ {resource.Cloud_NSX_Network_1.id}' Provider_LoadBalancer_1: type: Cloud.LoadBalancer properties: name: OC-LB routes: - protocol: HTTP port: '80' instanceProtocol: HTTP instancePort: '80' healthCheckConfiguration: protocol: HTTP port: '80' urlPath: /index.html intervalSeconds: 60 timeoutSeconds: 5 unhealthyThreshold: 5 healthyThreshold: 2 network: '\$ {resource.Cloud_NSX_Network_1.id}' internetFacing: false instances: '\${resource["ubuntu-vm"].id}' Cloud_NSX_Network_1: type: Cloud.NSX.Network properties: networkType: existing constraints: - tag: nsxt24prod </pre>

Meer informatie

Voor implementatiescenario's met netwerken en beveiligingsgroepen raadpleegt u VMware-blogs zoals:

- [vRealize Automation Cloud Assembly Load Balancer with NSX-T Deep Dive](#)
- [Network Automation with Cloud Assembly and NSX – Part 1](#) (omvat het gebruik van NSX-T- en vCenter-cloudaccounts en netwerk-CIDR)
- [Network Automation met Cloud Assembly en NSX – Part 2](#) (omvat het gebruik van bestaande en uitgaande netwerktypen)
- [Network Automation with Cloud Assembly and NSX – Part 3](#) (omvat het gebruik van bestaande beveiligingsgroepen en beveiligingsgroepen op aanvraag)
- [Network Automation with Cloud Assembly and NSX – Part 4](#) (omvat het gebruik van bestaande load balancers en load balancers op aanvraag)

Meer informatie over netwerkresources in vRealize Automation-cloudsjablonen

Wanneer u uw vRealize Automation-cloudsjablonen maakt of bewerkt, gebruikt u de meest geschikte netwerkresources voor uw doelstellingen. Kom meer te weten over de NSX- en cloudonafhankelijke netwerkopties die beschikbaar zijn in de cloudsjabloon.

Selecteer een van de beschikbare netwerkresourcetypes op basis van machine- en gerelateerde voorwaarden in uw vRealize Automation-cloudsjabloon.

Cloudonafhankelijke netwerkresource

U voegt een cloudonafhankelijk netwerk toe met de resource **Cloudonafhankelijk > Netwerk** op de pagina **Ontwerp** voor cloudsjablonen. De resource wordt in de cloudsjablooncode weergegeven als `Cloud.Network`-resourcetype. De standaardresource wordt weergegeven als:

```
Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkType: existing
```

Gebruik een cloudonafhankelijk netwerk wanneer u netwerkeigenschappen wilt opgeven voor een doelmachinetype dat niet is verbonden, of niet kan worden verbonden, met een NSX-netwerk.

De cloudonafhankelijke netwerkresource is beschikbaar voor deze resourcetypes:

- Cloudonafhankelijke machine
- vSphere
- Google Cloud Platform (GCP)
- Amazon Web Services (AWS)
- Microsoft Azure
- VMware Cloud on AWS (VMC)

De cloudonafhankelijke netwerkresource is beschikbaar voor deze instellingen voor netwerktype (`networkType`):

- openbaar
- privé
- uitgaand
- bestaand

vSphere-netwerkresource

U voegt een vSphere-netwerk toe met de resource **vSphere > Netwerk** op de pagina **Ontwerp** voor cloudsjablonen. De resource wordt in de cloudsjablooncode weergegeven als `Cloud.vSphere.Network`-resourcetype. De standaardresource wordt weergegeven als:

```
Cloud_vSphere_Network_1:
  type: Cloud.vSphere.Network
  properties:
    networkType: existing
```

Gebruik een vSphere-netwerk wanneer u netwerkeigenschappen wilt opgeven voor een vSphere-machinetype (`Cloud.vSphere.Machine`).

De vSphere-netwerkrecurso is alleen beschikbaar voor een `Cloud.vSphere.Machine-machinetype`.

De vSphere-resource is beschikbaar voor deze instellingen voor netwerktype (`networkType`):

- openbaar
- privé
- bestaand

Zie [Netwerkinstellingen gebruiken in netwerkprofielen en cloudsjablonen in vRealize Automation](#) voor voorbeelden.

NSX-netwerkrecurso

U voegt een NSX-netwerk toe met de resource **NSX > Netwerk** op de pagina **Ontwerp** voor cloudsjablonen. De resource wordt in de cloudsjablooncode weergegeven als `Cloud.NSX.Network-resourcetype`. De standaardresource wordt weergegeven als:

```
Cloud_NSX_Network_1:
  type: Cloud.NSX.Network
  properties:
    networkType: existing
```

Gebruik een NSX-netwerk wanneer u een netwerkrecurso wilt koppelen aan een of meer machines die zijn gekoppeld aan een NSX-V- of NSX-T-cloudaccount. Met de NSX-netwerkrecurso kunt u NSX-netwerkeigenschappen opgeven voor een vSphere-machineresource die is gekoppeld aan een NSX-V- of NSX-T-cloudaccount.

De `Cloud.NSX.Network`-resource is beschikbaar voor deze instellingen voor netwerktype (`networkType`):

- openbaar
- privé
- uitgaand
- bestaand
- gerouteerd - Gerouteerde netwerken zijn alleen beschikbaar voor NSX-V en NSX-T.

Als u wilt dat meerdere uitgaande of gerouteerde netwerken dezelfde NSX-T-laag-1-router of NSX-V Edge Service Gateway (ESG) delen, verbindt u één NSX-gatewayresource (`Cloud.NSX.Gateway`) met de verbonden netwerken in de sjabloon vóór de eerste implementatie.

Als u de gateway na implementatie toevoegt als een bewerking voor dag 2 of iteratieve ontwikkelingsbewerking, maakt elk netwerk een eigen router.

U kunt de NSX NAT-resource in de sjabloon gebruiken om regels voor port mapping van NAT en DNAT te ondersteunen.

Cloudonafhankelijke netwerkresource met Azure-, AWS- of GCP-implementatiedoel

VM's van een publieke cloudprovider kunnen specifieke eigenschapscombinaties van cloudsjablonen vereisen die niet noodzakelijkerwijs vereist zijn in NSX- of vSphere-gebaseerde machine-implementaties. Zie [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#) voor voorbeelden van cloudsjablooncode die bepaalde van deze scenario's ondersteunt.

NSX-gatewayresource

U kunt één NSX-T-laag-1-router of NSX-V Edge Service Gateway (ESG) opnieuw gebruiken of delen in één implementatie met behulp van een gatewayresource (`Cloud.NSX.Gateway`) in de cloudsjabloon. De gatewayresource vertegenwoordigt de laag-1 of ESG en kan worden verbonden met meerdere netwerken in de implementatie. De gatewayresource kan alleen worden gebruikt met uitgaande of gerouteerde netwerken.

Met de `Cloud.NSX.Gateway`-resource kunt u de NSX-T-laag-1-router of NSX-V Edge Service Gateway (ESG) delen tussen verbonden uitgaande of gerouteerde netwerken in een implementatie.

De gateway wordt vaak gekoppeld aan één uitgaand of gerouteerd netwerk. Als de gateway echter aan meerdere netwerken is gekoppeld, moeten de netwerken van hetzelfde type zijn, bijvoorbeeld allemaal uitgaande of allemaal gerouteerde netwerken. De gateway kan worden verbonden met meerdere machines of load balancers die zijn verbonden met dezelfde uitgaande of gerouteerde netwerken. De gateway moet verbonden zijn met een load balancer in het gedeelde netwerk op aanvraag, zodat deze de NSX-T-laag-1-router of NSX-V Edge Service Gateway (ESG) die door de gateway is gemaakt, kan hergebruiken.

Als u wilt toestaan dat meerdere uitgaande of gerouteerde netwerken dezelfde T1-router of Edge delen, moet u eerst één `Cloud.NSX.Gateway`-gatewayresource verbinden met alle netwerken. Alle beoogde netwerken en de afzonderlijke gateway moeten met elkaar zijn verbonden voordat u de cloudsjabloon implementeert, anders maakt elk netwerk een eigen router.

Voor een NSX-netwerk dat een gekoppelde computergatewayresource bevat, worden de instellingen voor de gateway toegepast op alle gekoppelde netwerken in de implementatie. Er wordt één logische laag-1-router voor NSX-T gemaakt voor elke implementatie en gedeeld door alle netwerken op aanvraag en load balancers in de implementatie. Er wordt één NSX-V Edge gemaakt voor elke implementatie en deze wordt gedeeld door alle netwerken op aanvraag en load balancers in de implementatie.

U kunt de gatewayresource aan een netwerk koppelen als een iteratieve implementatie-update. Hiermee wordt echter geen T1- of Edge-router gemaakt. De initiële netwerkimplementatie maakt de router.

Voor NSX-T-netwerken die geen gekoppelde gatewayresource gebruiken, blijven meerdere netwerken op aanvraag in de cloudsjabloon meerdere logische laag-1-routers maken in de implementatie.

Als de gateway NAT-regels bevat, kunt u de NAT- of DNAT-regels voor de laag-1-router of Edge-router opnieuw configureren of verwijderen. Als de gateway voor het eerst zonder NAT-regels wordt geïmplementeerd, zijn er geen acties voor dag 2 beschikbaar.

NSX NAT-resource

De `Cloud.NSX.NAT`-resource staat toe dat DNAT-regels en port mapping aan alle verbonden uitgaande netwerken worden gekoppeld via de `gatewayresource`. U kunt een NAT-resource koppelen aan een `gatewayresource` waarvoor de DNAT-regels moeten worden geconfigureerd.

Opmerking De `Cloud.NSX.Gateway`-resource was oorspronkelijk beschikbaar voor DNAT-regels. Het gebruik van de `Cloud.NSX.Gateway` als middel voor het definiëren van DNAT-regels en port mapping is echter afgeschaft. Het blijft wel beschikbaar voor achterwaartse compatibiliteit. Gebruik de cloudsjabloonresource `Cloud.NSX.NAT` voor DNAT-regels en port mapping. Er wordt een waarschuwing weergegeven in de cloudsjabloon als u het `resourcetype Cloud.NSX.Gateway` met NAT-regelspecificaties probeert te gebruiken.

De `Cloud.NSX.NAT`-resource ondersteunt DNAT-regels en port mapping wanneer deze is verbonden met een uitgaand NSX-V- of NSX-T-netwerk.

De instelling voor NAT-regels in de resource is `natRules:`. U kunt de NAT-resource aan de `gatewayresource` koppelen om de `natRules:`-vermeldingen in de gateway te configureren. DNAT-regels die zijn opgegeven in de resource, gebruiken de gekoppelde machines of load balancers als doel.

U kunt een machine-NIC of computergateway in een bestaande implementatie opnieuw configureren om de `natRules:`-instellingen te wijzigen door de regels voor DNAT port mapping toe te voegen, te herschikken, te bewerken of te verwijderen. U kunt geen DNAT-regels gebruiken met geclusterde machines. U kunt DNAT-regels voor afzonderlijke machines in het cluster opgeven als onderdeel van een bewerking voor dag 2.

Opties voor externe IPAM-integratie

Voor informatie over eigenschappen die beschikbaar zijn voor gebruik met uw Infoblox IPAM-integraties in cloudsjabloonontwerpen en -implementaties, zie [Infoblox-specifieke eigenschappen en uitbreidbaarheidskenmerken voor IPAM-integraties in vRealize Automation-cloudsjablonen gebruiken](#).

Restricties voor het gebruik van een vast toegewezen IP-adres in een cloudsjabloon

U kunt een vast toegewezen IP-adres alleen gebruiken in een vRealize Automation-cloudsjabloon wanneer u vRealize Automation IPAM gebruikt, wat betekent dat IPAM de door vRealize Automation geleverde interne IPAM is of een IPAM is die is afgeleid van een externe providerinvoegtoepassing die is gemaakt met behulp van de vRealize Automation IPAM SDK - bijvoorbeeld een van de Infoblox-invoegtoepassingen die kunnen worden gedownload via de vRealize Automation Marketplace. Het gebruik van een vast

toegewezen IP-adres (`assignment:static`) wordt niet ondersteund in een cloudsjabloon wanneer u een gebeurtenisonderwerp Netwerk configureren gebruikt (dat wordt gebruikt door een Cloud Assembly-uitbreidbaarheidsactie (ABX) of een vRealize Orchestrator-werkstroom). Niet-ondersteunde vast toegewezen IP-adressen veroorzaken een implementatiefout.

Adreswaarde in de sectie Algemeen van de geïmplementeerde cloudsjabloon

Bij het onderzoeken van een geïmplementeerde cloudsjabloon is de waarde **Adres** in de sectie **Algemeen** van de sjabloon het primaire IP-adres van de machine. Het primaire adres is vaak het openbare of anderszins toegankelijke machineadres. Voor vSphere-implementaties wordt het primaire IP-adres berekend door vRealize Automation. Alle IP-adressen voor alle NIC's, inclusief hun openbare, privé-, IPv6-, statische en dynamische eigenschappen, worden beschouwd en gerangschikt om het primaire IP-adres te bepalen. Voor niet-vSphere-implementaties wordt het primaire IP-adres van de machine berekend door het classificatiesysteem van elke cloudleverancier.

Beschikbare bewerkingen voor dag 2

Zie [Welke acties kan ik op Cloud Assembly-implementaties uitvoeren](#) voor een lijst met veelgebruikte bewerkingen voor dag 2 die beschikbaar zijn voor cloudsjabloon- en implementatieresources.

Zie [Een geïmplementeerde machine naar een ander netwerk verplaatsen](#) voor een voorbeeld van hoe u van het ene netwerk naar het andere kunt gaan.

Meer informatie

Zie [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#) voor gerelateerde informatie en voorbeelden die voorbeeldnetwerkresources en -instellingen illustreren.

Zie [Netwerkresources in vRealize Automation](#) voor informatie over het definiëren van netwerkresources.

Zie [Meer informatie over netwerkprofielen in vRealize Automation](#) voor informatie over het definiëren van netwerkprofielen.

Meer informatie over beveiligingsgroep- en tagresources in vRealize Automation-cloudsjablonen

Wanneer u uw vRealize Automation-cloudsjablonen maakt of bewerkt, gebruikt u de meest geschikte beveiligingsresourceopties om tegemoet te komen aan uw doelstellingen.

Cloudonafhankelijke beveiligingsgroeppresource

U voegt een beveiligingsgroeppresource toe met behulp van de resource **Cloudonafhankelijk > Beveiligingsgroep** op de ontwerppagina voor cloudsjablonen. De resource wordt in de cloudsjablooncode weergegeven als `Cloud.SecurityGroup`-resourcetype. De standaardresource wordt weergegeven als:

```
Cloud_SecurityGroup_1:
  type: Cloud.SecurityGroup
  properties:
    constraints: []
    securityGroupType: existing
```

U kunt een beveiligingsgroeppresource in een cloudsjabloonontwerp opgeven als bestaand (`securityGroupType: existing`) of op aanvraag (`securityGroupType: new`).

U kunt een bestaande beveiligingsgroep aan uw cloudsjabloon toevoegen of u kunt een bestaande beveiligingsgroep gebruiken die is toegevoegd aan een netwerkprofiel.

Voor NSX-V en NSX-T, evenals NSX-T met de beleidsbeheerschakelaar ingeschakeld in combinatie met VMware Cloud on AWS, kunt u een bestaande beveiligingsgroep toevoegen of een nieuwe beveiligingsgroep definiëren wanneer u uw cloudsjabloon ontwerpt of wijzigt. Beveiligingsgroepen op aanvraag worden ondersteund voor NSX-T en NSX-V, en voor VMware Cloud on AWS indien gebruikt met NSX-T-beleidsbeheerder.

Voor alle cloudaccounttypen, met uitzondering van Microsoft Azure, kunt u een of meer beveiligingsgroepen koppelen aan een machine-NIC. Een NIC van een virtuele Microsoft Azure-machine (*machineName*) kan slechts aan één beveiligingsgroep worden gekoppeld.

De eigenschap `securityGroupType` van de beveiligingsgroep is standaard ingesteld op `existing`. Als u een beveiligingsgroep op aanvraag wilt maken, voert u `new` in voor de eigenschap `securityGroupType`. Als u firewallregels wilt opgeven voor een beveiligingsgroep op aanvraag, gebruikt u de eigenschap `rules` in de sectie `Cloud.SecurityGroup` van de beveiligingsgroeppresource.

Bestaande beveiligingsgroepen

Bestaande beveiligingsgroepen worden gemaakt in een broncloudaccountresource, zoals NSX-T of Amazon Web Services. Deze gegevens worden door vRealize Automation verzameld vanaf de bron. U kunt een bestaande beveiligingsgroep uit een lijst met beschikbare resources selecteren als onderdeel van een vRealize Automation-netwerkprofiel. In een cloudsjabloonontwerp kunt u een bestaande beveiligingsgroep opgeven met het lidmaatschap van een bepaald netwerkprofiel of in het bijzonder op naam met de instelling `securityGroupType: existing` in een beveiligingsgroeppresource. Als u een beveiligingsgroep toevoegt aan een netwerkprofiel, voegt u ten minste één capaciteitstag toe aan het netwerkprofiel. Beveiligingsgroeppresources op aanvraag vereisen een beperkingstag wanneer ze worden gebruikt in een cloudsjabloonontwerp.

U kunt een beveiligingsgroeppresource in uw cloudsjabloonontwerp koppelen aan een of meer machineresources.

Opmerking Als u van plan bent om een machineresource in uw cloudsjabloonontwerp te gebruiken voor inrichting in de NIC van een virtuele Microsoft Azure-machine (*machineName*), moet u de machineresource slechts aan één beveiligingsgroep koppelen.

Beveiligingsgroepen op aanvraag

U kunt beveiligingsgroepen op aanvraag definiëren wanneer u een cloudsjabloonontwerp definieert of wijzigt met behulp van de instelling `securityGroupType: new` in de code van de beveiligingsgroeppresource.

U kunt een beveiligingsgroep op aanvraag gebruiken voor NSX-V en NSX-T, en voor Amazon Web Services indien gebruikt met het NSX-T-beleidstype, om een specifieke reeks firewallregels toe te passen op een machineresource in een netwerk of een set gegroepeerde resources. Elke beveiligingsgroep kan meerdere benoemde firewallregels bevatten. U kunt een beveiligingsgroep op aanvraag gebruiken om services of protocollen en poorten op te geven. Houd er rekening mee dat u een service of een protocol kunt opgeven, maar niet beide. U kunt naast een protocol ook een poort opgeven. U kunt geen poort opgeven als u een service opgeeft. Als de regel geen service of protocol bevat, is Willekeurig de standaardwaarde voor de service.

U kunt ook IP-adressen en IP-bereiken in firewallregels opgeven. U vindt voorbeelden van firewallregels in [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#).

Wanneer u firewallregels maakt in een NSX-V- of NSX-T-beveiligingsgroep op aanvraag, is niet alleen het opgegeven netwerkverkeer standaard toegestaan, maar ook het andere netwerkverkeer. Om netwerkverkeer te beheren, moet u voor elke regel een toegangstype opgeven. De toegangstypen voor regels zijn:

- Toestaan (standaard) - Het netwerkverkeer toestaan dat is opgegeven in deze firewallregel.
- Weigeren - Het netwerkverkeer blokkeren dat is opgegeven in deze firewallregel. Stelt de client actief op de hoogte dat de verbinding wordt geweigerd.
- Afbreken - Het netwerkverkeer blokkeren dat is opgegeven in deze firewallregel. Het pakket wordt op de achtergrond geannuleerd alsof de listener niet online is.

Zie [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#) voor een voorbeeld van een ontwerp dat gebruikmaakt van een firewallregel `access: Allow` en `access: Deny`.

Opmerking Een cloudbeheerder kan een cloudsjabloonontwerp maken dat alleen een NSX-beveiligingsgroep op aanvraag bevat en kan dit ontwerp implementeren om een herbruikbare bestaande beveiligingsgroeppresource te maken die leden van de organisatie als bestaande beveiligingsgroep kunnen toevoegen aan netwerkprofielen en cloudsjabloonontwerpen.

Firewallregels ondersteunen CIDR-waarden in IPv4- of IPv6-notatie voor bron- en doel-IP-adressen. Zie [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#) voor een voorbeeld van een ontwerp dat gebruikmaakt van IPv6 CIDR-waarden in een firewallregel.

Beveiligingsgroepen op aanvraag en bestaande beveiligingsgroepen voor VMware Cloud on AWS

U kunt een beveiligingsgroep op aanvraag voor een VMware Cloud on AWS-machine in een cloudsjabloon definiëren door de instelling `securityGroupType: new` in de resourcecode van de beveiligingsgroep te gebruiken.

Hieronder ziet u een fragment met voorbeeldcode voor een beveiligingsgroep op aanvraag:

```
resources:
  Cloud_SecurityGroup_1:
    type: Cloud.SecurityGroup
    properties:
      name: vmc-odsg
      securityGroupType: new
      rules:
        - name: datapath
          direction: inbound
          protocol: TCP
          ports: 5011
          access: Allow
          source: any
```

U kunt ook een bestaande beveiligingsgroep definiëren voor een VMware Cloud on AWS-machine in een netwerk en eventueel beperkingstags toevoegen, zoals u in de volgende voorbeelden ziet:

```
Cloud_SecurityGroup_2:
  type: Cloud.SecurityGroup
  properties:
    constraints: [xyz]
    securityGroupType: existing
```

```
Cloud_SecurityGroup_3:
  type: Cloud.SecurityGroup
  properties:
    securityGroupType: existing
    constraints:
      - tag: xyz
```

Iteratieve ontwikkeling van cloudsjablonen wordt ondersteund.

- Als een beveiligingsgroep is gekoppeld aan een of meer machines in de implementatie, wordt bij een verwijderactie in een bericht gemeld dat de beveiligingsgroep niet kan worden verwijderd.
- Als een beveiligingsgroep niet is gekoppeld aan een machine in de implementatie, wordt bij een verwijderactie in een bericht gemeld dat de beveiligingsgroep uit deze implementatie wordt verwijderd en de actie niet ongedaan kan worden gemaakt. Een bestaande beveiligingsgroep wordt uit de cloudsjabloon verwijderd terwijl een beveiligingsgroep op aanvraag wordt vernietigd.

NSX-V-beveiligingstags en NSX-T VM-tags gebruiken

U kunt NSX-V-beveiligingstags en NSX-T en NSX-T met VM-tags voor beleid van beheerde resources in vRealize Automation-cloudsjablonen zien en gebruiken.

NSX-V- en NSX-T-beveiligingstags worden ondersteund voor gebruik met vSphere. NSX-T-beveiligingstags worden ook ondersteund voor gebruik met VMware Cloud on AWS.

Opmerking Zoals met VM's die zijn geïmplementeerd op vSphere, kunt u machinetags configureren voor een VM die op VMware Cloud on AWS moet worden geïmplementeerd. U kunt de machinetag ook bijwerken na de eerste implementatie. Met deze machinetags kan vRealize Automation dynamisch een VM toewijzen aan een geschikte NSX-T-beveiligingsgroep tijdens de implementatie.

U kunt NSX-V-beveiligingstags opgeven door de `key: nsxSecurityTag` en een tagwaarde in de computerbron in de cloudsjabloon te gebruiken, zoals u in het volgende voorbeeld ziet, mits de machine is verbonden met een NSX-V-netwerk:

```
tags:
  - key: nsxSecurityTag
    value: security_tag_1
  - key: nsxSecurityTag
    value: security_tag_2
```

De opgegeven waarde moet overeenkomen met een NSX-V-beveiligingstag. Als er geen beveiligingstags in NSX-V zijn die overeenkomen met de opgegeven waarde voor de sleutel `nsxSecurityTag`, mislukt de implementatie.

Opmerking Voor NSX-V-beveiligingstags is vereist dat de machine is verbonden met een NSX-V-netwerk. Als de machine is verbonden met een vSphere-netwerk, worden de NSX-V-beveiligingstags genegeerd. In beide gevallen is de vSphere-machine ook getagd.

NSX-T heeft geen afzonderlijke beveiligingstag. Elke tag die op de computerbron in de cloudsjabloon is opgegeven, leidt ertoe dat de geïmplementeerde VM wordt gekoppeld aan alle tags die in NSX-T zijn opgegeven. Voor NSX-T, inclusief NSX-T met beleid, worden VM-tags ook uitgedrukt als sleutelwaardepaar in de cloudsjabloon. De instelling `key` komt overeen met de instelling `scope` in NSX-T en de instelling `value` komt overeen met de instelling `Tag Name` zoals opgegeven in NSX-T.

Als u de vRealize Automation V2T-migratieassistent hebt gebruikt om uw cloudaccounts te migreren van NSX-V naar NSX-T, inclusief NSX-T met beleid, maakt de migratieassistent een sleutelwaardepaar `nsxSecurityTag`. In dit scenario, of als de `nsxSecurityTag` om een of andere reden expliciet is opgegeven in een cloudsjabloon voor gebruik met NSX-T, inclusief NSX-T met beleid, maakt de implementatie een VM-tag met een lege instelling Bereik met een tagnaam die overeenkomt met de opgegeven `value`. Als u dergelijke tags in NSX-T bekijkt, is de kolom Bereik leeg.

Om verwarring te voorkomen, gebruikt u geen sleutelparen `nsxSecurityTag` voor NSX-T. Als u een sleutelwaardepaar `nsxSecurityTag` opgeeft voor gebruik met NSX-T, inclusief NSX-T met beleid, maakt de implementatie een VM-tag met een lege instelling Bereik met een tagnaam die overeenkomt met de opgegeven `value`. Als u dergelijke tags in NSX-T bekijkt, is de kolom Bereik leeg.

App-isolatiebeleid gebruiken in firewallregels voor beveiligingsgroepen op aanvraag

U kunt een app-isolatiebeleid inschakelen zodat alleen intern verkeer tussen de door de cloudsjabloon ingerichte resources wordt toegestaan. Met app-isolatie kunnen de machines die zijn ingericht door de cloudsjabloon met elkaar communiceren, maar geen verbindingen maken buiten de firewall. U kunt een app-isolatiebeleid maken in het netwerkprofiel. U kunt ook app-isolatie opgeven in een cloudsjabloonontwerp door gebruik te maken van een beveiligingsgroep op aanvraag met een firewallregel voor weigeren of een privé- of uitgaand netwerk.

Er wordt een app-isolatiebeleid gemaakt met een lagere prioriteit. Als u meerdere beleidsregels toepast, krijgen de beleidsregels met een hoger gewicht voorrang.

Wanneer u een beleid voor applicatie-isolatie maakt, wordt een automatisch gegenereerde beleidsnaam gegenereerd. Het beleid wordt ook beschikbaar gesteld voor hergebruik in andere cloudsjabloonontwerpen en -iteraties die specifiek zijn voor het gekoppelde resource-eindpunt en project. De naam van het beleid voor app-isolatie is niet zichtbaar in de cloudsjabloon, maar is zichtbaar als aangepaste eigenschap op de projectpagina (**Infrastructuur > Beheer > Projecten**) nadat het cloudsjabloonontwerp is geïmplementeerd.

Voor hetzelfde gekoppelde eindpunt in een project kan elke implementatie waarvoor een beveiligingsgroep op aanvraag is vereist voor app-isolatie, hetzelfde app-isolatiebeleid gebruiken. Het beleid wordt niet verwijderd nadat het is gemaakt. Wanneer u een app-isolatiebeleid opgeeft, zoekt vRealize Automation naar het beleid in het project en ten opzichte van het gekoppelde eindpunt. Als het beleid wordt gevonden, wordt het opnieuw gebruikt. Als het niet wordt gevonden, wordt het gemaakt. De naam van het app-isolatiebeleid is alleen zichtbaar na de eerste implementatie in de lijst met custom eigenschappen van het project.

Beveiligingsgroepen gebruiken in de iteratieve ontwikkeling van iteratieve cloudsjablonen

Wanneer de beperkingen van de beveiligingsgroep tijdens iteratieve ontwikkeling worden gewijzigd, waarbij de beveiligingsgroep niet is gekoppeld aan een machine in de cloudsjabloon, wordt de beveiligingsgroep zoals opgegeven bijgewerkt in de iteratie. Wanneer de beveiligingsgroep echter al aan een machine is gekoppeld, mislukt de herimplementatie. U moet bestaande beveiligingsgroepen en/of `securityGroupType`-resource-eigenschappen van gekoppelde machines loskoppelen tijdens de iteratieve ontwikkeling van de cloudsjabloon en vervolgens opnieuw koppelen tussen elke herimplementatie. De vereiste werkstroom is als volgt, ervan uitgaande dat u de cloudsjabloon in eerste instantie hebt geïmplementeerd.

- 1 Ontkoppel de beveiligingsgroep van alle gekoppelde machines in de cloudsjabloon in de ontwerpfunctie voor Cloud Assembly-sjablonen.
- 2 Implementeer de sjabloon opnieuw door op **Een bestaande implementatie bijwerken** te klikken.

- 3 Verwijder de beperkingstags van de bestaande beveiligingsgroep en/of `securityGroupType`-eigenschappen in de sjabloon.
- 4 Voeg nieuwe beperkingstags van de beveiligingsgroep en/of `securityGroupType`-eigenschappen in de sjabloon toe.
- 5 Koppel de beperkingstags van de nieuwe beveiligingsgroep en/of instanties van de eigenschap `securityGroupType` aan de machines in de sjabloon.
- 6 Implementeer de sjabloon opnieuw door op **Een bestaande implementatie bijwerken** te klikken.

Beschikbare bewerkingen voor dag 2

Zie [Welke acties kan ik op Cloud Assembly-implementaties uitvoeren](#) voor een lijst met veelgebruikte bewerkingen voor dag 2 die beschikbaar zijn voor cloudsjabloon- en implementatieresources.

Meer informatie

Zie [Beveiligingsresources in vRealize Automation](#) voor informatie over het gebruik van een beveiligingsgroep voor netwerkisolatie.

Zie [Meer informatie over netwerkprofielen in vRealize Automation](#) en [Instellingen voor beveiligingsgroepen gebruiken in netwerkprofielen en cloudsjabloonontwerpen in vRealize Automation](#) voor informatie over het gebruik van beveiligingsgroepen in netwerkprofielen.

Zie [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#) voor voorbeelden van het gebruik van beveiligingsgroepen in cloudsjablonen.

Meer informatie over load-balancerresources in vRealize Automation-cloudsjablonen

Wanneer u uw vRealize Automation-cloudsjablonen maakt of bewerkt, gebruikt u de meest geschikte load balancer-resources voor uw doelstellingen.

U kunt NSX- en cloudonafhankelijke load balancer-resources in een cloudsjabloon gebruiken om load balancing in een implementatie te beheren.

De cloudonafhankelijke load balancer kan in meerdere clouds worden geïmplementeerd. Een cloudspecifieke load balancer kan geavanceerde instellingen en functies opgeven die alleen beschikbaar zijn voor een specifieke cloud/topologie. Cloudspecifieke eigenschappen zijn beschikbaar in het resourcetype NSX load balancer (`Cloud.NSX.LoadBalancer`). Als u deze eigenschappen toevoegt op een cloudonafhankelijke load balancer (`Cloud.LoadBalancer`) worden deze genegeerd als bijvoorbeeld een load balancer van Amazon Web Services of Microsoft Azure is ingericht, maar worden deze gerespecteerd als een load balancer van NSX-V of NSX-T is ingericht. Kies een van de beschikbare resourcetypes voor load balancers op basis van voorwaarden in uw vRealize Automation-cloudsjabloon.

U kunt een load-balancerresource niet rechtstreeks verbinden met een beveiligingsgroepresource in het ontwerpcanvas.

Cloudonafhankelijke load-balancerresource

Gebruik een cloudonafhankelijke load balancer wanneer u netwerkeigenschappen wilt opgeven voor elk type doelmachine.

U voegt een cloudonafhankelijke load balancer toe met behulp van de resource

Cloudonafhankelijk > Load balancer op de ontwerppagina voor cloudsjablonen. De resource wordt in de cloudsjablooncode weergegeven als `Cloud.LoadBalancer-resourcetype`. De standaardresource wordt weergegeven als:

```
Cloud_LoadBalancer_1:
  type: Cloud.LoadBalancer
  properties:
    routes: []
    network: ''
    instances: []
    internetFacing: false
```

NSX-load-balancerresource

Gebruik een load balancer van NSX wanneer de cloudsjabloon kenmerken bevat die specifiek zijn voor NSX-V of NSX-T (Beleids-API- of Manager-API-methoden). U kunt een of meer load balancers koppelen aan een NSX-V- of NSX-T-netwerk of aan machines die zijn gekoppeld aan een NSX-V- of NSX-T-netwerk.

U voegt een NSX-load balancer toe met behulp van de **NSX > Load Balancer** resource. De resource wordt in de cloudsjablooncode weergegeven als `Cloud.NSX.LoadBalancer-resourcetype`. De standaardresource wordt weergegeven als:

```
Cloud_NSX_LoadBalancer_1:
  type: Cloud.NSX.LoadBalancer
  properties:
    routes: []
    network: ''
    instances: []
```

Opties voor load balancer in cloudsjablooncode

Door een of meer load balancer-resources toe te voegen aan uw cloudsjabloon kunt u de volgende instellingen opgeven. Er zijn enkele voorbeelden beschikbaar op [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#).

Het HTTP-protocol wordt ondersteund voor alle load balancers op aanvraag.

Het HTTPS-protocol wordt alleen ondersteund voor load balancers op aanvraag die zijn gekoppeld aan een NSX-T-cloudaccount waarvan de NSX-modus is ingesteld op **Beleid**. NSX-T-cloudaccounts waarvan de NSX-modus is ingesteld op **Manager** kan het HTTPS-protocol niet gebruiken.

■ Machinespecificatie

U kunt benoemde machineresources opgeven om deel te nemen aan een load balancing-pool. U kunt ook opgeven dat een specifieke machine-NIC deel uitmaakt van de load-balancerpool.

Deze optie is alleen beschikbaar voor de **NSX** load balancer-resource (`Cloud.NSX.LoadBalancer`).

- `resource.Cloud_Machine_1.id`

Hiermee geeft u op dat de load balancer de machine bevat die in de cloudsjablooncode is geïdentificeerd als `Cloud_Machine_1`.

- `resource.Cloud_Machine_2.networks[2].id`

Hiermee geeft u op dat de load balancer alleen de machine bevat die in de cloudsjablooncode is gedefinieerd als `Cloud_Machine_2` wanneer deze wordt geïmplementeerd op machine-NIC `Cloud_Machine_2.networks[2]`.

- Logboekregistratieniveau

De waarde van het registratieniveau bepaalt een ernstniveau voor het foutenlogboek. De opties zijn NONE, EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, INFO, DEBUG en NOTICE. De waarde van het logboekregistratieniveau is van toepassing op alle load balancers in de cloudsjabloon. Deze optie is specifiek voor NSX. Voor load balancers die een bovenliggende load balancer hebben, overschrijft de instelling van het bovenliggende logboekregistratieniveau alle instellingen voor logboekregistratieniveau in de onderliggende load balancers.

Raadpleeg onderwerpen zoals [Load balancers toevoegen](#) in de productdocumentatie voor NSX voor gerelateerde informatie.

- Type

Gebruik een load balancer-type om een schaalgrootte op te geven. De standaardwaarde is klein. Deze optie is specifiek voor NSX. Voor load balancers die een bovenliggende load balancer hebben, overschrijft de instelling van het bovenliggende type elke instelling voor type in de onderliggende load balancers.

- Klein

Komt overeen met compact in NSX-V en klein in NSX-T.

- Normaal

Komt overeen met groot in NSX-V en normaal in NSX-T.

- Groot

Komt overeen met quad-groot in NSX-V en groot in NSX-T.

- Extra groot

Komt overeen met extra groot in NSX-V en groot in NSX-T.

Raadpleeg voor gerelateerde informatie onderwerpen zoals [Resources voor het schalen van load balancers](#) in de productdocumentatie voor NSX.

Deze optie is alleen beschikbaar voor de **NSX-load-balancer**resource
(`Cloud.NSX.LoadBalancer`).

■ Algoritme (serverpool)

Gebruik een algoritmische methode voor de verdeling om te bepalen hoe binnenkomende verbindingen worden verdeeld over de leden van de serverpool. Het algoritme kan worden gebruikt op een serverpool of rechtstreeks op een server. Alle load balancing-algoritmen slaan servers over die aan een van de volgende voorwaarden voldoen:

- De status Beheerder is ingesteld op **UITGESCHAKELD**.
- De status Beheerder is ingesteld op **GRACEFUL_DISABLED** en er is geen overeenkomende persistentie-invoer.
- De status actieve of passieve gezondheidscontrole is **INACTIEF**.
- De verbindinglimiet voor het maximum aantal gelijktijdige verbindingen van de serverpool is bereikt.

Deze optie is specifiek voor NSX.

■ IP_HASH

Selecteert een server op basis van een hash van het oorspronkelijke IP-adres en het totale gewicht van alle actieve servers.

Komt overeen met IP-HASH in NSX-V en NSX-T.

■ LEAST_CONNECTION

Hiermee worden clientaanvragen naar meerdere servers gedistribueerd op basis van het aantal bestaande verbindingen op de server. Nieuwe verbindingen worden verzonden naar de server met het minste aantal verbindingen. De gewichtswaarden van de serverpoolonderdelen worden genegeerd, ook als ze zijn geconfigureerd.

Komt overeen met LEASTCONN in NSX-V en LEAST_CONNECTION in NSX-T.

■ ROUND_ROBIN

Binnenkomende clientaanvragen doorlopen een lijst met beschikbare servers die de aanvraag kunnen afhandelen. Negeert het gewicht van serverpoolleden, zelfs als dit geconfigureerd is. Standaard.

Komt overeen met ROUND_ROBIN in NSX-V en NSX-T.

■ WEIGHTED_LEAST_CONNECTION

Aan elke server wordt een gewichtswaarde toegewezen die aangeeft hoe die server presteert ten opzichte van andere servers in de pool. De waarde bepaalt hoeveel clientaanvragen 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 serverresources. De gewichtswaarde is standaard 1 als de waarde niet is geconfigureerd en langzame start is ingeschakeld.

Komt overeen met `WEIGHTED_LEAST_CONNECTION` in NSX-T. Er is geen correlatie in NSX-V.

- `WEIGHTED_ROUND_ROBIN`

Aan elke server wordt een gewichtswaarde toegewezen die aangeeft hoe die server presteert ten opzichte van andere servers in de pool. De waarde bepaalt hoeveel clientaanvragen naar een server worden verzonden in vergelijking met andere servers in de pool. Dit algoritme voor load balancing focust op de gelijke verdeling van de werklust tussen de beschikbare serverresources.

Komt overeen met `WEIGHTED_ROUND_ROBIN` in NSX-T. Er is geen correlatie in NSX-V.

- `URI`

Het linkergedeelte van de URI wordt ghasht en gedeeld door het totale gewicht van de actieve servers. 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. De URI-algoritmeparameter heeft twee opties: `uriLength=<len>` en `uriDepth=<dep>`. Het lengteparameterbereik moet $1 \leq \text{len} < 256$ zijn. Het diepteparameterbereik moet $1 \leq \text{dep} < 10$ zijn. 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. 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. 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. Als beide parameters zijn opgegeven, stopt de evaluatie wanneer een van de parameters is bereikt.

Komt overeen met `URI` in NSX-V. Er is geen correlatie in NSX-T.

- `HTTPHEADER`

De naam van de HTTP-koptekst wordt opgezocht in elke HTTP-aanvraag. De naam van de koptekst tussen haakjes is niet hoofdlettergevoelig. Als de koptekst afwezig is of geen waarde bevat, wordt het round-robin-algoritme toegepast. De algoritmeparameter `HTTPHEADER` heeft één optie: `headerName=<name>`.

Komt overeen met `HTTPHEADER` in NSX-V. Er is geen correlatie in NSX-T.

- `URL`

De URL-parameter die is opgegeven in het argument, wordt opgezocht in de querytekenreeks van elke HTTP GET-aanvraag. Als de parameter wordt gevolgd door een gelijkteken = en een waarde, wordt de waarde ghasht 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. Als geen waarde of parameter wordt gevonden, wordt het round-robin-algoritme toegepast. De URL-algoritme-parameter heeft één optie: `urlParam=<url>`.

Komt overeen met URL in NSX-V. Er is geen correlatie in NSX-T.

Raadpleeg onderwerpen zoals [Een serverpool toevoegen voor load balancing](#) in de NSX-productdocumentatie voor gerelateerde informatie.

■ Statusmonitor

Gebruik de opties van de statusmonitor om te testen of een server beschikbaar is. Actieve statusmonitor voor HTTP-, ICMP-, TCP- en UDP-protocollen wordt ondersteund. Passieve statusmonitor is alleen beschikbaar voor NSX-T.

Deze optie is specifiek voor NSX.

■ httpMethod

HTTP-methode die wordt gebruikt om de serverstatus voor de gezondheidscontroleaanvraag te detecteren. Methoden zijn GET, HEAD, OPTIONS, POST of PUT.

■ requestBody

Gezondheidscontrole van de inhoud van de aanvraagtekst. Gebruikt, en vereist, door HTTP-, TCP- en UDP-protocollen.

■ responseBody

Gezondheidscontrole van de inhoud van de verwachte reactietekst. Als de ontvangen tekenreeks overeenkomt met deze reactietekst, wordt de server als gezond beschouwd. Gebruikt, en vereist, door HTTP-, TCP- en UDP-protocollen.

Opmerking Als u het UDP-monitorprotocol gebruikt, zijn de parameters `UDP Data Sent` en `UDP Data Expected` vereist. De eigenschappen `requestBody` en `responseBody` worden aan deze parameters toegewezen.

Deze optie is beschikbaar voor de NSX-load-balancerresource (`Cloud.NSX.LoadBalancer`).

Raadpleeg onderwerpen zoals [Een actieve statusmonitor configureren](#) in de productdocumentatie voor NSX voor gerelateerde informatie.

■ Gezondheidscontrole

Gebruik de opties van de gezondheidscontrole om op te geven hoe de load balancer de gezondheidscontroles uitvoert.

Deze optie is alleen beschikbaar voor de NSX-load-balancerresource (`Cloud.NSX.LoadBalancer`).

Zie [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#) voor een voorbeeld van de beschikbare gezondheidscontrole-instellingen.

NSX-V- en NSX-T-netwerktypen en load-balanceropties

De opties voor load balancers zijn afhankelijk van het netwerk waaraan de load balancer-resource in de cloudsjabloon is gekoppeld. U kunt een load balancer configureren ten opzichte van het netwerktype en netwerkomstandigheden.

■ Netwerk op aanvraag

Als de load-balancerberekeningen aan een netwerk op aanvraag zijn gekoppeld, wordt een nieuwe laag-1-router gemaakt en gekoppeld aan de laag-0-router die in het netwerkprofiel is opgegeven. De load balancer wordt vervolgens aan de laag-1-router gekoppeld. De VIP-advertentie voor de laag-1-router wordt ingeschakeld als het VIP zich in een bestaand netwerk bevindt. Als een netwerk is geconfigureerd voor DHCP, delen het netwerk op aanvraag en de load balancer de laag-1-router.

■ Bestaand netwerk

Als de load balancer aan een bestaand netwerk is gekoppeld, wordt de load balancer gemaakt met de laag-1-router van het bestaande netwerk. Er wordt een nieuwe load balancer gemaakt als er geen load balancer aan de laag-1-router is gekoppeld. Als de load balancer al bestaat, worden er nieuwe virtuele servers aan gekoppeld. Als het bestaande netwerk niet aan een laag-1-router is gekoppeld, wordt een nieuwe laag-1-router gemaakt en gekoppeld aan een laag-0-router die in het netwerkprofiel is gedefinieerd. De VIP-advertentie voor de laag-1-router is niet ingeschakeld.

vRealize Automation biedt geen ondersteuning voor NSX-T twee-armige load balancer (inline load balancer) op twee verschillende bestaande netwerken. Houd er rekening mee dat de VIP-uplink zich in een scenario met een twee-armige load balancer op een bestaand netwerk bevindt terwijl de machines die lid zijn van de pool, verbonden zijn met een netwerk op aanvraag. Als u load balancing wilt opgeven wanneer u een bestaand netwerk gebruikt, moet u een éénarmige load balancer configureren waarin hetzelfde bestaande netwerk wordt gebruikt voor de load-balancer-VIP en de machines die lid zijn van de pool. Als u echter een load balancer gebruikt die u in het netwerkprofiel hebt geselecteerd, kunt u vanaf vRealize Automation 8.4.2 de load balancer tussen machines op twee verschillende bestaande netwerken instellen als er verbinding tussen de twee bestaande netwerken is.

■ Netwerkisolatie gedefinieerd in het netwerkprofiel

Voor netwerktypen van `outbound` of `private` kunt u netwerkisolatie-instellingen opgeven in een netwerkprofiel om een nieuwe beveiligingsgroep te emuleren. Omdat machines aan een bestaand netwerk worden gekoppeld en isolatie-instellingen in het profiel worden gedefinieerd, is deze optie vergelijkbaar met een load balancer die is gemaakt in een bestaand netwerk. Het verschil is dat het IP-adres van de laag-1-uplinkpoort aan de beveiligingsgroep van de isolatie wordt toegevoegd, om het gegevenspad in te schakelen.

U kunt instellingen voor load balancers opgeven voor NSX-gerelateerde netwerken door gebruik te maken van een NSX-load balancer-resource in het cloudsjabloonontwerp.

Zie het VMware-blogbericht [vRA Cloud Assembly Load Balancer with NSX-T Deep Dive](#) voor meer informatie.

Instellingen voor logboekregistratieniveau of -type opnieuw configureren wanneer meerdere load balancers een NSX-T Laag 1 of NSX-V Edge delen

Wanneer u een cloudsjabloon gebruikt die meerdere load balancers bevat die een laag-1-router delen in het NSX-T-eindpunt of een Edge-router in het NSX-V-eindpunt, worden de instellingen voor de andere load balancers niet bijgewerkt door het opnieuw configureren van de instellingen voor het logboekregistratieniveau of -type. Onjuiste instellingen leiden tot inconsistenties in NSX. Om inconsistenties te voorkomen bij het opnieuw configureren van deze instellingen voor logboekregistratieniveau en/of -type, gebruikt u dezelfde herconfiguratiewaarden voor alle load-balancerresources in de cloudsjabloon die een laag 1 of Edge in het gekoppelde NSX-eindpunt delen.

Beschikbare bewerkingen voor dag 2

Wanneer u een implementatie met een load balancer in- of uitschaalt, wordt de load balancer geconfigureerd om de recent toegevoegde machines op te nemen of om de machines voor taakverdeling te stoppen die in aanmerking komen voor ontkoppeling.

Zie [Welke acties kan ik op Cloud Assembly-implementaties uitvoeren](#) voor een lijst met veelgebruikte bewerkingen voor dag 2 die beschikbaar zijn voor cloudsjablonen en implementaties.

Meer informatie

Zie [Meer informatie over netwerkprofielen in vRealize Automation](#) voor informatie over het definiëren van load-balancerinstellingen in een netwerkprofiel.

Zie [Netwerken, beveiligingsgroepen en load balancers in vRealize Automation](#) voor voorbeelden van cloudsjabloonontwerpen die load balancers bevatten.

Voor Puppet ingeschakelde cloudsjabloon met gebruikersnaam- en wachtwoordtoegang

In dit voorbeeld voegt u Puppet-configuratiebeheer toe aan een cloudsjablonen die op een vCenter-computerbron is geïmplementeerd met gebruikersnaam- en wachtwoordtoegang.

Deze procedure toont een voorbeeld van hoe u een voor Puppet ingeschakelde implementeerbare resource kunt maken waarvoor gebruikersnaam- en wachtwoordverificatie is vereist. Gebruikersnaam- en wachtwoordtoegang betekent dat de gebruiker zich vanaf de berekeningsresource handmatig moet aanmelden bij de primaire Puppet-machine om Puppet-configuratiebeheer aan te roepen.

Optioneel kunt u verificatie van externe toegang configureren waarmee het configuratiebeheer in een cloudsjabloon wordt ingesteld, zodat de computerbron de verificatie met de primaire Puppet-machine afhandelt. Als externe toegang is ingeschakeld, genereert de berekeningsresource automatisch een sleutel om aan wachtwoordverificatie te voldoen. Een geldige gebruikersnaam is nog steeds vereist.

Zie [Cloudsjabloonvoorbeelden voor AWS Puppet-configuratiebeheer](#) en [Voorbeelden van cloudsjabloon voor vCenter Puppet-configuratie](#) voor meer voorbeelden van hoe u verschillende Puppet-scenario's in Cloud Assembly-blueprints kunt configureren.

Voorwaarden

- Stel een Puppet Enterprise-instantie in op een geldig netwerk.
- Voeg uw Puppet Enterprise-instantie toe aan Cloud Assembly met behulp van de functie Integraties. Zie [Puppet Enterprise-integratie configureren in Cloud Assembly](#)
- Stel een vSphere-account en een vCenter-berekeningsresource in.

Procedure

- 1 Voeg een Puppet-configuratiebeheeronderdeel aan een vSphere-computerbron toe op het canvas voor de gewenste cloudsjabloon.
 - a Selecteer **Infrastructuur > Beheren > Integraties**.
 - b Klik op **Integratie toevoegen** en selecteer Puppet.
 - c Voer de juiste informatie in op de Puppet-configuratiepagina.

Configuratie	Beschrijving	Voorbeeldwaarde
Hostnaam	Hostnaam of IP-adres van de primaire Puppet-machine	Puppet-Ubuntu
SSH-poort	Secure Shell-poort voor communicatie tussen Cloud Assembly en de primaire Puppet-machine. (Optioneel)	N.v.t.
Geheim voor automatisch ondertekenen	Het gedeelde geheim dat op primaire Puppet-machine is geconfigureerd en dat knooppunten moeten opgeven om certificaataanvragen voor automatische ondertekening te ondersteunen.	Gebruikersspecifiek
Locatie	Geef aan of de primaire Puppet-machine zich in een privé- of publieke cloud bevindt. Opmerking De implementatie in meerdere clouds wordt alleen ondersteund als er connectiviteit is tussen de berekeningsresource voor de implementatie en de primaire Puppet-machine.	
Cloud proxy	Niet vereist voor publieke cloudaccounts, zoals Microsoft Azure of Amazon Web Services. Als u een vCenter-gebaseerd cloudaccount gebruikt, selecteert u de juiste cloud proxy voor uw account.	N.v.t.
Gebruikersnaam	Secure Shell- en RBAC-gebruikersnaam voor de primaire Puppet-machine.	Gebruikersspecifiek. YAML-waarde is '\$ {input.username}'
Wachtwoord	Secure Shell- en RBAC-wachtwoord voor de primaire Puppet-machine.	Gebruikersspecifieke YAML-waarde is '\$ {input.password}'
Sudo-opdrachten voor deze gebruiker gebruiken	Selecteer deze optie om sudo-opdrachten voor de procidd te gebruiken.	waar
Naam	Naam primaire Puppet-machine.	PEMasterOnPrem
Beschrijving		

- 2 Voeg de eigenschappen voor gebruikersnaam en wachtwoord toe aan de Puppet-YAML, zoals in het volgende voorbeeld wordt weergegeven.
- 3 Zorg ervoor dat de waarde voor de eigenschap `remoteAccess` naar de Puppet-cloudsjabloon-YAML op `authentication: username and password` is ingesteld, zoals in het volgende voorbeeld wordt weergegeven.

Voorbeeld: YAML-code voor vCenter-gebruikersnaam en -wachtwoord

Het volgende voorbeeld toont de representatieve YAML-code voor het toevoegen van gebruikersnaam- en wachtwoordverificatie op een vCenter-berekeningsresource.

```
inputs:
  username:
    type: string
    title: Username
    description: Username to use to install Puppet agent
    default: puppet
  password:
    type: string
    title: Password
    default: VMware@123
    encrypted: true
    description: Password for the given username to install Puppet agent
resources:
  Puppet-Ubuntu:
    type: Cloud.vSphere.Machine
    properties:
      flavor: small
      imageRef: >-
        https://cloud-images.ubuntu.com/releases/16.04/release-20170307/ubuntu-16.04-server-
cloudimg-amd64.ova
      remoteAccess:
        authentication: usernamePassword
        username: '${input.username}'
        password: '${input.password}'
  Puppet_Agent:
    type: Cloud.Puppet
    properties:
      provider: PEMasterOnPrem
      environment: production
      role: 'role::linux_webserver'
      username: '${input.username}'
      password: '${input.password}'
      host: '${Puppet-Ubuntu.*}'
      useSudo: true
      agentConfiguration:
        certName: '${Puppet-Ubuntu.address}'
```

Cloudsjabloonvoorbeelden voor AWS Puppet-configuratiebeheer

Er zijn verschillende opties voor het configureren van cloudsjablonen om Puppet-gebaseerd configuratiebeheer op AWS-computerbronnen te ondersteunen.

Puppet-beheer op AWS met gebruikersnaam en wachtwoord

Voorbeeld van...	Voorbeeldblueprint-YAML
<p>Verificatie van cloudconfiguratie op elke ondersteunde image van een Amazon-machine.</p>	<pre> inputs: username: type: string title: Username default: puppet password: type: string title: Password encrypted: true default: VMware@123 resources: Webserver: type: Cloud.AWS.EC2.Instance properties: flavor: small image: centos cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' ssh-authorized-keys: - ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDytVL+Q6/+vGbmKXoRpX dmettem@dmettem-m01.vmware.com runcmd: - echo "Defaults:\${input.username} !requiretty" >> /etc/sudoers.d/\${input.username} Puppet_Agent: type: Cloud.Puppet properties: provider: PEOAWS environment: production role: 'role::linux_webserver' host: '\${Webserver.*}' osType: linux username: '\${input.username}' password: '\${input.password}' useSudo: true </pre>
<p>Verificatie van cloudconfiguratie op een aangepaste image van een Amazon-machine met een bestaande gebruiker.</p>	<pre> inputs: username: type: string title: Username default: puppet password: type: string title: Password encrypted: true default: VMware@123 </pre>

Voorbeeld van...	Voorbeeldblueprint-YAML
	<pre> resources: Webserver: type: Cloud.AWS.EC2.Instance properties: flavor: small image: centos cloudConfig: #cloud-config runcmd: - sudo sed -e 's/.*/PasswordAuthentication no.*/ PasswordAuthentication yes/' -i /etc/ssh/sshd_config - sudo service sshd restart Puppet_Agent: type: Cloud.Puppet properties: provider: PEOAWS environment: production role: 'role::linux_webserver' host: '\${Webserver.*}' osType: linux username: '\${input.username}' password: '\${input.password}' useSudo: true </pre>

Puppet-beheer in AWS met gegenereerde PublicPrivateKey

Voorbeeld van...	Voorbeeldblueprint-YAML
remoteAccess.authentication-verificatie in AWS met generatedPublicPrivateKey-toegang.	<pre> inputs: {} resources: Machine: type: Cloud.AWS.EC2.Instance properties: flavor: small imageRef: ami-a4dc46db remoteAccess: authentication: generatedPublicPrivateKey Puppet_Agent: type: Cloud.Puppet properties: provider: puppet-BlueprintProvisioningITSuite environment: production role: 'role::linux_webserver' host: '\${Machine.*}' osType: linux username: ubuntu useSudo: true agentConfiguration: runInterval: 15m certName: '\${Machine.address}' useSudo: true </pre>

Voorbeelden van cloudsjabloon voor vCenter Puppet-configuratie

Er zijn verschillende opties voor het configureren van cloudsjablonen om Puppet-gebaseerd configuratiebeheer op vCenter-computerbronnen te ondersteunen.

Puppet in vSphere met gebruikersnaam- en wachtwoordverificatie

In het volgende voorbeeld ziet u YAML-voorbeeldcode voor Puppet in een vSphere-OVA met gebruikersnaam- en wachtwoordverificatie.

Tabel 6-4.

Voorbeeld van...	Voorbeeldblueprint-YAML
<p>YAML-code voor Puppet in een vSphere-OVA met gebruikersnaam- en wachtwoordverificatie.</p>	<pre> inputs: username: type: string title: Username default: puppet password: type: string title: Password encrypted: true default: VMware@123 resources: Puppet_Agent: type: Cloud.Puppet properties: provider: PEonAWS environment: dev role: 'role::linux_webserver' username: '\${input.username}' password: '\${input.password}' useSudo: true host: '\${Webserver.*}' osType: linux agentConfiguration: runInterval: 15m certName: '\${Machine.address}' Webserver: type: Cloud.vSphere.Machine properties: cpuCount: 1 totalMemoryMB: 1024 imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' ssh-authorized-keys: - ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAQDytVL+Q6+vGbmKXoRpX dmettem@dmettem-m01.vmware.com runcmd: - echo "Defaults:\${input.username} </pre>
<p>YAML-code voor Puppet in een vSphere-OVA met gebruikersnaam- en wachtwoordverificatie op de berekeningsresource.</p>	<pre> inputs: username: type: string title: Username default: puppet </pre>

Tabel 6-4. (vervolg)

Voorbeeld van...	Voorbeeldblueprint-YAML
	<pre> password: type: string title: Password encrypted: true default: VMware@123 resources: Puppet_Agent: type: Cloud.Puppet properties: provider: PEonAWS environment: dev role: 'role::linux_webserver' username: '\${input.username}' password: '\${input.password}' useSudo: true host: '\${Webserver.*}' osType: linux agentConfiguration: runInterval: 15m certName: '\${Machine.address}' Webserver: type: Cloud.vSphere.Machine properties: cpuCount: 1 totalMemoryMB: 1024 imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' ssh-authorized-keys: - ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDytVL+Q6+vGbmKXoRpX dmettem@dmettem-m01.vmware.com runcmd: - echo "Defaults:\${input.username} </pre>
<p>YAML-code voor Puppet in een vCenter met wachtwoordverificatie voor externe toegang op de berekeningsresource.</p>	<pre> inputs: username: type: string title: Username description: Username to use to install Puppet agent default: puppet password: type: string title: Password default: VMware@123 encrypted: true </pre>

Tabel 6-4. (vervolg)

Voorbeeld van...	Voorbeeldblueprint-YAML
	<pre> description: Password for the given username to install Puppet agent resources: Puppet-Ubuntu: type: Cloud.vSphere.Machine properties: flavor: small imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova remoteAccess: authentication: usernamePassword username: '\${input.username}' password: '\${input.password}' Puppet_Agent: type: Cloud.Puppet properties: provider: PEMasterOnPrem environment: production role: 'role::linux_webserver' username: '\${input.username}' password: '\${input.password}' host: '\${Puppet-Ubuntu.*}' useSudo: true agentConfiguration: certName: '\${Puppet-Ubuntu.address}' </pre>

Puppet in vSphere met gegenereerde PublicPrivateKey-verificatie

Tabel 6-5.

Voorbeeld van...	Voorbeeldblueprint-YAML
YAML-code voor Puppet in een vSphere-OVA met gegenereerde PublicPrivateKey-verificatie op de berekeningsresource.	<pre> inputs: {} resources: Machine: type: Cloud.vSphere.Machine properties: flavor: small imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova remoteAccess: authentication: generatedPublicPrivateKey Puppet_Agent: type: Cloud.Puppet properties: provider: puppet-BlueprintProvisioningITSuite environment: production role: 'role::linux_webserver' host: '\${Machine.*}' osType: linux username: ubuntu useSudo: true agentConfiguration: runInterval: 15m certName: '\${Machine.address}' - echo "Defaults:\${input.username}" </pre>

vRealize Automation-schema met eigenschappen voor aangepaste resources

Met de Infrastructure-as-code-editor van vRealize Automation kunt u klikken of de muisaanwijzer bewegen voor hulp bij het voltooien van syntaxis en code. Als u de volledige set met resource-eigenschappen van de cloudsjabloon wilt weergeven, ook wel aangepaste eigenschappen genoemd, raadpleegt u het geconsolideerde resourceschema.

Het schema is beschikbaar op de VMware {code}-site. Volg de link en klik op **Modellen** om de resourceobjecten weer te geven die beschikbaar zijn voor cloudsjablonen, voorheen blueprints genoemd.

- [Schema van vRealize Automation-resourcetype op VMware {code}](#)

Speciale Cloud Assembly-eigenschappen

Cloud Assembly ondersteunt een klein aantal eigenschappen die handig kunnen zijn buiten de productieomgeving of in andere speciale situaties. De eigenschappen worden niet in het schema weergegeven.

Voorzichtig De volgende eigenschappen mogen alleen worden toegepast in gevallen waarin aanpassing van het gastbesturingssysteem niet wordt getest of verwacht.

awaitIp	<p>Standaard wordt inrichtingsstatus van vRealize Automation niet als voltooid gemeld totdat het gastbesturingssysteem volledig is ingeschakeld en de configuratie is voltooid.</p> <p>Door gebruik te maken van <code>awaitIp: false</code> kan de inrichting worden voltooid, ook als er geen volledige configuratie heeft plaatsgevonden.</p> <p>PAS OP: met deze instelling wordt het inrichtingsproces weliswaar eerder voltooid, maar krijgt u mogelijk ook te maken met een niet-geconfigureerde machine zonder IP-adres.</p>
awaitHostName	<p>Net als awaitIp kan het gebruik van <code>awaitHostName: false</code> de inrichting voltooien, ook als er nog geen hostnaam voor de machine is geconfigureerd.</p>

Andere manieren om Cloud Assembly-sjablonen te maken

U kunt een Cloud Assembly-sjabloon niet alleen samenstellen op basis van een leeg canvas, maar ook gebruikmaken van bestaande code.

Cloudsjabloon klonen

Om een sjabloon te klonen, gaat u naar **Ontwerp**, selecteert u een bron en klikt u op **Klonen**. U kloont een cloudsjabloon om een kopie op basis van de bron te maken. Vervolgens wijst u de kloon toe aan een nieuw project of gebruikt u deze als startcode voor een nieuwe applicatie.

Uploaden en downloaden

U kunt YAML-code voor cloudsjablonen uploaden, downloaden en delen op elke manier die zinvol is voor uw site. U kunt zelfs de sjablooncode aanpassen met behulp van externe editors en ontwikkelingsomgevingen.

Opmerking Een goede manier om de code van een gedeelde sjablooncode te valideren is deze te controleren in de Cloud Assembly-code-editor op de ontwerppagina.

Cloud Assembly integreren met een opslagplaats

Een geïntegreerde opslagplaats voor Git-bronbeheer kan cloudsjablonen beschikbaar maken voor gekwalificeerde gebruikers als basis voor een nieuwe implementatie. Zie [Hoe gebruik ik Git-integratie in Cloud Assembly](#).

Levenscycli van applicaties uitbreiden en automatiseren met uitbreidbaarheid

U kunt de levenscyclussen van applicaties uitbreiden door uitbreidbaarheidsacties of vRealize Orchestrator-werkstromen met uitbreidbaarheidsabonnementen te gebruiken.

Met Cloud Assembly-uitbreidbaarheid kunt u een uitbreidbaarheidsactie of vRealize Orchestrator-werkstroom aan een gebeurtenis toewijzen met behulp van abonnementen. Wanneer de opgegeven gebeurtenis plaatsvindt, start het abonnement de actie of de werkstroom en worden alle abonnees hiervan op de hoogte gesteld.

Uitbreidbaarheidsacties

Uitbreidbaarheidsacties zijn kleine, lichte codescripts om een actie op te geven en te bepalen hoe die actie moet worden uitgevoerd. U kunt uitbreidbaarheidsacties importeren uit vooraf gedefinieerde Cloud Assembly-actiesjablonen of uit een ZIP-bestand. U kunt ook de actie-editor gebruiken om aangepaste scripts voor uw uitbreidbaarheidsacties te maken. Wanneer meerdere actiescripts in één script worden samengebracht, maakt u een actiestroom. Met actiestromen kunt u een reeks acties maken. Zie [Wat is een actiestroom](#) voor informatie over het gebruik van actiestromen.

vRealize Orchestrator-werkstromen

Door Cloud Assembly te integreren met uw bestaande vRealize Orchestrator-omgeving, kunt u werkstromen in uw uitbreidbaarheidsabonnementen gebruiken.

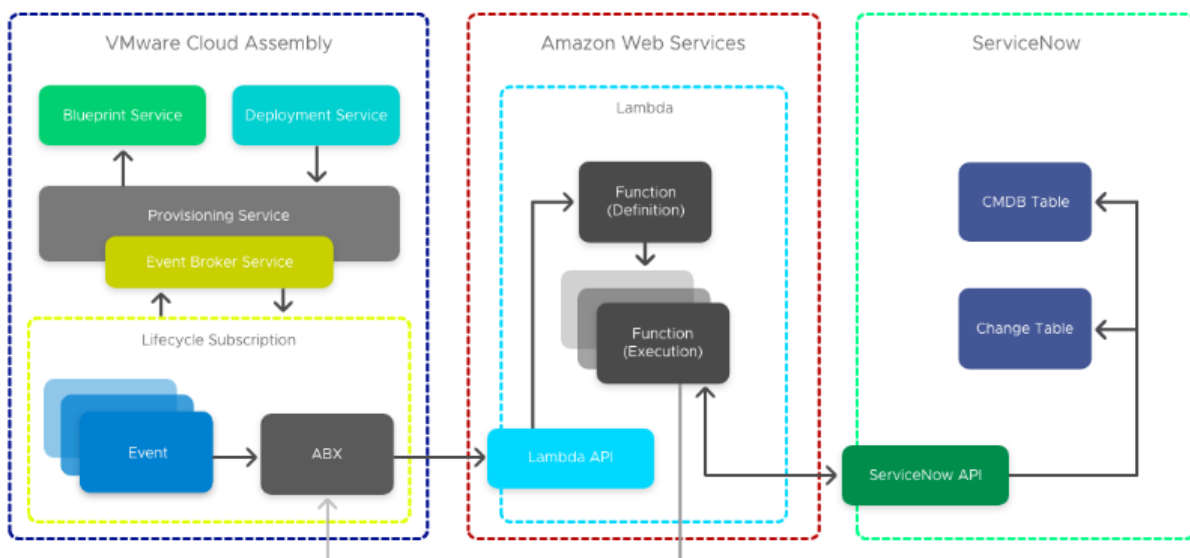
Abonnementen op uitbreidbaarheidsacties

U kunt een uitbreidbaarheidsactie aan een Cloud Assembly-abonnement toewijzen om de levenscyclus van uw applicatie uit te breiden.

Opmerking De volgende abonnementen zijn gebruiksscenario's en omvatten niet alle functionaliteit van uitbreidbaarheidsacties.

Hoe integreer ik Cloud Assembly met ServiceNow met behulp van uitbreidbaarheidsacties

Met uitbreidbaarheidsacties kunt u Cloud Assembly integreren met zakelijk ITSM, zoals ServiceNow.

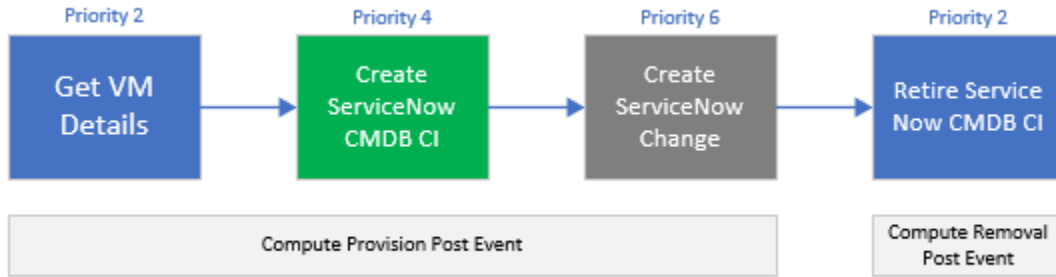


Zakelijke gebruikers integreren voor compliance doorgaans hun cloudbeheerplatform met een IT Service Management- (ITSM) en Configuration Management Database-platform (CMDB). In het volgende voorbeeld kunt u Cloud Assembly met ServiceNow voor CMDB en ITSM integreren door uitbreidbaarheidsactiescripts te gebruiken.

Opmerking U kunt ServiceNow ook met Cloud Assembly integreren door vRealize Orchestrator-werkstromen te gebruiken. Zie [Hoe integreer ik Cloud Assembly voor ITSM met ServiceNow met behulp van vRealize Orchestrator-werkstromen](#) voor informatie over het integreren van ServiceNow door werkstromen te gebruiken.

Om deze integratie te maken, gebruikt u vier uitbreidbaarheidsactiescripts. De eerste drie scripts worden tijdens het inrichten sequentieel geïnitieerd bij de post-gebeurtenis voor het inrichten van de berekening. Het vierde script wordt geactiveerd bij de post-gebeurtenis voor het verwijderen van de berekening.

Zie [De gebeurtenisonderwerpen van Cloud Assembly](#) voor meer informatie over gebeurtenisonderwerpen.



VM-gegevens ophalen

Het script VM-gegevens ophalen haalt aanvullende gegevens van de lading op die vereist zijn voor het maken van CI en een identiteitstoken dat is opgeslagen in Amazon Web Services Systems Manager Parameter Store (SSM). Verder werkt dit script `customProperties` bij met aanvullende eigenschappen voor later gebruik.

ServiceNow CMDB CI maken

Het script ServiceNow CMDB CI maken geeft de URL van de ServiceNow-instantie als invoer door en slaat de instantie in SSM op om aan de beveiligingsvereisten te voldoen. Dit script leest ook het unieke record-id-antwoord van ServiceNow CMDB (`sys_id`). Het geeft dit door als uitvoer en schrijft de aangepaste eigenschap `serviceNowSysId` tijdens het maken. Deze waarde wordt gebruikt om de CI als Buiten gebruik gesteld te markeren wanneer de instantie is vernietigd.

Opmerking Er moeten mogelijk aanvullende rechten aan uw vRealize Automation services Amazon Web Services-rol worden toegewezen om Lambda toegang tot de SSM Parameter Store te geven.

ServiceNow-wijziging maken

Dit script voltooit de ITSM-integratie door de URL van de ServiceNow-instantie als invoer door te geven en de ServiceNow-verificatiegegevens als SSM op te slaan om aan de beveiligingsvereisten te voldoen.

ServiceNow-wijziging maken

Het ServiceNow-script voor het buiten gebruik stellen van CMDB vraagt ServiceNow om te stoppen en markeert de CI als buiten gebruik gesteld op basis van de aangepaste eigenschap `serviceNowSysId` die in het aanmaakscript is gemaakt.

Voorwaarden

- Voordat u deze integratie configureert, filtert u alle gebeurtenisabonnementen met de voorwaardelijke cloudsjablooneigenschap: `event.data["customProperties"] ["enable_servicenow"] === "true"`

Opmerking Deze eigenschap bestaat in cloudsjablonen die een ServiceNow-integratie vereisen.

- Download en installeer Python.

Zie [Een uitbreidbaarheidsabonnement maken](#) voor meer informatie over het filteren van abonnementen.

Procedure

- 1 Open een opdrachtregelprompt vanaf uw virtuele machine.
- 2 Voer het script VM-gegevens ophalen uit.

```
from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):
    baseUri = inputs['url']
    casToken = client.get_parameter(Name="casToken",WithDecryption=True)

    url = baseUri + "/iaas/login"
    headers = {"Accept":"application/json","Content-Type":"application/json"}
    payload = {"refreshToken":casToken['Parameter']['Value']}

    results = requests.post(url,json=payload,headers=headers)

    bearer = "Bearer "
    bearer = bearer + results.json()["token"]

    deploymentId = inputs['deploymentId']
    resourceId = inputs['resourceIds'][0]

    print("deploymentId: " + deploymentId)
    print("resourceId:" + resourceId)

    machineUri = baseUri + "/iaas/machines/" + resourceId
    headers = {"Accept":"application/json","Content-Type":"application/json",
"Authorization":bearer }
    resultMachine = requests.get(machineUri,headers=headers)
    print("machine: " + resultMachine.text)

    print( "serviceNowCPUCount: " + json.loads(resultMachine.text)["customProperties"]
["cpuCount"] )
    print( "serviceNowMemoryInMB: " + json.loads(resultMachine.text)["customProperties"]
["memoryInMB"] )

    #update customProperties
    outputs = {}
    outputs['customProperties'] = inputs['customProperties']
    outputs['customProperties']['serviceNowCPUCount'] = int(json.loads(resultMachine.text)
["customProperties"]["cpuCount"])
    outputs['customProperties']['serviceNowMemoryInMB'] = json.loads(resultMachine.text)
["customProperties"]["memoryInMB"]
    return outputs
```

3 Voer de actie voor het maken van een CMDB-configuratie-item uit.

```

from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):

    snowUser = client.get_parameter(Name="serviceNowUserName",WithDecryption=False)
    snowPass = client.get_parameter(Name="serviceNowPassword",WithDecryption=True)
    table_name = "cmdb_ci_vmware_instance"
    url = "https://" + inputs['instanceUrl'] + "/api/now/table/{0}".format(table_name)
    headers = {'Content-type': 'application/json', 'Accept': 'application/json'}
    payload = {
        'name': inputs['customProperties']['serviceNowHostname'],
        'cpus': int(inputs['customProperties']['serviceNowCPUCount']),
        'memory': inputs['customProperties']['serviceNowMemoryInMB'],
        'correlation_id': inputs['deploymentId'],
        'disks_size': int(inputs['customProperties']['provisionGB']),
        'location': "Sydney",
        'vcenter_uuid': inputs['customProperties']['vcUuid'],
        'state': 'On',
        'sys_created_by': inputs['__metadata']['userName'],
        'owned_by': inputs['__metadata']['userName']
    }
    results = requests.post(
        url,
        json=payload,
        headers=headers,
        auth=(snowUser['Parameter']['Value'], snowPass['Parameter']['Value'])
    )
    print(results.text)

    #parse response for the sys_id of CMDB CI reference
    if json.loads(results.text)['result']:
        serviceNowResponse = json.loads(results.text)['result']
        serviceNowSysId = serviceNowResponse['sys_id']
        print(serviceNowSysId)

    #update the serviceNowSysId customProperty
    outputs = {}
    outputs['customProperties'] = inputs['customProperties']
    outputs['customProperties']['serviceNowSysId'] = serviceNowSysId;
    return outputs

```

4 Voer het script voor de aanmaakactie uit.

```

from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):
    snowUser = client.get_parameter(Name="serviceNowUserName",WithDecryption=False)

```

```

snowPass = client.get_parameter(Name="serviceNowPassword",WithDecryption=True)
table_name = "change_request"
url = "https://" + inputs['instanceUrl'] + "/api/now/table/{0}".format(table_name)
headers = {'Content-type': 'application/json', 'Accept': 'application/json'}
payload = {
    'short_description': 'Provision CAS VM Instance'
}
results = requests.post(
    url,
    json=payload,
    headers=headers,
    auth=(snowUser['Parameter']['Value'], snowPass['Parameter']['Value'])
)
print(results.text)

```

Resultaten

Cloud Assembly is geïntegreerd met ITSM ServiceNow.

Wat nu te doen

Indien gewenst kunt u uw CI buiten gebruik stellen door gebruik te maken van de actie voor het buiten gebruik stellen van het CMDB-configuratie-item:

```

from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):
    snowUser = client.get_parameter(Name="serviceNowUserName",WithDecryption=False)
    snowPass = client.get_parameter(Name="serviceNowPassword",WithDecryption=True)
    tableName = "cmdb_ci_vmware_instance"
    sys_id =inputs['customProperties']['serviceNowSysId']
    url = "https://" + inputs['instanceUrl'] + "/api/now/"+tableName+"/{0}".format(sys_id)
    headers = {'Content-type': 'application/json', 'Accept': 'application/json'}
    payload = {
        'state': 'Retired'
    }

    results = requests.put(
        url,
        json=payload,
        headers=headers,
        auth=(inputs['username'], inputs['password'])
    )
    print(results.text)

```

Voor meer informatie over hoe u uitbreidbaarheidsacties kunt gebruiken om ServiceNow in Cloud Assembly te integreren, raadpleegt u [Extending Cloud Assembly with Action Based Extensibility for ServiceNow Integration](#).

Hoe kan ik virtuele machines tijdens het inrichten taggen door uitbreidbaarheidsacties te gebruiken?

U kunt uitbreidbaarheidsacties gebruiken samen met abonnementen om het taggen van VM's te automatiseren en te vereenvoudigen.

Als cloudbeheerder kunt u implementaties maken die automatisch met opgegeven invoer en uitvoer worden getagd door uitbreidbaarheidsacties en uitbreidbaarheidsabonnementen te gebruiken. Wanneer een nieuwe implementatie wordt gemaakt voor het project dat het abonnement 'VM taggen' bevat, activeert de implementatiegebeurtenis het script 'VM taggen' om te worden uitgevoerd en worden de tags automatisch uitgevoerd. Dit bespaart tijd en bevordert de efficiëntie terwijl implementatiebeheer eenvoudiger wordt.

Voorwaarden

- Toegang tot de verificatiegegevens van de cloudbeheerder.
- Amazon Web Services-rol voor Lambda-functies.

Procedure

- 1 Navigeer naar **Uitbreidbaarheid > Bibliotheek > Acties > Nieuwe actie** en maak een actie met de volgende parameters.

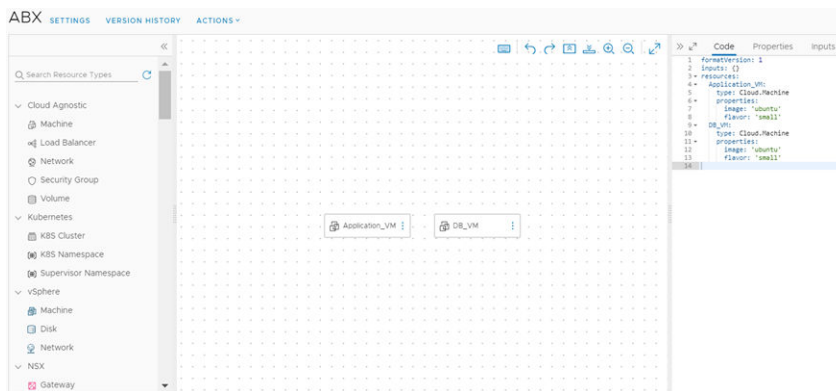
Parameter	Beschrijving
Actienaam	Naam van uitbreidbaarheidsactie, bij voorkeur met het voor- of achtervoegsel TagVM .
Project	Project waarop u de uitbreidbaarheidsactie kunt testen.
Actiesjabloon	VM taggen
Runtime	Python
Scriptbron	Script schrijven

- 2 Voer **Handler** in als **Hoofdfunctie**.
- 3 Voeg taginvoer toe om de uitbreidbaarheidsactie te testen.
Bijvoorbeeld: `resourceNames = ["DB_VM"]` en `target = world`.
- 4 Om uw actie op te slaan, klikt u op **Opslaan**.
- 5 Als u uw actie wilt testen, klikt u op **Testen**.
- 6 Als u de actie-editor wilt afsluiten, klikt u op **Sluiten**.
- 7 Navigeer naar **Uitbreidbaarheid > Abonnementen**.
- 8 Klik op **Nieuw abonnement**.

9 Voer de volgende abonnementsgegevens in.

Gegevens	Instelling
Gebeurtenisonderwerp	Selecteer een gebeurtenisonderwerp dat is gerelateerd aan de tagfase van de VM. Bijvoorbeeld: berekeningstoeewijzing. Opmerking Tags moeten deel uitmaken van de gebeurtenisparameters van het geselecteerde gebeurtenisonderwerp.
Blokkeren	Stel de time-out voor het abonnement in op 1 minuut.
Actie/werkstroom	Selecteer een runnable-type voor de uitbreidbaarheidsactie en selecteer uw aangepaste uitbreidbaarheidsactie.

- Klik op **Opslaan** om het abonnement voor de aangepaste uitbreidbaarheidsactie op te slaan.
- Navigeer naar **Ontwerp > Cloudsjablonen** en maak een cloudsjabloon op basis van een leeg canvas.
- Voeg twee virtuele machines toe aan de cloudsjabloon: `Application_VM` en `DB_VM`.



- Als u de VM's wilt implementeren, klikt u op **Implementeren**.
- Controleer tijdens het implementeren of de gebeurtenis is begonnen en de uitbreidbaarheidsactie wordt uitgevoerd.
- Om te controleren of de tags op de juiste wijze zijn toegepast, gaat u naar **Resources > Resources > Virtuele machines**.

Hoe kan ik de naam van een netwerkinterfacecontroller configureren met behulp van uitbreidbaarheidsacties

U kunt de interfacenaam van een netwerkinterfacecontroller (NIC) configureren met behulp van IaaS API-aanroepen die worden toegepast via uitbreidbaarheidsacties.

Als u de interfacenaam van een NIC wilt configureren, moet u `GET`- en `PATCH`-aanroepen naar de vRealize Automation IaaS API maken. Door een `GET`-aanroep naar `https://your_vRA_fqdn/iaas/api/machines/{id}` te maken, kunt u de NIC-link ophalen voor de computerbron die u wilt wijzigen. Vervolgens kunt u een `PATCH`-aanroep naar `https://your_vRA_fqdn/iaas/api/machines/{id}/network-interfaces/{nicId}` maken, die de NIC-interfacenaam als lading bevat, om de nieuwe naam voor uw NIC toe te voegen.

Het volgende scenario gebruikt een Python-voorbeeldscript dat kan worden gebruikt voor de configuratie van de NIC-interfacenaam. Voor uw eigen gebruiksscenario's kunt u een ander script en andere scripttaal gebruiken, zoals Node.js.

Voorwaarden

- U kunt de naam van de NIC-interface alleen configureren voordat u een computerbron inricht. Daarom kan alleen het gebeurtenisonderwerp **Berekeningsinrichting** worden geselecteerd voor relevante uitbreidbaarheidsabonnementen.
- U kunt alleen NIC-interfacenamen configureren voor NIC's die Microsoft Azure als provider gebruiken.

Procedure

- 1 Maak de uitbreidbaarheidsactie.
 - a Navigeer naar **Uitbreidbaarheid > Acties**.
 - b Klik op **Nieuwe Actie**.
 - c Voer een naam en een project in voor de uitbreidbaarheidsactie en klik op **Volgende**.

- d Voeg het NIC-configuratiescript toe.

Het volgende is een voorbeeld van een Python-script:

```
import json

def handler(context, inputs):

    # Get the machine info, which contains machine nic link
    response = context.request('/iaas/api/machines/'+inputs["resourceIds"][0], "GET",
    {})

    # Build PATCH machine nic payload here
    name = "customized-nic-02";
    data = {'name':name};

    # Convert machine data string to json object
    response_json = json.loads(response["content"])

    # Patch machine nic
    response_patch = context.request(response_json["_links"]["network-interfaces"]
    ["hrefs"][0] + "?apiVersion=2021-07-15", 'PATCH', data)

    # return value is empty since we are not changing any compute provisioning
    parameters
    outputs = {}
    return outputs
```

Het voorgaande voorbeeldscript voert twee primaire bewerkingen uit via de IaaS API. Eerst gebruikt het script een **GET**-aanroep om de NIC-link op te halen en vervolgens wordt een **PATCH**-aanroep gebruikt om de interfacenaam toe te passen. In dit voorbeeld is de naam van de NIC-interface als "customized-nic-02" in het script vastgelegd.

- e Als u het bewerken van de nieuwe uitbreidbaarheidsactie wilt voltooien, klikt u op **Opslaan**.

2 Maak een uitbreidbaarheidsabonnement.

- Navigeer naar **Uitbreidbaarheid > Abonnementen**.
- Klik op **Nieuw abonnement**.
- Voer een naam in voor het uitbreidbaarheidsabonnement.
- Selecteer onder **Gebeurtenisonderwerp Berekeningsinrichting** als gebeurtenisonderwerp voor het uitbreidbaarheidsabonnement.
- Selecteer onder **Actie/werkstroom** de uitbreidbaarheidsactie die u heeft gemaakt voor de NIC-configuratie.

- f Schakel gebeurtenisblokkering in.

Door blokkering in te schakelen, zorgt u ervoor dat het inrichtingsproces is geblokkeerd totdat de uitvoering van de uitbreidbaarheidsactie is voltooid.

- g Klik op **Opslaan** om het bewerken van het uitbreidbaarheidsabonnement te voltooien.

Resultaten

Het nieuwe uitbreidbaarheidsabonnement wordt uitgevoerd wanneer een computerinrichtingsgebeurtenis wordt geactiveerd en configureert de NIC-interfacenaam voor de in te richten computerbronnen.

Meer informatie over uitbreidbaarheidsacties

Actiegebaseerde uitbreidbaarheid gebruikt gestroomlijnde codescripts in Cloud Assembly om de uitbreidbaarheidsacties te automatiseren.

Actiegebaseerde uitbreidbaarheid biedt een lichte en flexibele runtime-engine-interface waarin u kleine scriptbare acties kunt definiëren en kunt configureren om te starten wanneer gebeurtenissen optreden die in uitbreidbaarheidsabonnementen zijn opgegeven.

U kunt deze uitbreidbaarheidsactiescripts van code in Cloud Assembly, of in uw lokale omgeving, maken en toewijzen aan abonnementen. Uitbreidbaarheidsactiescripts worden gebruikt voor een lichtere en eenvoudigere automatisering van taken en stappen. Zie [vRealize Orchestrator-integratie in Cloud Assembly configureren](#) voor meer informatie over het integreren van Cloud Assembly met een vRealize Orchestrator-server.

Actiegebaseerde uitbreidbaarheid biedt:

- Een alternatief voor vRealize Orchestrator-werkstromen met kleine en herbruikbare scriptbare acties, voor lichte integraties en aanpassingen.
- Een manier om actiesjablonen opnieuw te gebruiken die herbruikbare acties met parameters bevatten.

U kunt uitbreidbaarheidsacties maken door een aangepaste actiescriptcode te schrijven of een vooraf gedefinieerde scriptcode als ZIP-pakket te importeren. Actiegebaseerde uitbreidbaarheid ondersteunt de runtime-omgevingen Node.js, Python en PowerShell. De runtimes Node.js en Python zijn afhankelijk van Amazon Web Services Lambda. Daarom moet u een actief abonnement met Amazon Web Services Identiteits- en toegangsbeheer hebben en Amazon Web Services als eindpunt configureren in Cloud Assembly. Zie [ABX: Serverless Extensibility of Cloud Assembly Services](#) voor informatie over het aan de slag gaan met Amazon Web Services Lambda.

Opmerking Uitbreidbaarheidsacties zijn specifiek voor een project.

Hoe maak ik uitbreidbaarheidsacties

Met Cloud Assembly kunt u uitbreidbaarheidsacties maken voor gebruik in uitbreidbaarheidsabonnementen.

Uitbreidbaarheidsacties bieden zeer aanpasbare, lichte en flexibele manieren om de levenscyclus van applicaties uit te breiden met door gebruikers gedefinieerde scriptcode en actiesjablonen. Actiesjablonen bevatten vooraf gedefinieerde parameters die helpen bij het instellen van de basis van uw uitbreidbaarheidsactie.

Er zijn twee methoden om een uitbreidbaarheidsactie te maken:

- Door gebruiker gedefinieerde code schrijven voor een uitbreidbaarheidsactiescript.

Opmerking Voor het schrijven van door gebruikers gedefinieerde code in de uitbreidbaarheidsactie-editor is mogelijk een actieve internetverbinding vereist.

- Een implementatiepakket als ZIP-pakket voor een uitbreidbaarheidsactie importeren. Zie [Een ZIP-pakket maken voor uitbreidbaarheidsacties van Python-runtime](#), [Een ZIP-pakket voor uitbreidbaarheidsacties van Node.js-runtime maken](#) of [Een ZIP-pakket maken voor uitbreidbaarheidsacties van PowerShell-runtime](#) voor informatie over het maken van een ZIP-pakket voor uitbreidbaarheidsacties.

De volgende stappen beschrijven de procedure voor het maken van een uitbreidbaarheidsactie die Amazon Web Services als FaaS-provider gebruikt.

Voorwaarden

- Lidmaatschap van een actief en geldig project.
- Geconfigureerde Amazon Web Services-rol voor Lambda-functies. Bijvoorbeeld: `AWSLambdaBasicExecutionRole`.
- Rol van cloudbeheerder of `iam:PassRole`-rechten ingeschakeld.

Procedure

- 1 Selecteer **Uitbreidbaarheid > Bibliotheek > Acties**.
- 2 Klik op **Nieuwe Actie**.
- 3 Voer een naam in voor uw actie en selecteer een project.
- 4 (Optioneel) Voer een beschrijving voor uw actie in.
- 5 Klik op **Volgende**.
- 6 Zoek en selecteer een actiesjabloon.

Opmerking Als u een aangepaste actie wilt maken zonder een actiesjabloon te gebruiken, selecteert u **Aangepast script**.

Er worden nieuwe configureerbare parameters weergegeven.

- 7 Selecteer **Script schrijven** of **Pakket importeren**.
- 8 Selecteer een runtime van de actie.

- 9 Voer een naam voor **Hoofdfunctie** in voor het toegangspunt van de actie.

Opmerking Voor acties die zijn geïmporteerd uit een ZIP-pakket moet de hoofdfunctie ook de naam bevatten van het scriptbestand dat het toegangspunt bevat. Als uw hoofdscripbestand bijvoorbeeld `main.py` als titel heeft en uw toegangspunt `handler` (`context, inputs`) is, moet de naam van de hoofdfunctie `main.handler` zijn.

- 10 Definieer de invoer- en uitvoerparameters van de actie.

- 11 (Optioneel) Voeg geheimen of constanten voor uitbreidbaarheidsacties toe aan uw standaardinvoer.

Opmerking Zie [Hoe kan ik geheimen maken voor gebruik in uitbreidbaarheidsacties](#) en [Hoe kan ik constanten voor de uitbreidbaarheidsactie maken](#) voor meer informatie over geheimen en constanten voor uitbreidbaarheidsacties.

- 12 (Optioneel) Voeg applicatieafhankelijkheden toe aan de actie.

Opmerking Voor PowerShell-scripts kunt u uw applicatieafhankelijkheden definiëren zodat deze worden opgelost in de PowerShell Gallery-opslagplaats. Als u uw applicatieafhankelijkheden wilt definiëren, zodat ze vanuit de openbare opslagplaats kunnen worden omgezet, gebruikt u de volgende indeling:

```
@{
    Name = 'Version'
}

e.g.

@{
    Pester = '4.3.1'
}
```

Opmerking Voor acties die zijn geïmporteerd uit een ZIP-pakket, worden applicatieafhankelijkheden automatisch toegevoegd.

- 13 Als u time-outs en geheugenlimieten wilt definiëren, schakelt u de optie **Aangepaste time-outs en limieten instellen** in.
- 14 Klik op **Opslaan** en klik vervolgens op **Testen** om uw actie te testen.

Wat nu te doen

Nadat de uitbreidbaarheidsactie is gemaakt en geverifieerd, kunt u deze aan een abonnement toewijzen.

Opmerking Uitbreidbaarheidsabonnementen gebruiken de laatst uitgebrachte versie van een uitbreidbaarheidsactie. Nadat u een nieuwe versie van een actie hebt gemaakt, klikt u op **Versies** in de rechterbovenhoek van het editorvenster. Als u de versie wilt vrijgeven van de actie die u wilt gebruiken in uw abonnement, klikt u op **Vrijgeven**.

Een ZIP-pakket maken voor uitbreidbaarheidsacties van Python-runtime

U kunt een ZIP-pakket maken dat het Python-script en de afhankelijkheden bevat die worden gebruikt door uw Cloud Assembly-uitbreidbaarheidsacties.

Er zijn twee methoden om het script voor uw uitbreidbaarheidsacties te bouwen:

- Uw script rechtstreeks in de editor voor uitbreidbaarheidsacties in Cloud Assembly schrijven.
- Uw script in uw lokale omgeving maken en dit, met alle relevante afhankelijkheden, toevoegen aan een ZIP-pakket.

Door een ZIP-pakket te gebruiken, kunt u een aangepaste vooraf geconfigureerde sjabloon maken van actiescripts en afhankelijkheden die u kunt importeren in Cloud Assembly voor gebruik in uitbreidbaarheidsacties.

Daarnaast kunt u een ZIP-pakket gebruiken in scenario's waarin modules die zijn gekoppeld aan afhankelijkheden in uw actiescript niet kunnen worden omgezet door de Cloud Assembly-service, bijvoorbeeld wanneer uw omgeving geen internettoegang heeft.

U kunt ook een ZIP-pakket gebruiken om uitbreidbaarheidsacties te maken die meerdere Python-scriptbestanden bevatten. Het gebruik van meerdere scriptbestanden kan nuttig zijn voor het organiseren van de structuur van uw uitbreidbaarheidsactiecode.

Voorwaarden

Als u Python 3.3 of lager gebruikt, downloadt en configureert u het installatieprogramma van het PIP-pakket. Zie [Python Package Index](#).

Procedure

- 1 Maak een map voor uw actiescript en afhankelijkheden op uw lokale machine.

Bijvoorbeeld: `/home/user1/zip-action`.

- 2 Voeg uw Python-hoofdactiescript(s) aan de map toe.

Bijvoorbeeld: `/home/user1/zip-action/main.py`.

3 (Optioneel) Voeg afhankelijkheden voor uw Python-script toe aan de map.

- a Maak een bestand `requirements.txt` dat uw afhankelijkheden bevat. Zie [Requirements files](#).
- b Open een Linux-shell.

Opmerking De runtime van actiegebaseerde uitbreidbaarheid in Cloud Assembly is Linux-gebaseerd. Het is daarom mogelijk dat Python-afhankelijkheden die in een Windows-omgeving zijn gecompileerd het gegenereerde ZIP-pakket onbruikbaar maken voor het maken van uitbreidbaarheidsacties. Daarom moet u een Linux-shell gebruiken.

- c Installeer uw bestand `requirements.txt` in de scriptmap door de volgende opdracht uit te voeren:

```
pip install -r requirements.txt --target=home/user1/zip-action
```

4 Selecteer in de toegewezen map uw scriptelementen en, indien van toepassing, uw bestand `requirements.txt` en comprimeer ze in een ZIP-pakket.

Opmerking Zowel uw script- als afhankelijkheidselementen moeten worden opgeslagen op het rootniveau van het ZIP-pakket. Wanneer u het ZIP-pakket in een Linux-omgeving maakt, kan er een probleem optreden waarbij de inhoud van het pakket niet op het rootniveau is opgeslagen. Als u dit probleem ondervindt, maakt u het pakket door de `zip -r`-opdracht uit te voeren in uw opdrachtregelshell.

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

Wat nu te doen

Gebruik het ZIP-pakket om een uitbreidbaarheidsactiescript te maken. Zie [Hoe maak ik uitbreidbaarheidsacties](#).

Een ZIP-pakket voor uitbreidbaarheidsacties van Node.js-runtime maken

U kunt een ZIP-pakket maken dat het script en de afhankelijkheden van Node.js bevat die door uw Cloud Assembly-uitbreidbaarheidsacties worden gebruikt.

Er zijn twee methoden om het script voor uw uitbreidbaarheidsacties te bouwen:

- Uw script rechtstreeks in de editor voor uitbreidbaarheidsacties in Cloud Assembly schrijven.
- Uw script in uw lokale omgeving maken en dit, met alle relevante afhankelijkheden, toevoegen aan een ZIP-pakket.

Door een ZIP-pakket te gebruiken, kunt u een aangepaste vooraf geconfigureerde sjabloon maken van actiescripts en afhankelijkheden die u kunt importeren in Cloud Assembly voor gebruik in uitbreidbaarheidsacties.

Daarnaast kunt u een ZIP-pakket gebruiken in scenario's waarin modules die zijn gekoppeld aan afhankelijkheden in uw actiescript niet kunnen worden omgezet door de Cloud Assembly-service, bijvoorbeeld wanneer uw omgeving geen internettoegang heeft.

U kunt ook pakketten gebruiken om uitbreidbaarheidsacties te maken die meerdere Node.js-scriptbestanden bevatten. Het gebruik van meerdere scriptbestanden kan nuttig zijn voor het organiseren van de structuur van uw uitbreidbaarheidsactiecode.

Procedure

- 1 Maak een map voor uw actiescript en afhankelijkheden op uw lokale machine.

Bijvoorbeeld: `/home/user1/zip-action`.

- 2 Voeg uw Node.js-hoofdactiescript(s) toe aan de map.

Bijvoorbeeld: `/home/user1/zip-action/main.js`.

- 3 (Optioneel) Voeg alle afhankelijkheden voor uw Node.js-script toe aan de map.

- a Maak een `package.json`-bestand met afhankelijkheden in uw scriptmap. Zie [Creating a package.json file](#) en [Specifying dependencies and devDependencies in a package.json file](#).
- b Open een opdrachtregelshell.
- c Navigeer naar de map die u hebt gemaakt voor het actiescript en de afhankelijkheden.

```
cd /home/user1/zip-action
```

- d Installeer uw `package.json`-bestand in de scriptmap door de volgende opdracht uit te voeren:

```
npm install --production
```

Opmerking Met deze opdracht maakt u een `node_modules`-directory in uw map.

- 4 Selecteer in de toegewezen map uw scriptelementen en, indien van toepassing, uw `node_modules`-directory en comprimeer deze in een ZIP-pakket.

Opmerking Zowel uw script- als afhankelijkheidselementen moeten worden opgeslagen op het rootniveau van het ZIP-pakket. Wanneer u het ZIP-pakket in een Linux-omgeving maakt, kan er een probleem optreden waarbij de inhoud van het pakket niet op het rootniveau is opgeslagen. Als u dit probleem ondervindt, maakt u het pakket door de `zip -r`-opdracht uit te voeren in uw opdrachtregelshell.

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

Wat nu te doen

Gebruik het ZIP-pakket om een uitbreidbaarheidsactiescript te maken. Zie [Hoe maak ik uitbreidbaarheidsacties](#).

Een ZIP-pakket maken voor uitbreidbaarheidsacties van PowerShell-runtime

U kunt een ZIP-pakket maken dat uw PowerShell-script en -afhankelijkheidsmodules bevat voor gebruik in uitbreidbaarheidsacties.

Er zijn twee methoden om het script voor uw uitbreidbaarheidsacties te bouwen:

- Uw script rechtstreeks in de editor voor uitbreidbaarheidsacties in Cloud Assembly schrijven.
- Uw script in uw lokale omgeving maken en dit, met alle relevante afhankelijkheden, toevoegen aan een ZIP-pakket.

Door een ZIP-pakket te gebruiken, kunt u een aangepaste vooraf geconfigureerde sjabloon maken van actiescripts en afhankelijkheden die u kunt importeren in Cloud Assembly voor gebruik in uitbreidbaarheidsacties.

Opmerking U hoeft geen PowerCLI-cmdlets als afhankelijkheden te definiëren of ze in een ZIP-pakket te bundelen. PowerCLI-cmdlets zijn vooraf geconfigureerd met de PowerShell-runtime van uw Cloud Assembly-service.

Daarnaast kunt u een ZIP-pakket gebruiken in scenario's waarin modules die zijn gekoppeld aan afhankelijkheden in uw actiescript niet kunnen worden omgezet door de Cloud Assembly-service, bijvoorbeeld wanneer uw omgeving geen internettoegang heeft.

U kunt ook een ZIP-pakket gebruiken om uitbreidbaarheidsacties te maken die meerdere PowerShell-scriptbestanden bevatten. Het gebruik van meerdere scriptbestanden kan nuttig zijn voor het organiseren van de structuur van uw uitbreidbaarheidsactiecode.

Voorwaarden

Controleer of u bekend bent met PowerShell en PowerCLI. U kunt een Docker-image vinden met PowerShell Core, PowerCLI 10, PowerNSX en verschillende communitymodules en scriptvoorbeelden op [Docker Hub](#).

Procedure

- 1 Maak een map voor uw actiescript en afhankelijkheden op uw lokale machine.

Bijvoorbeeld: `/home/user1/zip-action`.

- 2 Voeg uw hoofd-PowerShell-script met de extensie `.psm1` toe aan de map.

Het volgende script biedt een eenvoudige PowerShell-functie met de naam `Main.psm1`:

```
function handler($context, $payload) {
    Write-Host "Hello " $payload.target
```

```
return $payload
```

Opmerking De uitvoer van een PowerShell-uitbreidbaarheidsactie is gebaseerd op de laatste variabele die wordt weergegeven in de hoofdtekst van de functie. Alle andere variabelen in de ingesloten functie worden verwijderd.

- 3 (Optioneel) Voeg een proxyconfiguratie toe aan uw hoofd-PowerShell-script met behulp van `context`-parameters. Zie [Contextparameters gebruiken om een proxyconfiguratie in uw PowerShell-script toe te voegen](#).
- 4 (Optioneel) Voeg eventuele afhankelijkheden voor uw PowerShell-script toe.

Opmerking Uw PowerShell-afhankelijkheidsscript moet de extensie `.psm1` gebruiken. Gebruik dezelfde naam voor het script en de submap waarin het script is opgeslagen.

- a Meld u aan bij een Linux PowerShell-shell.

Opmerking De runtime van actiegebaseerde uitbreidbaarheid in Cloud Assembly is Linux-gebaseerd. PowerShell-afhankelijkheden die in een Windows-omgeving zijn gecompileerd, kunnen het gegenereerde ZIP-pakket onbruikbaar maken. Alle geïnstalleerde afhankelijkheden van derden moeten compatibel zijn met het VMware Photon OS omdat PowerShell-scripts worden uitgevoerd op Photon OS.

- b Ga naar de map `/home/user1/zip-action`.
- c Download en sla de PowerShell-module met uw afhankelijkheden op door de `Save-Module`-cmdlet uit te voeren.

```
Save-Module -Name <module name> -Path ./
```

- d Herhaal de vorige substap voor alle aanvullende afhankelijkheidsmodules.

Belangrijk Controleer of elke afhankelijkheidsmodule zich in een afzonderlijke submap bevindt. Zie [How to Write a PowerShell Script Module](#) voor meer informatie over het schrijven en beheren van PowerShell-modules.

- 5 Selecteer in de toegewezen map uw scriptelementen en, indien van toepassing, de submappen van de afhankelijkheidsmodule en comprimeer deze in een ZIP-pakket.

Opmerking De submappen voor zowel uw script- als afhankelijkheidsmodule moeten worden opgeslagen op het rootniveau van het ZIP-pakket. Wanneer u het ZIP-pakket in een Linux-omgeving maakt, kan er een probleem optreden waarbij de inhoud van het pakket niet op het rootniveau is opgeslagen. Als u dit probleem ondervindt, maakt u het pakket door de `zip -r`-opdracht uit te voeren in uw opdrachtregelshell.

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

Wat nu te doen

Gebruik het ZIP-pakket om een uitbreidbaarheidsactiescript te maken. Zie [Hoe maak ik uitbreidbaarheidsacties](#).

Contextparameters gebruiken om een proxyconfiguratie in uw PowerShell-script toe te voegen. U kunt de communicatie van de netwerkproxy inschakelen in uw PowerShell-script met behulp van `context-parameters`.

Bepaalde PowerShell-cmdlets vereisen mogelijk dat u een netwerkproxy instelt als een omgevingsvariabele in uw PowerShell-functie. Proxyconfiguraties worden doorgegeven aan de PowerShell-functie met de `$context.proxy.host`- en `$context.proxy.port`-parameters.

U kunt deze `context-parameters` toevoegen aan het begin van uw PowerShell-script.

```
$proxyString = "http://" + $context.proxy.host + ":" + $context.proxy.port
$Env:HTTP_PROXY = $proxyString
$Env:HTTPS_PROXY = $proxyString
```

Als de cmdlets de `-Proxy`-parameter ondersteunen, kunt u de proxywaarde ook rechtstreeks doorgeven aan de specifieke PowerShell-cmdlets.

Cloudspecifieke uitbreidbaarheidsacties configureren

U kunt uitbreidbaarheidsacties configureren die met uw cloudaccounts werken.

Wanneer u een uitbreidbaarheidsactie maakt, kunt u deze configureren en koppelen aan diverse cloudgebaseerde accounts:

- Microsoft Azure
- Amazon Web Services

Voorwaarden

Een geldig cloudaccount is vereist.

Procedure

- 1 Selecteer **Uitbreidbaarheid > Bibliotheek > Actie**.

- 2 Klik op **Nieuwe Actie**.
- 3 Voer indien nodig de actieparameters in.
- 4 Selecteer uw cloudaccountprovider in het vervolgkeuzemenu **FaaS-provider** of selecteer **Automatisch selecteren**.

Opmerking Als u **Automatisch** selecteert, definieert de actie de FaaS-provider automatisch.

- 5 Klik op **Opslaan**.

Resultaten

Uw uitbreidbaarheidsactie is nu gekoppeld voor gebruik met het geconfigureerde cloudaccount.

Uitbreidbaarheidsacties op locatie configureren

U kunt uw uitbreidbaarheidsacties configureren om een FaaS-provider op locatie te gebruiken in plaats van een Amazon Web Services- of Microsoft Azure-cloudaccount.

Door gebruik te maken van een FaaS-provider op locatie voor uw uitbreidbaarheidsacties, kunt u services op locatie zoals LDAP-, CMDB- of vCenter-datacenters gebruiken in uw Cloud Assembly-uitbreidbaarheidsabonnementen.

Procedure

- 1 Selecteer **Uitbreidbaarheid > Bibliotheek > Acties**.
- 2 Klik op **Nieuwe Actie**.
- 3 Voer een naam en een project in voor de uitbreidbaarheidsactie.
- 4 (Optioneel) Voer een beschrijving in voor de uitbreidbaarheidsactie.
- 5 Klik op **Volgende**.
- 6 Maak of importeer uw uitbreidbaarheidsactiescript.
- 7 Klik op het vervolgkeuzemenu **FaaS-provider** en selecteer **Op locatie**.
- 8 Als u de nieuwe uitbreidbaarheidsactie wilt opslaan, klikt u op **Opslaan**.

Wat nu te doen

Gebruik de gemaakte uitbreidbaarheidsactie in uw Cloud Assembly-uitbreidbaarheidsabonnementen.

Hoe kan ik geheimen maken voor gebruik in uitbreidbaarheidsacties

U kunt versleutelde invoer toevoegen aan uw uitbreidbaarheidsactie met behulp van geheimen op projectniveau.

Met geheimen kunt u versleutelde invoerwaarden aan uw uitbreidbaarheidsacties toevoegen. Versleuteling is handig voor gebruikssituaties waarin uw invoer wordt gebruikt om gevoelige gegevens, zoals wachtwoorden en certificaten, te beheren. Geheimen zijn beschikbaar voor alle FaaS-providers en -runtimes.

Opmerking U kunt ook versleutelde invoerwaarden toevoegen door actieconstanten te gebruiken. Zie [Hoe kan ik constanten voor de uitbreidbaarheidsactie maken](#).

Toegang tot geheimen is afhankelijk van het project waarin ze zijn gemaakt. Zo zijn geheimen die in project A zijn gemaakt, bijvoorbeeld alleen toegankelijk voor gebruikers die deel uitmaken van project A.

Geheimen gebruiken de functie `context.getSecret()` om de geheime waarde te ontsleutelen wanneer deze aan uw script wordt toegevoegd. Deze functie gebruikt de naam van het geheim als parameter. U kunt bijvoorbeeld een geheim met de naam `abxsecret` gebruiken als versleutelde invoerparameter in uw actie. Als u deze invoerparameter wilt toevoegen aan uw actiescript, moet u een `context.getSecret(inputs["abxsecret"])` gebruiken.

Procedure

1 Maak een nieuw geheim.

- a Ga naar **Infrastructuur > Beheer > Geheimen**.
- b Selecteer **Nieuw geheim**.
- c Voer de naam in van het project waaraan het geheim is toegewezen.

Opmerking De uitbreidbaarheidsactie waaraan u het geheim wilt toewijzen, moet deel uitmaken van hetzelfde project als het geheim.

- d Voer een naam in voor uw geheim.
- e Voer de waarde in die u aan het geheim wilt toewijzen.
- f (Optioneel) Voer een beschrijving in.
- g Klik op **Maken**.

2 Voeg uw geheim toe aan een uitbreidbaarheidsactie.

- a Selecteer een bestaande uitbreidbaarheidsactie of maak een nieuwe uitbreidbaarheidsactie.
- b Schakel het selectievakje **Geheim** in onder **Standaardinvoer**.
- c Zoek naar uw geheim en voeg het toe aan de invoer voor de uitbreidbaarheidsactie.
- d Voeg het geheim toe aan het script voor de uitbreidbaarheidsactie met behulp van de functie `context.getSecret()`.
- e Als u uw geheim wilt testen, klikt u op **Testen**.

Hoe kan ik constanten voor de uitbreidbaarheidsactie maken

U kunt constanten maken en opslaan voor gebruik in uitbreidbaarheidsacties.

Met constanten voor uitbreidbaarheidsacties kunt u versleutelde invoerwaarden aan uw uitbreidbaarheidsacties toevoegen. Versleuteling is handig voor gebruikssituaties waarin uw invoer wordt gebruikt om gevoelige gegevens, zoals wachtwoorden en certificaten, te beheren. Constanten zijn beschikbaar voor alle FaaS-providers en -runtimes.

Opmerking In tegenstelling tot geheimen kunnen constanten voor uitbreidbaarheidsacties alleen worden gebruikt voor uitbreidbaarheidsgeheimen. Zie [Hoe kan ik geheimen maken voor gebruik in uitbreidbaarheidsacties](#) voor meer informatie over geheimen.

Constanten voor uitbreidbaarheidsacties zijn toegankelijk voor alle gebruikers in uw organisatie.

Constanten gebruiken de functie `context.getSecret()` om te worden uitgevoerd als onderdeel van uw script. Deze functie gebruikt de naam van de constante als parameter. U kunt bijvoorbeeld een constante voor een uitbreidbaarheidsactie met de naam `abxconstant` gebruiken als versleutelde invoerparameter in uw actie. Als u deze invoerparameter wilt toevoegen aan uw actiescript, moet u een `context.getSecret(inputs["abxconstant"])` gebruiken.

Procedure

- 1 Maak een constante voor een uitbreidbaarheidsactie.
 - a Navigeer naar **Uitbreidbaarheid > Bibliotheek > Acties**.
 - b Selecteer **Actieconstanten**.
 - c Als u een constante wilt maken, klikt u op **Nieuwe actieconstante**.
 - d Voer een naam en waarde voor de constante in en klik op **Opslaan**.
- 2 Voeg uw constante toe aan een uitbreidbaarheidsactie.
 - a Selecteer een bestaande uitbreidbaarheidsactie of maak een nieuwe uitbreidbaarheidsactie.
 - b Schakel het selectievakje **Geheim** in onder **Standaardinvoer**.
 - c Zoek naar uw constante en voeg deze toe aan de invoer voor de uitbreidbaarheidsactie.
 - d Voeg de constante toe aan het script voor de uitbreidbaarheidsactie met behulp van de functie `context.getSecret()`.
 - e Als u de constante voor de uitbreidbaarheidsactie wilt testen, klikt u op **Testen**.

Gedeelde uitbreidbaarheidsacties maken

Als Cloud Assembly-beheerder kunt u uitbreidbaarheidsacties maken die kunnen worden gedeeld tussen projecten zonder dat de actie wordt geëxporteerd en geïmporteerd.

Zie [Uitbreidbaarheidsacties exporteren en importeren](#) voor informatie over het exporteren en importeren van uitbreidbaarheidsacties.

Voorwaarden

Maak twee of meer projecten in uw Cloud Assembly-organisatie.

Procedure

- 1 Selecteer **Uitbreidbaarheid > Bibliotheek > Acties**.
- 2 Klik op **Nieuwe Actie**.
- 3 Voer een naam in voor uw uitbreidbaarheidsactie.
- 4 (Optioneel) Voer een beschrijving voor uw uitbreidbaarheidsactie in.
- 5 Selecteer een project waarin uw uitbreidbaarheidsactie wordt gemaakt.
- 6 Tik op het **Delen met alle projecten in deze organisatie**-selectievakje.
- 7 Klik op **Volgende**.
- 8 Maak of importeer uw actiescript en sla uw uitbreidbaarheidsactie op.

Opmerking U kunt het delen bij **Instellingen** in- of uitschakelen. Als de uitbreidbaarheidsactie wordt gebruikt voor abonnementen kunt u delen niet uitschakelen. Om delen uit te schakelen, moet u de uitbreidbaarheidsactie uit uw abonnementen verwijderen.

- 9 Maak een uitbreidbaarheidsabonnement, voeg de actie voor gedeelde uitbreidbaarheid toe en stel het abonnementsbereik in op **Alle projecten**.

Opmerking Zie [Een uitbreidbaarheidsabonnement maken](#) voor meer informatie over het maken van uitbreidbaarheidsabonnementen.

Het uitbreidbaarheidsabonnement wordt geactiveerd door overeenkomende gebeurtenissen in een van uw projecten.

Wat nu te doen

U kunt ook gedeelde uitbreidbaarheidsacties importeren als een contentbron in de Service Broker-catalogus. Wanneer u het bronproject selecteert, voert u het project in waarin de uitbreidbaarheidsactie is gemaakt. Zie [Uitbreidbaarheidsacties toevoegen aan de Service Broker-catalogus](#) voor meer informatie over het toevoegen van uitbreidbaarheidsacties aan Service Broker.

Azure-logboekregistratie voor Python-gebaseerde uitbreidbaarheidsacties

U kunt nu Microsoft Azure 3.x-logboekregistratiefuncties in uw uitbreidbaarheidsactiescript gebruiken.

Uitbreidbaarheidsacties in Cloud Assembly maken nu gebruik van de Microsoft Azure 3.x Scripting API, die de vorige 1.x-versie vervangt. De Microsoft Azure 3.x Scripting API is gebaseerd op Linux en wordt uitgevoerd in een containeromgeving.

Vanwege deze versiewijziging werken logboekregistratiefuncties die worden ingevoegd in het script van uitbreidbaarheidsacties waarvoor Microsoft Azure als FaaS-provider (Function as a Service) wordt gebruikt, op een andere manier. In de volgende twee scriptvoorbeelden laten we de verschillende logboekregistratiefuncties zien die in de twee API-versies worden gebruikt.

Microsoft Azure 1.x-scriptvoorbeeld.

```
def handler(context, inputs):
    greeting = "Hello, {0}!".format(inputs["target"])
    print(greeting)

    outputs = {
        "greeting": greeting
    }

    return outputs
```

Microsoft Azure 3.x-scriptvoorbeeld.

```
import logging

def handler(context, inputs):
    greeting = "Hello, {0}!".format(inputs["target"])
    logging.info(greeting)

    outputs = {
        "greeting": greeting
    }

    return outputs
```

In het voorgaande voorbeeld ziet u dat de 3.x-versie de functie `import logging` aan het begin van het script toevoegt terwijl de functie `print()` wordt vervangen door de functie `logging.info()`. Als u logboekregistratie wilt blijven gebruiken met uitbreidbaarheidsacties die zijn gemaakt in de Microsoft Azure 1.x API, moet u de logboekregistratiefuncties in uw script wijzigen zodat het overeenkomt met het Microsoft Azure 3.x-voorbeeld.

Zie de [Python-ontwikkelaarshandleiding voor Azure Functions](#) voor meer informatie over logboekregistratie.

Uitbreidbaarheidsacties exporteren en importeren

Met Cloud Assembly kunt u uitbreidbaarheidsacties exporteren en importeren voor gebruik in verschillende projecten.

Voorwaarden

Een bestaande uitbreidbaarheidsactie.

Procedure

- 1 Exporteer een uitbreidbaarheidsactie.
 - a Navigeer naar **Uitbreidbaarheid > Bibliotheek > Acties**.
 - b Selecteer een uitbreidbaarheidsactie en klik op **Exporteren**.
 Het actiescript en de bijbehorende afhankelijkheden worden in uw lokale omgeving opgeslagen als ZIP-bestand.
- 2 Importeer een uitbreidbaarheidsactie.
 - a Navigeer naar **Uitbreidbaarheid > Bibliotheek > Acties**.
 - b Klik op **Importeren**.
 - c Selecteer de geëxporteerde uitbreidbaarheidsactie en wijs deze toe aan een project.
 - d Klik op **Importeren**.

Opmerking Als de geïmporteerde uitbreidbaarheidsactie al aan het opgegeven project is toegewezen, wordt u gevraagd een conflictoplossingsbeleid te selecteren.

Wat is een actiestroom

Actiestromen zijn een set uitbreidbaarheidsactiescripts die worden gebruikt om levenscyclussen en automatisering verder uit te breiden.

Alle actiestromen beginnen met `flow_start` en eindigen op `flow_end`. U kunt verschillende uitbreidbaarheidsactiescripts aan elkaar koppelen door de volgende actiestroomelementen te gebruiken:

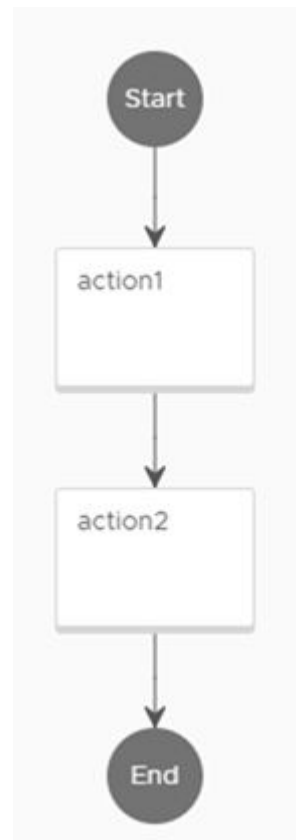
- **Sequentiële actiestromen** - Meerdere uitbreidbaarheidsactiescripts die sequentieel worden uitgevoerd.
- **Vertakkingsactiestromen** - Meerdere uitbreidbaarheidsactiescripts of -stromen die paden splitsen om bij te dragen aan dezelfde uitvoer.
- **Samenvoegingsactiestromen** - Meerdere uitbreidbaarheidsactiescripts of -stromen die worden samengevoegd en bijdragen aan dezelfde uitvoer.
- **Voorwaardelijke actiestromen** - Meerdere uitbreidbaarheidsactiescripts of -stromen die worden uitgevoerd nadat aan een voorwaarde is voldaan.

Sequentiële actiestromen

Meerdere uitbreidbaarheidsactiescripts die opeenvolgend worden uitgevoerd.

```
version: "1"
flow:
  flow_start:
    next: action1
  action1:
    action: <action_name>
    next: action2
  action2:
    action: <action_name>
    next: flow_end
```

Opmerking U kunt teruggaan naar een vorige actie door deze toe te wijzen als de `next`: actie. In dit voorbeeld kunt u in plaats van `next: flow_end` bijvoorbeeld `next: action1` invoeren om actie 1 opnieuw uit te voeren en de reeks acties opnieuw te starten.



Vertakkingsactiestromen

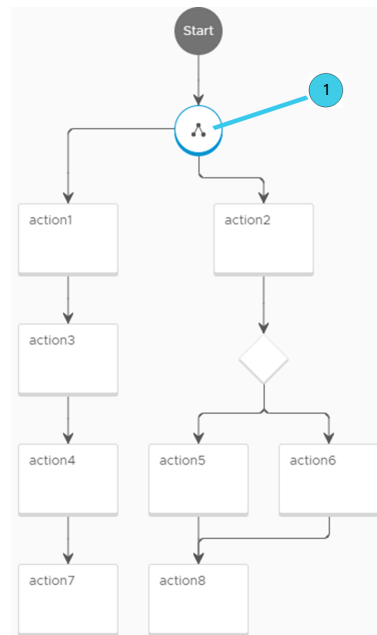
Meerdere uitbreidbaarheidsactiescripts of -stromen die paden splitsen om bij te dragen aan dezelfde uitvoer.

```

version: "1"
flow:
  flow_start:
    next: forkAction
  forkAction:
    fork:
      next: [action1, action2]
  action1:
    action: <action_name>
    next: action3
  action3:
    action: <action_name>
    next: action4
  action4:
    action: <action_name>
    next: action7
  action7:
    action: <action_name>
  action2:
    action: <action_name>

```

Opmerking U kunt teruggaan naar een vorige actie door deze toe te wijzen als de `next`: actie. In plaats van `next: flow_end` om uw actiestroom te beëindigen kunt u bijvoorbeeld `next: action1` invoeren om actie 1 opnieuw uit te voeren en de reeks acties opnieuw te starten.



1 Vertakkingselement

Samenvoegingsactiestromen

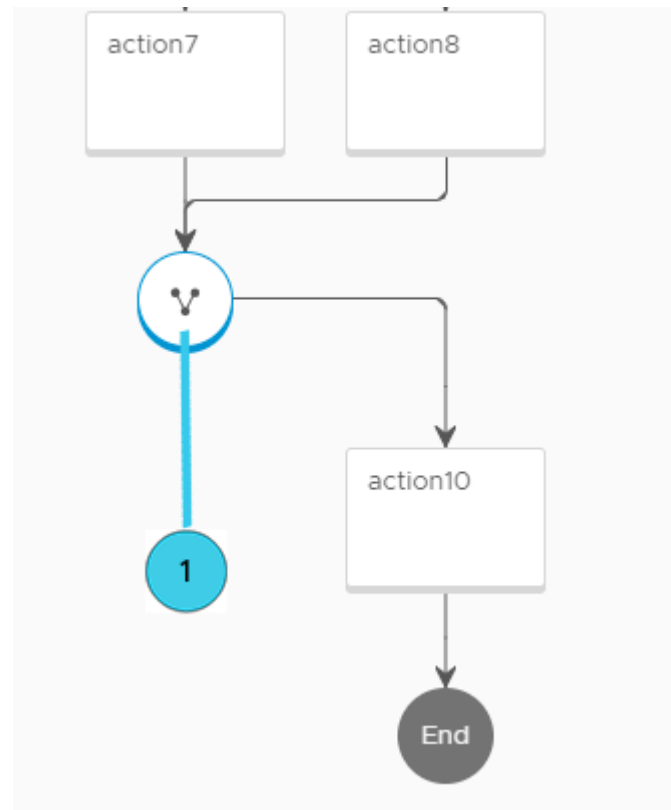
Meerdere uitbreidbaarheidsactiescripts of -stromen die paden samenvoegen en bijdragen aan dezelfde uitvoer.

```

version: "1"
action7:
  action: <action_name>
  next: joinElement
action8:
  action: <action_name>
  next: joinElement
joinElement:
  join:
    type: all
    next: action10
action10:
  action: <action_name>
  next: flow_end

```

Opmerking U kunt teruggaan naar een vorige actie door deze toe te wijzen als de `next`: actie. In dit voorbeeld kunt u in plaats van `next: flow_end` bijvoorbeeld `next: action1` invoeren om actie 1 opnieuw uit te voeren en de reeks acties opnieuw te starten.



1 Samenvoegingselement

Voorwaardelijke actiestromen

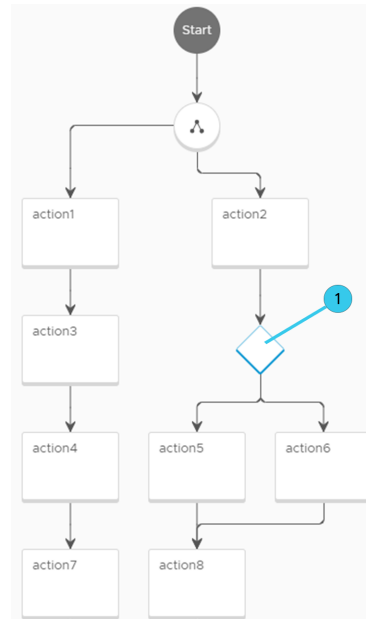
Meerdere uitbreidbaarheidsactiescripts of -stromen die worden uitgevoerd wanneer aan een voorwaarde is voldaan met een switch-element.

In sommige gevallen moet de voorwaarde gelijk zijn aan `true` om de actie uit te voeren. In andere gevallen, zoals in dit voorbeeld, moet aan parameterwaarden zijn voldaan voordat een actie kan worden uitgevoerd. Als aan geen van de voorwaarden is voldaan, mislukt de actiestroom.

```

version: 1
id: 1234
name: Test
inputs: ...
outputs: ...
flow:
  flow_start:
    next: forkAction
  forkAction:
    fork:
      next: [action1, action2]
  action1:
    action: <action_name>
    next: action3
  action3:
    action: <action_name>
    next: action4
  action4:
    action: <action_name>
    next: action7
  action7:
    action: <action_name>
    next: joinElement
  action2:
    action: <action_name>
    next: switchAction
  switchAction:
    switch:
      "${1 == 1}": action5
      "${1 != 1}": action6
  action5:
    action: <action_name>
    next: action8
  action6:
    action: <action_name>
    next: action8
  action8:
    action: <action_name>

```



1 Switch-element

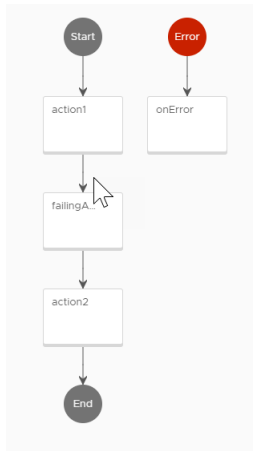
Opmerking U kunt teruggaan naar een vorige actie door deze toe te wijzen als de `next`: actie. In plaats van `next: flow_end` om uw actiestroom te beëindigen kunt u bijvoorbeeld `next: action1` invoeren om actie 1 opnieuw uit te voeren en de reeks acties opnieuw te starten.

Hoe gebruik ik een foutenhandler in actiestromen?

U kunt uw actiestroom zo configureren dat een fout wordt gemeld bij specifieke fasen van de stroom met behulp van een foutenhandler-element.

Voor een foutenhandler-element zijn twee soorten invoer nodig:

- Opgegeven foutbericht van de mislukte actie.
- Actiestroominvoer.



Als een actie in uw stroom mislukt en de actie een foutenhandler-element bevat, wordt een foutbericht afgegeven met de melding dat de actie is mislukt. De foutenhandler is een actie op zich. Het volgende script is een voorbeeld van een foutenhandler die kan worden gebruikt in een actiestroom.

```
def handler(context, inputs):

    errorMsg = inputs["errorMsg"]
    flowInputs = inputs["flowInputs"]

    print("Flow execution failed with error {0}".format(errorMsg))
    print("Flow inputs were: {0}".format(flowInputs))

    outputs = {
        "errorMsg": errorMsg,
        "flowInputs": flowInputs
    }

    return outputs
```

U kunt de geslaagde en mislukte uitvoeringen bekijken in het venster Actie-uitvoeringen.

Status	Run ID	Action
Completed	8a76996b6839fe3c01684...	error-handler
Failed	8a76996b6839fe3c01684...	failing-action
Completed	8a76996b6839fe3c01684...	simple-hello
Completed	8a76996b6839fe3c01684...	flow-with-handler

In dit voorbeeld is de actiestroom stroom-met-handler, die een foutenhandler-element bevat, met succes uitgevoerd. Een van de acties in de stroom is echter mislukt, waardoor de foutenhandler een fout heeft gemeld.

Hoe kan ik actie-uitvoeringen volgen

Op het tabblad Actie-uitvoeringen ziet u een logboek van geactiveerde uitbreidbaarheidsacties voor een abonnement en hun status.

U kunt het logboek met actie-uitvoeringen weergeven via **Uitbreidbaarheid > Activiteit > Actie-uitvoeringen**. U kunt de lijst met actie-uitvoeringen ook op een of meer eigenschappen tegelijk filteren.

Problemen met mislukte uitvoeringen van uitbreidbaarheidsacties oplossen

Als de uitvoering van uw uitbreidbaarheidsactie mislukt, kunt u probleemoplossingsstappen uitvoeren om deze te corrigeren.

Wanneer een actie-uitvoering mislukt, ontvangt u mogelijk een foutbericht, een mislukte status en een mislukt logboek. Als uw actie-uitvoering mislukt, is dit te wijten aan een implementatie- of codefout.

Probleem	Oplossing
Implementatie mislukt	Deze fouten zijn het gevolg van problemen met de configuratie van het cloudaccount, de actie-implementatie of andere afhankelijkheden die kunnen verhinderen dat de actie wordt geïmplementeerd. Zorg ervoor dat het door u gebruikte project is gedefinieerd in het geconfigureerde cloudaccount en rechten heeft om functies uit te voeren. Voordat u de actie opnieuw start, kunt u de actie testen met een specifiek project op de detailpagina voor de actie.
Codefout	Deze fouten zijn het gevolg van ongeldige scripts of code. Gebruik de logboeken met actie-uitvoeringen om problemen met de ongeldige scripts op te lossen en te corrigeren.

Abonnementen op uitbreidbaarheidswerkstromen

U kunt uw door vRealize Orchestrator gehoste werkstromen met Cloud Assembly gebruiken om de levenscyclus van applicaties uit te breiden.

Hoe kan ik eigenschappen van een virtuele machine wijzigen met behulp van een vRealize Orchestrator-werkstroomabonnement

U kunt een bestaande vRealize Orchestrator-werkstroom gebruiken om de eigenschappen van de virtuele machine te wijzigen en virtuele machines aan de Active Directory toe te voegen.

De parameters van het gebeurtenisonderwerp bepalen de indeling van de lading voor Event Broker Service-berichten (EBS). Om de lading van EBS-berichten in een werkstroom te ontvangen en te gebruiken, moet u de invoerparameters voor de `inputProperties`-werkstroominvoerparameters definiëren.

Voorwaarden

- Gebruikersrol cloudbbeheerder

- Bestaande vRealize Orchestrator-werkstromen op locatie.
- Succesvolle integratie en verbinding met de vRealize Orchestrator-clientserver.

Procedure

- 1 Selecteer **Uitbreidbaarheid > Abonnementen**.
- 2 Klik op **Nieuw abonnement**.
- 3 Maak een abonnement met de volgende parameters:

Parameter	Waarde
Naam	RenameVM
Gebeurtenisonderwerp	Selecteer een gebeurtenisonderwerp dat geschikt is voor de gewenste integratie van vRealize Orchestrator. Bijvoorbeeld: berekeningstoewijzing.
Blokkerend/niet-blokkerend	Niet-blokkerend
Actie/werkstroom	Selecteer een runnable-type van vRealize Orchestrator. Selecteer de gewenste werkstroom. Bijvoorbeeld: naam van virtuele machine instellen.

- 4 Klik op **Opslaan** om uw abonnement op te slaan.
- 5 Wijs uw abonnement toe en activeer het door een cloudsjabloon te maken of een bestaande cloudsjabloon te implementeren.

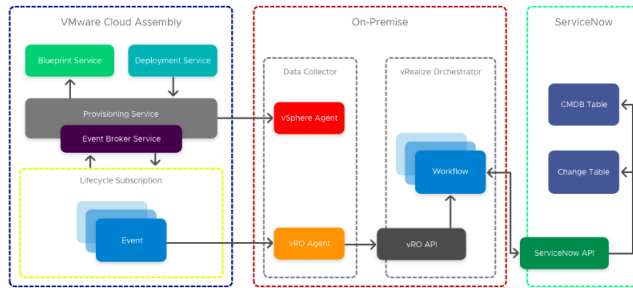
Wat nu te doen

Controleer met een van de volgende methoden of de werkstroom correct is gestart:

- Controleer het logboek met werkstroomuitvoeringen via **Uitbreidbaarheid > Activiteit > Werkstroomuitvoeringen**.
- Open de vRealize Orchestrator-client en controleer de werkstroomstatus door naar de werkstroom te navigeren en de status te bekijken of door het tabblad voor specifieke logboeken te openen.

Hoe integreer ik Cloud Assembly voor ITSM met ServiceNow met behulp van vRealize Orchestrator-werkstromen

Door vRealize Orchestrator gehoste werkstromen stellen u in staat om Cloud Assembly met ServiceNow te integreren voor ITSM-compliance.



Zakelijke gebruikers integreren voor compliance doorgaans hun cloudbeheerplatform met een IT Service Management- (ITSM) en Configuration Management Database-platform (CMDB). Overeenkomstig dit voorbeeld kunt u Cloud Assembly met ServiceNow voor CMDB en ITSM integreren met door vRealize Orchestrator gehoste werkstromen. Wanneer u met vRealize Orchestrator-integraties en -werkstromen werkt, zijn capaciteitstags vooral handig als u meerdere instanties voor verschillende omgevingen hebt. Zie [Capaciteitstags in Cloud Assembly gebruiken](#) voor meer informatie over capaciteitstags.

Opmerking U kunt ServiceNow ook met Cloud Assembly integreren met behulp van uitbreidbaarheidsactiescripts. Zie [Hoe integreer ik Cloud Assembly met ServiceNow met behulp van uitbreidbaarheidsacties](#) voor informatie over het integreren van ServiceNow met behulp van uitbreidbaarheidsactiescripts.

In dit voorbeeld is de ServiceNow-integratie samengesteld uit drie werkstromen op het hoogste niveau. Elke werkstroom heeft eigen abonnementen, zodat u elk onderdeel afzonderlijk kunt bijwerken en herhalen.

- Toegangspunt van gebeurtenisabonnement - Basislogboekregistratie identificeert de aanvrager en vCenter VM, indien van toepassing.
- Integratiewerkstroom - Scheidt objecten en levert invoer voor de technische werkstroom, zorgt voor updates van de logboekregistratie, eigenschappen en uitvoer.
- Technische werkstroom - Voer systeemintegratie voor ServiceNow API verderop in het proces uit om de CMDB CI, CR en Cloud Assembly IaaS API te maken met aanvullende eigenschappen voor de virtuele machine buiten de lading.

Voorwaarden

- Een standalone of geclusterde vRealize Orchestrator-omgeving.
- Een vRealize Orchestrator-integratie in Cloud Assembly. Zie [vRealize Orchestrator-integratie in Cloud Assembly configureren](#) voor informatie over het integreren van een standalone vRealize Orchestrator met Cloud Assembly.

Procedure

- 1 Maak een configuratiebestand dat een algemene configuratie bevat die in meerdere werkstromen wordt gebruikt, en sla het in vRealize Orchestrator op.

- 2 Sla uw Cloud Assembly API-token op dezelfde locatie op als het configuratiebestand uit stap 1.

Opmerking Het Cloud Assembly API-token heeft een vervaldatum.

- 3 Maak een werkstroom in vRealize Orchestrator met het opgegeven scriptelement. Dit script verwijst naar een REST-host en zoekt ernaar. Ook worden er REST-acties gestandaardiseerd die gebruikmaken van een optionele parameter van een token, dat als extra autorisatiekoptekst is toegevoegd.

```
var configPath = "CS"
var configName = "environmentConfig"
var attributeName = "CASRestHost"

//get REST Host from configuration element
var restHost =
System.getModule("au.com.cs.example").getRestHostFromConfig(configPath,configName,attribute
Name)

var ConfigurationElement =
System.getModule("au.com.cs.example").getConfigurationElementByName(configName,configPath);
System.debug("ConfigurationElement:" + ConfigurationElement);
var casToken = ConfigurationElement.getAttributeWithKey("CASToken")["value"]
if(!casToken){
    throw "no CAS Token";
}
//REST Template
var opName = "casLogin";
var opTemplate = "/iaas/login";
var opMethod = "POST";

// create the REST operation:
var opLogin =
System.getModule("au.com.cs.example").createOp(restHost,opName,opMethod,opTemplate);

//cas API Token
var contentObject = {"refreshToken":casToken}
postContent = JSON.stringify(contentObject);

var loginResponse =
System.getModule("au.com.cs.example").executeOp(opLogin,null,postContent,null) ;

try{
    var tokenResponse = JSON.parse(loginResponse)['token']
    System.debug("token: " + tokenResponse);
} catch (ex) {
    throw ex + " No valid token";
}

//REST Template Machine Details
var opName = "machineDetails";
var opTemplate = "/iaas/machines/" + resourceId;
var opMethod = "GET";

var bearer = "Bearer " + tokenResponse;
```

```

var opMachine =
System.getModule("au.com.cs.example").createOp(restHost,opName,opMethod,opTemplate);

// (Rest Operation, Params, Content, Auth Token)
var vmResponse =
System.getModule("au.com.cs.example").executeOp(opMachine,null,"",bearer) ;

try{
    var vm = JSON.parse(vmResponse);
} catch (ex) {
    throw ex + " failed to parse vm details"
}

System.log("cpuCount: " + vm["customProperties"]["cpuCount"]);
System.log("memoryInMB: " + vm["customProperties"]["memoryInMB"]);

cpuCount = vm["customProperties"]["cpuCount"];
memoryMB = vm["customProperties"]["memoryInMB"];

```

Dit script verzendt de uitvoer `cpuCount` en `memoryMB` naar de bovenliggende werkstroom en werkt de bestaande `customProperties`-eigenschappen bij. Deze waarden kunnen worden gebruikt in volgende werkstromen wanneer de CMDB wordt gemaakt.

- 4 Voeg het ServiceNow CMDB-scriptelement 'CI maken' toe aan uw werkstroom. Dit element zoekt de ServiceNow REST-host met behulp van het configuratie-item, maakt een REST-bewerking voor de tabel `cmdb_ci_vmware_instance`, maakt een tekenreeks met een inhoudsobject gebaseerd op de werkstroominvoer voor post-gegevens en voert de uitvoer van de geretourneerde `sys_id` uit.

```

var configPath = "CS"
var configName = "environmentConfig"
var attributeName = "serviceNowRestHost"
var tableName = "cmdb_ci_vmware_instance"

//get REST Host from configuration element
var restHost =
System.getModule("au.com.cs.example").getRestHostFromConfig(configPath,configName,attributeName)

//REST Template
var opName = "serviceNowCreatCI";
var opTemplate = "/api/now/table/" + tableName;
var opMethod = "POST";

// create the REST operation:
var opCI =
System.getModule("au.com.cs.example").createOp(restHost,opName,opMethod,opTemplate);

//cmdb_ci_vm_vmware table content to post;
var contentObject = {};
contentObject["name"] = hostname;

```

```

contentObject["cpus"] = cpuTotalCount;
contentObject["memory"] = MemoryInMB;
contentObject["correlation_id"] = deploymentId
contentObject["disks_size"] = diskProvisionGB
contentObject["location"] = "Sydney";
contentObject["vcenter_uuid"] = vcUuid;
contentObject["state"] = "On";
contentObject["owned_by"] = owner;

postContent = JSON.stringify(contentObject);
System.log("JSON: " + postContent);

// (Rest Operation, Params, Content, Auth Token)
var ciResponse =
System.getModule("au.com.cs.example").executeOp(opCI, null, postContent, null) ;

try{
    var cmdbCI = JSON.parse(ciResponse);
} catch (ex) {
    throw ex + " failed to parse ServiceNow CMDB response";
}

serviceNowSysId = cmdbCI['result']['sys_id'];

```

- 5 Maak met behulp van de uitvoer van de onderliggende werkstroom een eigenschappenobject met behulp van de bestaande `customProperties` en vervang de eigenschap `serviceNowSysId` door de waarde van ServiceNow. Deze unieke id wordt in de CMDB gebruikt om een instantie als buiten gebruik gesteld te markeren bij vernietiging.

Resultaten

Cloud Assembly is geïntegreerd met ITSM ServiceNow. Zie [Extending Cloud Assembly with vRealize Orchestrator for ServiceNow Integration](#) voor meer informatie over hoe u werkstromen kunt gebruiken om ServiceNow in Cloud Assembly te integreren.

Meer informatie over werkstroomabonnementen

Door gebruik te maken van een vRealize Orchestrator-integratie met Cloud Assembly, kunt u de levenscyclus van applicaties uitbreiden met werkstromen.

vRealize Automation omvat een ingesloten vRealize Orchestrator-implementatie. U kunt de werkstroombibliotheek van de ingesloten vRealize Orchestrator-implementatie in uw abonnementen gebruiken. U kunt werkstromen maken, wijzigen en verwijderen met de vRealize Orchestrator-client.

U kunt ook een externe vRealize Orchestrator-implementatie in Cloud Assembly integreren. Zie [vRealize Orchestrator-integratie in Cloud Assembly configureren](#).

Beste praktijken voor het maken van vRealize Orchestrator-werkstromen

Een werkstroomabonnement is gebaseerd op een specifiek gebeurtenisonderwerp en de gebeurtenisparameters van dat onderwerp. Om ervoor te zorgen dat de abonnementen de

vRealize Orchestrator-werkstromen in gang kunnen zetten, moet u de juiste invoerparameters opgeven zodat de gebeurtenisgegevens goed worden verwerkt.

Invoerparameters voor werkstroom

Uw aangepaste werkstroom kan alle parameters of een afzonderlijke parameter bevatten die alle gegevens in de datalading gebruikt.

Als u een afzonderlijke parameter wilt gebruiken, configureert u één parameter van het type `Properties` en met de naam `inputProperties`.

Uitvoerparameters voor werkstroom

Uw aangepaste werkstroom kan relevante uitvoerparameters voor de volgende gebeurtenissen bevatten in het kader van een beantwoordbaar gebeurtenisonderwerp.

Wanneer een gebeurtenisonderwerp een antwoord verwacht, moeten de uitvoerparameters van de werkstroom overeenkomen met de parameters van het antwoordschema.

Hoe volg ik werkstroomuitvoeringen

Het venster **Werkstroomuitvoeringen** toont de logboeken van de geactiveerde werkstromen van het abonnement en hun status.

U kunt de logboeken van uw werkstroomuitvoeringen bekijken door te navigeren naar

Uitbreidbaarheid > Activiteit > Werkstroomuitvoeringen.

Problemen met mislukte werkstroomabonnementen oplossen

Als uw werkstroomabonnement mislukt, kunt u probleemoplossingsstappen uitvoeren om dit te corrigeren.

Mislukte werkstroomuitvoeringen kunnen ervoor zorgen dat uw werkstroomabonnement niet wordt gestart of voltooid. De mislukking van de werkstroomuitvoering kan het gevolg zijn van verschillende veelvoorkomende problemen.

Probleem	Oorzaak	Oplossing
Uw vRealize Orchestrator-werkstroomabonnement is niet gestart of voltooid.	U hebt een werkstroomabonnement geconfigureerd waarmee na ontvangst van het gebeurtenisbericht een aangepaste werkstroom moet worden uitgevoerd. De werkstroom wordt echter niet uitgevoerd.	<ol style="list-style-type: none"> 1 Controleer of het werkstroomabonnement correct is opgeslagen. 2 Controleer of de voorwaarden voor het werkstroomabonnement correct zijn geconfigureerd. 3 Controleer of vRealize Orchestrator de opgegeven werkstroom bevat. 4 Controleer of de werkstroom in vRealize Orchestrator correct is geconfigureerd.
Uw vRealize Orchestrator-werkstroomabonnement voor de goedkeuringsaanvraag is niet uitgevoerd.	U hebt een werkstroomabonnement voor goedkeuring vooraf of achteraf geconfigureerd om een vRealize Orchestrator-werkstroom uit te voeren. De werkstroom wordt niet uitgevoerd wanneer een machine die voldoet aan de ingestelde criteria, in de servicecatalogus wordt aangevraagd.	<p>Om een werkstroomabonnement voor goedkeuring uit te voeren, moet u controleren of alle onderdelen correct zijn geconfigureerd.</p> <ol style="list-style-type: none"> 1 Controleer of het goedkeuringsbeleid actief is en correct is toegepast. 2 Controleer of het werkstroomabonnement correct is geconfigureerd en opgeslagen. 3 Controleer de gebeurtenislogboeken op berichten over goedkeuringen.
Uw vRealize Orchestrator-werkstroomabonnement voor de goedkeuringsaanvraag is geweigerd.	U hebt een werkstroomabonnement voor goedkeuring vooraf of achteraf geconfigureerd dat een opgegeven vRealize Orchestrator-werkstroom uitvoert, maar de aanvraag is geweigerd op het externe goedkeuringsniveau. Een mogelijke oorzaak is een foute interne werkstroomuitvoering in vRealize Orchestrator. Mogelijk ontbreekt de werkstroom of wordt de vRealize Orchestrator-server niet uitgevoerd.	<ol style="list-style-type: none"> 1 Controleer de logboeken op berichten over goedkeuringen. 2 Controleer of de vRealize Orchestrator-server wordt uitgevoerd. 3 Controleer of vRealize Orchestrator de opgegeven werkstroom bevat.

Meer informatie over uitbreidbaarheidsabonnementen

U kunt de levenscyclus van applicaties uitbreiden door uitbreidbaarheidsacties of door vRealize Orchestrator gehoste werkstromen met uitbreidbaarheidsabonnementen te gebruiken.

Wanneer een activeringsgebeurtenis in uw omgeving plaatsvindt, wordt het abonnement geïnitieerd en wordt de opgegeven werkstroom- of uitbreidbaarheidsactie uitgevoerd. U kunt systeemgebeurtenissen in het gebeurtenislogboek weergeven, werkstroomuitvoeringen in het venster Werkstroomuitvoeringen en actie-uitvoeringen in het venster Actie-uitvoeringen. Abonnementen zijn specifiek voor een project, wat betekent dat deze via het opgegeven project aan de cloudsjablonen en implementaties zijn gekoppeld.

Uitbreidbaarheidsterminologie

Wanneer u met uitbreidbaarheidsabonnementen in Cloud Assembly werkt, kunt u terminologie tegenkomen die specifiek is voor de abonnementen en gebeurtenisbrokerservice.

Tabel 6-6. Uitbreidbaarheidsterminologie

Term	Beschrijving
Gebeurtenisonderwerp	<p>Geeft een beschrijving van een verzameling gebeurtenissen met dezelfde logische opzet en dezelfde structuur. Elke gebeurtenis is een instantie van een gebeurtenisonderwerp.</p> <p>U kunt blokkerende parameters aan bepaalde gebeurtenisonderwerpen toewijzen. Zie Gebeurtenisonderwerpen blokkeren voor meer informatie.</p>
Gebeurtenis	Duidt op een wijziging van de status van de producer of andere entiteiten die erdoor worden beheerd. De gebeurtenis is de entiteit die informatie over het optreden ervan registreert.
Gebeurtenisbrokerservice	De service die ervoor zorgt dat de berichten die een producer publiceert, worden doorgestuurd naar de abonnees.
Lading	De gebeurtenisgegevens die alle relevante eigenschappen voor dat gebeurtenisonderwerp bevatten.
Abonnement	<p>Geeft aan dat een abonnee op de hoogte wil worden gehouden over een gebeurtenis. Dit gebeurt door een abonnement te nemen op een gebeurtenisonderwerp en de criteria te definiëren die de melding activeren.</p> <p>Abonnementen koppelen uitbreidbaarheidsacties of -werkstromen aan activeringsgebeurtenissen die worden gebruikt om delen van de levenscyclus van applicaties te automatiseren.</p>
Abonnee	De gebruiker die meldingen ontvangt voor gebeurtenissen die conform het ingestelde abonnement naar de gebeurtenisbrokerservice worden gepubliceerd. De abonnee kan ook een consument worden genoemd.
Systeembeheerder	Een gebruiker met rechten om werkstroomabonnementen op tenant- en systeemniveau te maken, te lezen, bij te werken en te verwijderen met behulp van Cloud Assembly.

Tabel 6-6. Uitbreidbaarheidsterminologie (vervolg)

Term	Beschrijving
Werkstroomabonnement	Geeft aan voor welk gebeurtenisonderwerp en onder welke voorwaarden een vRealize Orchestrator-werkstroom wordt geactiveerd.
Actieabonnement	Geeft aan voor welk gebeurtenisonderwerp en onder welke voorwaarden een uitbreidbaarheidsactie wordt geactiveerd.
Werkstroom	Een vRealize Orchestrator-werkstroom die in Cloud Assembly is geïntegreerd. U kunt deze werkstromen aan gebeurtenissen in abonnementen koppelen.
Uitbreidbaarheidsactie	Een gestroomlijnd script met code dat kan worden uitgevoerd nadat een gebeurtenis in een abonnement is geactiveerd. Uitbreidbaarheidsacties lijken op werkstromen, maar zijn lichter. Uitbreidbaarheidsacties kunnen vanuit Cloud Assembly worden aangepast.
Actie-uitvoeringen	Toegankelijk via het tabblad Actie-uitvoeringen . Een actie-uitvoering is een gedetailleerd logboek met uitbreidbaarheidsacties die zijn uitgevoerd als reactie op activeringsgebeurtenissen.

Gebeurtenisonderwerpen blokkeren

Bepaalde gebeurtenisonderwerpen ondersteunen blokkeringsgebeurtenissen. Het gedrag van een uitbreidbaarheidsabonnement wordt bepaald door de ondersteuning die het onderwerp voor deze gebeurtenistypen biedt en uw configuratie van het abonnement.

Cloud Assembly-uitbreidbaarheidsabonnementen kunnen twee grote typen gebeurtenisonderwerpen gebruiken: niet-blokkerende en blokkerende gebeurtenisonderwerpen. Het type gebeurtenisonderwerp definieert het gedrag van het uitbreidbaarheidsabonnement.

Niet-blokkerende gebeurtenisonderwerpen

Met niet-blokkerende gebeurtenisonderwerpen kunt u alleen niet-blokkerende abonnementen maken. Niet-blokkerende abonnementen worden asynchroon geactiveerd en u kunt niet vertrouwen op de volgorde waarin de abonnementen worden geactiveerd.

Gebeurtenisonderwerpen blokkeren

Bepaalde gebeurtenisonderwerpen ondersteunen blokkering. Als een abonnement is gemarkeerd als 'blokkeren', worden alle berichten die voldoen aan de ingestelde voorwaarden niet ontvangen door andere abonnementen met overeenkomende voorwaarden totdat het runnable-item van het blokkerende abonnement wordt uitgevoerd.

Blokkerende abonnementen worden op volgorde van prioriteit uitgevoerd. De waarde 0 (nul) heeft de hoogste prioriteit. Als u voor hetzelfde gebeurtenisonderwerp meer dan één blokkerend abonnement hebt met hetzelfde prioriteitsniveau, worden de abonnementen op basis van de naam van het abonnement in omgekeerde alfabetische volgorde uitgevoerd. Wanneer alle

blokkerende abonnementen zijn verwerkt, wordt het bericht gelijktijdig verstuurd naar alle niet-blokkerende abonnementen. Door de synchrone uitvoering van blokkerende abonnementen wordt de lading van de gebeurtenis steeds aangepast, zodat de bijgewerkte gebeurtenis wordt doorgestuurd naar de volgende abonnementen.

Met behulp van blokkerende gebeurtenisonderwerpen kunt u meerdere abonnementen beheren die afhankelijk zijn van elkaar.

U kunt bijvoorbeeld abonnementen hebben voor twee inrichtingswerkstromen, waarbij het tweede abonnement afhankelijk is van de resultaten van het eerste abonnement. Met het eerste abonnement wordt een eigenschap tijdens de inrichting gewijzigd, terwijl het tweede abonnement de nieuwe eigenschap, zoals een machinenaam, in een bestandssysteem registreert. Het abonnement `ChangeProperty` krijgt prioriteit 0 terwijl `RecordProperty` prioriteit 1 krijgt omdat het tweede abonnement de resultaten van het eerste abonnement gebruikt. Het abonnement `ChangeProperty` wordt uitgevoerd wanneer een machine wordt ingericht. Omdat de voorwaarden van het abonnement `RecordProperty` zijn gebaseerd op een voorwaarde na inrichting, wordt het abonnement `RecordProperty` geactiveerd door een gebeurtenis. Maar omdat de werkstroom `ChangeProperty` blokkerend is, wordt deze gebeurtenis pas ontvangen wanneer deze werkstroom is voltooid. Wanneer de machinenaam is gewijzigd en het eerste werkstroomabonnement gereed is, wordt het tweede werkstroomabonnement uitgevoerd om de machinenaam in het bestandssysteem te registreren.

Runnable-item voor herstel

Voor het blokkeren van gebeurtenisonderwerpen kunt u een runnable-item voor herstel toevoegen aan het abonnement. Het runnable-item voor herstel in een abonnement wordt uitgevoerd als het primaire runnable-item mislukt. U kunt bijvoorbeeld een werkstroomabonnement maken waarbij het primaire runnable-item een werkstroom is die records maakt in een CMDB-systeem zoals ServiceNow. Zelfs als het werkstroomabonnement mislukt, kunnen bepaalde records worden gemaakt in het CMDB-systeem. In dit scenario kan een runnable-item voor herstel worden gebruikt om de records op te schonen die door het mislukte runnable-item in het CMDB-systeem zijn achtergelaten.

Voor gebruikssituaties waarin meerdere abonnementen zijn opgenomen die afhankelijk zijn van elkaar, kunt u een eigenschap `ebs.recover.continuation` toevoegen aan het runnable-item voor herstel. Met deze eigenschap kunt u bepalen of de uitbreidbaarheidsservice moet doorgaan met het volgende abonnement in uw keten als het huidige abonnement mislukt.

De gebeurtenisonderwerpen van Cloud Assembly

Cloud Assembly bevat vooraf gedefinieerde gebeurtenisonderwerpen.

Gebeurtenisonderwerpen

Gebeurtenisonderwerpen zijn categorieën die soortgelijke gebeurtenissen groeperen. Wanneer gebeurtenisonderwerpen aan een abonnement zijn toegewezen, bepalen deze welke gebeurtenis het abonnement activeert. De volgende gebeurtenisonderwerpen worden standaard met Cloud Assembly geleverd. Alle onderwerpen kunnen worden gebruikt om aangepaste eigenschappen of codes van de resource toe te voegen of bij te werken. Als een vRealize Orchestrator-werkstroom of uitbreidbaarheidsactie mislukt, mislukt ook de overeenkomende taak.

Tabel 6-7. Gebeurtenisonderwerpen voor Cloud Assembly

Gebeurtenisonderwerp	Blokkeerbaar	Beschrijving
Cloud template configuration	Nee	Uitgegeven wanneer een cloudsjabloonconfiguratiegebeurtenis, zoals het maken of verwijderen van een cloudsjabloon, plaatsvindt. Dit gebeurtenisonderwerp kan nuttig zijn voor het melden van dergelijke gebeurtenissen aan externe systemen.
Cloud template version configuration	Nee	Uitgegeven wanneer een nieuwe versiegebeurtenis voor een cloudsjabloon plaatsvindt, zoals het maken, vrijgeven, opheffen van de vrijgave of herstellen van een versie. Dit gebeurtenisonderwerp kan nuttig zijn voor integraties met versiecontrolesystemen van derden.
Compute allocation	Ja	Uitgegeven vóór de toewijzing van <code>resourceNames</code> en <code>hostSelections</code> . Beide eigenschappen kunnen tijdens deze fase worden gewijzigd. Eenmaal uitgegeven voor een cluster van machines.
Compute gateway post provisioning	Ja	Uitgegeven nadat een <code>computergatewayresource</code> is ingericht.
Compute gateway post removal	Ja	Uitgegeven nadat een <code>computergateway</code> is verwijderd.
Compute gateway provisioning	Ja	Uitgegeven voordat een <code>computergateway</code> is ingericht.
Compute gateway removal	Ja	Uitgegeven voordat een <code>computergateway</code> is verwijderd.

Tabel 6-7. Gebeurtenisonderwerpen voor Cloud Assembly (vervolg)

Gebeurtenisonderwerp	Blokkeerbaar	Beschrijving
Compute initial power on	Ja	<p>Uitgegeven nadat een resource is ingericht op de hypervisorlaag, maar voordat de resource voor de eerste keer wordt ingeschakeld. Momenteel wordt dit gebeurtenisonderwerp alleen ondersteund voor vSphere. Gebeurtenissen worden voor elke machine in een cluster verzonden.</p> <p>Opmerking U kunt de eerste inschakeling voor de resource overslaan.</p>
Compute nat post provisioning	Ja	Uitgegeven nadat een computer-NAT-resource is ingericht.
Compute nat post removal	Ja	Uitgegeven nadat een computer-NAT-resource is verwijderd.
Compute nat provisioning	Ja	Uitgegeven voordat een computer-NAT is ingericht.
Compute nat removal	Ja	Uitgegeven voordat een computer-NAT is verwijderd.
Compute post provision	Ja	Uitgegeven nadat een resource is ingericht. Gebeurtenissen worden voor elke machine in een cluster verzonden.
Compute post removal	Ja	Uitgegeven nadat een computerbron is verwijderd. Gebeurtenissen worden voor elke machine in een cluster verzonden.
Compute provision	Ja	<p>Uitgegeven voordat de resource wordt ingericht op de hypervisorlaag. Gebeurtenissen worden voor elke machine in een cluster verzonden.</p> <p>Opmerking U kunt het toegewezen IP-adres wijzigen.</p>
Compute removal	Ja	Uitgegeven voordat de resource wordt verwijderd. Gebeurtenissen worden voor elke machine in een cluster verzonden.
Compute reservation	Ja	<p>Uitgegeven op het moment van de reservering. Eenmaal uitgegeven voor een cluster van machines.</p> <p>Opmerking U kunt de volgorde van plaatsingen wijzigen.</p>

Tabel 6-7. Gebeurtenisonderwerpen voor Cloud Assembly (vervolg)

Gebeurtenisonderwerp	Blokkeerbaar	Beschrijving
Custom resource post provision	Ja	Uitgegeven voor gebeurtenissen na inrichting die worden geactiveerd door aangepaste resourcebewerkingen.
Custom resource pre provision	Ja	Uitgegeven voor gebeurtenissen vóór inrichting die worden geactiveerd door aangepaste resourcebewerkingen.
Deployment action completed	Ja	Uitgegeven na het voltooiën van een implementatieactie.
Deployment action requested	Ja	Uitgegeven voordat een implementatieactie is voltooid.
Deployment completed	Ja	Uitgegeven na de implementatie van een cloudsjabloon- of catalogusaanvraag.
Deployment onboarded	Nee	Uitgegeven wanneer het onboarden van een nieuwe implementatie is voltooid.
Deployment requested	Ja	Uitgegeven vóór de implementatie van een cloudsjabloon- of catalogusaanvraag.
Deployment resource action completed	Ja	Uitgegeven na de implementatie van een resourceactie.
Deployment resource action requested	Ja	Uitgegeven vóór de implementatie van een resourceactie.
Deployment resource completed	Ja	Uitgegeven na de inrichting van een implementatieresource.
Deployment resource requested	Ja	Uitgegeven vóór de inrichting van een implementatieresource.
Disk allocation	Ja	Uitgegeven vóór de voorafgaande toewijzing van schijfresources.

Tabel 6-7. Gebeurtenisonderwerpen voor Cloud Assembly (vervolg)

Gebeurtenisonderwerp	Blokkeerbaar	Beschrijving
Disk attach	Ja	<p>Uitgegeven voordat een schijf aan een machine is gekoppeld. <code>Disk attach</code> is een gebeurtenis voor lezen en schrijven. Schijfeigenschappen die worden ondersteund voor write-back zijn:</p> <ul style="list-style-type: none"> ■ <code>diskFullPaths</code> ■ <code>diskDatastoreNames</code> ■ <code>diskParentDirs</code> <p>De drie vSphere-specifieke schijfeigenschappen zijn allemaal vereist voor updates. Alle andere eigenschappen zijn alleen-lezen.</p> <p>Opmerking Write-back is optioneel voor vSphere-eersteklasschijven.</p>
Disk detach	Ja	Uitgegeven nadat een schijf van een machine is ontkoppeld. <code>Disk detach</code> is een alleen-lezen-gebeurtenis.
Disk post removal	Ja	Uitgegeven nadat een schijfresource is verwijderd.
Disk post resize	Ja	Uitgegeven nadat de grootte van de schijfresource is gewijzigd.
Kubernetes cluster allocation	Ja	Uitgegeven vóór de toewijzing vooraf van resources voor een Kubernetes-cluster.
Kubernetes cluster post provision	Ja	Uitgegeven nadat een Kubernetes-cluster is ingericht.
Kubernetes cluster post removal	Ja	Uitgegeven nadat een Kubernetes-cluster is verwijderd.
Kubernetes cluster provision	Ja	Uitgegeven voordat een Kubernetes-cluster is ingericht.
Kubernetes cluster removal	Ja	Uitgegeven voordat het proces voor het verwijderen van een Kubernetes-cluster is gestart.
Kubernetes namespace allocation	Ja	Uitgegeven tijdens de toewijzing vooraf voor Kubernetes-naamruimteresources.
Kubernetes namespace post provision	Ja	Uitgegeven nadat een Kubernetes-naamruimterresource is ingericht.
Kubernetes namespace post removal	Ja	Uitgegeven nadat een Kubernetes-naamruimterresource is verwijderd.
Kubernetes namespace provision	Ja	Uitgegeven voordat een Kubernetes-naamruimte is ingericht.

Tabel 6-7. Gebeurtenisonderwerpen voor Cloud Assembly (vervolg)

Gebeurtenisonderwerp	Blokkeerbaar	Beschrijving
Kubernetes namespace removal	Ja	Uitgegeven voordat een naamruimteclusterresource is verwijderd.
Kubernetes supervisor namespace allocation	Ja	Uitgegeven tijdens de toewijzing vooraf voor Kubernetes-supervisor-naamruimteresources.
Kubernetes supervisor namespace post provision	Ja	Uitgegeven nadat een supervisor-naamruimte is ingericht.
Kubernetes supervisor namespace post removal	Ja	Uitgegeven nadat een supervisor-naamruimterresource is verwijderd.
Kubernetes supervisor namespace provision	Ja	Uitgegeven voordat een supervisor-naamruimte is ingericht.
Kubernetes supervisor namespace removal	Ja	Uitgegeven voordat een supervisor-naamruimterresource is verwijderd.
Load balancer post provision	Ja	Uitgegeven na het inrichten van een load balancer.
Load balancer post removal	Ja	Uitgegeven na het verwijderen van een load balancer.
Load balancer provision	Ja	Uitgegeven vóór het inrichten van een load balancer.
Load balancer removal	Ja	Uitgegeven vóór het verwijderen van een load balancer.
Network Configure	Ja	Uitgegeven wanneer het netwerk wordt geconfigureerd tijdens de berekeningstoewijzing. Opmerking Het onderwerp Netwerk configureren ondersteunt meerdere IP-adressen/NIC's.
Network post provisioning	Ja	Uitgegeven nadat een netwerkresource is ingericht.
Network post removal	Ja	Uitgegeven nadat een netwerkresource is verwijderd.
Network provisioning	Ja	Uitgegeven voordat een netwerkresource is ingericht.
Network removal	Ja	Uitgegeven voordat een netwerkresource is verwijderd.
Project Lifecycle Event Topic	Nee	Uitgegeven wanneer een project wordt gemaakt, bijgewerkt of verwijderd.

Tabel 6-7. Gebeurtenisonderwerpen voor Cloud Assembly (vervolg)

Gebeurtenisonderwerp	Blokkeerbaar	Beschrijving
Provisioning request	Ja	Uitgegeven voordat een beveiligingsgroep is verwijderd.
Security group post provision	Ja	Uitgegeven nadat een beveiligingsgroep is ingericht.
Security group post removal	Ja	Uitgegeven nadat een beveiligingsgroep is verwijderd.
Security group provisioning	Ja	Uitgegeven voordat een beveiligingsgroep is ingericht.
Security group removal	Ja	Uitgegeven voordat een beveiligingsgroep is verwijderd.

Gebeurtenisparameters

Nadat u een gebeurtenisonderwerp hebt toegevoegd, kunt u de parameters van dat gebeurtenisonderwerp weergeven. Deze gebeurtenisparameters bepalen de structuur van de lading van de gebeurtenis of `inputProperties`. Bepaalde gebeurtenisparameters kunnen niet worden gewijzigd en worden als alleen-lezen gemarkeerd. U kunt deze alleen-lezen-parameters identificeren door op het informatiepictogram rechts naast de parameter te klikken.

Logboek met uitbreidbaarheidsgebeurtenissen

Op de pagina Uitbreidbaarheidsgebeurtenissen wordt een lijst weergegeven met alle gebeurtenissen die in uw omgeving hebben plaatsgevonden.

U kunt het logboek met uitbreidbaarheidsgebeurtenissen bekijken door te navigeren naar **Uitbreidbaarheid > Gebeurtenissen**. U kunt de lijst met gebeurtenissen ook op een of meer eigenschappen filteren. Als u meer informatie over een afzonderlijke gebeurtenis wilt bekijken, selecteert u de id van de gebeurtenis.

ID	Timestamp	Event Topic	User Name	Target ID	Description
cba156ce-a324-f5ae-5dd1-66d1e591f1a6	04/28/20, 1:10 PM	N/A	N/A	endpoints	CREATE
e1621151-2906-dce2-44ab-68c17132d756	03/25/20, 4:22 PM	N/A	N/A	endpoints	CREATE
468a8955-cf27-e77e-0179-fb5b736717b3	03/25/20, 10:12 AM	N/A	N/A	endpoints	CREATE
d9482883-d1ae-5899-fb06-852c202cc178	03/20/20, 2:41 PM	N/A	N/A	endpoints	CREATE
38584d40-e663-6311-7098-3747aa528d12	01/30/20, 5:35 PM	N/A	N/A	endpoints	CREATE

Een uitbreidbaarheidsabonnement maken

Door een vRealize Orchestrator-integratie, of uitbreidbaarheidsacties met Cloud Assembly, te gebruiken, kunt u abonnementen maken om uw applicaties uit te breiden.

Met behulp van uitbreidbaarheidsabonnementen kunt u uw applicaties uitbreiden door werkstromen of acties te activeren bij specifieke levenscyclusgebeurtenissen. U kunt ook filters toepassen op uw abonnementen om booleaanse voorwaarden in te stellen voor de opgegeven gebeurtenis. De gebeurtenis en werkstroom of actie worden bijvoorbeeld alleen geactiveerd als de booleaanse expressie 'true' is. Dit is handig voor scenario's waarbij u wilt bepalen wanneer gebeurtenissen, acties of werkstromen worden geactiveerd.

Voorwaarden

- Controleer of u de gebruikersrol van cloudbeheerder hebt.
- Als u vRealize Orchestrator-werkstromen gebruikt:
 - De bibliotheek van de ingesloten vRealize Orchestrator-client of de bibliotheek van een geïntegreerde externe vRealize Orchestrator-instantie.
- Als u uitbreidbaarheidsacties gebruikt:
 - Bestaande uitbreidbaarheidsactiescripts. Zie [Hoe maak ik uitbreidbaarheidsacties](#) voor meer informatie.

Procedure

- 1 Selecteer **Uitbreidbaarheid > Abonnementen**.
- 2 Klik op **Nieuw abonnement**.
- 3 Voer de details van uw abonnement in.
- 4 Stel het **organisatiebereik** van het abonnement in.

Opmerking Zie [Uitbreidbaarheidsabonnementen voor providers of tenants maken](#) voor meer informatie over het maken van uitbreidbaarheidsabonnementen voor de providers en tenants van de organisatie.

- 5 Selecteer een **gebeurtenisonderwerp**.
- 6 (Optioneel) Stel voorwaarden in voor het gebeurtenisonderwerp.

Opmerking Voorwaarden kunnen worden gemaakt met behulp van een expressie in JavaScript-syntaxis. Deze expressie kan booleaanse operatoren bevatten, zoals "&&" (AND), "||" (OR), "^" (XOR) en "!" (NOT). U kunt ook rekenkundige operatoren gebruiken, zoals "==" (equal to), "!=" (not equal to), ">=" (greater than or equal), "<=" (less than or equal), ">" (greater than) en "<" (lesser than). Meer complexe booleaanse expressies kunnen worden samengesteld uit eenvoudige expressies. Als u de lading van de gebeurtenis wilt openen volgens de opgegeven onderwerpparameters, gebruikt u 'event.data' of een van de kopteksteigenschappen van de gebeurtenis: sourceType, sourceIdentity, timeStamp, eventType, eventTopicId, correlationType, correlationId, description, targetType, targetId, userName en orgId.

- 7 Selecteer onder **Actie/werkstroom** een activeerbaar item voor uw uitbreidbaarheidsabonnement.

- 8 (Optioneel) Configureer zo nodig het blokkeergedrag voor het gebeurtenisonderwerp.
- 9 (Optioneel) Om het projectbereik van het uitbreidbaarheidsabonnement te definiëren, schakelt u **Een project** uit en klikt u op **Projecten toevoegen**.

Opmerking Als het organisatiebereik van het abonnement is ingesteld op **Een tenantorganisatie**, wordt het projectbereik altijd ingesteld op **Een project** en kan het projectbereik niet worden gewijzigd. U kunt het projectbereik alleen wijzigen als het organisatiebereik is ingesteld op de providerorganisatie.

- 10 Klik op **Opslaan** om uw abonnement op te slaan.

Resultaten

Uw abonnement is gemaakt. Wanneer een gebeurtenis plaatsvindt die is gecategoriseerd door het geselecteerde gebeurtenisonderwerp, wordt de gekoppelde werkstroom of uitbreidbaarheidsactie van vRealize Orchestrator gestart en worden alle abonnees hiervan op de hoogte gesteld.

Wat nu te doen

Nadat u uw abonnement hebt gemaakt, kunt u een cloudsjabloon maken of implementeren om het abonnement te koppelen en te gebruiken. U kunt ook de status van de uitvoering van de werkstroom of uitbreidbaarheidsactie controleren op het tabblad **Uitbreidbaarheid** in Cloud Assembly. Voor abonnementen met vRealize Orchestrator-werkstromen kunt u de uitvoering en werkstroomstatus ook controleren vanuit de vRealize Orchestrator-client.

Uitbreidbaarheidsabonnementen gebruiken om de vervaldatum van de implementatie te beheren

U kunt verlopen implementaties en bijbehorende resources beheren met behulp van de `Expire`-actie naast bestaande gebeurtenisonderwerpen.

Nadat een implementatielease in uw omgeving is verlopen, kunt u uitbreidbaarheidsgebeurtenisonderwerpen gebruiken om taken uit te voeren, zoals het stoppen van het maken van back-ups of het bewaken van implementatieresources. Om deze bewerkingen voor dag 2 uit te voeren, gebruikt de vRealize Automation-API een `Expire`-actie op systeemniveau. Deze actie wordt automatisch door het systeem geactiveerd wanneer een implementatielease in uw organisatie eindigt. De trigger voor de `Expire`-actie gaat vooraf aan de uitschakelgebeurtenis voor resources die zijn gekoppeld aan die implementatie.

Opmerking In eerdere productreleases werd de uitschakelgebeurtenis geactiveerd op implementatieniveau na het einde van de lease. Nu wordt de uitschakelgebeurtenis geactiveerd op resourceniveau voor elke implementatieresource die de ingeschakelde status heeft.

De `Expire`-actie is opgenomen in de lading van bestaande gebeurtenisonderwerpen, zoals **Implementatieactie aangevraagd** en **Implementatieactie voltooid** en gebruikt de parameter `deploymentid` om taken vóór en na het verlopen uit te voeren die zijn gekoppeld aan de implementatieresources.

Opmerking De actie `Expire` wordt ongeveer 10 tot 15 minuten na het einde van de lease van uw implementatie geactiveerd. Het systeem activeert geen lease-eindegebeurtenissen voorafgaand aan het werkelijke einde van de lease. De actie `Expire` is een actie op systeemniveau en gebruikers kunnen de bijbehorende gebeurtenissen niet handmatig activeren.

Voor het huidige scenario gebruikt u het gebeurtenisonderwerp **Implementatieactie aangevraagd** samen met de actie `Expire` om een back-up van een virtuele machine in uw implementatie als sjabloon te maken. In dit geval wordt de back-up uitgevoerd met behulp van een vRealize Orchestrator-werkstroom, maar dezelfde taak kan ook worden uitgevoerd door een uitbreidbaarheidsactie te gebruiken als het runnable-item van het abonnement.

Procedure

- 1 Ga naar **Uitbreidbaarheid > Abonnementen** en klik op **Nieuw abonnement**.
- 2 Voer een naam in voor het abonnement.
- 3 Controleer onder **Status** of het abonnement is ingeschakeld.
- 4 Selecteer onder **Gebeurtenisonderwerp** het gebeurtenisonderwerp **Implementatieactie aangevraagd**.
- 5 Schakel de optie **Voorwaarde** in en voeg een filter toe voor de vervalactie:

```
event.data.actionName == 'Expire'
```

Opmerking Het gebeurtenisonderwerp **Implementatieactie aangevraagd** kan worden geactiveerd door verschillende bewerkingen voor dag 2 van de implementatie, zoals het wijzigen van de leaseduur van de implementatie. Door het actiefilter voor het einde van de lease toe te voegen, zorgt u ervoor dat het abonnement alleen wordt geactiveerd voor eindegebeurtenissen.

- 6 Voeg onder **Actie/werkstroom** de vRealize Orchestrator-werkstroom toe.

Het schema van deze voorbeeldwerkstroom bevat een scriptbare taak en een werkstroomelement dat de werkstroom **Virtuele machine klonen, geen aanpassing** bevat die vooraf is geconfigureerd met vRealize Orchestrator. Het element Scriptbare taak bevat het volgende voorbeeldscript:

```
System.log("Lease expiry action triggered to clone a VM...")

System.log("Deployment Id is: " + inputProperties.deploymentId);
inputHeaders = new Properties();
deploymentId = inputProperties.deploymentId;
pathUriVariable = "/deployment/api/deployments/" + deploymentId + "/resources";
```

```

var restClient = vRAHost.createRestClient();
var request = restClient.createRequest("GET", pathUriVariable, null);
var keys = inputHeaders.keys;
for(var key in keys){
    request.setHeader(keys[key], inputHeaders.get(keys[key]));
}
var response = restClient.execute(request);
System.log("Content as string: " + response.contentAsString);
var content = response.contentAsString;
var obj = JSON.parse(content);

var object = new Properties(obj);
var contentJson = object.content;
for (var i = 0; i < contentJson.length; i++) {
    var resources = contentJson[i];

    var resourceProperties = resources.properties;
    System.log("Resource name is: " + resourceProperties.resourceName);
    resourceName = resourceProperties.resourceName;
}

var query = "xpath:name='" + resourceName + "'";
var vms=Server.findAllForType("VC:VirtualMachine", query);
vcVM=vms[0];

System.log("VM input is: " + vcVM);
dataStoreOutput = datastore
template= true;
name="test-vm-name"

```

- 7 Bepaal of het abonnement als blokkerend of niet-blokkerend moet worden ingesteld.

Opmerking Door het abonnement blokkerend te maken, wordt de uitschakelgebeurtenis voor de implementatieresources alleen geactiveerd nadat het runnable-item, in dit geval de werkstroom voor het einde van de lease, is voltooid. Als u het abonnement niet-blokkerend maakt, wordt de uitschakelgebeurtenis geactiveerd voor de implementatieresources, ongeacht de status van de uitvoering van de werkstroom.

- 8 Klik op **Opslaan** om het bewerken van het abonnement te voltooien.

Wat nu te doen

Nadat het uitbreidbaarheidsabonnement is geactiveerd door de lease-eindegebeurtenis en de uitvoering van de werkstroom is gelukt, gaat u naar de vSphere Web Client en valideert u of uw virtuele machine is geconverteerd naar een sjabloon.

Problemen met een uitbreidbaarheidsabonnement oplossen

Los problemen met mislukte uitbreidbaarheidsabonnementen op.

Wanneer uw abonnement mislukt, is dit doorgaans het gevolg van fouten met uw werkstroom of uitbreidbaarheidsactiescript.

Onderwerpparameters en lading weergeven

U kunt een script voor het dumpen van parameters van abonnementsonderwerpen gebruiken om de specifieke parameters en de lading van uw virtuele machine te bekijken in een gebeurtenisfase.

Dit script is voornamelijk handig voor het opsporen van fouten en het controleren van de beschikbare invoer voor uw vRealize Orchestrator-werkstroom. Als u alle parameters van uw virtuele machine wilt weergeven, gebruikt u het volgende script in uw werkstroom:

```
function dumpProperties(props, lvl) {
    var keys = props.keys;
    var prefix = ""
    for (var i=0; i<lvl; i++){
        prefix = prefix + "";
    }
    for (k in keys){
        var key = keys[k];
        var value = props.get(keys[k])
        if ("Properties" == System.getObjectType(value)){
            System.log(prefix + key + "[")
            dumpProperties(value, (lvl+2));
            System.log(prefix+ "]")
        } else{
            System.log( prefix + key + ":" + value)
        }
    }
}

dumpProperties(inputProperties, 0)

customProps = inputProperties.get("customProperties")
```

Geschiedenis van abonnementsversie

Als uw abonnement mislukt, kunt u de versiegeschiedenis bekijken.

Versiegeschiedenis van abonnement weergeven

Op het tabblad **Versiegeschiedenis** van de abonnementseditor kunt u de wijzigingsgeschiedenis van uw abonnement, inclusief de gebruiker en de datum van de wijziging, bekijken. U kunt ook verschillende abonnementsversies vergelijken door te klikken **Vergelijken met**. Als uw abonnement mislukt of onjuist wordt uitgevoerd, kan de versiegeschiedenis helpen bij het identificeren van de oorzaak.

Implementaties en resources in Cloud Assembly beheren

7

Als cloudbeheerder of cloudsjabloonontwikkelaar gebruikt u het tabblad Resources om uw resources te beheren. De resources kunnen de resources zijn die u heeft geïmplementeerd, maar ze kunnen ook de resources zijn die worden gedetecteerd voor uw cloudaccounts, gedetecteerde resources die u heeft geonboard of anderszins beschikbaar zijn voor beheer met Cloud Assembly

Dit hoofdstuk omvat de volgende onderwerpen:

- [Cloud Assembly-implementaties beheren](#)
- [Resources beheren in Cloud Assembly](#)

Cloud Assembly-implementaties beheren

Als Cloud Assembly-cloudbeheerder of -cloudsjabloonontwikkelaar gebruikt u de pagina Implementaties om uw implementaties en de gekoppelde resources te beheren. U kunt problemen met mislukte inrichtingsprocessen oplossen, wijzigingen aanbrengen in resources en ongebruikte implementaties vernietigen.

De implementaties omvatten geïmplementeerde cloudsjablonen en geonboarde resources. Ook kunnen resources die met de IaaS API zijn gemaakt, als implementaties worden weergegeven.

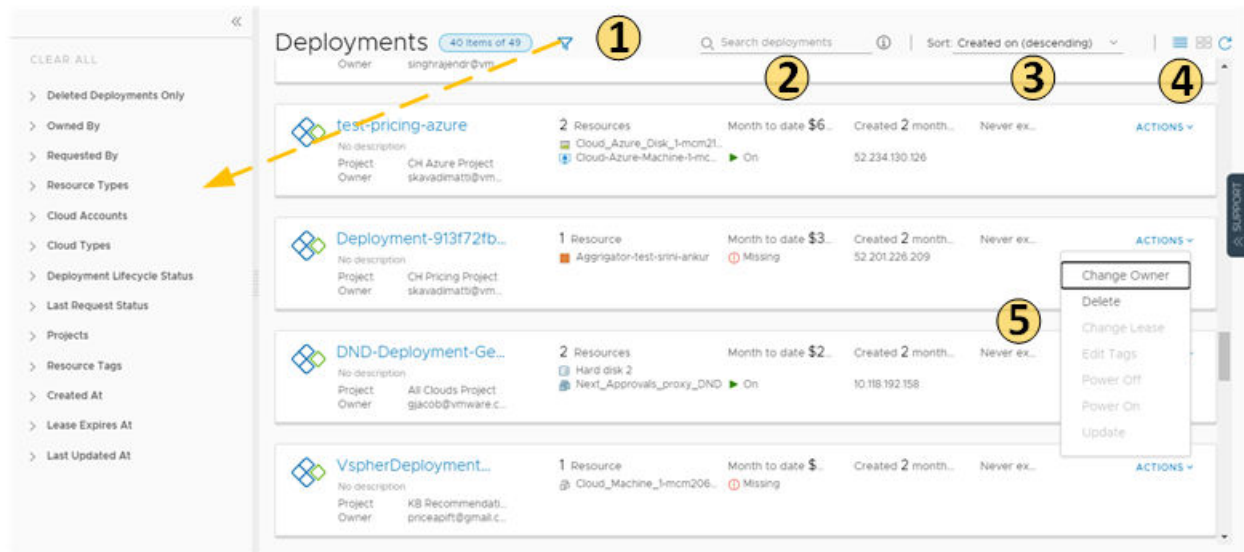
Als u een klein aantal implementaties beheert, bieden de implementatiekaarten een grafische weergave om ze te beheren. Als u een groot aantal implementaties beheert, bieden de implementatielijst en de resourcelijst een meer robuuste beheerweergave.

Als u uw implementaties wilt weergeven, selecteert u **Resources > Implementaties**.

Werken met implementatiekaarten en de implementatielijst

U kunt uw implementaties zoeken en beheren met de lijst met kaarten. U kunt specifieke implementaties filteren of zoeken en vervolgens acties op die implementaties uitvoeren.

Figuur 7-1. Kaartweergave van de pagina Implementaties



1 Filter uw aanvragen op basis van kenmerken.

U kunt bijvoorbeeld filteren op basis van eigenaar, projecten, vervaldatum van lease of andere filteropties. Of mogelijk wilt u alle implementaties vinden voor twee projecten met een specifieke tag. Wanneer u het filter bouwt voor de projecten en het voorbeeld van de tags, voldoen de resultaten aan de volgende criteria: (Project1 OF Project2) EN Tag1.

De waarden die u in het filtervenster ziet, zijn afhankelijk van de huidige implementaties waarvoor u weergave- en beheerrechten hebt.

De meeste filters en het gebruik ervan zijn relatief duidelijk. Hieronder vindt u meer informatie over sommige van deze filters.

2 Zoek naar implementaties op basis van trefwoorden of aanvrager.

3 Sorteert de lijst om deze op tijd of naam te rangschikken.

4 Schakel tussen de implementatiekaartweergave en de implementatielijstweergave.

5 Voer acties op implementatieniveau uit voor de implementatie, zoals het verwijderen van ongebruikte implementaties om resources opnieuw te claimen.

U kunt ook implementatiekosten, vervaldatum en status zien.

U kunt schakelen tussen de kaartweergave en de lijstweergave in de rechterbovenhoek van de pagina, rechts van het tekstvak Sorteren. U kunt de lijstweergave gebruiken om een groot aantal implementaties op minder pagina's te beheren.

Figuur 7-2. Lijstweergave van de pagina Implementaties

Deployments 40 items of 208 🔍 Search deployments ⓘ Sort: Created on (descending) ⌵ ☰ ⌂ ↻

	Actions	Address	Owner	Project	Status	Expires on	Price
▼	⚙ shared-ip-ranges-d...		bratanov@vmware.com	bratanov-ipa...		Never	
	⚙ nikola-ipam-test-0...	192.168.0.6			▶ On		
	⚙ net.90						
>	⚙ shared-ip-ranges-d...		bratanov@vmware.com	bratanov-ipa...		Never	
>	⚙ test-depl		bratanov@vmware.com	bratanov-ipa...	❗ Create — Failed	Never	
>	⚙ test2222		tdimitrova@vmware.com	vraikov		Never	
>	⚙ afd54234		vraikov@vmware.com	vraikov		Never	
>	⚙ 4erasd		vraikov@vmware.com	vraikov		Never	
>	⚙ grigor test 2412412		gganekov@vmware.com	vp-project		Never	

Werken met geselecteerde implementatiefilters

De volgende tabel is geen definitieve lijst met filteropties. De meeste zijn duidelijk. Voor sommige filters is echter iets meer kennis vereist.

Tabel 7-1. Geselecteerde filterinformatie

Filternaam	Beschrijving
Alleen optimaliseerbare resources	Als u vRealize Operations Manager hebt geïntegreerd en de integratie gebruikt om vrij te maken resources te identificeren, kunt u het filter inschakelen om de lijst met in aanmerking komende implementaties te beperken.
Levenscyclusstatus van implementatie	<p>De filters Levenscyclusstatus van implementatie en Laatste aanvraagstatus kunnen individueel of in combinatie worden gebruikt, in het bijzonder als u een groot aantal implementaties beheert. Voorbeelden vindt u aan het einde van het gedeelte Laatste aanvraagstatus hieronder.</p> <p>Levenscyclusstatus van implementatie filtert op de huidige status van de implementatie op basis van de beheerbewerkingen.</p> <p>Dit filter is niet beschikbaar voor verwijderde implementaties.</p> <p>Welke waarden u in het filtervenster ziet, is afhankelijk van de huidige status van de vermelde implementaties. Wellicht ziet u niet alle mogelijke waarden. De volgende lijst bevat alle mogelijke waarden. Acties voor dag 2 worden opgenomen in de updatestatus.</p> <ul style="list-style-type: none"> ■ Maken - Geslaagd ■ Maken - In behandeling ■ Maken - Mislukt ■ Bijwerken - Geslaagd ■ Bijwerken - In behandeling ■ Bijwerken - Mislukt ■ Verwijderen - In behandeling ■ Verwijderen - Mislukt
Filters Laatste aanvraagstatus	<p>De filters Laatste aanvraagstatus voor de laatste bewerking of actie die op de implementatie is uitgevoerd. Dit filter is niet beschikbaar voor verwijderde implementaties.</p> <p>De waarden die u in het filtervenster ziet, zijn afhankelijk van de laatste bewerkingen die op de vermelde implementaties zijn uitgevoerd. Wellicht ziet u niet alle mogelijke waarden. De volgende lijst bevat alle mogelijke waarden.</p> <ul style="list-style-type: none"> ■ In behandeling. De eerste fase van een aanvraag waarbij de actie is ingediend, maar het implementatieproces nog niet is gestart. ■ Mislukt. Er is een fout opgetreden bij de aanvraag tijdens een fase van het implementatieproces. ■ Geannuleerd. De aanvraag is geannuleerd door een gebruiker terwijl het implementatieproces bezig was en nog niet was voltooid. ■ Geslaagd. De aanvraag heeft een implementatie gemaakt, bijgewerkt of verwijderd.

Tabel 7-1. Geselecteerde filterinformatie (vervolg)

Filternaam	Beschrijving
	<ul style="list-style-type: none"> ■ In behandeling. Het implementatieproces wordt momenteel uitgevoerd. Aanvullende implementatiestatusen, zoals Initialisatie en Voltooiing die u op het tabblad Geschiedenis voor de implementatie ziet, worden niet als filters opgegeven, maar u kunt het filter In behandeling gebruiken om implementaties met deze statussen te vinden. ■ Goedkeuring in behandeling. Uw aanvraag heeft een of meer goedkeuringsbeleidsregels geactiveerd. Het proces wacht op een reactie op de goedkeuringsaanvraag. ■ Goedkeuring geweigerd. De aanvraag is geweigerd door de goedkeurders in het geactiveerde goedkeuringsbeleid. De aanvraag gaat niet verder. <p>In de volgende voorbeelden ziet u hoe u de filters Levenscyclusstatus van implementatie en Laatste aanvraagstatus individueel of samen kunt gebruiken.</p> <ul style="list-style-type: none"> ■ Als u alle verwijderaanvragen wilt vinden die zijn mislukt, selecteert u Verwijderen - Mislukt in het filter Levenscyclusstatus van implementatie. ■ Als u alle aanvragen wilt vinden die op goedkeuring wachten, selecteert u Goedkeuring in behandeling in het filter Laatste aanvraagstatus. ■ Als u wilt zoeken naar de verwijderaanvragen waar de goedkeuringsaanvraag nog in behandeling is, selecteert u Verwijderen - In behandeling in het filter Levenscyclusstatus van implementatie en Goedkeuring in behandeling in het filter Laatste aanvraagstatus.

Hoe kan ik implementaties controleren in Cloud Assembly

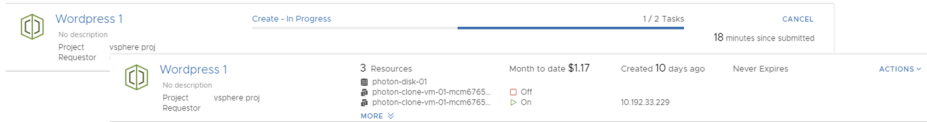
Nadat u een Cloud Assembly-cloudsjabloon hebt geïmplementeerd, kunt u uw aanvraag controleren om er zeker van te zijn dat de resources ingericht en actief zijn. Vanaf de implementatiekaart kunt u de inrichting van uw resources controleren. Vervolgens kunt u de details van de implementatie controleren. Tenslotte kunt u verwijderde implementaties tot 90 dagen na verwijdering bekijken en filteren.

Procedure

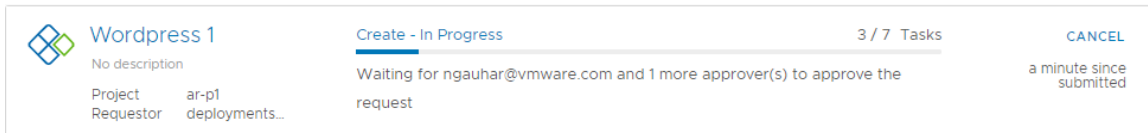
- 1 Klik op **Resources > Implementaties** en zoek uw implementatie met behulp van het filter en de zoekfunctie, indien nodig.

2 Controleer de kaartstatus.

Als de implementatie wordt uitgevoerd, geeft de voortgangsbalk het aantal resterende taken aan. Als de implementatie is voltooid, geeft de kaart de voornaamste details van de implementatie weer.

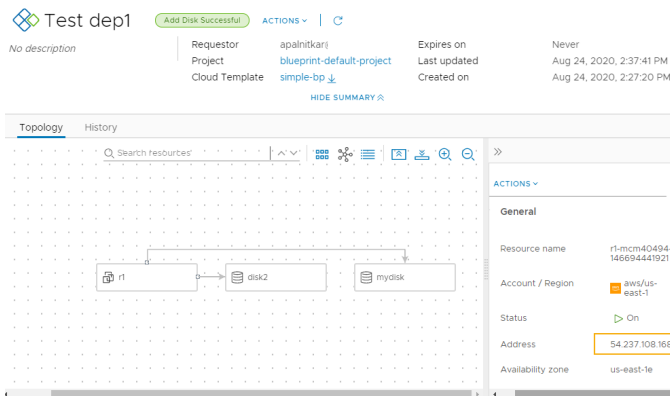


Als er een goedkeuringsbeleid wordt geactiveerd voor uw aanvraag, ziet u mogelijk dat de aanvraag de status In behandeling heeft met de naam van ten minste één goedkeurder. Goedkeuringsbeleid wordt in Service Broker gedefinieerd door uw beheerder. De goedkeurders worden in het beleid gedefinieerd. De goedkeurders keuren aanvragen goed in Service Broker. U kunt ook goedkeuringen tegenkomen op acties van dag 2.



3 Als u wilt weten waar uw resources werden geïmplementeerd, klikt u op de naam van de implementatie en bekijkt u de details op de pagina Topologie.

U hebt waarschijnlijk het IP-adres voor het primaire onderdeel nodig. Wanneer u op elk onderdeel klikt, ziet u de specifieke informatie van het onderdeel. In dit voorbeeld is het IP-adres gemarkeerd.



De beschikbaarheid van de externe link is afhankelijk van de cloudprovider. Waar de link beschikbaar is, hebt u de verificatiegegevens voor die provider nodig om toegang te krijgen tot het onderdeel.

Wat nu te doen

- U kunt wijzigingen in uw implementatie aanbrengen. Zie [Hoe kan ik de levenscyclus van een voltooide Cloud Assembly-implementatie beheren](#).
- Zie [Wat kan ik doen als een Cloud Assembly-implementatie mislukt](#) als uw implementatie mislukt.

Wat kan ik doen als een Cloud Assembly-implementatie mislukt

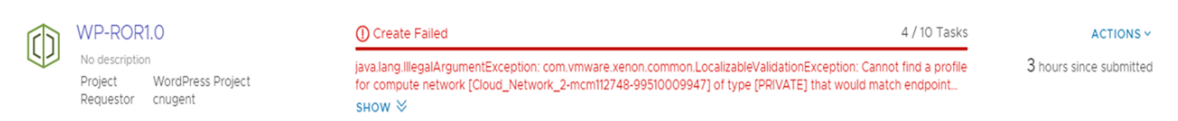
Uw implementatieaanvraag kan om een groot aantal redenen mislukken. Dit wordt mogelijk veroorzaakt door netwerkverkeer, een gebrek aan resources bij de doelcloudprovider of een gebrekkige implementatiespecificatie. Ofwel is de inrichtingsaanvraag gelukt, maar lijkt de implementatie niet te werken. U kunt Cloud Assembly gebruiken om uw implementatie te onderzoeken, eventuele foutmeldingen te bekijken en te bepalen of het probleem de omgeving, de gevraagde belastingsspecificatie of iets anders is.

U gebruikt deze werkstroom om te beginnen met uw onderzoek. Mogelijk komt tijdens het proces aan het licht dat de mislukking is veroorzaakt door een tijdelijk omgevingsprobleem. U kunt dit type probleem oplossen door de aanvraag opnieuw te implementeren nadat u hebt gecontroleerd of de voorwaarden zijn verbeterd. In andere gevallen vereist het onderzoek mogelijk dat u andere gebieden grondig onderzoekt.

Als lid van een project kunt u de details van de aanvraag bekijken in Cloud Assembly.

Procedure

- 1 Om te bepalen of een aanvraag is mislukt, selecteert u **Resources > Implementaties** en zoekt u de implementatiekaart.



Mislukte implementaties worden op de kaart aangegeven.

- a Bekijk het foutbericht.
- b Klik op de implementatienaam om de implementatiedetails weer te geven.

2 Klik op het tabblad **Geschiedenis** van de pagina Implementatiedetails.

The screenshot displays the 'Create' action details for a resource named 'WP - ROR2'. The status is 'Create Failed'. The 'History' tab is active, showing a list of events. The first event, 'REQUEST_FAILED', is highlighted, and its details are expanded, showing the error message: 'Could not find any profile to match network 'WP-Network-Private' of type 'EXISTING' with constraints '[type:isolated-net, env:dev]'.'.

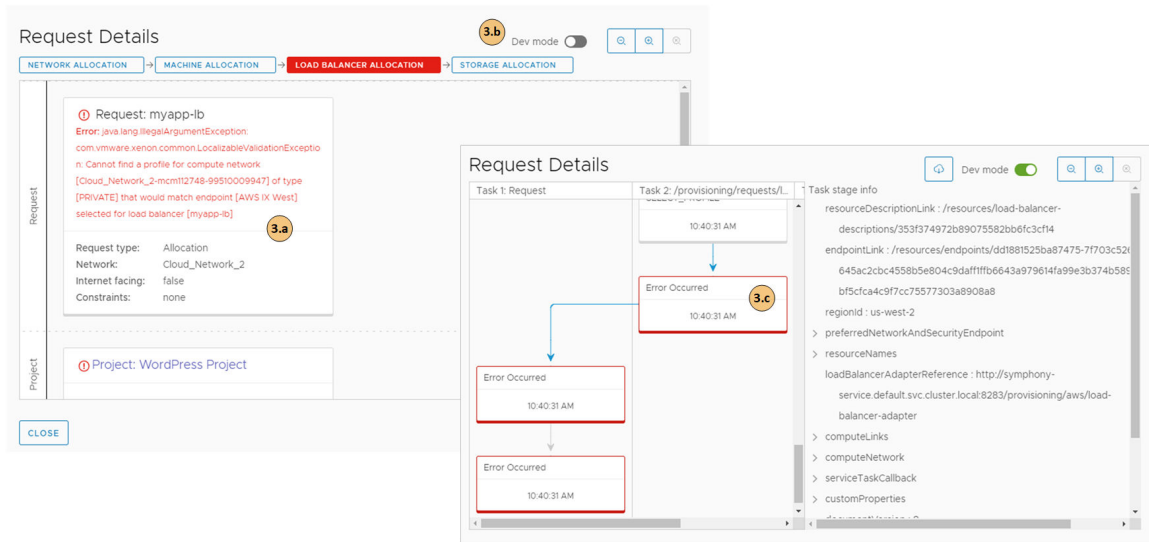
Timestamp	Status	Resource type	Resource name	Details
Sep 9, 2020, ...	REQUEST_FAILED			Could not find any profile to match network 'WP-Network-Private' of type 'EXISTING' with constraints '[type:isolated-net, env:dev]'.
Sep 9, 2020, ...	COMPLETION_FINISHED			
Sep 9, 2020, ...	COMPLETION_IN_PROGRE...			
Sep 9, 2020, ...	ALLOCATE_FAILED	Cloud.Network	WP-Network-Private	Could not find any profile to match...

- Bekijk de gebeurtenissenstructuur om te zien waar het inrichtingsproces is mislukt. Deze structuur is handig wanneer u een implementatie wijzigt, maar de wijziging mislukt.
De structuur wordt ook weergegeven wanneer u implementatieacties uitvoert. U kunt de structuur gebruiken om problemen met mislukte wijzigingen op te lossen.
- De **Details** bevatten een meer uitgebreide versie van de foutmelding.
- Als het aangevraagde item een Cloud Assembly-cloudsjabloon is, opent u Cloud Assembly met de link rechts van het bericht, zodat u de **Aanvraagdetails** kunt zien.

3 De **Aanvraagdetails** bieden de inrichtingswerkstroom voor mislukte onderdelen, zodat u het probleem kunt onderzoeken.

De aanvraaggeschiedenis wordt gedurende 48 uur bewaard.

Bekijk en filter de verwijderde implementatiegeschiedenis tot 90 dagen na verwijdering

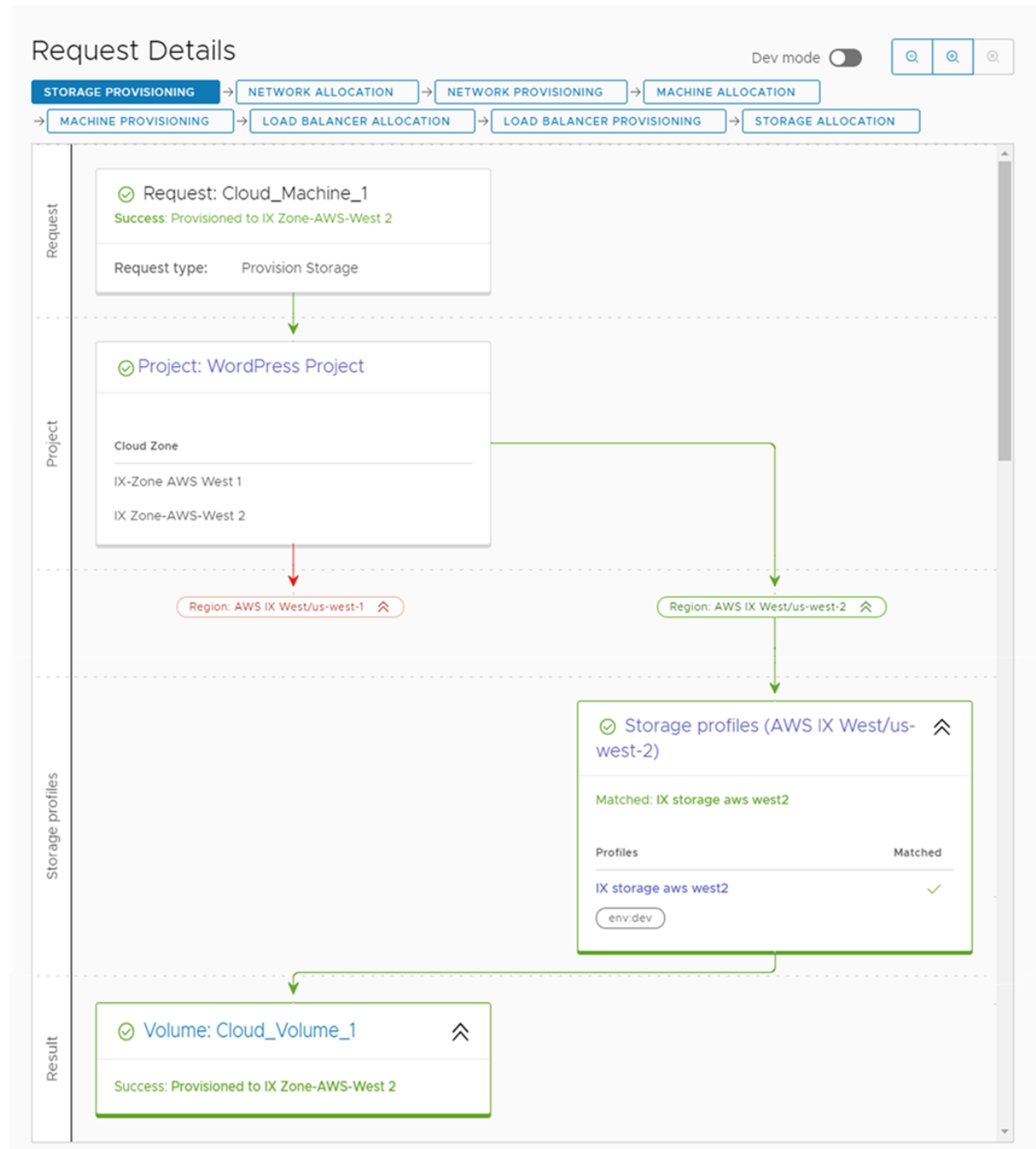


- a Bekijk het foutbericht.
 - b U kunt de **Dev-modus** inschakelen om te wisselen tussen de eenvoudige inrichtingswerkstroom en een meer gedetailleerd stroomdiagram.
 - c Klik op de kaart om het implementatiescript te controleren.
- 4 Los de fouten op en implementeer de cloudsjabloon opnieuw.

De fouten doen zich mogelijk voor in de sjabloonconstructie of kunnen zijn gerelateerd aan de manier waarop uw infrastructuur is geconfigureerd.

Wat nu te doen

Wanneer de fouten zijn opgelost en de cloudsjabloon is geïmplementeerd, kunt u in de Aanvraagdetails informatie bekijken zoals deze in het volgende voorbeeld. Als u de aanvraagdetails wilt zien, selecteert u **Infrastructuur > Activiteit > Aanvragen**.



Hoe kan ik de levenscyclus van een voltooide Cloud Assembly-implementatie beheren

Nadat een implementatie is ingericht en uitgevoerd, kunt u verschillende acties uitvoeren om de implementatie te beheren. Het levenscyclusbeheer kan het in- of uitschakelen, het wijzigen van de grootte en het verwijderen van een implementatie omvatten. U kunt ook verschillende acties voor afzonderlijke onderdelen uitvoeren om ze te beheren.

Procedure

- 1 Selecteer **Resources > Implementaties** en zoek uw implementatie.
- 2 Klik op de naam van de implementatie om toegang te krijgen tot de details van de implementatie.

U gebruikt de implementatiegegevens om inzicht te krijgen in de manier waarop de resources worden geïmplementeerd en welke wijzigingen zijn aangebracht. U ziet ook prijsinformatie, de huidige status van de implementatie en of u resources hebt die moeten worden gewijzigd.

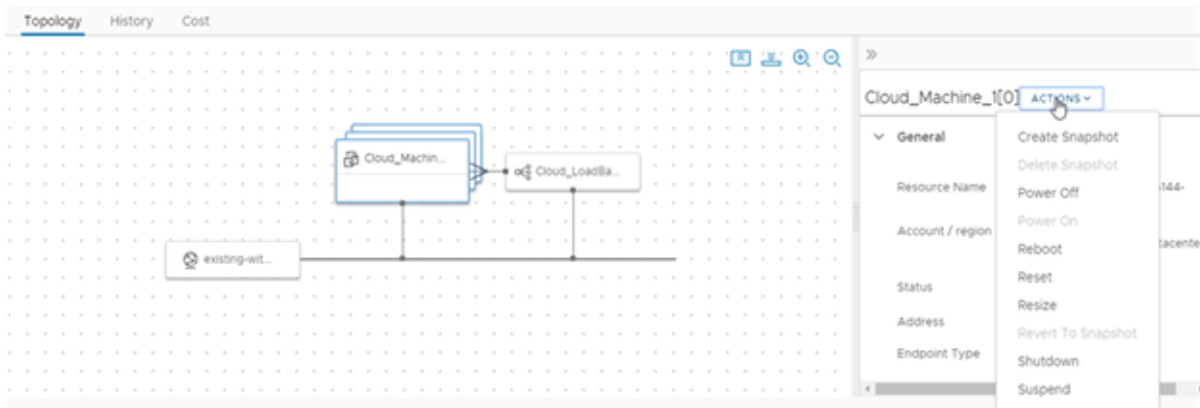
The screenshot displays the vRealize Automation Cloud Assembly interface for a deployment named 'sb-demo-03'. The interface is divided into several sections:

- Header:** Shows the deployment name 'sb-demo-03', a 'Create Successful' status, and metadata including Owner, Requestor, Project, and Cloud Template.
- Summary:** A 'HIDE SUMMARY' button is visible.
- Topology:** A tab showing a search bar and a diagram of the deployment structure, including 'Cloud_vSphere_Machine_1[0]' and 'Cloud_vSphere_Machine_1[1]'.
- History:** A tab showing a 'Create' action with a 'Successful' status, requested by 'sbhandari@vmware.com', with a timestamp of 'Mar 2, 2021, 8:41 AM'.
- Price:** A tab showing a 'Price analysis' section with 'Overall' and 'Details' views. It displays a price of '\$0.38' per month, with a bar chart showing price over time.
- Monitor:** A tab showing a 'Monitor' section with a 'CPU (%)' graph and a table of resource usage for 'Cloud_vSphere_Machine_1-mcm306191-163093649552'.
- Alerts:** A tab showing a list of alerts, including 'Definition_Deployment_VM' and 'AlertDefinition_Deployment_has_cost'.
- Optimize:** A tab showing a 'Underutilized VMs' section with a table of VMs that are idle or powered off.

- **Tabblad Topologie.** U kunt het tabblad Topologie gebruiken om inzicht te krijgen in de implementatiestructuur en -resources.
- **Tabblad Geschiedenis.** Het tabblad Geschiedenis bevat alle inrichtingsgebeurtenissen en alle gebeurtenissen die zijn gerelateerd aan acties die u uitvoert nadat het aangevraagde item is geïmplementeerd. Als er problemen zijn met het inrichtingsproces, kunnen de gebeurtenissen op het tabblad Geschiedenis u helpen bij het oplossen van de fouten.

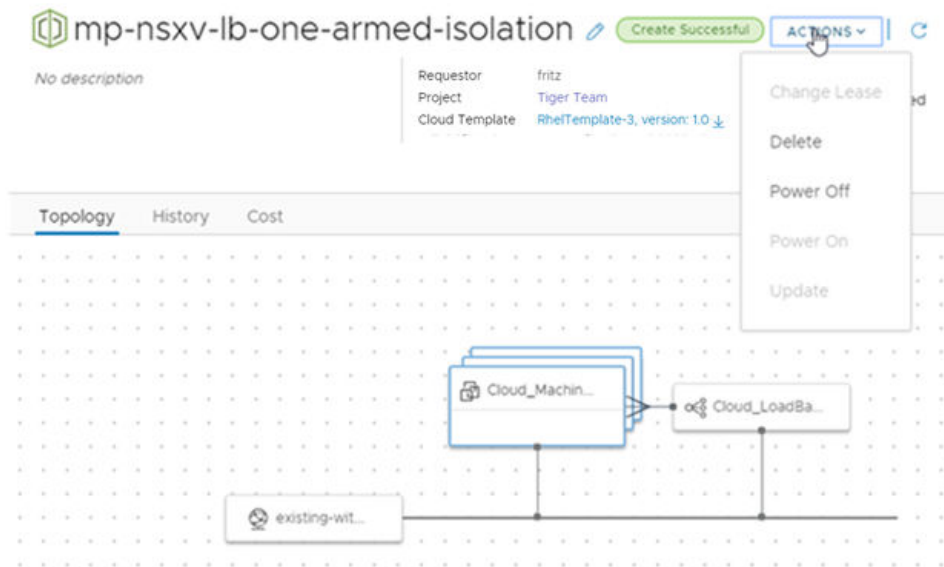
- Tabblad **Prijzen**. U kunt de prijskaart gebruiken om te begrijpen hoeveel de implementatie kost voor uw organisatie. Prijsinformatie is gebaseerd op vRealize Operations Manager- of CloudHealth-integraties.
 - Tabblad **Controleren**. De gegevens op het tabblad Controleren bieden informatie over de status van uw implementatie op basis van gegevens uit vRealize Operations Manager.
 - Tabblad **Waarschuwingen**. Het tabblad Waarschuwingen bevat actieve waarschuwingen over de implementatieresources. U kunt de waarschuwing sluiten of referentienotities toevoegen. De waarschuwingen zijn gebaseerd op gegevens uit vRealize Operations Manager.
 - Tabblad **Optimaliseren**. Het tabblad Optimaliseren biedt gebruiksinformatie over uw implementatie evenals suggesties voor het terugwinnen of anderszins wijzigen van de resources om het resourceverbruik te optimaliseren. De informatie over optimalisatie is gebaseerd op gegevens uit vRealize Operations Manager.
- 3 Als u vaststelt dat een implementatie te duur is in de huidige configuratie en u het formaat van een onderdeel wilt wijzigen, selecteert u het onderdeel op de topologiepagina en selecteert u vervolgens **Acties > Formaat wijzigen** op de onderdeelpagina.

Welke acties beschikbaar zijn, is afhankelijk van het onderdeel, het cloudaccount en uw rechten.



- 4 Een van uw implementaties is niet langer nodig als onderdeel van uw ontwikkelingslevenscyclus. Als u de implementatie wilt verwijderen en resources wilt terugwinnen, selecteert u **Acties > Verwijderen**.

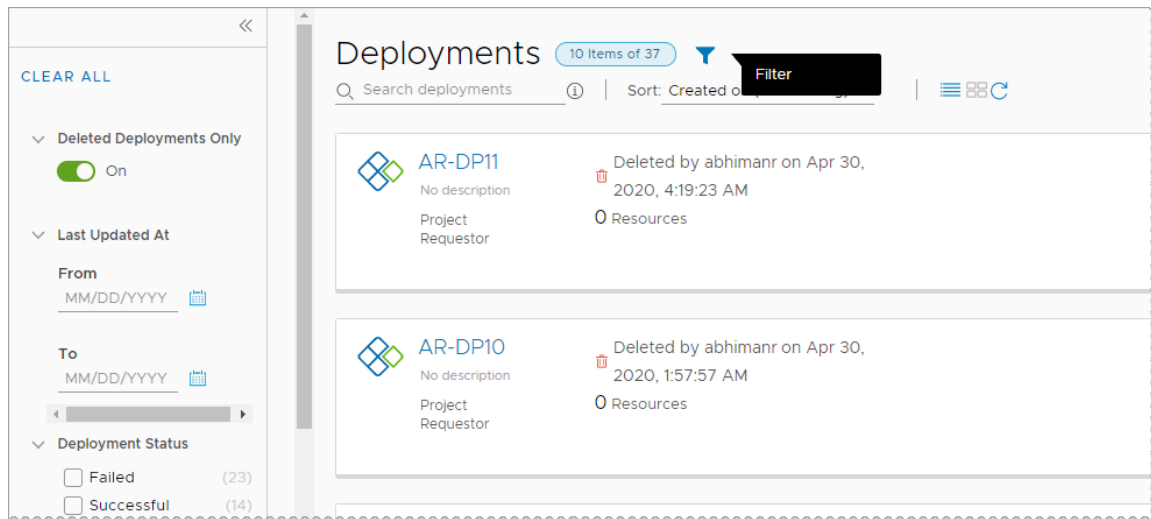
Welke acties beschikbaar zijn, hangt af van de status van de implementatie.



- 5 Als u uw verwijderde implementaties wilt bekijken, klikt u op het filter op de pagina **Implementaties** en schakelt u vervolgens **Alleen verwijderde implementaties** in.

De lijst met implementaties is nu beperkt tot de verwijderde implementaties. Mogelijk wilt u de geschiedenis van een bepaalde implementatie bekijken. Bijvoorbeeld om de naam van een verwijderde machine op te halen.

De verwijderde implementaties worden 90 dagen weergegeven.



Wat nu te doen

Zie [Welke acties kan ik op Cloud Assembly-implementaties uitvoeren](#) voor meer informatie over mogelijke acties.

Welke acties kan ik op Cloud Assembly-implementaties uitvoeren

Nadat u cloudsjablonen hebt geïmplementeerd, kunt u acties uitvoeren in Cloud Assembly om de resources te beheren. Welke acties beschikbaar zijn, is afhankelijk van het resourcetype en van het feit of de acties worden ondersteund op een bepaald cloudaccount of integratieplatform.

De beschikbare acties zijn ook afhankelijk van de rechten die uw beheerder u heeft verleend om acties uit te voeren.

Als beheerder of projectbeheerder kunt u het beleid voor Dag 2-acties instellen in Service Broker. Zie [Hoe geef ik consumenten rechten op Service Broker-actiebeleid voor dag 2?](#)

U kunt ook acties zien die niet zijn opgenomen in de lijst. Dit zijn waarschijnlijk custom acties die uw beheerder heeft toegevoegd. Bijvoorbeeld: een [Een aangepaste Cloud Assembly-resourceactie maken voor een virtuele machine met vMotion](#).

Tabel 7-2. Lijst met mogelijke acties

Actie	Van toepassing op deze resource type	Beschikbaar voor deze cloudtypen	Oorsprong van resource	Beschrijving
Schijf toevoegen	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbedoend is voltooid 	<p>Voeg extra schijven toe aan bestaande virtuele machines.</p> <p>Als u een schijf toevoegt aan een Azure-machine, wordt de persistente schijf of niet-persistente schijf geïmplementeerd in de resourcegroep die de machine bevat.</p> <p>Wanneer u een schijf aan een Azure-machine toevoegt, kunt u ook de nieuwe schijf versleutelen met behulp van de Azure-schijfversleutelingsset die is geconfigureerd in het opslagprofiel.</p> <p>U kunt geen schijf toevoegen aan een Azure-machine met een onbeheerde schijf.</p> <p>Wanneer u een schijf toevoegt aan vSphere-machines, kunt u de SCSI-controller selecteren, waarvan de volgorde in de cloudsjabloon is ingesteld en is geïmplementeerd. U kunt ook het eenheidsnummer voor de nieuwe schijf opgeven. U kunt geen eenheidsnummer opgeven zonder een geselecteerde controller. Als u geen controller selecteert of geen eenheidsnummer opgeeft, wordt de nieuwe schijf geïmplementeerd op de eerst beschikbare controller en toegewezen aan het volgende beschikbare eenheidsnummer op die controller.</p> <p>Als u een schijf toevoegt aan een vSphere machine voor een project met gedefinieerde opslaglimieten, mag de toegevoegde schijf de opslaglimieten niet overschrijden.</p> <p>Als u VMware Storage DRS (SDRS) gebruikt en het gegevensopslagcluster is geconfigureerd in het opslagprofiel, kunt u schijven op SDRS toevoegen aan vSphere-machines.</p>
Salt-configuratie toepassen	Machines	<ul style="list-style-type: none"> ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbedoend is voltooid 	<p>Installeer een Salt-minion of werk de Salt-configuratie bij op een virtuele machine.</p> <p>De optie Salt-configuratie toepassen is beschikbaar als u de SaltStack Config-integratie hebt geconfigureerd.</p> <p>Opmerking Voordat u deze methode gebruikt om de Salt-minion te installeren, bestaat er een meer robuuste optie waarbij u de minion in de cloudsjabloon opneemt. De sjabloonmethode bevat een SaltStack Config-resource type in de implementatie. Raadpleeg Hoe voegt u de SaltStack Config-resource toe aan sjablonen voor meer informatie.</p>

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resource	Beschikbaar voor deze cloudtypen	Oorsprong van resource	Beschrijving
				<p>Als u een configuratie wilt toepassen, moet u een verificatiemethode selecteren. De Externe toegang met bestaande verificatiegegevens maakt gebruik van de verificatiegegevens voor externe toegang die zijn opgenomen in de implementatie. Als u de verificatiegegevens op de machine na implementatie hebt gewijzigd, kan de actie mislukken. Als u de nieuwe verificatiegegevens weet, gebruikt u de verificatiemethode Wachtwoord.</p> <p>Het Wachtwoord en de Persoonlijke sleutel gebruiken de gebruikersnaam en het wachtwoord of de sleutel om uw verificatiegegevens te valideren en vervolgens via SSH verbinding te maken met de virtuele machine.</p> <p>Als u geen waarde opgeeft voor de master-ID en Minion-ID, maakt Salt de waarden voor u.</p>
Annuleren	<ul style="list-style-type: none"> ■ Implementaties ■ Verschillende resource typen in implementaties 	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbieden is voltooid 	<p>Annuleer een implementatie of een actie voor dag 2 voor een implementatie of een resource terwijl de aanvraag wordt verwerkt.</p> <p>U kunt de aanvraag annuleren op de implementatiekaart of in de implementatiegegevens.</p> <p>Nadat u de aanvraag heeft geannuleerd, wordt deze als mislukte aanvraag weergegeven op de pagina Implementaties. Gebruik de actie Verwijderen om geïmplementeerde resources vrij te geven en uw implementatielijst op te schonen.</p> <p>Het annuleren van een aanvraag waarvan u denkt dat deze te lang wordt uitgevoerd, is één methode voor het beheren van de implementatietijd. Het is echter efficiënter om Time-out voor aanvraag in te stellen in de projecten. De standaardtime-out is twee uur. U kunt een langere tijdsperiode instellen als de workloadimplementatie voor een project meer tijd vereist.</p>
Lease wijzigen	Implementaties	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbieden is voltooid 	<p>Controleer de vervaldatum en -tijd van de lease.</p> <p>Wanneer een lease verloopt, wordt de implementatie vernietigd en worden de resources teruggewonnen.</p> <p>Leasebeleidsregels worden ingesteld in Service Broker.</p>

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resource	Beschikbaar voor deze clouddtypen	Oorsprong van resource	Beschrijving
Eigenaar wijzigen	Implementaties	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbetrokken is voortdurend 	<p>Wijzigt de eigenaar van de implementatie in de geselecteerde gebruiker. De geselecteerde gebruiker, als persoon of lid van een groep, moet een beheerder of lid zijn van hetzelfde project dat de aanvraag heeft geïmplementeerd.</p> <p>Wanneer een ontwerpfunctie voor cloudsjablonen een sjabloon implementeert, is de ontwerper zowel de aanvrager als de eigenaar. Een aanvrager kan echter een ander lid van het project de eigenaar maken.</p> <p>U kunt beleid gebruiken om te bepalen wat een eigenaar kan doen met een implementatie, zodat deze rechten krijgt die meer beperkend of minder beperkend zijn.</p>

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resourcetypen	Beschikbaar voor deze cloudtypen	Oorsprong van resource	Beschrijving
Project wijzigen	Implementaties	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ NSX-T ■ NSX-V ■ VMware Cloud Director ■ VMware Cloud Foundation ■ VMware Cloud on AWS ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbevoegd 	<p>U gebruikt de actie Project wijzigen gebruiken om een implementatie van een project naar een ander project te verplaatsen.</p> <p>De actie Project wijzigen is beschikbaar voor implementaties met geïmplementeerde resources en implementaties met geonboarde resources. Deze actie wordt niet ondersteund voor implementaties die zowel geonboarde als geïmplementeerde resources bevatten. De actie is niet beschikbaar voor gemigreerde implementaties.</p> <p>Ondersteunde resources omvatten de volgende resourcetypen en beperkingen:</p> <ul style="list-style-type: none"> ■ Implementaties met geïmplementeerde resources kunnen virtuele machines, schijven, load balancers, netwerken, beveiligingsgroepen, Azure-groepen, NAT's en gateways bevatten. ■ Implementaties met geonboarde resources kunnen virtuele machines, schijven en netwerken bevatten. ■ Als u een niet-ondersteund resourcetype toevoegt aan een van beide implementatietypen (met geïmplementeerde resources of met geonboarde resources), kunt u de actie Project wijzigen niet uitvoeren. Als u bijvoorbeeld een Terraform-configuratie toevoegt aan een implementatie, is de actie Project wijzigen niet beschikbaar. <p>Rollen, overwegingen en beperkingen voor implementaties met geïmplementeerde resources:</p> <ul style="list-style-type: none"> ■ Om het project van een implementatie met geïmplementeerde resources te wijzigen, moet de initiële gebruiker de volgende rol hebben: <ul style="list-style-type: none"> ■ Cloudbeheerder. ■ U kunt het project alleen wijzigen wanneer het doelproject alle cloudzones bevat waar de machines en schijven van de implementatie worden geïmplementeerd. De verplaatste implementatie is dan onderhevig aan de geconfigureerde limieten van het doelproject, zoals aantal instanties, geheugen, CPU en opslag. Na de verplaatsing wordt het huidige gebruik vrijgegeven vanuit het bronproject. ■ Nadat u een implementatie naar het doelproject heeft verplaatst, is deze onderworpen aan het beleid van het doelproject. Bijvoorbeeld: lease, acties voor dag 2, resourcequotum en

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resources	Beschikbaar voor deze cloudtypen	Oorsprong van resources	Beschrijving
				<p>andere beleidsregels. Om een implementatie te verplaatsen, kan de implementatielease die is gedefinieerd door het leasebeleid van het doelproject, niet binnen 24 uur vervallen.</p> <p>Rollen, overwegingen en beperkingen voor implementaties met geonboarde resources:</p> <ul style="list-style-type: none"> ■ Om een implementatie met geonboarde resources te verplaatsen, moet de initiële gebruiker ten minste een van de volgende rollen hebben: <ul style="list-style-type: none"> ■ Cloudbeheerder. ■ Recht Implementaties beheren. Dit recht kan worden gedefinieerd als aangepaste rol. ■ Projectbeheerder van het doelproject. ■ Projectlid van het doelproject en de implementaties worden gedeeld tussen alle gebruikers in het doelproject. ■ Hoewel u geonboarde resources kunt verplaatsen naar een project dat niet dezelfde cloudzones bevat, als het doelproject niet dezelfde cloudzones heeft, werken toekomstige acties voor dag 2 met betrekking tot cloudaccount/regioresources die u uitvoert, mogelijk niet. <p>Algemene overwegingen:</p> <ul style="list-style-type: none"> ■ Als u een beheerder bent die de implementatie verplaatst, kunt u de implementatie mogelijk verplaatsen naar een project waarbij de eigenaar geen lid is en bijgevolg toegang verliest. U kunt de eigenaar toevoegen aan het doelproject of de implementatie verplaatsen naar een project waarvan de gebruiker lid is.

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resource	Beschikbaar voor deze cloudtypen	Oorsprong van resource	Beschrijving
Beveiligingsgroepen wijzigen	Machines	■ VMware vSphere	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onboarden is voltooid 	<p>U kunt beveiligingsgroepen koppelen aan en loskoppelen van machinenetwerken in een implementatie. De wijzigingsactie is van toepassing op bestaande en beveiligingsgroepen op aanvraag voor NSX-V en NSX-T. Deze actie is alleen beschikbaar voor enkele computers en niet voor machineclusters.</p> <p>Als u een beveiligingsgroep wilt koppelen aan het machinenetwerk moet de beveiligingsgroep aanwezig zijn in de implementatie.</p> <p>Als u een beveiligingsgroep loskoppelt van alle netwerken van alle computers in een implementatie wordt de beveiligingsgroep niet uit de implementatie verwijderd.</p> <p>Deze wijzigingen hebben geen invloed op beveiligingsgroepen die zijn toegepast als onderdeel van de netwerkprofielen.</p> <p>Deze actie wijzigt de configuratie van de beveiligingsgroep van de machine zonder de machine opnieuw te maken. Dit is een niet-destructieve wijziging.</p> <ul style="list-style-type: none"> ■ Als u de configuratie van de beveiligingsgroep van de machine wilt wijzigen, selecteert u de machine in het deelvenster topologie en klikt u vervolgens op het menu Actie in het rechterdeelvenster en selecteert u Beveiligingsgroepen wijzigen. U kunt nu de associatie van de beveiligingsgroepen met de machinenetwerken toevoegen of verwijderen.
Verbinden met externe console	Machines	■ VMware vSphere	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Gedeactiveerd ■ Onboarden is voltooid 	<p>Open een externe sessie op de geselecteerde machine.</p> <p>Bekijk de volgende vereisten voor een geslaagde verbinding.</p> <ul style="list-style-type: none"> ■ Controleer als implementatiegebruiker of de ingerichte machine is ingeschakeld.

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resource	Beschikbaar voor deze clouddtypen	Oorsprong van resource	Beschrijving
Momentopname van schijf maken	Machines en schijven	<ul style="list-style-type: none"> ■ Microsoft Azure 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbeschikbaar is voltooid 	<p>Maak een momentopname van een VM-schijf of een opslagschijf.</p> <ul style="list-style-type: none"> ■ Voor machines maakt u momentopnamen voor afzonderlijke machineschijven, zoals opstartschijf, imageschijven en opslagschijven. ■ Voor opslagschijven maakt u momentopnamen van onafhankelijke beheerde schijven, geen onbeheerde schijven. <p>Naast het opgeven van een naam voor een momentopname kunt u ook de volgende informatie voor de momentopname opgeven:</p> <ul style="list-style-type: none"> ■ Incrementele momentopname. Schakel het selectievakje in om een momentopname te maken van de wijzigingen sinds de laatste momentopname, in plaats van een volledige momentopname te maken. ■ Resourcegroep. Voer de naam in van de doelresourcegroep waar u de momentopname wilt maken. Standaard wordt de momentopname gemaakt in dezelfde resourcegroep die wordt gebruikt door de bovenliggende schijf. ■ Versleutelingsset-ID. Selecteer de versleutelingssleutel voor de momentopname. Standaard wordt de momentopname versleuteld met dezelfde sleutel die wordt gebruikt door de bovenliggende schijf. ■ Tags. Voer tags in om de momentopnamen in Microsoft Azure makkelijker te beheren.
Momentopname maken	Machines	<ul style="list-style-type: none"> ■ Google Cloud Platform ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbeschikbaar is voltooid 	<p>Een momentopname maken van de virtuele machine. Als u toestemming hebt voor slechts twee momentopnamen in vSphere en die allebei al hebt gemaakt, moet u eerst een momentopname verwijderen voordat deze opdracht weer beschikbaar is.</p>

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resource type	Beschikbaar voor deze cloudtypen	Oorsprong van resource	Beschrijving
Verwijderen	Implementaties	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	<p>Een implementatie vernietigen.</p> <p>Alle resources worden verwijderd en vervolgens opnieuw geclaimd.</p> <p>Als een verwijdering mislukt, kunt u de verwijderactie een tweede keer uitvoeren op een implementatie.</p> <p>Tijdens de tweede poging kunt u Ignore Delete Failures selecteren. Als u deze optie selecteert, wordt de implementatie verwijderd, maar worden de resources mogelijk niet teruggewonnen. U moet de systemen controleren waarop de implementatie is ingericht om ervoor te zorgen dat alle resources worden verwijderd. Als dit niet het geval is, moet u de overige resources op deze systemen handmatig verwijderen.</p>
	NSX-gateway	<ul style="list-style-type: none"> ■ NSX 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	Verwijder de regels voor NAT-port mapping van een NSX-T- of NSX-V-gateway.
	Machines en load balancers	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere ■ VMware NSX 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	Verwijder een machine of load balancer uit een implementatie. Deze actie kan ertoe leiden dat de implementatie onbruikbaar wordt.

Tabel 7-2. Lijst met mogelijke acties (vervolg)

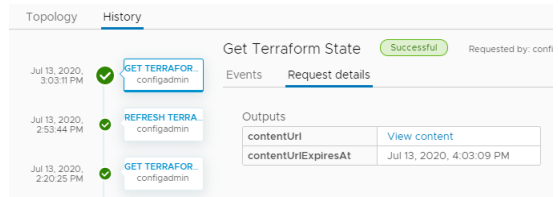
Actie	Van toepassing op deze resource type	Beschikbaar voor deze cloudtypen	Oorsprong van resource	Beschrijving
Beveiliging sgroepen		<ul style="list-style-type: none"> ■ NSX-T ■ NSX-V 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	<p>Als de beveiligingsgroep niet is gekoppeld aan een machine in de implementatie, verwijdert het proces de beveiligingsgroep uit de implementatie.</p> <ul style="list-style-type: none"> ■ Als de beveiligingsgroep op aanvraag is, wordt deze op het eindpunt vernietigd. ■ Als de beveiligingsgroep wordt gedeeld, mislukt de actie.
Tanzu Kubernetes -clusters		<ul style="list-style-type: none"> ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	Verwijder een Tanzu Kubernetes-cluster uit een implementatie.
Momentopname van schijf verwijderen	Machines en schijven	<ul style="list-style-type: none"> ■ Microsoft Azure 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	Verwijder de schijf van een virtuele machine of een momentopname van een beheerde schijf in Azure. Deze actie is beschikbaar wanneer er ten minste één momentopname is.
Momentopname verwijderen	Machines	<ul style="list-style-type: none"> ■ VMware vSphere ■ Google Cloud Platform 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	Een momentopname van de virtuele machine verwijderen.

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resource type	Beschikbaar voor deze cloudtypen	Oorsprong van resource	Beschrijving
Opstart diagnose uitschakelen	Machines	■ Microsoft Azure	■ Geïmplementeerd ■ Onbeschikbaar is voltooid	Schakel de foutopsporingsfunctie voor virtuele Azure-machines uit. De optie Uitschakelen is alleen beschikbaar als de functie is ingeschakeld.
Tags bewerken	Implementaties	■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere	■ Geïmplementeerd ■ Onbeschikbaar is voltooid	Voeg resource tags toe die worden toegepast op individuele implementatieresources of wijzig deze.
Opstart diagnose inschakelen	Machines	■ Microsoft Azure	■ Geïmplementeerd ■ Onbeschikbaar is voltooid	Schakel de foutopsporingsfunctie voor virtuele Azure-machines in om de opstartfouten van de virtuele machine te diagnosticeren. De diagnostische gegevens van het opstarten zijn beschikbaar in uw Azure-console. De optie Inschakelen is alleen beschikbaar als de functie momenteel niet is ingeschakeld.

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resource type	Beschikbaar voor deze cloudtypen	Oorsprong van resource	Beschrijving
Terraform-status ophalen	Terraform-configuratie	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbepaald 	<p>Toon het Terraform-statusbestand.</p> <p>Als u wijzigingen wilt weergeven die zijn aangebracht op de Terraform-machines op de cloudplatformen waarop ze zijn geïmplementeerd en de implementatie wilt bijwerken, voert u eerst de actie Terraform-status vernieuwen uit en voert u dan de actie Terraform-status ophalen uit.</p> <p>Wanneer het bestand in een dialoogvenster wordt weergegeven. Het bestand is ongeveer 1 uur beschikbaar voordat u een nieuwe actie voor vernieuwen moet uitvoeren. U kunt het kopiëren als u het later nodig hebt.</p> <p>U kunt het bestand ook bekijken op het tabblad implementatiegeschiedenis. Selecteer de gebeurtenis Terraform-status ophalen op het tabblad Gebeurtenissen en klik vervolgens op Aanvraagdetails. Als het bestand niet is verlopen, klikt u op Inhoud weergeven. Als het bestand is verlopen, voert u opnieuw Vernieuwen en Acties ophalen uit.</p>



U kunt andere dag 2-acties uitvoeren op de Terraform-resources die zijn ingesloten in de configuratie. De beschikbare acties zijn afhankelijk van het resource type, het cloudplatform waarop ze worden geïmplementeerd en of u bevoegd bent om de acties uit te voeren op basis van een beleid voor dag 2.

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resource type	Beschikbaar voor deze cloudtypen	Oorsprong van resource	Beschrijving
Uitschakelen	Implementaties	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Gedeteteerd ■ Onbarend is voltooid 	Schakel de implementatie uit na de eerste poging om de gastbesturingssystemen uit te schakelen. Als de softwarematige uitschakeling mislukt, wordt een uitschakeling hardwarematig uitgevoerd.
	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	Schakel de machine uit na de eerste poging om de gastbesturingssystemen uit te schakelen. Als de softwarematige uitschakeling mislukt, wordt de uitschakeling hardwarematig uitgevoerd.
Inschakelen	Implementaties	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	De implementatie inschakelen. Als de resources zijn onderbroken, wordt de normale werking hervat vanaf het punt waarop de resources zijn onderbroken.

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resource type	Beschikbaar voor deze cloudtypen	Oorsprong van resource	Beschrijving
	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Gedetecteerd ■ Onbarend is voltooid 	De machine inschakelen. Als de machine is onderbroken, wordt de normale werking hervat vanaf het punt waarop de machine is onderbroken.
Opnieuw opstarten	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	Het gastbesturingssysteem van een virtuele machine opnieuw opstarten. Voor een vSphere-machine moet VMware Tools op de machine zijn geïnstalleerd als u deze actie wilt gebruiken.
Opnieuw configureren	Load balancers	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware NSX 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	Wijzig de grootte van de load balancer en het logboekregistratieniveau. U kunt ook routes toevoegen of verwijderen en de instellingen voor het protocol, de poort, de statusconfiguratie en de ledenpool wijzigen. Voor NSX load balancers kunt u de statuscontrole in- of uitschakelen en de statusopties wijzigen. Voor NSX-T kunt u de controle instellen op actief of passief. Voor NSX-V worden geen passieve gezondheidscontroles ondersteund.

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resource	Beschikbaar voor deze cloudtypen	Oorsprong van resource	Beschrijving
Port mapping NSX-gateway		<ul style="list-style-type: none"> ■ NSX-T ■ NSX-V 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbeschikbaar is vroeger 	De regels voor NAT-port mapping van een NSX-T- of NSX-V-gateway toevoegen, bewerken of verwijderen.
Beveiligingsgroepen		<ul style="list-style-type: none"> ■ NSX-T ■ NSX-V ■ VMware Cloud ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbeschikbaar is vroeger 	<p>U kunt firewallregels of beperkingen toevoegen, bewerken of verwijderen op basis van het feit of het een beveiligingsgroep op aanvraag of een bestaande beveiligingsgroep is.</p> <ul style="list-style-type: none"> ■ Beveiligingsgroep op aanvraag <p>Voeg firewallregels voor NSX-T- en VMware Cloud-beveiligingsgroepen op aanvraag toe, of bewerk of verwijder ze.</p> <ul style="list-style-type: none"> ■ Om een regel toe te voegen of te verwijderen, selecteert u de beveiligingsgroep in het deelvenster Topologie, klikt u op het menu Actie in het rechterdeelvenster en selecteert u Opnieuw configureren. U kunt nu de regels toevoegen, bewerken of verwijderen. ■ Bestaande beveiligingsgroep <p>U kunt beperkingen voor bestaande NSX V-, NSX-T- of VMware Cloud-beveiligingsgroepen toevoegen, bewerken of verwijderen.</p> <ul style="list-style-type: none"> ■ Om een beperking toe te voegen of te verwijderen, selecteert u de beveiligingsgroep in het deelvenster Topologie, klikt u op het menu Actie in het rechterdeelvenster en selecteert u Opnieuw configureren. U kunt nu de beperkingen toevoegen, bewerken of verwijderen.

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resource	Beschikbaar voor deze cloudtypen	Oorsprong van resource	Beschrijving
Terraform-status vernieuwen	Terraform-configuratie	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	<p>Haal de laatste iteratie van het Terraform-statusbestand op.</p> <p>Als u wijzigingen wilt ophalen die zijn aangebracht op de Terraform-machines op de cloudplatforms waarop deze zijn geïmplementeerd en de implementatie wilt bijwerken, voert u eerst de actie Terraform-status vernieuwen uit.</p> <p>Als u het bestand wilt weergeven, voert u de actie Terraform-status ophalen uit voor de configuratie.</p> <p>Gebruik het tabblad implementatiegeschiedenis om het vernieuwingsproces te controleren.</p>
Schijf verwijderen	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	<p>Verwijder schijven van bestaande virtuele machines.</p> <p>Als u de actie voor dag 2 uitvoert op een implementatie die is geïmplementeerd als vSphere-machines en -schijven, wordt het aantal schijven vrijgemaakt, zoals van toepassing is op de projectopslaglimieten. De projectopslaglimieten zijn niet van toepassing op extra schijven die u na de implementatie hebt toegevoegd als een actie voor dag 2.</p>
Opnieuw instellen	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	<p>Het opnieuw opstarten van de virtuele machine afdwingen zonder het gastbesturingssysteem af te sluiten.</p>
Grootte wijzigen	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ Google Cloud Platform ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	<p>De CPU en het geheugen van een virtuele machine vergroten of verkleinen.</p>

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resource	Beschikbaar voor deze cloudtypen	Oorsprong van resource	Beschrijving
Grootte van opstartschijf wijzigen	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbedoeld 	<p>Vergroot of verklein de grootte van het medium voor de opstartschijf.</p> <p>Als u de actie voor dag 2 uitvoert op een implementatie die is geïmplementeerd als vSphere-machines en -schijven, en de actie mislukt met een bericht zoals 'De aangevraagde opslag is hoger dan de beschikbare opslagplaatsing', wordt dit mogelijk veroorzaakt door de gedefinieerde opslaglimieten in uw vSphere VM-sjablonen en de inhoudsbibliotheek die zijn gedefinieerd in het project. De projectopslaglimieten zijn niet van toepassing op extra schijven die u na de implementatie hebt toegevoegd als een actie voor dag 2.</p>
Grootte van schijf wijzigen	Opslag	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbedoeld 	<p>De capaciteit van een opslagschijf vergroten.</p> <p>Als u de actie voor dag 2 uitvoert op een implementatie die is geïmplementeerd als vSphere-machines en -schijven, en de actie mislukt met een bericht zoals 'De aangevraagde opslag is hoger dan de beschikbare opslagplaatsing', wordt dit mogelijk veroorzaakt door de gedefinieerde opslaglimieten in uw vSphere VM-sjablonen en de inhoudsbibliotheek die zijn gedefinieerd in het project. De projectopslaglimieten zijn niet van toepassing op extra schijven die u na de implementatie hebt toegevoegd als een actie voor dag 2.</p>
	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbedoeld 	<p>De grootte van schijven in de machine-imagesjabloon en eventuele gekoppelde schijven vergroten of verkleinen.</p>

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resource type	Beschikbaar voor deze cloudtypen	Oorsprong van resource	Beschrijving
Opnieuw opstarten	Machines	■ Microsoft Azure	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbeschikbaar is voltooid 	Een actieve machine afsluiten en opnieuw opstarten.
Terugzetten naar momentopname	Machines	■ VMware vSphere	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbeschikbaar is voltooid 	<p>Een vorige momentopname van de machine terugzetten.</p> <p>U kunt deze actie alleen gebruiken als u een bestaande momentopname hebt.</p>
Puppet-taak uitvoeren	Beheerde resources	■ Puppet Enterprise	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbeschikbaar is voltooid 	<p>Voer de geselecteerde taak uit op machines in uw implementatie.</p> <p>De taken zijn gedefinieerd in uw Puppet-instantie. U moet de taak kunnen identificeren en de invoerparameters opgeven.</p>
Werkerknooppunten schalen	Tanzu Kubernetes-clusters	■ VMware vSphere	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbeschikbaar is voltooid 	Verhoog of verklein het aantal virtuele machines van het Tanzu Kubernetes-werkerknooppunt in uw implementatie.

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resource	Beschikbaar voor deze cloudtypen	Oorsprong van resource	Beschrijving
Afsluiten	Machines	<ul style="list-style-type: none"> ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd 	Het gastbesturingssysteem afsluiten en de machine uitschakelen. U kunt deze actie alleen gebruiken als VMware Tools op de machine is geïnstalleerd.
Opheffen	Machines	<ul style="list-style-type: none"> ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	Pauzeer de machine zodat deze niet kan worden gebruikt en deze geen andere systeemresources verbruikt dan de opslag die de machine gebruikt.
Bijwerken	Implementaties	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	<p>De implementatie wijzigen op basis van de invoerparameters.</p> <p>Zie Een geïmplementeerde machine naar een ander netwerk verplaatsen voor een voorbeeld.</p> <p>Als de implementatie is gebaseerd op vSphere-resources, en de machine en schijven de optie Aantal bevatten, kunnen de opslaglimieten die in het project zijn gedefinieerd, van toepassing zijn wanneer u het aantal verhoogt. Als de actie mislukt met een bericht zoals 'De aangevraagde opslag is groter dan de beschikbare opslagplaatsing', wordt dit mogelijk veroorzaakt door de gedefinieerde opslaglimieten in uw vSphere VM-sjablonen die zijn gedefinieerd in het project. De projectopslaglimieten zijn niet van toepassing op extra schijven die u na de implementatie hebt toegevoegd als een actie voor dag 2.</p>
Tags bijwerken	Machines en schijven	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onbarend is voltooid 	Voeg een tag toe of wijzig of verwijder een tag die op een individuele resource wordt toegepast.

Tabel 7-2. Lijst met mogelijke acties (vervolg)

Actie	Van toepassing op deze resourcetypen	Beschikbaar voor deze clouddtypen	Oorsprong van resource	Beschrijving
Tanzu-versie bijwerken	Tanzu Kubernetes-clusters	<ul style="list-style-type: none"> ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onboarden is voltooid 	Werk de huidige Kubernetes-versie bij naar een hogere versie.
Registratie ongedaan maken	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Geïmplementeerd ■ Onboarden is voltooid 	<p>De actie Registratie ongedaan maken is alleen beschikbaar voor geonboarde implementatiemachines.</p> <p>Niet-geregistreerde machines worden samen met gekoppelde schijven uit de implementatie verwijderd. Door de resources te verwijderen, kunt u vervolgens de onboardingwerkstroom voor de niet-geregistreerde machine opnieuw uitvoeren. Mogelijk wilt u de resource opnieuw onboarden voor een nieuw project.</p> <p>Als u wijzigingen in de machine aanbrengt, bijvoorbeeld door een schijf toe te voegen, voordat u de registratie van de machine ongedaan maakt, mislukt de actie voor het ongedaan maken van de registratie.</p>

Resources beheren in Cloud Assembly

Als Cloud Assembly-cloudbeheerder of -cloudsjabloonontwikkelaar gebruikt u het tabblad Resources om uw cloudresources te beheren. Het tabblad Resources fungeert als resourcecentrum waar u resources in de clouds kunt controleren, er wijzigingen in kunt aanbrengen en ze zelfs kunt vernietigen of verwijderen.

U kunt uw resources zoeken en beheren met de verschillende weergaven. U kunt de lijsten filteren, resourcedetails weergeven en vervolgens acties voor de afzonderlijke items uitvoeren. De beschikbare acties zijn afhankelijk van het resourcetype en het beleid voor dag 2.

Als u een Cloud Assembly-beheerder bent, kunt u ook gedetecteerde machines weergeven en beheren.

Als u uw resources wilt weergeven, selecteert u **Resources > Resources**.

Werken met de resourcelijsten

U kunt de resourcelijsten gebruiken om de volgende resourcetypes te beheren: machines, opslagvolumes, netwerken, load balancers en beveiligingsgroepen die deel uitmaken van uw implementaties. In de resourcelijst kunt u deze in resourcetypegroepen beheren in plaats van op implementaties.

- **Alle resources**

Bevat alle gedetecteerde, geïmplementeerde, gemigreerde en geonboarde resources die in de volgende secties worden beschreven.

- **Virtual machines**

Individuele virtuele machines. De machines kunnen deel uitmaken van grotere implementaties.

- **Volumes**

Opslagvolumes die zijn gedetecteerd of gekoppeld aan implementaties.

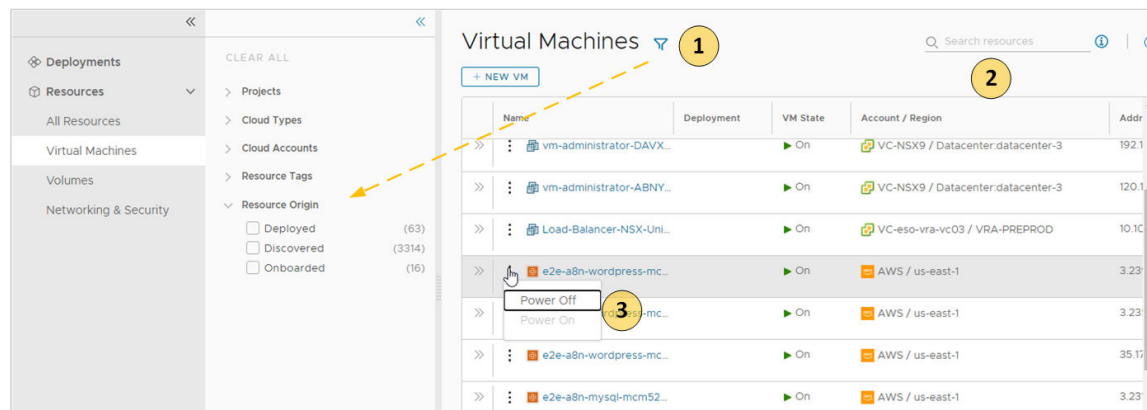
- **Netwerk en beveiliging**

Omvat netwerken, load balancers en beveiligingsgroepen.

Net zoals in de lijstweergave van implementaties kunt u de lijst filteren, een resourcetype selecteren, zoeken, sorteren en acties uitvoeren.

Als u op de resourcenaam klikt, kunt u met de resource werken in de context van de resourcedetails.

Figuur 7-3. Lijst op de pagina Resources



- 1 Filter uw lijst op basis van resourcekenmerken.

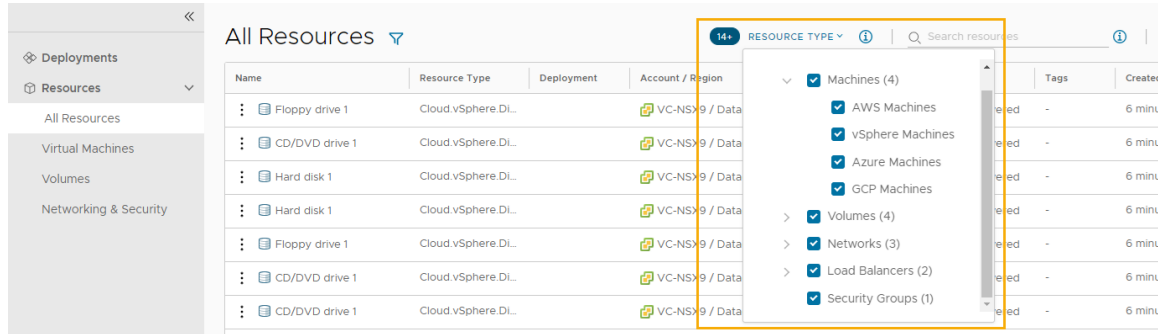
U kunt bijvoorbeeld filteren op basis van project, cloudtypen, oorsprong of andere kenmerken.

- 2 Zoek naar resources op basis van naam, accountregio's of andere waarden.

- 3 Voer beschikbare acties voor dag 2 uit die specifiek zijn voor het resourcetype en de resourcestatus.

U kunt bijvoorbeeld een gedetecteerde machine inschakelen als deze is uitgeschakeld. Of u kunt de grootte van een geonboarde machine wijzigen.

Naast de zoek- en filteropties op elke pagina bevat de pagina Alle resources een resourcetypekiezer waar u een filter kunt samenstellen voor alle resources.



Lijst van beheerde resources op basis van oorsprong

U kunt het tabblad Resources gebruiken om de volgende typen resources te beheren.

Tabel 7-3. Oorsprong van resource

Beheerde resource	Beschrijving
Geïmplementeerd	<p>Implementaties zijn volledig beheerde workloads die geïmplementeerde cloudsjablonen of geonboarde resources zijn. De workloadresources kunnen machines, opslagvolumes, netwerken, load balancers en beveiligingsgroepen zijn.</p> <p>U kunt uw implementaties in de sectie Implementaties of de sectie Resources beheren.</p>
Gedetecteerd	<p>Gedetecteerde resources zijn de machines, opslagvolumes, netwerken, load balancers en beveiligingsgroepen die het detectieproces heeft geïdentificeerd voor elke cloudaccountregio die u heeft toegevoegd.</p> <p>Alleen Cloud Assembly-beheerders kunnen gedetecteerde resources zien en beheren in de sectie Resources.</p>

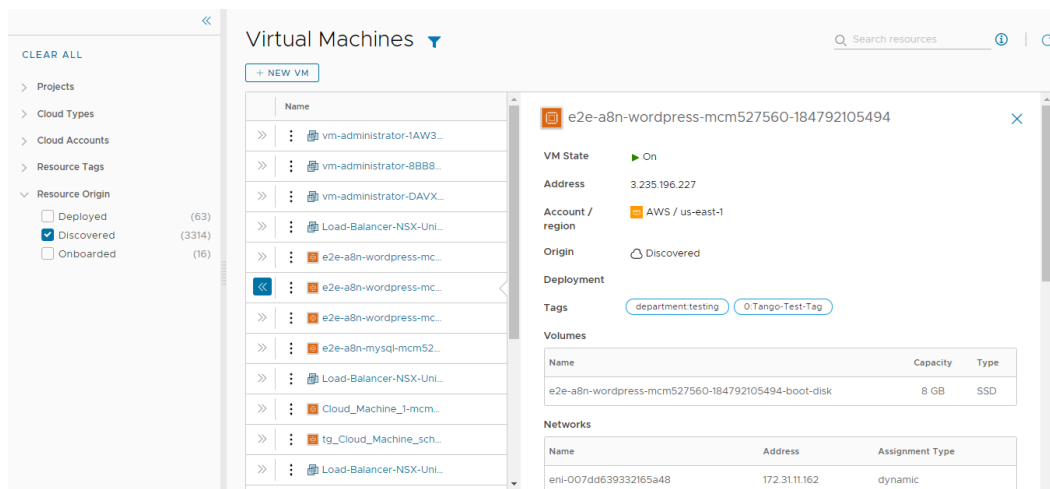
Tabel 7-3. Oorsprong van resource (vervolg)

Gemigreerd	<p>Gemigreerde resources zijn de 7.x-implementaties die u heeft gemigreerd naar vRealize Automation. De gemigreerde resources kunnen machines, opslagvolumes, netwerken, load balancers en beveiligingsgroepen zijn. Gemigreerde resources worden beheerd zoals implementaties.</p> <p>U kunt gemigreerde resources in de sectie Implementaties of de sectie Resources beheren.</p>
Onboarden is voltooid	<p>Geonboarde resources zijn gedetecteerde resources die u onder meer robuust vRealize Automation-beheer brengt. Geonboarde resources worden beheerd zoals implementaties.</p> <p>U kunt geonboarde resources in de sectie Implementaties of de sectie Resources beheren.</p>

Wat is de resourcedetailweergave

U kunt de resourcedetailweergave gebruiken om de geselecteerde resource dieper te bekijken. Afhankelijk van de resource kunnen de gegevens netwerken, poorten en andere informatie over de machine bevatten. De diepte van de informatie varieert afhankelijk van het type cloudaccount en de herkomst.

Als u het detailvenster wilt openen, klikt u op de resourcenaam of op de dubbele pijlen.

Figuur 7-4. Deelvenster met resourcedetails

Welke acties voor dag 2 kan ik uitvoeren op resources

De beschikbare acties voor dag 2 zijn afhankelijk van de oorsprong van de resource, het cloudaccount, het resourcetype en de status.

Tabel 7-4. Lijst van acties op basis van oorsprong

Oorsprong van resource	Acties voor dag 2
Geïmplementeerd	Welke acties beschikbaar zijn om op de resources uit te voeren, is afhankelijk van het resourcetype, het cloudaccount en de status. Zie Welke acties kan ik op Cloud Assembly-implementaties uitvoeren voor een gedetailleerde lijst.
Gedetecteerd	De beschikbare acties voor gedetecteerde resources zijn beperkt tot virtuele machines. Afhankelijk van de status kunt u de volgende acties uitvoeren. <ul style="list-style-type: none"> ■ Uitschakelen ■ Inschakelen Aanvullende vSphere-actie voor virtuele machines. <ul style="list-style-type: none"> ■ Verbinding maken met externe console
Gemigreerd	Gemigreerde resources hebben dezelfde beheeropties voor acties voor dag 2 als implementaties. Welke acties beschikbaar zijn om op de gemigreerde resources uit te voeren, is afhankelijk van het resourcetype, het cloudaccount en het beleid voor dag 2. Zie Welke acties kan ik op Cloud Assembly-implementaties uitvoeren voor een gedetailleerde lijst.
Onboarden is voltooid	Geonboarde resources hebben dezelfde beheeropties voor acties voor dag 2 als implementaties. Welke acties beschikbaar zijn om op de geonboarde resources uit te voeren, is afhankelijk van het resourcetype, het cloudaccount en de status. Zie Welke acties kan ik op Cloud Assembly-implementaties uitvoeren voor een gedetailleerde lijst.

Hoe werk ik met individuele resources in Cloud Assembly?

Als cloudbeheerder of projectlid met resources voor uw project kunt u de sectie Resources van het tabblad Resources gebruiken om uw geïmplementeerde, geonboarde en gemigreerde resources als individuele resources per resourcetype te beheren.

De werkstroom, die is gericht op het beheren van virtuele machines, biedt een handleiding voor het beheer van de levenscyclus van resources op hoog niveau die u kunt toepassen op de andere resourcetypes.

Resources van virtuele machine zoeken

Geïmplementeerde, geonboarde en gemigreerde virtuele machines zijn beschikbaar op de pagina Alle resources en op de pagina Virtuele machines op het tabblad Resources. Dit voorbeeld is gericht op virtuele machines, maar u kunt dezelfde werkstroom toepassen op de andere resourcetypes.

- 1 Selecteer **Resources > Resources > Virtuele machines**.
- 2 Zoek uw virtuele machine.

U kunt de filters of de zoekfunctie gebruiken om specifieke resources te vinden.

Virtual Machines 🔍 Search resources

[+ NEW VM](#)

	Name	Deployment	VM State	Account / Region	Address	Project	Origin	Tags
>>	vm-administrator-VLDX...		▶ On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
>>	vm-administrator-N6CE...		▶ On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...	192.167.211.142		Discovered	-
>>	mcm-20211203215331-0...	Google Cloud Create VM_6f...	▶ On	yingzhi-GCP / us-east1	34.74.168.22	Create VM Proj...	Deployed	-

De details van de virtuele machine controleren

De resourcedetails bieden een snelle weergave van de machine-informatie, inclusief netwerken, aangepaste eigenschappen en andere verzamelde informatie.

- 1 Zoek de machine in de lijst Virtuele machines.
- 2 Klik op de resourcenaam of de dubbele pijlen in de linkerkolom van de tabel.

Het detailvenster wordt geopend aan de rechterkant van de lijst.

Virtual Machines 🔍 Search resources

[+ NEW VM](#)

	Name
>>	vm-administrator-VLDX...
>>	vm-administrator-N6CE...
<<	mcm-20211203215331-0...
>>	vm-administrator-7COL...
>>	vm-administrator-Q628...
>>	vm-administrator-BBJM...
>>	vm-administrator-7RQZ...
>>	vm-administrator-BON...
>>	vm-administrator-2M3...
>>	vm-administrator-BSKX...
>>	Load-Balancer-NSX-Uni...
>>	vm-administrator-X4FT...
>>	vm-administrator-GLA...
>>	vm-administrator-757X...
>>	Load-Balancer-NSX-Uni...
>>	e2e-a8n-mcm545178-18...
>>	mcm-20211203165342-...
>>	Load-Balancer-NSX-Uni...
>>	TimWin7-LinkedClone...

1-20 / 3555

mcm-20211203215331-000020

VM State ▶ On

Address 34.74.168.22

Account / region yingzhi-GCP / us-east1

Origin Deployed

Deployment Google Cloud Create VM_6f6d0315-ddc8-4f5d-9e1e-563c149a836d

Tags

Volumes

Name	Capacity	Type
create-vm-new-disk-1-524598563851	4 GB	HDD
mcm-20211203215331-000020	10 GB	HDD

Networks

Name	Address	Assignment Type
default	10.142.0.56	dynamic

Custom Properties

Name	Value
resourceId	3b43b1a6-105c-4d68-8562-f84d545d07a0
zone_overlapping_migrated	true
project	d952119a-7354-4dc2-afd5-718755917230
zone	us-east1-b
environmentName	Google Cloud Platform
providerId	1393403671676923083
id	/resources/compute/3b43b1a6-105c-4d68-8562-f84d545d07a0

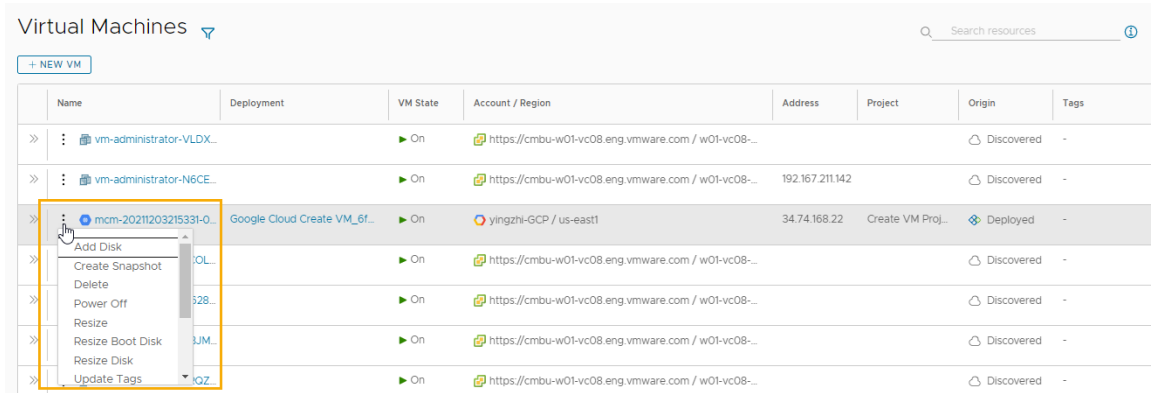
- 3 Als u het deelvenster wilt sluiten, klikt u op de dubbele pijlen of de resourcenaam.

Acties voor dag 2 uitvoeren op de virtuele machine

U gebruikt de acties voor dag 2 om uw resources te beheren. Welke acties beschikbaar zijn, is afhankelijk van het resourcetype, de status van de resource en het actiebeleid voor dag 2 dat wordt afgedwongen.

- 1 Zoek de machine in de lijst Virtuele machines.
- 2 Klik op de verticale drie punten om de beschikbare acties te bekijken.

3 Klik op de actie.



Name	Deployment	VM State	Account / Region	Address	Project	Origin	Tags
vm-administrator-VLDX...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-N6CE...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...	192.167.211.142		Discovered	-
mcm-20211203215331-0...	Google Cloud Create VM_6f...	On	yingzhi-GCP / us-east1	34.74.168.22	Create VM Proj...	Deployed	-
...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-

Hoe werk ik met gedetecteerde resources in Cloud Assembly?

Als Cloud Assembly-beheerder gebruikt u de sectie Resources van het tabblad Resources om uw gedetecteerde machines te beheren. Alleen beheerders zien gedetecteerde resources op de verschillende pagina's.

Deze werkstroom is gericht op het beheren van gedetecteerde virtuele machines.

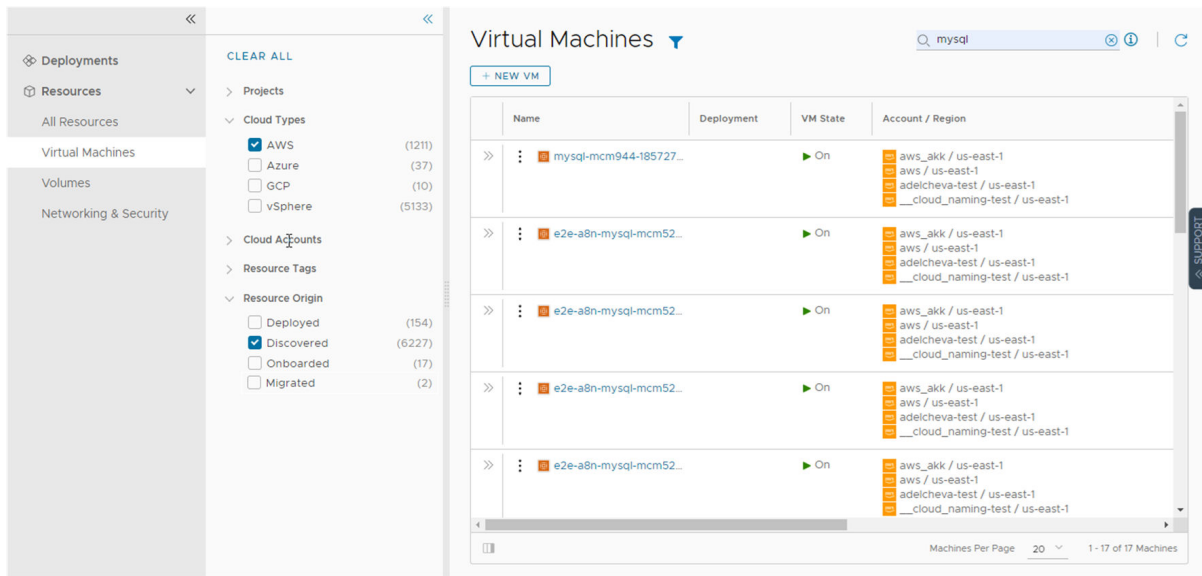
Wat moet u eerst doen

- Voeg een cloudaccount toe voor de resources die u wilt detecteren. In deze werkstroom wordt een Amazon Web Services-machine als voorbeeld gebruikt. Zie [Cloudaccounts aan Cloud Assembly toevoegen](#) om een cloudaccount toe te voegen.

Gedetecteerde virtuele machines zoeken

Gedetecteerde resources worden verzameld uit de cloudaccountregio en toegevoegd aan de resources op het tabblad Resource. Dit voorbeeld richt zich op virtuele machines, maar er worden andere resourcetypes verzameld, waaronder opslag- en netwerkinformatie.

- 1 Selecteer **Resources > Resources > Virtuele machines**.



- Als u de virtuele AWS-machines wilt vinden, klikt u op het pictogram **Filter** bij het paginalabel
- Vouw **Cloudtypen** uit in de filterlijst en selecteer **AWS**.

De lijst is nu beperkt tot de virtuele AWS-machines. U kunt geïmplementeerde, gedetecteerde en andere oorsprongtypen zien.

- Vouw **Oorsprong van resource** uit in de filterlijst en selecteer **Gedetecteerd**.

De lijst is nu beperkt tot de gedetecteerde virtuele AWS-machines.

- Om een specifieke machine te vinden, kunt u de optie **Resources gebruiken** gebruiken om te zoeken op naam, IP-adres, tags of waarden.

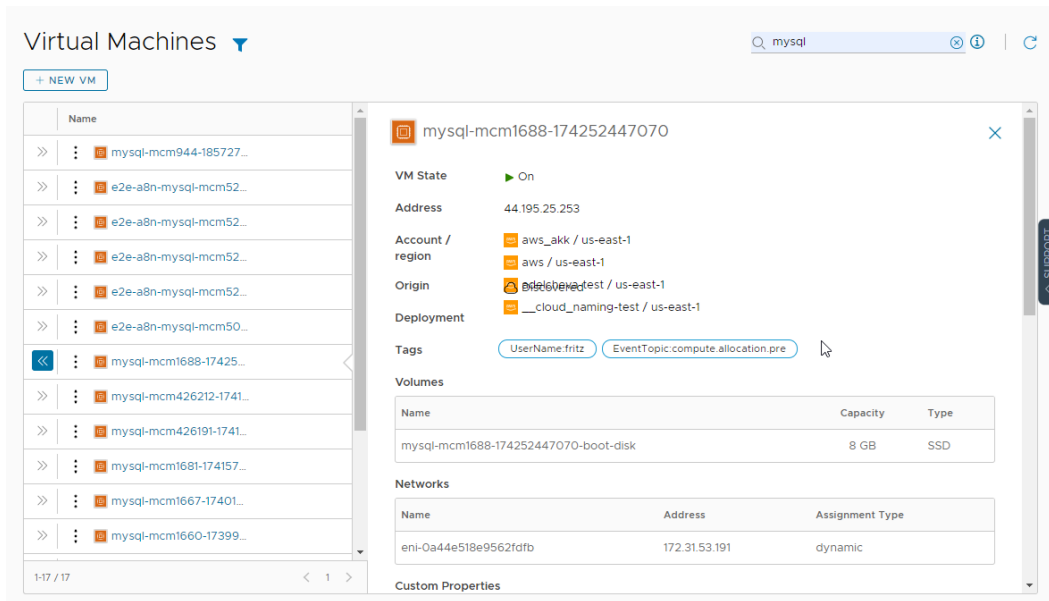
In dit voorbeeld is **mysql** de zoekterm.

Details van virtuele machine controleren

De resourcedetails bevatten alle verzamelde informatie voor de resource. U kunt deze informatie gebruiken om de resource en alle koppelingen met andere resources te begrijpen.

- Zoek de virtuele machine in de lijst met virtuele machines.
- Als u de resourcedetails wilt weergeven, klikt u op de machinenaam of klikt u op de dubbele pijlen in de linkerkolom.

Het detailvenster wordt geopend aan de rechterkant van de lijst.



- Controleer de details, waaronder opslag, netwerken, aangepaste eigenschappen en andere verzamelde informatie.
- Als u het deelvenster wilt sluiten, klikt u op de dubbele pijlen of klikt u op de resourcenaam.

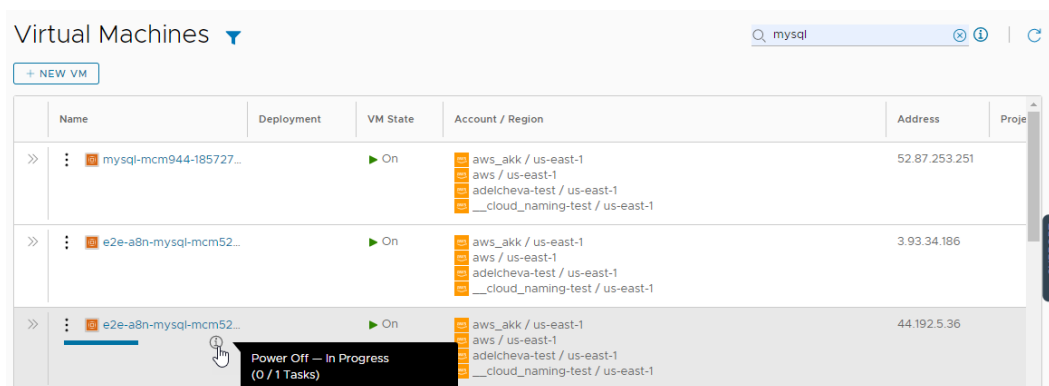
Acties voor dag 2 uitvoeren op de virtuele machine

U gebruikt de acties voor dag 2 om de resources te beheren. Tot de huidige acties voor gedetecteerde virtuele machines horen Inschakelen en Uitschakelen. Als u een virtuele vSphere-machine beheert, kunt u ook Verbinding maken met externe console uitvoeren.

- Zoek de machine in de lijst Virtuele machines.
- Klik op de verticale drie punten om de beschikbare acties te bekijken.

De mogelijke acties voor een virtuele AWS-machine zijn Uitschakelen en Inschakelen. Inschakelen is niet actief omdat de machine al is ingeschakeld.

- Klik op **Uitschakelen** en dien de aanvraag in.



Wanneer het proces is voltooid, wordt de machine uitgeschakeld. U kunt deze nu weer inschakelen.

Wat kan ik nog meer doen met de gedetecteerde virtuele machine

Als u gedetecteerde resources onder volledig beheer wilt brengen, kunt u deze onboarden. Zie [Wat zijn onboardingplannen in Cloud Assembly](#).