

Verwalten von vRealize Automation

Oktober 2022

vRealize Automation 8.3

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

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

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2022 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

1	Verwalten von vRealize Automation	4
2	Verwalten von Benutzern	5
	Aktivieren von Active Directory-Gruppen in vRealize Automation für Projekte	6
	Entfernen von Benutzern in vRealize Automation	7
	Wie bearbeite ich Benutzerrollen in vRealize Automation?	8
	Vorgehensweise zum Bearbeiten der Rollenzuweisung für Gruppen in vRealize Automation	8
	Definition der vRealize Automation-Benutzerrollen	9
3	Verwalten der Appliance	20
	Starten und Stoppen von vRealize Automation	20
	Horizontales Hochskalieren von vRealize Automation von einem auf drei Knoten	22
	Ersetzen eines Appliance-Knotens	24
	Verfügbarmachen von mehr Festplattenspeicher für die vRealize Automation-Appliance	25
	Aktualisieren der DNS-Zuweisung für vRealize Automation	26
	Vorgehensweise zum Aktivieren der Uhrzeitsynchronisierung	26
	Wie setze ich das Root-Kennwort zurück?	28
4	Verwenden von Mandantenkonfigurationen für mehrere Organisationen in vRealize Automation	30
	Einrichten von Mandantenfähigkeit für mehrere Organisationen für vRealize Automation	33
	Verwalten von Zertifikaten und DNS-Konfiguration in Bereitstellungen mit einem Knoten und mehreren Organisationen	35
	Verwalten der Zertifikat- und DNS-Konfiguration unter vRealize Automation-Clusterbereitstellungen	37
	Anmelden bei Mandanten und Hinzufügen von Benutzern in vRealize Automation	40
	Verwenden von vRealize Orchestrator in vRealize Automation-Bereitstellungen mit mehreren Organisationen	40
5	Arbeiten mit Protokollen	42
	Wie arbeite ich mit Protokollen und Protokollpaketen?	42
	Wie konfiguriere ich die Protokollweiterleitung zu vRealize Log Insight?	45
	Vorgehensweise zum Erstellen oder Aktualisieren einer Syslog-Integration	50
	Vorgehensweise zum Löschen einer Syslog-Integration für die Protokollierung	52
	Vorgehensweise zum Arbeiten mit Inhaltspaketen	52
6	Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit	55
	Wie nehme ich am Programm teil bzw. wie beende ich die Teilnahme?	55
	Wie konfiguriere ich die Datenerfassungszeit für das Programm?	56

Verwalten von vRealize Automation

1

In diesem Handbuch wird beschrieben, wie Sie wichtige Infrastruktur- und Benutzerverwaltungsaspekte einer vRealize Automation-Bereitstellung überwachen und verwalten.

Die hier beschriebenen Schritte sind von entscheidender Bedeutung, um eine vRealize Automation-Bereitstellung betriebsbereit zu halten. Zu diesen Aufgaben zählen die Benutzer- und Gruppenverwaltung sowie die Überwachung von Systemprotokollen.

Darüber hinaus wird beschrieben, wie Sie Bereitstellungen mit mehreren Organisationen konfigurieren und verwalten.

Einige vRealize Automation-Verwaltungsaufgaben werden innerhalb von vRealize Automation abgeschlossen, für andere müssen verwandte Produkte wie vRealize Suite Lifecycle Manager und Workspace ONE Access genutzt werden. Die Benutzer sollten sich mit diesen Produkten und ihren Funktionalitäten vertraut machen, bevor sie die entsprechenden Aufgaben ausführen.

Informationen zur Sicherung, Wiederherstellung und zur Notfallwiederherstellung finden Sie z. B. im Abschnitt über **Sicherung und Wiederherstellung und Notfallwiederherstellung > 2019** in der [vRealize Suite-Produktdokumentation](#).

Hinweis Die Notfallwiederherstellung wird in vRealize Automation 8.0.1 und höher unterstützt.

Informationen zur Arbeit mit vRealize Suite Lifecycle Manager-Installation, -Upgrade und -Verwaltung finden Sie in der [Lifecycle Manager-Produktdokumentation](#).

Verwalten von Benutzern und Gruppen in vRealize Automation

2

vRealize Automation verwendet VMware Workspace ONE Access, die von VMware zur Verfügung gestellte Identitätsverwaltungsanwendung, zum Importieren und Verwalten von Benutzern und Gruppen. Nach dem Importieren oder Erstellen von Benutzern und Gruppen können Sie die Rollenzuweisungen in Bereitstellungen für Einzelmandanten über die Seite „Identitäts- und Zugriffsverwaltung“ verwalten.

vRealize Automation wird mithilfe von VMware Lifecycle Manager (vRSLCM oder LCM) installiert. Bei der Installation von vRealize Automation müssen Sie eine vorhandene Workspace ONE Access-Instanz importieren oder eine neue bereitstellen, damit die Identitätsverwaltung unterstützt wird. Diese beiden Szenarien definieren Ihre Verwaltungsoptionen.

- Wenn Sie eine neue Workspace ONE Access-Instanz bereitstellen, können Sie Benutzer und Gruppen über LCM verwalten. Während der Installation können Sie eine Active Directory-Verbindung mithilfe von Workspace ONE Access einrichten. Alternativ können Sie einige Aspekte von Benutzern und Gruppen innerhalb von vRealize Automation über die Seite „Identitäts- und Zugriffsverwaltung“ anzeigen und bearbeiten. Das wird hier beschrieben.
- Wenn Sie eine vorhandene Workspace ONE Access-Instanz verwenden, importieren Sie sie während der Installation für die Verwendung mit vRealize Automation über LCM. In diesem Fall können Sie zum Verwalten von Benutzern und Gruppen weiterhin Workspace ONE Access verwenden, oder Sie können die Verwaltungsfunktionen in LCM verwenden.

Weitere Informationen zum Verwalten von Benutzern in einer Bereitstellung mit mehreren Organisationen finden Sie in [Anmelden bei Mandanten und Hinzufügen von Benutzern in vRealize Automation](#).

vRealize Automation-Benutzern müssen Rollen zugewiesen werden. Rollen definieren die Zugriffsrechte auf Funktionen innerhalb der Anwendung. Wenn vRealize Automation mit einer Workspace ONE Access-Instanz installiert wird, wird eine Standardorganisation erstellt und dem Installationsprogramm wird die Rolle des Organisationsbesitzers zugewiesen. Alle anderen vRealize Automation-Rollen werden vom Organisationsbesitzer zugewiesen.

In vRealize Automation gibt es drei Arten von Rollen: Organisationsrollen, Dienstrollen und Projektrollen. Für vRealize Automation Cloud Assembly, Service Broker und Code Stream können Rollen auf Benutzerebene typischerweise Ressourcen verwenden, während Rollen auf Administratorebene erforderlich sind, um Ressourcen zu erstellen und zu konfigurieren.

Organisationsrollen definieren Berechtigungen innerhalb des Mandanten. Organisationsbesitzer verfügen über Berechtigungen auf Administratorebene, während Organisationsmitglieder über Berechtigungen auf Benutzerebene verfügen. Organisationsbesitzer können andere Benutzer hinzufügen und verwalten.

Organisationsrollen	Dienstrollen
■ Organisationsbesitzer	■ Cloud Assembly-Administrator
■ Organisationsmitglied	■ Cloud Assembly-Benutzer
	■ Cloud Assembly-Viewer
	■ Service Broker-Administrator
	■ Service Broker-Benutzer
	■ Service Broker-Viewer
	■ Code Stream-Administrator
	■ Code Stream-Benutzer
	■ Code Stream-Betrachter

Darüber hinaus gibt es zwei Hauptrollen auf Projektebene, die nicht in der Tabelle angezeigt werden: Projektadministrator und Projektbenutzer. Diese Rollen werden projektbezogen ad hoc mit Cloud Assembly zugewiesen. Diese Rollen sind fließend. Derselbe Benutzer kann ein Administrator für ein Projekt und ein Benutzer in einem anderen Projekt sein. Weitere Informationen finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).

Weitere Informationen zum Arbeiten mit LCM und Workspace ONE Access finden Sie unter [Benutzerverwaltung mit VMware Identity Manager](#).

Dieses Kapitel enthält die folgenden Themen:

- [Aktivieren von Active Directory-Gruppen in vRealize Automation für Projekte](#)
- [Entfernen von Benutzern in vRealize Automation](#)
- [Wie bearbeite ich Benutzerrollen in vRealize Automation?](#)
- [Vorgehensweise zum Bearbeiten der Rollenzuweisung für Gruppen in vRealize Automation](#)
- [Definition der vRealize Automation-Benutzerrollen](#)

Aktivieren von Active Directory-Gruppen in vRealize Automation für Projekte

Ist eine Gruppe auf der Seite „Gruppen hinzufügen“ nicht verfügbar, wenn Sie Benutzer zu Projekten hinzufügen, überprüfen Sie die Seite „Identitäts- und Zugriffsverwaltung“ und fügen Sie die Gruppe hinzu, sofern sie verfügbar ist. Wenn die Gruppe auf der Seite „Identitäts- und Zugriffsverwaltung“ in vRealize Automation nicht aufgeführt ist, wurde die Gruppe möglicherweise nicht in Ihrer Workspace ONE Access-Instanz synchronisiert. Sie können überprüfen, ob die Synchronisierung durchgeführt wurde, und dann mit diesem Verfahren die Gruppe wie hier dargestellt hinzufügen.

Um Mitglieder einer Active Directory-Gruppe zu einem Projekt hinzuzufügen, müssen Sie sicherstellen, dass die Gruppe mit Ihrer Workspace ONE Access-Instanz synchronisiert wurde und dass die Gruppe zur Organisation hinzugefügt wird.

Voraussetzungen

Wenn Sie versuchen, nicht synchronisierte Gruppen zu einem Projekt hinzuzufügen, sind sie nicht verfügbar. Sie müssen Ihre Active Directory-Gruppen mit Ihrer Lifecycle Manager-Instanz synchronisiert haben.

Verfahren

- 1 Melden Sie sich bei vRealize Automation als Benutzer aus derselben Active Directory-Domäne an, die Sie hinzufügen. Beispiel: @mycompany.com
- 2 Klicken Sie in Cloud Assembly rechts oben in der Navigationsleiste auf „Identitäts- und Zugriffsverwaltung“.
- 3 Klicken Sie auf **Unternehmensgruppen** und anschließend auf **Rollen zuweisen**.
- 4 Suchen Sie mithilfe der Suchfunktion die Gruppe, die Sie hinzufügen, und wählen Sie sie aus.
- 5 Weisen Sie eine Organisationsrolle zu.

Die Gruppe muss mindestens über die Organisationsmitglied-Rolle verfügen. Weitere Informationen hierzu finden Sie unter [Was sind die Cloud Assembly-Benutzerrollen](#).
- 6 Klicken Sie auf **Dienstzugriff hinzufügen**, fügen Sie einen oder mehrere Dienste hinzu und wählen Sie für jeden eine Rolle aus.
- 7 Klicken Sie auf **Zuweisen**.

Ergebnisse

Sie können nun die Active Directory-Gruppe zu einem Projekt hinzufügen.

Entfernen von Benutzern in vRealize Automation

Sie können Benutzer nach Bedarf in vRealize Automation entfernen.

Alle Benutzer sind standardmäßig aufgeführt und Sie können keine Benutzer über die Seite „Identitäts- und Zugriffsverwaltung“ hinzufügen. Sie können Benutzer löschen.

Verfahren

- 1 Wählen Sie auf der Seite „Identitäts- und Zugriffsverwaltung“ die Registerkarte „Aktive Benutzer“ aus.
- 2 Suchen und wählen Sie die Benutzer aus, die Sie löschen möchten.
- 3 Klicken Sie auf **Benutzer entfernen**.

Ergebnisse

Die ausgewählten Benutzer werden entfernt.

Wie bearbeite ich Benutzerrollen in vRealize Automation?

Sie können Rollen bearbeiten, die in vRealize Automation importierten Workspace ONE Access-Benutzern zugewiesen wurden.

Voraussetzungen

Verfahren

- 1 Klicken Sie in Cloud Assembly rechts oben in der Navigationsleiste auf „Identitäts- und Zugriffsverwaltung“.
- 2 Wählen Sie den gewünschten Benutzer auf der Registerkarte „Aktive Benutzer“ aus und klicken Sie auf **Rollen bearbeiten**.
- 3 Sie können die Organisations- und Dienstrollen für den Benutzer bearbeiten.
 - Über die Auswahl im Dropdown-Menü neben der Überschrift „Organisationsrollen zuweisen“ können Sie die Beziehung des Benutzers zur Organisation ändern.
 - Klicken Sie auf „Dienstzugriff hinzufügen“, um neue Dienstrollen für den Benutzer hinzuzufügen.
 - Um Benutzerrollen zu entfernen, klicken Sie auf das X neben dem entsprechenden Dienst.
- 4 Klicken Sie auf **Speichern**.

Ergebnisse

Die Zuweisung der Benutzerrolle wird wie angegeben aktualisiert.

Vorgehensweise zum Bearbeiten der Rollenzuweisung für Gruppen in vRealize Automation

Sie können Rollenzuweisungen für Gruppen in vRealize Automation bearbeiten.

Voraussetzungen

Benutzer und Gruppen wurden aus einer gültigen vIDM-Instanz importiert, die Ihrer vRealize Automation-Bereitstellung zugeordnet ist.

Verfahren

- 1 Klicken Sie in Cloud Assembly rechts oben in der Navigationsleiste auf „Identitäts- und Zugriffsverwaltung“.
- 2 Wählen Sie die Registerkarte „Unternehmensgruppen“ aus.
- 3 Geben Sie den Namen der Gruppe, deren Rollenzuweisungen Sie bearbeiten möchten, im Suchfeld ein.

- 4 Bearbeiten Sie die Rollenzuweisungen für die ausgewählte Gruppe. Sie haben zwei Möglichkeiten:
 - Organisationsrollen zuweisen
 - Dienstrollen zuweisen
- 5 Klicken Sie auf **Zuweisen**.

Ergebnisse

Rollenzuweisungen werden wie angegeben aktualisiert.

Definition der vRealize Automation-Benutzerrollen

Als Organisationsbesitzer können Sie Benutzern Organisationsrollen und Dienstrollen zuweisen. Die Rollen bestimmen, was die Benutzer tun oder anzeigen können. Anschließend kann der Dienstadministrator in den Diensten Projektrollen zuweisen. Um die Rolle zu ermitteln, die Sie zuweisen möchten, werten Sie die Aufgaben in den folgenden Tabellen aus.

Cloud Assembly-Dienstrollen

Über die vRealize Automation Cloud Assembly-Dienstrolle wird festgelegt, was Benutzern in vRealize Automation Cloud Assembly angezeigt wird und welche Aufgaben sie ausführen können. Diese Dienstrollen werden in der Konsole von einem Organisationsbesitzer definiert.

Tabelle 2-1. Beschreibungen der vRealize Automation Cloud Assembly-Dienstrollen

Rolle	Beschreibung
Cloud Assembly-Administrator	Ein Benutzer, der über Lese- und Schreibzugriff auf die gesamte Benutzeroberfläche und die API-Ressourcen verfügt. Dies ist die einzige Benutzerrolle, mit alles angezeigt und durchgeführt werden kann, einschließlich Cloud-Konten hinzufügen, neue Projekte erstellen und einen Projektadministrator zuweisen.
Cloud Assembly-Benutzer	Ein Benutzer, der nicht über die Rolle des Cloud Assembly-Administrators verfügt. In einem vRealize Automation Cloud Assembly-Projekt fügt der Administrator Projekten Benutzer als Projektmitglieder, -administratoren oder -Viewer hinzu. Der Administrator kann auch einen Projektadministrator hinzufügen.
Cloud Assembly-Viewer	Ein Benutzer, der Lesezugriff zum Anzeigen von Informationen hat, Werte jedoch nicht erstellen, aktualisieren oder löschen kann. Dies ist eine Rolle, die für alle Projekte nur über Leserechte verfügt. Benutzer mit der Rolle „Viewer“ können alle für den Administrator verfügbaren Informationen anzeigen. Er kann keine Aktionen ausführen, es sei denn, er wird zu einem Projektadministrator oder Projektmitglied gemacht. Wenn der Benutzer zu einem Projekt gehört, verfügt er über die Berechtigungen, die mit dieser Rolle verbunden sind. Der Projekt-Viewer erweitert seine Berechtigungen nicht in der Weise, wie dies bei den Rollen „Projektadministrator“ oder „Projektmitglied“ der Fall ist.

Zusätzlich zu den Dienstrollen verfügt vRealize Automation Cloud Assembly über Projektrollen. Jedes Projekt ist in allen Diensten verfügbar.

Die Projektrollen sind in vRealize Automation Cloud Assembly definiert und können zwischen Projekten variieren.

Beachten Sie in den folgenden Tabellen, in denen die Berechtigungen der verschiedenen Dienst- und Projektrollen beschrieben werden, dass die Dienstadministratoren über Vollzugriff auf alle Bereiche der Benutzeroberfläche verfügen.

Die Beschreibungen der Projektrollen helfen Ihnen bei der Entscheidung, welche Berechtigungen Sie Ihren Benutzern erteilen möchten.

- Projektadministratoren nutzen die vom Dienstadministrator erstellte Infrastruktur, um sicherzustellen, dass die Projektmitglieder über die Ressourcen verfügen, die sie für ihre Entwicklungsarbeit benötigen.
- Projektmitglieder arbeiten im Rahmen ihrer Projekte daran, Cloud-Vorlagen zu entwerfen und bereitzustellen.
- Projekt-Viewer weisen lediglich Lesezugriff auf, außer in einigen Fällen, in denen sie nicht zerstörerische Vorgänge wie das Herunterladen von Cloud-Vorlagen durchführen können.

Tabelle 2-2. vRealize Automation Cloud Assembly-Dienstrollen und -Projektrollen

UI-Kontext	Aufgabe	Cloud Assembly- Administrator	Cloud Assembly- Viewer	Cloud Assembly-Benutzer	
				Der Benutzer muss ein Projektadministrationsmitglied sein, um projektbezogene Aufgaben anzeigen und durchführen zu können.	
				Projektadministrator	Projektmitglied
Zugriff auf Cloud Assembly					
Konsole	In der vRA-Konsole können Sie Cloud Assembly anzeigen und öffnen	Ja	Ja	Ja	Ja
Infrastruktur					
	Die Registerkarte „Infrastruktur“ anzeigen und öffnen	Ja	Ja	Ja	Ja
Konfigurieren – Projekte	Projekte erstellen	Ja			
	Werte aus der Projektübersicht, aus Bereitstellungen, Kubernetes und Integrationen aktualisieren oder löschen und Projektkonfigurationen testen.	Ja			
	Benutzer und Gruppen hinzufügen und Rollen in Projekten zuweisen.	Ja		Ja. Ihre Projekte.	
	Projekte anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Konfigurieren – Cloud-Zonen	Cloud-Zonen erstellen, aktualisieren oder löschen	Ja			
	Cloud-Zonen anzeigen	Ja	Ja		
Konfigurieren – Kubernetes-Zonen	Kubernetes-Zonen erstellen, aktualisieren oder löschen	Ja			
	Kubernetes-Zonen anzeigen	Ja	Ja		
Konfigurieren – Konfigurationen	Konfigurationen erstellen, aktualisieren oder löschen	Ja			
	Konfigurationen anzeigen	Ja	Ja		
Konfigurieren – Image-Zuordnungen	Image-Zuordnungen erstellen, aktualisieren oder löschen	Ja			
	Image-Zuordnungen anzeigen	Ja	Ja		
Konfigurieren – Netzwerkprofile	Netzwerkprofile erstellen, aktualisieren oder löschen	Ja			
	Image-Netzwerkprofile anzeigen	Ja	Ja		
Konfigurieren – Speicherprofile	Speicherprofile erstellen, aktualisieren oder löschen	Ja			

Tabelle 2-2. vRealize Automation Cloud Assembly-Dienstrollen und -Projektrollen (Fortsetzung)

UI-Kontext	Aufgabe	Cloud Assembly-Administrator	Cloud Assembly-Viewer	Cloud Assembly-Benutzer Der Benutzer muss ein Projektadministrationsmitglied sein, um projektbezogene Aufgaben anzeigen und durchführen zu können.	
				Projektadministrator	Projektmitglied
	Image-Speicherprofile anzeigen	Ja	Ja		
Konfigurieren – Preisgestaltungskarten	Preisgestaltungskarten erstellen, aktualisieren oder löschen	Ja			
	Preisgestaltungskarten anzeigen	Ja	Ja		
Konfigurieren – Tags	Tags erstellen, aktualisieren oder löschen	Ja			
	Tags anzeigen	Ja	Ja		
Ressourcen – Computing	Erkannten Computing-Ressourcen Tags hinzufügen	Ja			
	Erkannte Computing-Ressourcen anzeigen	Ja	Ja		
Ressourcen – Netzwerke	Netzwerktags, IP-Bereiche, IP-Adresse ändern	Ja			
	Erkannte Netzwerkressourcen anzeigen	Ja	Ja		
Ressourcen – Sicherheit	Tags zu erkannten Sicherheitsgruppen hinzufügen	Ja			
	Erkannte Sicherheitsgruppen anzeigen	Ja	Ja		
Ressourcen – Speicher	Tags zu erfasstem Speicher	Ja			
	Speicher anzeigen	Ja	Ja		
Ressourcen – Maschinen	Maschinen hinzufügen und löschen	Ja			
	Maschinen anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Ressourcen – Volumes	Erkannte Speicher-Volumes löschen	Ja			
	Erkannte Speicher-Volumes anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Ressourcen – Kubernetes	Kubernetes-Cluster bereitstellen oder hinzufügen und Namespace erstellen oder hinzufügen	Ja			
	Kubernetes-Cluster und Namespaces anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte

Tabelle 2-2. vRealize Automation Cloud Assembly-Dienstrollen und -Projektrollen (Fortsetzung)

UI-Kontext	Aufgabe	Cloud Assembly-Administrator	Cloud Assembly-Viewer	Cloud Assembly-Benutzer Der Benutzer muss ein Projektadministrationsmitglied sein, um projektbezogene Aufgaben anzeigen und durchführen zu können.	
				Projektadministrator	Projektmitglied
Aktivität – Anforderungen	Datensätze der Bereitstellungsanforderung löschen	Ja			
	Datensätze der Bereitstellungsanforderung anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Aktivität – Ereignisprotokolle	Ereignisprotokolle anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Verbindungen – Cloud-Konten	Cloud-Konten erstellen, aktualisieren oder löschen	Ja			
	Cloud-Konten anzeigen	Ja	Ja		
Verbindungen – Integrationen	Integrationen erstellen, aktualisieren oder löschen	Ja			
	Integrationen anzeigen	Ja	Ja		
Onboarding	Onboarding-Pläne erstellen, aktualisieren oder löschen	Ja			
	Onboarding-Pläne anzeigen	Ja	Ja		
Marketplace					
	Die Registerkarte „Download-Center“ anzeigen und öffnen	Ja	Ja		
	Die heruntergeladenen Cloud-Vorlagen auf der Registerkarte „Design“ verwenden	Ja		Ja. Wenn sie mit Ihren Projekten verknüpft sind.	Ja. Wenn sie mit Ihren Projekten verknüpft sind.
Marketplace – Cloud-Vorlagen	Cloud-Vorlage herunterladen	Ja			
	Cloud-Vorlagen anzeigen	Ja	Ja		
Download-Center – Images	Images herunterladen	Ja			
	Images anzeigen	Ja	Ja		
Download-Center – Downloads	Protokoll aller heruntergeladenen Elemente anzeigen	Ja	Ja		
Erweiterbarkeit					
	Die Registerkarte „Erweiterbarkeit“ anzeigen und öffnen	Ja	Ja		

Tabelle 2-2. vRealize Automation Cloud Assembly-Dienstrollen und -Projektrollen (Fortsetzung)

UI-Kontext	Aufgabe	Cloud Assembly-Administrator	Cloud Assembly-Viewer	Cloud Assembly-Benutzer Der Benutzer muss ein Projektadministrationsmitglied sein, um projektbezogene Aufgaben anzeigen und durchführen zu können.	
				Projektadministrator	Projektmitglied
Ereignisse	Erweiterbarkeitsereignisse anzeigen	Ja	Ja		
Abonnements	Erweiterbarkeitsabonnements erstellen, aktualisieren oder löschen	Ja			
	Abonnements deaktivieren	Ja			
	Abonnements anzeigen	Ja	Ja		
Bibliothek – Ereignisthemen	Ereignisthemen anzeigen	Ja	Ja		
Bibliothek – Aktionen	Erweiterbarkeitsaktionen erstellen, aktualisieren oder löschen	Ja			
	Erweiterbarkeitsaktionen anzeigen	Ja	Ja		
Bibliothek – Workflows	Erweiterbarkeits-Workflows anzeigen	Ja	Ja		
Aktivität – Aktionsausführungen	Erweiterbarkeitsaktionsausführungen abbrechen oder löschen	Ja			
	Erweiterbarkeitsaktionsausführungen anzeigen	Ja	Ja		
Aktivität – Workflow-Ausführungen	Erweiterbarkeits-Workflow-Ausführungen anzeigen	Ja	Ja		
Design					
Design	Registerkarte „Design“ öffnen und eine Liste der Cloud-Vorlagen anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Cloud-Vorlagen	Cloud-Vorlagen erstellen, aktualisieren und löschen	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte
	Cloud-Vorlagen anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
	Cloud-Vorlagen herunterladen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
	Cloud-Vorlagen hochladen	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte
	Cloud-Vorlagen bereitstellen	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte
	Cloud-Vorlagen versionieren und wiederherstellen	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte

Tabelle 2-2. vRealize Automation Cloud Assembly-Dienstrollen und -Projektrollen (Fortsetzung)

UI-Kontext	Aufgabe	Cloud Assembly-Administrator	Cloud Assembly-Viewer	Cloud Assembly-Benutzer Der Benutzer muss ein Projektadministrationsmitglied sein, um projektbezogene Aufgaben anzeigen und durchführen zu können.	
				Projektadministrator	Projektmitglied
	Cloud-Vorlagen für Katalog freigeben	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte
Benutzerdefinierte Ressourcen	Benutzerdefinierte Ressourcen erstellen, aktualisieren oder löschen	Ja			
	Benutzerdefinierte Ressourcen anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Benutzerdefinierte Aktionen	Benutzerdefinierte Aktionen erstellen, aktualisieren oder löschen	Ja			
	Benutzerdefinierte Aktionen anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Bereitstellungen					
	Die Registerkarte „Bereitstellungen“ anzeigen und öffnen	Ja	Ja	Ja	Ja
	Bereitstellungen anzeigen, einschließlich Bereitstellungsdetails, Bereitstellungsverlauf und Informationen zur Fehlerbehebung.	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
	Tag-2-Aktionen für Bereitstellungen basierend auf Richtlinien ausführen.	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte

Service Broker-Dienstrollen

Über die vRealize Automation Service Broker-Dienstrolle wird festgelegt, was Benutzern in vRealize Automation Service Broker angezeigt wird und welche Aufgaben sie ausführen können. Diese Dienstrollen werden in der Konsole von einem Organisationsbesitzer definiert.

Tabelle 2-3. Beschreibungen der Service Broker-Dienstrollen

Rolle	Beschreibung
Service Broker-Administrator	Muss über Lese- und Schreibzugriff auf die gesamte Benutzeroberfläche und die API-Ressourcen verfügen. Dies ist die einzige Benutzerrolle, mit der alle Aufgaben ausgeführt werden können, zum Beispiel das Erstellen eines neuen Projekts und die Zuweisung eines Projektadministrators.
Service Broker-Benutzer	Jeder Benutzer, der nicht über die vRealize Automation Service Broker-Administratorrolle verfügt. In einem vRealize Automation Service Broker-Projekt fügt der Administrator Projekten Benutzer als Projektmitglieder, -administratoren oder -Viewer hinzu. Der Administrator kann auch einen Projektadministrator hinzufügen.
Service Broker-Viewer	Ein Benutzer, der Lesezugriff zum Anzeigen von Informationen hat, Werte jedoch nicht erstellen, aktualisieren oder löschen kann. Benutzer mit der Rolle „Viewer“ können alle für den Administrator verfügbaren Informationen anzeigen. Er kann keine Aktionen ausführen, es sei denn, er wird zu einem Projektadministrator oder Projektmitglied gemacht. Wenn der Benutzer zu einem Projekt gehört, verfügt er über die Berechtigungen, die mit dieser Rolle verbunden sind. Der Projekt-Viewer erweitert seine Berechtigungen nicht in der Weise, wie dies bei den Rollen „Projektadministrator“ oder „Projektmitglied“ der Fall ist.

Zusätzlich zu den Dienstrollen verfügt vRealize Automation Service Broker über Projektrollen. Jedes Projekt ist in allen Diensten verfügbar.

Die Projektrollen sind in vRealize Automation Service Broker definiert und können zwischen Projekten variieren.

Beachten Sie in den folgenden Tabellen, in denen die Berechtigungen der verschiedenen Dienst- und Projektrollen beschrieben werden, dass die Dienstadministratoren über Vollzugriff auf alle Bereiche der Benutzeroberfläche verfügen.

Die folgenden Beschreibungen von Projektrollen helfen Ihnen bei der Entscheidung, welche Berechtigungen Sie Ihren Benutzern erteilen möchten.

- Projektadministratoren nutzen die vom Dienstadministrator erstellte Infrastruktur, um sicherzustellen, dass die Projektmitglieder über die Ressourcen verfügen, die sie für ihre Entwicklungsarbeit benötigen.
- Projektmitglieder arbeiten im Rahmen ihrer Projekte daran, Cloud-Vorlagen zu entwerfen und bereitzustellen.
- Projekt-Viewer sind auf Lesezugriff beschränkt.

Tabelle 2-4. Service Broker-Dienstrollen und -Projektrollen

UI-Kontext	Aufgabe	Service Broker-Administrator	Service Broker-Viewer	Service Broker-Benutzer		
				Der Benutzer muss ein Projektadministrator sein, um projektbezogene Aufgaben anzeigen und durchführen zu können.		
				Projektadministrator	Projektmitglied	Projekt-Viewer
Zugriff auf Service Broker						
Konsole	In der Konsole können Sie Service Broker anzeigen und öffnen	Ja	Ja	Ja	Ja	Ja
Infrastruktur						
	Die Registerkarte „Infrastruktur“ anzeigen und öffnen	Ja	Ja			
Konfigurieren – Projekte	Projekte erstellen	Ja				
	Werte aus der Projektübersicht, aus Bereitstellungen, Kubernetes und Integrationen aktualisieren oder löschen und Projektkonfigurationen testen.	Ja				
	Benutzer und Gruppen hinzufügen und Rollen in Projekten zuweisen.	Ja		Ja. Ihre Projekte.		
	Projekte anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte	Ja. Ihre Projekte
Konfigurieren – Cloud-Zonen	Cloud-Zonen erstellen, aktualisieren oder löschen	Ja				
	Cloud-Zonen anzeigen	Ja	Ja			
Konfigurieren – Kubernetes-Zonen	Kubernetes-Zonen erstellen, aktualisieren oder löschen	Ja				
	Kubernetes-Zonen anzeigen	Ja	Ja			
Verbindungen – Cloud-Konten	Cloud-Konten erstellen, aktualisieren oder löschen	Ja				
	Cloud-Konten anzeigen	Ja	Ja			
Verbindungen – Integrationen	Integrationen erstellen, aktualisieren oder löschen	Ja				
	Integrationen anzeigen	Ja	Ja			

Tabelle 2-4. Service Broker-Dienstrollen und -Projektrollen (Fortsetzung)

UI-Kontext	Aufgabe	Service Broker-Administrator	Service Broker-Viewer	Service Broker-Benutzer Der Benutzer muss ein Projektadministrator sein, um projektbezogene Aufgaben anzeigen und durchführen zu können.		
				Projektadministrator	Projektmitglied	Projekt-Viewer
Aktivität – Anforderungen	Datensätze der Bereitstellungsanforderung löschen	Ja				
	Datensätze der Bereitstellungsanforderung anzeigen	Ja				
Aktivität – Ereignisprotokolle	Ereignisprotokolle anzeigen	Ja				
Inhalt und Richtlinien						
	Die Registerkarte „Inhalt und Richtlinien“ anzeigen und öffnen	Ja	Ja			
Inhaltsquellen	Inhaltsquellen erstellen, aktualisieren oder löschen	Ja				
	Inhaltsquellen anzeigen	Ja	Ja			
Inhaltsfreigabe	Freigegebene Inhalte hinzufügen oder entfernen	Ja				
	Freigegebene Inhalte anzeigen	Ja	Ja			
Inhalt	Format anpassen und Element konfigurieren	Ja				
	Inhalt anzeigen	Ja	Ja			
Richtlinien – Definitionen	Richtliniendefinitionen erstellen, aktualisieren oder löschen	Ja				
	Richtliniendefinitionen anzeigen	Ja	Ja			
Richtlinien – Durchsetzung	Durchsetzungsprotokoll anzeigen	Ja	Ja			
Benachrichtigungen – E-Mail-Server	E-Mail-Server konfigurieren	Ja				
Katalog						
	Die Registerkarte „Katalog“ anzeigen und öffnen	Ja	Ja	Ja	Ja	Ja

Tabelle 2-4. Service Broker-Dienstrollen und -Projektrollen (Fortsetzung)

UI-Kontext	Aufgabe	Service Broker-Administrator	Service Broker-Viewer	Service Broker-Benutzer Der Benutzer muss ein Projektadministrator sein, um projektbezogene Aufgaben anzeigen und durchführen zu können.		
				Projektadministrator	Projektmitglied	Projekt-Viewer
	Verfügbare Katalogelemente anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte	Ja. Ihre Projekte
	Ein Katalogelement anfordern	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte	
Bereitstellungen						
	Die Registerkarte „Bereitstellungen“ anzeigen und öffnen	Ja	Ja	Ja.	Ja	Ja
	Bereitstellungen anzeigen, einschließlich Bereitstellungsdetails, Bereitstellungsverlauf und Informationen zur Fehlerbehebung.	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte	Ja. Ihre Projekte
	Tag-2-Aktionen für Bereitstellungen basierend auf Richtlinien ausführen	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte	
Genehmigungen						
	Die Registerkarte „Genehmigungen“ anzeigen und öffnen	Ja	Ja	Ja	Ja	Ja
	Auf Genehmigungsanforderungen antworten	Ja		Nur Service Broker-Benutzerrolle	Nur Service Broker-Benutzerrolle	Nur Service Broker-Benutzerrolle

Verwalten der vRealize Automation-Appliance

3

Als Systemadministrator müssen Sie möglicherweise verschiedene Aufgaben ausführen, um sicherzustellen, dass die installierte vRealize Automation-Anwendung ordnungsgemäß funktioniert.

Wenn Sie zum ersten Mal mit vRealize Automation arbeiten, sind diese Aufgaben nicht erforderlich. Kenntnisse bezüglich der Durchführung dieser Aufgaben sind nützlich, wenn Sie Probleme bei der Leistung oder dem Produktverhalten beheben müssen.

Dieses Kapitel enthält die folgenden Themen:

- [Starten und Stoppen von vRealize Automation](#)
- [Horizontales Hochskalieren von vRealize Automation von einem auf drei Knoten](#)
- [Ersetzen eines vRealize Automation-Appliance-Knotens](#)
- [Verfügbarmachen von mehr Festplattenspeicher für die vRealize Automation-Appliance](#)
- [Aktualisieren der DNS-Zuweisung für vRealize Automation](#)
- [Vorgehensweise zum Aktivieren der Uhrzeitsynchronisierung in vRealize Automation](#)
- [Vorgehensweise zum Zurücksetzen des Root-Kennworts für vRealize Automation](#)

Starten und Stoppen von vRealize Automation

Gehen Sie beim Starten oder Herunterfahren von vRealize Automation ordnungsgemäß vor.

Zum Herunterfahren und Starten von vRealize Automation-Komponenten wird empfohlen, die im Abschnitt **Lebenszyklusvorgänge > Umgebungen** von vRealize Suite Lifecycle Manager bereitgestellte Funktion zum Aus- und Einschalten zu verwenden. In den folgenden Verfahren werden manuelle Methoden zum Herunterfahren und Starten von vRealize Automation-Komponenten für den Fall dargelegt, dass vRealize Suite Lifecycle Manager aus irgendeinem Grund nicht verfügbar ist.

vRealize Automation herunterfahren

Um die Datenintegrität zu erhalten, fahren Sie die vRealize Automation-Dienste herunter, bevor Sie die virtuellen Appliances ausschalten. Mithilfe von SSH oder VMRC können Sie alle Knoten über eine einzelne Appliance herunterfahren oder starten.

Hinweis Vermeiden Sie die Verwendung der `vracli reset vidm`-Befehle, falls dies überhaupt möglich ist. Dieser Befehl setzt die gesamte Konfiguration von Workspace ONE Access zurück und unterbricht die Zuordnung zwischen Benutzern und bereitgestellten Ressourcen.

- 1 Melden Sie sich bei der Konsole einer vRealize Automation-Appliance entweder per SSH oder per VMRC an.
- 2 Um die vRealize Automation-Dienste auf allen Clusterknoten herunterzufahren, führen Sie die folgenden Befehle aus.

Hinweis Wenn Sie einen dieser Befehle zum Ausführen kopieren und er fehlschlägt, fügen Sie ihn zuerst in Notepad ein und kopieren Sie ihn dann erneut, bevor Sie ihn ausführen. Bei diesem Vorgang werden alle ausgeblendeten Zeichen und anderen Artefakte, die in der Dokumentationsquelle vorhanden sein könnten, ausgeblendet.

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

- 3 Fahren Sie die vRealize Automation-Appliances herunter.

Ihre Bereitstellung von vRealize Automation wird jetzt heruntergefahren.

vRealize Automation starten

Nach einem ungeplanten Ausfall, einem kontrollierten Herunterfahren oder einem Wiederherstellungsvorgang müssen Sie die vRealize Automation-Komponenten in einer bestimmten Reihenfolge neu starten. vRLCM ist eine nicht kritische Komponente. Sie können sie also jederzeit starten. Komponenten von VMware Workspace ONE Access, vormals VMware Identity Management, müssen vor dem Starten von vRealize Automation gestartet werden.

Hinweis Überprüfen Sie, ob die entsprechenden Lastausgleichsdienste ausgeführt werden, bevor Sie die vRealize Automation-Komponenten starten.

- 1 Schalten Sie alle vRealize Automation-Appliances ein und warten Sie, bis sie gestartet wurden.
- 2 Melden Sie sich für jede Appliance mit SSH oder VMRC bei der Konsole an und führen Sie den folgenden Befehl aus, um die Dienste auf allen Knoten wiederherzustellen.

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

- 3 Stellen Sie mit folgendem Befehl sicher, dass alle Dienste in Betrieb sind.

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

Hinweis Sie sollten drei Instanzen jedes Dienstes im Status „Wird ausgeführt“ oder „Abgeschlossen“ sehen.

Wenn alle Dienste als „Wird ausgeführt“ oder „Abgeschlossen“ aufgelistet sind, ist vRealize Automation betriebsbereit.

vRealize Automation neu starten

Sie können alle vRealize Automation-Dienste zentral von jeder der Appliances in Ihrem Cluster neu starten. Folgen Sie den vorausgehenden Anweisungen, um vRealize Automation herunterzufahren, und starten Sie dann vRealize Automation anhand der Anweisungen. Bevor Sie vRealize Automation neu starten, stellen Sie sicher, dass alle anwendbaren Lastausgleichsdienste und VMware Workspace ONE Access-Komponenten ausgeführt werden.

Wenn alle Dienste als „Wird ausgeführt“ oder „Abgeschlossen“ aufgelistet sind, ist vRealize Automation betriebsbereit.

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob alle Dienste ausgeführt werden:

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

Horizontales Hochskalieren von vRealize Automation von einem auf drei Knoten

Bei zunehmendem Bedarf können Sie eine vRealize Automation-Bereitstellung horizontal von einem auf drei Knoten hochskalieren.

Zum Abschließen vieler der Schritte dieses Verfahrens müssen Sie Funktionen von vRealize Suite Lifecycle Manager verwenden. Informationen zur Arbeit mit vRealize Suite Lifecycle Manager-Installation, -Upgrade und -Verwaltung finden Sie in der [Lifecycle Manager-Produktdokumentation](#).

Wenn Sie eine geclusterter Bereitstellung mit drei Knoten verwenden, kann vRealize Automation in der Regel den Ausfall eines Knotens verkraften und funktioniert weiterhin. Wenn zwei Knoten in einem Cluster mit drei Knoten ausfallen, funktioniert vRealize Automation nicht mehr.

Voraussetzungen

Bei diesem Verfahren wird davon ausgegangen, dass Sie bereits über eine funktionierende vRealize Automation-Bereitstellung mit einem einzelnen Knoten verfügen.

Verfahren

- 1 Fahren Sie alle vRealize Automation-Appliances herunter.

Um die vRealize Automation-Dienste auf allen Clusterknoten herunterzufahren, führen Sie die folgenden Befehle aus.

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

Sie können die vRealize Automation-Appliances jetzt herunterfahren.

- 2 Erstellen Sie einen Snapshot der Bereitstellung.

Verwenden Sie die Option „Snapshot erstellen“ in vRealize Suite Lifecycle Manager **Lifecycle Operations > Umgebungen > vRA > Details anzeigen**.

Hinweis Online-Snapshots, die ohne Herunterfahren der vRealize Automation-Knoten erstellt wurden, werden ab Version 8.0.1 unterstützt. Bei vRealize Automation 8.0-Umgebungen müssen Sie die vRealize Automation-Knoten zunächst beenden.

- 3 Schalten Sie die vRealize Automation-Appliance ein und fahren Sie alle Container hoch.
- 4 Generieren oder importieren Sie mithilfe der Locker-Funktion unter **LCM > Locker > Zertifikate** in vRealize Suite Lifecycle Manager vRealize Automation-Zertifikate für alle Komponenten, einschließlich vRealize Suite Lifecycle Manager-Knoten-FQDNs und dem vollqualifizierten Domännennamen des vRealize Automation-Lastausgleichsdiensts.
Fügen Sie die Namen aller drei Appliances unter „Alternative Antragstellernamen“ hinzu.
- 5 Importieren Sie das neue Zertifikat in vRealize Suite Lifecycle Manager.
- 6 Ersetzen Sie das vorhandene vRealize Suite Lifecycle Manager-Zertifikat durch das im vorherigen Schritt mithilfe der LCM-Option „Zertifikat ersetzen“ unter **Lifecycle Operations > Umgebungen > vRA > Details anzeigen** generierte Zertifikat.
- 7 Skalieren Sie vRealize Automation horizontal auf drei Knoten hoch, indem Sie in **LCM > Lifecycle Operations > Umgebungen > vRA > Details anzeigen** „Komponenten hinzufügen“ auswählen.

Ergebnisse

vRealize Automation wurde auf eine Bereitstellung mit drei Knoten skaliert.

Ersetzen eines vRealize Automation-Appliance-Knotens

Wenn eine vRealize Automation-Appliance in einer Hochverfügbarkeitskonfiguration (HA) mit mehreren Knoten fehlgeschlagen ist, müssen Sie den fehlerhaften Knoten unter Umständen ersetzen.

Vorsicht Bevor Sie fortfahren, sollten Sie sich gemäß der Empfehlungen von VMware an den technischen Support wenden, um das HA-Problem zu beheben und sicherzustellen, dass das Problem auf einen Knoten begrenzt ist.

Wenn der technische Support feststellt, dass der Knoten ersetzt werden muss, gehen Sie wie folgt vor.

- 1 Erstellen Sie in vCenter Backup-Snapshots von jeder Appliance in der HA-Konfiguration.
In den Backup-Snapshots sollte kein VM-Arbeitsspeicher enthalten sein.

- 2 Fahren Sie den fehlerhaften Knoten herunter.

- 3 Notieren Sie sich die Build-Nummer der vRealize Automation-Software des fehlerhaften Knotens und die Netzwerkeinstellungen.

Notieren Sie sich den FQDN, die IP-Adresse, das Gateway, die DNS-Server und insbesondere die MAC-Adresse. Diese Werte werden dem Ersatzknoten zu einem späteren Zeitpunkt zugewiesen.

- 4 Der primäre Datenbankknoten muss einer der fehlerfreien Knoten sein. Führen Sie die folgenden Schritte aus:
 - a Melden Sie sich als Root-Benutzer bei der Befehlszeile eines fehlerfreien Knotens an.
 - b Suchen Sie nach dem Namen des primären Datenbankknotens, indem Sie folgenden Befehl ausführen.

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

Das Ergebnis sollte mit diesem Beispiel vergleichbar sein, bei dem postgres-1 als primärer Datenbankknoten fungiert.

```
"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 Stellen Sie sicher, dass der primäre Datenbankknoten ordnungsgemäß ausgeführt wird, indem Sie folgenden Befehl verwenden.

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


Das Ergebnis sollte mit diesem Beispiel vergleichbar sein, bei dem postgres-1 in der Liste als „ausgeführt“ und „fehlerfrei“ angezeigt wird.

```
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>
```

Wichtig Wenden Sie sich bei einem fehlerhaften primären Datenbankknoten an den technischen Support, anstatt den Vorgang fortzusetzen.

- 5 Entfernen Sie den fehlerhaften Knoten aus der Root-Befehlszeile des fehlerfreien Knotens.

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

- 6 Verwenden Sie vCenter zum Bereitstellen eines neuen vRealize Automation-Ersatzknotens.

Stellen Sie die Build-Nummer derselben vRealize Automation-Software bereit und wenden Sie die Netzwerkeinstellungen des fehlerhaften Knotens an. Geben Sie den FQDN, die IP-Adresse, das Gateway, die DNS-Server und insbesondere die MAC-Adresse an, die Sie zuvor notiert haben.

- 7 Schalten Sie den Ersatzknoten ein.

- 8 Melden Sie sich als Root-Benutzer bei der Befehlszeile des Ersatzknotens an.

- 9 Stellen Sie sicher, dass die anfängliche Startsequenz abgeschlossen ist, indem Sie folgenden Befehl ausführen.

```
vraccli status first-boot
```

Suchen Sie nach einer Meldung vom Typ `First boot complete`.

- 10 Treten Sie dem vRealize Automation-Cluster über den Ersatzknoten bei.

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

- 11 Melden Sie sich als Root-Benutzer bei der Befehlszeile des primären Datenbankknotens an.

- 12 Stellen Sie den reparierten Cluster durch Ausführen des folgenden Skripts bereit.

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

Verfügbarmachen von mehr Festplattenspeicher für die vRealize Automation-Appliance

Möglicherweise müssen Sie für Zwecke wie die Speicherung von Protokolldateien mehr Festplattenspeicher für die vRealize Automation-Appliance verfügbar machen.

Verfahren

- 1 Verwenden Sie vSphere, um die VMDK in der vRealize Automation-Appliance zu erweitern.
- 2 Melden Sie sich bei der Befehlszeile der vRealize Automation-Appliance als Root-Benutzer an.

- 3 Führen Sie bei der Eingabeaufforderung folgenden vRealize Automation-Befehl aus.

```
vracli disk-mgr resize
```

Wenn die Größenänderung von vRealize Automation fehlschlägt, finden Sie weitere Informationen dazu im [Knowledgebase-Artikel 79925](#).

Aktualisieren der DNS-Zuweisung für vRealize Automation

Ein Administrator kann die DNS-Zuweisungen für vRealize Automation aktualisieren.

Verfahren

- 1 Melden Sie sich bei der Konsole einer beliebigen vRealize Automation-Appliance mithilfe von SSH oder VMRC an.
- 2 Führen Sie den folgenden Befehl aus.

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

- 3 Stellen Sie mit dem Befehl `vracli network dns status` sicher, dass die neuen DNS-Server ordnungsgemäß auf alle vRealize Automation-Knoten angewendet wurden.
- 4 Führen Sie die folgenden Befehle aus, um die vRealize Automation-Dienste auf allen Clusterknoten herunterzufahren.

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

- 5 Starten Sie die vRealize Automation-Knoten neu und warten Sie, bis sie vollständig hochgefahren wurden.
- 6 Melden Sie sich bei jedem vRealize Automation-Knoten mit SSH an und stellen Sie sicher, dass die neuen DNS-Server unter `/etc/Resolve.conf` aufgeführt werden.
- 7 Führen Sie auf einem der vRealize Automation-Knoten den folgenden Befehl aus, um die vRealize Automation-Dienste zu starten: `/opt/scripts/deploy.sh`

Ergebnisse

Die DNS-Einstellungen von vRealize Automation werden wie angegeben geändert.

Vorgehensweise zum Aktivieren der Uhrzeitsynchronisierung in vRealize Automation

Sie können die Uhrzeitsynchronisierung in Ihrer vRealize Automation-Bereitstellung mithilfe der Befehlszeile der vRealize Automation-Appliance aktivieren.

Sie können die Uhrzeitsynchronisierung für Ihre eigenständige oder geclusterte vRealize Automation-Bereitstellung mithilfe des NTP-Netzwerkprotokolls (Network Time Protocol) konfigurieren. vRealize Automation bietet Unterstützung für zwei sich gegenseitig ausschließende NTP-Konfigurationen:

NTP-Konfiguration	Beschreibung
ESXi	<p>Diese Konfiguration kann verwendet werden, wenn der ESXi-Server, der die vRealize Automation hostet, mit einem NTP-Server synchronisiert ist. Wenn Sie eine geclusterte Bereitstellung verwenden, müssen alle ESXi-Hosts mit einem NFS-Server synchronisiert werden. Weitere Informationen zum Konfigurieren von NTP für ESXi finden Sie im KB-Artikel 57147 Konfigurieren von NTP (Network Time Protocol) auf einem ESXi-Host mithilfe des vSphere Web Client.</p> <p>Hinweis Wenn die vRealize Automation-Bereitstellung auf einen ESXi-Host migriert wird, der nicht mit einem NTP-Server synchronisiert ist, kann es zu einem Uhrenfehler kommen.</p>
systemd	<p>Diese Konfiguration verwendet den systemd-timesyncd-Daemon, um die Uhren Ihrer vRealize Automation-Bereitstellung zu synchronisieren.</p> <p>Hinweis Der systemd-timesyncd-Daemon ist standardmäßig aktiviert, aber ohne NFS-Server konfiguriert. Wenn die vRealize Automation-Appliance eine dynamische IP-Konfiguration verwendet, kann die Appliance alle vom DHCP-Protokoll empfangenen NTP-Server verwenden.</p>

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Automation-Appliance als **root** an.
- 2 Aktivieren Sie NTP mit ESXi.
 - a Führen Sie den Befehl `vracli ntp esxi` aus.
 - b (Optional) Führen Sie den Befehl `vracli ntp status` aus, um den Status der NTP-Konfiguration zu bestätigen.

3 Aktivieren Sie NTP mit systemd.

- a Führen Sie den Befehl `vracli ntp systemd --set FQDN_or_IP_of_systemd_server` aus.

Hinweis Sie können mehrere NTP-Server vom Typ `systemd` hinzufügen, indem Sie deren Netzwerkadressen durch ein Komma trennen. Jede Netzwerkadresse muss in einfache Anführungszeichen eingeschlossen werden. Beispiel: `vracli ntp systemd --set 'ntp_address_1','ntp_address_2'`

- b (Optional) Führen Sie den Befehl `vracli ntp status` aus, um den Status der NTP-Konfiguration zu bestätigen.

Ergebnisse

Sie haben Uhrzeitsynchronisierung für die Bereitstellung Ihrer vRealize Automation-Appliance aktiviert.

Nächste Schritte

Die NTP-Konfiguration kann fehlschlagen, wenn zwischen dem NTP-Server und der vRealize Automation-Bereitstellung eine Zeitdifferenz von mehr als 10 Minuten besteht. Um dieses Problem zu beheben, starten Sie die vRealize Automation-Appliance neu.

Vorgehensweise zum Zurücksetzen des Root-Kennworts für vRealize Automation

Sie können ein verloren gegangenes oder vergessenes vRealize Automation-Root-Kennwort zurücksetzen.

In diesem Verfahren verwenden Sie ein Befehlszeilenfenster auf der vCenter-Host-Appliance, um das vRealize Automation-Root-Kennwort Ihrer Organisation zurückzusetzen.

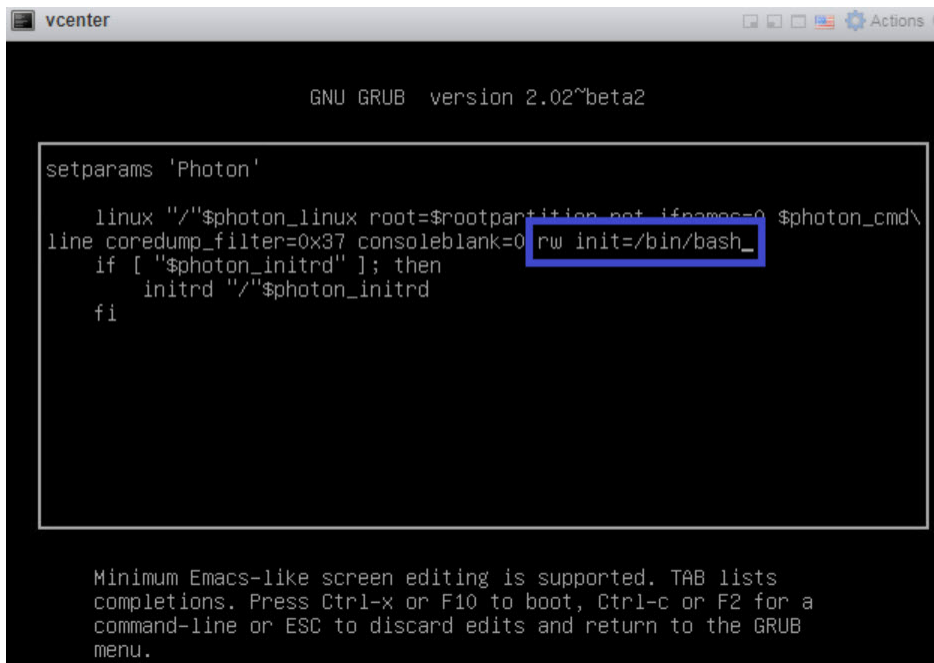
Voraussetzungen

Dieser Vorgang kann von vRealize Automation-Administratoren durchgeführt werden und erfordert die Anmeldedaten, die für den Zugriff auf die vCenter-Host-Appliance benötigt werden.

Verfahren

- 1 Fahren Sie vRealize Automation herunter und starten Sie das Programm mithilfe des in [Starten und Stoppen von vRealize Automation](#) beschriebenen Verfahrens.
- 2 Wenn das Befehlszeilenfenster des Photon-Betriebssystems angezeigt wird, geben Sie `e` ein und drücken die **Eingabetaste**, um den Editor des GNU GRUB-Startmenüs zu öffnen.

- 3 Geben Sie wie unten angezeigt im GNU GRUB-Editor den Wert `rw init=/bin/bash` am Ende der Zeile ein, die mit `linux "/" $photon_linux root=rootpartition` beginnt:



```

GNU GRUB  version 2.02~beta2

setparams 'Photon'

  linux "/"$photon_linux root=$rootpartition root_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 Drücken Sie **F10**, um die Änderung weiterzugeben und vRealize Automation neu zu starten.
- 5 Warten Sie, bis vRealize Automation neu gestartet wurde.
- 6 Geben Sie an der `root [/]#`-Eingabeaufforderung den Wert `passwd` ein und drücken Sie die **Eingabetaste**.
- 7 Geben Sie an der `New password:-`Eingabeaufforderung Ihr neues Kennwort ein und drücken Sie die **Eingabetaste**.
- 8 Geben Sie an der `Retype new password:-`Eingabeaufforderung erneut Ihr neues Kennwort ein und drücken Sie die **Eingabetaste**.
- 9 Geben Sie an der `root [/]#`-Eingabeaufforderung den Wert `reboot -f` ein und drücken Sie die **Eingabetaste**, um den Vorgang zum Zurücksetzen des Root-Kennworts abzuschließen.

```

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

```

Nächste Schritte

Als vRealize Automation-Administrator können Sie sich jetzt mit dem neuen Root-Kennwort bei vRealize Automation anmelden.

Verwenden von Mandantenkonfigurationen für mehrere Organisationen in vRealize Automation

4

Mithilfe von vRealize Automation können Kunden-IT-Anbieter mehrere Mandanten oder Organisationen innerhalb jeder Bereitstellung einrichten. Anbieter können mehrere Mandantenorganisationen einrichten und in jeder Bereitstellung eine Infrastruktur zuteilen. Anbieter können auch Benutzer für Mandanten verwalten. Jeder Mandant verwaltet seine eigenen Projekte, Ressourcen und Bereitstellungen.

In einer vRealize Automation-Konfiguration mit mehreren Organisationen können Anbieter mehrere Organisationen erstellen. Jede Mandantenorganisation verwendet hierbei eigene Projekte, Ressourcen und Bereitstellungen. Obwohl Anbieter die Mandanteninfrastruktur nicht remote verwalten können, können sie sich bei Mandanten anmelden und die Infrastruktur innerhalb der Mandanten verwalten.

Mehrmandantenfähigkeit basiert auf der Koordination und Konfiguration von drei verschiedenen VMware-Produkten, wie im Folgenden beschrieben:

- **Workspace ONE Access:** Dieses Produkt bietet die Infrastrukturunterstützung für Mehrmandantenfähigkeit und die Active Directory-Domänenverbindungen, die Benutzer- und Gruppenverwaltung innerhalb von Mandantenorganisationen ermöglichen.
- **vRealize Suite Lifecycle Manager:** Dieses Produkt unterstützt die Erstellung und Konfiguration von Mandanten für unterstützte Produkte, wie z. B. vRealize Automation. Darüber hinaus bietet es einige Zertifikatverwaltungsfunktionen.
- **vRealize Automation:** Anbieter und Benutzer melden sich bei vRealize Automation an, um auf Mandanten zuzugreifen, in denen sie Bereitstellungen erstellen und verwalten.

Bei der Konfiguration der Mehrmandantenfähigkeit sollten die Benutzer mit allen drei Produkten und der zugehörigen Dokumentationen vertraut sein.

Weitere Informationen zum Arbeiten mit Lifecycle Manager und Workspace ONE Access finden Sie unter [Benutzerverwaltung mit VMware Identity Manager](#) und [Verwalten von Benutzern und Gruppen](#).

Administratoren mit vRealize Suite Lifecycle Manager-Berechtigungen erstellen und verwalten Mandanten über die Seite „Lifecycle Manager-Mandanten“, die sich unterhalb des Identitäts- und Mandantenverwaltungsdiensts befindet. Mandanten werden mithilfe einer Active Directory IWA- oder LDAP-Verbindung erstellt und von der verknüpften VMware Workspace ONE Access-Instanz unterstützt, die für vRealize Automation-Bereitstellungen benötigt wird. Weitere Informationen zur Verwendung von Lifecycle Manager finden Sie in der zugehörigen Dokumentation.

Beim Konfigurieren der Mehrmandantenfähigkeit beginnen Sie mit einem Basis- oder Mastermandanten. Dieser Mandant ist der Standardmandant, der bei der Bereitstellung der zugrunde liegenden Workspace ONE Access-Anwendung erstellt wird. Andere Mandanten, die als Submandanten bezeichnet werden, können auf dem Master-Mandanten basieren. vRealize Automation unterstützt aktuell bis zu 20 Mandantenorganisationen mit der aus drei Knoten bestehenden Standardbereitstellung.

Wenn Sie vRealize Automation für Mehrmandantenfähigkeit konfigurieren, müssen Sie die Anwendung zunächst in einer einzelnen Organisationskonfiguration installieren und dann mithilfe von Lifecycle Manager eine mehrere Organisationen umfassende Konfiguration einrichten. Eine Workspace ONE Access-Bereitstellung unterstützt die Verwaltung von Mandanten und der zugehörigen Active Directory-Domänenverbindungen.

Bei der erstmaligen Konfiguration der Mehrmandantenfähigkeit wird in Lifecycle Manager ein Anbieteradministrator festgelegt. Sie können diesen Anbieteradministrator ändern oder Administratoren zu einem späteren Zeitpunkt hinzufügen. In Konfigurationen mit mehreren Organisationen werden vRealize Automation-Benutzer und -Gruppen in erster Linie über Workspace ONE Access verwaltet.

Nach der Erstellung von Organisationen können sich autorisierte Benutzer bei ihren Anwendungen anmelden, um Projekte und Ressourcen zu erstellen oder zu bearbeiten und Bereitstellungen zu erstellen. Administratoren können Benutzerrollen in vRealize Automation verwalten.

Einrichten einer Konfiguration mit mehreren Organisationen

Sie können eine Bereitstellung mit mehreren Organisationen aktivieren, nachdem Sie eine vRealize Automation-Installation abgeschlossen haben. Beim Einrichten einer Konfiguration mit mehreren Organisationen müssen Sie externen Workspace ONE Access für die Verwendung der Mehrmandantenfähigkeit konfigurieren und dann mithilfe von Lifecycle Manager Mandanten erstellen und konfigurieren. Dies gilt für neue und vorhandene Bereitstellungen. Als ersten Schritt zum Einrichten von Mandanten müssen Sie Lifecycle Manager verwenden, um einen Alias für den Mastermandanten festzulegen, der standardmäßig auf Workspace ONE Access erstellt wurde. Submandanten, die Sie anhand dieses Master-Mandanten erstellen, erben die Active Directory-Domänenverbindungen dieses Master-Mandanten.

In Lifecycle Manager weisen Sie einem Produkt, wie z. B. vRealize Automation, und einer bestimmten Umgebung Mandanten zu. Beim Einrichten eines Mandanten müssen Sie auch einen Mandantenadministrator festlegen. Standardmäßig wird die Mehrmandantenfähigkeit basierend auf dem Hostnamen des Mandanten aktiviert. Benutzer können den Mandantennamen manuell nach DNS-Namen konfigurieren. Während dieses Vorgangs müssen Sie verschiedene Flags zur Unterstützung der Mehrmandantenfähigkeit festlegen und einen Lastausgleichsdienst konfigurieren.

Wenn Sie eine Clusterinstanz verwenden, zeigen die auf dem Workspace ONE Access- und dem vRealize Automation-Mandanten basierenden Hostnamen auf den Lastausgleichsdienst.

Wenn die geclusterten vRealize Automation- und Workspace ONE Access-Lastausgleichsdienste keine Platzhalterzertifikate verwenden, müssen Benutzer Mandantenhostnamen als SAN-Einträge in den Zertifikaten hinzufügen. .

Sie können Mandanten in vRealize Automation oder Lifecycle Manager nicht löschen. Wenn Sie einer vorhandenen Bereitstellung mit Mehrmandantenfähigkeit Mandanten hinzufügen müssen, ist dies mithilfe von Lifecycle Manager möglich. In diesem Fall muss eine Ausfallzeit von drei bis vier Stunden in Kauf genommen werden.

Hostnamen und Mehrmandantenfähigkeit

In früheren Versionen von vRealize Automation riefen Benutzer Mandanten mit URLs auf, die auf dem Verzeichnispfad basierten. Bei der aktuellen Implementierung von Mehrmandantenfähigkeit greifen Benutzer auf der Basis des Hostnamens auf Mandanten zu.

Darüber hinaus unterscheidet sich das Hostnamenformat, das vRealize Automation-Benutzer für den Zugriff auf Mandanten verwenden, von dem Format, das für den Zugriff auf Mandanten innerhalb von Workspace ONE Access verwendet wird. Beispielsweise sieht ein gültiger Hostnamen wie folgt aus: `tenant1.example.eng.vmware.com`, im Gegensatz zu `vidm-nodel.eng.vmware.com`.

Mehrmandantenfähigkeit und Zertifikate

Sie müssen Zertifikate für alle Komponenten erstellen, die zu einer Konfiguration mit mehreren Organisationen gehören. Sie benötigen mindestens ein Zertifikat für Workspace ONE Access, Lifecycle Manager und vRealize Automation, je nachdem, ob Sie eine Konfiguration mit einem einzelnen Knoten oder eine Clusterkonfiguration verwenden.

Bei der Konfiguration von Zertifikaten können Sie Platzhalter mit den SAN- oder dedizierten Namen verwenden. Die Verwendung von Platzhaltern vereinfacht die Zertifikatsverwaltung, da Zertifikate aktualisiert werden müssen, wenn Sie neue Mandanten hinzufügen. Wenn die vRealize Automation- und Workspace ONE Access-Lastausgleichsdienste keine Platzhalterzertifikate verwenden, müssen Sie für jeden neu erstellten Mandanten Mandantenhostnamen als SAN-Einträge in den Zertifikaten hinzufügen. Bei Verwendung von SAN müssen Zertifikate darüber hinaus manuell aktualisiert werden, wenn Sie Hosts hinzufügen oder löschen oder einen Hostnamen ändern. Außerdem müssen Sie DNS-Einträge für Mandanten aktualisieren.

Beachten Sie, dass Lifecycle Manager keine separaten Zertifikate für jeden Mandanten erstellt. Stattdessen wird ein einzelnes Zertifikat erstellt, in dem der Hostname jedes Mandanten aufgelistet ist. In Basiskonfigurationen wird für den CNAME des Mandanten folgendes Format verwendet: *tenantname.vrahostname.domain*. In Hochverfügbarkeitskonfigurationen wird für den Namen folgendes Format verwendet: *tenantname.vraLBhostname.domain*.

Beachten Sie bei Verwendung einer Workspace ONE Access-Clusterkonfiguration, dass Lifecycle Manager das Zertifikat des Lastausgleichsdiensts nicht aktualisieren kann. Das Zertifikat muss in diesem Fall manuell aktualisiert werden. Darüber hinaus müssen Produkte oder Dienste, die sich außerhalb von Lifecycle Manager befinden, manuell neu registriert werden.

Dieses Kapitel enthält die folgenden Themen:

- [Einrichten von Mandantenfähigkeit für mehrere Organisationen für vRealize Automation](#)
- [Anmelden bei Mandanten und Hinzufügen von Benutzern in vRealize Automation](#)
- [Verwenden von vRealize Orchestrator in vRealize Automation-Bereitstellungen mit mehreren Organisationen](#)

Einrichten von Mandantenfähigkeit für mehrere Organisationen für vRealize Automation

Sie können Mandantenfähigkeit für mehrere Organisationen für vRealize Automation mithilfe von vRealize Suite Lifecycle Manager einrichten.

Im Folgenden finden Sie eine allgemeine Beschreibung des Verfahrens zur Einrichtung von Mehrmandantenfähigkeit für vRealize Automation, einschließlich der Konfiguration von DNS und Zertifikaten. Sie bezieht sich auf eine Bereitstellung mit einem Knoten, enthält aber Hinweise für eine Clusterkonfiguration.

Unter <https://vmwarelab.org/2020/04/14/vrealize-automation-8-1-multi-tenancy-setup-with-vrealize-suite-lifecycle-manager-8-1/> finden Sie weitere Informationen und eine Videopräsentation zum Einrichten einer vRealize Automation-Konfiguration mit mehreren Organisationen.

Voraussetzungen

- Installieren und Konfigurieren von Workspace ONE Access Version 3.3.4.
- Installieren und Konfigurieren Sie vRealize Suite Lifecycle Manager Version 8.3.

Verfahren

- 1 Erstellen Sie die erforderlichen DNS-Datensätze vom Typ „A“ und „CNAME“.
 - Sie müssen für den Mastermandanten und jeden Untermantanten ein SAN-Zertifikat erstellen und anwenden.
 - Für Bereitstellungen mit einem Knoten verweist der vRealize Automation-FQDN auf die vRealize Automation-Appliance, und der Workspace ONE Access-FQDN verweist auf die Workspace ONE Access-Appliance.

- Für Clusterbereitstellungen müssen die mandantenbasierten FQDNs sowohl für Workspace ONE Access als auch für vRealize Automation auf ihre entsprechenden Lastausgleichsdienste verweisen. Da Workspace ONE Access mit SSL-Terminierung konfiguriert ist, wird das Zertifikat sowohl auf den Workspace ONE Access-Cluster als auch auf den Lastausgleichsdienst angewendet. Der vRealize Automation-Lastausgleichsdienst verwendet SSL Passthrough, sodass das Zertifikat nur auf den vRealize Automation-Cluster angewendet wird.

Weitere Einzelheiten hierzu finden Sie unter [Verwalten von Zertifikaten und DNS-Konfiguration in Bereitstellungen mit einem Knoten und mehreren Organisationen](#) und [Verwalten der Zertifikat- und DNS-Konfiguration unter vRealize Automation-Clusterbereitstellungen](#).

- 2 Erstellen oder importieren Sie die erforderlichen Zertifikate für mehrere Domänen (SAN) für Workspace ONE Access und vRealize Automation.

Sie können Zertifikate in Lifecycle Manager mithilfe des Locker-Dienstes erstellen, mit dem Sie Zertifikatlizenzen und Kennwörter erstellen können. Alternativ dazu können Sie einen Zertifizierungsstellenserver oder einen anderen Mechanismus zum Generieren von Zertifikaten verwenden.

Wenn Sie zusätzliche Mandanten hinzufügen oder erstellen möchten, müssen Sie Ihre vRealize Automation- und Workspace ONE Access-Mandanten neu erstellen und anwenden.

Nachdem Sie Ihre Zertifikate erstellt haben, können Sie sie in Lifecycle Manager mit der Lifecycle Operations-Funktion anwenden. Sie müssen die Umgebung und das Produkt und dann die Option „Zertifikat ersetzen“ im Menü auf der rechten Seite auswählen. Anschließend können Sie das Produkt auswählen. Wenn Sie ein Zertifikat ersetzen, müssen Sie allen zugehörigen Produkten in Ihrer Umgebung erneut vertrauen.

Sie müssen warten, bis das Zertifikat angewendet und alle Dienste neu gestartet wurden, bevor Sie mit dem nächsten Schritt fortfahren.

Weitere Einzelheiten hierzu finden Sie unter [Verwalten von Zertifikaten und DNS-Konfiguration in Bereitstellungen mit einem Knoten und mehreren Organisationen](#) und [Verwalten der Zertifikat- und DNS-Konfiguration unter vRealize Automation-Clusterbereitstellungen](#).

- 3 Wenden Sie die Workspace ONE Access-SAN-Zertifikate auf die Workspace ONE Access-Instanz oder den Cluster an.
- 4 Führen Sie in vRealize Suite Lifecycle Manager den Assistenten zum Aktivieren der Mandantenfähigkeit aus, um die Mehrmandantenfähigkeit zu aktivieren, und erstellen Sie einen Alias für den standardmäßigen Mastermandanten.

Die Aktivierung der Mandantenfähigkeit erfordert, dass Sie einen Alias für den Mastermandanten oder den Standardmandanten der Anbieterorganisation erstellen. Nachdem Sie die Mandantenfähigkeit aktiviert haben, können Sie über den FQDN des Mastermandanten auf Workspace ONE Access zugreifen.

Wenn beispielsweise der vorhandene Workspace ONE Access-FQDN `idm.example.local` ist und Sie einen Alias des Standardmandanten erstellen, ändert sich der Workspace ONE Access-FQDN nach dem Aktivieren der Mandantenfähigkeit zu `default-tenant.example.local`, und alle Clients, die mit Workspace ONE Access kommunizieren, kommunizieren dann über `default-tenant.example.local`.

- 5 Wenden Sie die vRealize Automation-SAN-Zertifikate auf die vRealize Automation-Instanz oder den Cluster an.

Sie können SAN-Zertifikate über den Lifecycle Operations-Dienst von Lifecycle Manager anwenden. Sie müssen die Details der Umgebung anzeigen und dann im rechten Menü die Option „Zertifikate ersetzen“ auswählen. Sie müssen warten, bis die Zertifikatersetzungsaufgabe abgeschlossen ist, bevor Sie Mandanten hinzufügen. Im Rahmen der Zertifikatersetzung werden vRealize Automation-Dienste neu gestartet.

- 6 Führen Sie in Lifecycle Manager den Assistenten zum Hinzufügen von Mandanten aus, um die gewünschten Mandanten zu konfigurieren.

Sie fügen Mandanten mithilfe der Seite „Mandantenverwaltung in Lifecycle Manager unter „Identitäts- und Mandantenverwaltung“ hinzu. Sie können nur Mandanten hinzufügen, für die Sie zuvor Zertifikate und DNS-Einstellungen konfiguriert haben.

Beim Erstellen eines Mandanten müssen Sie einen Mandantenadministrator zuweisen, und Sie können die Active Directory-Verbindungen für diesen Mandanten auswählen. Verfügbare Verbindungen basieren auf denen, die in Ihrem Standard- oder Mastermandanten konfiguriert sind. Sie müssen auch das Produkt oder die Produktinstanz auswählen, der der Mandant zugeordnet werden soll.

Nächste Schritte

Nachdem Sie Mandanten erstellt haben, können Sie die Seite „Mandantenverwaltung“ in Lifecycle Manager unter „Identitäts- und Mandantenverwaltung“ verwenden, um Mandantenadministratoren zu ändern oder hinzuzufügen, Active Directory-Verzeichnisse zum Mandanten hinzuzufügen und Produktzuordnungen für den Mandanten zu ändern.

Sie können sich auch bei Ihrer Workspace ONE Access-Instanz anmelden, um Ihre Mandantenkonfiguration anzuzeigen und zu validieren.

Verwalten von Zertifikaten und DNS-Konfiguration in Bereitstellungen mit einem Knoten und mehreren Organisationen

vRealize Automation-Konfigurationen mit Mandantenfähigkeit für mehrere Organisationen stützten sich auf die koordinierte Konfiguration zwischen mehreren Produkten. Es muss sichergestellt werden, dass DNS-Einstellungen und Zertifikate ordnungsgemäß konfiguriert sind, damit die Konfiguration mit Mandantenfähigkeit für mehrere Organisationen funktioniert.

Diese Konfiguration für mehrere Organisationen setzt Knotenbereitstellungen für die folgenden Komponenten voraus:

- Lifecycle Manager

- Workspace ONE Access Identity Manager
- vRealize Automation

Außerdem wird davon ausgegangen, dass Sie mit einem Standardmandanten beginnen, der als Anbieterorganisation fungiert, und dass Sie zwei Untermantanten erstellen, die als Mandant-1 und Mandant-2 bezeichnet werden.

Sie können Zertifikate mithilfe des Locker-Diensts in vRealize Suite Lifecycle Manager erstellen und anwenden. Sie können aber auch einen anderen Mechanismus verwenden. Mit Lifecycle Manager können Sie Zertifikate in vRealize Automation oder Workspace ONE Access ersetzen oder diesen erneut vertrauen.

DNS-Anforderungen

Sie müssen sowohl Datensätze mit dem Haupttyp A sowie Datensätze mit dem Typ CNAME für Systemkomponenten erstellen (siehe folgende Beschreibung).

- Erstellen Sie Hauptdatensätze des Typs A für jede Systemkomponente und für jeden Mandanten, den Sie beim Aktivieren der Mehrmandantenfähigkeit erstellen.
- Erstellen Sie mehrmandantenfähige Datensätze des Typs A für jeden von Ihnen erstellten Mandanten sowie für den Mastermandanten.
- Erstellen Sie mehrmandantenfähige Datensätze des Typs CNAME für jeden von Ihnen erstellten Mandanten mit Ausnahme des Mastermandanten.

Zertifikatsanforderungen für eine Mehrmandantenbereitstellung mit einem Knoten

Sie müssen außerdem zwei SAN-Zertifikate (Subject Alternative Name) erstellen, eines für Workspace ONE Access und eines für vRealize Automation.

- Das vRealize Automation-Zertifikat listet den Hostnamen des vRealize Automation-Servers sowie die Namen der von Ihnen erstellten Mandanten auf.
- Das Workspace ONE Access-Zertifikat listet den Hostnamen des Workspace ONE Access-Servers und die Namen der von Ihnen erstellten Mandanten auf.
- Bei Verwendung von dedizierten SAN-Namen müssen Zertifikate manuell aktualisiert werden, wenn Sie Hosts hinzufügen oder löschen oder einen Hostnamen ändern. Außerdem müssen Sie DNS-Einträge für Mandanten aktualisieren. Als Option zur Vereinfachung der Konfiguration können Sie Platzhalter für die Workspace ONE Access- und vRealize Automation-Zertifikate verwenden. Beispiel: *.example.com und *.vra.example.com.

Hinweis vRealize Automation 8.x unterstützt Platzhalterzertifikate nur für DNS-Namen, die mit den Spezifikationen in der Liste der öffentlichen Suffixe unter <https://publicsuffix.org> übereinstimmen. Beispielsweise ist *.myorg.com ein gültiger Name, wohingegen *.myorg.local ungültig ist.

Beachten Sie, dass Lifecycle Manager keine separaten Zertifikate für jeden Mandanten erstellt. Stattdessen wird ein einzelnes Zertifikat erstellt, in dem der Hostname jedes Mandanten aufgelistet ist. In Basiskonfigurationen wird für den CNAME des Mandanten folgendes Format verwendet: *tenantname.vrahostname.domain*. In Hochverfügbarkeitskonfigurationen wird für den Namen folgendes Format verwendet: *tenantname.vraLBhostname.domain*.

Zusammenfassung

In der folgenden Tabelle werden die DNS- und Zertifikatsanforderungen für eine Workspace ONE Access- und vRealize Automation-Bereitstellung mit einem Knoten zusammengefasst.

DNS-Anforderungen	Anforderungen an SAN-Zertifikate
Main A Type Records lcm.example.local WorkspaceOne.example.local vra.example.local	Workspace One Certificate Hostname: 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 Hostname: vra.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local

Verwalten der Zertifikat- und DNS-Konfiguration unter vRealize Automation-Clusterbereitstellungen

Sie müssen die Zertifikat- und DNS-Konfiguration zwischen allen zutreffenden Komponenten koordinieren, um eine geclusterte vRealize Automation-Bereitstellung mit mehreren Organisationen einzurichten.

In einer typischen geclusterten Konfiguration gibt es drei Workspace ONE Access-Appliances und drei vRealize Automation-Appliances sowie eine einzelne Lifecycle Manager-Appliance.

Diese Konfiguration setzt Clusterbereitstellungen für die folgenden Komponenten voraus:

- Workspace ONE Access Identity Manager-Appliances:
 - idm1.example.local
 - idm2.example.local
 - idm3.example.local
 - idm-lb.example.local
- vRealize Automation-Appliances:
 - vra1.example.local
 - vra2.example.local

- vra3.example.local
- vra-lb.example.local
- Lifecycle Manager-Appliance

DNS-Anforderungen

Sie müssen Datensätze vom Typ „Main A“ sowohl für jede Komponente als auch für jeden der Mandanten erstellen, die Sie beim Aktivieren der Mehrmandantenfähigkeit erstellen. Darüber hinaus müssen Sie mehrmandantenfähige Datensätze des Typs CNAME für jeden erstellten Mandanten außer dem Mastermandanten erstellen. Schließlich müssen Sie auch Datensätze vom Typ „Main A“ für die Workspace ONE Access- und vRealize Automation-Lastausgleichsdienste erstellen.

- Erstellen Sie Datensätze des Typs A für die drei Workspace ONE Access-Appliances und für die vRealize Automation-Appliances, die auf die jeweiligen FQDNs verweisen.
- Erstellen Sie außerdem Datensätze des Typs A für die Workspace ONE Access- und vRealize Automation-Lastausgleichsdienste, die auf die jeweiligen FQDNs verweisen.
- Erstellen Sie mehrmandantenfähige Datensätze des Typs A für den Standardmandanten und für Mandant-1 und Mandant-2, die auf die IP-Adresse des Workspace ONE Access-Lastausgleichsdiensts verweisen.
- Erstellen Sie CNAME-Datensätze für Mandant-1 und Mandant-2, die auf die IP-Adresse des vRealize Automation-Lastausgleichsdiensts verweisen.

Anforderungen für SAN-Zertifikate (Subject Alternative Name)

Sie müssen zwei Workspace ONE Access-Zertifikate erstellen, eines für die Clusteranwendungen und eines für den Lastausgleichsdienst. Erstellen Sie außerdem ein Zertifikat, das für die vRealize Automation-Appliances, die von Ihnen erstellten Mandanten (ausschließlich des Standardmandanten) und den Lastausgleichsdienst gilt.

- Erstellen Sie ein Zertifikat für die Workspace ONE Access-Appliances, das die FQDNs der Workspace ONE Access-Appliances sowie den Standardmandanten und andere von Ihnen erstellte Mandanten auflistet. Dieses Zertifikat muss die IP-Adressen der Workspace ONE Access-Appliances enthalten.
- Erstellen Sie als Best Practice eine SSL-Terminierung auf dem Lastausgleichsdienst. Erstellen Sie zur Unterstützung dieser Terminierung ein Zertifikat für den Workspace ONE Access-Lastausgleichsdienst, das den FQDN des Workspace ONE Access-Lastausgleichsdiensts sowie den Standardmandanten und alle anderen von Ihnen erstellten Mandanten auflistet. Dieses Zertifikat muss die IP-Adresse des Lastausgleichsdiensts enthalten.
- Sie müssen ein Zertifikat für vRealize Automation erstellen, in dem die Hostnamen der drei vRealize Automation-Appliances sowie der dazugehörige Lastausgleichsdienst und die von Ihnen erstellten Mandanten aufgelistet werden. Darüber hinaus müssen die IP-Adressen der drei vRealize Automation-Appliances aufgelistet werden.

- Als Option zur Vereinfachung der Konfiguration können Sie Platzhalter für die Workspace ONE Access- und vRealize Automation-Zertifikate verwenden. Beispiel: *.example.com, *.vra.example.com und *.vra-lb.example.com.

Hinweis vRealize Automation 8.x unterstützt Platzhalterzertifikate nur für DNS-Namen, die mit den Spezifikationen in der Liste der öffentlichen Suffixe unter <https://publicsuffix.org> übereinstimmen. Beispielsweise ist *.myorg.com ein gültiger Name, wohingegen *.myorg.local ungültig ist.

Beachten Sie bei Verwendung einer Workspace ONE Access-Clusterkonfiguration, dass Lifecycle Manager die Zertifikate des Lastausgleichsdiensts nicht aktualisieren kann. Die Zertifikate müssen in diesem Fall manuell aktualisiert werden. Darüber hinaus müssen Produkte oder Dienste, die sich außerhalb von Lifecycle Manager befinden, manuell neu registriert werden.

Zusammenfassung der DNS-Einträge und -Zertifikate für eine Clusterkonfiguration mit mehreren Organisationen

In der folgenden Tabelle werden die DNS- und Zertifikatsanforderungen für eine geclusterte Workspace ONE Access- und vRealize Automation-Bereitstellung mit mehreren Organisationen dargestellt.

DNS-Anforderungen	Anforderungen an SAN-Zertifikate
Main A Type Records lcm.example.local WorkspaceOne-1.example.local WorkspaceOne-2.example.local WorkspaceOne-3.example.local vra.example-1.local vra.example-2.local vra.example-3.local	Workspace One Certificate Hostname: WorkspaceOne.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) Hostname: 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.exmple.local	vRealize Automation Certificate Hostname: vra-1.example.local, vra-2.example.local, vra-3.example.local, vra-lb.example.local, tenant-1.example.local, tenant-2.example.local Für den vRealize Automation-Lastausgleichsdienst ist kein Zertifikat erforderlich, da es SSL Passthrough verwendet.

Anmelden bei Mandanten und Hinzufügen von Benutzern in vRealize Automation

Nachdem Sie Mandanten für vRealize Automation in Lifecycle Manager erstellt haben, können Sie sich bei Workspace ONE Access anmelden, um Ihre Mandanten anzuzeigen und Benutzer hinzuzufügen.

Sie können Mandanten anzeigen, die für eine vRealize Automation-Bereitstellung erstellt wurden, indem Sie sich bei der zugeordneten Workspace ONE Access-Instanz anmelden.

Die zu verwendende URL ist `https://default-tenant_name.domainname.local` bzw. `https://idm.domainname.local` für eine nicht geclusterte Bereitstellung, die Sie zurück zur Standardmandanten-URL für Workspace ONE Access leitet.

Sie können bestimmte Mandanten in Workspace ONE Access mithilfe der folgenden URL validieren: `https://tenant-1.domainname.local`. Mit dieser URL wird eine Seite geöffnet, auf der die Benutzer für den angegebenen Mandanten angezeigt werden. Sie können auf **Benutzer hinzufügen** klicken, um auf Ad-hoc-Basis zusätzliche Benutzer zu erstellen.

Autorisierte Benutzer können sich mithilfe von `https://vra.domainname.local` bei der Hauptanbieterorganisation in vRealize Automation anmelden. Diese Ansicht bietet Zugriff auf alle mit vRealize Automation zusammenhängenden Dienste.

Autorisierte Benutzer können sich bei den entsprechenden Mandanten in vRealize Automation mit `https://tenantname.vra.domainname.local` anmelden.

Weitere Informationen zum Verwalten von Benutzern in Workspace ONE Access finden Sie unter [Verwalten von Benutzern und Gruppen](#) in der Workspace ONE Access-Produktdokumentation.

Hinzufügen von lokalen Benutzern

Sie können lokale Benutzer mithilfe der zugeordneten Workspace ONE Access-Instanz zu Ihrer Bereitstellung hinzufügen. Lokale Benutzer sind Benutzer, die in keinem externen Identitätsanbieter gespeichert sind.

Verwenden von vRealize Orchestrator in vRealize Automation-Bereitstellungen mit mehreren Organisationen

Sie können vRealize Orchestrator mit vRealize Automation-Bereitstellungen mit Mandantenfähigkeit für mehrere Organisationen verwenden.

Der Standardmandant unterstützt die Integration in die vorkonfigurierte eingebettete vRealize Orchestrator-Integration. vRealize Orchestrator steht auf der Seite „Integrationen“ vorkonfiguriert zur Verfügung. Submandanten verfügen nicht über eine vorab registrierte vRealize Orchestrator-Integration. Für sie gibt es jedoch mehrere Optionen zum Hinzufügen von vRealize Orchestrator-Integration.

- Sie können die Integration mit dem eingebetteten vRealize Orchestrator hinzufügen, indem sie zu „Authentifizierungsanbieter konfigurieren“ in vRealize Orchestrator navigieren und die Verbindung über die Hostadresse des jeweiligen vRealize Automation-Mandanten herstellen. Anschließend können sie **Infrastruktur > Verbindungen > Integrationen** auswählen und den eingebetteten vRO als Integration hinzufügen.
- Sie können eine externe vRealize Orchestrator-Instanz hinzufügen, die vRealize Automation mit mehreren Organisationen als Authentifizierungsanbieter verwendet.

Jede vRealize Orchestrator-Instanz, die eine vRealize Automation-Bereitstellung mit mehreren Organisationen als Authentifizierungsanbieter verwendet, kann für jeden der Mandanten registriert werden, indem eine neue Integration erstellt und der vRealize Orchestrator-FQDN ohne Angabe von Anmeldedaten bereitgestellt wird.

Arbeiten mit Protokollen in vRealize Automation

5

Mit den bereitgestellten Befehlszeilendienstprogramm `vracli` können Sie Protokolle in vRealize Automation erstellen und verwenden.

Sie können die Protokolle direkt in vRealize Automation verwenden oder stattdessen alle Protokolle an vRealize Log Insight weiterleiten.

Dieses Kapitel enthält die folgenden Themen:

- [Wie arbeite ich mit Protokollen und Protokollpaketen in vRealize Automation?](#)
- [Vorgehensweise zum Konfigurieren der Protokollweiterleitung zu vRealize Log Insight in vRealize Automation](#)
- [Vorgehensweise zum Erstellen oder Aktualisieren einer Syslog-Integration in vRealize Automation](#)
- [Vorgehensweise zum Arbeiten mit Inhaltspaketen](#)

Wie arbeite ich mit Protokollen und Protokollpaketen in vRealize Automation?

Protokolle werden automatisch von den verschiedenen Diensten generiert. Sie können Protokollpakete in vRealize Automation generieren. Sie können Ihre Umgebung auch so konfigurieren, dass Protokolle automatisch an vRealize Log Insight weitergeleitet werden.

Sie erhalten Informationen zur Nutzung des Befehlszeilendienstprogramms `vracli` zum Generieren von Protokollpaketen, wenn Sie das Argument `--help` in der Befehlszeile von `vracli` verwenden (Beispiel: `vracli log-bundle --help`).

Verwandte Informationen zur Verwendung von vRealize Log Insight finden Sie unter [Vorgehensweise zum Konfigurieren der Protokollweiterleitung zu vRealize Log Insight in vRealize Automation](#).

Protokollpaketbefehle

Sie können ein Protokollpaket erstellen, das alle Protokolle enthält, die von den von Ihnen ausgeführten Diensten generiert werden. Ein Protokollpaket enthält alle Ihre Dienstprotokolle und wird für die Fehlerbehebung benötigt.

Führen Sie in einer geclusterten Umgebung (Hochverfügbarkeitsmodus) den Befehl `vracli log-bundle` auf nur einem Knoten aus. Protokolle werden aus allen Knoten in der Umgebung abgerufen. Bei einem Netzwerkproblem oder einem anderen Clusterproblem werden Protokolle jedoch aus allen Knoten abgerufen, die erreicht werden können. Wenn beispielsweise ein Knoten in einem Cluster mit drei Knoten getrennt ist, werden Protokolle nur von den beiden fehlerfreien Knoten erfasst. Die Ausgabe des Befehls `vracli log-bundle` enthält Informationen zu allen gefundenen Problemen und den Schritten zur Probleumlösung.

- Um ein Protokollpaket zu erstellen, müssen Sie eine SSH-Verbindung zu einem beliebigen Knoten erstellen und folgenden `vracli`-Befehl ausführen:

```
vracli log-bundle
```

- Um den Zeitüberschreitungswert für die Erfassung von Protokollen von den einzelnen Knoten zu ändern, führen Sie den folgenden `vracli`-Befehl aus:

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

Wenn Ihre Umgebung beispielsweise große Protokolldateien enthält, das Netzwerk langsam oder die CPU-Auslastung hoch ist, müssen Sie den Zeitüberschreitungswert möglicherweise auf einen höheren Wert als den Standardwert von 1000 Sekunden festlegen.

- Verwenden Sie zum Konfigurieren anderer Optionen wie z. B. der Zeitüberschreitung für die Assembly und den Pufferspeicherort den folgenden `vracli`-Befehl:

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

Protokollpaketstrukturen

Das Protokollpaket ist eine TAR-Datei mit Zeitstempel. Der Paketname entspricht dem Dateimuster `log-bundle-<Datum>T<Uhrzeit>.tar`, z. B. `log-bundle-20200629T131312.tar`. Ein normales Protokollpaket enthält Protokolle aller Knoten in der Umgebung. Im Falle eines Fehlers enthält es so viele Protokolle wie möglich. Es enthält mindestens die Protokolle des lokalen Knotens.

Das Protokollpaket besteht aus folgendem Inhalt:

- Umgebungsdatei

Die Umgebungsdatei enthält die Ausgabe verschiedener Kubernetes-Wartungsbefehle. Sie liefert Informationen zur aktuellen Ressourcennutzung pro Knoten und pro Pod. Sie enthält außerdem Clusterinformationen und Beschreibungen für alle verfügbaren Kubernetes-Elemente.

- Hostprotokolle und -konfiguration

Die Konfiguration jedes einzelnen Hosts (z. B. sein `/etc`-Verzeichnis) und die hostspezifischen Protokolle (z. B. `journal`) werden in einem Verzeichnis für jeden Clusterknoten oder jeden Host erfasst. Der Name des Verzeichnisses entspricht dem Hostnamen des Knotens. Die internen Inhalte des Verzeichnisses stimmen mit dem Dateisystem des Hosts überein. Die Anzahl der Verzeichnisse entspricht der Anzahl der Clusterknoten.

■ Dienstprotokolle

Protokolle für Kubernetes-Dienste befinden sich in der folgenden Ordnerstruktur:

- `<hostname>/services-logs/<namespace>/<app-name>/file-logs/<container-name>.log`
- `<hostname>/services-logs/<namespace>/<app-name>/console-logs/<container-name>.log`

Ein Beispieldateiname ist `my-host-01/services-logs/prelude/vco-app/file-logs/vco-server-app.log`.

- *hostname* ist der Hostname des Knotens, auf dem der Anwendungscontainer ausgeführt wird oder wurde. In der Regel gibt es eine Instanz für jeden Knoten für jeden Dienst. Beispielsweise 3 Knoten = 3 Instanzen.
- *namespace* ist der Kubernetes-Namespaces, in dem die Anwendung bereitgestellt wird oder wurde. Für benutzerorientierte Dienste ist dieser Wert `prelude`.
- *app-name* ist der Name der Kubernetes-Anwendung, in der die Protokolle erstellt wurden, z. B. `provisioning-service-app`.
- *container-name* ist der Name des Containers, der die Protokolle erstellt hat. Einige Apps bestehen aus mehreren Containern. Beispielsweise enthält `vco-app` die Container `vco-server-app` und `vco-controlcenter-app`.

■ (Veraltet) Pod-Protokolle

Vor den Änderungen an der Protokollierungsarchitektur, die in vRealize Automation 8.2 vorgenommen wurden, befanden sich die Dienstprotokolle (im vorherigen Punkt beschrieben) im Verzeichnis jedes Pods im Protokollpaket. Sie können zwar weiterhin Pod-Protokolle im Paket erstellen, indem Sie die Befehlszeile `vracli log-bundle --include-legacy-pod-logs` verwenden, dies wird jedoch nicht empfohlen, da sich die Protokollinformationen bereits in den Protokollen der einzelnen Dienste befinden. Die Aufnahme von Pod-Protokollen kann die Zeit und den Speicherplatz, die zum Generieren des Protokollpakets erforderlich sind, unnötig erhöhen.

Verstehen der Protokollrotation

Dienstprotokolle liegen zunächst in einem nicht komprimierten Zustand vor. Nach der Verarbeitung der Protokolldaten durch einen vRealize Log Insight-Agent werden die Dienstprotokolle mithilfe eines vRealize Automation `cron`-Jobs komprimiert.

Wenn 70 Prozent der `/var/log`-Festplattenpartition verwendet werden, löscht ein vRealize Automation `cron`-Job die ältesten Dienstprotokolle.

Führen Sie die folgenden `vracli`-Befehle aus, um die Daten der Protokollrotation zu überprüfen.

```
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'
```

Vorgehensweise zum Konfigurieren der Protokollweiterleitung zu vRealize Log Insight in vRealize Automation

Sie können Protokolle von vRealize Automation an vRealize Log Insight weiterleiten, um die Vorteile einer robusteren Protokollanalyse und Berichtsgenerierung zu nutzen.

vRealize Automation ist mit einem [fluentd-basierten](#) Protokollierungsagenten gebündelt. Der Agent sammelt und speichert Protokolle, damit sie in ein Protokollpaket aufgenommen und später untersucht werden können. Sie können den Agenten so konfigurieren, dass er eine Kopie der Protokolle an einen vRealize Log Insight-Server weiterleitet. Verwenden Sie dazu die vRealize Log Insight-REST API. Die API ermöglicht anderen Programmen die Kommunikation mit vRealize Log Insight.

Weitere Informationen über vRealize Log Insight, einschließlich der Dokumentation für die vRealize Log Insight-REST API, finden Sie in der [Dokumentation zu vRealize Log Insight](#).

Konfigurieren Sie den Protokollierungsagenten so, dass er vRealize Automation-Protokolle kontinuierlich an vRealize Log Insight weiterleitet. Verwenden Sie dazu das bereitgestellte Befehlszeilendienstprogramm `vracli`.

Alle Protokollzeilen werden mit einem Hostnamen und einem Umgebungs-Tag gekennzeichnet und können in vRealize Log Insight überprüft werden. In einer Hochverfügbarkeitsumgebung (HA) werden Protokolle je nach dem Knoten, von dem sie stammen, mit verschiedenen Hostnamen gekennzeichnet. Das Umgebungs-Tag kann mithilfe der Option `--environment ENV` konfiguriert werden, die weiter unten im Abschnitt *Konfigurieren oder Aktualisieren der Integration von vRealize Log Insight* beschrieben wird. In einer Hochverfügbarkeitsumgebung (HA) weist das Umgebungs-Tag denselben Wert für alle Protokollzeilen auf. Dabei spielt es keine Rolle, von welchem Knoten die Protokollzeilen stammen.

Sie erhalten Informationen zur Nutzung des Befehlszeilendienstprogramms `vracli`, wenn Sie das Argument `--help` in der Befehlszeile von `vracli` verwenden. Beispiel: `vracli vrli --help`.

Hinweis Sie können nur eine einzelne Remoteprotokollierungsintegration konfigurieren. vRealize Log Insight wird priorisiert, wenn sowohl ein vRealize Log Insight-Server als auch ein Syslog-Server zur Verfügung stehen.

Überprüfen der vorhandenen Konfiguration von vRealize Log Insight

Command

```
vracli vrli
```

Arguments

Es gibt keine Befehlszeilenargumente.

Output

Die aktuelle Konfiguration für die vRealize Log Insight-Integration wird im JSON-Format ausgegeben.

Exit codes

Folgende Exit-Codes sind möglich:

- 0 – Integration mit vRealize Log Insight ist konfiguriert.
- 1 – Im Rahmen der Befehlsausführung ist eine Ausnahme aufgetreten. Sehen Sie sich die Details der Fehlermeldung an.
- 61 (ENODATA) – Integration mit vRealize Log Insight ist nicht konfiguriert. Sehen Sie sich die Details der Fehlermeldung an.

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
}
```

Konfigurieren oder Aktualisieren der Integration von vRealize Log Insight

Command

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

Hinweis Nachdem Sie den Befehl ausgeführt haben, kann es bis zu 2 Minuten dauern, bis der Protokollierungsagent Ihre angegebene Konfiguration anwenden kann.

Arguments

- IP_OR_URL

Gibt die IP- oder URL-Adresse des vRealize Log Insight-Servers an, die zum Senden von Protokollen verwendet werden soll. Standardmäßig werden Port 9543 und HTTPS verwendet. Wenn eine dieser Einstellungen geändert werden muss, können Sie stattdessen eine URL verwenden.

Hinweis Sie können ein anderes Hostschema (Standard ist HTTPS) und einen anderen Port (Standard für HTTPS ist 9543, Standard für HTTP ist 9000) zum Senden der Protokolle verwenden. Siehe hierzu folgende Beispiele:

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

Die Ports 9543 für HTTPS und 9000 für HTTP werden von der vRealize Log Insight-Aufnahme-REST API verwendet, die im Thema *Verwalten von vRealize Log Insight* unter *Ports und externe Schnittstellen* in der [Dokumentation zu vRealize Log Insight](#) beschrieben wird.

■ Optionen

■ --agent-id SOME_ID

Legt die ID des Protokollierungsagenten für diese Appliance fest. Die Standardeinstellung ist 0. Wird verwendet, um den Agent beim Senden von Protokollen an vRealize Log Insight mithilfe der vRealize Log Insight-REST API zu identifizieren.

■ --environment ENV

Legt einen Bezeichner für die aktuelle Umgebung fest. Steht in den vRealize Log Insight-Protokollen als Tag für jeden Protokolleintrag zur Verfügung. Die Standardeinstellung ist `prod`.

■ --ca-file /path/to/server-ca.crt

Gibt eine Datei an, die das Zertifikat der Zertifizierungsstelle enthält, die zum Signieren des Zertifikats des vRealize Log Insight-Servers verwendet wurde. Dadurch wird erzwungen, dass der Protokollierungsagent der angegebenen Zertifizierungsstelle vertraut, und er wird befähigt, das Zertifikat des vRealize Log Insight-Servers zu überprüfen, wenn es von einer nicht vertrauenswürdigen Zertifizierungsstelle signiert wurde. Die Datei kann eine ganze Zertifikatskette enthalten, wenn dies zur Verifizierung des Zertifikats erforderlich ist. Übergeben Sie im Falle eines selbstsignierten Zertifikats das Zertifikat selbst.

■ --ca-cert CA_CERT

Die Definition ist identisch mit der von `--ca-file` oben, aber stattdessen wird das Zertifikat (die Kette) inline als Zeichenfolge übergeben.

■ --insecure

Deaktiviert SSL-Überprüfung des Serverzertifikats. Zwingt den Protokollierungsagenten, beim Senden von Protokollen ein beliebiges SSL-Zertifikat zu akzeptieren.

■ Erweiterte Optionen

■ --request-max-size BYTES

Mehrere Protokollereignisse werden mit einem einzelnen API-Aufruf aufgenommen. Mit diesem Argument wird die maximale Nutzlastgröße in Byte für jede Anforderung gesteuert. Gültige Werte liegen zwischen 4000 und 4000000. Der Standardwert ist 256000. Verwandte Informationen zu zulässigen Werten finden Sie unter vRealize Log Insight-Ereignisaufnahme in der Dokumentation zur vRealize Log Insight-REST API. Wenn Sie diesen Wert zu niedrig festlegen, können Protokollierungsereignisse, die größer als die zulässige Größe sind, gelöscht werden.

■ --request-timeout SECONDS

Ein Aufruf an die API kann aus mehreren Gründen hängen, darunter Probleme mit der Remoteumgebung, Netzwerkprobleme usw. Dieser Parameter steuert, wie viele Sekunden auf den Abschluss jedes Vorgangs gewartet wird, z. B. das Öffnen einer Verbindung, das Schreiben von Daten oder das Warten auf eine Antwort, bevor der Aufruf als fehlgeschlagen erkannt wird. Der Wert darf nicht kleiner als 1 Sekunde sein. Die Standardeinstellung ist 30.

■ --request-immediate-retries RETRIES

Protokolle werden in aggregierten Blöcken gepuffert, bevor sie an vRealize Log Insight gesendet werden (siehe --buffer-flush-thread-count unten). Falls eine API-Anforderung fehlschlägt, wird das Protokoll sofort wiederholt. Die Standardanzahl der sofortigen Wiederholungen ist 3. Wenn keine der Wiederholungen erfolgreich ist, wird der gesamte Protokollblock zurückgesetzt und der Vorgang zu einem späteren Zeitpunkt wiederholt.

■ --request-http-compress

Zum Verringern des Netzwerkdatenverkehrsvolumens können Sie GZIP-Komprimierung auf Anforderungen anwenden, die an den vRealize Log Insight-Server gesendet werden. Bei Nichtangabe dieses Parameters wird keine Komprimierung verwendet.

■ --buffer-flush-thread-count THREADS

Zur besseren Leistung und zum Beschränken des Netzwerkdatenverkehrs werden die Protokolle lokal in Blöcken gepuffert, bevor sie geleert und an den Protokollserver gesendet werden. Jeder Block enthält Protokolle von einem einzelnen Dienst. Abhängig von Ihrer Umgebung können Blöcke sehr groß und ihre Leerung zeitaufwändig sein. Dieses Argument steuert, wie viele Blöcke gleichzeitig geleert werden können. Die Standardeinstellung ist 2.

Hinweis Wenn beim Konfigurieren der Integration über HTTPS der vRealize Log Insight-Server so konfiguriert ist, dass er ein nicht vertrauenswürdiges Zertifikat (z. B. ein selbstsigniertes Zertifikat oder ein Zertifikat, das von einer nicht vertrauenswürdigen Zertifizierungsstelle signiert wurde) verwendet, müssen Sie eine der Optionen `--ca-file`, `--ca-cert` oder `--insecure` verwenden. Andernfalls kann der Protokollierungsagent die Serveridentität nicht validieren und keine Protokolle senden. Wenn Sie `--ca-file` oder `--ca-cert` verwenden, muss das vRealize Log Insight-Serverzertifikat für den Hostnamen des Servers gültig sein. Überprüfen Sie in allen Fällen die Integration, indem Sie einige Minuten für die Verarbeitung abwarten und dann prüfen, ob vRealize Log Insight die Protokolle empfangen hat.

Output

Es wird keine Ausgabe erwartet.

Exit codes

Folgende Exit-Codes sind möglich:

- 0 – Die Konfiguration wurde aktualisiert.
- 1 – Im Rahmen der Ausführung ist eine Ausnahme aufgetreten. Sehen Sie sich die Details der Fehlermeldung an.

Examples – Configure or update integration configuration

Die folgenden Beispielanweisungen werden in separaten Befehlszeilen angezeigt. Die Argumente können jedoch in einer einzelnen Befehlszeile kombiniert werden. Sie können beispielsweise mehrere Argumente einschließen, wenn Sie `vracli vrli set {somehost}` oder `vracli vrli set --ca-file path/to/server-ca.crt` zum Ändern der Standardwerte für die Agent-ID oder die Umgebung verwenden. Weitere Informationen finden Sie in der Onlinebefehlshilfe unter `vracli vrli --help`.

```
$ 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
```

Löschen der Integration von vRealize Log Insight

Command

```
vracli vrli unset
```

Hinweis Nachdem Sie den Befehl ausgeführt haben, kann es bis zu 2 Minuten dauern, bis der Protokollierungsagent Ihre angegebene Konfiguration anwenden kann.

Arguments

Es gibt keine Befehlszeilenargumente.

Output

Die Bestätigung wird im reinen Textformat ausgegeben.

Exit codes

Folgende Exit-Codes sind verfügbar:

- 0 – Die Konfiguration wurde gelöscht oder es war keine Konfiguration vorhanden.
- 1 – Im Rahmen der Ausführung ist eine Ausnahme aufgetreten. Sehen Sie sich die Details der Fehlermeldung an.

Examples - Clear integration

```
$ vracli vrli unset
Clearing vRLI integration configuration

$ vracli vrli unset
No vRLI integration configured
```

Vorgehensweise zum Erstellen oder Aktualisieren einer Syslog-Integration in vRealize Automation

Sie können vRealize Automation so konfigurieren, dass Ihre Protokollierungsinformationen an Remote-Syslog-Server gesendet werden.

Der Befehl `vracli remote-syslog set` wird verwendet, um eine Syslog-Integration zu erstellen oder vorhandene Integrationen zu überschreiben.

vRealize Automation-Remote-Syslog-Integration unterstützt die folgenden Verbindungstypen:

- Über UDP.
- Über TCP ohne TLS.

Hinweis Zum Erstellen einer Syslog-Integration ohne TLS fügen Sie das Flag `--disable-ssl` zum Befehl `vracli remote-syslog set` hinzu.

- Über TCP mit TLS.

Hinweis Sie können nur eine einzelne Remoteprotokollierungsintegration konfigurieren. vRealize Log Insight wird priorisiert, wenn sowohl ein vRealize Log Insight-Server und ein Syslog-Server zur Verfügung stehen.

Informationen zum Konfigurieren der Protokollierungsintegration mit vRealize Log Insight finden Sie unter [Vorgehensweise zum Konfigurieren der Protokollweiterleitung zu vRealize Log Insight in vRealize Automation](#).

Voraussetzungen

Konfigurieren Sie einen Remote-Syslog-Server.

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Automation-Appliance als **root** an.
- 2 Führen Sie zum Erstellen einer Integration mit einem Syslog-Server den Befehl `vracli remote-syslog set` aus.

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

Hinweis Wenn Sie im Befehl `vracli remote-syslog set` keinen Port eingeben, wird der Standardwert 514 für den Port angenommen.

Hinweis Sie können ein Zertifikat zur Syslog-Konfiguration hinzufügen. Verwenden Sie das Flag `--ca-file`, um eine Zertifikatsdatei hinzuzufügen. Verwenden Sie das Flag `--ca-cert`, um ein Zertifikat als Klartext hinzuzufügen.

- 3 (Optional) Zum Überschreiben einer vorhandenen Syslog-Integration führen Sie `vracli remote-syslog set` aus und setzen den Wert des `-id`-Flags auf den Namen der zu überschreibenden Integration.

Hinweis Standardmäßig werden Sie von der vRealize Automation-Appliance aufgefordert, die Überschreibung der Syslog-Integration zu bestätigen. Zum Überspringen der Bestätigungsanforderung fügen Sie das Flag `-f` oder `--force` zum Befehl `vracli remote-syslog set` hinzu.

Nächste Schritte

Zur Anzeige der aktuellen Syslog-Integrationen in der Appliance führen Sie den Befehl `vracli remote-syslog` aus.

Vorgehensweise zum Löschen einer Syslog-Integration für die Protokollierung in vRealize Automation

Sie können Syslog-Integrationen aus Ihrer vRealize Automation-Appliance löschen, indem Sie den Befehl `vracli remote-syslog unset` ausführen.

Voraussetzungen

Erstellen Sie eine oder mehrere Syslog-Integrationen in der vRealize Automation-Appliance. Weitere Informationen finden Sie unter [Vorgehensweise zum Erstellen oder Aktualisieren einer Syslog-Integration in vRealize Automation](#).

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Automation-Appliance als **Root**-Benutzer an.
- 2 Löschen Sie mithilfe einer der folgenden Methoden Syslog-Integrationen aus der vRealize Automation-Appliance:
 - Zum Löschen einer bestimmten Syslog-Integration führen Sie den Befehl `vracli remote-syslog unset -id Integration_name` aus.
 - Zum Löschen aller Syslog-Integrationen in der vRealize Automation-Appliance führen Sie den Befehl `vracli remote-syslog unset` ohne das Flag `-id` aus.

Hinweis Standardmäßig werden Sie von der vRealize Automation-Appliance aufgefordert, das Löschen aller Syslog-Integrationen zu bestätigen. Zum Überspringen der Bestätigungsanforderung fügen Sie das Flag `-f` oder `--force` zum Befehl `vracli remote-syslog unset` hinzu.

Vorgehensweise zum Arbeiten mit Inhaltspaketen

Inhaltspakete werden in Log Insight gehostet und enthalten Dashboards, extrahierte Felder, gespeicherte Abfragen und Warnungen, die sich auf ein bestimmtes Produkt oder auf eine Gruppe von Protokollen beziehen. Sie können von der Community unterstützte Inhaltspakete über VMware Sample Exchange und andere Inhaltspakete über das Download-Center für Inhaltspakete installieren.

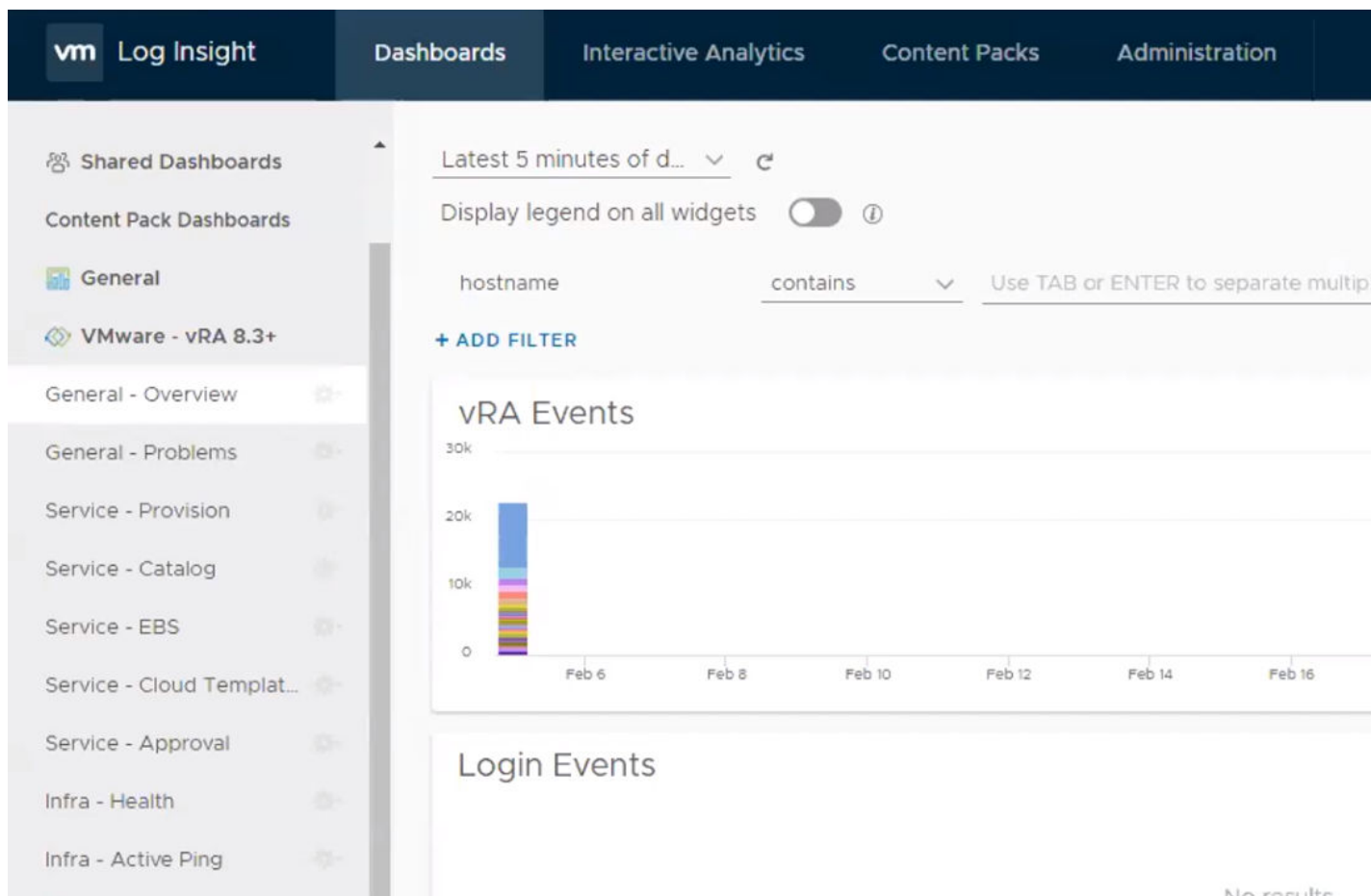
VMware vRealize Log Insight stellt automatisierte Protokollverwaltung mittels Zusammenfassungen, Analysen und Suchvorgängen bereit und ermöglicht auf diese Weise die Bereitstellung operativer Informationen und unternehmensweiter Transparenz in dynamischen Hybrid Cloud-Umgebungen. Bei Inhaltspaketen handelt es sich um Plug-Ins in VMware vRealize Log Insight, die vordefinierte Informationen zu bestimmten Ereignistypen bereitstellen, wie z. B. Protokollmeldungen.

Zum Herunterladen eines Inhaltspakets navigieren Sie über Log Insight zu **Inhaltspakete > Marketplace**. Sie können Inhaltspakete auch importieren, indem Sie auf **+ Inhaltspaket importieren** klicken.

vRA 8.x-Inhaltspaket

Das VMware vRealize Automation-Inhaltspaket enthält eine konsolidierte Zusammenfassung der Protokollereignisse für alle vRA-Umgebungskomponenten. Das Inhaltspaket umfasst mehrere Dashboards, in denen ein allgemeiner Überblick, Einblicke in Fehler und Vorgänge sowie der allgemeine Systemzustand der vRA-Instanz zur Verfügung gestellt werden. Diese Dashboards werden auf der Registerkarte **Dashboard** zusammen mit allen anderen Log Insight-Dashboards aufgeführt. Nach dem Laden kann es bis zu 30 Sekunden dauern, bis die Dashboards mit Metriken befüllt werden.

Hinweis Ein Upgrade vom vRA 7.5+-Inhaltspaket auf das vRA 8.3-Inhaltspaket ist nicht möglich. Sie müssen das vRA 8.3-Inhaltspaket installieren. Nach der Installation werden das 8.3- und das 7.5-Inhaltspaket getrennt ausgeführt.



Das vRealize Automation-Inhaltspaket enthält die folgenden Dashboards:

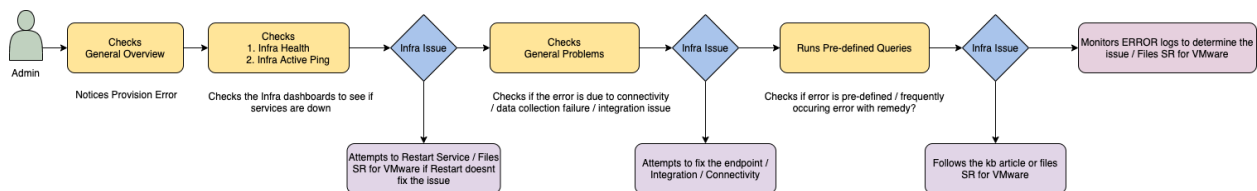
- Allgemein – Übersicht: Erfasst eine Übersicht über allgemeine Metriken für vRA.
- Allgemein – Probleme:
- Dienst – Bereitstellung: Erfasst Probleme im Zusammenhang mit dem Bereitstellungsdienst.
- Dienst – Katalog: Erfasst Probleme im Zusammenhang mit dem Katalogdienst.

- Dienst – EBS: Erfasst Probleme im Zusammenhang mit dem Ereignisbrokerdienst.
- Dienst – Cloud-Vorlagen: Erfasst Fehler und Metriken im Zusammenhang mit Cloud Assembly Cloud-Vorlagen, benutzerdefinierten Ressourcen und Ressourcenaktionen.
- Dienst – Genehmigung: Erfasst Fehler und Metriken im Zusammenhang mit Genehmigungen.
- Infrastruktur – Integrität: Erfasst, wenn Pods im Laufe der Zeit neu gestartet werden. Dieses Dashboard spielt bei der Erkennung von Ausfällen aufgrund von Ressourcengrenzwerten eine wichtige Rolle.
- Infrastruktur – Aktiver Ping: Erfasst die URL der Integritätsprüfung im Laufe der Zeit.

Jedes Dashboard enthält einzelne Widgets mit gezielten Analysen. Zum Anzeigen des in jedem

Widget durchgeführten Analysetyps klicken Sie auf das Informationssymbol .

Als vRealize Automation-Administrator können Sie diesen allgemeinen Workflow für Inhaltspakete verwenden, um Fehler zu erkennen und zu beheben.



Weitere Informationen zum vRealize Automation 8.3-Inhaltspaket finden Sie unter [vRealize Automation 8.3+ Log Insight-Inhaltspaket](#) und [Vorgehensweise zum Konfigurieren von Protokollweiterleitung für vRealize Log Insight](#).

Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) für vRealize Automation

6

Dieses Produkt nimmt am Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) von VMware teil. Mit dem CEIP werden Informationen für VMware bereitgestellt, mit denen es VMware ermöglicht wird seine Produkte und Dienste zu verbessern, Probleme zu beheben und Benutzern Hinweise zur optimalen Bereitstellung und Verwendung unserer Produkte zu geben.

Einzelheiten zu den im Rahmen des CEIP erfassten Daten sowie zum Zweck der Verwendung durch VMware können im Trust & Assurance Center unter <http://www.vmware.com/trustvmware/ceip.html> eingesehen werden.

Dieses Kapitel enthält die folgenden Themen:

- Wie nehme ich am Programm zur Verbesserung der Kundenzufriedenheit (Customer Experience Improvement Program) für vRealize Automation teil bzw. wie beende ich die Teilnahme?
- Wie konfiguriere ich die Datenerfassungszeit für das Programm zur Verbesserung der Benutzerfreundlichkeit für vRealize Automation?

Wie nehme ich am Programm zur Verbesserung der Kundenzufriedenheit (Customer Experience Improvement Program) für vRealize Automation teil bzw. wie beende ich die Teilnahme?

Über die Befehlszeile der vRealize Automation-Appliance können Sie dem Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) beitreten oder es verlassen.

Sie können dem CEIP-Programm bei der Installation von vRealize Automation und mit dem vRealize Lifecycle Manager (LCM) beitreten. Sie können dem Programm auch nach der Installation mithilfe von Befehlszeilenoptionen beitreten oder es verlassen.

So treten Sie dem Programm zur Verbesserung der Benutzerfreundlichkeit mithilfe von Befehlszeilenoptionen bei:

- 1 Melden Sie sich bei der Befehlszeile der vRealize Automation-Appliance als **Root**-Benutzer an.

- 2 Führen Sie den Befehl `vracli ceip on` aus.
- 3 Überprüfen Sie die Informationen des Programms zur Verbesserung der Benutzerfreundlichkeit und führen Sie den Befehl `vracli ceip on --acknowledge-ceip` aus.
- 4 Um die vRealize Automation-Dienste neu zu starten, führen Sie den Befehl `/opt/scripts/deploy.sh` aus.

So verlassen Sie das Programm zur Verbesserung der Benutzerfreundlichkeit mithilfe von Befehlszeilenoptionen:

- 1 Melden Sie sich bei der Befehlszeile der vRealize Automation-Appliance als **Root**-Benutzer an.
- 2 Führen Sie den Befehl `vracli ceip off` aus.
- 3 Um die vRealize Automation-Dienste neu zu starten, führen Sie den Befehl `/opt/scripts/deploy.sh` aus.

Wie konfiguriere ich die Datenerfassungszeit für das Programm zur Verbesserung der Benutzerfreundlichkeit für vRealize Automation?

Sie können den Tag und die Uhrzeit festlegen, an dem bzw. zu der das Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) Daten an VMware sendet.

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Automation-Appliance als **Root**-Benutzer an.
- 2 Öffnen Sie die folgende Datei in einem Texteditor.
`/etc/telemetry/telemetry-collector-vami.properties`
- 3 Bearbeiten Sie die Eigenschaften für den Wochentag (dow, day-of-week) und die Wochenstunde (hod, hour-of-day).

Eigenschaft	Beschreibung
<code>frequency.dow=<day-of-week></code>	Tag, an dem die Datenerfassung stattfindet.
<code>frequency.hod=<hour-of-day></code>	Lokale Uhrzeit des Tages, an dem die Datenerfassung stattfindet. Mögliche Werte sind 0 bis 23.

- 4 Speichern und schließen Sie `telemetry-collector-vami.properties`.
- 5 Wenden Sie die Einstellung an, indem Sie den folgenden Befehl eingeben.

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

Die Änderungen werden auf alle Knoten in Ihrer Bereitstellung angewendet.