

vRealize Automation beheren

Oktober 2022

vRealize Automation 8.5

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

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

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

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

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

Inhoud

1 vRealize Automation beheren 5

2 Gebruikers beheren 6

Hoe kan ik Active Directory-groepen inschakelen voor projecten? 7

Hoe kan ik gebruikers verwijderen uit vRealize Automation 8

Hoe kan ik gebruikersrollen in vRealize Automation bewerken 9

Hoe kan ik toewijzingen van groepsrollen in vRealize Automation bewerken 9

Wat zijn de vRealize Automation-gebruikersrollen 10

Kennisgevings- en instemmingsbanner van het Amerikaanse Ministerie van Defensie inschakelen 20

3 De appliance beheren 22

vRealize Automation starten en stoppen 22

vRealize Automation van één naar drie knooppunten uitschalen 24

Een anti-affiniteitsregel en een VM-groep configureren voor een geclusterde Workspace ONE Access-instantie 25

Een applianceknooppunt vervangen 26

Schijfruimte van vRealize Automation-appliance vergroten 28

De DNS-toewijzing voor vRealize Automation bijwerken 28

Hoe kan ik tijdsynchronisatie inschakelen 29

Hoe kan ik het rootwachtwoord opnieuw instellen 31

4 Tenantconfiguraties voor meerdere organisaties gebruiken in vRealize Automation 33

Multitenancy voor meerdere organisaties instellen voor vRealize Automation 36

Certificaat- en DNS-configuratie beheren bij implementaties voor meerdere organisaties en een enkel knooppunt 38

Certificaat- en DNS-configuratie beheren voor geclusterde implementaties van vRealize Automation 40

vRealize Automation: aanmelden bij tenants en gebruikers toevoegen 42

vRealize Orchestrator gebruiken met vRealize Automation-implementaties voor meerdere organisaties 43

5 Werken met logboeken 44

Hoe werk ik met logboeken en logboekbundels 44

Hoe configureer ik het doorsturen van logboeken naar vRealize Log Insight 47

Hoe kan ik een syslog-integratie maken of bijwerken 53

Hoe verwijder ik een syslog-integratie voor logboekregistraties 54

Hoe werk ik met inhoudspakketten 54

6 Deelname aan het Customer Experience Improvement Program 57

Hoe kan ik me aan- of afmelden voor het programma 57

Hoe configureer ik het tijdstip van gegevensverzameling voor het programma 58

vRealize Automation beheren

1

In deze handleiding wordt beschreven hoe u belangrijke aspecten op het vlak van infrastructuur en gebruikersbeheer van een vRealize Automation-implementatie bewaakt en beheert.

De taken die hier worden beschreven zijn essentieel voor de juiste werking van een vRealize Automation-implementatie. Het gaat om taken voor gebruikers- en groepsbeheer en logboeken voor systeembewaking.

Daarnaast wordt beschreven hoe u implementaties in meerdere organisaties configureert en beheert.

Hoewel een aantal vRealize Automation-beheertaken wordt gedaan vanuit vRealize Automation, hebt u voor andere taken gerelateerde producten nodig zoals vRealize Suite Lifecycle Manager en Workspace ONE Access. Gebruikers kunnen deze taken alleen uitvoeren als ze vertrouwd zijn met die producten en hun functionaliteit.

Voor meer informatie over back-up, herstel en noodherstel raadpleegt u bijvoorbeeld de sectie **Backup and Restore, and Disaster Recovery > 2019** van de [productdocumentatie voor vRealize Suite](#).

Opmerking Noodherstel wordt ondersteund in vRealize Automation 8.0.1 en hoger.

Raadpleeg [productdocumentatie voor Lifecycle Manager](#) voor informatie over het werken met installatie, upgrade en beheer van vRealize Suite Lifecycle Manager.

Gebruikers en groepen beheren in vRealize Automation

2

vRealize Automation gebruikt VMware Workspace ONE Access, de VMware-applicatie voor identiteitsbeheer, om gebruikers en groepen te importeren en beheren. Nadat u de gebruikers en groepen hebt geïmporteerd of gemaakt, kunt u de roltoewijzingen voor implementaties met één enkele tenant beheren op de pagina Identiteits- en toegangsbeheer.

vRealize Automation wordt geïnstalleerd met behulp van VMware Lifecycle Manager (vRSLCM of LCM). Wanneer u vRealize Automation installeert, moet u voor het identiteitsbeheer een bestaande Workspace ONE Access-instantie importeren of een nieuwe instantie maken. Deze twee scenario's geven aan welke beheeropties u heeft.

- Als u een nieuwe Workspace ONE Access-instantie implementeert, kunt u gebruikers en groepen beheren via LCM. Tijdens de installatie kunt u een Active Directory-verbinding instellen met behulp van Workspace ONE Access. Ook kunt u via de pagina Identiteits- en toegangsbeheer bepaalde aspecten van gebruikers en groepen in vRealize Automation op de beschreven wijze weergeven en bewerken.
- Als u een bestaande Workspace ONE Access-instantie gebruikt, geeft u tijdens de LCM-installatie aan of u deze wilt importeren voor gebruik met vRealize Automation. U hebt dan de keuze om Workspace ONE Access te blijven gebruiken voor het beheer van gebruikers en groepen, of dit in het vervolg te doen met de beheerfuncties van LCM.

Zie [vRealize Automation: aanmelden bij tenants en gebruikers toevoegen](#) voor meer informatie over het beheren van gebruikers bij een implementatie met meerdere organisaties.

U moet een rol toewijzen aan vRealize Automation-gebruikers. Een rol bepaalt welke toegang iemand heeft tot de functies van een applicatie. Wanneer vRealize Automation met een Workspace ONE Access-instantie wordt geïnstalleerd, wordt een standaardorganisatie gemaakt en krijgt degene die de installatie verricht de rol van eigenaar van de organisatie toegewezen. Alle andere vRealize Automation-rollen worden toegewezen door de eigenaar van de organisatie.

Er zijn drie soorten rollen in vRealize Automation: organisatierollen, servicerollen en projectrollen. In Cloud Assembly, Service Broker en Code Stream maken rollen op gebruikersniveau doorgaans gebruik van resources die zijn gemaakt en geconfigureerd door rollen op beheerdersniveau. Organisatorische rollen bepalen de rechten op het niveau van de tenant, waarbij de eigenaars van de organisatie rechten op beheerdersniveau hebben en de leden van de organisatie rechten op gebruikersniveau. Eigenaars van de organisatie kunnen andere gebruikers toevoegen en beheren.

| Organisatirollen | Servicrollen |
|-------------------------------|----------------------------|
| ■ Eigenaar van de organisatie | ■ Cloud Assembly-beheerder |
| ■ Lid van de organisatie | ■ Cloud Assembly-gebruiker |
| | ■ Cloud Assembly-kijker |
| | ■ Service Broker-beheerder |
| | ■ Service Broker-gebruiker |
| | ■ Service Broker-kijker |
| | ■ Code Stream-beheerder |
| | ■ Code Stream-gebruiker |
| | ■ Code Stream-lezer |

Daarnaast zijn er twee hoofdrollen op projectniveau die niet worden weergegeven in de tabel: projectbeheerder en projectgebruiker. Deze rollen worden op ad-hocbasis per project toegewezen met Cloud Assembly. Deze rollen zijn niet in beton gegoten. Dezelfde gebruiker kan beheerder zijn voor het ene project en gebruiker voor het andere project. Zie [Wat zijn de vRealize Automation-gebruikersrollen](#) voor meer informatie.

Zie het volgende voor meer informatie over het werken met vRealize Suite Lifecycle Manager en Workspace ONE Access.

Dit hoofdstuk omvat de volgende onderwerpen:

- [Hoe kan ik Active Directory-groepen inschakelen in vRealize Automation voor projecten?](#)
- [Hoe kan ik gebruikers verwijderen uit vRealize Automation](#)
- [Hoe kan ik gebruikersrollen in vRealize Automation bewerken](#)
- [Hoe kan ik toewijzingen van groepsrollen in vRealize Automation bewerken](#)
- [Wat zijn de vRealize Automation-gebruikersrollen](#)
- [Kennisgevings- en instemmingsbanner van het Amerikaanse Ministerie van Defensie inschakelen](#)

Hoe kan ik Active Directory-groepen inschakelen in vRealize Automation voor projecten?

Als een groep niet beschikbaar is op de pagina Groepen toevoegen wanneer u gebruikers aan projecten toevoegt, controleert u de pagina Identiteits- en toegangsbeheer en voegt u de groep toe als deze beschikbaar is. Als de groep niet wordt vermeld op de pagina Identiteits- en toegangsbeheer in vRealize Automation, kan de groep niet worden gesynchroniseerd in uw Workspace ONE Access-instantie. U kunt controleren of het is gesynchroniseerd en vervolgens deze procedure gebruiken om de groep toe te voegen zoals hier wordt weergegeven.

Om leden van een Active Directory-groep aan een project toe te voegen, moet u ervoor zorgen dat de groep wordt gesynchroniseerd met uw Workspace ONE Access-instantie en dat de groep is toegevoegd aan de organisatie.

Voorwaarden

Als de groepen niet zijn gesynchroniseerd, zijn ze niet beschikbaar wanneer u ze probeert toe te voegen aan een project. Controleer of u uw Active Directory-groepen met uw Lifecycle Manager-instantie heeft gesynchroniseerd.

Procedure

- 1 Meld u aan bij vRealize Automation als een gebruiker van hetzelfde Active Directory-domein dat u toevoegt. Bijvoorbeeld @mycompany.com
- 2 Klik in Cloud Assembly op Identiteits- en toegangsbeheer in de koptekst van het rechter navigatiegebied.
- 3 Klik op **Bedrijfsgroepen** en klik vervolgens op **Rollen toewijzen**.
- 4 Gebruik de zoekfunctie om de groep te vinden die u toevoegt en selecteer deze.
- 5 Wijs een organisatirol toe.
De groep moet minimaal een rol van Organisatielid hebben. Zie [Wat zijn de vRealize Automation Cloud Assembly-gebruikersrollen?](#) voor meer informatie.
- 6 Klik op **Servicetoegang toevoegen**, voeg een of meer services toe en selecteer een rol voor elke service.
- 7 Klik op **Toewijzen**.

Resultaten

U kunt nu de Active Directory-groep aan een project toevoegen.

Hoe kan ik gebruikers verwijderen uit vRealize Automation

U kunt gebruikers indien nodig verwijderen uit vRealize Automation.

Op de pagina Identiteits- en toegangsbeheer worden standaard alle gebruikers weergegeven. Op deze pagina kunt u geen gebruikers toevoegen. Wel kunt u gebruikers verwijderen.

Procedure

- 1 Selecteer het tabblad Actieve gebruikers op de pagina Identiteits- en toegangsbeheer.
- 2 Zoek de gebruikers die u wilt verwijderen.
- 3 Klik op **Gebruikers verwijderen**.

Resultaten

De geselecteerde gebruikers worden verwijderd.

Hoe kan ik gebruikersrollen in vRealize Automation bewerken

U kunt rollen bewerken die zijn toegewezen aan Workspace One Access-gebruikers die zijn geïmporteerd in vRealize Automation.

Voorwaarden

Procedure

- 1 Klik in Cloud Assembly op Identiteits- en toegangsbeheer in de koptekst van het rechter navigatiegebied.
- 2 Selecteer de gewenste gebruiker op het tabblad Actieve gebruikers en klik op **Rollen bewerken**.
- 3 U kunt de organisatie- en servicerollen van de gebruiker bewerken.
 - Selecteer de vervolgkeuzelijst naast de kop Organisatierollen toewijzen om de relatie van de gebruiker met de organisatie te wijzigen.
 - Klik op Servicetoegang toevoegen om nieuwe servicerollen voor de gebruiker toe te voegen.
 - Als u gebruikersrollen wilt verwijderen, klikt u op de X naast de betreffende service.
- 4 Klik op **Opslaan**.

Resultaten

De toegewezen gebruikersrol wordt overeenkomstig de instellingen bijgewerkt.

Hoe kan ik toewijzingen van groepsrollen in vRealize Automation bewerken

U kunt roltoewijzingen voor groepen bewerken in vRealize Automation

Voorwaarden

De gebruikers en groepen moeten zijn geïmporteerd uit een geldige vIDM-instantie die is gekoppeld aan uw vRealize Automation-implementatie.

Procedure

- 1 Klik in Cloud Assembly op Identiteits- en toegangsbeheer in de koptekst van het rechter navigatiegebied.
- 2 Selecteer het tabblad Bedrijfsgroepen.
- 3 Typ in het zoekveld de naam van de groep waarvan u roltoewijzingen wilt bewerken.

4 Bewerk de roltoewijzingen voor de geselecteerde groep. U hebt twee opties.

- Organisatierollen toewijzen
- Servicerollen toewijzen

5 Klik op **Toewijzen**.

Resultaten

De roltoewijzingen worden bijgewerkt op basis van uw invoer.

Wat zijn de vRealize Automation-gebruikersrollen

Als organisatie-eigenaar kunt u organisatie- en servicerollen toewijzen aan gebruikers. Deze rollen bepalen wat de gebruikers kunnen doen of zien. Vervolgens kan de servicebeheerder projectrollen voor de services toewijzen. Om te bepalen welke rol u wilt toewijzen, bekijkt u de taken in de volgende tabellen.

Cloud Assembly-servicerollen

De Cloud Assembly-servicerollen bepalen wat u kunt zien en doen in Cloud Assembly. Deze servicerollen worden in de console gedefinieerd door een organisatie-eigenaar.

Tabel 2-1. Beschrijvingen van Cloud Assembly-servicerollen

| Rol | Beschrijving |
|--------------------------|--|
| Cloud Assembly-beheerder | Een gebruiker die lees- en schrijftoegang heeft tot de volledige gebruikersinterface en API-resources. Dit is de enige gebruikersrol die alles kan zien en doen, inclusief cloudaccounts toevoegen, nieuwe projecten maken en een projectbeheerder toewijzen. |
| Cloud Assembly-gebruiker | Een gebruiker die niet de rol van Cloud Assembly-beheerder heeft. In een Cloud Assembly-project voegt de beheerder gebruikers toe aan projecten als projectleden, beheerders of lezers. De beheerder kan ook een projectbeheerder toevoegen. |
| Cloud Assembly-kijker | Een gebruiker die leestoegang heeft om informatie te bekijken, maar geen waarden kan maken, bijwerken of verwijderen. Dit is een alleen-lezenrol in alle projecten. Gebruikers met de rol van lezer kunnen alle informatie zien die beschikbaar is voor de beheerder. Ze kunnen geen acties uitvoeren tenzij u ze projectbeheerder of projectlid maakt. Als de gebruiker is gekoppeld aan een project, hebben ze de rechten voor de rol. De projectkijker breidt hun rechten niet uit zoals de rol van beheerder of lid dit doet. |

Naast de servicerollen heeft Cloud Assembly projectrollen. Elk project is beschikbaar in alle services.

De projectrollen worden gedefinieerd in Cloud Assembly en kunnen verschillen tussen projecten.

In de volgende tabellen, waarin wordt uitgelegd wat de verschillende service- en projectrollen kunnen zien en doen, moet u er rekening mee houden dat de servicebeheerders volledige rechten hebben voor alle gebieden van de gebruikersinterface.

De beschrijvingen van projectrollen helpen u te bepalen welke rechten u aan uw gebruikers geeft.

- Projectbeheerders gebruiken de infrastructuur die door de servicebeheerder is gemaakt, om ervoor te zorgen dat hun projectleden de resources hebben die nodig zijn voor hun ontwikkelingstaken.
- Projectleden werken binnen hun projecten om cloudsjablonen te ontwerpen en te implementeren.
- Projectkijkers zijn beperkt tot alleen-lezen toegang, behalve in een paar gevallen waarin zij niet-destructieve handelingen kunnen uitvoeren, zoals het downloaden van cloudsjablonen.

Tabel 2-2. Cloud Assembly-servicerollen en -projectrollen

| UI-context | Taak | Cloud Assembly-beheerder | Cloud Assembly-kijker | Cloud Assembly-gebruiker | | |
|------------------------------------|--|--------------------------|-----------------------|---|------------------|------------------|
| | | | | Gebruiker moet een projectbeheerder of -lid zijn om projectgerelateerde taken te zien en uitvoeren te voeren. | | |
| | | | | Projectbeheerder | Projectleden | Projectkijkers |
| Toegang krijgen tot Cloud Assembly | | | | | | |
| Console | In de vRA-console kunt u Cloud Assembly zien en openen | Ja | Ja | Ja | Ja | Ja |
| Infrastructuur | | | | | | |
| | Het tabblad Infrastructuur zien en openen | Ja | Ja | Ja | Ja | Ja |
| Configureren - Projecten | Projecten maken | Ja | | | | |
| | Waarden van projectsamenvatting, inrichting, Kubernetes, integraties en testprojectconfiguraties bijwerken of verwijderen. | Ja | | | | |
| | Gebruikers en groepen toevoegen en rollen aan projecten toewijzen. | Ja | | Ja. Uw projecten. | | |
| | Projecten weergeven | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten |
| Configureren - Cloudzones | Cloudzones maken, bijwerken of verwijderen | Ja | | | | |
| | Cloudzones weergeven | Ja | Ja | | | |

Tabel 2-2. Cloud Assembly-servicerollen en -projectrollen (vervolg)

| UI-context | Taak | Cloud Assembly-beheerder | Cloud Assembly-kijker | Cloud Assembly-gebruiker | | |
|-----------------------------------|--|--------------------------|-----------------------|---|--------------|----------------|
| | | | | Gebruiker moet een projectbeheerder of -lid zijn om projectgerelateerde taken te zien en uitvoeren te voeren. | | |
| | | | | Projectbeheerder | Projectleden | Projectkijkers |
| | Het dashboard Inzichten van de cloudzone weergeven | Ja | Ja | | | |
| | Waarschuwingen voor cloudzones weergeven | Ja | Ja | | | |
| Configureren - Kubernetes-zones | Kubernetes-zones maken, bijwerken of verwijderen | Ja | | | | |
| | Kubernetes-zones weergeven | Ja | Ja | | | |
| Configureren - Soorten | Soorten maken, bijwerken of verwijderen | Ja | | | | |
| | Soorten weergeven | Ja | Ja | | | |
| Configureren - Imagemtoewijzingen | Imagemtoewijzingen maken, bijwerken of verwijderen | Ja | | | | |
| | Imagemtoewijzingen weergeven | Ja | Ja | | | |
| Configureren - Netwerktoprofielen | Netwerktoprofielen maken, bijwerken of verwijderen | Ja | | | | |
| | Netwerktoprofielen voor images weergeven | Ja | Ja | | | |
| Configureren - Opslagtoprofielen | Opslagtoprofielen maken, bijwerken of verwijderen | Ja | | | | |
| | Opslagtoprofielen voor images weergeven | Ja | Ja | | | |
| Configureren - Prijskaarten | Prijskaarten maken, bijwerken of verwijderen | Ja | | | | |
| | De prijskaarten weergeven | Ja | Ja | | | |
| Configureren - Tags | Tags maken, bijwerken of verwijderen | Ja | | | | |
| | Tags weergeven | Ja | Ja | | | |
| Resources - Berekenen | Tags aan gedetecteerde computerbronnen toevoegen | Ja | | | | |
| | Gedetecteerde computerbronnen weergeven | Ja | Ja | | | |
| Resources - Netwerken | Netwerktoprofielen, IP-bereiken en IP-adressen aanpassen | Ja | | | | |
| | Gedetecteerde netwerkresources weergeven | Ja | Ja | | | |

Tabel 2-2. Cloud Assembly-servicerollen en -projectrollen (vervolg)

| UI-context | Taak | Cloud Assembly-beheerder | Cloud Assembly-kijker | Cloud Assembly-gebruiker | | |
|-----------------------------------|--|--------------------------|-----------------------|---|------------------|-------------------|
| | | | | Gebruiker moet een projectbeheerder of -lid zijn om projectgerelateerde taken te zien en uitvoeren te voeren. | | |
| | | | | Projectbeheerder | Projectleden | Projectkijkers |
| Resources - Beveiliging | Tags aan gedetecteerde beveiligingsgroepen toevoegen | Ja | | | | |
| | Gedetecteerde beveiligingsgroepen weergeven | Ja | Ja | | | |
| Resources - Opslag | Tags aan gedetecteerde opslag toevoegen | Ja | | | | |
| | Opslag weergeven | Ja | Ja | | | |
| Resources - Machines | Machines toevoegen en verwijderen | Ja | | | | |
| | Machines weergeven | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten |
| Resources - Volumes | Gedetecteerde opslagvolumes verwijderen | Ja | | | | |
| | Gedetecteerde opslagvolumes weergeven | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten. |
| Resources - Kubernetes | Kubernetes-clusters implementeren of toevoegen en naamruimten maken of toevoegen | Ja | | | | |
| | Kubernetes-clusters en -naamruimten weergeven | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten |
| Activiteit - Aanvragen | Records voor implementatieaanvragen verwijderen | Ja | | | | |
| | Records voor implementatieaanvragen weergeven | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten |
| Activiteit - Gebeurtenislogboeken | Gebeurtenislogboeken weergeven | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten |
| Verbindingen - Cloudaccounts | Cloudaccounts maken, bijwerken of verwijderen | Ja | | | | |
| | Cloudaccounts weergeven | Ja | Ja | | | |
| Verbindingen - Integraties | Integraties maken, bijwerken of verwijderen | Ja | | | | |
| | Integraties weergeven | Ja | Ja | | | |
| Onboarding | Onboardingplannen maken, bijwerken of verwijderen | Ja | | | | |

Tabel 2-2. Cloud Assembly-servicerollen en -projectrollen (vervolg)

| UI-context | Taak | Cloud Assembly-beheerder | Cloud Assembly-kijker | Cloud Assembly-gebruiker | | |
|--------------------------------------|--|--------------------------|-----------------------|---|--|------------------|
| | | | | Gebruiker moet een projectbeheerder of -lid zijn om projectgerelateerde taken te zien en uitvoeren te voeren. | | |
| | | | | Projectbeheerder | Projectleden | Projectkijkers |
| | Onboardingplannen weergeven | Ja | Ja | | | Ja. Uw projecten |
| Marketplace | | | | | | |
| | Het tabblad Marketplace zien en openen | Ja | Ja | | | |
| | De gedownloade cloudsjablonen op het tabblad Ontwerp gebruiken | Ja | | Ja. Indien aan uw projecten gekoppeld. | Ja. Indien aan uw projecten gekoppeld. | |
| Marketplace - Cloudsjablonen | Een cloudsjabloon downloaden | Ja | | | | |
| | De cloudsjablonen weergeven | Ja | Ja | | | |
| Marketplace - Images | Images downloaden | Ja | | | | |
| | Images weergeven | Ja | Ja | | | |
| Marketplace - Downloads | Het logboek van alle gedownloade items weergeven | Ja | Ja | | | |
| Uitbreidbaarheid | | | | | | |
| | Het tabblad Uitbreidbaarheid zien en openen | Ja | Ja | | | Ja |
| Gebeurtenissen | Uitbreidbaarheidsgebeurtenissen weergeven | Ja | Ja | | | |
| Abonnementen | Uitbreidbaarheidsabonnementen maken, bijwerken of verwijderen | Ja | | | | |
| | Abonnementen deactiveren | Ja | | | | |
| | Abonnementen weergeven | Ja | Ja | | | |
| Bibliotheek - Gebeurtenisonderwerpen | Gebeurtenisonderwerpen weergeven | Ja | Ja | | | |
| Bibliotheek - Acties | Uitbreidbaarheidsacties maken, bijwerken of verwijderen | Ja | | | | |
| | Uitbreidbaarheidsacties weergeven | Ja | Ja | | | |
| Bibliotheek - Werkstromen | Uitbreidbaarheidswerkstromen weergeven | Ja | Ja | | | |

Tabel 2-2. Cloud Assembly-servicerollen en -projectrollen (vervolg)

| UI-context | Taak | Cloud Assembly-beheerder | Cloud Assembly-kijker | Cloud Assembly-gebruiker | | |
|-------------------------------------|--|--------------------------|-----------------------|---|------------------|------------------|
| | | | | Gebruiker moet een projectbeheerder of -lid zijn om projectgerelateerde taken te zien en uitvoeren te voeren. | | |
| | | | | Projectbeheerder | Projectleden | Projectkijkers |
| Activiteit - Actie-uitvoeringen | Uitvoeringen van uitbreidbaarheidsacties annuleren of verwijderen | Ja | | | | |
| | Uitvoeringen van uitbreidbaarheidsacties weergeven | Ja | Ja | | | Ja. Uw projecten |
| Activiteit - Werkstroomuitvoeringen | Uitvoeringen voor uitbreidbaarheidswerkstromen weergeven | Ja | Ja | | | |
| Ontwerp | | | | | | |
| Ontwerp | Het tabblad Ontwerp openen en een lijst met cloudsjablonen weergeven | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten |
| Cloudsjablonen | Cloudsjablonen maken, bijwerken en verwijderen | Ja | | Ja. Uw projecten | Ja. Uw projecten | |
| | Cloudsjablonen weergeven | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten |
| | Cloudsjablonen downloaden | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten |
| | Cloudsjablonen uploaden | Ja | | Ja. Uw projecten | Ja. Uw projecten | |
| | Cloudsjablonen implementeren | Ja | | Ja. Uw projecten | Ja. Uw projecten | |
| | Versie van cloudsjablonen weergeven en herstellen | Ja | | Ja. Uw projecten | Ja. Uw projecten | |
| | Cloudsjablonen vrijgeven aan de catalogus | Ja | | Ja. Uw projecten | Ja. Uw projecten | |
| Custom resources | Aangepaste resources maken, bijwerken of verwijderen | Ja | | | | |
| | Custom resources weergeven | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten |
| Aangepaste acties | Aangepaste acties maken, bijwerken of verwijderen | Ja | | | | |
| | Aangepaste acties weergeven | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten |
| Implementaties | | | | | | |

Tabel 2-2. Cloud Assembly-servicerollen en -projectrollen (vervolg)

| UI-context | Taak | Cloud Assembly-beheerder | Cloud Assembly-kijker | Cloud Assembly-gebruiker | | |
|-----------------------|--|--------------------------|-----------------------|---|------------------|------------------|
| | | | | Gebruiker moet een projectbeheerder of -lid zijn om projectgerelateerde taken te zien en uitvoeren te voeren. | | |
| | | | | Projectbeheerder | Projectleden | Projectkijkers |
| | Het tabblad Implementaties zien en openen | Ja | Ja | Ja | Ja | Ja |
| | Implementaties, inclusief implementatiedetails, implementatiegeschiedenis en informatie over prijs, bewaking, waarschuwingen, optimalisatie en probleemoplossing weergeven | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten |
| | Waarschuwingen beheren | Ja | | Ja. Uw project | Ja. uw project | |
| | Acties voor dag 2 uitvoeren op implementaties op basis van beleidsregels | Ja | | Ja. Uw projecten | Ja. Uw projecten | |
| Waarschuwingen | | | | | | |
| | Het tabblad Catalogus bekijken en openen | Ja | Ja | Ja | Ja | Ja |
| | Waarschuwingen beheren | Ja | | Ja. Uw projecten | Ja. Uw projecten | |
| | Waarschuwingen weergeven | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten |

Service Broker-servicerollen

De Service Broker-servicerollen bepalen wat u kunt zien en doen in Service Broker. Deze servicerollen worden in de console gedefinieerd door een organisatie-eigenaar.

Tabel 2-3. Beschrijvingen van Service Broker-servicerollen

| Rol | Beschrijving |
|--------------------------|--|
| Service Broker-beheerder | Moet lees- en schrijftoegang hebben tot de volledige gebruikersinterface en API-resources. Dit is de enige gebruikersrol die alle taken kan uitvoeren, waaronder het maken van een nieuw project en het toewijzen van een projectbeheerder. |
| Service Broker-gebruiker | Elke gebruiker die niet de rol van Service Broker-beheerder heeft. In een Service Broker-project voegt de beheerder gebruikers toe aan projecten als projectleden, beheerders of lezers. De beheerder kan ook een projectbeheerder toevoegen. |
| Service Broker-kijker | Een gebruiker die leestoegang heeft om informatie te bekijken, maar geen waarden kan maken, bijwerken of verwijderen. Gebruikers met de rol van lezer kunnen alle informatie zien die beschikbaar is voor de beheerder. Ze kunnen geen acties uitvoeren tenzij u ze projectbeheerder of projectlid maakt. Als de gebruiker is gekoppeld aan een project, hebben ze de rechten voor de rol. De projectkijker breidt hun rechten niet uit zoals de rol van beheerder of lid dit doet. |

Naast de servicerollen heeft Service Broker projectrollen. Elk project is beschikbaar in alle services.

De projectrollen worden gedefinieerd in Service Broker en kunnen verschillen tussen projecten.

In de volgende tabellen, waarin wordt uitgelegd wat de verschillende service- en projectrollen kunnen zien en doen, moet u er rekening mee houden dat de servicebeheerders volledige rechten hebben voor alle gebieden van de gebruikersinterface.

Gebruik de volgende beschrijvingen van projectrollen om u te helpen bepalen welke rechten u uw gebruikers wilt geven.

- Projectbeheerders gebruiken de infrastructuur die door de servicebeheerder is gemaakt, om ervoor te zorgen dat hun projectleden de resources hebben die nodig zijn voor hun ontwikkelingstaken.
- Projectleden werken binnen hun projecten om cloudsjablonen te ontwerpen en te implementeren.
- Projectkijkers zijn beperkt tot alleen-lezen toegang.

Tabel 2-4. Service Broker-servicerollen en -projectrollen

| UI-context | Taak | Service Broker-beheerder | Service Broker-kijker | Service Broker-gebruiker | | |
|---|--|--------------------------|-----------------------|--|------------------|------------------|
| | | | | De gebruiker moet een projectbeheerder zijn om projectgerelateerde taken te zien en uit te voeren. | | |
| | | | | Projectbeheerder | Projectleden | Projectkijker |
| Toegang krijgen tot Service Broker | | | | | | |
| Console | In de console kunt u Service Broker zien en openen | Ja | Ja | Ja | Ja | Ja |
| Infrastructuur | | | | | | |
| | Het tabblad Infrastructuur zien en openen | Ja | Ja | | | |
| Configureren - Projecten | Projecten maken | Ja | | | | |
| | Waarden van projectsamenvatting, inrichting, Kubernetes, integraties en testprojectconfiguraties bijwerken of verwijderen. | Ja | | | | |
| | Gebruikers en groepen toevoegen en rollen aan projecten toewijzen. | Ja | | Ja. Uw projecten. | | |
| | Projecten weergeven | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten |
| Configureren - Cloudzones | Cloudzones maken, bijwerken of verwijderen | Ja | | | | |
| | Cloudzones weergeven | Ja | Ja | | | |
| Configureren - Kubernetes-zones | Kubernetes-zones maken, bijwerken of verwijderen | Ja | | | | |
| | Kubernetes-zones weergeven | Ja | Ja | | | |
| Verbindingen - Cloudaccounts | Cloudaccounts maken, bijwerken of verwijderen | Ja | | | | |
| | Cloudaccounts weergeven | Ja | Ja | | | |
| Verbindingen - Integraties | Integraties maken, bijwerken of verwijderen | Ja | | | | |
| | Integraties weergeven | Ja | Ja | | | |
| Activiteit - Aanvragen | Records voor implementatieaanvragen verwijderen | Ja | | | | |

Tabel 2-4. Service Broker-servicerollen en -projectrollen (vervolg)

| UI-context | Taak | Service Broker-beheerder | Service Broker-kijker | Service Broker-gebruiker | | |
|-----------------------------------|--|--------------------------|-----------------------|--|------------------|------------------|
| | | | | De gebruiker moet een projectbeheerder zijn om projectgerelateerde taken te zien en uit te voeren. | | |
| | | | | Projectbeheerder | Projectleden | Projectkijker |
| | Records voor implementatieaanvragen weergeven | Ja | | | | |
| Activiteit - Gebeurtenislogboeken | Gebeurtenislogboeken weergeven | Ja | | | | |
| Inhoud en beleidsregels | | | | | | |
| | Het tabblad Inhoud en beleidsregels zien en openen | Ja | Ja | | | |
| Inhoudsbronnen | Inhoudsbronnen maken, bijwerken of verwijderen | Ja | | | | |
| | Inhoudsbronnen weergeven | Ja | Ja | | | |
| Inhoud delen | Gedeelde inhoud toevoegen of verwijderen | Ja | | | | |
| | Gedeelde inhoud weergeven | Ja | Ja | | | |
| Inhoud | Formulier aanpassen en item configureren | Ja | | | | |
| | Inhoud weergeven | Ja | Ja | | | |
| Beleidsregels - Definities | Beleidsdefinities maken, bijwerken of verwijderen | Ja | | | | |
| | Beleidsdefinities weergeven | Ja | Ja | | | |
| Beleidsregels - Afdwinging | Afdwingingslogboek weergeven | Ja | Ja | | | |
| Meldingen - E-mailserver | Een e-mailserver configureren | Ja | | | | |
| Catalogus | | | | | | |
| | Het tabblad Catalogus zien en openen | Ja | Ja | Ja | Ja | Ja |
| | Beschikbare catalogusitems weergeven | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten |
| | Een catalogusitem aanvragen | Ja | | Ja. Uw projecten | Ja. Uw projecten | |

Tabel 2-4. Service Broker-servicerollen en -projectrollen (vervolg)

| UI-context | Taak | Service Broker-beheerder | Service Broker-kijker | Service Broker-gebruiker | | |
|-----------------------|--|--------------------------|-----------------------|--|-------------------------------------|-------------------------------------|
| | | | | De gebruiker moet een projectbeheerder zijn om projectgerelateerde taken te zien en uit te voeren. | | |
| | | | | Projectbeheerder | Projectleden | Projectkijker |
| Implementaties | | | | | | |
| | Het tabblad Implementaties zien en openen | Ja | Ja | Ja. | Ja | Ja |
| | Implementaties, inclusief implementatiedetails, implementatiegeschiedenis en informatie over prijs, bewaking, waarschuwingen, optimalisatie en probleemoplossing weergeven | Ja | Ja | Ja. Uw projecten | Ja. Uw projecten | Ja. Uw projecten |
| | Waarschuwingen beheren | Ja | | Ja. Uw projecten | Ja. Uw projecten | |
| | Acties voor dag 2 uitvoeren op implementaties op basis van beleidsregels | Ja | | Ja. Uw projecten | Ja. Uw projecten | |
| Goedkeuringen | | | | | | |
| | Het tabblad Goedkeuringen zien en openen | Ja | Ja | Ja | Ja | Ja |
| | Reageren op goedkeuringsaanvragen | Ja | | Alleen Service Broker-gebruikersrol | Alleen Service Broker-gebruikersrol | Alleen Service Broker-gebruikersrol |

Kennisgevings- en instemmingsbanner van het Amerikaanse Ministerie van Defensie inschakelen

Voor sommige overheidsklanten moet een beheerder de standaardkennisgevings- en instemmingsbanner van het Amerikaanse Ministerie van Defensie in Workspace ONE Access configureren zodat gebruikers toegang krijgen tot vRealize Automation.

De tekst van de verplichte standaardkennisgevings- en instemmingsbanner van het Amerikaanse Ministerie van Defensie luidt als volgt:

U krijgt toegang tot een informatiesysteem van de Amerikaanse overheid dat alleen wordt geleverd voor gebruik met toestemming van de Amerikaanse overheid. Door dit informatiesysteem te gebruiken (inclusief alle apparaten die aan dit informatiesysteem zijn gekoppeld), gaat u akkoord met de volgende voorwaarden:

- De Amerikaanse overheid onderschept en bewaakt communicatie op dit informatiesysteem voor doeleinden zoals, maar niet beperkt tot, het testen van penetratie, COMSEC-controle, netwerkbewerkingen en -verdediging, en onderzoek naar wangedrag van personeel (PM), ordehandhaving (LE) en counterintelligence (CI).
- De Amerikaanse overheid kan op elk moment gegevens onderzoeken en in beslag nemen die op dit informatiesysteem zijn opgeslagen.
- Communicatie met, of gegevens die zijn opgeslagen op dit informatiesysteem, zijn niet privé, worden onderworpen aan routinecontrole, interceptie en spoorwerk, en kunnen worden onthuld of gebruikt voor een door de Amerikaanse overheid geautoriseerd doel.

De volgende stappen beschrijven hoe u deze banner configureert in Workspace ONE Access. Zie de documentatie voor de Workspace ONE Access-beheerconsole voor meer informatie.

Procedure

- 1 Meld u als beheerder aan bij de Workspace ONE-beheerconsole.
- 2 Klik in de VMware Identity Manager-console op de tab Identiteits- en toegangsbeheer.
- 3 Klik op Instellen en klik vervolgens op de tab Connectoren.
- 4 Klik op de link Werker voor elke connector die u wilt configureren.
- 5 Klik op het tabblad Verificatieadapters en klik vervolgens op `CertificateAuthAdapter`.
- 6 Klik op het selectievakje Instemmingsformulier inschakelen vóór verificatie.
- 7 Plak de tekst van de verplichte standaardkennisgevings- en instemmingsbanner van het Ministerie van Defensie in het tekstvak Inhoud van instemmingsformulier.
- 8 Sla uw wijzigingen op.

Resultaten

De vRealize Automation-appliance beheren

3

Als systeembeheerder moet u mogelijk verschillende taken uitvoeren om de juiste werking van uw geïnstalleerde vRealize Automation-applicatie te waarborgen.

In de beginfase van het gebruik van vRealize Automation zijn deze taken in principe nog niet aan de orde. De kennis over het uitvoeren van deze taken komt van pas als u problemen met de prestatie of werking van het product moet oplossen.

Dit hoofdstuk omvat de volgende onderwerpen:

- [vRealize Automation starten en stoppen](#)
- [vRealize Automation van één naar drie knooppunten uitschalen](#)
- [Een anti-affiniteitsregel en een VM-groep configureren voor een geclusterde Workspace ONE Access-instantie](#)
- [Een vRealize Automation-applianceknooppunt vervangen](#)
- [Schijfruimte van vRealize Automation-appliance vergroten](#)
- [De DNS-toewijzing voor vRealize Automation bijwerken](#)
- [Hoe kan ik de tijdsynchronisatie van vRealize Automation inschakelen](#)
- [Hoe kan ik het rootwachtwoord opnieuw instellen voor vRealize Automation](#)

vRealize Automation starten en stoppen

Houd rekening met de juiste procedures bij het starten of afsluiten van vRealize Automation.

De aanbevolen manier om de vRealize Automation-onderdelen af te sluiten en te starten, is het gebruik van de functies Uitschakelen en Inschakelen die beschikbaar zijn in de sectie **Levenscyclusacties > Omgevingen** van vRealize Suite Lifecycle Manager. In de volgende procedures worden handmatige methoden beschreven om de vRealize Automation-onderdelen af te sluiten en te starten voor het geval vRealize Suite Lifecycle Manager om een bepaalde reden niet beschikbaar is.

vRealize Automation afsluiten

Om de gegevensintegriteit te behouden, moet u de vRealize Automation-services afsluiten voordat u de virtual appliances uitschakelt. Met SSH of VMRC kunt u alle knooppunten afsluiten of starten vanuit elke afzonderlijke appliance.

Opmerking Vermijd voor zover mogelijk het gebruik van `vracli reset vidm`-opdrachten. Met deze opdracht worden alle configuraties van Workspace ONE Access opnieuw ingesteld en wordt de koppeling tussen gebruikers en ingerichte resources verbroken.

- 1 Meld u via SSH of VMRC aan bij de console van een vRealize Automation-appliance.
- 2 Als u de vRealize Automation-services op alle clusterknooppunten wilt afsluiten, voert u de volgende reeks opdrachten uit.

Opmerking Als u deze opdrachten kopieert en de uitvoering ervan mislukt, plakt u ze eerst in Kladblok en kopieert u ze vervolgens terug voordat u ze uitvoert. Met deze procedure worden eventueel verborgen tekens en andere artefacten uit de documentatiebron verwijderd.

```
/opt/scripts/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

- 3 Sluit de vRealize Automation-appliances af.

Uw vRealize Automation-implementatie is nu afgesloten.

vRealize Automation starten

Na een niet-geplande afsluiting, een gecontroleerde afsluiting of een herstelprocedure, moet u vRealize Automation-onderdelen in een specifieke volgorde opnieuw starten. vRLCM is een niet-kritisch onderdeel, dat u op elk gewenst moment kunt starten. De onderdelen van VMware Workspace ONE Access, voorheen VMware Identity Management, moeten worden gestart voordat u vRealize Automation start.

Opmerking Controleer of relevante load balancers worden uitgevoerd voordat u de vRealize Automation-onderdelen start.

- 1 Schakel alle vRealize Automation-appliances in en wacht totdat deze zijn gestart.
- 2 Meld u via SSH of VMRC aan bij de console van een appliance en voer de volgende opdracht uit om de services op alle knooppunten te herstellen.

```
/opt/scripts/deploy.sh
```

- 3 Gebruik de volgende opdracht om te controleren of alle services worden uitgevoerd.

```
kubectl get pods --all-namespaces
```

Opmerking U moet drie instanties van elke service zien, met de status Actief of Voltooid.

Wanneer alle services de status Actief of Voltooid hebben, is vRealize Automation klaar voor gebruik.

vRealize Automation opnieuw starten

U kunt alle vRealize Automation-services centraal opnieuw starten vanaf een van de appliances in uw cluster. Volg de voorgaande instructies om vRealize Automation af te sluiten en gebruik vervolgens de instructies om vRealize Automation te starten. Voordat u vRealize Automation opnieuw start, controleert u of alle toepasselijke onderdelen voor de load balancer en VMware Workspace ONE Access worden uitgevoerd.

Wanneer alle services de status Actief of Voltooid hebben, is vRealize Automation klaar voor gebruik.

Voer de volgende opdracht uit om te controleren of alle services worden uitgevoerd:

```
kubectl -n prelude get pods
```

vRealize Automation van één naar drie knooppunten uitschalen

Als u wilt uitbreiden, kunt u een vRealize Automation-implementatie van één knooppunt naar drie knooppunten uitschalen.

U moet de functies van vRealize Suite Lifecycle Manager gebruiken om veel stappen van deze procedure uit te voeren. Raadpleeg [productdocumentatie voor Lifecycle Manager](#) voor informatie over het werken met installatie, upgrade en beheer van vRealize Suite Lifecycle Manager.

Als u een geclusterde implementatie met drie knooppunten gebruikt, kan vRealize Automation een storing op één knooppunt doorgaans doorstaan en blijven functioneren. Als twee knooppunten in een cluster met drie knooppunten mislukken, zal vRealize Automation niet meer functioneren.

Voorwaarden

Bij deze procedure wordt ervan uitgegaan dat u al een functionerende vRealize Automation-implementatie met één knooppunt hebt.

Procedure

- 1 Sluit alle vRealize Automation-appliances af.

Als u de vRealize Automation-services op alle clusterknooppunten wilt afsluiten, voert u de volgende reeks opdrachten uit.

```
/opt/scripts/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

Nu kunt u de vRealize Automation-appliances afsluiten.

- 2 Maak een momentopname van de implementatie.

Gebruik de optie Momentopname maken in vRealize Suite Lifecycle Manager

Levenscyclusbewerkingen > Omgevingen > vRA > Details weergeven.

Opmerking Onlinemomentopnamen die worden gemaakt zonder dat vRealize Automation-knooppunten worden afgesloten, worden ondersteund vanaf 8.0.1. Voor omgevingen met vRealize Automation 8.0 moet u vRealize Automation-knooppunten eerst stoppen.

- 3 Schakel de vRealize Automation-appliance in en geef alle containers weer.
- 4 Met behulp van de kluisfunctionaliteit in **LCM > Kluis > Certificaten** in vRealize Suite Lifecycle Manager genereert of importeert u vRealize Automation-certificaten voor alle onderdelen, inclusief FQDN's van het vRealize Suite Lifecycle Manager-knooppunt en de volledig gekwalificeerde domeinnaam van de vRealize Automation load balancer.
Voeg de namen van de drie appliances toe aan de alternatieve namen.
- 5 Importeer het nieuwe certificaat in vRealize Suite Lifecycle Manager.
- 6 Vervang het bestaande vRealize Suite Lifecycle Manager-certificaat door de versie die in de vorige stap is gegenereerd met behulp van de LCM-optie **Levenscyclusbewerkingen > Omgevingen > vRA > Details weergeven** Certificaat vervangen.
- 7 U kunt vRealize Automation naar drie knooppunten uitschalen met behulp van de selectie Onderdelen toevoegen in **LCM > Levenscyclusbewerkingen > Omgevingen > vRA > Details weergeven**.

Resultaten

vRealize Automation is geschaald naar een implementatie met drie knooppunten.

Een anti-affiniteitsregel en een VM-groep configureren voor een geclusterde Workspace ONE Access-instantie

Als uw vRealize Automation-omgeving een geclusterde Workspace ONE Access-instantie gebruikt, maakt u een anti-affiniteitsregel en machinecluster om te zorgen voor een geschikte werkstroom voor hoge beschikbaarheid van vSphere.

Om de geclusterde Workspace ONE Access-knooppunten te beschermen tegen een fout op hostniveau, configureert u een anti-affiniteitsregel om virtuele machines uit te voeren die op verschillende hosts in het standaardbeheercluster van vSphere bestaan. Nadat u een anti-affiniteitsregel heeft gemaakt, configureert u een VM-groep om de gewenste opstartvolgorde van machines te definiëren. Door een gedefinieerde opstartvolgorde voor machines te gebruiken, kunt u ervoor zorgen dat de hoge beschikbaarheid van vSphere de geclusterde Workspace ONE Access-knooppunten in de juiste volgorde inschakelt voor uw omgeving.

Voor meer informatie over het configureren van anti-affiniteitsregels en een VM-groep raadpleegt u [Een anti-affiniteitsregel en een VM-groep configureren voor een geclusterde Workspace ONE Access-instantie](#) in de [productdocumentatie voor VMware Cloud Foundation](#).

Overwegingen voor affiniteitsregel bij het upgraden van een vRealize Automation-release naar een andere

vRealize Suite Lifecycle Manager ondersteunt geen anti-affiniteitsregels voor vRealize Automation 8.x. Omdat vRealize Suite Lifecycle Manager door vRealize Easy Installer wordt gebruikt tijdens de vRealize Automation-upgrade en er geen specifieke volgorde is om vRealize Automation-knooppunten tijdens de upgrade in en uit te schakelen, kunnen er problemen optreden als de gebruikte volgorde conflicteert met affiniteitsregels die de volgorde bepalen waarin machines worden uitgeschakeld en ingeschakeld. Wanneer u vRealize Suite Lifecycle Manager of vRealize Easy Installer gebruikt om van de ene vRealize Automation-release naar de andere te upgraden, moet u affiniteitsregels uitschakelen voordat u de upgrade start.

Raadpleeg [vRealize Automation installeren met vRealize Easy Installer](#) in de [productdocumentatie voor vRealize Automation](#) voor informatie over het upgraden van één vRealize Automation naar een andere.

Een vRealize Automation-applianceknooppunt vervangen

Wanneer een vRealize Automation-appliance in een configuratie met meerdere knooppunten en hoge beschikbaarheid (HA) is mislukt, moet u mogelijk het defecte knooppunt vervangen.

Voorzichtig Voordat u doorgaat, raadt VMware u aan contact op te nemen met de technische ondersteuning om het HA-probleem op te lossen en te controleren of het probleem op één knooppunt is geïsoleerd.

Als de technische ondersteuning bepaalt dat het knooppunt moet worden vervangen, volgt u de volgende stappen.

- 1 Maak in vCenter back-upmomentopnamen van elke appliance in de HA-configuratie.
Neem geen geheugen voor de virtuele machine op in de back-upmomentopnamen.
- 2 Sluit het defecte knooppunt af.
- 3 Noteer het buildnummer van de vRealize Automation-software van het defecte knooppunt evenals de netwerkinstellingen.

Noteer de FQDN, het IP-adres, de gateway, de DNS-servers en in het bijzonder het MAC-adres. Later wijst u dezelfde waarden toe aan het vervangende knooppunt.

- 4 Het primaire databaseknooppunt moet een van de gezonde knooppunten zijn. Volg deze stappen:

- a Meld u als root aan op de commandoregel van een gezond knooppunt.
- b Zoek de naam van het primaire databaseknooppunt door het volgende commando uit te voeren.

```
vraccli status | grep primary -B 1
```

Het resultaat moet lijken op dit voorbeeld, waarbij postgres-1 het primaire databaseknooppunt is.

```
"Conninfo":
"host=postgres-1.postgres.prelude.svc.cluster.local
dbname=repmgr-db user=repmgr-db passfile=/scratch/repmgr-db.cred
connect_timeout=10",
"Role": "primary",
```

- c Controleer of het primaire databaseknooppunt een gezonde status heeft door het volgende commando uit te voeren.

```
kubect1 -n prelude get pods -o wide | grep postgres
```

Het resultaat moet lijken op dit voorbeeld, waarbij postgres-1 in de lijst wordt weergegeven als actief en gezond.

```
postgres-1 1/1 Running 0 39h 12.123.2.14 vc-vm-224-84.company.com <none> <none>
postgres-2 1/1 Running 0 39h 12.123.1.14 vc-vm-224-85.company.com <none> <none>
```

Belangrijk Als het primaire databaseknooppunt defect is, neemt u contact op met de technische ondersteuning in plaats van verder te gaan.

- 5 Verwijder het defecte knooppunt vanuit de rootcommandoregel van het gezonde knooppunt.

```
vraccli cluster remove faulty-node-FQDN
```

- 6 Gebruik vCenter om een nieuw, vervangend vRealize Automation-knooppunt te implementeren.

Implementeer hetzelfde buildnummer van de vRealize Automation-software en pas de netwerkinstellingen van het defecte knooppunt toe. Voeg de FQDN, het IP-adres, de gateway, de DNS-servers en in het bijzonder het MAC-adres toe.

- 7 Schakel het vervangende knooppunt in.
- 8 Meld u als root aan op de commandoregel van het vervangende knooppunt.
- 9 Controleer of de initiële opstartvolgorde is voltooid door het volgende commando uit te voeren.

```
vracli status first-boot
```

Zoek naar het bericht `First boot complete`.

- 10 Neem vanaf het vervangende knooppunt deel aan het vRealize Automation-cluster.

```
vracli cluster join primary-DB-node-FQDN
```

- 11 Meld u als root aan op de commandoregel van het primaire databaseknooppunt.

- 12 Implementeer de herstelde cluster door het volgende script uit te voeren.

```
/opt/scripts/deploy.sh
```

Schijfruimte van vRealize Automation-appliance vergroten

Mogelijk moet u de schijfruimte van de vRealize Automation-appliance vergroten voor bepaalde doeleinden, zoals logboekbestandopslag.

Procedure

- 1 Gebruik vSphere om de VMDK op de vRealize Automation-appliance uit te vouwen.
- 2 Meld u aan bij de opdrachtregel van de vRealize Automation-appliance als rootgebruiker.
- 3 Voer bij de opdrachtprompt de volgende vRealize Automation-opdracht uit:

```
vracli disk-mgr resize
```

Als het wijzigen van de grootte voor vRealize Automation mislukt, raadpleegt u [Knowledge Base-artikel 79925](#).

De DNS-toewijzing voor vRealize Automation bijwerken

Een beheerder kan de DNS-toewijzingen voor vRealize Automation bijwerken.

Procedure

- 1 Meld u aan bij de console voor een vRealize Automation-appliance met behulp van SSH of VMRC.
- 2 Voer het volgende commando uit.

```
vracli network dns set --servers DNS1,DNS2
```

- 3 Controleer of de nieuwe DNS-servers correct op alle vRealize Automation-knooppunten zijn toegepast met het commando `vracli network dns status`.

- 4 Voer de volgende reeks commando's uit om de vRealize Automation-services op alle clusterknooppunten af te sluiten.

```
/opt/scripts/svc-stop.sh  
sleep 120  
/opt/scripts/deploy.sh --onlyClean
```

- 5 Start de vRealize Automation-knooppunten opnieuw en wacht totdat deze volledig zijn gestart.
- 6 Meld u aan bij elk vRealize Automation-knooppunt met SSH en controleer of de nieuwe DNS-servers worden weergegeven in `/etc/resolve.conf`.
- 7 Voer het volgende commando uit op een van de vRealize Automation-knooppunten om de vRealize Automation-services te starten: `/opt/scripts/deploy.sh`

Resultaten

De DNS-instellingen van vRealize Automation worden gewijzigd zoals opgegeven.

Hoe kan ik de tijdsynchronisatie van vRealize Automation inschakelen

U kunt de tijdsynchronisatie op uw vRealize Automation-implementatie inschakelen met behulp van de opdrachtregel van de vRealize Automation-appliance.

U kunt de tijdsynchronisatie voor uw standalone of geclusterde vRealize Automation-implementatie configureren met behulp van het NTP-netwerkprotocol (Network Time Protocol). vRealize Automation ondersteunt twee NTP-configuraties die elkaar wederzijds uitsluiten:

| NTP-configuratie | Beschrijving |
|------------------|--|
| ESXi | <p>U kunt deze configuratie gebruiken wanneer de ESXi-server waarop vRealize Automation wordt gehost, met een NTP-server wordt gesynchroniseerd. Als u een geclusterde implementatie gebruikt, moeten alle ESXi-hosts worden gesynchroniseerd met een NTP-server. Zie het KB-artikel 57147 vSphere Web Client gebruiken voor het configureren van NTP (Network Time Protocol) op een ESXi-host voor meer informatie over het configureren van NTP voor ESXi.</p> <hr/> <p>Opmerking Als uw vRealize Automation-implementatie wordt gemigreerd naar een ESXi-host die niet is gesynchroniseerd met een NTP-server, krijgt u mogelijk te maken met klokdrift.</p> |
| systemd | <p>Deze configuratie gebruikt de systemd-timesyncd-daemon om de klokken van uw vRealize Automation-implementatie te synchroniseren.</p> <hr/> <p>Opmerking De systemd-timesyncd-daemon is standaard ingeschakeld, maar geconfigureerd zonder NTP-servers. vRealize Automation-appliances met een dynamische IP-configuratie kunnen elke NTP-server gebruiken die via het DHCP-protocol communiceert.</p> |

Procedure

- 1 Meld u als **root** aan via de opdrachtregel van de vRealize Automation-appliance.
- 2 Schakel NTP in met ESXi.
 - a Voer de opdracht `vracli ntp esxi` uit.
 - b (Optioneel) Voer de opdracht `vracli ntp status` uit om de status van de NTP-configuratie te bevestigen.

U kunt ook de NTP-configuratie opnieuw instellen op de standaardstatus door het commando `vracli ntp reset` uit te voeren.
- 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. Elk netwerkadres moet tussen enkele aanhalingstekens worden geplaatst. Bijvoorbeeld: `vracli ntp systemd --set 'ntp_address_1', 'ntp_address_2'`

 - b (Optioneel) Voer de opdracht `vracli ntp status` uit om de status van de NTP-configuratie te bevestigen.

Resultaten

U hebt tijdsynchronisatie voor de implementatie van uw vRealize Automation-appliance ingeschakeld.

Wat nu te doen

De NTP-configuratie kan mislukken als er tussen de NTP-server en de vRealize Automation-implementatie een tijdverschil is van meer dan 10 minuten. Los dit probleem op door de vRealize Automation-appliance opnieuw op te starten.

Hoe kan ik het rootwachtwoord opnieuw instellen voor vRealize Automation

U kunt een verloren of vergeten rootwachtwoord voor vRealize Automation opnieuw instellen.

In deze procedure gebruikt u een commandoregelvenster op de vCenter-hostappliance om het hoofdwachtwoord voor vRealize Automation van uw organisatie opnieuw in te stellen.

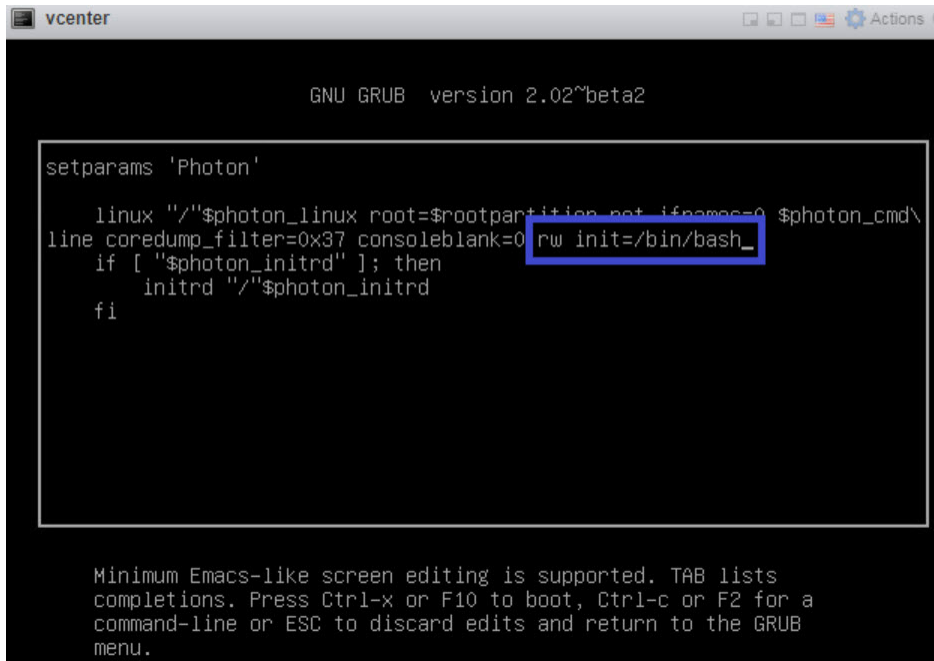
Voorwaarden

Dit is een procedure voor vRealize Automation-beheerders die de vereiste inloggegevens hebben voor de hostappliance van vCenter.

Procedure

- 1 Sluit vRealize Automation af en start deze opnieuw met behulp van de procedure die wordt beschreven in [vRealize Automation starten en stoppen](#).
- 2 Wanneer het opdrachtregelvenster van het Photon-besturingssysteem wordt weergegeven, voert u `e` in en drukt u op **ENTER** om de editor van het GNU GRUB-opstartmenu te openen.

- 3 Typ in de GNU GRUB-editor `rw init=/bin/bash` aan het einde van de regel die begint met `linux "/" $photon_linux root=rootpartition`. Dit ziet er als volgt uit:



```

GNU GRUB  version 2.02~beta2


setparams 'Photon'

  linux "/"$photon_linux root=$rootpartition boot ifnames=0 $photon_cmd\
line coredump_filter=0x37 consoleblank=0 rw init=/bin/bash_
  if [ "$photon_initrd" ]; then
    initrd "/"$photon_initrd
  fi

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.

```

- 4 Druk op **F10** om uw wijziging te pushen en vRealize Automation opnieuw te starten.
- 5 Wacht tot vRealize Automation opnieuw is gestart.
- 6 Typ `passwd` bij de prompt `root [/]#` en druk op **Enter**.
- 7 Typ het nieuwe wachtwoord bij de prompt `New password:` en druk op **Enter**.
- 8 Typ het nieuwe wachtwoord nogmaals bij de prompt `Retype new password:` en druk op **Enter**.
- 9 Typ `reboot -f` bij de prompt `root [/]#` en druk op **Enter** om de procedure voor het opnieuw instellen van het rootwachtwoord te voltooien.



```

root [/]# passwd
New password:
Retype new password:
passwd: password updated successfully
root [/]# reboot -f_

```

Wat nu te doen

U kunt zich nu als vRealize Automation-beheerder met het nieuwe rootwachtwoord aanmelden bij vRealize Automation.

Tenantconfiguraties voor meerdere organisaties gebruiken in vRealize Automation

4

Met vRealize Automation kunnen klanten in de vorm van IT-providers gebruiken om meerdere tenants of organisaties in te stellen binnen elke implementatie. Een provider kan voor elke implementatie multi-tenantorganisaties instellen en de infrastructuur toewijzen. De providers kunnen ook de gebruikers van de tenants beheren. Elke tenant houdt het beheer over zijn eigen projecten, resources en implementaties.

In een vRealize Automation-configuratie voor meerdere organisaties kunnen providers meerdere organisaties maken, waarbij elke tenantorganisatie zijn eigen projecten, resources en implementaties in gebruik heeft. De providers kunnen de tenantinfrastructuur weliswaar niet extern beheren, maar kunnen zich wel aanmelden bij de tenants en de infrastructuur van daaruit beheren.

Multitenancy is gebaseerd op de hieronder beschreven coördinatie en configuratie van drie verschillende VMware-producten:

- **Workspace ONE Access:** dit product biedt de infrastructurele ondersteuning voor multitenancy en de Active Directory-domeinverbindingen waarmee het gebruikers- en groepsbeheer binnen tenantorganisaties wordt geregeld.
- **vRealize Suite Lifecycle Manager:** met dit product kunt u tenants maken en configureren voor ondersteunde producten, zoals vRealize Automation. Daarnaast hebt u hiermee een beperkt aantal mogelijkheden voor certificaatbeheer.
- **vRealize Automation:** providers en gebruikers melden zich aan bij vRealize Automation om toegang te krijgen tot tenants waarin ze implementaties maken en beheren.

Wanneer u multitenancy configureert, moeten gebruikers bekend zijn met alle drie de producten en bijbehorende documentatie.

Zie het volgende voor meer informatie over het werken met vRealize Suite Lifecycle Manager en Workspace ONE Access.

- vRealize Suite Lifecycle Manager - zie de [productdocumentatie voor Lifecycle Manager](#)
- Workspace ONE Access - zie [Gebruikersbeheer met VMware Identity Manager](#) en [Beheer van VMware Workspace ONE Access](#)

Beheerders met rechten voor vRealize Suite Lifecycle Manager kunnen tenants maken en beheren via de pagina Tenants onder de service Identiteits- en tenantbeheer van Lifecycle Manager. Tenants worden gemaakt met behulp van een Active Directory-IWA of LDAP-verbinding en ondersteund door de bijbehorende VMware Workspace ONE Access-instantie die is vereist voor vRealize Automation-implementaties. Raadpleeg de bijbehorende documentatie voor informatie over het gebruik van Lifecycle Manager.

Wanneer u multitenancy configureert, begint u met een basis- of hoofdtenant. Deze tenant is de standaardtenant die wordt gemaakt wanneer de onderliggende Workspace ONE Access-applicatie wordt geïmplementeerd. Andere tenants, ook wel subtenants genoemd, kunnen worden gebaseerd op de hoofdtenant. vRealize Automation ondersteunt momenteel maximaal 20 tenantorganisaties met een standaardimplementatie van drie knooppunten.

Voordat u vRealize Automation inschakelt voor multitenancy, moet u de applicatie eerst in een configuratie met een afzonderlijke organisatie installeren en vervolgens Lifecycle Manager gebruiken om een configuratie met meerdere organisaties in te stellen. Een Workspace ONE Access-implementatie faciliteert het beheer van de tenants en bijbehorende Active Directory-domeinverbindingen.

Wanneer u multitenancy voor het eerst instelt, wordt een beheerder voor de provider aangewezen in Lifecycle Manager. U kunt deze aanstelling op een later tijdstip desgewenst wijzigen of nieuwe beheerders toevoegen. Onder configuraties voor meerdere organisaties worden vRealize Automation-gebruikers en -groepen voornamelijk via Workspace ONE Access beheerd.

Als de organisaties zijn gemaakt, kunnen bevoegde gebruikers zich aanmelden bij hun applicaties om projecten en resources te maken of gebruiken en implementaties te verrichten. Beheerders kunnen gebruikersrollen beheren in vRealize Automation.

Een configuratie voor meerdere organisaties instellen

Als u de installatie van vRealize Automation hebt voltooid, kunt u een implementatie met meerdere organisaties uitvoeren. Voor een configuratie met meerdere organisaties moet u eerst multitenancy instellen in uw externe Workspace ONE Access-applicatie en vervolgens Lifecycle Manager gebruiken om de tenants te maken en configureren. Dit geldt voor zowel nieuwe als bestaande implementaties. Voor de instelling van de tenants gaat u eerst naar Lifecycle Manager om een alias in te stellen voor de hoofdtenant, die standaard wordt gemaakt in Workspace ONE Access. Alle subtenants die u op basis van deze hoofdtenant maakt, nemen de Active Directory-domeinconfiguratie over van deze hoofdtenant.

In Lifecycle Manager wijst u tenants toe aan een product, zoals vRealize Automation, en aan een specifieke omgeving. Wanneer u een tenant instelt, moet u ook een tenantbeheerder aanwijzen. Multitenancy wordt standaard geregeld op basis van de hostnaam van de tenant. Gebruikers kunnen ervoor kiezen om de naam van de tenant handmatig te configureren op basis van DNS-naam. Tijdens deze procedure moet u verschillende vlaggen instellen om multitenancy mogelijk te maken en moet u tevens de load balancer configureren.

Als u een geclusterde instantie gebruikt, verwijzen de hostnamen van zowel de Workspace ONE Access- als vRealize Automation-tenant naar de load balancer.

Als de load balancers in deze geclusterde configuratie van vRealize Automation en Workspace ONE Access geen jokertekencertificaten gebruiken, moet de gebruiker de SAN-velden voor de hostnamen van de tenants toevoegen op de certificaten. Dit geldt voor elke nieuwe tenant die wordt gemaakt.

U kunt geen tenants verwijderen in vRealize Automation of Lifecycle Manager. Als u tenants wilt toevoegen aan een bestaande implementatie met meerdere tenants, kunt u dit doen met behulp van Lifecycle Manager, maar moet u wel rekening houden met een uitvaltijd van drie tot vier uur.

Zie de documentatielinks aan het begin van dit onderwerp voor meer informatie over het gebruik van vRealize Suite Lifecycle Manager en Workspace ONE Access.

Hostnamen en multitenancy

In eerdere versies van vRealize Automation hadden gebruikers toegang tot de tenants via een URL met een directorypad. In de huidige multitenancy implementatie krijgen gebruikers toegang tot tenants op basis van de hostnaam.

Daarnaast wordt voor de hostnamen waarmee vRealize Automation-gebruikers toegang krijgen tot de tenants, een andere indeling gebruikt dan die voor Workspace ONE Access-tenants.

Een geldige hostnaam ziet er bijvoorbeeld als volgt uit: `tenant1.example.eng.vmware.com`, in tegenstelling tot `vidm-node1.eng.vmware.com`.

Multitenancy en certificaten

U moet certificaten maken voor alle onderdelen die zijn betrokken bij een configuratie met meerdere organisaties. U hebt een of meer certificaten nodig voor Workspace ONE Access, Lifecycle Manager en vRealize Automation, afhankelijk van of u een configuratie met één knooppunt of een geclusterde configuratie gebruikt.

Bij het configureren van certificaten kunt u SAN-namen met jokertekens of unieke namen gebruiken. Aangezien de certificaten moeten worden bijgewerkt wanneer u nieuwe tenants toevoegt, wordt het certificaatbeheer enigszins vereenvoudigd als u gebruikmaakt van jokertekens. Als de load balancer van vRealize Automation en Workspace ONE Access geen jokertekencertificaten gebruikt, moet u voor alle nieuwe tenants SAN-velden voor de hostnamen van de tenants toevoegen op de certificaten. Als u SAN gebruikt, moet u de certificaten bovendien handmatig bijwerken wanneer u hosts toevoegt of verwijdert of een hostnaam wijzigt. Ook moet u de DNS-vermeldingen voor tenants bijwerken.

Houd er rekening mee dat Lifecycle Manager geen afzonderlijke certificaten maakt voor elke tenant. In plaats daarvan wordt een enkel certificaat gemaakt waarbij voor elke tenant de hostnaam wordt weergegeven. Voor basisconfiguraties gebruikt u de volgende notatie voor het CNAME-record van de tenant: *tenantname.vrahostname.domain*. Voor configuraties met hoge beschikbaarheid gebruikt u de volgende notatie voor de hostnaam: *tenantname.vraLBhostname.domain*.

Als u een geclusterde Workspace ONE Access-configuratie gebruikt, moet u er rekening mee houden dat Lifecycle Manager het load balancer-certificaat niet kan bijwerken, zodat u dit handmatig moet doen. Ook een eventuele hernieuwde registratie van externe producten of services van Lifecycle Manager moet u handmatig doen.

Dit hoofdstuk omvat de volgende onderwerpen:

- [Multitenancy voor meerdere organisaties instellen voor vRealize Automation](#)
- [vRealize Automation: aanmelden bij tenants en gebruikers toevoegen](#)
- [vRealize Orchestrator gebruiken met vRealize Automation-implementaties voor meerdere organisaties](#)

Multitenancy voor meerdere organisaties instellen voor vRealize Automation

Met behulp van vRealize Suite Lifecycle Manager kunt u een multitenancy voor meerdere organisaties instellen voor vRealize Automation.

Hier volgt een globale beschrijving van de procedure voor het instellen van multitenancy voor vRealize Automation, inclusief het configureren van DNS en certificaten. De procedure is bedoeld voor een implementatie met één knooppunt, maar bevat ook opmerkingen voor een geclusterde configuratie.

Zie <https://vmwarelab.org/2020/04/14/vrealize-automation-8-1-multi-tenancy-setup-with-vrealize-suite-lifecycle-manager-8-1/> voor meer informatie en een video voor het instellen van een vRealize Automation-configuratie met meerdere organisaties.

Voorwaarden

- Installeer en configureer Workspace ONE Access versie 3.3.4 of hoger.
- Installeer en configureer vRealize Suite Lifecycle Manager versie 8.5.

Procedure

- 1 Maak de vereiste DNS-records van het type A en CNAME.
 - Maak voor uw hoofdtenant en elke subtenant een SAN-certificaat en pas dit toe.
 - In implementaties met één knooppunt verwijst de FQDN van vRealize Automation naar de vRealize Automation-appliance en de FQDN van Workspace ONE Access naar de Workspace ONE Access-appliance.

- Voor geclusterde implementaties moeten zowel de Workspace ONE Access- en vRealize Automation-FQDN's op basis van tenants naar hun respectieve load balancers wijzen. Workspace ONE Access is geconfigureerd met SSL-beëindiging, zodat het certificaat wordt toegepast op zowel de Workspace ONE Access-cluster als de load balancer. De load balancer van vRealize Automation gebruikt SSL-passthrough, zodat het certificaat alleen op de vRealize Automation-cluster wordt toegepast.

Zie [Certificaat- en DNS-configuratie beheren bij implementaties voor meerdere organisaties en een enkel knooppunt](#) en [Certificaat- en DNS-configuratie beheren voor geclusterde implementaties van vRealize Automation](#) voor meer informatie.

- 2 Maak of importeer de vereiste SAN-certificaten voor meerdere domeinen voor zowel Workspace ONE Access als vRealize Automation.

Gebruik de kluis-service van Lifecycle Manager om certificaten inclusief licenties en wachtwoorden te maken. U kunt ook een CA-server of een ander mechanisme gebruiken om certificaten te genereren.

Als u extra tenants wilt toevoegen of maken, moet u uw vRealize Automation- en Workspace ONE Access-tenants opnieuw maken en toepassen.

Nadat u uw certificaten hebt gemaakt, kunt u deze toepassen in Lifecycle Manager met behulp van de levenscyclusbewerkingsfunctie. Selecteer eerst de omgeving en het product en vervolgens de optie Certificaat vervangen in het menu aan de rechterzijde. Selecteer vervolgens het product. Wanneer u een certificaat vervangt, moet u alle bijbehorende producten in uw omgeving opnieuw vertrouwen.

U kunt pas doorgaan met de volgende stap nadat het certificaat is toegepast en alle services opnieuw zijn opgestart.

Zie [Certificaat- en DNS-configuratie beheren bij implementaties voor meerdere organisaties en een enkel knooppunt](#) en [Certificaat- en DNS-configuratie beheren voor geclusterde implementaties van vRealize Automation](#) voor meer informatie.

- 3 Pas het SAN-certificaat voor Workspace ONE Access toe op de instantie of het cluster van Workspace ONE Access.

- 4 Voer in vRealize Suite Lifecycle Manager de wizard Tenancy inschakelen uit om multitenancy in te schakelen en een alias te maken voor de standaardhoofdtenant.

Als u tenancy inschakelt, moet u een alias maken voor de hoofdtenant of standaardtenant die als providerorganisatie fungeert. Als u tenancy hebt ingeschakeld, krijgt u via de FQDN van de hoofdtenant toegang tot Workspace ONE Access.

Als de bestaande FQDN van Workspace ONE Access bijvoorbeeld `idm.example.local` is en u een alias voor de hoofdtenant maakt terwijl tenancy is ingeschakeld, wordt de FQDN van Workspace ONE Access gewijzigd in `default-tenant.example.local` en verloopt de communicatie van alle clients die met Workspace ONE Access communiceren nu via `default-tenant.example.local`.

- 5 Pas de SAN-certificaten voor vRealize Automation toe op de vRealize Automation-instantie of -cluster.

U kunt SAN-certificaten toepassen via de service levenscyclusbewerkingen van Lifecycle Manager. Bekijk de details van de omgeving en selecteer vervolgens Certificaten vervangen in het rechtermenu. Wacht tot de taak voor het vervangen van certificaten is voltooid voordat u tenants toevoegt. Alle vRealize Automation-services worden als onderdeel van de certificaatvervanging opnieuw gestart.

- 6 Voer in Lifecycle Manager de wizard Tenants toevoegen uit om de gewenste tenants te configureren.

U kunt tenants toevoegen op de pagina Tenantbeheer onder Identiteits- en tenantbeheer van Lifecycle Manager. U kunt alleen tenants toevoegen waarvoor u eerder certificaten en DNS-instellingen hebt geconfigureerd.

Wanneer u een tenant maakt, moet u een tenantbeheerder aanwijzen en de Active Directory-verbindingen voor deze tenant instellen. De beschikbare verbindingen zijn gebaseerd op de instellingen van uw standaard- of hoofdtenant. U moet ook het product of de productinstantie selecteren waaraan de tenant wordt gekoppeld.

Wat nu te doen

Nadat u de tenants hebt gemaakt, gebruikt u de pagina Tenantbeheer onder Identiteits- en tenantbeheer van Lifecycle Manager om tenantbeheerders te wijzigen of toe te voegen, Active Directory-directory's aan de tenant toe te voegen en productkoppelingen van de tenant te wijzigen.

U kunt ook inloggen bij uw Workspace ONE Access-instantie om uw tenantconfiguratie te bekijken en valideren.

Certificaat- en DNS-configuratie beheren bij implementaties voor meerdere organisaties en een enkel knooppunt

Multitenancy vRealize Automation-configuraties voor meerdere organisaties vereisen een goede coördinatie tussen de verschillende producten en juiste configuratie van de DNS-instellingen en certificaten.

In deze configuratie voor meerdere configuraties wordt aangenomen dat de volgende onderdelen op één knooppunt zijn geïmplementeerd:

- Lifecycle Manager
- Workspace ONE Access Identity Manager
- vRealize Automation

Daarnaast wordt ervan uitgegaan dat u een standaardtenant als providerorganisatie hebt en twee subtenants, genaamd tenant-1 en tenant-2, maakt.

U kunt certificaten maken en toepassen met behulp van de kluisservice in vRealize Suite Lifecycle Manager of u kunt een ander mechanisme gebruiken. Met Lifecycle Manager kunt u ook certificaten voor vRealize Automation of Workspace ONE Access vervangen of opnieuw vertrouwen.

DNS-vereisten

U moet voor de systeemonderdelen een hoofdrecord van het type A maken en een record van het type CNAME (zie hieronder).

- Maak de A-hoofdrecords niet alleen voor alle systeemonderdelen maar ook voor alle tenants die u maakt wanneer u multitenancy inschakelt.
- Maak de multitenancy A-records voor zowel alle tenants die u maakt als voor de hoofdtenant.
- Maak de records van het type CNAME voor alle gewenste tenants, met uitzondering van de hoofdtenant.

Certificaatvereisten voor multitenancy implementatie met één knooppunt

U moet twee SAN-certificaten (met alternatieve namen) maken: een voor Workspace ONE Access en een voor vRealize Automation.

- Het vRealize Automation-certificaat bevat de hostnaam van de vRealize Automation-server en de namen van de tenants die u wilt maken.
- Het Workspace ONE Access-certificaat bevat de hostnaam van de Workspace ONE Access-server en de namen van de tenants die u maakt.
- Als u gereserveerde SAN-namen gebruikt, moet u de certificaten handmatig bijwerken wanneer u hosts toevoegt of verwijdert of een hostnaam wijzigt. Ook moet u de DNS-vermeldingen voor tenants bijwerken. U kunt de configuratie eventueel vereenvoudigen door jokertekens te gebruiken voor de Workspace ONE Access- en vRealize Automation-certificaten. Bijvoorbeeld: `*.example.com` en `*.vra.example.com`.

Opmerking vRealize Automation 8.x ondersteunt alleen wildcard-certificaten voor DNS-namen die voldoen aan de specificaties in de lijst met Openbare achtervoegsels bij <https://publicsuffix.org>. `*.myorg.com` is bijvoorbeeld een geldige naam, terwijl `*.myorg.local` ongeldig is.

Houd er rekening mee dat Lifecycle Manager geen afzonderlijke certificaten maakt voor elke tenant. In plaats daarvan wordt een enkel certificaat gemaakt waarbij voor elke tenant de hostnaam wordt weergegeven. Voor basisconfiguraties gebruikt u de volgende notatie voor het CNAME-record van de tenant: `tenantname.vrahostname.domain`. Voor configuraties met hoge beschikbaarheid gebruikt u de volgende notatie voor de hostnaam: `tenantname.vraLBhostname.domain`.

Samenvatting

In de volgende tabel vindt u een overzicht van de DNS- en certificaatvereisten voor een Workspace ONE Access- en vRealize Automation-implementatie met één knooppunt.

| DNS-vereisten | Vereisten voor SAN-certificaten |
|--|---|
| Main A Type Records lcm.example.local WorkspaceOne.example.local vra.example.local | Workspace One Certificate Hostnaam: WorkspaceOne.example.local, default-tenant.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local |
| Multi-tenancy A Type Records default-tenant.example.local tenant-1.example.local tenant-2.example.local | |
| Multi-Tenancy CNAME Type Records tenant-1.vra.example.local tenant-2.vra.example.local | vRealize Automation Certificate Hostnaam: vra.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local |

Certificaat- en DNS-configuratie beheren voor geclusterde implementaties van vRealize Automation

De instelling van een geclusterde vRealize Automation-implementatie met meerdere organisaties vereist een goede coördinatie van de certificaat- en DNS-configuratie tussen alle toepasselijke onderdelen.

Een geclusterde configuratie bestaat doorgaans uit drie Workspace ONE Access-appliances, drie vRealize Automation-appliances en één Lifecycle Manager-appliance.

In deze configuratie wordt aangenomen dat de volgende onderdelen geclusterd zijn geïmplementeerd:

- Workspace ONE Access Identity Manager-appliances:
 - idm1.example.local
 - idm2.example.local
 - idm3.example.local
 - idm-lb.example.local
- vRealize Automation-appliances:
 - vra-1.example.local
 - vra-2.example.local
 - vra-3.example.local
 - vra-lb.example.local
- Lifecycle Manager-appliance

DNS-vereisten

U moet de A-hoofdrecords niet alleen voor alle onderdelen maken, maar ook voor alle tenants die u maakt wanneer u multitenancy inschakelt. Tevens moet u de records van het type CNAME maken voor alle gewenste tenants, met uitzondering van de hoofdtenant. Ten slotte moet u ook A-hoofdrecords maken voor de Workspace ONE Access- en vRealize Automation-load balancers.

- Maak voor de drie Workspace ONE Access-appliances en voor de vRealize Automation-appliances A-records inclusief verwijzing naar hun bijbehorende FQDN.
- Maak daarnaast A-records voor de load balancers van Workspace ONE Access en vRealize Automation met een verwijzing naar hun bijbehorende FQDN.
- Maak multitenancy A-records voor zowel de standaardtenant als tenant-1 en tenant-2 met een verwijzing naar het IP-adres van de Workspace ONE Access-load balancer.
- Maak CNAME-records voor tenant-1 en tenant-2 met een verwijzing naar het IP-adres van de vRealize Automation-load balancer.

Vereisten voor SAN-certificaten (met alternatieve namen)

U moet twee Workspace ONE Access-certificaten maken: één voor de clusterappliances en één voor de load balancer. Daarnaast maakt u een certificaat voor de vRealize Automation-appliances (de gemaakte tenants), met uitzondering van de standaardtenant en de load balancer.

- Maak een certificaat voor de Workspace ONE Access-appliances waarin de FQDN's worden vermeld van zowel Workspace ONE Access-appliances als van de standaardtenant en andere tenants die u maakt. Dit certificaat moet de IP-adressen van de Workspace ONE Access-appliances bevatten.
- Het is aan te bevelen om een SSL-beëindiging te maken op de load balancer. Om deze beëindiging mogelijk te maken, maakt u een certificaat voor de Workspace ONE Access-load balancer waarin de FQDN wordt vermeld van zowel Workspace ONE Access-load balancer als van de standaardtenant en andere tenants die u maakt. Dit certificaat moet het IP-adres van de load balancer bevatten.
- U moet een certificaat maken voor vRealize Automation waarin de hostnamen worden vermeld van zowel de drie vRealize Automation-appliances als van de gerelateerde load balancer en gemaakte tenants. Daarnaast moeten de IP-adressen van de drie vRealize Automation-appliances worden vermeld.
- U kunt de configuratie eventueel vereenvoudigen door jokertekens te gebruiken voor de Workspace ONE Access- en vRealize Automation-certificaten. Bijvoorbeeld `*.example.com`, `*.vra.example.com` en `*.vra-lb.example.com`.

Opmerking vRealize Automation 8.x ondersteunt alleen wildcard-certificaten voor DNS-namen die voldoen aan de specificaties in de lijst met Openbare achtervoegsels bij <https://publicsuffix.org>. `*.myorg.com` is bijvoorbeeld een geldige naam, terwijl `*.myorg.local` ongeldig is.

Als u een geclusterde Workspace ONE Access-configuratie gebruikt, moet u er rekening mee houden dat Lifecycle Manager de load balancer-certificaten niet kan bijwerken, zodat u dit handmatig moet doen. Ook een eventuele hernieuwde registratie van externe producten of services van Lifecycle Manager moet u handmatig doen.

Samenvatting van DNS-vermeldingen en certificaten voor een geclusterde configuratie met meerdere organisaties

In de volgende tabel vindt u een overzicht van de vereisten voor DNS en certificaten voor een geclusterde Workspace ONE Access- en geclusterde vRealize Automation-implementatie met meerdere organisaties.

| DNS-vereisten | Vereisten voor SAN-certificaten |
|---|---|
| Main A Type Records lcm.example.local WorkspaceOne-1.example.local WorkspaceOne-2.example.local WorkspaceOne-3.example.local vra-1.example.local vra-2.example.local vra-3.example.local | Workspace One Certificate Hostnaam: WorkspaceOne-1.example.local, WorkspaceOne-2.example.local, WorkspaceOne-3.example.local, default-tenant.example.local, tenant-1.example.local, tenant-2.example.local |
| Multi-Tenancy A Type Records default-tenant.example.local tenant-1.vra.example.local tenant-2.vra.example.local | Workspace One LB Certificate (LB Terminated) Hostnaam: WorkSpaceOne-lb.example.local, default-tenant.example.local, vra.example.local, tenant-1.example.local, tenant-2.example.local |
| Multi-Tenancy CNAME Type Records tenant-1.vra-lb.example.local - vra-lb.example.local tenant-2.vra-lb.example.local - vra.lb.example.local | vRealize Automation Certificate Hostnaam: vra-1.example.local, vra-2.example.local, vra-3.example.local, vra-lb.example.local, tenant-1.example.local, tenant-2.example.local Door het gebruik van SSL-passthrough is hier geen certificaat vereist voor de vRealize Automation-load balancer. |

vRealize Automation: aanmelden bij tenants en gebruikers toevoegen

Nadat u tenants voor vRealize Automation hebt gemaakt in Lifecycle Manager, kunt u zich aanmelden bij Workspace ONE Access om uw tenants te bekijken en gebruikers toe te voegen.

Meld u aan bij de bijbehorende Workspace ONE Access-instantie om te zien welke tenants zijn gemaakt voor een vRealize Automation-implementatie. Gebruik `https://default-tenant.name.domainname.local` als URL of in het geval van een niet-geclusterde implementatie, `https://idm.domainname.local`, waarmee u wordt teruggeleid naar de Workspace ONE Access-URL van de standaardtenant.

U kunt specifieke tenants in Workspace ONE Access valideren met behulp van de volgende URL: `https://tenant-1.domainname.local`. Deze URL opent een pagina met een overzicht van de gebruikers voor de opgegeven tenant. Klik op **Gebruiker toevoegen** om op ad-hocbasis aanvullende gebruikers te maken.

Geautoriseerde gebruikers kunnen zich via `https://vra.domainname.local` aanmelden bij de providerorganisatie van vRealize Automation. Deze weergave biedt toegang tot alle gerelateerde vRealize Automation-services.

Geautoriseerde gebruikers kunnen zich via `https://tenantname.vra.domainname.local` aanmelden bij de toepasselijke tenants van vRealize Automation.

Zie [Gebruikers en groepen beheren](#) voor meer informatie over het beheer van gebruikers in Workspace ONE Access.

Lokale gebruikers toevoegen

U kunt lokale gebruikers aan uw implementatie toevoegen met behulp van de bijbehorende Workspace ONE Access-instantie. Lokale gebruikers zijn gebruikers die niet in een externe identiteitsprovider zijn opgeslagen.

vRealize Orchestrator gebruiken met vRealize Automation-implementaties voor meerdere organisaties

U kunt vRealize Orchestrator gebruiken met vRealize Automation-tenantimplementaties met meerdere organisaties.

De standaardtenant biedt zonder verdere configuratie ondersteuning voor integratie met de ingesloten vRealize Orchestrator-applicatie. vRealize Orchestrator is beschikbaar als vooraf geconfigureerd op de pagina Integraties van de standaardtenant. Subtenants hebben geen vooraf geregistreerde vRealize Orchestrator-integratie. Maar deze tenants hebben wel verschillende manieren om een vRealize Orchestrator-integratie toe te voegen.

- Subtenants kunnen een integratie met de ingesloten vRealize Orchestrator toevoegen door naar **Infrastructuur > Connectoren > Integraties** te gaan.

Opmerking Als de ingesloten vRealize Orchestrator als integratie aan meerdere tenants wordt toegevoegd, wordt alle vRealize Orchestrator-inhoud, inclusief de inventaris van invoegtoepassingen, gedeeld tussen deze tenants.

- Subtenants kunnen een externe vRealize Orchestrator-instantie toevoegen die vRealize Automation voor meerdere organisaties als verificatieprovider gebruikt.

Elke vRealize Orchestrator-instantie die een vRealize Automation-implementatie met meerdere organisaties als verificatieprovider gebruikt, kan bij elk van de tenants worden geregistreerd door een nieuwe integratie te maken en de FQDN van vRealize Orchestrator op te geven zonder verdere inloggegevens.

Werken met logboeken in vRealize Automation

5

U kunt het meegeleverde opdrachtregelhulpprogramma `vracli` gebruiken om logboeken in vRealize Automation te maken en gebruiken.

U kunt logboeken rechtstreeks in vRealize Automation gebruiken of in plaats daarvan alle logboeken doorsturen naar vRealize Log Insight.

Dit hoofdstuk omvat de volgende onderwerpen:

- [Hoe werk ik met logboeken en logboekbundels in vRealize Automation](#)
- [Hoe configureer ik het doorsturen van logboeken naar vRealize Log Insight in vRealize Automation](#)
- [Hoe kan ik een syslog-integratie maken of bijwerken in vRealize Automation](#)
- [Hoe werk ik met inhoudspakketten](#)

Hoe werk ik met logboeken en logboekbundels in vRealize Automation

Diverse services genereren automatisch logboeken. U kunt logboekbundels genereren in vRealize Automation. U kunt ook uw omgeving configureren om logboeken te sturen naar vRealize Log Insight.

Informatie over het gebruik van het hulpprogramma voor de `vracli`-opdrachtregel om logboekbundels te genereren, is beschikbaar via het argument `--help` in de `vracli`-opdrachtregel (bijvoorbeeld `vracli log-bundle --help`).

Zie [Hoe configureer ik het doorsturen van logboeken naar vRealize Log Insight in vRealize Automation](#) voor gerelateerde informatie over het gebruik van vRealize Log Insight.

Opdrachten voor logboekbundels

U kunt een logboekbundel maken om alle logboeken te bevatten die worden gegenereerd door de services die u uitvoert. Een logboekbundel bevat al uw servicelogboeken en is nodig voor het oplossen van problemen.

In een geclusterde omgeving (hoge beschikbaarheidsmodus) voert u de opdracht `vracli log-bundle` uit op slechts één knooppunt. Logboeken worden opgehaald van alle knooppunten in de omgeving. In het geval van een netwerkprobleem of een ander clusterprobleem worden logboeken echter opgehaald van het aantal knooppunten dat kan worden bereikt. Bijvoorbeeld: als een knooppunt in een cluster met drie knooppunten wordt ontkoppeld, worden logboeken alleen van de twee gezonde knooppunten verzameld. De uitvoer van de opdracht `vracli log-bundle` bevat informatie over eventuele gevonden problemen en de stappen voor een tijdelijke oplossing.

- Als u een logboekbundel wilt maken, moet u SSH gebruiken om verbinding te maken met een knooppunt en voert u de volgende `vracli`-opdracht uit:

```
vracli log-bundle
```

- Als u de time-outwaarde voor het verzamelen van logboeken van elk knooppunt wilt wijzigen, voert u de volgende `vracli`-opdracht uit:

```
vracli log-bundle --collector-timeout $CUSTOM_TIMEOUT_IN_SECONDS
```

In een omgeving met grote logboekbestanden, een traag netwerk of hoog CPU-gebruik kunt u de time-out bijvoorbeeld instellen op een grotere waarde dan de standaardwaarde van 1000 seconden.

- Als u andere opties, zoals time-out van Assembly en bufferlocatie, wilt configureren, gebruikt u de volgende Help-opdracht `vracli`:

```
vracli log-bundle --help
```

Indeling van logboekbundels

De logboekbundel is een tar-bestand met tijdstempel. De naam van de bundel komt overeen met het patroon `log-bundle-<datum>T<tijd>.tar`, bijvoorbeeld `log-bundle-20200629T131312.tar`. Een logboekbundel bevat doorgaans logboeken van alle knooppunten in de omgeving. In geval van een fout bevat deze zo veel mogelijk logboeken. Deze bevat minimaal logboeken van het lokale knooppunt.

De logboekbundel bestaat uit de volgende inhoud:

- Omgevingsbestand

Het omgevingsbestand bevat de uitvoer van diverse Kubernetes-onderhoudsopdrachten. Het geeft informatie over het huidige resourceverbruik per knooppunt en per pod. Tevens bevat het clusterinformatie en beschrijvingen van alle beschikbare Kubernetes-entiteiten.

- Hostlogboeken en -configuratie

De configuratie van elke host (bijvoorbeeld de directory `/etc`) en de hostspecifieke logboeken (bijvoorbeeld `journal`) worden in één directory verzameld voor elk clusterknooppunt of elke host. De naam van de directory komt overeen met de hostnaam van het knooppunt. De interne inhoud van de directory komt overeen met het bestandssysteem van de host. Het aantal dergelijke directory's komt overeen met het aantal clusterknooppunten.

■ Services-logboeken

Logboeken voor Kubernetes-services vindt u in de volgende mapstructuur:

- `<hostnaam>/services-logs/<naamruimte>/<appnaam>/file-logs/<containernaam>.log`
- `<hostnaam>/services-logs/<naamruimte>/<appnaam>/console-logs/
<containernaam>.log`

Een voorbeeld van een bestandsnaam is `my-host-01/services-logs/prelude/vco-app/file-logs/vco-server-app.log`.

- *hostnaam* is de hostnaam van het knooppunt waarop de applicatiecontainer actief is of was. Doorgaans is er één instantie voor elk knooppunt voor elke service. Bijvoorbeeld: 3 knooppunten = 3 instanties.
- *naamruimte* is de Kubernetes-naamruimte waarin de applicatie is of was geïmplementeerd. Voor gebruikersgerichte services is deze waarde `prelude`.
- *appnaam* is de naam van de Kubernetes-applicatie die de logboeken heeft geproduceerd, bijvoorbeeld `provisioning-service-app`.
- *containernaam* is de naam van de container die de logboeken heeft geproduceerd. Sommige apps bestaan uit meerdere containers. `vco-app` bevat bijvoorbeeld de `vco-server-app` en `vco-controlcenter-app-containers`.

■ (Oudere) Pod-logboeken

Vóór de wijzigingen in de architectuur van de logboekregistratie in vRealize Automation 8.2, bevonden de servicelogboeken (zoals beschreven in het vorige punt) zich in de directory van elke pod in de logboekbundel. Hoewel u kunt doorgaan met het genereren van pod-logboeken in de bundel met behulp van de `vracli log-bundle --include-legacy-pod-logs`-opdrachtregel, wordt dit niet aanbevolen, omdat alle logboekinformatie al in de logboeken van de services aanwezig is. Het opnemen van pod-logboeken kan de tijd en ruimte verhogen die vereist zijn om de logboekbundel te genereren.

De grootte van de logboekbundel verkleinen

Als u een kleinere logboekbundel wilt genereren, gebruikt u een van de volgende commando's met `vracli log-bundle`:

- `vracli log-bundle --since-days n`

Gebruik dit commando om alleen de logboekbestanden te verzamelen die in de afgelopen dagen zijn gegenereerd. Anders worden logboeken 7 dagen bewaard en verzameld.

Bijvoorbeeld:

```
vracli log-bundle --since-days 3
```

- `vracli log-bundle --services service_A,service_B,service_C`

Gebruik dit commando om alleen de logboeken te verzamelen voor de benoemde opgegeven services. Bijvoorbeeld:

```
vracli log-bundle --services ebs-app,vco-app
```

- `vracli log-bundle --skip-heap-dumps`

Gebruik dit commando om alle heapdumps uit de gegenereerde logboekbundel uit te sluiten.

De logboeken van een servicepod of -app uitvoeren

U kunt de logboeken van een servicepod of -app uitvoeren met het commando `vracli logs <pod_name>`.

De volgende opties zijn beschikbaar voor commando's:

- `--service`

Geeft een samengevoegd logboek weer voor alle knooppunten van de app in plaats van één pod

Bijvoorbeeld: `vracli logs --service abx-service-app`

- `--tail n`

Geeft de laatste *n* regels van het logboek weer. De standaardwaarde voor *n* is 10.

Bijvoorbeeld: `vracli logs --tail 20 abx-service-app-8598fcd4b4-tjwhk`

- `--file`

Geeft alleen het opgegeven bestand weer. Als er geen bestandsnaam wordt opgegeven, worden alle bestanden weergegeven.

Bijvoorbeeld: `vracli logs --file abx-service-app.log abx-service-app-8598fcd4b4-tjwhk`

Inzicht in logboekrotatie

Servicelogboeken bestaan aanvankelijk in een niet-gecomprimeerde toestand. Nadat een vRealize Log Insight-agent de logboekgegevens heeft verwerkt, worden door een vRealize Automation-opdracht `cron` de servicelogboeken gecomprimeerd.

Als zeventig procent van de `/var/log`-schijfpartitie wordt gebruikt, verwijdert een vRealize Automation-opdracht `cron` de oudste servicelogboeken.

Voer het volgende `vracli`-commando uit om informatie over de logboekrotatie te bekijken.

```
vracli cluster exec -- bash -c 'current_node; vracli disk-mgr; exit 0'
vracli cluster exec -- bash -c 'current_node; service prune-logs status; exit 0'
```

Hoe configureer ik het doorsturen van logboeken naar vRealize Log Insight in vRealize Automation

U kunt logboeken van vRealize Automation doorsturen naar vRealize Log Insight, waarmee u uitgebreide mogelijkheden hebt voor het analyseren van logboeken en genereren van rapporten.

vRealize Automation is gebundeld met een agent voor logboekregistratie van [Fluentd](#). Deze agent verzamelt en bewaart logboeken zodat u ze op een later tijdstip als logboekbundel kunt opvragen en onderzoeken. U kunt de agent configureren om een kopie van de logboeken met behulp van de vRealize Log Insight REST API door te sturen naar een vRealize Log Insight-server. Andere programma's kunnen via de meegeleverde API communiceren met vRealize Log Insight.

Zie de [documentatie voor vRealize Log Insight](#) voor meer informatie over vRealize Log Insight, inclusief documentatie voor de vRealize Log Insight REST API.

Configureer de logboekregistratieagent zodat deze doorlopend vRealize Automation-logboeken doorstuurt naar vRealize Log Insight met behulp van het meegeleverde `vracli` opdrachtregelhulpprogramma.

Alle logboekregels zijn voorzien van een tag voor hostnaam en omgeving en kunnen worden gecontroleerd in vRealize Log Insight. In een omgeving met hoge beschikbaarheid (HA) hebben logboeken, afhankelijk van het knooppunt waarop ze zijn gemaakt, tags met verschillende hostnamen. De omgevingstag kan worden geconfigureerd met behulp van de optie `--environment ENV`, zoals hieronder beschreven in de sectie *Integratie van vRealize Log Insight configureren en bijwerken*. In een HA-omgeving heeft de omgevingstag dezelfde waarde voor alle logboekregels, ongeacht het knooppunt waarvan ze afkomstig zijn.

Informatie over het gebruik van het hulpprogramma voor de `vracli`-opdrachtregel is beschikbaar via het argument `--help` in de `vracli`-opdrachtregel. Bijvoorbeeld: `vracli vrli --help`.

Opmerking U kunt slechts één integratie voor logboekregistratie op afstand configureren. vRealize Log Insight krijgt voorrang als er zowel een vRealize Log Insight-server als een Syslog-server beschikbaar is.

Controleer de bestaande configuratie van vRealize Log Insight

Command

```
vracli vrli
```

Arguments

De opdrachtregel bevat geen argumenten.

Output

De huidige configuratie voor de vRealize Log Insight-integratie wordt uitgevoerd in de JSON-indeling.

Exit codes

De volgende afsluitcodes zijn mogelijk:

- 0 - De integratie met vRealize Log Insight is geconfigureerd.
- 1 - Er is een uitzondering opgetreden tijdens het uitvoeren van de opdracht. Bekijk het foutbericht voor meer informatie.

- 61 (ENODATA) - De integratie met vRealize Log Insight is niet geconfigureerd. Bekijk het foutbericht voor meer informatie.

Example - check integration configuration

```
$ vracli vrli
No vRLI integration configured

$ vracli vrli
{
  "agentId": "0",
  "environment": "prod",
  "host": "my-vrli.local",
  "port": 9543,
  "scheme": "https",
  "sslVerify": false
}
```

Integratie van vRealize Log Insight configureren en bijwerken

Command

```
vracli vrli set [options] IP_OR_URL
```

Opmerking Nadat u de opdracht hebt uitgevoerd, kan het maximaal 2 minuten duren voordat de logboekregistratieagent uw opgegeven configuratie toepast.

Arguments

■ IP_OR_URL

Geeft de IP of het URL-adres op van de vRealize Log Insight-server die moet worden gebruikt voor het posten van logboeken. Standaard worden poort 9543 en https gebruikt. Als een van deze instellingen moet worden gewijzigd, kunt u in plaats daarvan een URL gebruiken.

Opmerking U kunt een ander hostschema (https is standaard) en andere poort (9543 is standaard voor https, 9000 is standaard voor http) instellen om logboeken te verzenden. Hier volgen enkele voorbeelden:

```
vracli vrli set https://IP:9543
vracli vrli set --insecure IP
vracli vrli set http://http://IP:9000
```

Poorten 9543 voor https en 9000 voor http worden gebruikt door de opname- REST API voor vRealize Log Insight-opname, zoals beschreven bij het onderwerp *Poorten en externe interfaces* onder *vRealize Log Insight beheren* in de [documentatie voor vRealize Log Insight](#).

■ Opties

- --agent-id SOME_ID

Stelt de id van de logboekregistratieagent voor deze appliance in. De standaardwaarde is 0. Wordt gebruikt om de agent te identificeren wanneer u logboeken post naar vRealize Log Insight met behulp van de vRealize Log Insight REST API.

- `--environment ENV`

Stelt een id voor de huidige omgeving in. Deze id wordt als tag weergegeven voor elke logboekvermelding in vRealize Log Insight-logboeken. De standaardwaarde is `prod`.

- `--ca-file /path/to/server-ca.crt`

Geeft een bestand op dat het certificaat bevat van de certificaatautoriteit (CA) die is gebruikt om het certificaat van de vRealize Log Insight-server te ondertekenen. Dit dwingt de logboekregistratieagent om de opgegeven CA te vertrouwen en zorgt dat de agent het certificaat van de vRealize Log Insight-server kan controleren als dit is ondertekend door een niet-vertrouwde autoriteit. Om het certificaat te verifiëren, kan het bestand een hele certificaatketen bevatten. Als het een zelfondertekend certificaat betreft, geeft u het certificaat zelf door.

- `--ca-cert CA_CERT`

Definitie is identiek aan die van `--ca`-bestand als hierboven, maar geeft in plaats daarvan het certificaat (keten) inline als tekenreeks door.

- `--insecure`

Deactiveert SSL-verificatie van het servercertificaat. Dit dwingt de logboekregistratieagent om elk SSL-certificaat te accepteren wanneer logboeken worden gepost.

- Geavanceerde opties

- `--request-max-size BYTES`

Meerdere logboekgebeurtenissen worden opgenomen met één API-aanroep. Dit argument bepaalt de maximale grootte van de lading, in bytes, voor elke aanvraag. Geldige waarden liggen tussen 4000 en 4000000. De standaardwaarde is 256000. Zie opname van vRealize Log Insight-gebeurtenissen in de documentatie voor de vRealize Log Insight REST API voor gerelateerde informatie over toegestane waarden. Als u deze waarde te laag instelt, kunnen logboekregistratiegebeurtenissen die groter zijn dan de toegestane grootte, worden verwijderd.

- `--request-timeout SECONDS`

Een aanroep naar de API kan om een aantal redenen vastlopen, inclusief problemen met het externe systeem, netwerkproblemen, enzovoort. Deze parameter regelt het aantal seconden dat wordt gewacht op de voltooiing van elke bewerking, zoals het openen van een verbinding, het schrijven van gegevens of het wachten op een reactie, voordat de aanroep wordt herkend als mislukt. De waarde mag niet minder dan 1 seconde zijn. De standaardwaarde is 30.

- `--request-immediate-retries RETRIES`

Logboeken worden gebufferd in samengevoegde segmenten voordat ze worden verzonden naar vRealize Log Insight. (Zie `--buffer-flush-thread-count` hieronder.) Als een API-aanvraag mislukt, wordt onmiddellijk een nieuwe poging ondernomen voor het logboek. Het standaard aantal directe pogingen is 3. Als geen van de nieuwe pogingen lukt, wordt het hele logboeksegment teruggedraaid en wordt het later opnieuw geprobeerd.

- `--request-http-compress`

Om de netwerkverkeervolumes te verlagen, kunt u gzip-compressie toepassen op aanvragen die naar de vRealize Log Insight-server worden verzonden. Als deze parameter niet is opgegeven, wordt er geen compressie gebruikt.

- `--buffer-flush-thread-count THREADS`

Voor betere prestaties en om netwerkverkeer te beperken, worden logboeken lokaal in een buffer opgeslagen voordat ze worden leeggemaakt en naar de logboekserver worden verzonden. Elk segment bevat logboeken van één service. Afhankelijk van uw omgeving kunnen segmenten groot worden waardoor het leegmaken ervan tijdrovend wordt. Dit argument bepaalt het aantal segmenten dat gelijktijdig kan worden leeggemaakt. De standaardwaarde is 2.

Opmerking Wanneer u integratie via https configureert en de vRealize Log Insight-server is geconfigureerd voor het gebruik van een niet-vertrouwd certificaat zoals een zelfondertekend certificaat of een certificaat dat is ondertekend door een niet-vertrouwde autoriteit, moet u een van de opties `--ca-file`, `--ca-cert` of `--insecure` gebruiken. Anders kan de logboekregistratieagent de serveridentiteit niet valideren en worden geen logboeken verzonden. Wanneer u `--ca-file` of `--ca-cert` gebruikt, moet het vRealize Log Insight-servercertificaat geldig zijn voor de hostnaam van de server. Controleer in alle gevallen de integratie door enkele minuten te wachten op de verwerking en vervolgens te controleren of vRealize Log Insight de logboeken heeft ontvangen.

Output

Er wordt geen uitvoer verwacht.

Exit codes

De volgende afsluitcodes zijn mogelijk:

- 0 - De configuratie is bijgewerkt.
- 1 - Er is een uitzondering opgetreden tijdens het uitvoeren van de opdracht. Bekijk het foutbericht voor meer informatie.

Examples - Configure or update integration configuration

De volgende voorbeeldinstructies worden weergegeven op afzonderlijke commandoregels, maar de argumenten kunnen worden gecombineerd op één commandoregel. U kunt bijvoorbeeld meerdere argumenten opnemen wanneer u `vracli vrli set {somehost}` of `vracli vrli set --ca-file path/to/server-ca.crt` gebruikt om de standaardwaarden van de agent-id of de omgeving te wijzigen. Zie de online help voor commando's bij `vracli vrli --help` voor gerelateerde informatie.

```
$ vracli vrli set my-vrli.local
$ vracli vrli set 10.20.30.40
$ vracli vrli set --ca-file /etc/ssl/certs/ca.crt 10.20.30.40
$ vracli vrli set --ca-cert "$(cat /etc/ssl/certs/ca.crt)" 10.20.30.40
$ vracli vrli set --insecure http://my-vrli.local:8080
$ vracli vrli set --agent-id my-vrli-agent my-vrli.local
$ vracli vrli set --request-http-compress
$ vracli vrli set --environment staging my-vrli.local
$ vracli vrli set --environment staging --request-max-size 10000 --request-timeout 120 --
request-immediate-retries 5 --buffer-flush-thread-count 4 my-vrli.local
```

Integratie van vRealize Log Insight wissen

Command

```
vracli vrli unset
```

Opmerking Nadat u de opdracht hebt uitgevoerd, kan het maximaal 2 minuten duren voordat de logboekregistratieagent uw opgegeven configuratie toepast.

Arguments

De opdrachtregel bevat geen argumenten.

Output

Bevestiging wordt uitgevoerd als tekst zonder opmaak.

Exit codes

De volgende afsluitcodes zijn beschikbaar:

- 0 - De configuratie is gewist of er bestond geen configuratie.
- 1 - Er is een uitzondering opgetreden tijdens het uitvoeren van de opdracht. Bekijk het foutbericht voor meer informatie.

Examples - Clear integration

```
$ vracli vrli unset
Clearing vRLI integration configuration

$ vracli vrli unset
No vRLI integration configured
```

Hoe kan ik een syslog-integratie maken of bijwerken in vRealize Automation

U kunt vRealize Automation configureren om uw logboekinformatie te verzenden naar externe syslog-servers.

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

De externe syslog-integratie van vRealize Automation ondersteunt de volgende verbindingstypen:

- Via UDP.
- Via TCP zonder TLS.

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

- Via TCP met TLS.

Opmerking U kunt slechts één integratie voor logboekregistratie op afstand configureren. vRealize Log Insight krijgt prioriteit als er zowel een vRealize Log Insight-server als een Syslog-server beschikbaar is.

Zie [Hoe configureer ik het doorsturen van logboeken naar vRealize Log Insight in vRealize Automation](#) voor informatie over het configureren van logboekintegraties met vRealize Log Insight.

Voorwaarden

Configureer een externe Syslog-server.

Procedure

- 1 Meld u als **root** aan via de opdrachtregel van de vRealize Automation-appliance.
- 2 Als u een integratie met een syslog-server wilt maken, 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 opgeeft voor 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 vlag `--ca-file` om een certificaatbestand toe te voegen. Gebruik de vlag `--ca-cert` om een certificaat als platte tekst toe te voegen.

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

Opmerking De vRealize Automation-appliance vraagt u standaard om te bevestigen dat u de syslog-integratie wilt overschrijven. Voeg de vlag `-f` of `--force` toe aan de opdracht `vracli remote-syslog set` om deze bevestiging over te slaan.

Wat nu te doen

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

Hoe verwijder ik een syslog-integratie voor logboekregistraties in vRealize Automation

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

Voorwaarden

Maak een of meer syslog-integraties in de vRealize Automation-appliance. Zie [Hoe kan ik een syslog-integratie maken of bijwerken in vRealize Automation](#).

Procedure

- 1 Meld u als **root** aan via de opdrachtregel van de vRealize Automation-appliance.
- 2 Verwijder syslog-integraties van de vRealize Automation-appliance met behulp van een van de volgende methoden:
 - Als u een specifieke syslog-integratie wilt verwijderen, voert u de opdracht `vracli remote-syslog unset -id Integration_name` uit.
 - Als u alle syslog-integraties van de vRealize Automation-appliance wilt verwijderen, voert u de opdracht `vracli remote-syslog unset` uit zonder de vlag `-id`.

Opmerking De vRealize Automation-appliance vraagt u standaard om te bevestigen dat u alle syslog-integraties wilt verwijderen. Voeg de vlag `-f` of `--force` toe aan de opdracht `vracli remote-syslog unset` om deze bevestiging over te slaan.

Hoe werk ik met inhoudspakketten

Inhoudspakketten worden in Log Insight gehost en bevatten dashboards, uitgepakte velden, opgeslagen query's en waarschuwingen die zijn gerelateerd aan een specifiek product of een set logboeken. U kunt door de community ondersteunde inhoudspakketten installeren vanaf VMware Sample Exchange en andere inhoudspakketten vanaf de Content Pack Marketplace.

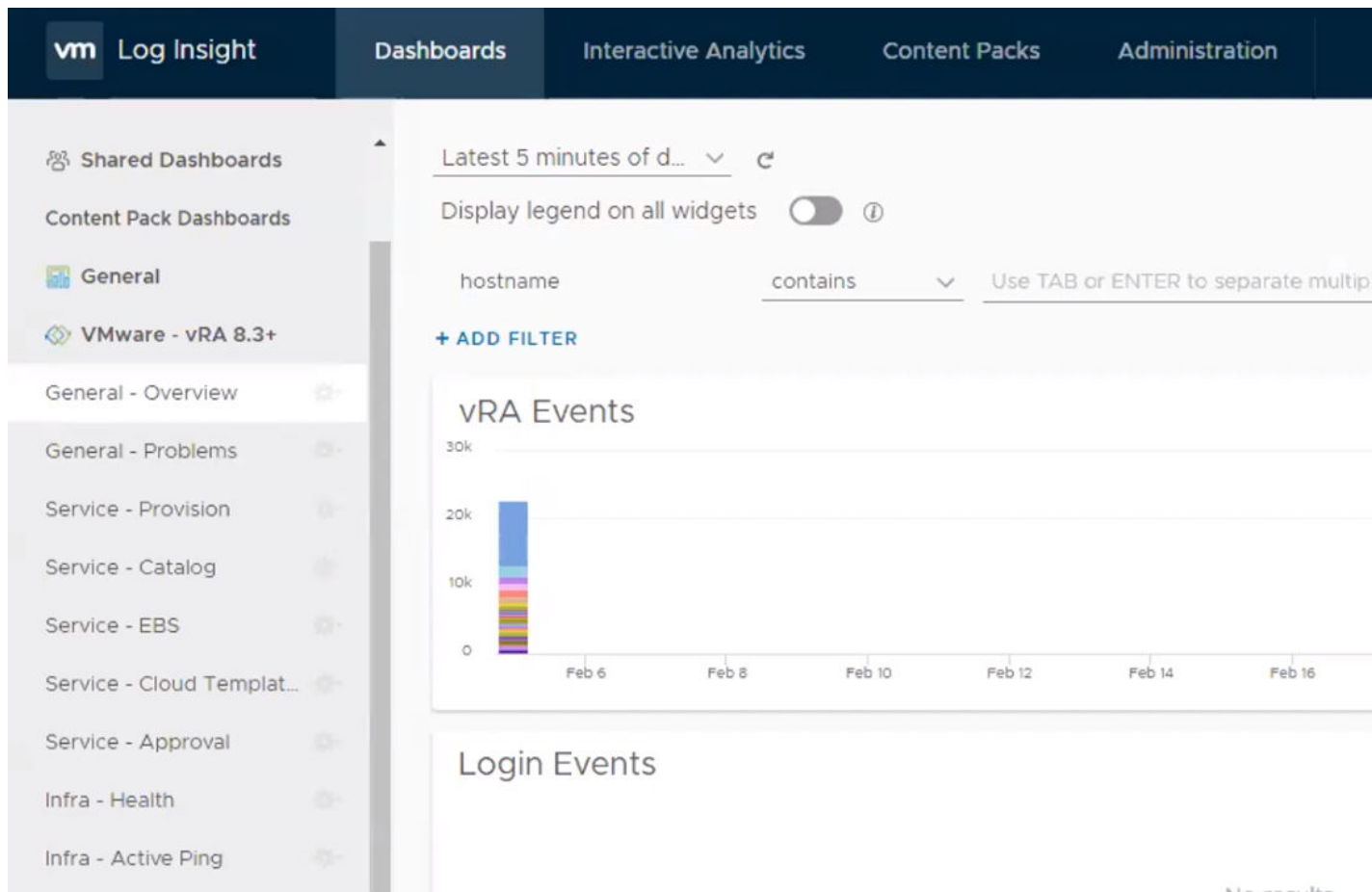
VMware vRealize Log Insight biedt geautomatiseerd logboekbeheer via aggregatie, analyses en zoekopdrachten, zodat operationele intelligentie en zichtbaarheid voor het hele bedrijf in dynamische hybride cloudomgevingen mogelijk worden. Inhoudspakketten zijn invoegtoepassingen voor VMware vRealize Log Insight die vooraf gedefinieerde kennis van specifieke typen gebeurtenissen zoals logberichten bieden.

Als u een inhoudspakket wilt downloaden, gaat u via Log Insight naar **Content Packs > Marketplace**. U kunt ook inhoudspakketten importeren door te klikken op **+ Import Content Pack**.

vRA 8.x-inhoudspakket

Het VMware vRealize Automation-inhoudspakket bevat een geconsolideerde samenvatting van logboekgebeurtenissen voor alle vRA-omgevingsonderdelen. Het bevat diverse dashboards die een algemeen overzicht, inzicht in fouten en bewerkingen en de algemene gezondheid van uw vRA-instantie bieden. Deze dashboards staan op het tabblad **Dashboard** samen met alle andere Log Insight-dashboards. Wanneer ze zijn geladen, kan het tot 30 seconden duren voordat de dashboards zijn gevuld met statistieken.


Opmerking U kunt niet van een vRA 7.5+-inhoudspakket upgraden naar het vRA 8.3-inhoudspakket. U moet het vRA 8.3-inhoudspakket installeren. Eenmaal geïnstalleerd, werken de 8.3- en 7.5-inhoudspakketten afzonderlijk.



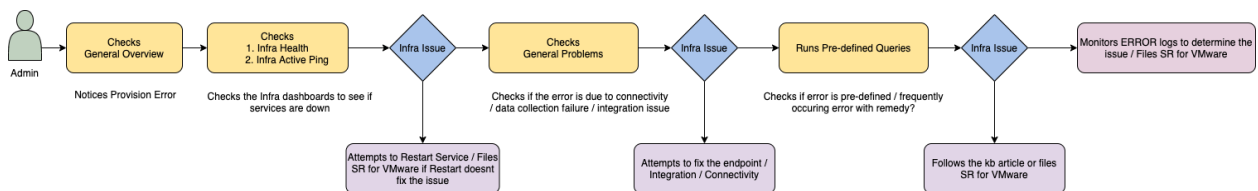
Het vRealize Automation-inhoudspakket bevat deze dashboards:

- Algemeen - Overzicht: toont een overzicht van statistieken op hoog niveau voor vRA.
- Algemeen - Problemen:
- Service - Inrichting: toont problemen met betrekking tot de inrichtingsservice.
- Service - Catalogus: toont problemen met betrekking tot de catalogusservice.
- Service - EBS: toont problemen met betrekking tot de gebeurtenisbrokerservice.
- Service - Cloudsjablonen: toont fouten en statistieken die zijn gerelateerd aan Cloud Assembly-cloudsjablonen, aangepaste resources en resourceacties.
- Service - Goedkeuring: toont fouten en statistieken met betrekking tot goedkeuringen.
- Infra - Gezondheid: toont wanneer pods in de loop van de tijd opnieuw worden gestart. Dit dashboard is essentieel om uitval te detecteren vanwege resourcelimieten.
- Infra - Actieve ping: toont de URL voor de gezondheidscontrole in de loop van de tijd.

Elk dashboard bevat individuele widgets die een gerichtere analyse bieden. Klik op het

informatiepictogram  om te bekijken welk type analyse in elke widget wordt uitgevoerd.

Als vRealize Automation-beheerder kunt u deze algemene inhoudspakketwerkstroom volgen om fouten te identificeren en problemen op te lossen.



Zie [vRealize Automation 8.3+ Log Insight Content Pack](#) en [How do I configure log forwarding to vRealize Log Insight](#) voor meer informatie over het vRealize Automation 8.3-inhoudspakket.

Deelname aan het Customer Experience Improvement Program voor vRealize Automation

6

Dit product neemt deel aan het Customer Experience Improvement Program (CEIP) van VMware. Het CEIP verstrekt VMware informatie op basis waarvan VMware haar producten en diensten kan verbeteren, problemen kan oplossen en u kan adviseren hoe u producten het beste kunt implementeren en gebruiken.

In het Trust & Assurance Center op <http://www.vmware.com/trustvmware/ceip.html> vindt u meer informatie over de gegevens die met CEIP worden verzameld en voor welke doeleinden deze worden gebruikt door VMware.

Dit hoofdstuk omvat de volgende onderwerpen:

- [Hoe kan ik me aan- of afmelden voor het Customer Experience Improvement Program van vRealize Automation](#)
- [Hoe configureer ik het tijdstip van gegevensverzameling voor het Customer Experience Improvement Program voor vRealize Automation](#)

Hoe kan ik me aan- of afmelden voor het Customer Experience Improvement Program van vRealize Automation

U kunt zich aan- of afmelden voor het Customer Experience Improvement Program (CEIP) via de opdrachtregel van de vRealize Automation-appliance.

Uw deelname aan het CEIP-programma kunt u regelen tijdens de installatie van vRealize Automation of met behulp van de vRealize Lifecycle Manager (LCM). U kunt uw deelname aan het programma ook na de installatie instellen met behulp van opdrachtregelopties.

Deelnemen aan het Customer Experience Improvement Program met behulp van opdrachtregelopties:

- 1 Meld u als **root** aan via de opdrachtregel van de vRealize Automation-appliance.
- 2 Voer de opdracht `vracli ceip on` uit.
- 3 Bekijk de informatie over het Customer Experience Improvement Program en voer de opdracht `vracli ceip on --acknowledge-ceip` uit.
- 4 Voer de opdracht `/opt/scripts/deploy.sh` uit om de vRealize Automation-services opnieuw te starten.

Deelname aan het Customer Experience Improvement Program opzeggen met behulp van opdrachtregelopties:

- 1 Meld u als **root** aan via de opdrachtregel van de vRealize Automation-appliance.
- 2 Voer de opdracht `vracli ceip off` uit.
- 3 Voer de opdracht `/opt/scripts/deploy.sh` uit om de vRealize Automation-services opnieuw te starten.

Hoe configureer ik het tijdstip van gegevensverzameling voor het Customer Experience Improvement Program voor vRealize Automation

U kunt instellen op welke datum en tijd het Customer Experience Improvement Program (CEIP) gegevens verstuurt naar VMware.

Procedure

- 1 Meld u als **root** aan via de opdrachtregel van de vRealize Automation-appliance.
- 2 Open het volgende bestand in een teksteditor.
`/etc/telemetry/telemetry-collector-vami.properties`
- 3 Wijzig de eigenschappen voor dag van de week (dow) en uur van de dag (hod).

| Eigenschap | Beschrijving |
|--|--|
| <code>frequency.dow=<day-of-week></code> | De dag waarop de gegevensverzameling plaatsvindt. |
| <code>frequency.hod=<hour-of-day></code> | De lokale tijd waarop de gegevensverzameling plaatsvindt. Mogelijke waarden zijn 0 t/m 23. |

- 4 Sla het bestand `telemetry-collector-vami.properties` op en sluit het.
- 5 Voer de volgende opdracht in om de instellingen toe te passen.

```
vcac-config telemetry-config-update --update-info
```

De wijzigingen worden toegepast op alle knooppunten in uw implementatie.