

# VMware vRealize Orchestrator installeren en configureren

6 OKTOBER 2020

vRealize Orchestrator 8.2

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](http://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](http://www.vmware.com/nl)

Copyright © 2008-2020 VMware, Inc. Alle rechten voorbehouden. [Informatie over copyright en handelsmerken.](#)

# Inhoud

## VMware vRealize Orchestrator installeren en configureren 6

### 1 Inleiding tot VMware vRealize Orchestrator 7

- Belangrijke functies van het Orchestrator-platform 7
- vRealize Orchestrator-gebruikersrollen 10
- vRealize Orchestrator-architectuur 11
- vRealize Orchestrator-invoegtoepassingen 12

### 2 Systeemvereisten voor vRealize Orchestrator 13

- Hardwarevereisten voor de vRealize Orchestrator Appliance 13
- Browsers die worden ondersteund door vRealize Orchestrator 14
- vRealize Orchestrator-database 14
- vRealize Orchestrator Appliance-onderdelen 14
- Niveau van ondersteuning voor internationalisatie en lokalisatie 14
- vRealize Orchestrator-poorten en -endpoints 15

### 3 vRealize Orchestrator-onderdelen instellen 17

- vCenter Server-configuratie 17
- Verificatiemethoden 18

### 4 vRealize Orchestrator installeren 19

- De vRealize Orchestrator Appliance downloaden en implementeren 19
- De vRealize Orchestrator Appliance inschakelen en de startpagina openen 21
- De duur van het rootwachtwoord wijzigen 21
- SSH-toegang tot de vRealize Orchestrator Appliance in- of uitschakelen 21

### 5 Initiële configuratie 23

- Een standalone vRealize Orchestrator-server configureren 23
  - Een standalone vRealize Orchestrator-server configureren met vRealize Automation-verificatie 23
  - Een standalone vRealize Orchestrator-server configureren met vSphere-verificatie 25
- vRealize Orchestrator-functies inschakelen met licenties 26
- vRealize Orchestrator-databaseverbinding 27
- Certificaten beheren 27
  - vRealize Orchestrator-certificaten beheren 27
- De vRealize Orchestrator-invoegtoepassingen configureren 32
  - vRealize Orchestrator-invoegtoepassingen beheren 32
  - Een vRealize Orchestrator-invoegtoepassing installeren of bijwerken 33

Een invoegtoepassing verwijderen	34
Beschikbaarheid en schaalbaarheid van vRealize Orchestrator	34
Een vRealize Orchestrator-cluster configureren	35
Een vRealize Orchestrator-clusterknooppunt verwijderen	37
Een standalone vRealize Orchestrator-implementatie uitschalen	37
Een vRealize Orchestrator-cluster controleren	39
Het Customer Experience Improvement Program configureren	39
Categorieën van informatie die VMware ontvangt	39
Deelnemen aan het Customer Experience Improvement Program	40
<b>6 De vRealize Orchestrator API-services gebruiken</b>	<b>41</b>
SSL-certificaten beheren via de REST API	41
Een TLS-certificaat verwijderen met behulp van de REST API	42
TLS-certificaten importeren met behulp van de REST API	42
Een sleutelarchief maken met behulp van de REST API	44
Een sleutelarchief verwijderen met behulp van de REST API	44
Een sleutel toevoegen met behulp van de REST API	45
<b>7 Aanvullende configuratieopties</b>	<b>46</b>
Verificatie opnieuw configureren	46
De verificatieprovider wijzigen	46
De verificatieparameters wijzigen	47
De eigenschappen voor werkstroomuitvoeringen configureren	47
vRealize Orchestrator-logboekbestanden	48
Persistentie van logboekregistratie	48
Configuratie van vRealize Orchestrator-logboeken	49
Integratie van logboekregistratie met vRealize Log Insight configureren	49
Een syslog-integratie in vRealize Orchestrator maken of overschrijven	50
Logboekregistratie voor Kerberos-foutopsporing inschakelen	52
OpenTracing- en Wavefront-extensies inschakelen	53
De OpenTracing-extensie configureren	53
De Wavefront-extensie configureren	54
Tijdssynchronisatie voor vRealize Orchestrator inschakelen	55
Tijdssynchronisatie voor vRealize Orchestrator uitschakelen	57
<b>8 Toepassingsvoorbeelden voor configuratie en probleemoplossing</b>	<b>58</b>
vRealize Orchestrator-invoegtoepassing voor vSphere Web Client configureren	58
Actieve werkstromen annuleren	59
Foutopsporing voor de vRealize Orchestrator-server inschakelen	60
De grootte van de vRealize Orchestrator Appliance-schijven wijzigen	62
De grootte van het heapgeheugen van de vRealize Orchestrator-server aanpassen	63

Noodherstel van vRealize Orchestrator met behulp van Site Recovery Manager 65

Virtuele machines voor vSphere Replication configureren 65

Protection groups maken 66

Een herstelplan maken 68

Herstelplannen in mappen indelen 69

Een herstelplan bewerken 70

## 9 Systeemeigenschappen instellen 71

Toegang tot het serverbestandssysteem instellen voor werkstromen en acties 71

Regels in het bestand js-io-rights.conf die schrijftoegang tot het vRealize Orchestrator-systeem toestaan 71

Toegang tot bestandssysteem op server instellen voor werkstromen en acties 72

Toegang tot opdrachten van het besturingssysteem instellen voor werkstromen en acties 73

JavaScript-toegang tot Java-klassen instellen 74

Aangepaste time-outeigenschap instellen 75

Een JDBC-connector toevoegen voor de SQL-invoegtoepassing voor vRealize Orchestrator 76

## 10 Wat is de volgende stap 78

# VMware vRealize Orchestrator installeren en configureren

*VMware vRealize Orchestrator installeren en configureren* biedt u informatie en instructies over het installeren en configureren van VMware® vRealize Orchestrator.

## Doelgroep

Deze informatie is bedoeld voor ervaren vSphere-beheerders en systeembeheerders die vertrouwd zijn met de technologie van virtuele machines en datacentrumbewerkingen.

# Inleiding tot VMware vRealize Orchestrator

# 1

VMware vRealize Orchestrator is een platform voor ontwikkeling en procesautomatisering dat een bibliotheek met uitbreidbare werkstromen biedt om u in staat te stellen geautomatiseerde, configureerbare processen te maken en uit te voeren om VMware-producten en andere technologieën van derden te beheren.

vRealize Orchestrator automatiseert beheer- en operationele taken van zowel VMware-applicaties als applicaties van derden, zoals servicedesks, wijzigingsbeheersystemen en IT-assetbeheersystemen.

Dit hoofdstuk omvat de volgende onderwerpen:

- [Belangrijke functies van het Orchestrator-platform](#)
- [vRealize Orchestrator-gebruikersrollen](#)
- [vRealize Orchestrator-architectuur](#)
- [vRealize Orchestrator-invoegtoepassingen](#)

## Belangrijke functies van het Orchestrator-platform

vRealize Orchestrator bestaat uit drie verschillende lagen: een orkestratieplatform dat de gemeenschappelijke functies biedt die nodig zijn voor een orkestratietool, een invoegtoepassingsarchitectuur om het beheer van subsystemen te integreren en een bibliotheek met werkstromen. vRealize Orchestrator is een open platform dat kan worden uitgebreid met nieuwe invoegtoepassingen en inhoud, en kan worden geïntegreerd in grotere architecturen via een REST API.

vRealize Orchestrator bevat verschillende belangrijke functies die helpen bij het uitvoeren en beheren van werkstromen.

### Persistentie

Een PostgreSQL-database met productiekwaliteit wordt gebruikt om relevante informatie op te slaan, zoals processen, werkstroomstaten en de configuratie van de vRealize Orchestrator.

### Centraal beheer

vRealize Orchestrator biedt een centraal hulpprogramma om uw processen te beheren. Het platform van de applicatieserver, met de volledige versiegeschiedenis, kan scripts en procesgerelateerde primitieven in dezelfde opslaglocatie opslaan. Op deze manier kunt u scripts zonder versiebeheer en het correct besturen van wijzigingen voor uw servers voorkomen.

### **Plaatsing van controlepunten**

Elke stap van een werkstroom wordt opgeslagen in de database, waardoor gegevensverlies wordt voorkomen als u de server opnieuw moet opstarten. Deze functie is vooral nuttig voor langlopende processen.

### **Control Center**

Control Center is een webgebaseerde portal die de beheerefficiëntie van vRealize Orchestrator-instanties vergroot door een gecentraliseerde beheerinterface te bieden voor runtimebewerkingen, werkstroombewaking en correlatie tussen de werkstroomuitvoeringen en systeembronnen.

### **Versiebeheer**

Alle vRealize Orchestrator-platformobjecten hebben een gekoppelde versiegeschiedenis. Versiegeschiedenis is handig voor basiswijzigingsbeheer bij het distribueren van processen naar projectfasen of locaties.

### **Git-integratie**

Met de vRealize Orchestrator Client kunt u een Git-opslagplaats integreren om de versie en broncontrole van uw vRealize Orchestrator-inhoud verder te verbeteren. Met Git kunt u de werkstroomontwikkeling beheren voor meerdere vRealize Orchestrator-instanties. Raadpleeg *Git gebruiken met de vRealize Orchestrator-client* in de handleiding *De VMware vRealize Orchestrator-client gebruiken*.

### **Scriptverwerkingsengine**

De Mozilla Rhino JavaScript-engine biedt een manier om bouwstenen te maken voor het vRealize Orchestrator Client-platform. De scriptverwerkingsengine is verbeterd met basisversiecontrole, controle van variabeletypen, naamruimtebeheer en afhandeling van uitzonderingen. De engine kan worden gebruikt in de volgende bouwstenen:

- Acties
- Werkstromen
- Beleid

### **Werkstroomengine**



De werkstroomengine stelt u in staat om bedrijfsprocessen te automatiseren. De volgende objecten worden gebruikt voor het maken van een stapsgewijze procesautomatisering in werkstromen:

- Werkstromen en acties die vRealize Orchestrator Client biedt.
- Aangepaste bouwstenen die door de klant zijn gemaakt.
- Objecten die invoegtoepassingen aan vRealize Orchestrator Client toevoegen.

Gebruikers, andere werkstromen, schema's of beleidsregels kunnen werkstromen starten.

## Beleidsengine

U kunt de beleidsengine gebruiken om gebeurtenissen te controleren en te genereren om te reageren op veranderende voorwaarden in de vRealize Orchestrator Client-server of een technologie met invoegtoepassingen. Beleidsregels kunnen gebeurtenissen van het platform of de invoegtoepassingen samenvoegen, zodat u het wijzigen van de voorwaarden voor een van de geïntegreerde technologieën kunt afhandelen.

## vRealize Orchestrator Client

Maak, gebruik, bewerk en bewaak werkstromen met de vRealize Orchestrator Client. U kunt ook de vRealize Orchestrator Client gebruiken om elementen voor acties, configuraties, beleidsregels en bronnen te beheren. Zie *De vRealize Orchestrator-client gebruiken*.

## Ontwikkeling en bronnen

De landingspagina voor vRealize Orchestrator biedt snelle toegang tot resources om u te helpen bij het ontwikkelen van uw eigen invoegtoepassingen, voor gebruik in vRealize Orchestrator. U vindt ook informatie over het gebruik van de vRealize Orchestrator REST API om aanvragen naar de vRealize Orchestrator-server te verzenden.

## Beveiliging

vRealize Orchestrator biedt de volgende geavanceerde beveiligingsfuncties:

- PKI (Public Key Infrastructure) om inhoud die is geïmporteerd en geëxporteerd tussen servers te ondertekenen en versleutelen.
- DRM (Digital Rights Management) om te bepalen hoe geëxporteerde inhoud kan worden bekeken, bewerkt en geherdistribueerd.
- TLS (Transport Layer Security) om versleutelde communicatie tussen de vRealize Orchestrator Client, vRealize Orchestrator-server en HTTPS-toegang tot de webfrontend te bieden.
- Geavanceerd beheer van toegangsrechten om controle te krijgen over toegang tot processen en de objecten die door deze processen worden gemanipuleerd.

## Versleuteling

vRealize Orchestrator gebruikt een FIPS-compatibele AES (Advanced Encryption Standard) met een 256-bits coderingssleutel voor versleuteling van tekenreeksen. De coderingssleutel

wordt willekeurig gegenereerd en is uniek voor alle toepassingen die geen deel uitmaken van een cluster. Alle knooppunten in een cluster delen een coderingssleutel.

## vRealize Orchestrator-gebruikersrollen

vRealize Orchestrator biedt verschillende tools en interfaces op basis van de specifieke verantwoordelijkheden van de globale gebruikersrollen. In vRealize Orchestrator kunt u gebruikers met volledige rechten hebben, die deel uitmaken van de beheerdersgroep (**beheerders**), ontwikkelaars (**werkstroomontwikkelaars**) en gebruikers met beperkte toegang.

## vRealize Orchestrator-rollen en -verantwoordelijkheden

vRealize Orchestrator-gebruikersrollen worden beheerd in het menu **Rollenbeheer** van de vRealize Orchestrator Client. Voor meer informatie over het configureren van gebruikersrollen in de vRealize Orchestrator Client raadpleegt u *Rollen toewijzen in de vRealize Orchestrator-client* in de handleiding *De VMware vRealize Orchestrator-client gebruiken*.

---

**Opmerking** Voor vRealize Orchestrator-implementaties die zijn geverifieerd met vRealize Automation of met een vRealize Automation-licentie, worden gebruikersrollen toegewezen met de service Identiteits- en toegangsbeheer van het vRealize Automation-platform. Zie *vRealize Orchestrator-clientrollen in vRealize Automation configureren* in *VMware vRealize Orchestrator-client gebruiken*.

---

### Beheerder

Deze gebruiker heeft volledige toegang tot alle vRealize Orchestrator-platformmogelijkheden en -inhoud, inclusief inhoud die door specifieke groepen is gemaakt. De gebruikersverantwoordelijkheden van de primaire beheerder zijn onder meer:

- vRealize Orchestrator installeren en configureren.
- Gebruikers toevoegen aan de vRealize Orchestrator Client, rollen toewijzen en groepen maken en verwijderen. Zie *Groepen in de vRealize Orchestrator-client maken* in *VMware vRealize Orchestrator-client gebruiken*.
- Maak een integratie met een Git-opslagplaats voor de ontwikkelaars in hun vRealize Orchestrator-omgeving. Zie *Een verbinding met een Git-opslagplaats configureren* in *VMware vRealize Orchestrator-client gebruiken*.
- Problemen met de vRealize Orchestrator-omgeving oplossen via functies zoals werkstroomvalidatie en scripts voor foutopsporing in werkstromen.

### Werkstroomontwikkelaar

Deze gebruiker kan de functionaliteit van het vRealize Orchestrator-platform uitbreiden door objecten te maken en te bewerken. Werkstroomontwikkelaars hebben geen toegang tot de

functies voor beheer en probleemoplossing van de vRealize Orchestrator Client. De belangrijkste verantwoordelijkheden van de werkstroomontwikkelaar zijn:

- Het maken, bewerken, uitvoeren en verwijderen van vRealize Orchestrator-objecten zoals werkstromen, acties, beleidsregels en configuratie-elementen.
- Werkstroomuitvoeringen plannen. Zie *Werkstromen in vRealize Orchestrator-client plannen* in *VMware vRealize Orchestrator-client gebruiken*.
- Voeg inhoud die door de werkstroomontwikkelaar is gemaakt, toe aan groepen waaraan deze is toegewezen.
- Lokale wijzigingen in de vRealize Orchestrator-inhoudsinventaris pushen naar de Git-opslagplaats voor verbinding. Zie *Wijzigingen naar Git-opslagplaats pushen* in *VMware vRealize Orchestrator-client gebruiken*.

### Gebruikers met beperkte rechten

Gebruikers zonder een toegewezen rol kunnen zich nog steeds aanmelden bij de vRealize Orchestrator Client, maar hebben beperkte toegang tot clientfuncties en inhoud. Als ze aan een groep zijn toegewezen, kan deze gebruiker inhoud die is opgenomen in die groep, bekijken en uitvoeren.

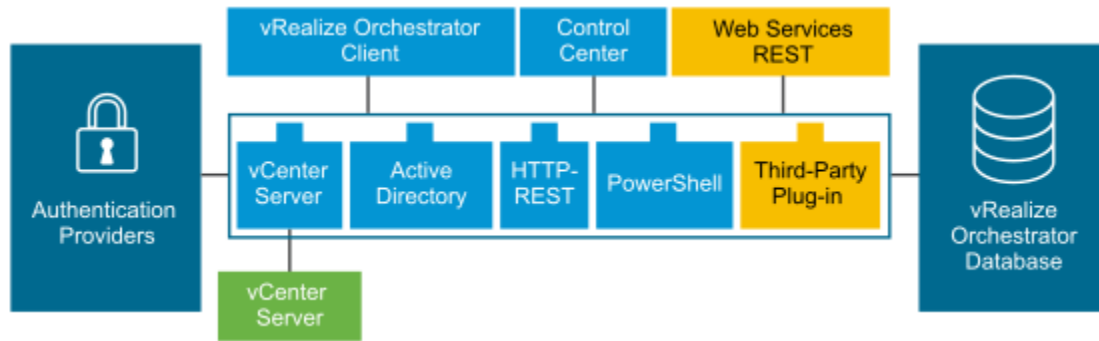
## vRealize Orchestrator-architectuur

vRealize Orchestrator bevat een werkstroombibliotheek en een werkstroomengine zodat u werkstromen kunt maken en uitvoeren die orkestratieprocessen automatiseren. U voert werkstromen op de objecten van andere technologieën uit waartoe vRealize Orchestrator toegang heeft via een reeks invoegtoepassingen.

vRealize Orchestrator biedt een standaardset invoegtoepassingen, waaronder een invoegtoepassing voor vCenter Server, zodat u taken kunt organiseren in de verschillende omgevingen die de invoegtoepassingen beschikbaar stellen.

vRealize Orchestrator biedt ook een open architectuur voor het invoegen van toepassingen van derden in het orkestratieplatform. U kunt de werkstromen uitvoeren op de objecten van de ingevoegde technologieën die u zelf definieert. vRealize Orchestrator maakt verbinding met een verificatieprovider om gebruikersaccounts te beheren, en met een vooraf geconfigureerde PostgreSQL-database om informatie op te slaan voor de werkstromen die ermee worden uitgevoerd. U kunt vRealize Orchestrator, de objecten die worden getoond, en de vRealize Orchestrator-werkstromen vinden via de vRealize Orchestrator Client, of via de webservices. Bewaking en configuratie van vRealize Orchestrator-werkstromen en services vindt plaats via de vRealize Orchestrator Client en het Control Center.

Figuur 1-1. VMware vRealize Orchestrator-architectuur



## vRealize Orchestrator-invoegtoepassingen

Met invoegtoepassingen kunt u vRealize Orchestrator gebruiken om toegang te krijgen tot externe technologieën en toepassingen en deze te beheren. Doordat een externe technologie beschikbaar wordt gemaakt in een vRealize Orchestrator-invoegtoepassing, kunt u objecten en functies opnemen in werkstromen die toegang krijgen tot de objecten en functies van de externe technologie.

De externe technologieën waartoe u toegang heeft via invoegtoepassingen, omvatten beheertools voor virtualisatie, e-mailsystemen, databases, directoryservices en interfaces voor extern beheer.

vRealize Orchestrator biedt een set standaardinvoegtoepassingen die u kunt gebruiken om in werkstromen te integreren, zoals de VMware vCenter Server API en e-mailmogelijkheden. Met de invoegtoepassingen kunt u de levering van nieuwe IT-services automatiseren of de mogelijkheden van bestaande infrastructuur en applicatieservices aanpassen. U kunt bovendien de open vRealize Orchestrator-architectuur voor invoegtoepassingen gebruiken om invoegtoepassingen te maken voor toegang tot andere toepassingen.

De vRealize Orchestrator-invoegtoepassingen die VMware ontwikkelt, worden gedistribueerd als .vmoapp-bestanden. Zie [Externe vRealize Orchestrator-invoegtoepassingen](#) voor meer informatie over de vRealize Orchestrator-invoegtoepassingen die VMware ontwikkelt en distribueert. Raadpleeg [VMware Solution Exchange](#) voor meer informatie over vRealize Orchestrator-invoegtoepassingen van derden.

# Systeemvereisten voor vRealize Orchestrator

## 2

Uw systeem moet voldoen aan de technische vereisten die nodig zijn om vRealize Orchestrator correct te laten werken.

Raadpleeg [VMware Product Interoperability Matrix](#) voor een lijst met ondersteunde versies van vCenter Server, de vSphere Web Client, vRealize Automation en andere VMware oplossingen.

Dit hoofdstuk omvat de volgende onderwerpen:

- [Hardwarevereisten voor de vRealize Orchestrator Appliance](#)
- [Browsers die worden ondersteund door vRealize Orchestrator](#)
- [vRealize Orchestrator-database](#)
- [vRealize Orchestrator Appliance-onderdelen](#)
- [Niveau van ondersteuning voor internationalisatie en lokalisatie](#)
- [vRealize Orchestrator-poorten en -endpoints](#)

## Hardwarevereisten voor de vRealize Orchestrator Appliance

De vRealize Orchestrator Appliance is een vooraf geconfigureerde op Photon gebaseerde virtuele machine die in containers wordt uitgevoerd. Voordat u de appliance implementeert, controleert u of uw systeem voldoet aan de minimale hardwarevereisten.

De vRealize Orchestrator Appliance heeft de volgende hardwarevereisten:

- 4 CPU's
- 12 GB geheugen
- 200 GB harde schijf

Verklein de standaardgrootte van het geheugen niet, omdat de vRealize Orchestrator-server minimaal 8 GB aan vrij geheugen vereist.

## Browsers die worden ondersteund door vRealize Orchestrator

Controleer of uw browsers vRealize Orchestrator ondersteunen.

Om toegang te krijgen tot de vRealize Orchestrator Client en Control Center, moet u een van de volgende browsers gebruiken:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome

## vRealize Orchestrator-database

De vRealize Orchestrator-server bevat een vooraf geconfigureerde PostgreSQL-database die gereed is voor productie.

## vRealize Orchestrator Appliance-onderdelen

De vRealize Orchestrator Appliance is een Photon-gebaseerde virtual appliance die in containers wordt uitgevoerd.

De vRealize Orchestrator Appliance omvat de volgende onderdelen:

- Een Kubernetes-laag op infrastructuurniveau.
- Een vooraf geconfigureerde PostgreSQL-database.
- De belangrijkste vRealize Orchestrator-services: de serverservice, de Control Center-service en de orkestratie-UI-service.

De standaard vRealize Orchestrator Appliance-databaseconfiguratie is gereed voor productie.

---

**Opmerking** Als u de vRealize Orchestrator Appliance in een productieomgeving wilt gebruiken, moet u de vRealize Orchestrator-server configureren om te verifiëren via vRealize Automation of vSphere. Zie [Een standalone vRealize Orchestrator-server configureren](#).

---

## Niveau van ondersteuning voor internationalisatie en lokalisatie

Het vRealize Orchestrator Control Center en vRealize Orchestrator Client bevatten ondersteuning voor niet-Engelse besturingssystemen, niet-Engelse gegevensopmaak en ondersteuning voor meerdere talen voor het Control Center en de clientgebruikersinterface.

Het vRealize Orchestrator Control Center en vRealize Orchestrator Client ondersteunen het gebruik van niet-Engelse besturingssystemen, niet-Engelse invoer en uitvoer en ondersteuning voor niet-Engelse opmaak van gegevens zoals datums, tijden en nummers.

De gebruikersinterfaces van de vRealize Orchestrator en vRealize Orchestrator Client worden gelokaliseerd in de volgende talen:

- Spaans
- Frans
- Duits
- Traditioneel Chinees
- Vereenvoudigd Chinees
- Koreaans
- Japans
- Italiaans
- Nederlands
- Braziliaans-Portugees
- Russisch

## vRealize Orchestrator-poorten en -endpoints

De vRealize Orchestrator Kubernetes-service omvat twee endpoints en verschillende hoofdnetwerkpoorten.

### vRealize Orchestrator-netwerkpoorten en -endpoints

U hebt toegang tot vRealize Orchestrator via poort 443. De 443-poort wordt beveiligd met een zelfondertekend certificaat dat wordt gegenereerd tijdens de installatie en kan niet worden vervangen door de gebruiker. Wanneer u een externe load balancer gebruikt, moet deze zijn ingesteld op poort 443.

Protocol	Poortnummer	Beschrijving
TCP	22	Poort die wordt gebruikt om toegang te krijgen tot de vRealize Orchestrator Appliance via SSH.
TCP	443	Poort die wordt gebruikt om toegang te krijgen tot vRealize Orchestrator.
TCP	2379	Interne poort die wordt gebruikt door het etcd-sleutel-waardearchief.
TCP	2380	Interne poort die wordt gebruikt door het etcd-sleutel-waardearchief.
TCP	6443	Interne poort die wordt gebruikt door de kube-apiserver-API-server.
TCP	8008	Interne poort die wordt gebruikt door de kube-proxy-netwerkproxy.

Protocol	Poortnummer	Beschrijving
TCP	10250	Poort die wordt gebruikt door de kubelet-agent.
TCP	16000	Interne poort.
TCP	20849	Interne poort.
TCP	30333	Interne poort die wordt gebruikt door de mitm proxy-service.
TCP	30821	Interne poort.
TCP	31090	Interne poort.
UDP	500	Interne poort die wordt gebruikt door de IKE-verkeersservice (Internal Key Exchange).
UDP	4500	Interne poort die wordt gebruikt door de NAT-service (Network Address Transition).
UDP	8285	Interne poort die wordt gebruikt door de kube-proxy-netwerkproxy.

U hebt toegang tot de vRealize Orchestrator-clientservices en Control Center-services op de volgende endpoints:

`https://uw_orchestrator_FQDN/orchestration-ui`

`https://uw_orchestrator_FQDN/vco-controlcenter`



# vRealize Orchestrator-onderdelen instellen

## 3

Wanneer u de vRealize Orchestrator Appliance downloadt en implementeert, is de vRealize Orchestrator-server vooraf geconfigureerd. Na de implementatie worden de services automatisch gestart.

Volg deze richtlijnen om de beschikbaarheid en schaalbaarheid van uw vRealize Orchestrator-installatie te verbeteren:

- Installeer en configureer een verificatieprovider en configureer vRealize Orchestrator om met de provider te werken. Zie [Een standalone vRealize Orchestrator-server configureren](#).
- Voor geclusterde vRealize Orchestrator-omgevingen installeert en configureert u een server met load balancer en configureert u deze om de workload tussen de vRealize Orchestrator-servers te verdelen.

Dit hoofdstuk omvat de volgende onderwerpen:

- [vCenter Server-configuratie](#)
- [Verificatiemethoden](#)

## vCenter Server-configuratie

Het verhogen van het aantal vCenter Server-instanties in uw vRealize Orchestrator-configuratie zorgt ervoor dat vRealize Orchestrator meer sessies beheert. Te veel actieve sessies kunnen ervoor zorgen dat vRealize Orchestrator time-outs ondervindt wanneer er meer dan 10 vCenter Server-verbindingen zijn.

Zie de [VMware Product Interoperability Matrix](#) voor een lijst met ondersteunde versies van vCenter Server.

---

**Opmerking** Als uw netwerk over voldoende bandbreedte en latentie beschikt, kunt u meerdere vCenter Server-instanties uitvoeren op verschillende virtual machines in uw vRealize Orchestrator-configuratie. Als u LAN gebruikt om de communicatie tussen vRealize Orchestrator en vCenter Server te verbeteren, is een 100 MB regel verplicht.

---

## Verificatiemethoden

Om gebruikersrechten te verifiëren en beheren, moet vRealize Orchestrator verbinding maken met een vRealize Automation- of vSphere-serverinstantie.

Wanneer u vRealize Orchestrator Appliance downloadt en implementeert, moet u de server configureren met een vRealize Automation- of vSphere-verificatie. Zie [Een standalone vRealize Orchestrator-server configureren](#).

---

**Opmerking** vRealize Orchestrator 8.x-verificatie met vRealize Automation wordt alleen ondersteund met vRealize Automation 8.x.

---

# vRealize Orchestrator installeren

# 4

vRealize Orchestrator bestaat uit een serveronderdeel en een clientonderdeel.

Om vRealize Orchestrator te gebruiken, moet u de vRealize Orchestrator Appliance implementeren en de vRealize Orchestrator-server configureren.

U kunt de standaardinstellingen voor configuratie van vRealize Orchestrator wijzigen met behulp van het vRealize Orchestrator Control Center.

Dit hoofdstuk omvat de volgende onderwerpen:

- [De vRealize Orchestrator Appliance downloaden en implementeren](#)

## De vRealize Orchestrator Appliance downloaden en implementeren

Voordat u toegang krijgt tot de vRealize Orchestrator-inhoud en -services, moet u de vRealize Orchestrator Appliance downloaden en implementeren.

### Voorwaarden

- Controleer of u een actieve vCenter Server-instantie heeft. De vCenter Server-versie moet 6.0 of hoger zijn.
- Controleer of de host waarop u de vRealize Orchestrator Appliance implementeert, voldoet aan de minimale hardwarevereisten. Zie [Hardwarevereisten voor de vRealize Orchestrator Appliance](#).
- Als uw systeem is geïsoleerd en geen internettoegang heeft, moet u het .ova-bestand voor de appliance van de VMware-website downloaden.

### Procedure

- 1 Meld u aan bij de vSphere Web Client als een **beheerder**.
- 2 Selecteer een inventarisobject dat een geldig bovenliggend object is van een virtuele machine, zoals een datacentrum, map, cluster, resourcepool of host.
- 3 Selecteer **Acties > OVF-sjabloon implementeren**.
- 4 Voer het bestandspad of de URL in naar het .ova-bestand en klik op **Volgende**.

- 5 Voer een naam en locatie voor de vRealize Orchestrator Appliance in en klik op **Volgende**.
- 6 Selecteer een host, cluster, resourcepool of vApp als bestemming waarop u de appliance wilt uitvoeren en klik op **Volgende**.
- 7 Bekijk de implementatiedetails en klik op **Volgende**.
- 8 Accepteer de voorwaarden van de licentieovereenkomst en klik op **Volgende**.
- 9 Selecteer de opslagindeling die u wilt gebruiken voor de vRealize Orchestrator Appliance.

Indeling	Beschrijving
<b>Thick Provisioned Lazy Zeroed</b>	Maakt een virtuele schijf in een standaard thick format. De vereiste ruimte voor de virtuele schijf wordt toegewezen wanneer de virtuele schijf wordt gemaakt. Als er gegevens op het fysieke apparaat blijven staan, worden deze niet gewist tijdens het maken, maar worden deze on demand op nul gezet wanneer voor de eerste keer vanaf de virtuele machine wordt geschreven.
<b>Thick Provisioned Eager Zeroed</b>	Ondersteunt clusterfuncties zoals fouttolerantie. De vereiste ruimte voor de virtuele schijf wordt toegewezen wanneer de virtuele schijf wordt gemaakt. Als er gegevens op het fysieke apparaat blijven staan, worden deze op nul gezet wanneer de virtuele schijf wordt gemaakt. Mogelijk duurt het langer om schijven in deze indeling te maken dan om schijven in andere indelingen te maken.
<b>Thin Provisioned Format</b>	Bespaart ruimte op de harde schijf. Voor de thin disk moet u zoveel gegevensopslagruimte inrichten als de schijf vereist op basis van de waarde die u selecteert voor de schijfgrootte. De Thin Disk start klein en gebruikt in eerste instantie slechts zoveel gegevensopslagruimte als de schijf nodig heeft voor de eerste bewerkingen.

- 10 Klik op **Volgende**.
- 11 Configureer de netwerkinstellingen en voer het **root**-wachtwoord in.

Wanneer u de netwerkinstellingen van de vRealize Orchestrator Appliance configureert, moet u het IPv4-protocol gebruiken. Voor zowel DHCP- als statische netwerkconfiguraties moet u een volledig gekwalificeerde domeinnaam (FQDN) toevoegen voor uw vRealize Orchestrator Appliance.

Als de naam van de host die wordt weergegeven in de shell van de geïmplementeerde vRealize Orchestrator Appliance *photon-machine* is, wordt niet voldaan aan de voorgaande vereisten voor de netwerkconfiguratie.

- 12 (Optioneel) Configureer aanvullende netwerkinstellingen voor de vRealize Orchestrator Appliance, zoals het inschakelen van SSH-toegang.
- 13 Klik op **Volgende**.
- 14 Controleer de pagina **Gereed om te voltooien** en klik op **Voltooien**.

## Resultaten

De vRealize Orchestrator Appliance is met succes geïmplementeerd.

## Wat nu te doen

Meld u aan bij de vRealize Orchestrator Appliance-opdrachtregel als **root** en bevestig dat u een forward of reverse DNS-zoekopdracht kunt uitvoeren.

- Voer de opdracht `nslookup your_orchestrator_FQDN` uit om een forward DNS-zoekactie uit te voeren. De opdracht moet het IP-adres van de vRealize Orchestrator Appliance retourneren.
- Voer de opdracht `nslookup your_orchestrator_IP` uit om een reverse DNS-zoekactie uit te voeren. De opdracht moet de FQDN van de vRealize Orchestrator Appliance retourneren.

## De vRealize Orchestrator Appliance inschakelen en de startpagina openen

Als u de standalone vRealize Orchestrator Appliance wilt gebruiken, moet u deze eerst inschakelen.

### Procedure

- 1 Meld u aan bij de vSphere Web Client als **beheerder**.
- 2 Klik met de rechtermuisknop op de vRealize Orchestrator Appliance en selecteer **Energie > Inschakelen**.
- 3 Ga in een webbrowser naar het hostadres van uw virtual machine met vRealize Orchestrator Appliance die u hebt geconfigureerd tijdens de OVA-implementatie.

`https://uw_orchestrator_FQDN/vco.`

## De duur van het rootwachtwoord wijzigen

Het rootwachtwoord van de vRealize Orchestrator Appliance verloopt standaard na 365 dagen.

### Voorwaarden

- Download en implementeer de vRealize Orchestrator Appliance.
- Controleer of de vRealize Orchestrator Appliance actief is.

### Procedure

- 1 Meld u aan bij de vRealize Orchestrator Appliance via SSH als **root**.
- 2 Voer de opdracht `passwd -x number_of_daysnumber_of_daysroot` uit.
- 3 Als u de duur van het rootwachtwoord oneindig wilt verlengen, voert u de opdracht `passwd -x 99999 root` uit.

## SSH-toegang tot de vRealize Orchestrator Appliance in- of uitschakelen

U kunt SSH-toegang tot de vRealize Orchestrator Appliance in- of uitschakelen.

### Voorwaarden

- Download en implementeer de vRealize Orchestrator Appliance.
- Controleer of de vRealize Orchestrator Appliance actief is.

### Procedure

- 1** Meld u als **root** aan op de vRealize Orchestrator Appliance-opdrachtregel.
- 2** Voer de opdracht `/usr/bin/toggle-ssh enable` uit om SSH-toegang in te schakelen.
- 3** Voer de opdracht `/usr/bin/toggle-ssh disable` uit om SSH-toegang uit te schakelen.

# Initiële configuratie

# 5

Voordat u begint met het automatiseren van taken en het beheren van systemen en applicaties met vRealize Orchestrator, moet u het vRealize Orchestrator Control Center gebruiken om een externe verificatieprovider te configureren. U kunt ook het vRealize Orchestrator Control Center gebruiken voor aanvullende configuratietaken, zoals het beheren van licentie- en certificaatinformatie, het installeren van invoegtoepassingen en het controleren van de status van uw vRealize Orchestrator-cluster.

Dit hoofdstuk omvat de volgende onderwerpen:

- [Een standalone vRealize Orchestrator-server configureren](#)
- [vRealize Orchestrator-functies inschakelen met licenties](#)
- [vRealize Orchestrator-databaseverbinding](#)
- [Certificaten beheren](#)
- [De vRealize Orchestrator-invoegtoepassingen configureren](#)
- [Beschikbaarheid en schaalbaarheid van vRealize Orchestrator](#)
- [Het Customer Experience Improvement Program configureren](#)

## Een standalone vRealize Orchestrator-server configureren

Hoewel de vRealize Orchestrator Appliance een vooraf geconfigureerde, op Photon gebaseerde virtuele machine is, moet u een verificatieprovider configureren voordat u de volledige functionaliteit van het vRealize Orchestrator Control Center en de vRealize Orchestrator Client kunt openen.

### Een standalone vRealize Orchestrator-server configureren met vRealize Automation-verificatie

Om de vRealize Orchestrator Appliance voor te bereiden voor gebruik, moet u de hostinstellingen en de verificatieprovider configureren. U kunt vRealize Orchestrator configureren om te verifiëren met vRealize Automation. Gebruik vRealize Automation-verificatie met vRealize Automation 8.x.

## Voorwaarden

- Download en implementeer de nieuwste versie van de vRealize Orchestrator Appliance. Zie [De vRealize Orchestrator Appliance downloaden en implementeren](#).
- Installeer en configureer vRealize Automation 8.x en controleer of uw vRealize Automation-server wordt uitgevoerd. Zie de documentatie bij vRealize Automation.

Als u van plan bent een cluster te maken:

- Stel een load balancer in om het verkeer tussen verschillende instanties van vRealize Orchestrator te verdelen. Zie de [handleiding voor VMware vRealize Orchestrator Load Balancing](#).

## Procedure

- 1 Open het Control Center om de configuratiewizard te starten.
  - a Ga naar `https://your_orchestrator_FQDN/vco-controlcenter`.
  - b Meld u aan als **root** met het wachtwoord dat u heeft ingevoerd tijdens de OVA-implementatie.
- 2 Configureer de verificatieprovider.
  - a Selecteer op de pagina **Verificatieprovider configureren** de optie **vRealize Automation** in het vervolgkeuzemenu **Verificatiemodus**.
  - b Voer in het tekstvak **Hostadres** het vRealize Automation-hostadres in en klik op **VERBINDEN**.  
  
De indeling van het vRealize Automation-hostadres moet `https://your_vra_hostname` zijn.
  - c Klik op **Certificaat accepteren**.
  - d Voer de inloggegevens in van de vRealize Automation-organisatie-eigenaar waaronder vRealize Orchestrator zal worden geconfigureerd. Klik op **REGISTREREN**.
  - e Klik op **WIJZIGINGEN OPSLAAN**.  
  
Er verschijnt een bericht dat uw configuratie is opgeslagen.

## Resultaten

De configuratie van de vRealize Orchestrator-server is voltooid.

## Wat nu te doen

- Controleer of **CSP** de geconfigureerde licentieprovider is op de pagina **Licenties**.
- Controleer of het knooppunt correct is geconfigureerd op de pagina **Configuratie valideren**.

---

**Opmerking** Na de configuratie van de verificatieprovider wordt de vRealize Orchestrator-server na 2 minuten automatisch opnieuw opgestart. Als u de configuratie onmiddellijk controleert na de verificatie, kan een ongeldige configuratiestatus worden geretourneerd.

---



## Een standalone vRealize Orchestrator-server configureren met vSphere-verificatie

U registreert de vRealize Orchestrator-server met een vCenter Single Sign-On-server met behulp van de vSphere-verificatiemodus. Gebruik vCenter Single Sign-On-verificatie met vCenter Server 6.0 en hoger.

### Voorwaarden

- Download en implementeer de nieuwste versie van de vRealize Orchestrator Appliance. Zie [De vRealize Orchestrator Appliance downloaden en implementeren](#).
- Installeer en configureer een vCenter Server waarop vCenter Single Sign-On wordt uitgevoerd. Zie de documentatie voor vSphere.

Als u van plan bent een cluster te maken:

- Stel een load balancer in om het verkeer tussen verschillende instanties van vRealize Orchestrator te verdelen. Zie de [handleiding voor VMware vRealize Orchestrator Load Balancing](#).

### Procedure

- 1 Open het Control Center om de configuratiewizard te starten.
  - a Ga naar `https://your_orchestrator_FQDN/vco-controlcenter`.
  - b Meld u aan als **root** met het wachtwoord dat u heeft ingevoerd tijdens de OVA-implementatie.
- 2 Configureer de verificatieprovider.
  - a Selecteer op de pagina **Verificatieprovider configureren** de optie **vSphere** in het vervolgkeuzemenu **Verificatiemodus**.
  - b Voer in het tekstvak **Hostadres** de volledig gekwalificeerde domeinnaam of het IP-adres in van de instantie van de Platform Services-controller die de vCenter Single Sign-On bevat en klik op **Verbinden**.

---

**Opmerking** Als u een externe Platform Services-controller of meerdere Platform Services-controllerinstanties achter een load balancer gebruikt, moet u de certificaten van alle Platform Services-controllers die een vCenter Single Sign-On-domein delen, handmatig importeren.

---

**Opmerking** Om een andere vSphere Client te integreren met uw geconfigureerde vRealize Orchestrator-omgeving, moet u vSphere configureren om dezelfde Platform Services-controller te gebruiken die is geregistreerd voor vRealize Orchestrator. Voor vRealize Orchestrator-omgevingen voor hoge beschikbaarheid moet u de PCS-instanties achter de vRealize Orchestrator load balancer-server repliceren.

---

- c Controleer de certificaatgegevens van de verificatieprovider en klik op **Certificaat accepteren**.

- d Voer de verificatiegegevens in van het lokale beheerdersaccount voor het vCenter Single Sign-On-domein. Klik op **REGISTREREN**.

Dit account is standaard **administrator@vsphere.local** en de naam van de standaardtenant is **vsphere.local**.

- e Voer in het tekstvak **Beheerdersgroep** de naam van een beheerdersgroep in en klik op **ZOEKEN**.

Bijvoorbeeld **vsphere.local\vcoadmins**

- f Selecteer de beheerdersgroep die u wilt gebruiken.

- g Klik op **WIJZIGINGEN OPSLAAN**.

Er verschijnt een bericht dat uw configuratie is opgeslagen.

## Resultaten

De configuratie van de vRealize Orchestrator-server is voltooid.

## Wat nu te doen

- Controleer of **CIS** de geconfigureerde licentieprovider is op de pagina **Licenties**.
- Controleer of het knooppunt correct is geconfigureerd op de pagina **Configuratie valideren**.

---

**Opmerking** Na de configuratie van de verificatieprovider wordt de vRealize Orchestrator-server na 2 minuten automatisch opnieuw opgestart. Als u de configuratie onmiddellijk controleert na de verificatie, kan een ongeldige configuratiestatus worden geretourneerd.

---

# vRealize Orchestrator-functies inschakelen met licenties

Toegang tot bepaalde vRealize Orchestrator-functies is gebaseerd op de licentie die is toegepast op uw vRealize Orchestrator-implementatie.

Na verificatie wordt aan uw vRealize Orchestrator-instantie een licentie toegewezen op basis van die verificatieprovider. Licenties beheren toegang tot de volgende vRealize Orchestrator-functies:

- Git-integratie
- Rollenbeheer
- Ondersteuning voor meerdere talen (Python, Node.js en PowerShell)

U kunt de licentie van de vRealize Orchestrator-server handmatig wijzigen op de pagina **Licenties** van het Control Center.

Verificatie	Licentie	Git-integratie	Rollenbeheer	Ondersteuning voor meerdere talen
vSphere	vSphere	Nee	Nee	Nee
vSphere	vRealize Automation/vRealize Suite	Ja	Ja	Ja
vRealize Automation	vRealize Automation/vRealize Suite	Ja	Rollen worden beheerd vanuit de vRealize Automation-instantie die wordt gebruikt om vRealize Orchestrator te verifiëren.	Ja

## vRealize Orchestrator-databaseverbinding

De vRealize Orchestrator-server vereist een database om gegevens op te slaan.

De geïmplementeerde vRealize Orchestrator Appliance bevat een vooraf geconfigureerde PostgreSQL-database die door de vRealize Orchestrator-server wordt gebruikt om gegevens op te slaan.

De postgresQL-database is niet toegankelijk voor gebruikers.

## Certificaten beheren

Met het certificaat, dat is uitgegeven voor een bepaalde server en informatie bevat over de openbare sleutel van de server, kunt u alle elementen ondertekenen die zijn gemaakt in vRealize Orchestrator en de echtheid garanderen. Wanneer de client een element van uw server ontvangt, meestal een pakket, controleert de client uw identiteit en bepaalt deze of uw handtekening moet worden vertrouwd.

### ■ [vRealize Orchestrator-certificaten beheren](#)

U kunt de vRealize Orchestrator-certificaten beheren via de pagina **Certificaten** in het vRealize Orchestrator Control Center of met de vRealize Orchestrator Client, door de getagde *SSL\_Trust\_Manager*-werkstromen te gebruiken.

## vRealize Orchestrator-certificaten beheren

U kunt de vRealize Orchestrator-certificaten beheren via de pagina **Certificaten** in het vRealize Orchestrator Control Center of met de vRealize Orchestrator Client, door de getagde *SSL\_Trust\_Manager*-werkstromen te gebruiken.

## Een certificaat importeren in het Orchestrator-vertrouwensarchief

vRealize Orchestrator Control Center gebruikt een beveiligde verbinding om te communiceren met vCenter Server, relationeel databasebeheersysteem (RDBMS), LDAP, Single Sign-On en andere servers. U kunt het vereiste TLS-certificaat importeren uit een URL of PEM-gecodeerd bestand. Telkens wanneer u een TLS-verbinding met een serverinstantie wilt gebruiken, moet u het overeenkomende certificaat importeren van het tabblad **Vertrouwde certificaten** op de pagina **Certificaten** en het bijbehorende TLS-certificaat importeren.

U kunt het TLS-certificaat in vRealize Orchestrator laden uit een URL-adres of PEM-gecodeerd bestand.

Optie	Beschrijving
<b>Importeren uit URL of proxy-URL</b>	De URL van de externe server: <code>https://uw_server_IP_adres</code> of <code>uw_server_IP_adres:poort</code>
<b>Importeren uit bestand</b>	Pad naar het PEM-gecodeerd certificaatbestand.
<b>Opmerking</b> U kunt ook een vertrouwd certificaat importeren door de werkstroom <b>Een vertrouwd certificaat uit een bestand importeren</b> in de vRealize Orchestrator Client uit te voeren. Het bestand dat via deze werkstroom wordt geïmporteerd, moet DER-gecodeerd zijn.	

Zie [Een vertrouwd certificaat importeren met het Control Center](#) voor meer informatie over het importeren van een certificaat.

## Handtekeningcertificaat voor pakketten

Pakketten die van een vRealize Orchestrator-server worden geëxporteerd, worden digitaal ondertekend. Importeer, exporteer of genereer een nieuw certificaat dat moet worden gebruikt voor het ondertekenen van pakketten. Handtekeningcertificaten voor pakketten zijn een vorm van digitale identificatie die wordt gebruikt om versleutelde communicatie en een handtekening voor uw Orchestrator-pakketten te garanderen.

De vRealize Orchestrator Appliance bevat een handtekeningcertificaat voor pakketten dat automatisch wordt gegenereerd op basis van de netwerkinstellingen van de appliance. Als de netwerkinstellingen van de appliance veranderen, moet u handmatig een nieuw handtekeningcertificaat voor pakketten genereren. Nadat u een nieuw handtekeningcertificaat voor pakketten hebt gegenereerd, worden alle toekomstige geëxporteerde pakketten met het nieuwe certificaat ondertekend.

## Een aangepast TLS-certificaat genereren voor vRealize Orchestrator

U kunt de vRealize Orchestrator Appliance gebruiken om een nieuw TLS-certificaat te genereren voor uw omgeving of een bestaand aangepast certificaat in te stellen.

De vRealize Orchestrator Appliance bevat een certificaat voor TLS (Trusted Layer Security) dat automatisch wordt gegenereerd op basis van de netwerkinstellingen van de appliance. Als de netwerkinstellingen van de appliance wijzigen, moet u handmatig een nieuw certificaat genereren. U kunt een certificaatketen maken om versleutelde communicatie te garanderen en

om een handtekening voor uw pakketten op te geven. De ontvanger kan er echter niet zeker van zijn dat het zelfondertekende pakket werkelijk een pakket is dat is uitgegeven door uw server en niet van een derde die beweert u te zijn. Om de identiteit van uw server te bewijzen, gebruikt u een certificaat dat is ondertekend door een certificaatautoriteit (CA).

vRealize Orchestrator genereert een servercertificaat dat uniek is voor uw omgeving. De persoonlijke sleutel wordt opgeslagen in de tabel `vmo_keystore` van de vRealize Orchestrator-database.

---

**Opmerking** Zie [Een aangepast TLS-certificaat voor vRealize Orchestrator instellen](#) als u uw vRealize Orchestrator Appliance wilt configureren om een bestaand aangepast TLS-certificaat te gebruiken.

---

### Voorwaarden

Controleer of SSH-toegang voor de vRealize Orchestrator Appliance is ingeschakeld. Zie [SSH-toegang tot de vRealize Orchestrator Appliance in- of uitschakelen](#).

### Procedure

- 1 Meld u via SSH als **rootgebruiker** aan bij de vRealize Orchestrator Appliance-opdrachtregel.
- 2 Voer de opdracht `vracli certificate ingress --generate auto --set stdin` uit.
- 3 Voer het implementatiescript uit om het aangepaste certificaat toe te passen op uw vRealize Orchestrator Appliance.
  - a Ga naar de map `/opt/scripts/`.

```
cd /opt/scripts/
```

- b Voer het script `./deploy.sh` uit.

---

**Belangrijk** Onderbreek het implementatiescript niet. Wanneer het script wordt voltooid, wordt het volgende bericht weergegeven:

```
Prelude is geïmplementeerd. Ga naar your_orchestrator_address om toegang te krijgen.
```

---

### Wat nu te doen

Voer de opdracht `vracli certificate ingress --list` uit om te bevestigen dat de nieuwe certificaatketen is toegepast.

## Een aangepast TLS-certificaat voor vRealize Orchestrator instellen

Stel een aangepast TLS-certificaat in voor uw vRealize Orchestrator Appliance.

De vRealize Orchestrator Appliance bevat een certificaat voor TLS (Trusted Layer Security) dat automatisch wordt gegenereerd op basis van de netwerkinstellingen van de appliance.

U kunt uw vRealize Orchestrator Appliance configureren om een bestaand aangepast TLS-certificaat te gebruiken. U kunt het certificaat instellen door het relevante PEM-bestand van uw lokale machine te importeren in de vRealize Orchestrator Appliance. U kunt ook uw aangepaste TLS-certificaat instellen door de certificaatketen rechtstreeks naar de vRealize Orchestrator Appliance te kopiëren. Voor beide procedures moet u het script `./deploy.sh` uitvoeren voordat het nieuwe TLS-certificaat kan worden gebruikt in uw vRealize Orchestrator-implementatie.

Zie [Een aangepast TLS-certificaat genereren voor vRealize Orchestrator](#) voor informatie over het genereren van een nieuw aangepast TLS-certificaat.

#### Voorwaarden

- Controleer of SSH-toegang voor de vRealize Orchestrator Appliance is ingeschakeld. Zie [SSH-toegang tot de vRealize Orchestrator Appliance in- of uitschakelen](#).
- Controleer of het PEM-bestand met het TLS-certificaat de volgende onderdelen bevat in de ingestelde volgorde:
  - a De persoonlijke sleutel voor het certificaat.
  - b Het primaire certificaat.
  - c Indien van toepassing, een of meer tussenliggende certificaten van de certificaatautoriteit (CA).
  - d Het CA-rootcertificaat.

Het TLS-certificaat kan bijvoorbeeld de volgende structuur hebben:

```
-----BEGIN RSA PRIVATE KEY-----
<Private Key>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<Primary TLS certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA certificate>
-----END CERTIFICATE-----
```

## Procedure

- 1 Stel het certificaat in door het PEM-bestand in de vRealize Orchestrator Appliance te importeren.

- a Importeer het certificaat-PEM van uw lokale machine door een Secure Copy-opdracht (SCP) uit te voeren vanaf een SSH-shell.

Voor Linux kunt u een SCP-terminalopdracht gebruiken:

```
scp ~/PEM_local_filepath/your_cert_file.PEM root@orchestrator_FQDN_or_IP:/
PEM_orchestrator_filepath/your_cert_file.PEM
```

Voor Windows kunt u een PSCP-opdracht voor een PuTTY-client gebruiken:

```
pscp C:\PEM_local_filepath\your_cert_file.PEM root@<orchestrator_FQDN_or_IP>:/
PEM_orchestrator_filepath/your_cert_file.PEM
```

- b Meld u via SSH als **rootgebruiker** aan bij de vRealize Orchestrator Appliance-opdrachtreel.
  - c Voer de opdracht `vracli certificate ingress --set uw_cert_bestand.PEM` uit.
- 2 (Optioneel) Stel het certificaat in door de certificaatketen rechtstreeks in de appliance te kopiëren.

- a Meld u via SSH als **rootgebruiker** aan bij de vRealize Orchestrator Appliance-opdrachtreel.
  - b Voer de opdracht `vracli certificate ingress --set stdin` uit.
  - c Kopieer en plak de certificaatketen en druk op CTRL+D.

- 3 Voer het implementatiescript uit om het nieuwe TLS-certificaat toe te passen.

- a Ga naar de map `/opt/scripts/`.

```
cd /opt/scripts/
```

- b Voer het script `./deploy.sh` uit.

---

**Belangrijk** Onderbreek het implementatiescript niet. Wanneer het script wordt voltooid, wordt het volgende bericht weergegeven:

```
Prelude is geïmplementeerd. Ga naar https://uw_orchestrator_FQDN voor toegang.
```

---

## Resultaten

U hebt een aangepast TLS-certificaat ingesteld voor uw vRealize Orchestrator Appliance.

## Wat nu te doen

Voer de opdracht `vracli certificate ingress --list` uit om te bevestigen dat de nieuwe certificaatketen is toegepast.

## Een vertrouwd certificaat importeren met het Control Center

Om veilig met andere servers te communiceren, moet de vRealize Orchestrator-server hun identiteit kunnen verifiëren. Hiertoe moet u mogelijk het TLS-certificaat van de externe entiteit importeren in het vertrouwensarchief van vRealize Orchestrator. Als u een certificaat wilt vertrouwen, kunt u het in het vertrouwensarchief importeren door een verbinding met een specifieke URL tot stand te brengen of direct als een PEM-gecodeerd bestand te importeren.

### Procedure

- 1 Meld u aan bij Control Center als **root**.
- 2 Ga naar de pagina **Certificaten**.
- 3 Selecteer **Vertrouwde certificaten** en klik op **Importeren**.
- 4 Als u het certificaat wilt importeren uit een bestand, selecteert u **Importeren uit een PEM-gecodeerd bestand**.
- 5 Blader naar het certificaatbestand en klik op **Importeren**.
- 6 Als u het certificaat wilt importeren van een URL-adres, selecteert u **Importeren uit URL**.
- 7 Voer het URL-adres in waar uw certificaat is opgeslagen en klik op **Importeren**.

### Resultaten

U heeft een extern servercertificaat geïmporteerd naar het vertrouwensarchief van vRealize Orchestrator.

## De vRealize Orchestrator-invoegtoepassingen configureren

De vRealize Orchestrator-standaardinvoegtoepassingen worden geconfigureerd met specifieke werkstromen voor invoegtoepassingen die in de vRealize Orchestrator Client worden uitgevoerd.

De vRealize Orchestrator Appliance biedt toegang tot een vooraf geïnstalleerde bibliotheek met standaardinvoegtoepassingen. U kunt deze standaardinvoegtoepassingen configureren door specifieke werkstromen van de vRealize Orchestrator Client uit te voeren.

Als u bijvoorbeeld de tags *AMQP* en *Configuration* in het zoekvak van de werkstroombibliotheek invoert, vindt u werkstromen die worden gebruikt om AMQP-brokers en abonnementen te beheren.

## vRealize Orchestrator-invoegtoepassingen beheren

Op de pagina **Invoegtoepassingen beheren** van het vRealize Orchestrator Control Center kunt u een lijst bekijken met alle invoegtoepassingen die in vRealize Orchestrator zijn geïnstalleerd en basisbeheeracties uitvoeren.



## Een nieuwe invoegtoepassing installeren of upgraden

Met de vRealize Orchestrator-invoegtoepassingen kan de vRealize Orchestrator-server integreren met andere softwareproducten. De vRealize Orchestrator Appliance bevat een aantal vooraf geïnstalleerde invoegtoepassingen. U kunt de mogelijkheden van het vRealize Orchestrator-platform verder uitbreiden door aangepaste invoegtoepassingen te installeren.

U kunt invoegtoepassingen installeren of upgraden vanaf de pagina **Invoegtoepassingen beheren** van de vRealize Orchestrator. De bestandsextensies die kunnen worden gebruikt, zijn `.vmoapp` en `.dar`. Een `.vmoapp`-bestand kan een verzameling van verschillende `.dar`-bestanden bevatten en kan als toepassing worden geïnstalleerd. Een `.dar`-bestand bevat alle bronnen die aan één invoegtoepassing zijn gekoppeld.

---

**Opmerking** De gewenste bestandsindeling voor vRealize Orchestrator-invoegtoepassingen is `.vmoapp`.

---

Zie [Een vRealize Orchestrator-invoegtoepassing installeren of bijwerken](#) voor meer informatie over het installeren of upgraden van vRealize Orchestrator-invoegtoepassingen.

## Logboekregistratieniveau voor invoegtoepassingen wijzigen

In plaats van het logboekregistratieniveau voor vRealize Orchestrator te wijzigen, kunt u het ook alleen voor specifieke invoegtoepassingen wijzigen.

## Een invoegtoepassing uitschakelen

U kunt een invoegtoepassing uitschakelen door de selectie van de optie **Invoegtoepassing inschakelen** naast de naam van de invoegtoepassing op te heffen.

Deze actie verwijdert het invoegtoepassingsbestand niet. Zie [Een invoegtoepassing verwijderen](#) voor meer informatie over het verwijderen van een invoegtoepassing in vRealize Orchestrator.

## Een vRealize Orchestrator-invoegtoepassing installeren of bijwerken

U kunt invoegtoepassingen van derden installeren of bijwerken in het vRealize Orchestrator Control Center.

### Voorwaarden

Download het bestand `.dar` of `.vmoapp` van de invoegtoepassing.

---

**Opmerking** De gewenste bestandsindeling voor vRealize Orchestrator-invoegtoepassingen is `.vmoapp`.

---

### Procedure

- 1 Meld u aan bij het Control Center als **root**.
- 2 Selecteer de pagina **Invoegtoepassingen beheren**.
- 3 Klik op **Bladeren** en selecteer het bestand `.dar` of `.vmoapp` van de invoegtoepassing die u wilt installeren of bijwerken.

#### 4 Klik op **Uploaden**.

#### 5 Controleer de informatie van de invoegtoepassing, indien van toepassing, accepteer de licentieovereenkomst voor eindgebruikers en klik op **Installeren**.

De invoegtoepassing is geïnstalleerd of bijgewerkt en de vRealize Orchestrator-serverservice wordt opnieuw gestart.

#### Wat nu te doen

Controleer of de juiste informatie voor de invoegtoepassing wordt weergegeven op de pagina **Invoegtoepassingen beheren**.

## Een invoegtoepassing verwijderen


U kunt invoegtoepassingen van derden uit de vRealize Orchestrator Appliance verwijderen via het Control Center.

---

**Opmerking** Vanaf vRealize Orchestrator 8.0 verwijdert u het invoegtoepassingspakket niet langer handmatig van de vRealize Orchestrator Client.

---

#### Procedure

- 1 Meld u aan bij het Control Center als **root**.
- 2 Selecteer **Invoegtoepassingen beheren**.
- 3 Zoek de invoegtoepassing die u wilt verwijderen en klik op het verwijderingspictogram (  ).
- 4 Bevestig dat u de invoegtoepassing wilt verwijderen en klik op **Verwijderen**.

#### Resultaten

U hebt de invoegtoepassing van de vRealize Orchestrator Appliance verwijderd.

## Beschikbaarheid en schaalbaarheid van vRealize Orchestrator

Om de beschikbaarheid van de vRealize Orchestrator-services te vergroten, start u meerdere vRealize Orchestrator-serverinstanties in een cluster met een gedeelde database. vRealize Orchestrator werkt als één instantie totdat deze is geconfigureerd om als onderdeel van een cluster te werken.

### vRealize Orchestrator-cluster

Meerdere vRealize Orchestrator-serverinstanties met identieke server- en invoegtoepassingsconfiguraties werken samen in een cluster en delen één database.

Alle vRealize Orchestrator-serverinstanties communiceren met elkaar door heartbeats uit te wisselen. Elke heartbeat is een tijdstempel dat het knooppunt binnen een bepaald tijdsinterval naar de gedeelde database van het cluster schrijft. Netwerkproblemen, een niet-reagerende databaseserver of overbelasting zorgt er mogelijk voor dat een vRealize Orchestrator-clusterknooppunt niet meer reageert. Als een actieve vRealize Orchestrator-serverinstantie geen heartbeats kan verzenden binnen de time-outperiode voor failover, wordt deze als niet-reagerend beschouwd. De time-out voor failover is gelijk aan de waarde van het heartbeatinterval vermenigvuldigd met het aantal failoverheartbeats. Deze fungeert als definitie voor een onbetrouwbaar knooppunt en kan worden aangepast op basis van de beschikbare bronnen en de productiebelasting.

Een vRealize Orchestrator-knooppunt schakelt de stand-by-modus in wanneer de verbinding met de database wordt verbroken en blijft in deze modus totdat de verbinding met de database wordt hersteld. De andere knooppunten in het cluster nemen de controle over van het actieve werk, door alle onderbroken werkstromen te hervatten vanaf de laatste onvoltooide items, zoals scriptbare taken of werkstroomaanroepen.

U kunt de status van uw vRealize Orchestrator-cluster controleren op de pagina **Orchestrator-clusterbeheer** van het vRealize Orchestrator Control Center. U kunt deze pagina ook gebruiken om de heartbeat van het cluster, het aantal failoverheartbeats en het aantal actieve vRealize Orchestrator-knooppunten te configureren.

## Een vRealize Orchestrator-cluster configureren

U kunt uw nieuwe vRealize Orchestrator-implementatie configureren om in hoge beschikbaarheid uit te voeren door drie knooppunten te implementeren en deze als een cluster te verbinden.

Een vRealize Orchestrator-cluster bestaat uit drie vRealize Orchestrator-instanties die een gemeenschappelijke PostgreSQL-database delen. De database van het geconfigureerde vRealize Orchestrator-cluster kan alleen in de asynchrone modus worden uitgevoerd.

Als u een vRealize Orchestrator-cluster wilt maken, moet u één vRealize Orchestrator-instantie selecteren als het primaire knooppunt van het cluster. Na het configureren van het primaire knooppunt voegt u de secundaire knooppunten hieraan toe.

Het gemaakte vRealize Orchestrator-cluster is vooraf geconfigureerd met automatische failover.

---

**Opmerking** Uitval van de automatische failover kan leiden tot het verlies van databasegegevens.

---

### Voorwaarden

- Download en implementeer drie standalone vRealize Orchestrator-instanties. Zie [De vRealize Orchestrator Appliance downloaden en implementeren](#).

---

**Opmerking** Het aanbevolen aantal knooppunten dat kan worden gebruikt om een geclusterde vRealize Orchestrator-omgeving te maken, is drie.

---

- Controleer of SSH-toegang is ingeschakeld voor alle vRealize Orchestrator-knooppunten. Zie [SSH-toegang tot de vRealize Orchestrator Appliance in- of uitschakelen](#).
- Configureer een load balancer-server. Zie de [handleiding voor VMware vRealize Orchestrator Load Balancing](#).

## Procedure

### 1 Configureer het primaire knooppunt.

- a Meld u via SSH aan als **root** bij de vRealize Orchestrator Appliance van het primaire knooppunt.
- b Als u de load balancer-server van het cluster wilt configureren, voert u de opdracht `vracli load-balancer set load_balancer_FQDN` uit.
- c Meld u aan bij het Control Center van het primaire knooppunt en selecteer **Hostinstellingen**.
- d Klik op **Wijzigen** en stel het hostadres van de verbonden load balancer-server in.
- e Configureer de verificatieprovider. Zie [Een standalone vRealize Orchestrator-server configureren](#).

### 2 Voeg secundaire knooppunten toe aan het primaire knooppunt.

- a Meld u via SSH aan als **root** bij de vRealize Orchestrator Appliance van het secundaire knooppunt.
- b Om het secundaire knooppunt toe te voegen aan het primaire knooppunt, voert u de opdracht `vracli cluster join primary_node_hostname_or_IP` uit.
- c Voer het rootwachtwoord van het primaire knooppunt in.
- d Herhaal de procedure voor andere secundaire knooppunten.

### 3 (Optioneel) Als op uw primaire knooppunt een aangepast certificaat wordt gebruikt, moet u het certificaat in de toepassing instellen of een nieuw certificaat genereren. Zie [Een aangepast TLS-certificaat genereren voor vRealize Orchestrator](#).

---

**Opmerking** Het bestand met de certificaatketen moet PEM-gecodeerd zijn.

---

### 4 Voltooi de clusterimplementatie.

- a Meld u via SSH aan als **root** bij de vRealize Orchestrator Appliance van het primaire knooppunt.
- b Voer de opdracht `kubect1 -n prelude get nodes` uit om te bevestigen dat alle knooppunten gereed zijn.
- c Voer het `/opt/scripts/deploy.sh`-script uit en wacht totdat de implementatie is voltooid.

## Resultaten

U heeft een vRealize Orchestrator-cluster gemaakt. Nadat u het cluster heeft gemaakt, kunt u uw vRealize Orchestrator-omgeving alleen openen vanaf het FQDN-adres van uw load balancer-server.

---

**Opmerking** Omdat u alleen toegang heeft tot het Control Center van het cluster met het rootwachtwoord van de load balancer, kunt u de configuratie van een clusterknooppunt niet bewerken als het een ander rootwachtwoord heeft. Als u de configuratie van dit knooppunt wilt bewerken, verwijdt u dit uit de load balancer, bewerkt u de configuratie in het Control Center en voegt u het knooppunt weer toe aan de load balancer.

---

## Wat nu te doen

Als u de status van het vRealize Orchestrator-cluster wilt bewaken, meldt u zich aan bij het Control Center en selecteert u de pagina **Orchestrator-clusterbeheer**. Zie [Een vRealize Orchestrator-cluster controleren](#).

## Een vRealize Orchestrator-clusterknooppunt verwijderen

U kunt een vRealize Orchestrator verwijderen zodat u uw clustercapaciteit kunt beperken.

Nadat een knooppunt van uw vRealize Orchestrator-cluster is verwijderd, zal dat knooppunt niet langer functioneel zijn. Als u dit knooppunt opnieuw wilt gebruiken, moet u de vRealize Orchestrator Appliance ervan van uw vCenter Server verwijderen en opnieuw implementeren. Zie [De vRealize Orchestrator Appliance downloaden en implementeren](#).

## Voorwaarden

Maak een vRealize Orchestrator-cluster. Zie [Een vRealize Orchestrator-cluster configureren](#).

## Procedure

- 1 Meld u aan bij de vRealize Orchestrator Appliance-opdrachtregel van het knooppunt dat u wilt verwijderen als **root**.
- 2 Voer de opdracht `vracli cluster leave` uit om het knooppunt uit uw vRealize Orchestrator te verwijderen.
- 3 Meld u aan bij de vRealize Orchestrator Appliance-opdrachtregel van een van de resterende knooppunten als **root**.
- 4 Voer de opdracht `kubect1 -n prelude get nodes` uit en bevestig dat het verwijderde knooppunt niet langer deel uitmaakt van het cluster.

## Een standalone vRealize Orchestrator-implementatie uitschalen

U kunt de beschikbaarheid en schaalbaarheid van uw geconfigureerde vRealize Orchestrator-implementatie verhogen door deze uit te schalen.

## Voorwaarden

- Download, implementeer en configureer een vRealize Orchestrator-instantie. Zie [De vRealize Orchestrator Appliance downloaden en implementeren](#) en [Een standalone vRealize Orchestrator-server configureren](#).
- Download en implementeer twee extra vRealize Orchestrator-instanties. Zie [De vRealize Orchestrator Appliance downloaden en implementeren](#).
- Configureer een load balancer-server. Zie de [handleiding voor VMware vRealize Orchestrator 8.x Load Balancing](#).

## Procedure

### 1 Configureer het primaire knooppunt.

- a Meld u aan bij het Control Center van uw geconfigureerde vRealize Orchestrator-implementatie als **root**.
- b Selecteer **Verificatieprovider configureren** en maak de registratie van uw verificatieprovider ongedaan.
- c Selecteer **Hostinstellingen** en voer de hostnaam van de server met load balancer in.
- d Selecteer **Verificatieprovider configureren** en registreer uw verificatieprovider opnieuw.
- e Meld u aan op de vRealize Orchestrator Appliance-opdrachtregel van de geconfigureerde instantie als **root**.
- f Als u alle services van de vRealize Orchestrator-instantie wilt stoppen, voert u de opdracht `/opt/scripts/deploy.sh --onlyClean` uit.
- g Voer `vracli load-balancer set load_balancer_FQDN` uit om de load balancer in te stellen.
- h (Optioneel) Als uw vRealize Orchestrator-instantie een aangepast certificaat gebruikt, voert u de opdracht `vracli certificate ingress --set uw_cert_bestand.pem` uit.

---

**Opmerking** Het bestand met de certificaatketen moet PEM-gecodeerd zijn.

---

### 2 Voeg secundaire knooppunten toe aan de geconfigureerde instantie.

- a Meld u aan op de vRealize Orchestrator Appliance-opdrachtregel van het secundaire knooppunt als **root**.
- b Om het secundaire knooppunt toe te voegen aan de geconfigureerde instantie, voert u de opdracht `vracli cluster joinprimair_knooppunt_hostnaam_of_IP` uit.
- c Herhaal dit voor het andere secundaire knooppunt.

### 3 Voltooi het uitschalingsproces.

- a Meld u aan op de vRealize Orchestrator Appliance-opdrachtregel van de geconfigureerde instantie als **root**.
- b Voer `/opt/scripts/deploy.sh` uit en wacht totdat het script is voltooid.

## Resultaten

U hebt uw vRealize Orchestrator-implementatie uitgeschaald.

## Een vRealize Orchestrator-cluster controleren

U kunt uw bestaande vRealize Orchestrator-cluster controleren via het vRealize Orchestrator Control Center.

U kunt de configuratiesynchronisatiestatus van de vRealize Orchestrator-instanties die deel uitmaken van een cluster, controleren via de pagina **Orchestrator-clusterbeheer** in het Control Center.

Configuratiesynchronisatiestatus	Beschrijving
IN UITVOERING	De vRealize Orchestrator-service is beschikbaar en kan aanvragen accepteren.
STAND-BY	<p>De vRealize Orchestrator-service kan aanvragen niet verwerken om de volgende redenen:</p> <ul style="list-style-type: none"> <li>■ Het knooppunt maakt deel uit van een cluster met hoge beschikbaarheid (HA) en blijft in de stand-by-modus totdat het hoofdknooppunt mislukt.</li> <li>■ De service kan de configuratievereisten niet verifiëren, zoals een geldige verbinding met de database, verificatieprovider en de vRealize Orchestrator-instantielicentie.</li> </ul>
Kan de gezondheidsstatus van de service niet ophalen	Kan geen verbinding maken met de vRealize Orchestrator-serverservice omdat deze is gestopt of omdat er een netwerkprobleem is.
Herstarten in behandeling	Het Control Center detecteert een configuratiewijziging en de vRealize Orchestrator-server wordt automatisch opnieuw opgestart.

## Het Customer Experience Improvement Program configureren

Als u ervoor kiest om deel te nemen aan het Customer Experience Improvement Program (CEIP), ontvangt VMware anonieme informatie waarmee u de kwaliteit, betrouwbaarheid en functionaliteit van VMware-producten en -services kunt verbeteren.

## Categorieën van informatie die VMware ontvangt

Het Customer Experience Improvement Program (CEIP) biedt VMware informatie waarmee VMware zijn producten en diensten kan verbeteren en problemen kan oplossen.

Gedetailleerde informatie over de gegevens die worden verzameld via het CEIP en de doelen waarvoor deze gegevens worden gebruikt door VMware vindt u in het Trust & Assurance Center op <http://www.vmware.com/trustvmware/ceip.html>. Zie [Deelnemen aan het Customer Experience Improvement Program](#) als u wilt deelnemen aan het CEIP voor dit product of als u het programma wilt verlaten.

## Deelnemen aan het Customer Experience Improvement Program

Neem deel aan het Customer Experience Improvement Program via de vRealize Orchestrator Appliance-opdrachtregel.

### Procedure

- 1 Meld u als **root** aan op de vRealize Orchestrator Appliance-opdrachtregel.
- 2 Als u wilt deelnemen aan het Customer Experience Improvement Program, voert u de opdracht `vracli ceip on` uit.
- 3 Controleer de informatie over het Customer Experience Improvement Program en voer de opdracht `vracli ceip on --acknowledge-ceip` uit.
- 4 Start de vRealize Orchestrator-services opnieuw.
  - a Om de serverservice opnieuw te starten, voert u de opdracht `kubect1 -n prelude exec -it your_vro_pod-c vco-server-app /bin/bash` uit.
  - b Voer de opdracht `kill 1` uit om de service te stoppen.
  - c Om de Control Center-service opnieuw te starten, voert u de opdracht `kubect1 -n prelude exec -it your_vro_pod-c vco-controlcenter-app /bin/bash` uit.
  - d Voer de opdracht `kill 1` uit om de service te stoppen.
- 5 Als u het Customer Experience Improvement Program wilt verlaten, voert u de opdracht `vracli ceip off` uit.
- 6 Herhaal de stappen om de services opnieuw te starten.



# De vRealize Orchestrator API-services gebruiken

## 6

Naast het configureren van vRealize Orchestrator met behulp van het Control Center kunt u de configuratie-instellingen van de vRealize Orchestrator-server wijzigen met behulp van de vRealize Orchestrator REST API, de Control Center REST API of het opdrachtregelhulpprogramma, dat is opgeslagen in de toepassing.

De configuratie-invoegtoepassing is standaard opgenomen in het vRealize Orchestrator-pakket. U heeft toegang tot de werkstromen voor de configuratie-invoegtoepassing via de vRealize Orchestrator-werkstroombibliotheek of de vRealize Orchestrator REST API. Met deze werkstromen kunt u de instellingen voor vertrouwde certificaten en sleutelarchieven van de vRealize Orchestrator-server wijzigen. Voor meer informatie over alle beschikbare vRealize Orchestrator REST API-serviceaanroepen raadpleegt u de documentatie voor de *vRealize Orchestrator-server-API*, te vinden op [https://your\\_orchestrator\\_FQDN/vco/api/docs](https://your_orchestrator_FQDN/vco/api/docs).

### ■ TLS-certificaten en -sleutelarchieven beheren met de REST API

Naast het beheren van TLS-certificaten met het Control Center kunt u ook vertrouwde certificaten en sleutelarchieven beheren wanneer u werkstromen uitvoert vanuit de configuratie-invoegtoepassing of door de REST API te gebruiken.

## TLS-certificaten en -sleutelarchieven beheren met de REST API

Naast het beheren van TLS-certificaten met het Control Center kunt u ook vertrouwde certificaten en sleutelarchieven beheren wanneer u werkstromen uitvoert vanuit de configuratie-invoegtoepassing of door de REST API te gebruiken.

De configuratie-invoegtoepassing bevat werkstromen voor het importeren en verwijderen van TLS-certificaten en -sleutelarchieven. U hebt toegang tot deze werkstromen door te navigeren naar **Bibliotheek > Werkstromen > SSL Trust Manager** en **Bibliotheek > Werkstromen > Sleutelarchieven** in de vRealize Orchestrator Client. U kunt deze werkstromen ook uitvoeren met de vRealize Orchestrator REST API.

De Control Center REST API biedt toegang tot bronnen voor het configureren van de vRealize Orchestrator-server. U kunt de Control Center REST API met systemen van derden gebruiken om de vRealize Orchestrator-configuratie te automatiseren. Het rootendpoint van de Control Center REST API is `https://uw_orchestrator_FQDN/vco/api`. Voor informatie over alle beschikbare serviceaanroepen die u kunt uitvoeren in de Control Center REST API, raadpleegt u de documentatie *vRealize Orchestrator Control Center API*, op `https://uw_orchestrator_FQDN/vco-controlcenter/docs`.

## Een TLS-certificaat verwijderen met behulp van de REST API

U kunt een TLS-certificaat verwijderen door de werkstroom Vertrouwd certificaat verwijderen van de configuratie-invoegtoepassing uit te voeren of door de REST API te gebruiken.

### Procedure

- 1 Maak een GET-aanvraag bij de URL van de werkstroomservice van de werkstroom Vertrouwd certificaat verwijderen.

```
GET https://{orchestrator_host}:{poort}/vco/api/workflows?conditions=name>Delete trusted certificate
```

- 2 Haal de definitie van de werkstroom Vertrouwd certificaat verwijderen op door een GET-aanvraag te maken bij de URL van de definitie.

```
GET https://{orchestrator_host}:{poort}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd
```

- 3 Maak een POST-aanvraag bij de URL die de uitvoeringsobjecten bevat van de werkstroom Vertrouwd certificaat verwijderen.

```
POST https://{orchestrator_host}:{poort}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd/executions/
```

- 4 Geef de naam op van het certificaat dat u wilt verwijderen als invoerparameter van de werkstroom Vertrouwd certificaat verwijderen in een element voor uitvoeringscontext in de hoofdtekst van de aanvraag.

## TLS-certificaten importeren met behulp van de REST API

U kunt TLS-certificaten importeren door een werkstroom uit te voeren vanuit de configuratie-invoegtoepassing of door de REST API te gebruiken.

U kunt een vertrouwd certificaat importeren vanuit een bestand of een URL. Zie [Een vertrouwd certificaat importeren met het Control Center](#)

## Procedure

- 1 Maak een GET-aanvraag bij de URL van de werkstroom.

Optie	Beschrijving
<b>Vertrouwd certificaat uit een bestand importeren</b>	Hiermee wordt een vertrouwd certificaat uit een bestand geïmporteerd.
<b>Vertrouwd certificaat uit een URL importeren</b>	Hiermee wordt een vertrouwd certificaat uit een URL-adres geïmporteerd.
<b>Vertrouwd certificaat uit een URL importeren met een proxyserver</b>	Hiermee wordt een vertrouwd certificaat van een URL-adres geïmporteerd met behulp van een proxyserver.
<b>Vertrouwd certificaat uit een URL met certificaatalias importeren</b>	Hiermee wordt een vertrouwd certificaat met een certificaatalias geïmporteerd van een URL-adres.

Als u een vertrouwd certificaat uit een bestand wilt importeren, moet u de volgende GET-aanvraag doen:

```
GET https://{orchestrator_host}:{poort}/vco/api/workflows?conditions=name=Import
trusted certificate from a file
```

- 2 Haal de definitie van de werkstroom op door een GET-aanvraag te maken bij de URL van de definitie.

Om de definitie van de werkstroom Vertrouwd certificaat uit een bestand importeren op te halen, moet u de volgende GET-aanvraag doen:

```
GET https://{orchestrator_host}:{poort}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5
```

- 3 Maak een POST-aanvraag bij de URL die de uitvoeringsobjecten van de werkstroom bevat.

Voor de werkstroom Vertrouwd certificaat uit een bestand importeren moet u de volgende POST-aanvraag doen:

```
POST https://{orchestrator_host}:{poort}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5/
executions
```

- 4 Geef waarden op voor de invoerparameters van de werkstroom in een element voor uitvoeringscontext in de hoofdtekst van de aanvraag.

Parameter	Beschrijving
<b>cer</b>	Het CER-bestand vanwaar u het TLS-certificaat wilt importeren. Deze parameter is van toepassing op de werkstroom Vertrouwd certificaat uit een bestand importeren.
<b>url</b>	De URL vanwaar u het TLS-certificaat wilt importeren. Voor niet-HTTPS-services is de ondersteunde indeling <i>IP_address_or_DNS_name:port</i> . Deze parameter is van toepassing op de werkstroom Vertrouwd certificaat uit een URL importeren.

## Een sleutelarchief maken met behulp van de REST API

U kunt een sleutelarchief maken door de werkstroom Een sleutelarchief maken van de configuratie-invoegtoepassing te starten of door de REST API te gebruiken.

### Procedure

- 1 Maak een GET-aanvraag bij de URL van de werkstroomservice van de werkstroom Een sleutelarchief maken.

```
GET https://{orchestrator_host}:{poort}/vco/api/workflows?conditions=name=Create a keystore
```

- 2 Haal de definitie van de werkstroom Een sleutelarchief maken op door een GET-aanvraag te maken bij de URL van de definitie.

```
GET https://{orchestrator_host}:{poort}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
```

- 3 Maak een POST-aanvraag bij de URL die de uitvoeringsobjecten bevat van de werkstroom Een sleutelarchief maken.

```
POST https://{orchestrator_host}:{poort}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
executions/
```

- 4 Geef de naam op van het sleutelarchief dat u wilt maken als invoerparameter van de werkstroom Een sleutelarchief maken in een element voor uitvoeringscontext in de hoofdtekst van de aanvraag.

## Een sleutelarchief verwijderen met behulp van de REST API

U kunt een sleutelarchief verwijderen door de werkstroom Een sleutelarchief verwijderen van de configuratie-invoegtoepassing uit te voeren of door de REST API te gebruiken.

### Procedure

- 1 Maak een GET-aanvraag bij de URL van de werkstroomservice van de werkstroom Een sleutelarchief verwijderen.

```
GET https://{orchestrator_host}:{poort}/vco/api/workflows?conditions=name=Delete a keystore
```

- 2 Haal de definitie van de werkstroom Een sleutelarchief verwijderen op door een GET-aanvraag te maken bij de URL van de definitie.

```
GET https://{orchestrator_host}:{poort}/vco/api/workflows/7a3389eb-1fab-4d77-860b-81b66bb45b86/
```

- 3 Maak een POST-aanvraag bij de URL die de uitvoeringsobjecten bevat van de werkstroom Een sleutelarchief verwijderen.

```
POST https://{orchestrator_host}:{poort}/vco/api/workflows/7a3389eb-1fab-4d77-860b-81b66bb45b86/
executions/
```

- 4 Geef de naam op van het sleutelarchief dat u wilt verwijderen als invoerparameter van de werkstroom Een sleutelarchief verwijderen in een element voor uitvoeringscontext in de hoofdtekst van de aanvraag.

## Een sleutel toevoegen met behulp van de REST API

U kunt een sleutel toevoegen door de werkstroom Sleutel toevoegen van de configuratie-invoegtoepassing uit te voeren of door de REST API te gebruiken.

### Procedure

- 1 Dien een GET-aanvraag in bij de URL van de werkstroomservice van de werkstroom Sleutel toevoegen.

```
GET https://{orchestrator_host}:{poort}/vco/api/workflows?conditions=name=Add key
```

- 2 Haal de definitie van de werkstroom Sleutel toevoegen op door een GET-aanvraag te maken bij de URL van de definitie.

```
GET https://{orchestrator_host}:{poort}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
```

- 3 Dien een POST-aanvraag in bij de URL die de uitvoeringsobjecten van de werkstroom Sleutel toevoegen bevat.

```
POST https://{orchestrator_host}:{poort}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/executions/
```

- 4 Geef het sleutelarchief, de sleutelalias, de PEM-gecodeerde sleutel, de certificaatketen en het sleutelwachtwoord op als invoerparameters van de werkstroom Sleutel toevoegen in een element voor uitvoeringscontext in de hoofdtekst van de aanvraag.

# Aanvullende configuratieopties

# 7

U kunt het Control Center gebruiken om het standaardgedrag van vRealize Orchestrator te wijzigen.

Dit hoofdstuk omvat de volgende onderwerpen:

- [Verificatie opnieuw configureren](#)
- [De eigenschappen voor werkstroomuitvoeringen configureren](#)
- [vRealize Orchestrator-logboekbestanden](#)
- [OpenTracing- en Wavefront-extensies inschakelen](#)
- [Tijdssynchronisatie voor vRealize Orchestrator inschakelen](#)
- [Tijdssynchronisatie voor vRealize Orchestrator uitschakelen](#)

## Verificatie opnieuw configureren

Nadat u de verificatiemethode hebt ingesteld tijdens de eerste configuratie van het Control Center, kunt u de verificatieprovider of de geconfigureerde parameters op elk gewenst moment wijzigen.

### De verificatieprovider wijzigen

Als u de verificatiemodus of de verbindinginstellingen voor de verificatieprovider wilt wijzigen, moet u eerst de registratie van de bestaande verificatieprovider ongedaan maken.

#### Procedure

- 1 Meld u aan bij Control Center als **root**.
- 2 Klik op de pagina **Verificatieprovider configureren** op de knop **REGISTRATIE ONGEDAAN MAKEN** naast het tekstvak voor het hostadres om de registratie van de verificatieprovider die in gebruik is, te verwijderen.

#### Resultaten

U heeft de registratie van de verificatieprovider ongedaan gemaakt.

## Wat nu te doen

Configureer de verificatie opnieuw in het Control Center. Zie [Een standalone vRealize Orchestrator-server configureren](#).

## De verificatieparameters wijzigen

Wanneer u vSphere als verificatieprovider gebruikt in het Control Center, kunt u de standaardtenant van de vRealize Orchestrator-beheerdersgroep wijzigen.

### Voorwaarden

Configureer vSphere als verificatieprovider voor uw vRealize Orchestrator-implementatie. Zie [Een standalone vRealize Orchestrator-server configureren met vSphere-verificatie](#).

---

**Opmerking** De vRealize Automation-verificatie bevat deze parameters niet.

---

### Procedure

- 1 Meld u aan bij het Control Center als **root**.
- 2 Selecteer **Verificatieprovider configureren**.
- 3 Klik op de knop **WIJZIGEN** naast het tekstvak **Standaardtenant**.
- 4 Vervang de naam van de tenant.
- 5 Klik op de knop **WIJZIGEN** naast het tekstvak **Beheerdersgroep**.

---

**Opmerking** Als u de beheerdersgroep niet opnieuw configureert, blijft deze leeg en kunt u het Control Center niet meer openen.

---

- 6 Voer de naam van een beheerdersgroep in en klik op **ZOEKEN**.
- 7 Selecteer een beheerdersgroep.
- 8 Wijzig de beheerdersgroep.
- 9 Als u het bewerken van de verificatieparameters wilt voltooien, klikt u op **WIJZIGINGEN OPSLAAN**.

## De eigenschappen voor werkstroomuitvoeringen configureren

Standaard kunt u maximaal 300 werkstromen per knooppunt uitvoeren en maximaal 10.000 werkstromen in de wachtrij plaatsen als het aantal actief uitgevoerde werkstromen is bereikt.

Wanneer het vRealize Orchestrator-knooppunt meer dan 300 gelijktijdige werkstromen moet uitvoeren, worden de wachtende werkstroomuitvoeringen in de wachtrij geplaatst. Wanneer een actieve werkstroomuitvoering is voltooid, wordt de volgende werkstroom in de wachtrij uitgevoerd. Als het maximum aantal werkstromen in de wachtrij is bereikt, wordt de volgende werkstroom uitgevoerd totdat een van de in behandeling zijnde werkstromen wordt uitgevoerd.

Op de pagina **Geavanceerde opties** in het Control Center kunt u de eigenschappen van de werkstroomuitvoering configureren.

Optie	Beschrijving
<b>Veilige modus inschakelen</b>	Als de veilige modus is ingeschakeld, worden alle actieve werkstromen geannuleerd en worden ze niet hervat wanneer het Orchestrator-knooppunt de volgende keer wordt opgestart.
<b>Aantal gelijktijdige actieve werkstromen</b>	Het maximum aantal Orchestrator-knooppuntwerkstromen die tegelijk worden uitgevoerd.
<b>Maximum aantal actieve werkstromen in de wachtrij</b>	Het aantal aanvragen voor werkstroomuitvoeringen dat het Orchestrator-knooppunt accepteert voordat deze onbeschikbaar wordt.
<b>Maximum aantal bewaarde uitvoeringen per werkstroom</b>	Het maximum aantal voltooide werkstroomuitvoeringen dat wordt opgeslagen als geschiedenis per werkstroom in een cluster. Als het aantal wordt overschreden, worden de oudste werkstroomuitvoeringen verwijderd.
<b>Vervaldagen voor logboekgebeurtenissen</b>	Het aantal dagen dat logboekgebeurtenissen voor het cluster in de database worden bewaard voordat ze worden leeggemaakt.

## vRealize Orchestrator-logboekbestanden

VMware Technical Support vraagt doorgaans om diagnostische gegevens wanneer u een ondersteuningsaanvraag verzendt. Deze diagnostische informatie bevat productspecifieke logboeken en configuratiebestanden van de host waarop het product wordt uitgevoerd.

vRealize Orchestrator Appliance-logboeken worden opgeslagen in de directory /data/vco/usr/lib/vco/app-server/logs/. U exporteert de logboeken van uw vRealize Orchestrator Appliance-implementatie door u aan te melden op de opdrachtregel van de appliance en de `vracli log-bundle`-opdracht uit te voeren. De gegenereerde logboekbundel wordt opgeslagen in de rootmap van uw vRealize Orchestrator Appliance.

## Persistentie van logboekregistratie

U kunt informatie in elk type vRealize Orchestrator-script vastleggen, bijvoorbeeld werkstroom, beleid of actie. Deze informatie heeft typen en niveaus. Het type kan persistent of niet-persistent zijn. Het niveau kan DEBUG, INFO, WARN, ERROR, TRACE en FATAL zijn.

**Tabel 7-1. Persistente en niet-persistente logboeken maken**

Logboekniveau	Persistent type	Niet-persistent type
DEBUG	<code>Server.debug("short text", "long text");</code>	<code>System.debug("text")</code>
INFO	<code>Server.log("short text", "long text");</code>	<code>System.log("text");</code>
WARN	<code>Server.warn("short text", "long text");</code>	<code>System.warn("text");</code>
ERROR	<code>Server.error("short text", "long text");</code>	<code>System.error("text");</code>



## Persistente logboeken

Persistente logboeken (serverlogboeken) houden logboeken bij van vroegere werkstroomuitvoeringen en worden opgeslagen in de vRealize Orchestrator-database.

## Niet-persistente logboeken

Wanneer u een niet-persistent logboek (systeemlogboek) gebruikt om scripts te maken, stelt de vRealize Orchestrator-server alle actieve vRealize Orchestrator-applicaties op de hoogte over dit logboek, maar deze informatie wordt niet opgeslagen in de database. Wanneer de applicatie opnieuw wordt gestart, gaat de logboekinformatie verloren. Niet-persistente logboeken worden gebruikt voor foutopsporing en voor live-informatie. Als u systeemlogboeken wilt weergeven, moet u een voltooide werkstroomuitvoering selecteren in de vRealize Orchestrator Client en het tabblad **Logboeken** selecteren.

## Configuratie van vRealize Orchestrator-logboeken

Op de pagina **Logboeken configureren** in het Control Center kunt u het niveau van het serverlogboek en het scriptlogboek instellen dat u nodig heeft. Als een van de logboeken meerdere malen per dag is gegenereerd, is het lastig om te bepalen waardoor de problemen worden veroorzaakt.

Het standaardlogboekniveau van het serverlogboek en het scriptlogboek is INFO. Het wijzigen van het logboekniveau beïnvloedt alle nieuwe berichten die de server in de logboeken invoert en het aantal actieve verbindingen met de database. De uitgebreide logboekregistratie neemt af in aflopende volgorde.

---

**Voorzichtig** Stel het logboekniveau alleen in op DEBUG of ALL om een probleem op te lossen. Gebruik deze instellingen niet in een productieomgeving omdat dit de prestaties ernstig kan beïnvloeden.

---

## vRealize Orchestrator-logboeken genereren

U kunt de logboeken van uw implementatie exporteren door u aan te melden bij de vRealize Orchestrator Appliance-opdrachtregel als **root** en de `vraccli log-bundle`-opdracht uit te voeren. De gegenereerde logboekbundel wordt opgeslagen in de hoofdmap van de appliance.

---

**Opmerking** Wanneer u meer dan één vRealize Orchestrator-instantie in een cluster heeft, bevat de logboekbundel de logboeken van alle vRealize Orchestrator-instanties in het cluster.

---

## Integratie van logboekregistratie met vRealize Log Insight configureren

U kunt vRealize Orchestrator configureren om uw logboekinformatie naar een vRealize Log Insight-server te verzenden.

U kunt een integratie van logboekregistratie op een vRealize Log Insight-server configureren via de vRealize Orchestrator Appliance-opdrachtregel.

---

**Opmerking** Zie [Een syslog-integratie in vRealize Orchestrator maken of overschrijven](#) voor informatie over het configureren van een integratie van logboekregistratie met een externe syslog-server.

---

#### Voorwaarden

- Configureer uw vRealize Log Insight-server. Raadpleeg de *Documentatie voor vRealize Log Insight*.
- Controleer of uw vRealize Log Insight-versie 4.7.1 of hoger is.

#### Procedure

- 1 Meld u als **root** aan op de vRealize Orchestrator Appliance-opdrachtregel.
- 2 Als u de integratie van logboekregistratie met vRealize Log Insight wilt configureren, voert u de opdracht `vracli vrli setvRLI_FQDN` uit.

---

**Opmerking** Als uw vRealize Orchestrator-instantie een zelfondertekend certificaat gebruikt, kunt u de SSL-verificatie uitschakelen door het optionele argument `-k` of `--insecure` op te nemen.

---

#### Wat nu te doen

Voer de opdracht `vracli vrli -h` uit voor meer informatie over vRealize Log Insight-configuratieopties.

## Een syslog-integratie in vRealize Orchestrator maken of overschrijven

U kunt vRealize Orchestrator configureren om uw logboekinformatie te verzenden naar een of meer externe syslog-servers.

De opdracht `vracli remote-syslog set` wordt gebruikt om een syslog-integratie te maken of om bestaande integraties te overschrijven.

Externe syslog-integratie met vRealize Orchestrator ondersteunt drie verbindingstypen:

- Via UDP.
- Via TCP zonder TLS.

---

**Opmerking** Als u een syslog-integratie wilt maken zonder gebruik van TLS, voegt u de `--disable-ssl`-markering toe aan de `vracli remote-syslog set`-opdracht.

---

- Via TCP met TLS.

Zie [Integratie van logboekregistratie met vRealize Log Insight configureren](#) voor informatie over het configureren van een integratie van logboeken met vRealize Log Insight.

## Voorwaarden

Configureer een of meer externe syslog-servers.

## Procedure

- 1 Meld u als **root** aan op de vRealize Orchestrator Appliance-opdrachtregel.
- 2 Als u een integratie wilt maken met een syslog-server, voert u de opdracht `vracli remote-syslog set` uit.

```
vracli remote-syslog set -id name_of_integration protocol_type://syslog_URL_or_FQDN:syslog_port
```

**Opmerking** Als u geen poort invoert in de opdracht `vracli remote-syslog set`, wordt de poortwaarde standaard ingesteld op 514.

**Opmerking** U kunt een certificaat toevoegen aan de syslog-configuratie. Gebruik de `--ca-file`-markering om een certificaatbestand toe te voegen. Gebruik de `--ca-cert`-markering om een certificaat als tekst zonder opmaak toe te voegen.

- 3 (Optioneel) Als u een bestaande syslog-integratie wilt overschrijven, voert u de opdracht `vracli remote-syslog set` uit en stelt u de waarde van de `-id`-markering in op de naam van de integratie die u wilt overschrijven.

**Opmerking** Standaard vraagt de vRealize Orchestrator Appliance dat u bevestigt dat u de syslog-integratie wilt overschrijven. Voeg de markering `-f` of `--force` toe aan de opdracht `vracli remote-syslog set` om de bevestigingsaanvraag over te slaan.

## Wat nu te doen

Voer de opdracht `vracli remote-syslog` uit om de huidige syslog-integraties in de toepassing te bekijken.

## Een syslog-integratie in vRealize Orchestrator verwijderen

U kunt syslog-integraties van uw vRealize Orchestrator Appliance verwijderen door de opdracht `vracli remote-syslog unset` uit te voeren.

## Voorwaarden

Maak een of meer syslog-integraties in de vRealize Orchestrator Appliance. Zie [Een syslog-integratie in vRealize Orchestrator maken of overschrijven](#).

## Procedure

- 1 Meld u als **root** aan op de vRealize Orchestrator Appliance-opdrachtregel.

- 2 Verwijder syslog-integraties van de vRealize Orchestrator Appliance.
  - a Als u een specifieke syslog-integratie wilt verwijderen, voert u de opdracht `vracli remote-syslog unset -id Integration_name` uit.
  - b Als u alle syslog-integraties wilt verwijderen op de vRealize Orchestrator Appliance, voert u de opdracht `vracli remote-syslog unset` uit zonder de markering `-id`.

**Opmerking** Standaard vraagt de vRealize Orchestrator Appliance dat u bevestigt dat u alle syslog-integraties wilt verwijderen. Voeg de markering `-f` of `--force` toe aan de opdracht `vracli remote-syslog unset` om de bevestigingsaanvraag over te slaan.

## Logboekregistratie voor Kerberos-foutopsporing inschakelen

U kunt problemen met vRealize Orchestrator-invoegtoepassingen oplossen door het Kerberos-configuratiebestand te wijzigen dat door de invoegtoepassing wordt gebruikt.

Het Kerberos-configuratiebestand bevindt zich in de map `/data/vco/usr/lib/vco/app-server/conf/` van de vRealize Orchestrator Appliance.

### Procedure

- 1 Meld u als **root** aan op de vRealize Orchestrator Appliance-opdrachtregel.
- 2 Voer de opdracht `kubect1 -n prelude edit deployment vco-app` uit.
- 3 Zoek en bewerk de tekenreeks `-Djava.security.krb5.conf=/usr/lib/vco/app-server/conf/krb5.conf` in het implementatiebestand.

```
-Djava.security.krb5.conf=/usr/lib/vco/app-server/conf/krb5.conf -Dsun.security.krb5.debug=true'
```

- 4 Sla de wijzigingen op en sluit de bestandseditor.
- 5 Voer de opdracht `kubect1 -n prelude get pods` uit.  
Wacht totdat alle pods worden uitgevoerd.
- 6 Controleer of logboekregistratie voor Kerberos-foutopsporing is ingeschakeld.

```
kubect1 -n prelude log {vco_app_name} -c vco-server-app | grep krb5
```

Controleer of de logboeken een vergelijkbaar bericht bevatten.

```
kubect1 -n prelude log vco-app-5c965f9b9d-v8srd -c vco-server-app | grep krb5
12:23:05,417 INFO 011N:75 - Sysprop: java.security.krb5.conf = /usr/lib/vco/app-server/conf/krb5.conf
12:23:05,421 INFO 011N:75 - Sysprop: sun.security.krb5.debug = true
2019-10-22 12:23:38.521+0000 [Thread-19] INFO {} [011N] Sysprop: java.security.krb5.conf = /usr/lib/vco/app-server/conf/krb5.conf
2019-10-22 12:23:38.525+0000 [Thread-19] INFO {} [011N] Sysprop: sun.security.krb5.debug = true
Java config name: /usr/lib/vco/app-server/conf/krb5.conf
EType: sun.security.krb5.internal.crypto.Aes256CtsHmacSha1ETType
```

## OpenTracing- en Wavefront-extensies inschakelen

De OpenTracing- en Wavefront-extensies voor vRealize Orchestrator bieden hulpprogramma's voor het verzamelen van gegevens over uw vRealize Orchestrator-omgeving. U kunt deze gegevens gebruiken voor het oplossen van problemen met het vRealize Orchestrator-systeem en de werkstromen ervan.

Voordat u vRealize Orchestrator kunt configureren om de OpenTracing- en Wavefront-extensies te gebruiken, moet u deze in de vRealize Orchestrator Appliance inschakelen.

### Voorwaarden

Controleer of de vRealize Orchestrator Appliance SSH-service is ingeschakeld. Zie [SSH-toegang tot de vRealize Orchestrator Appliance in- of uitschakelen](#).

### Procedure

- 1 Meld u aan bij de vRealize Orchestrator Appliance via SSH als **root**.
- 2 Voer de opdracht `kubectl -n prelude get pod` uit.
- 3 Voer de opdracht `kubectl -n prelude exec -it vco-app-your_pod_ID -c vco-server-app -- ls /var/lib/vco/app-server/extensions` uit om alle beschikbare extensies weer te geven.
- 4 Voer de volgende opdracht uit om de OpenTracing-extensie in te schakelen:  

```
kubectl -n prelude exec -it vco-app-your_pod_ID -c vco-server-app -
mv /var/lib/vco/app-server/extensions/
opentracing-8.1.0.jar.inactive /var/lib/vco/app-server/extensions/
opentracing-8.1.0.jar
```
- 5 Voer de volgende opdracht uit om de Wavefront-extensie in te schakelen:  

```
kubectl -n prelude exec -it vco-app-your_pod_ID -c vco-server-app -
mv /var/lib/vco/app-server/extensions/wavefront-8.1.0.jar.inactive /var/lib/vco/
app-server/extensions/wavefront-8.1.0.jar
```
- 6 Meld u aan bij het Control Center en controleer of de extensies worden weergegeven op de pagina **Extensie-eigenschappen**.

### Wat nu te doen

Configureer OpenTracing- en Wavefront-integratie met vRealize Orchestrator op de pagina **Extensie-eigenschappen**. Zie [De OpenTracing-extensie configureren](#) en [De Wavefront-extensie configureren](#).

## De OpenTracing-extensie configureren

De OpenTracing-extensie stuurt gegevens over werkstroomuitvoeringen naar een Jaeger-server. Gegevens omvatten de werkstroomstatus, in- en uitvoerparameters, de gebruiker die de werkstroomuitvoering heeft gestart en de werkstroom-id-gegevens.

### Voorwaarden

- Controleer of OpenTracing is ingeschakeld in de vRealize Orchestrator Appliance. Zie [OpenTracing- en Wavefront-extensies inschakelen](#).
- Implementeer een Jaeger-server voor gebruik in de OpenTracing-extensie. Voor meer informatie raadpleegt u de [Documentatie om aan de slag te gaan met Jaeger](#).

### Procedure

- 1 Meld u aan bij het Control Center als **root**.
- 2 Selecteer de pagina **Extensie-eigenschappen**.
- 3 Selecteer de OpenTracing-extensie.
- 4 Voer het hostadres en de poort van de Jaeger-server in.

---

**Opmerking** Voeg twee slashes ("/") toe voordat u het serveradres invoert.

---

- 5 Klik op **Opslaan**.

### Resultaten

U heeft de OpenTracing -extensie voor vRealize Orchestrator geconfigureerd.

### Wat nu te doen

- Om toegang te krijgen tot de Jaeger-gebruikersinterface met de gegevens die zijn verzameld door de OpenTracing-extensie, gaat u naar het hostadres dat is ingevoerd tijdens de configuratie.
- Selecteer **Werkstromen** onder de optie **Service**.
- Gebruik de optie **Tags** om op te geven welke gegevens moeten worden weergegeven. Als u bijvoorbeeld gegevens over mislukte werkstromen wilt weergeven, voert u **status=failed** in.

## De Wavefront-extensie configureren

Gebruik de Wavefront-extensie om metrische gegevens over uw vRealize Orchestrator-systeem en werkstromen te verzamelen.

### Voorwaarden

- 1 Controleer of Wavefront is ingeschakeld in de vRealize Orchestrator Appliance. Zie [OpenTracing- en Wavefront-extensies inschakelen](#).
- 2 Importeer het Wavefront-certificaat:
  - a Meld u aan bij het vRealize Orchestrator Control Center als **root**.
  - b Selecteer de pagina **Certificaten**.
  - c Klik op het vervolgkeuzemenu **Importeren** en selecteer **Importeren vanaf URL**.
  - d Voer de Wavefront-URL in en klik op **Importeren**.

- 3 Configureer een Wavefront-proxy. Zie [Wavefront-proxy's installeren en beheren](#) voor meer informatie.

#### Procedure

- 1 Meld u aan bij het vRealize Orchestrator Control Center als **root**.
- 2 Selecteer de pagina **Extensie-eigenschappen**.
- 3 Selecteer de Wavefront-extensie.
- 4 Configureer de Wavefront-eigenschappen.

Optie	Beschrijving
<b>Proxy</b>	Het Wavefront-proxyadres.
<b>Host</b>	Optioneel. Het Wavefront-hostadres.
<b>Token</b>	Optioneel. Het Wavefront-API-token. Zie <a href="#">Een API-token genereren</a> voor meer informatie over het genereren van een Wavefront-API-token.
<b>Voorvoegsel</b>	Voeg voorvoegsellabels toe voor elke metriek die naar Wavefront wordt verzonden. Voorvoegsellabels worden gescheiden door een puntsymbool.

- 5 (Optioneel) Selecteer **Standaarddashboard verzenden bij volgende start**.
- 6 Klik op **Opslaan**.

#### Resultaten

U heeft de Wavefront-extensie voor vRealize Orchestrator geconfigureerd.

#### Wat nu te doen

- Om toegang te krijgen tot de metriekeken die door Wavefront worden verzameld, opent u het dashboard op het adres dat tijdens de configuratie is ingevoerd.
- Als u meldingen wilt ontvangen over specifieke gebeurtenissen in uw vRealize Orchestrator-omgeving, kunt u Wavefront-waarschuwingen gebruiken. Raadpleeg de [Documentatie voor Wavefront-waarschuwingen](#) voor meer informatie.

## Tijdssynchronisatie voor vRealize Orchestrator inschakelen

U kunt de tijdssynchronisatie op uw vRealize Orchestrator-implementatie inschakelen met de vRealize Orchestrator Appliance-opdrachtregel.

U kunt de tijdssynchronisatie voor uw standalone of geclusterde vRealize Orchestrator-implementatie configureren met behulp van het NTP-communicatieprotocol (Network Time Protocol). vRealize Orchestrator ondersteunt twee elkaar wederzijds uitsluitende NTP-configuraties:

NTP-configuratie	Beschrijving
ESXi	<p>Deze configuratie kan worden gebruikt wanneer de ESXi-server die als host fungeert van de vRealize Orchestrator Appliance, wordt gesynchroniseerd met een NTP-server. Als u een geclusterde implementatie gebruikt, moeten alle ESXi-hosts worden gesynchroniseerd met een NTP-server. Zie voor meer informatie over het configureren van NTP voor ESXi <a href="#">NTP (Network Time Protocol) op een ESXi-host configureren met behulp van de vSphere Web Client</a>.</p> <hr/> <p><b>Opmerking</b> Als uw vRealize Orchestrator-implementatie wordt gemigreerd naar een ESXi-host die niet is gesynchroniseerd met een NTP-server, kan klokdrift optreden.</p>
systemd	<p>Deze configuratie gebruikt de systemd-timesyncd-daemon om de klokken van uw vRealize Orchestrator-implementatie te synchroniseren.</p> <hr/> <p><b>Opmerking</b> De systemd-timesyncd-daemon is standaard ingeschakeld, maar geconfigureerd zonder NTP-servers. Als de vRealize Orchestrator Appliance een dynamische IP-configuratie gebruikt, kan de toepassing alle NTP-servers gebruiken die door het DHCP-protocol worden ontvangen.</p>

## Procedure

- 1 Meld u als **root** aan op de vRealize Orchestrator Appliance-opdrachtregel.
- 2 Schakel NTP in met ESXi.
  - a Voer de opdracht `vracli ntp esxi` uit.
  - b Voer de opdracht `vracli ntp apply` uit.

De ESXi NTP-configuratie wordt toegepast op de vRealize Orchestrator-implementatie.
- 3 Schakel NTP in met systemd.
  - a Voer de opdracht `vracli ntp systemd --set FQDN_or_IP_of_systemd_server` uit.

---

**Opmerking** U kunt meerdere systemd NTP-servers toevoegen door hun netwerkadressen te scheiden met een komma.

---

  - b Voer de opdracht `vracli ntp apply` uit.

De systemd NTP-configuratie wordt toegepast op de vRealize Orchestrator-implementatie.
- 4 (Optioneel) Voer de opdracht `vracli ntp status` uit om de status van de NTP-configuratie te bevestigen.



## Wat nu te doen

De NTP-configuratie kan mislukken als er een tijdsverschil van meer dan 10 minuten tussen de NTP-server en de vRealize Orchestrator-implementatie bestaat. Om dit probleem op te lossen, moet u de vRealize Orchestrator Appliance opnieuw opstarten.

## Tijdssynchronisatie voor vRealize Orchestrator uitschakelen

U kunt de NTP-tijdssynchronisatie (Network Time Protocol) voor uw vRealize Orchestrator-implementatie uitschakelen met de vRealize Orchestrator Appliance-opdrachtregel.

U kunt de NTP-configuratie van uw vRealize Orchestrator Appliance ook opnieuw instellen op de standaardstatus door de `vraccli ntp reset`-opdracht uit te voeren. Nadat u de configuratie opnieuw heeft ingesteld, moet u de wijzigingen toepassen door de `vraccli ntp apply`-opdracht uit te voeren.

### Voorwaarden

Controleer of u de tijdssynchronisatie met ESXi of systemd heeft geconfigureerd. Zie [Tijdssynchronisatie voor vRealize Orchestrator inschakelen](#).

### Procedure

- 1 Meld u als **root** aan op de vRealize Orchestrator Appliance-opdrachtregel.
- 2 Voer de opdracht `vraccli ntp disable` uit om de tijdssynchronisatie met ESXi of systemd uit te schakelen.
- 3 Voer de opdracht `vraccli ntp apply` uit.
- 4 (Optioneel) Voer de opdracht `vraccli ntp status` uit om de status van de NTP-configuratie te bevestigen.

# Toepassingsvoorbeelden voor configuratie en probleemoplossing

## 8

De toepassingsvoorbeelden voor configuratie bieden taakstromen die u kunt uitvoeren om te voldoen aan de specifieke configuratievereisten van uw vRealize Orchestrator-server en probleemoplossingsonderwerpen die u kunt raadplegen bij het oplossen van een probleem.

Dit hoofdstuk omvat de volgende onderwerpen:

- [vRealize Orchestrator-invoegtoepassing voor vSphere Web Client configureren](#)
- [Actieve werkstromen annuleren](#)
- [Foutopsporing voor de vRealize Orchestrator-server inschakelen](#)
- [De grootte van de vRealize Orchestrator Appliance-schijven wijzigen](#)
- [De grootte van het heapgeheugen van de vRealize Orchestrator-server aanpassen](#)
- [Noodherstel van vRealize Orchestrator met behulp van Site Recovery Manager](#)

## vRealize Orchestrator-invoegtoepassing voor vSphere Web Client configureren

Als u de vRealize Orchestrator-invoegtoepassing voor de vSphere Web Client wilt gebruiken, moet u vRealize Orchestrator registreren als een extensie van vCenter Server.

Nadat u uw vRealize Orchestrator-server met vCenter Single Sign-On heeft geregistreerd en geconfigureerd om met vCenter Server te werken, moet u vRealize Orchestrator registreren als een extensie van vCenter Server.

### Voorwaarden

- Controleer of SSH-toegang is ingeschakeld voor de vRealize Orchestrator Appliance. Zie [SSH-toegang tot de vRealize Orchestrator Appliance in- of uitschakelen](#).
- U moet vRealize Orchestrator met vSphere-verificatie registreren voor dezelfde Platform Services-controller die door uw beheerde vCenter Server wordt geverifieerd.
- Kopieer de vco-plugin.zip naar de vRealize Orchestrator Appliance:
  - a Download het bestand vco-plugin.zip van het [VMware-technologienetwerk](#).

- b Open een SSH-client.

---

**Opmerking** Voor Linux- of MacOS-omgevingen kunt u de opdrachtregelinterface van Terminal gebruiken. Voor Windows-omgevingen kunt u de PuTTY-client gebruiken.

---

- c Als u het bestand `vco-plugin.zip` wilt kopiëren, voert u de opdracht Secure Copy uit.

```
For Linux/MacOS: scp ~/<zip_download_dir>/vco-plugin.zip root@<orchestrator_FQDN_or_IP>:/data/vco/usr/lib/vco/downloads/vco-plugin.zip
```

```
For Windows: pscp C:\<zip_download_dir>\vco-plugin.zip root@<orchestrator_FQDN_or_IP>:/data/vco/usr/lib/vco/downloads/vco-plugin.zip
```

#### Procedure

- 1 Meld u aan bij de vRealize Orchestrator Client.
- 2 Ga naar **Bibliotheek > Werkstromen**.
- 3 Zoek de werkstroom **vCenter Orchestrator registreren als een vCenter Server-extensie** en klik op **Uitvoeren**.
- 4 Selecteer de vCenter Server-instantie waarmee u vRealize Orchestrator wilt registreren.
- 5 Voer `https://your_orchestrator_FQDN` of de service-URL in van de load balancer die de aanvragen omleidt naar de vRealize Orchestrator-serverknooppunten.
- 6 Klik op **Uitvoeren**.

## Actieve werkstromen annuleren

U kunt het vRealize Orchestrator Control Center gebruiken om werkstromen te annuleren die niet correct worden voltooid.

#### Procedure

- 1 Meld u aan bij Control Center als **root**.
- 2 Klik op **Problemen oplossen**.

### 3 Annuleer actieve werkstromen.

Optie	Beschrijving
<b>Alle werkstroomuitvoeringen annuleren</b>	Voer een werkstroom-id in om alle tokens voor die werkstroom te annuleren.
<b>Werkstroomuitvoeringen annuleren op id</b>	Voer alle token-id's in, die u wilt annuleren. Scheid id's met een komma.
<b>Alle actieve werkstromen annuleren</b>	Annuleer alle actieve werkstromen op de server.

**Opmerking** Handelingen waarbij u werkstromen op id annuleert, kunnen mogelijk niet correct worden uitgevoerd omdat er geen betrouwbare manier is om de uitvoeringsthread onmiddellijk te annuleren.

#### Resultaten

Op de volgende start van de server worden de werkstromen ingesteld met de status Geannuleerd.

## Foutopsporing voor de vRealize Orchestrator-server inschakelen

U kunt de vRealize Orchestrator-server in de foutopsporingsmodus starten om problemen op te lossen bij het ontwikkelen van een invoegtoepassing.

#### Voorwaarden

Installeer en configureer het Kubernetes-opdrachtregelprogramma op uw lokale machine. Zie [Kubectl installeren en instellen](#).

#### Procedure

- 1 Meld u als **root** aan op de vRealize Orchestrator Appliance-opdrachtregel.
- 2 Voer de opdracht `kubectl -n prelude edit deployment vco-app` uit.
- 3 Bewerk het YAML-implementatiebestand door een omgevingsvariabele voor foutopsporing toe te voegen aan de container `vco-server-app`. De variabele moet worden toegevoegd onder de sectie `env` van de container `vco-server-app`.

```
containers:
  - command:
    ...
    env:
      - name: DEBUG_PORT
```

```

        value: "your_desired_debug_port"
        ...
    name: vco-server-app
    ...

```

---

**Opmerking** Wanneer u de omgevingsvariabele voor foutopsporing toevoegt aan de sectie `env`, moet u de opmaak van de YAML-inspringing volgen zoals weergegeven in het vorige voorbeeld.

---

- 4 Sla de wijzigingen in het implementatiebestand op.

Als de bewerking naar het implementatiebestand is gelukt, ontvangt u het bericht `deployment.extensions/vco-app bewerkt`.

- 5 Genereer het Kubernetes-configuratiebestand door de opdracht `vracli dev kubeconfig` uit te voeren.

Aangezien kubeconfig een ontwikkelaarsomgeving is, wordt u gevraagd om te bevestigen dat u wilt doorgaan. Voer **Ja** in om door te gaan of **Nee** om te stoppen.

- 6 Kopieer de inhoud van het gegenereerde configuratiebestand van `apiVersion: v1` tot en met de `client-key-data`-inhoud.
- 7 Sla het gegenereerde Kubernetes-configuratiebestand op uw lokale machine op.
- 8 Meld u af bij de vRealize Orchestrator Appliance.
- 9 Voltooi de configuratie van de foutopsporingsmodus op uw lokale machine.
  - a Open een opdrachtregelshell.
  - b Bind de `KUBECONFIG`-omgevingsvariabele aan het opgeslagen configuratiebestand.

---

**Opmerking** Dit voorbeeld is gebaseerd op een Linux-omgeving.

---

```
export KUBECONFIG=/file/path/fileName
```

- c Voer de opdracht `kubectl cluster-info` uit om te valideren of de services worden uitgevoerd.
- d Om het configureren van de foutopsporingsmodus te voltooien, voert u de volgende Kubernetes API-aanvraag uit.

---

**Opmerking** De waarde van de `localhost_debug_port`-variabele is de poort die is ingesteld in uw configuratie voor externe foutopsporing van uw IDE (Integrated Development Environment). De waarde van de `vro_debug_port`-variabele wordt gegenereerd tijdens stap 3 van deze procedure.

---

```
kubectl port-forward pod/vco_app_pod_ID localhost_debug_port:vro_debug_port
```

---

**Belangrijk** Wanneer u het foutopsporingsprogramma configureert, geeft u de DNS- en IP-instellingen op van de lokale machine waarop u de opdracht voor het doorsturen van poorten heeft uitgevoerd.

---

## Resultaten

U heeft foutopsporing voor de server geconfigureerd voor uw vRealize Orchestrator Appliance.

## De grootte van de vRealize Orchestrator Appliance-schijven wijzigen

U kunt de schijfgrootte van de vRealize Orchestrator Appliance wijzigen door de instellingen voor de schijfgrootte van de vRealize Orchestrator Appliance virtuele machine in vSphere te bewerken.

## Voorwaarden

Controleer of de vRealize Orchestrator Appliance SSH-service is ingeschakeld. Zie [SSH-toegang tot de vRealize Orchestrator Appliance in- of uitschakelen](#).

## Procedure

- 1 Controleer de momenteel beschikbare schijfruimte in de vRealize Orchestrator Appliance.

---

**Opmerking** De vRealize Orchestrator Appliance-schijven hebben ten minste 20 procent vrije schijfruimte nodig.

---

- a Meld u via SSH als **rootgebruiker** aan bij de vRealize Orchestrator Appliance-opdrachtregel.
- b Voer de opdracht `vracli disk-mgr` uit.

- 2 Wijzig de grootte van de schijf van de vRealize Orchestrator Appliance virtuele machine in vSphere.
  - a Meld u aan bij de vSphere Client als een **beheerder**.
  - b Schakel de vRealize Orchestrator Appliance virtuele machine uit.
  - c Klik met de rechtermuisknop op de virtuele machine en selecteer **Instellingen bewerken**.
  - d Vouw op het tabblad **Virtuele hardware Harde schijf** uit om de schijfinstellingen weer te geven en te wijzigen en klik op **OK**.

Zie voor meer informatie over het wijzigen van de schijfgrootte van vSphere virtuele machines *De configuratie van de virtuele schijf wijzigen in Beheer van vSphere-virtuele machines*.

## De grootte van het heapgeheugen van de vRealize Orchestrator-server aanpassen

U kunt de grootte van het heapgeheugen van de vRealize Orchestrator-server aanpassen door het implementatiebestand te bewerken.

U kunt de grootte van het heapgeheugen van de vRealize Orchestrator-server aanpassen, zodat uw Orchestration-omgeving het wijzigen van belastingen kan beheren. U kunt bijvoorbeeld het heapgeheugen van uw vRealize Orchestrator-implementatie vergroten als u van plan bent meerdere vCenter-servers te beheren.

### Voorwaarden

- Schakel SSH-toegang tot de vRealize Orchestrator Appliance in. Zie [SSH-toegang tot de vRealize Orchestrator Appliance in- of uitschakelen](#).
- Vergroot het RAM-geheugen van de virtuele machine waarop vRealize Orchestrator wordt geïmplementeerd tot de volgende geschikte verhoging. Voor informatie over het vergroten van het RAM-geheugen van een virtuele machine in vSphere raadpleegt u *De geheugenconfiguratie wijzigen in Beheer van vSphere-virtuele machines*.

### Procedure

- 1 Meld u via SSH als **rootgebruiker** aan bij de vRealize Orchestrator Appliance-opdrachtregel.
- 2 Ga naar de map `/opt/charts/vco/templates/`.
- 3 Maak een back-up van het bestand `deployment.yaml`.

```
cp deployment.yaml /tmp/
```

- 4 Bewerk het bestand `deployment.yaml` met behulp van uw voorkeurseditor.

```
vi deployment.yaml
```

- 5 Zoek naar regels met de env-tekenreeks totdat u de vco-server-app-container vindt.

```
- name: vco-server-app
  image: {{ .Values.image.repository }}:{{ .Values.image.tag }}
  env:
    - name: JAVA_PROXY_SCHEMEE
```

- 6 Voeg in de sectie env een JVM\_HEAP-omgevingsvariabele toe met een waarde, waarbij {DESIRED\_HEAP\_SIZE} overeenkomt met de nieuwe gewenste grootte van het heapgeheugen, bijvoorbeeld 4G.

```
- name: vco-server-app
  image: {{ .Values.image.repository }}:{{ .Values.image.tag }}
  env:
    - name: JVM_HEAP
      value: {DESIRED_HEAP_SIZE}
    - name: JAVA_PROXY_SCHEME
```

- 7 Zoek naar regels met de memory: 5G-tekenreeks in het implementatiebestand.

---

**Opmerking** Het implementatiebestand mag slechts één memory: 5G-tekenreeks hebben.

---

```
resources:
  limits:
    memory: 5G
  requests:
    memory: 4G
```

- 8 Verhoog de limieten en aanvragen van de container.

---

**Voorzichtig** De memory:-waarde van de limieten moet een waarde hebben die 2 GB hoger is dan de waarde voor het JVM\_HEAP-geheugen in stap 6. Als de waarde in stap 6 bijvoorbeeld value: 4G is, moet u de geheugenwaarde voor limieten instellen op memory: 6G. De requests: memory-waarde moet 1 GB hoger zijn dan de waarde voor het JVM\_HEAP-geheugen in stap 6. Als de heapwaarde in stap 6 bijvoorbeeld value: 4G is, moet u de geheugenwaarde voor de aanvraag instellen op memory: 5G.

---

```
resources:
  limits:
    memory: {Desired heap size + 2G}
  requests:
    memory: {Desired heap size + 1G}
```

- 9 Sla uw wijzigingen in het implementatiebestand op en ga naar de map /opt/scripts.

---

**Opmerking** Voor geclusterde omgevingen voert u de voorgaande stappen uit op alle knooppunten van het cluster.

---



10 Voer de opdracht `deploy.sh` uit.

---

**Opmerking** Voor geclusterde omgevingen voert u het implementatiescript op het primaire knooppunt uit.

---

## Resultaten

U heeft de grootte van het heapgeheugen van uw vRealize Orchestrator-server gewijzigd.

## Noodherstel van vRealize Orchestrator met behulp van Site Recovery Manager

U moet Site Recovery Manager configureren om uw vRealize Orchestrator te beveiligen. Bevestig deze beveiliging door de algemene configuratietaken voor Site Recovery Manager in te vullen.

### De omgeving voorbereiden

U moet ervoor zorgen dat u voldoet aan de volgende vereisten voordat u begint met het configureren van Site Recovery Manager.

- Controleer of vSphere 6.0 of hoger is geïnstalleerd op de beveiligde sites en herstelsites.
- Controleer of u Site Recovery Manager 8.1 of hoger gebruikt.
- Controleer of vRealize Orchestrator is geconfigureerd.

### Virtuele machines voor vSphere Replication configureren

U moet de virtuele machines voor vSphere Replication of op array gebaseerde replicatie configureren om Site Recovery Manager te kunnen gebruiken.

Voer de volgende stappen uit om vSphere Replication op de vereiste virtuele machines in te schakelen.

#### Procedure

- 1 Selecteer in de vSphere Web Client een virtuele machine waarop vSphere Replication moet worden ingeschakeld en klik op **Acties > Alle vSphere Replication-acties > Replicatie configureren**.
- 2 Selecteer in het venster **Replicatietype Repliceren naar een vCenter Server** en klik op **Volgende**.
- 3 Selecteer in het venster **Doelsite** de vCenter voor de herstellocatie en klik op **Volgende**.
- 4 Selecteer in het venster **Replicatieserver** een vSphere Replication-server en klik op **Volgende**.
- 5 Klik in het venster **Doellocatie** op **Bewerken** en selecteer de doelgegevensopslag waar de gerepliceerde bestanden worden opgeslagen en klik op **Volgende**.
- 6 Behoud de standaardinstelling in het venster **Replicatieopties** en klik op **Volgende**.

- 7 Voer in het venster **Herstelinstellingen** de tijd in voor **Recovery Point Objective (RPO)** en **Tijds puntinstanties** en klik op **Volgende**.
- 8 Controleer de instellingen in het venster **Gereed om te voltooien** en klik op **Voltooien**.
- 9 Herhaal deze stappen voor alle virtuele machines waarop vSphere Replication moet worden ingeschakeld.

## Protection groups maken

U maakt protection groups om Site Recovery Manager in te schakelen om uw virtuele machines te beveiligen.

U kunt protection groups in mappen indelen. Op het tabblad **Protection groups** worden de namen van de protection groups weergegeven, maar wordt niet weergegeven in welke map ze worden geplaatst. Als u twee protection groups met dezelfde naam in verschillende mappen heeft, kan het lastig zijn om ze uit elkaar te houden. Zorg er daarom voor dat de namen van de protection groups uniek zijn in alle mappen. In omgevingen waarin niet alle gebruikers weergaverechten hebben voor alle mappen, moet u de protection groups niet in mappen plaatsen om de uniekheid van de namen van protection groups te garanderen.

Wanneer u protection groups maakt, moet u ervoor zorgen dat de bewerkingen zoals verwacht worden voltooid. Zorg ervoor dat Site Recovery Manager de protection group maakt en dat de beveiliging van de virtuele machines in de groep succesvol is.

### Voorwaarden

Controleer of u een van de volgende taken heeft uitgevoerd:

- U heeft virtuele machines opgenomen in gegevensopslagplaatsen waarvoor u op array gebaseerde replicatie heeft geconfigureerd.
- U voldoet aan de vereisten in *Voorwaarden voor de protection groups voor opslagbeleid* en heeft de *Beperkingen van de protection groups voor opslagbeleid* in de handleiding voor *Beheer van Site Recovery Manager* gecontroleerd.
- U heeft vSphere Replication op uw virtuele machines geconfigureerd.
- U heeft een combinatie van enkele of alle bovenstaande opties uitgevoerd.

### Procedure

- 1 Klik in de vSphere Client of vSphere Web Client op **Site Recovery > Site Recovery openen**.
- 2 Selecteer op het starttabblad Site Recovery een sitepaar en klik op **Details weergeven**.
- 3 Selecteer het tabblad **Protection groups** en klik op **Nieuw** om een protection group te maken.
- 4 Voer op de pagina voor de naam en richting een naam en beschrijving voor de protection group in, selecteer een richting en klik op **Volgende**.

- 5 Selecteer op de pagina Type protection group het type protection group en klik op **Volgende**.

Optie	Actie
Een protection group voor op array gebaseerde replicatie maken	Selecteer <b>Gegevensopslaggroepen (op array gebaseerde replicatie)</b> en selecteer een arraypaar.
Een protection group voor vSphere Replication maken	Selecteer <b>Afzonderlijke VM's (vSphere Replication)</b> .
Een protection group voor opslagbeleid maken	Selecteer <b>Opslagbeleid (op array gebaseerde replicatie)</b> .

- 6 Selecteer gegevensopslaggroepen, virtuele machines of opslagbeleidsregels om toe te voegen aan de protection group.

Optie	Actie
Protection groups voor op array gebaseerde replicatie	Selecteer gegevensopslaggroepen en klik op <b>Volgende</b> . Wanneer u een gegevensopslaggroep selecteert, worden de virtuele machines die de groep bevat, weergegeven in de tabel met virtuele machines.
Protection groups voor vSphere Replication	Selecteer virtuele machines in de lijst en klik op <b>Volgende</b> . Alleen virtuele machines die u voor vSphere Replication heeft geconfigureerd en die nog niet in een protection group staan, worden in de lijst weergegeven.
Beveiligingsgroepen voor opslagbeleid	Selecteer opslagbeleid in de lijst en klik op <b>Volgende</b> .

- 7 Op de pagina Herstelplan kunt u optioneel de protection group toevoegen aan een herstelplan.

Optie	Actie
Toevoegen aan bestaand herstelplan	Hiermee voegt u de protection group toe aan een bestaand herstelplan.
Toevoegen aan nieuw herstelplan	Hiermee voegt u de protection group toe aan een nieuw herstelplan. Als u deze optie selecteert, moet u een naam voor het herstelplan invoeren.
Nu niet toevoegen aan het herstelplan	Selecteer deze optie als u de protection group niet wilt toevoegen aan een herstelplan.

- 8 Controleer uw instellingen en klik op **Voltooien**.

U kunt de voortgang van het maken van de protection group opvolgen op het tabblad **Protection group**.

- Voor protection groups voor op array gebaseerde replicatie en vSphere Replication geldt dat de beveiligingsstatus van de protection group OK is als Site Recovery Manager succesvol de inventaristoewijzingen op de beveiligde virtuele machines heeft toegepast.

- Voor protection groups voor opslagbeleid is de beveiligingsstatus van de protection group *OK* als Site Recovery Manager alle virtuele machines heeft beveiligd die zijn gekoppeld aan het opslagbeleid.
- Voor protection groups voor op array gebaseerde replicatie en vSphere Replication geldt dat de beveiligingsstatus van de protection group *Niet geconfigureerd* is als u geen inventaristoewijzingen heeft geconfigureerd of als Site Recovery Manager deze niet kon toepassen.
- Voor protection groups voor opslagbeleid is de beveiligingsstatus van de protection group *Niet geconfigureerd* als Site Recovery Manager niet alle virtuele machines die zijn gekoppeld aan het opslagbeleid, kan beveiligen.

### Wat nu te doen

Voor protection groups voor op array gebaseerde replicatie en vSphere Replication moet u inventaristoewijzingen toepassen op de virtuele machines als de beveiligingsstatus van de protection groups *Niet geconfigureerd* is:

- Als u inventaristoewijzingen op de hele site wilt toepassen of als u wilt controleren of de inventaristoewijzingen die u al heeft ingesteld, geldig zijn, raadpleegt u *Inventaristoewijzingen configureren* in de handleiding voor *Beheer van Site Recovery Manager*. Zie *Inventaristoewijzingen toepassen op alle leden van een protection group* in de handleiding *Beheer van Site Recovery Manager* om deze toewijzingen toe te passen op alle virtuele machines.
- Als u inventaristoewijzingen afzonderlijk wilt toepassen op elke virtuele machine in de protection group, raadpleegt u *Inventaristoewijzingen configureren voor een afzonderlijke virtuele machine in een protection group* in de handleiding voor *Beheer van Site Recovery Manager*.

Voor protection groups voor opslagbeleid, als de beveiligingsstatus van de protection group *Niet geconfigureerd* is, controleert u of u voldoet aan de vereisten in *Voorwaarden voor de protection groups voor opslagbeleid* en controleert u de *Beperkingen van de protection groups voor opslagbeleid* in de handleiding voor *Beheer van Site Recovery Manager*.

## Een herstelplan maken

U maakt een herstelplan om vast te stellen hoe Site Recovery Manager virtuele machines herstelt.

### Procedure

- 1 Klik in de vSphere Client of de vSphere Web Client op **Site Recovery > Site Recovery openen**.
- 2 Selecteer op het starttabblad Site Recovery een sitepaar en klik op **Details weergeven**.
- 3 Selecteer het tabblad **Herstelplannen** en klik op **Nieuw** om een herstelplan te maken.
- 4 Voer een naam, beschrijving en richting voor het plan in, selecteer een map en klik op **Volgende**.

- 5 Selecteer het groepstype in het menu.

Optie	Beschrijving
<b>Beveiligingsgroepen voor individuele VM's of gegevensopslagsgroepen</b>	Selecteer deze optie om een herstelplan te maken dat beveiligingsgroepen voor op array gebaseerde replicatie en vSphere Replication bevat.
<b>Beveiligingsgroepen voor opslagbeleid</b>	Selecteer deze optie om een herstelplan te maken dat beveiligingsgroepen voor opslagbeleid bevat. Als u een uitgerekte opslag gebruikt, selecteert u deze optie.

- 6 Selecteer een of meer beveiligingsgroepen voor het plan dat u wilt herstellen en klik op **Volgende**.
- 7 Selecteer in het vervolgkeuzemenu **Testnetwerk** een netwerk dat u wilt gebruiken tijdens testherstel en klik op **Volgende**.
- Als er geen toewijzingen op siteniveau zijn, wordt met de standaardoptie **Toewijzing op siteniveau gebruiken** een geïsoleerd testnetwerk gemaakt.
- 8 Controleer de samenvattingsinformatie en klik op **Voltooien** om het herstelplan te maken.

## Herstelplannen in mappen indelen

Als u de toegang van verschillende gebruikers of groepen tot herstelplannen wilt controleren, kunt u uw herstelplannen in mappen indelen.

Het indelen van herstelplannen in mappen is nuttig als u veel herstelplannen hebt. U kunt de toegang tot herstelplannen beperken door deze in mappen te plaatsen en verschillende rechten aan de mappen toe te wijzen voor verschillende gebruikers of groepen. Zie *Rollen en rechten voor Site Recovery Manager toewijzen* in de handleiding *Beheer van Site Recovery Manager* voor informatie over het toewijzen van rechten aan mappen.

### Procedure

- 1 Selecteer op het starttabblad **Site Recovery** een sitepaar en klik op **Details weergeven**.
- 2 Klik op het tabblad **Herstelplannen** en klik in het linkerdeelvenster met de rechtermuisknop op **Herstelplannen** en klik vervolgens op **Nieuwe map**.
- 3 Voer een naam in voor de map die u wilt maken en klik op **Toevoegen**.
- 4 Voeg nieuwe of bestaande herstelplannen toe aan de map.

Optie	Beschrijving
<b>Een nieuw herstelplan maken</b>	Klik met de rechtermuisknop op de map en selecteer <b>Nieuw herstelplan</b> .
<b>Een bestaand herstelplan toevoegen</b>	Klik met de rechtermuisknop op een herstelplan in de inventarisstructuur en klik op <b>Verplaatsen</b> . Selecteer een doelmap en klik op <b>Verplaatsen</b> .

## Een herstelplan bewerken

U kunt een herstelplan bewerken om de eigenschappen te wijzigen die u heeft opgegeven wanneer u het plan heeft gemaakt. U kunt herstelplannen vanaf de beveiligde site of vanaf de herstelsite bewerken.

### Procedure

- 1** Klik in de vSphere Client of de vSphere Web Client op **Site Recovery > Site Recovery** **openen**.
- 2** Selecteer op het starttabblad **Site Recovery** een sitepaar en klik op **Details weergeven**.
- 3** Klik op het tabblad **Herstelplannen**, klik met de rechtermuisknop op een herstelplan en klik op **Bewerken**.
- 4** (Optioneel) Wijzig de naam of beschrijving van het plan en klik op **Volgende**.  
U kunt de richting en de locatie van het herstelplan niet wijzigen.
- 5** (Optioneel) Selecteer of deselecteer een of meer beveiligingsgroepen om ze toe te voegen aan of te verwijderen uit het plan en klik op **Volgende**.
- 6** (Optioneel) Selecteer in het vervolgkeuzemenu een ander testnetwerk op de herstelsite en klik op **Volgende**.
- 7** Controleer de samenvattingsinformatie en klik op **Voltooien** om de opgegeven wijzigingen door te voeren in het herstelplan.  
U kunt de update van het plan controleren in de weergave **Recente taken**.

# Systeemeigenschappen instellen

## 9

U kunt systeemeigenschappen instellen om het Orchestrator-standaardgedrag te wijzigen.

Dit hoofdstuk omvat de volgende onderwerpen:

- [Toegang tot het serverbestandssysteem instellen voor werkstromen en acties](#)
- [Toegang tot opdrachten van het besturingssysteem instellen voor werkstromen en acties](#)
- [JavaScript-toegang tot Java-klassen instellen](#)
- [Aangepaste time-outeigenschap instellen](#)
- [Een JDBC-connector toevoegen voor de SQL-invoegtoepassing voor vRealize Orchestrator](#)

## Toegang tot het serverbestandssysteem instellen voor werkstromen en acties

In vRealize Orchestrator hebben de werkstromen en acties beperkte toegang tot specifieke directory's in het bestandssysteem. U kunt toegang tot andere delen van het serverbestandssysteem uitbreiden door het configuratiebestand `js-io-rights.conf` te wijzigen.

### Regels in het bestand `js-io-rights.conf` die schrijftoegang tot het vRealize Orchestrator-systeem toestaan

Het bestand `js-io-rights.conf` bevat regels die schrijftoegang tot gedefinieerde directory's in het serverbestandssysteem toestaan.

### Verplichte inhoud van het bestand `js-io-rights.conf`

Elke regel van het bestand `js-io-rights.conf` moet de volgende informatie bevatten:

- Een plusteken (+) of minteken (-) om aan te geven of rechten zijn toegestaan of geweigerd
- De rechtenniveaus voor lezen (r), schrijven (w) en uitvoeren (x)

- Het pad waarop de rechten worden toegepast.

---

**Opmerking** De rootmap voor het bestand `js-io-rights.conf` is altijd `/var/run/vco`. In het vRealize Orchestrator Appliance-bestandssysteem bevindt deze map zich onder `/data/vco/var/run/vco`. Alle inhoud met toegang tot het vRealize Orchestrator-bestandssysteem moet worden toegewezen onder deze rootmap.

---

## Standaardinhoud van het bestand `js-io-rights.conf`

De standaardinhoud van het configuratiebestand `js-io-rights.conf` in de Orchestrator Appliance is als volgt:

```
-rwx /
+rwX /var/run/vco
-rwx /etc/vco/app-server/security/
+rx /etc/vco
+rx /var/log/vco/
```

De eerste twee regels in het standaardconfiguratiebestand `js-io-rights.conf` staan de volgende toegangsrechten toe:

**-rwx /**

Alle toegang tot het bestandssysteem wordt geweigerd.

**+rwX /var/run/vco**

Toegang voor lezen, schrijven en uitvoeren is toegestaan in de directory `/var/run/vco`.

## Regels in het bestand `js-io-rights.conf`

vRealize Orchestrator verhelpt toegangsrechten in de volgorde waarin ze worden weergegeven in het bestand `js-io-rights.conf`. Elke regel kan de vorige regels overschrijven.

---

**Belangrijk** U kunt toegang tot alle delen van het bestandssysteem toestaan door `+rwx /` in te stellen in het bestand `js-io-rights.conf`. Dit houdt echter een hoog beveiligingsrisico in.

---

## Toegang tot bestandssysteem op server instellen voor werkstromen en acties

Als u wilt wijzigen tot welke delen van het serverbestandssysteem de werkstromen en de vRealize Orchestrator-API toegang hebben, wijzigt u het configuratiebestand `js-io-rights.conf`. Het bestand `js-io-rights.conf` wordt gemaakt wanneer een werkstroom probeert toegang te krijgen tot het bestandssysteem van de vRealize Orchestrator-server.

### Procedure

- 1 Meld u als **root** aan op de vRealize Orchestrator Appliance-opdrachtregel.
- 2 Ga naar de directory `/data/vco/var/run/vco/`.
- 3 Open het configuratiebestand `js-io-rights.conf` in een teksteditor.



- 4 Voeg de nodige regels toe aan het bestand `js-io-rights.conf` om toegang tot gebieden van het bestandssysteem toe te staan of te weigeren.

De volgende regel weigert bijvoorbeeld de uitvoeringsrechten in de directory `/data/vco/var/run/vco/noexec`:

```
-x /data/vco/var/run/vco/noexec
```

`/data/vco/var/run/vco/noexec` behoudt uitvoeringsrechten, maar `/data/vco/var/run/vco/noexec/bar` behoudt die niet. Beide directory's blijven leesbaar en schrijfbaar.

## Resultaten

U hebt de toegangsrechten voor het bestandssysteem voor werkstromen en voor de vRealize Orchestrator API gewijzigd.

## Toegang tot opdrachten van het besturingssysteem instellen voor werkstromen en acties

De vRealize Orchestrator API biedt een scriptklasse, `Command`, die opdrachten op het besturingssysteem van de vRealize Orchestrator-serverhost uitvoert. Om onbevoegde toegang tot de serverhost te blokkeren, hebben vRealize Orchestrator-toepassingen standaard geen toestemming om de `Command`-klasse uit te voeren. Als vRealize Orchestrator-toepassingen rechten nodig hebben om opdrachten uit te voeren op het host-besturingssysteem, kunt u de `Command`-scriptklasse activeren.

U verleent rechten om de `Command`-klasse te gebruiken door een vRealize Orchestrator-configuratiesysteemeigenschap in te stellen.

### Procedure

- 1 Meld u aan bij Control Center als **root**.
- 2 Klik op **Systeemeigenschappen**.
- 3 Klik op **Nieuw**.
- 4 Voer **com.vmware.js.allow-local-process** in het tekstvak **Sleutel** in.
- 5 Voer **True** in het tekstvak **Waarde** in.
- 6 Voer in het tekstvak **Beschrijving** een beschrijving in voor de systeemeigenschap.
- 7 Klik op **Toevoegen**.
- 8 Klik op **Wijzigingen opslaan** in het pop-upmenu.  
Een melding geeft aan dat de wijzigingen zijn opgeslagen.
- 9 Wacht totdat de vRealize Orchestrator-server opnieuw wordt opgestart.

## Resultaten

U hebt rechten voor vRealize Orchestrator-toepassingen verleend om lokale opdrachten uit te voeren op het besturingssysteem van de vRealize Orchestrator-serverhost.

---

**Opmerking** Door de `com.vmware.js.allow-local-process-systeemeigenschap` in te stellen op `true`, staat u toe dat de `Command-scriptklasse` overal in het bestandssysteem schrijft. Deze eigenschap overschrijft alle toegangsrechten van het bestandssysteem die u in het bestand `js-io-rights.conf` alleen instelt voor de `Command-scriptklasse`. De toegangsrechten van het bestandssysteem die u instelt in het bestand `js-io-rights.conf` blijven van toepassing op alle scriptklassen behalve `Command`.

---

## JavaScript-toegang tot Java-klassen instellen

vRealize Orchestrator beperkt JavaScript-toegang standaard tot een beperkte set Java-klassen. Als u JavaScript-toegang tot een groter aantal Java-klassen nodig hebt, moet u een vRealize Orchestrator-systeemeigenschap instellen.

Door de JavaScript-engine volledige toegang tot de Java Virtual Machine (JVM) te geven, veroorzaakt u mogelijk beveiligingsproblemen. Onjuist gevormde of schadelijke scripts kunnen toegang hebben tot alle systeemonderdelen waartoe de gebruiker die de vRealize Orchestrator-server uitvoert, toegang heeft. Daarom heeft de JavaScript-engine van vRealize Orchestrator standaard alleen toegang tot de klassen in het `java.util.*`-pakket.

Als u JavaScript-toegang tot klassen buiten het `java.util.*`-pakket nodig hebt, kunt u in een configuratiebestand de Java-pakketten weergeven waartoe u JavaScript-toegang wilt toestaan. Vervolgens stelt u de systeemeigenschap `com.vmware.scripting.rhino-class-shutter-file` in om naar dit bestand te verwijzen.

### Procedure

- 1 Maak een tekstconfiguratiebestand om de lijst met Java-pakketten op te slaan waartoe u JavaScript-toegang wilt toestaan.

Als u JavaScript bijvoorbeeld toegang wilt geven tot alle klassen in het `java.net`-pakket en tot de `java.lang.Object`-klasse, voegt u de volgende inhoud toe aan het bestand.

```
java.net.*
java.lang.Object
```

- 2 Voer een naam voor het configuratiebestand in.
- 3 Sla het configuratiebestand op in een subdirectory van `/data/vco/usr/lib/vco`.

---

**Opmerking** Het configuratiebestand kan niet worden opgeslagen in een andere directory.

---

- 4 Meld u aan bij Control Center als **root**.
- 5 Klik op **Systeemeigenschappen**.

- 6 Klik op **Nieuw**.
- 7 Voer **com.vmware.scripting.rhino-class-shutter-file** in het tekstvak **Sleutel** in.
- 8 Voer `vco/usr/lib/vco/uw_configuratie_bestand_subdirectory` in het tekstvak **Waarde** in.
- 9 Voer in het tekstvak **Beschrijving** een beschrijving in voor de systeemeigenschap.
- 10 Klik op **Toevoegen**.
- 11 Klik op **Wijzigingen opslaan** in het pop-upmenu.  
Een melding geeft aan dat de wijzigingen zijn opgeslagen.
- 12 Wacht totdat de vRealize Orchestrator-server opnieuw wordt opgestart.

## Resultaten

De JavaScript-engine heeft toegang tot de Java-klassen die u hebt opgegeven.

## Aangepaste time-outeigenschap instellen

Wanneer vCenter Server overbelast is, duurt het langer om het antwoord naar de vRealize Orchestrator-server terug te sturen dan de 20.000 milliseconden die standaard zijn ingesteld. Om deze situatie te voorkomen, moet u het vRealize Orchestrator-configuratiebestand wijzigen om de standaardtime-outperiode te verhogen.

Als de standaardtime-outperiode voor het voltooiën van bepaalde bewerkingen verloopt, bevat het vRealize Orchestrator-serverlogboek fouten.

```
Operation 'getPropertyContent' total time : '5742228' for 1823 calls, mean time :
'3149.0', min time : '0', max time : '32313' Timeout, unable to get property 'info'
com.vmware.vmo.plugin.vi4.model.TimeoutException
```

## Procedure

- 1 Meld u aan bij Control Center als **root**.
- 2 Klik op **Systeemeigenschappen**.
- 3 Klik op **Nieuw**.
- 4 Voer **com.vmware.vmo.plugin.vi4.waitUpdatesTimeout** in het tekstvak **Sleutel** in.
- 5 Voer in het tekstvak **Waarde** de nieuwe time-outperiode in milliseconden in.
- 6 (Optioneel) Voer in het tekstvak **Beschrijving** een beschrijving in voor de systeemeigenschap.
- 7 Klik op **Toevoegen**.
- 8 Klik op **Wijzigingen opslaan** in het pop-upmenu.  
Een melding geeft aan dat de wijzigingen zijn opgeslagen.
- 9 Start de Orchestrator-server opnieuw op.

## Resultaten

De waarde die u instelt, overschrijft de standaardinstelling voor time-outs van 20.000 milliseconden.

## Een JDBC-connector toevoegen voor de SQL-invoegtoepassing voor vRealize Orchestrator

In dit voorbeeld ziet u hoe u een MySQL-connector kunt toevoegen voor de SQL-invoegtoepassing voor vRealize Orchestrator.

### Procedure

- 1 Voeg het bestand MySQL connector.jar toe aan de vRealize Orchestrator Appliance.

- a Meld u via SSH als **rootgebruiker** aan bij de vRealize Orchestrator Appliance-opdrachtregel.
- b Ga naar de directory `/data/vco/var/run/vco`.

```
cd /data/vco/var/run/vco
```

- c Maak een directory `plugins/SQL/lib/`.

```
mkdir -p plugins/SQL/lib/
```

- d Kopieer het bestand MySQL connector.jar van uw lokale machine naar de directory `/data/vco/var/run/vco/plugins/SQL/lib/` door een SCP-opdracht (Secure Copy) uit te voeren.

```
scp ~/local_machine_dir/your_mysql_connector.jar root@orchestrator_FQDN_or_IP:/data/vco/var/run/vco/plugins/SQL/lib/
```

---

**Opmerking** U kunt ook alternatieve methoden gebruiken om het bestand connector.jar te kopiëren naar de vRealize Orchestrator Appliance, zoals PSCP.

---

- 2 Voeg de nieuwe MySQL-eigenschap toe aan het Control Center.

- a Meld u aan bij het Control Center als **root**.
- b Selecteer **Systeemeigenschappen**.
- c Klik op **Nieuw**.
- d Voer in **Sleutel o11n.plugin.SQL.classpath** in.

- e Voer bij **Waarde** `/var/run/vco/plugins/SQL/lib/your_mysql_connector.jar` in.

---

**Opmerking** Het tekstvak Waarde kan meerdere JDBC-connectoren bevatten. Elke JDBC-connector wordt gescheiden door een puntkomma (","). Bijvoorbeeld:

```
/var/run/vco/plugins/SQL/lib/your_mysql_connector.jar;/var/run/vco/plugins/SQL/lib/  
your_mssql_connector.jar;/var/run/vco/plugins/SQL/lib/your_other_connector.jar
```

- f (Optioneel) Voer een beschrijving in voor de MySQL-systeemeigenschap.
- g Klik op **Toevoegen** en wacht totdat de vRealize Orchestrator-server opnieuw wordt opgestart.

---

**Opmerking** Sla uw bestand JDBC connector.jar niet op in een andere directory en stel geen andere waarde in voor de eigenschap `o11n.plugin.SQL.classpath`. Hierdoor wordt de JDBC-connector niet beschikbaar gemaakt voor uw vRealize Orchestrator-implementatie.

---

## Wat is de volgende stap

# 10

Wanneer u vRealize Orchestrator hebt geïnstalleerd en geconfigureerd, kunt u vRealize Orchestrator gebruiken om regelmatig herhaalde processen te automatiseren die betrekking hebben op het beheer van de virtuele omgeving.

- Meld u aan bij de vRealize Orchestrator Client, start en plan werkstromen op de vCenter Server-inventarisobjecten of andere objecten waartoe vRealize Orchestrator toegang heeft via de invoegtoepassingen. Zie *De VMware vRealize Orchestrator-client gebruiken*.
- Dupliceer en wijzig de standaard vRealize Orchestrator-werkstromen en schrijf uw eigen acties en werkstromen om bewerkingen in vCenter Server te automatiseren.
- Om de functionaliteit van het vRealize Orchestrator-platform uit te breiden, ontwikkelt u invoegtoepassingen.
- Beheer uw vRealize Orchestrator-inventaris op meerdere vRealize Orchestrator-instanties met de integratie van een externe Git-opslagplaats. Zie *De VMware vRealize Orchestrator-client gebruiken*.
- Voer werkstromen uit op uw vSphere-inventarisobjecten met behulp van de vSphere Web Client.