

Installieren und Konfigurieren von VMware vRealize Orchestrator

Februar 2022

vRealize Orchestrator 8.7

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 © 2008-2022 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

Installieren und Konfigurieren von VMware vRealize Orchestrator 6

1 Einführung in VMware vRealize Orchestrator 7

Schlüsselfunktionen der Orchestrator-Plattform 7

vRealize Orchestrator-Benutzerrollen 10

Architektur von vRealize Orchestrator 11

vRealize Orchestrator Plug-ins 12

2 Systemvoraussetzungen für vRealize Orchestrator 13

Standardkomponenten der Appliance 13

Hardwareanforderungen 14

Maximalwerte für die Skalierbarkeit 14

Netzwerkanforderungen 15

Ports und Endpoints 15

Browser-Unterstützung 15

Unterstützung der Internationalisierung 16

3 Einrichten von vRealize Orchestrator-Komponenten 17

Einrichtung von vCenter Server 17

Authentifizierungsmethoden 18

4 Installieren von vRealize Orchestrator 19

Herunterladen und Bereitstellen der vRealize Orchestrator Appliance 19

Schalten Sie die vRealize Orchestrator Appliance ein und öffnen Sie die Startseite 22

Aktivieren oder Deaktivieren des SSH-Zugriffs auf die vRealize Orchestrator Appliance 22

5 Erstkonfiguration 23

Konfigurieren eines eigenständigen vRealize Orchestrator-Servers 23

Konfigurieren eines eigenständigen vRealize Orchestrator-Servers mit vRealize Automation-Authentifizierung 23

Konfigurieren eines eigenständigen vRealize Orchestrator-Servers mit vSphere-Authentifizierung 25

Aktivieren von vRealize Orchestrator-Funktionen mit Lizenzen 27

vRealize Orchestrator-Datenbankverbindung 28

Zertifikate verwalten 28

Verwalten von vRealize Orchestrator-Zertifikaten 29

Generieren eines benutzerdefinierten TLS-Zertifikats für vRealize Orchestrator 29

Festlegen eines benutzerdefinierten TLS-Zertifikats für vRealize Orchestrator 31

| | |
|---|-----------|
| Importieren eines vertrauenswürdigen Zertifikats über Control Center | 33 |
| Konfigurieren des vRealize Orchestrator-Plug-Ins | 33 |
| Verwalten von vRealize Orchestrator-Plug-Ins | 34 |
| Installieren oder Aktualisieren eines vRealize Orchestrator-Plug-Ins | 34 |
| Löschen eines Plug-Ins | 35 |
| vRealize Orchestrator-Hochverfügbarkeit | 35 |
| Maximalwerte für die Skalierbarkeit | 36 |
| Konfigurieren eines vRealize Orchestrator-Clusters | 36 |
| Entfernen eines vRealize Orchestrator-Clusterknotens | 38 |
| Horizontales Skalieren einer eigenständigen vRealize Orchestrator-Bereitstellung | 39 |
| Überwachen eines vRealize Orchestrator-Clusters | 40 |
| Konfigurieren des Programms zur Verbesserung der Benutzerfreundlichkeit | 41 |
| Kategorien von Daten, die VMware erhält | 41 |
| Teilnehmen am Programm zur Verbesserung der Benutzerfreundlichkeit bzw. Verlassen des Programms | 41 |
| 6 Verwenden der vRealize Orchestrator-API-Dienste | 43 |
| Verwalten von SSL-Zertifikaten über die REST-API | 43 |
| Löschen eines TLS-Zertifikats mithilfe der REST-API | 44 |
| Importieren von TLS-Zertifikaten mithilfe der REST-API | 44 |
| Erstellen eines Keystore mithilfe der REST-API | 46 |
| Löschen eines Keystore mithilfe der REST-API | 46 |
| Hinzufügen eines Schlüssels mithilfe der REST-API | 47 |
| 7 Zusätzliche Konfigurationsoptionen | 48 |
| Neukonfigurieren der Authentifizierung | 48 |
| Ändern des Authentifizierungsanbieters | 48 |
| Ändern der Authentifizierungsparameter | 49 |
| Konfigurieren der Workflow-Ausführungseigenschaften | 49 |
| vRealize Orchestrator-Protokolldateien | 50 |
| Protokollierungspersistenz | 50 |
| Konfiguration der vRealize Orchestrator-Protokolle | 51 |
| Konfigurieren der Protokollierungsintegration mit vRealize Log Insight | 52 |
| Erstellen oder überschreiben einer Syslog-Integration in vRealize Orchestrator | 52 |
| Löschen einer Syslog-Integration in vRealize Orchestrator | 54 |
| Aktivieren der Debug-Protokollierung für Kerberos | 54 |
| Aktivieren der Opentracing- und Wavefront-Erweiterungen | 55 |
| Konfigurieren der Opentracing-Erweiterung | 56 |
| Konfigurieren der Wavefront-Erweiterung | 57 |
| Aktivieren der Uhrzeitsynchronisierung für vRealize Orchestrator | 58 |
| Deaktivieren der Uhrzeitsynchronisierung für vRealize Orchestrator | 59 |
| Konfigurieren von vRealize Orchestrator-Kubernetes-CIDR | 60 |

Aktualisieren der DNS-Einstellungen für vRealize Orchestrator 61

8 Anwendungsbeispiele für die Konfiguration und Fehlerbehebung 63

Überprüfen der Build-Nummer des vRealize Orchestrator-Servers 63

Konfigurieren des vRealize Orchestrator-Plug-Ins für vSphere Web Client 64

Abbrechen laufender Workflows 65

Aktivieren des vRealize Orchestrator-Server-Debuggings 65

Ändern der Größe der vRealize Orchestrator Appliance-Festplatten 67

Skalieren der Heap-Arbeitsspeichergröße des vRealize Orchestrator-Servers 69

Notfallwiederherstellung von vRealize Orchestrator mithilfe von Site Recovery Manager 70

Konfigurieren virtueller Maschinen für vSphere Replication 70

Erstellen von Schutzgruppen 71

Erstellen eines Wiederherstellungsplans 74

Organisieren von Wiederherstellungsplänen in Ordnern 75

Bearbeiten eines Wiederherstellungsplans 75

9 Festlegen von Systemeigenschaften 77

Festlegen des Dateisystemzugriffs auf dem Server für Workflows und Aktionen 77

Regeln in der Datei js-io-rights.conf, die Schreibzugriff auf das vRealize Orchestrator-System ermöglichen 77

Festlegen des Dateisystemzugriffs auf dem Server für Workflows und Aktionen 78

Festlegen des Zugriffs auf Betriebssystembefehle für Workflow und Aktionen 79

Setzen von JavaScript-Zugriff auf Java-Klassen 80

Festlegen der Eigenschaft für benutzerdefinierte Zeitüberschreitung 81

Hinzufügen eines JDBC-Connectors für das vRealize Orchestrator-SQL-Plug-In 82

Festlegen einer Eigenschaft für die Verlängerung von Authentifizierungstoken in geplanten Aufgaben oder Richtlinien 83

10 Weitere Schritte 85

Installieren und Konfigurieren von VMware vRealize Orchestrator

Installieren und Konfigurieren von VMware vRealize Orchestrator bietet Informationen und Anleitungen zur Installation und Konfiguration von VMware[®] vRealize Orchestrator.

Zielgruppe

Diese Informationen sind für erfahrene vSphere-Administratoren und Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und den Vorgängen von Datencentern vertraut sind.

Einführung in VMware vRealize Orchestrator

1

VMware vRealize Orchestrator ist eine Entwicklungs- und Prozessautomatisierungsplattform, die eine Bibliothek mit erweiterbaren Workflows bereitstellt, damit Sie automatisierte, konfigurierbare Prozesse erstellen und ausführen können, mit denen VMware-Produkte sowie andere Technologien von Drittanbietern verwaltet werden.

vRealize Orchestrator automatisiert Verwaltungs- und Betriebsaufgaben sowohl von VMware als auch von Drittanbieteranwendungen wie Service-Desks, Change-Management-Systeme und IT-Ressourcenmanagementsysteme.

Dieses Kapitel enthält die folgenden Themen:

- [Schlüsselfunktionen der Orchestrator-Plattform](#)
- [vRealize Orchestrator-Benutzerrollen](#)
- [Architektur von vRealize Orchestrator](#)
- [vRealize Orchestrator Plug-ins](#)

Schlüsselfunktionen der Orchestrator-Plattform

vRealize Orchestrator besteht aus drei Ebenen, der Orchestrierungsplattform mit gemeinsamen Funktionen, die für ein Orchestrierungswerkzeug erforderlich sind, einer Plug-In-Architektur zur Steuerung von Subsystemen und einer Bibliothek von Workflows. vRealize Orchestrator ist eine offene Plattform, die mit neuen Plug-Ins und Inhalten erweitert und über eine REST-API in eine größere Architektur integriert werden kann.

vRealize Orchestrator enthält mehrere wichtige Funktionen, die bei der Ausführung und Verwaltung von Workflows hilfreich sind.

Persistenz

Relevante Informationen wie etwa Prozesse, Workflow-Status und die vRealize Orchestrator-Konfiguration werden in einer PostgreSQL-Produktionsdatenbank gespeichert.

Zentrale Verwaltung

vRealize Orchestrator bietet eine zentrale Möglichkeit zur Verwaltung Ihrer Prozesse. Die auf einem Anwendungsserver basierende Plattform mit umfassendem Versionsverlauf kann Skripte und prozessbezogene Primitive an demselben Speicherort speichern. Damit

vermeiden Sie, dass Skripte ohne Versionierung und korrekte Änderungskontrolle auf Ihren Servern liegen.

Checkpointerstellung

Jeder Schritt eines Workflows wird in der Datenbank gespeichert, wodurch Datenverlust vermieden wird, wenn Sie den Server neu starten müssen. Diese Funktion ist vor allem bei Prozessen mit langer Ausführungsdauer sinnvoll.

Control Center

Bei Control Center handelt es sich um ein webbasiertes Portal, das die administrative Effizienz von vRealize Orchestrator-Instanzen erhöht, indem eine zentrale administrative Schnittstelle für Laufzeitvorgänge, Überwachung von Workflows sowie Korrelation zwischen der Workflow-Ausführung und Systemressourcen bereitgestellt wird.

Versionierung

Alle Objekte der vRealize Orchestrator-Plattform haben einen ihnen zugewiesenen Versionsverlauf. Der Versionsverlauf ist für ein einfaches Änderungsmanagement sinnvoll, wenn Prozesse an Projektphasen oder Standorte verteilt werden.

Git-Integration

Mit dem vRealize Orchestrator Client können Sie ein Git-Repository integrieren, um die Versions- und Quellcodeverwaltung Ihrer vRealize Orchestrator-Inhalte weiter zu verbessern. Mit Git können Sie die Workflow-Entwicklung über mehrere vRealize Orchestrator-Instanzen hinweg verwalten. Weitere Informationen finden Sie unter *Verwenden von Git mit dem vRealize Orchestrator-Client* im Handbuch *Verwenden des VMware vRealize Orchestrator Client*.

Skripterstellungseengine

Die Mozilla Rhino JavaScript-Engine bietet eine Möglichkeit, Bausteine für die vRealize Orchestrator Client-Plattform zu erstellen. Die Skripterstellungseengine wurde durch eine einfache Versionskontrolle, die Prüfung von Variablentypen, die Verwaltung von Namespaces und die Verarbeitung von Ausnahmen ergänzt. Die Engine kann in den folgenden Bausteinen eingesetzt werden:

- Aktionen
- Workflows
- Richtlinien

Workflowengine

Mit der Workflowengine können Sie Geschäftsprozesse automatisieren. Sie verwendet folgende Objekte, um eine schrittweise Prozessautomation in Workflows zu erstellen:

- Workflows und Aktionen, die von vRealize Orchestrator Client bereitgestellt werden
- Benutzerdefinierte Bausteine, die vom Kunden erstellt werden

- Objekte, die vRealize Orchestrator Client von Plug-Ins hinzugefügt werden

Benutzer, andere Workflows, Zeitpläne oder Richtlinien können Workflows starten.

Richtlinienengine

Sie können die Richtlinienengine zur Überwachung und Generierung von Ereignissen verwenden, mit denen auf veränderte Bedingungen im vRealize Orchestrator Client-Server oder in der mit Plug-Ins integrierten Technologie reagiert wird. Richtlinien können Ereignisse aus der Plattform oder den Plug-Ins sammeln, sodass Sie veränderte Bedingungen in jeder der integrierten Technologien verarbeiten können.

vRealize Orchestrator Client

Nehmen Sie die Erstellung, Ausführung, Bearbeitung und Überwachung von Workflows mit dem vRealize Orchestrator Client vor. Sie können den vRealize Orchestrator Client auch verwenden, um Aktions-, Konfigurations-, Richtlinien- und Ressourcenelemente zu verwalten. Weitere Informationen finden Sie unter *Verwenden des vRealize Orchestrator-Client*.

Entwicklung und Ressourcen

Die vRealize Orchestrator-Zielseite bietet schnellen Zugriff auf Ressourcen, die Sie bei der Entwicklung Ihrer eigenen Plug-Ins für die Verwendung in vRealize Orchestrator unterstützen. Darüber hinaus finden Sie dort Informationen zur Verwendung der vRealize Orchestrator-REST-API für das Senden von Anforderungen an den vRealize Orchestrator-Server.

Sicherheit

vRealize Orchestrator stellt die folgenden erweiterten Sicherheitsfunktionen bereit:

- Public Key Infrastructure (PKI) zum Signieren und Verschlüsseln von Inhalten, die zwischen Servern importiert und exportiert werden
- Digital Rights Management (DRM), um zu kontrollieren, wie exportierte Inhalte angezeigt, bearbeitet und weiterverteilt werden
- Transport Layer Security (TLS), um eine verschlüsselte Kommunikation zwischen dem vRealize Orchestrator Client, dem vRealize Orchestrator-Server und dem HTTPS-Zugriff auf das Web-Front-End bereitzustellen
- Erweitertes Management von Zugriffsrechten zur Kontrolle über den Zugriff auf Prozesse und die von diesen Prozessen manipulierten Objekte

Verschlüsselung

vRealize Orchestrator verwendet einen FIPS-kompatiblen erweiterten Verschlüsselungsstandard (Advanced Encryption Standard, AES) mit einem 256-Bit-Chiffreschlüssel für die Verschlüsselung von Zeichenfolgen. Der Chiffreschlüssel wird zufällig generiert und ist in allen Appliances, die nicht Teil eines Clusters sind, eindeutig. Alle Knoten in einem Cluster nutzen einen Chiffreschlüssel gemeinsam.

vRealize Orchestrator-Benutzerrollen

vRealize Orchestrator stellt verschiedene Tools und Schnittstellen basierend auf den spezifischen Verantwortungen der globalen Benutzerrollen bereit. In vRealize Orchestrator können Sie Benutzer mit vollständigen Rechten haben, die Teil der Administratorgruppe (**Administratoren**), Entwickler, (**Workflow-Designer**), Fehlerbehebungsbenutzer (**Viewer**) und Benutzer mit eingeschränktem Zugriff sind.

vRealize Orchestrator-Benutzerrollen werden im Menü **Rollenverwaltung** des vRealize Orchestrator Client verwaltet. Weitere Informationen zum Konfigurieren von Benutzerrollen im vRealize Orchestrator Client finden Sie unter *Zuweisen von Rollen im vRealize Orchestrator-Client* im Handbuch *Verwenden des VMware vRealize Orchestrator Client*.

Hinweis Für vRealize Orchestrator-Bereitstellungen, die mit vRealize Automation authentifiziert wurden oder eine vRealize Automation-Lizenz verwenden, werden Benutzerrollen dem Identitäts- und Zugriffsverwaltungsdienst der vRealize Automation-Plattform zugewiesen. Weitere Informationen finden Sie unter *Konfigurieren von vRealize Orchestrator Client-Rollen in vRealize Automation* in *Verwenden des VMware vRealize Orchestrator Client*.

| Benutzerrolle | Beschreibung |
|---------------|---|
| Administrator | <p>Dieser Benutzer hat unbeschränkten Zugriff auf alle Funktionen und Inhalte der vRealize Orchestrator-Plattform, einschließlich von bestimmten Gruppen erstellter Inhalte. Zu den wichtigsten Aufgaben des Administrators gehören:</p> <ul style="list-style-type: none"> ■ Installieren und Konfigurieren von vRealize Orchestrator. ■ Hinzufügen von Benutzern zu vRealize Orchestrator Client, Zuweisen von Rollen sowie Erstellen und Löschen von Gruppen. Weitere Informationen finden Sie unter <i>Erstellen von Gruppen im vRealize Orchestrator Client</i> in <i>Verwenden des VMware vRealize Orchestrator Client</i>. ■ Erstellen einer Integration mit einem Git-Repository für die Entwickler in deren vRealize Orchestrator-Umgebung. Weitere Informationen finden Sie unter <i>Konfigurieren einer Verbindung mit einem Git-Repository</i> in <i>Verwenden des VMware vRealize Orchestrator Client</i>. ■ Fehlerbehebung ihrer vRealize Orchestrator-Umgebung über Funktionen wie Workflow-Validierung und das Debuggen von Workflow-Skripts. |
| Viewer | <p>Dieser Benutzer verfügt über Lesezugriff auf alle vRealize Orchestrator Client, einschließlich aller Gruppen und Gruppeninhalte. Dieser Benutzer kann Inhalte anzeigen, bearbeiten oder ausführen oder Workflow-Ausführungen, Workflow-Ausführungsprotokolle oder Pakete exportieren. Viewer sind nicht durch Gruppenberechtigungen beschränkt.</p> <p>Hinweis Die Rolle „Viewer“ wird nur für vRealize Orchestrator-Instanzen unterstützt, die mit vRealize Automation authentifiziert sind. Diese Rolle ist nicht standardmäßig einer vRealize Automation-Rolle zugeordnet, sodass sie explizit den Benutzern zugewiesen werden muss.</p> |

| Benutzerrolle | Beschreibung |
|-----------------------------------|--|
| Workflow-Designer | <p>Dieser Benutzer kann die Funktionalität der vRealize Orchestrator-Plattform durch das Erstellen und Bearbeiten von Objekten erweitern. Workflow-Designer haben keinen Zugriff auf die Verwaltungs- und Fehlerbehebungsfunktionen des vRealize Orchestrator Client. Zu den wichtigsten Aufgaben des Workflow-Designers gehören:</p> <ul style="list-style-type: none"> ■ Erstellen, Bearbeiten, Ausführen und Löschen von vRealize Orchestrator-Objekten wie Workflows, Aktionen, Richtlinien und Konfigurationselementen. ■ Planen von Workflow-Ausführungen. Weitere Informationen finden Sie unter <i>Planen von Workflows im vRealize Orchestrator Client</i> in <i>Verwenden des VMware vRealize Orchestrator Client</i>. ■ Hinzufügen der vom Workflow-Entwickler erstellten Inhalte zu Gruppen, denen sie zugewiesen sind. ■ Weitergeben von lokalen Änderungen an der vRealize Orchestrator-Inhaltsbestandsliste an das verbundene Git-Repository. Weitere Informationen finden Sie unter <i>Weitergeben von Änderungen an ein Git-Repository</i> in <i>Verwenden des VMware vRealize Orchestrator Client</i>. |
| Benutzer mit beschränkten Rechten | <p>Benutzer ohne zugewiesene Rolle können sich weiterhin beim vRealize Orchestrator Client anmelden, haben aber nur eingeschränkten Zugriff auf die Funktionen und Inhalte des Clients. Wenn die Benutzer einer Gruppe zugewiesen sind, können sie Inhalte anzeigen und ausführen, die ihrer Gruppe zugeordnet sind.</p> |

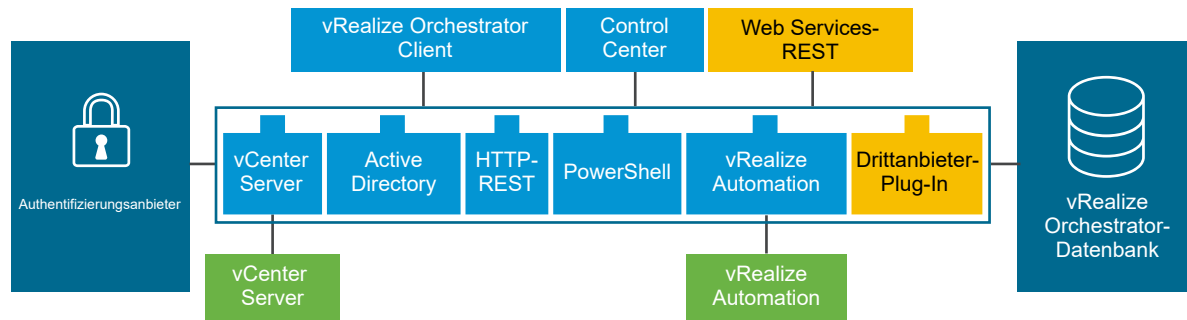
Architektur von vRealize Orchestrator

vRealize Orchestrator enthält eine Workflowbibliothek und eine Workflowengine, damit Sie Workflows erstellen und ausführen können, die Orchestrierungsprozesse automatisieren. Die Workflows werden mit den Objekten verschiedener Technologien ausgeführt, auf die vRealize Orchestrator über eine Serie von Plug-Ins zugreift.

vRealize Orchestrator stellt eine Standardgruppe von Plug-Ins bereit, unter anderem Plug-Ins für vCenter Server und vRealize Automation, damit Sie Aufgaben in den verschiedenen Umgebungen koordinieren können, für die die Plug-Ins verfügbar sind.

Zudem bietet vRealize Orchestrator eine offene Architektur für die Einbindung von externen Drittanbieteranwendungen in die Orchestrierungsplattform. Sie können Workflows mit den Objekten der Plug-In-Technologien ausführen, die Sie selbst definieren. vRealize Orchestrator verbindet sich mit einem Authentifizierungsanbieter, um Benutzerkonten zu verwalten, und mit einer vorkonfigurierten PostgreSQL-Datenbank, um Informationen aus den Workflows zu speichern, die unter vRealize Orchestrator ausgeführt werden. Der Zugriff auf vRealize Orchestrator, die damit bereitgestellten Objekte sowie die vRealize Orchestrator-Workflows ist über den vRealize Orchestrator Client oder über Webdienste möglich. Die Überwachung und Konfiguration der vRealize Orchestrator-Workflows und -Dienste erfolgen über den vRealize Orchestrator Client und Control Center.

Abbildung 1-1. Architektur von VMware vRealize Orchestrator



vRealize Orchestrator Plug-ins

Plug-Ins ermöglichen Ihnen den Zugriff auf und die Steuerung von externen Technologien und Anwendungen über vRealize Orchestrator. Indem Sie eine externe Technologie in einem vRealize Orchestrator-Plug-In verfügbar machen, können Sie Objekte und Funktionen in Workflows einbinden, die auf die Objekte und Funktionen dieser externen Technologie zugreifen.

Zu den externen Technologien, auf die Sie mithilfe von Plug-Ins zugreifen können, zählen Tools zum Virtualisierungsmanagement, E-Mail-Systeme, Datenbanken, Verzeichnisdienste und Remotesteuerungsschnittstellen.

vRealize Orchestrator bietet eine Reihe von Standard-Plug-Ins, mit denen Sie Technologien wie die VMware vCenter Server-API und E-Mail-Funktionen in Workflows einbinden können. Mithilfe der Plug-Ins können Sie die Bereitstellung neuer IT-Dienste automatisieren oder die Funktionen der vorhandenen Infrastruktur und Anwendungsdienste anpassen. Darüber hinaus können Sie mit der offenen Plug-In-Architektur von vRealize Orchestrator Plug-Ins für den Zugriff auf andere Anwendungen entwickeln.

Von VMware entwickelte vRealize Orchestrator-Plug-Ins werden als .vmoapp-Dateien verteilt.

Weitere Informationen zu den vRealize Orchestrator-Plug-Ins finden Sie unter [Verwenden der VMware vRealize Orchestrator- Plug-Ins](#).

Weitere Informationen zu vRealize Orchestrator-Plug-Ins von Drittanbietern finden Sie unter [VMware Marketplace](#).

Systemvoraussetzungen für vRealize Orchestrator

2

Ihr System muss die technischen Anforderungen erfüllen, die für eine reibungslose Funktion von vRealize Orchestrator erforderlich sind.

Eine Liste der unterstützten Versionen von vCenter Server, dem vSphere Web Client, vRealize Automation und anderen VMware-Lösungen finden Sie in der [VMware-Produkt-Interoperabilitätmatrix](#).

Dieses Kapitel enthält die folgenden Themen:

- [Komponenten der vRealize Orchestrator Appliance](#)
- [Hardwareanforderungen für die vRealize Orchestrator Appliance](#)
- [vRealize Orchestrator-Maximalwerte für die Skalierbarkeit](#)
- [Netzwerkanforderungen für vRealize Orchestrator](#)
- [vRealize Orchestrator-Ports und -Endpoints](#)
- [Von vRealize Orchestrator unterstützte Browser](#)
- [Internationalisierungsgrad und Lokalisierungsunterstützung](#)

Komponenten der vRealize Orchestrator Appliance

Die vRealize Orchestrator Appliance ist eine Photon-basierte virtuelle Appliance, die in Containern ausgeführt wird.

Die vRealize Orchestrator Appliance enthält die folgenden Komponenten:

- Ein Kubernetes-Layer auf Infrastrukturebene.
- Eine vorkonfigurierte PostgreSQL-Datenbank
- Die wichtigsten vRealize Orchestrator-Dienste: den Serverdienst, den Control Center-Dienst und den Orchestrierungs-UI-Dienst.

Die Standardkonfiguration der vRealize Orchestrator Appliance-Datenbank ist bereit für den Einsatz in Produktionssystemen.

Hinweis Um die vRealize Orchestrator Appliance in einer Produktionsumgebung verwenden zu können, müssen Sie den vRealize Orchestrator-Server für die Authentifizierung durch vRealize Automation oder vSphere konfigurieren. Weitere Informationen finden Sie unter [Konfigurieren eines eigenständigen vRealize Orchestrator-Servers](#).

Hardwareanforderungen für die vRealize Orchestrator Appliance

Die vRealize Orchestrator Appliance ist eine vorkonfigurierte Photon-basierte virtuelle Maschine, die in Containern ausgeführt wird. Stellen Sie vor der Bereitstellung der Appliance sicher, dass Ihr System die Mindestanforderungen an die Hardware erfüllt.

Für die vRealize Orchestrator Appliance gelten die folgenden Hardwareanforderungen:

- 4 CPUs
- 12 GB Arbeitsspeicher
- 200 GB Festplattenspeicher

Verringern Sie die Standardgröße des Arbeitsspeichers nicht, da der vRealize Orchestrator-Server mindestens 8 GB freien Arbeitsspeicher benötigt.

vRealize Orchestrator-Maximalwerte für die Skalierbarkeit

In der Tabelle für den Skalierbarkeitsgrenzwert werden die empfohlenen Maximalwerte für vRealize Orchestrator 8.x-Bereitstellungen beschrieben.

| Komponente | Skalierungsziele | Weitere Informationen |
|---|-------------------|---|
| Virtuelle Maschinen | 35.000 | |
| vCenter Server-Verbindungen | 10 | Weitere Informationen hierzu finden Sie unter Einrichtung von vCenter Server |
| Aktive Knoten in einem Cluster | 3 | Weitere Informationen hierzu finden Sie unter Konfigurieren eines vRealize Orchestrator-Clusters |
| Gleichzeitig laufende Workflows | 300 pro Knoten | Weitere Informationen hierzu finden Sie unter Konfigurieren der Workflow-Ausführungseigenschaften |
| In der Warteschlange befindliche laufende Workflows | 10.000 pro Knoten | |
| Beibehaltene Workflow-Runs | 100 pro Knoten | |
| Ablauf von Protokollereignissen (in Tagen) | 15 | |

Netzwerkanforderungen für vRealize Orchestrator

Jeder vRealize Orchestrator-Knoten erfordert eine Netzwerkeinrichtung.

Die Netzwerkanforderungen für vRealize Orchestrator lauten:

- Einzelne, statische IPv4- und Netzwerkadresse
- Erreichbarer, manuell festgelegter DNS-Server
- Gültiger, manuell festgelegter vollqualifizierter Domänenname (FQDN), der sowohl vorwärts als auch rückwärts über den DNS-Server aufgelöst werden kann

Hinweis Die Änderung der IP-Adresse oder die Änderung des Hostnamens nach der Installation wird nicht unterstützt und führt zu einem fehlerhaften Setup, das nicht wiederhergestellt werden kann.

vRealize Orchestrator-Ports und -Endpoints

Der vRealize Orchestrator-Kubernetes-Dienst enthält zwei Endpoints und mehrere Hauptnetzwerkports.

vRealize Orchestrator-Netzwerkports

Sie können auf vRealize Orchestrator über Port 443 zugreifen. Der Port 443 wird mit einem selbstsignierten Zertifikat gesichert, das während der Installation generiert wird. Wenn Sie einen externe Lastausgleichsdienst verwenden, muss er für den Ausgleich an Port 443 eingerichtet sein.

Zum Anzeigen aller vRealize Orchestrator-Ports können Sie das Tool [Ports und Protokolle](#) verwenden.

vRealize Orchestrator-Endpoints

Sie können auf die vRealize Orchestrator Client- und Control Center-Dienste an den folgenden Endpoints zugreifen.

| Dienst | Endpoint |
|------------------------------|---|
| vRealize Orchestrator Client | <code>https://your_orchestrator_FQDN/orchestration-ui</code> |
| Control Center | <code>https://your_orchestrator_FQDN/vco-controlcenter</code> |

Von vRealize Orchestrator unterstützte Browser

Vergewissern Sie sich, dass Ihre Browser vRealize Orchestrator unterstützen.

Für den Zugriff auf den vRealize Orchestrator Client und auf das Control Center müssen Sie einen der folgenden Browser verwenden:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome

Internationalisierungsgrad und Lokalisierungsunterstützung

Das Control Center von vRealize Orchestrator und der vRealize Orchestrator Client enthalten Unterstützung für nichtenglische Betriebssysteme, nichtenglische Datenformatierung und Unterstützung mehrerer Sprachen für das Control Center und die Client-Benutzeroberfläche.

Das Control Center von vRealize Orchestrator und der vRealize Orchestrator Client unterstützen die Verwendung von nichtenglischen Betriebssystemen, nichtenglischen Eingaben und Ausgaben sowie die Unterstützung nichtenglischer Datenformate wie Datum, Uhrzeit und Zahlen.

Die Benutzeroberflächen von vRealize Orchestrator und vRealize Orchestrator Client sind in den folgenden Sprachen lokalisiert:

- Spanisch
- Französisch
- Deutsch
- Traditionelles Chinesisch
- Vereinfachtes Chinesisch
- Koreanisch
- Japanisch
- Italienisch
- Niederländisch
- Portugiesisch (Brasilien)
- Russisch

Einrichten von vRealize Orchestrator-Komponenten

3

Wenn Sie die vRealize Orchestrator Appliance herunterladen und bereitstellen, wird der vRealize Orchestrator-Server vorkonfiguriert. Die Dienste werden nach der Bereitstellung automatisch gestartet.

Befolgen Sie die folgenden Richtlinien, um Verfügbarkeit und Skalierbarkeit Ihrer vRealize Orchestrator-Konfiguration zu verbessern:

- Installieren und konfigurieren Sie einen Authentifizierungsanbieter und konfigurieren Sie vRealize Orchestrator für die Verwendung mit dem Anbieter. Weitere Informationen finden Sie unter [Konfigurieren eines eigenständigen vRealize Orchestrator-Servers](#).
- Installieren und konfigurieren Sie für geclusterte vRealize Orchestrator-Umgebungen einen Lastausgleichsserver. Legen Sie in seiner Konfiguration fest, dass er die Arbeitslast auf den vRealize Orchestrator-Servern verteilt.

Dieses Kapitel enthält die folgenden Themen:

- [Einrichtung von vCenter Server](#)
- [Authentifizierungsmethoden](#)

Einrichtung von vCenter Server

Eine Erhöhung der Anzahl an vCenter Server-Instanzen in der vRealize Orchestrator-Einrichtung bedeutet auch, dass vRealize Orchestrator mehr Sitzungen verwalten muss. Zu viele aktive Sitzungen können zu Zeitüberschreitungen in vRealize Orchestrator führen, wenn mehr als zehn vCenter Server-Verbindungen bestehen.

Eine Liste der unterstützten Versionen von vCenter Server finden Sie in der [VMware-Produkt-Interoperabilitätsmatrix](#).

Hinweis Wenn Ihr Netzwerk über ausreichend Bandbreite und Latenz verfügt, können Sie mehrere vCenter Server-Instanzen auf unterschiedlichen virtuellen Maschinen in Ihrem vRealize Orchestrator-Setup ausführen. Wenn Sie ein LAN verwenden, um die Kommunikation zwischen vRealize Orchestrator und vCenter Server zu verbessern, ist eine Leitung mit 100 Mbit/s unerlässlich.

Authentifizierungsmethoden

Zur Authentifizierung und Verwaltung von Benutzerberechtigungen benötigt vRealize Orchestrator eine Verbindung mit einer vRealize Automation- oder einer vSphere-Serverinstanz.

Wenn Sie die vRealize Orchestrator Appliance herunterladen und bereitstellen, müssen Sie den Server mit einer vRealize Automation- oder vSphere-Authentifizierung konfigurieren. Weitere Informationen finden Sie unter [Konfigurieren eines eigenständigen vRealize Orchestrator-Servers](#).

Hinweis Die vRealize Orchestrator 8.x-Authentifizierung bei vRealize Automation wird nur mit vRealize Automation 8.x unterstützt.

Installieren von vRealize Orchestrator

4

vRealize Orchestrator besteht aus einer Server- und einer Clientkomponente.

Um vRealize Orchestrator zu verwenden, müssen Sie die vRealize Orchestrator Appliance auf dem vRealize Orchestrator-Server bereitstellen.

Sie können die Standardkonfigurationseinstellungen von vRealize Orchestrator über das Control Center von vRealize Orchestrator ändern.

Dieses Kapitel enthält die folgenden Themen:

- [Herunterladen und Bereitstellen der vRealize Orchestrator Appliance](#)

Herunterladen und Bereitstellen der vRealize Orchestrator Appliance

Bevor Sie auf die Inhalte und Dienste von vRealize Orchestrator zugreifen können, müssen Sie die vRealize Orchestrator Appliance herunterladen und bereitstellen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über eine laufende vCenter Server-Instanz verfügen. Die vCenter Server-Version muss 6.0 oder höher sein.
- Stellen Sie sicher, dass der Host, auf dem Sie die vRealize Orchestrator Appliance bereitstellen, die Mindestanforderungen für die Hardware erfüllt. Weitere Informationen finden Sie unter [Hardwareanforderungen für die vRealize Orchestrator Appliance](#).
- Wenn Ihr System isoliert ist und kein Internetzugriff besteht, müssen Sie die .ova-Datei für die Appliance von der VMware-Website herunterladen.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client als **Administrator** an.
- 2 Wählen Sie ein Bestandslistenobjekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, z. B. ein Datacenter, Ordner, Cluster, Ressourcenpool oder Host.
- 3 Wählen Sie **Aktionen > OVF-Vorlage bereitstellen** aus.
- 4 Geben Sie den Pfad oder die URL zur .ova-Datei ein und klicken Sie auf **Weiter**.

- 5 Geben Sie den Namen und den Speicherort der vRealize Orchestrator Appliance an und klicken Sie auf **Weiter**.
- 6 Wählen Sie einen Host, ein Cluster, einen Ressourcenpool oder eine vApp als Ziel für die Ausführung der Appliance aus und klicken Sie auf **Weiter**.
- 7 Überprüfen Sie die Bereitstellungsdetails und klicken Sie auf **Weiter**.
- 8 Akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 9 Wählen Sie das Speicherformat aus, das Sie für die vRealize Orchestrator Appliance verwenden möchten.

| Format | Beschreibung |
|---------------------------------------|--|
| Thick Provisioned Lazy Zeroed | Erstellt eine virtuelle Festplatte im Thick-Standardformat. Der für die virtuelle Festplatte erforderliche Speicherplatz wird zugeteilt, wenn die virtuelle Festplatte erstellt wird. Wenn Daten auf dem physischen Gerät verbleiben, werden diese nicht beim Anlegen gelöscht, sondern später, während der ersten Schreibvorgänge der virtuellen Maschine. |
| Thick Provisioned Eager Zeroed | Unterstützt Clustering-Funktionen wie Fault Tolerance. Der für die virtuelle Festplatte erforderliche Speicherplatz wird zugeteilt, wenn die virtuelle Festplatte erstellt wird. Wenn Daten auf dem physischen Gerät verbleiben, werden sie gelöscht („zeroed out“), wenn die virtuelle Festplatte erstellt wird. Das Erstellen von Festplatten in diesem Format kann wesentlich länger dauern als bei anderen Formaten. |
| Thin Provisioned Format | Benötigt weniger Festplattenspeicher. Für eine Festplatte mit diesem Format stellen Sie genau so viel Datenspeicherplatz bereit, wie die Festplatte ausgehend von dem Wert erfordert, den Sie für die Datenträgergröße auswählen. Die Festplatte besitzt zunächst nur eine geringe Größe und verwendet nur so viel Datenspeicherplatz, wie sie für ihre anfänglichen Vorgänge benötigt. |

- 10 Klicken Sie auf **Weiter**.
- 11 Konfigurieren Sie die Netzwerkeinstellungen und geben Sie das **root**-Kennwort ein.

Bei der Konfiguration der Netzwerkeinstellungen der vRealize Orchestrator Appliance müssen Sie das IPv4-Protokoll verwenden. Für DHCP- und statische Netzwerkkonfigurationen müssen Sie einen vollqualifizierten Domännennamen (FQDN) für Ihre vRealize Orchestrator Appliance hinzufügen.

Wenn der Hostname, der in der Shell der bereitgestellten vRealize Orchestrator Appliance angezeigt wird, *photon-machine* lautet, sind die obigen Netzwerkkonfigurationsanforderungen nicht erfüllt.

- 12 (Optional) Konfigurieren Sie zusätzliche Netzwerkeinstellungen für die vRealize Orchestrator Appliance, z. B. das Aktivieren von SSH-Zugriff.

Hinweis Beim Konfigurieren eines Kubernetes-Netzwerks müssen die Werte des internen Cluster-CIDR und des internen Dienst-CIDR mindestens 1.024 Hosts zulassen. Aufgrund dieser Anforderung muss der Wert für die Netzwerkmaske 22 oder weniger sein. Netzwerkmaskenwerte über 22 sind ungültig. Die Kubernetes-Netzwerkeigenschaften müssen die folgenden Standardwerte aufweisen:

| Kubernetes network property | Default value | Property description |
|---------------------------------------|---------------|---|
| CIDR des internen Kubernetes-Clusters | 10.244.0.0/22 | Das CIDR, das für Pods verwendet wird, die innerhalb des Kubernetes-Clusters ausgeführt werden. |
| CIDR des internen Kubernetes-Diensts | 10.244.4.0/22 | Das CIDR, das für Kubernetes-Dienste verwendet wird, die innerhalb des Kubernetes-Clusters ausgeführt werden. |

Hinweis Sie können auch die Kubernetes-CIDR-Netzwerkeigenschaften nach der Bereitstellung ändern. Weitere Informationen finden Sie unter [Konfigurieren von vRealize Orchestrator-Kubernetes-CIDR](#).

- 13 (Optional) Um den FIPS-Modus für die vRealize Orchestrator Appliance zu aktivieren, legen Sie **FIPS-Modus** auf **strict**.

Hinweis Die FIPS 140-2-Aktivierung wird nur für neue vRealize Orchestrator-Umgebungen unterstützt. Wenn Sie den FIPS-Modus in Ihrer Umgebung aktivieren möchten, müssen Sie dies während der Installation tun.

- 14 Klicken Sie auf **Weiter**.

- 15 Überprüfen Sie die Seite **Bereit zum Abschließen** und klicken Sie auf **Beenden**.

Ergebnisse

Die vRealize Orchestrator Appliance wurde bereitgestellt.

Nächste Schritte

Melden Sie sich bei der vRealize Orchestrator Appliance-Befehlszeile als **root** an und bestätigen Sie, dass Sie ein Forward- oder Reverse-DNS-Lookup durchführen können.

- Führen Sie für ein Forward-DNS-Lookup den Befehl `nslookup your_orchestrator_FQDN` aus. Der Befehl muss die vRealize Orchestrator Appliance-IP-Adresse zurückgeben.
- Führen Sie für ein Reverse-DNS-Lookup den Befehl `nslookup your_orchestrator_IP` aus. Der Befehl muss den vRealize Orchestrator Appliance-FQDN zurückgeben.

Hinweis Wenn Sie SSH während der Bereitstellung nicht aktiviert haben, können Sie DNS-Suchvorgänge auch über die Konsole der virtuellen Maschine im vSphere Web Client durchführen.

Schalten Sie die vRealize Orchestrator Appliance ein und öffnen Sie die Startseite

Um die eigenständige vRealize Orchestrator Appliance zu verwenden, müssen Sie sie zuerst einschalten.

Verfahren

- 1 Melden Sie sich als **Administrator** beim vSphere Web Client an.
- 2 Klicken Sie mit der rechten Maustaste auf die vRealize Orchestrator Appliance und dann auf **Betrieb > Einschalten**.
- 3 Navigieren Sie in einem Webbrowser zur Hostadresse Ihrer virtuellen vRealize Orchestrator Appliance-Maschine, die Sie während der OVA-Bereitstellung konfiguriert haben.

https://your_orchestrator_FQDN/vco.

Aktivieren oder Deaktivieren des SSH-Zugriffs auf die vRealize Orchestrator Appliance

Sie können den SSH-Zugriff auf die vRealize Orchestrator Appliance aktivieren oder deaktivieren.

Voraussetzungen

- Laden Sie die vRealize Orchestrator Appliance herunter und stellen Sie sie bereit.
- Stellen Sie sicher, dass die vRealize Orchestrator Appliance aktiv ist und ausgeführt wird.

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance als **root** an.
- 2 Um den SSH-Zugriff zu aktivieren, führen Sie den Befehl `/usr/bin/toggle-ssh enable` aus.
- 3 Um den SSH-Zugriff zu deaktivieren, führen Sie den Befehl `/usr/bin/toggle-ssh disable` aus.

Erstkonfiguration

5

Bevor Sie mit der Automatisierung von Aufgaben und der Verwaltung von Systemen und Anwendungen mit vRealize Orchestrator beginnen, müssen Sie mithilfe des Control Center von vRealize Orchestrator einen externen Authentifizierungsanbieter konfigurieren. Sie können auch das Control Center von vRealize Orchestrator für zusätzliche Konfigurationsaufgaben wie das Verwalten von Lizenz- und Zertifikatsinformationen, das Installieren von Plug-Ins oder das Überwachen des Status Ihres vRealize Orchestrator-Clusters verwenden.

Dieses Kapitel enthält die folgenden Themen:

- Konfigurieren eines eigenständigen vRealize Orchestrator-Servers
- Aktivieren von vRealize Orchestrator-Funktionen mit Lizenzen
- vRealize Orchestrator-Datenbankverbindung
- Zertifikate verwalten
- Konfigurieren des vRealize Orchestrator-Plug-Ins
- vRealize Orchestrator-Hochverfügbarkeit
- Konfigurieren des Programms zur Verbesserung der Benutzerfreundlichkeit

Konfigurieren eines eigenständigen vRealize Orchestrator-Servers

Obwohl es sich bei vRealize Orchestrator Appliance um eine vorkonfigurierte Photon-basierte virtuelle Maschine handelt, müssen Sie einen Authentifizierungsanbieter konfigurieren, bevor Sie auf die vollständigen Funktionen des Control Center von vRealize Orchestrator und auf vRealize Orchestrator Client zugreifen können.

Konfigurieren eines eigenständigen vRealize Orchestrator-Servers mit vRealize Automation-Authentifizierung

Um die vRealize Orchestrator Appliance für die Verwendung vorzubereiten, müssen Sie die Hosteinstellungen und den Authentifizierungsanbieter konfigurieren. Sie können vRealize Orchestrator für die Authentifizierung mit vRealize Automation konfigurieren. Verwenden Sie die vRealize Automation-Authentifizierung mit vRealize Automation 8.x.

Voraussetzungen

- Laden Sie die neueste Version der vRealize Orchestrator Appliance herunter und stellen Sie diese bereit. Weitere Informationen finden Sie unter [Herunterladen und Bereitstellen der vRealize Orchestrator Appliance](#).
- Installieren und konfigurieren Sie vRealize Automation 8.x und stellen Sie sicher, dass Ihr vRealize Automation-Server ausgeführt wird. Weitere Informationen finden Sie in der vRealize Automation-Dokumentation.

Wichtig Die Produktversion des vRealize Automation-Authentifizierungsanbieters muss mit der Produktversion Ihrer vRealize Orchestrator-Bereitstellung übereinstimmen. Um beispielsweise eine vRealize Orchestrator 8.7-Bereitstellung zu authentifizieren, müssen Sie eine vRealize Automation 8.7-Bereitstellung verwenden.

Wenn Sie vorhaben, einen Cluster zu erstellen, gehen Sie wie folgt vor:

- Richten Sie einen Lastausgleichsdienst ein, um den Datenverkehr auf mehrere Instanzen von vRealize Orchestrator zu verteilen. Weitere Informationen finden Sie im [Handbuch für den Lastausgleich von VMware vRealize Orchestrator 8.x](#).

Verfahren

- 1 Rufen Sie das Control Center auf, um den Konfigurationsassistenten zu starten.
 - a Navigieren Sie zu `https://your_orchestrator_FQDN/vco-controlcenter`.
 - b Melden Sie sich als **root** mit dem Kennwort an, das Sie bei der OVA-Bereitstellung eingegeben haben.
- 2 Konfigurieren Sie den Authentifizierungsanbieter.
 - a Wählen Sie auf der Seite **Anbieter für Authentifizierung konfigurieren** im Dropdown-Menü **Authentifizierungsmodus** den Eintrag **vRealize Automation** aus.
 - b Geben Sie in das Textfeld **Hostadresse** die Adresse Ihres vRealize Automation-Hosts ein und klicken Sie auf **VERBINDEN**.

Das Format der vRealize Automation-Hostadresse muss `https://your_vra_hostname` lauten.
 - c Klicken Sie auf **Zertifikat akzeptieren**.
 - d Geben Sie die Anmeldedaten des vRealize Automation-Organisationsbesitzers ein, unter dem vRealize Orchestrator konfiguriert werden soll. Klicken Sie auf **REGISTRIEREN**.
 - e Klicken Sie auf **ÄNDERUNGEN SPEICHERN**.

Eine Meldung zeigt an, dass Ihre Konfiguration erfolgreich gespeichert wurde.

Ergebnisse

Sie haben die vRealize Orchestrator-Serverkonfiguration erfolgreich abgeschlossen.

Nächste Schritte

- Vergewissern Sie sich auf der Seite **Lizenzierung**, dass als Lizenzgeber **CSP** konfiguriert ist.
- Überprüfen Sie auf der Seite **Konfiguration überprüfen**, ob der Knoten ordnungsgemäß konfiguriert ist.

Hinweis Nach der Konfiguration des Authentifizierungsanbieters wird der vRealize Orchestrator-Server nach 2 Minuten automatisch neu gestartet. Wenn Sie die Konfiguration unmittelbar nach der Authentifizierung überprüfen, kann es vorkommen, dass ein ungültiger Konfigurationsstatus zurückgegeben wird.

Konfigurieren eines eigenständigen vRealize Orchestrator-Servers mit vSphere-Authentifizierung

Sie registrieren den vRealize Orchestrator-Server mithilfe des vSphere-Authentifizierungsmodus bei einem vCenter Single Sign-On-Server. Verwenden Sie die vCenter Single Sign-On-Authentifizierung mit vCenter Server 6.0 und höher.

Voraussetzungen

- Laden Sie die neueste Version der vRealize Orchestrator Appliance herunter und stellen Sie diese bereit. Weitere Informationen finden Sie unter [Herunterladen und Bereitstellen der vRealize Orchestrator Appliance](#).
- Installieren und konfigurieren Sie vCenter Server mit aktivem vCenter Single Sign-On. Weitere Informationen finden Sie in der vSphere-Dokumentation.

Wenn Sie vorhaben, einen Cluster zu erstellen, gehen Sie wie folgt vor:

- Richten Sie einen Lastausgleichsdienst ein, um den Datenverkehr auf mehrere Instanzen von vRealize Orchestrator zu verteilen. Weitere Informationen finden Sie im [Handbuch für den Lastausgleich von VMware vRealize Orchestrator 8.x](#).

Verfahren

- 1 Rufen Sie das Control Center auf, um den Konfigurationsassistenten zu starten.
 - a Navigieren Sie zu `https://your_orchestrator_FQDN/vco-controlcenter`.
 - b Melden Sie sich als **root** mit dem Kennwort an, das Sie bei der OVA-Bereitstellung eingegeben haben.

2 Konfigurieren Sie den Authentifizierungsanbieter.

- a Wählen Sie auf der Seite **Anbieter für Authentifizierung konfigurieren** im Dropdown-Menü **Authentifizierungsmodus** den Eintrag **vSphere** aus.
- b Geben Sie in das Textfeld **Hostadresse** den vollqualifizierten Domännennamen oder die IP-Adresse der Platform Services Controller-Instanz ein, die den vCenter Single Sign-On enthält, und klicken Sie auf **Verbinden**.

Hinweis Wenn Sie eine externe Platform Services Controller-Instanz oder mehrere Platform Services Controller-Instanzen mit einem Lastausgleichsdienst verwenden, müssen Sie die Zertifikate aller Platform Services Controller manuell importieren, die eine vCenter Single Sign-On-Domäne gemeinsam nutzen.

Hinweis Um einen anderen vSphere Client in ihre konfigurierte vRealize Orchestrator-Umgebung zu integrieren, müssen Sie vSphere so konfigurieren, dass derselbe Platform Services Controller verwendet wird, der für vRealize Orchestrator registriert ist. Für vRealize Orchestrator-Umgebungen mit Hochverfügbarkeit müssen Sie die-PCS-Instanzen hinter dem vRealize Orchestrator-Lastausgleichsserver replizieren.

- c Überprüfen Sie die Zertifikatinformationen des Authentifizierungsanbieters und klicken Sie auf **Zertifikat akzeptieren**.
- d Geben Sie die Anmeldedaten des lokalen Administratorkontos für die vCenter Single Sign-On-Domäne ein. Klicken Sie auf **REGISTRIEREN**.

Standardmäßig wird das Konto **administrator@vsphere.local** verwendet, und der Name des Standardmandanten lautet **vsphere.local**.

- e Geben Sie in das Textfeld **Admin-Gruppe** den Namen einer Administratorgruppe ein und klicken Sie auf **SUCHEN**.

Beispiel: **vsphere.local\vcoadmins**

- f Wählen Sie die Administratorgruppe aus, die Sie verwenden möchten.
- g Klicken Sie auf **ÄNDERUNGEN SPEICHERN**.

Eine Meldung zeigt an, dass Ihre Konfiguration erfolgreich gespeichert wurde.

Ergebnisse

Sie haben die vRealize Orchestrator-Serverkonfiguration erfolgreich abgeschlossen.

Nächste Schritte

- Vergewissern Sie sich auf der Seite **Lizenzierung**, dass als Lizenzgeber **CIS** konfiguriert ist.

- Überprüfen Sie auf der Seite **Konfiguration überprüfen**, ob der Knoten ordnungsgemäß konfiguriert ist.

Hinweis Nach der Konfiguration des Authentifizierungsanbieters wird der vRealize Orchestrator-Server nach 2 Minuten automatisch neu gestartet. Wenn Sie die Konfiguration unmittelbar nach der Authentifizierung überprüfen, kann es vorkommen, dass ein ungültiger Konfigurationsstatus zurückgegeben wird.

Aktivieren von vRealize Orchestrator-Funktionen mit Lizenzen

Der Zugriff auf bestimmte vRealize Orchestrator-Funktionen basiert auf der Lizenz, die auf Ihre vRealize Orchestrator-Bereitstellung angewendet wird.

Nach der Authentifizierung wird Ihrer vRealize Orchestrator-Instanz eine auf dem Authentifizierungsanbieter basierende Lizenz zugewiesen. Lizenzen steuern den Zugriff auf die folgenden vRealize Orchestrator-Funktionen:

- Git-Integration
- Rollenverwaltung
- Unterstützung mehrerer Sprachen (Python, Node.js und PowerShell)

Sie können die Lizenz des vRealize Orchestrator-Servers manuell auf der Seite **Lizenzen** des Control Centers ändern.

Hinweis Es gibt keine Beschränkung für die Anzahl der vRealize Orchestrator-Bereitstellungen, auf die Sie dieselbe Lizenz anwenden können, unabhängig vom Lizenztyp. Für vRealize Automation-Lizenzen ist die Bereitstellung und Konfiguration einer vRealize Automation-Umgebung nicht erforderlich.

| Authentifizierung | Lizenz | Git-Integration | Rollenverwaltung | Unterstützung mehrerer Sprachen |
|---------------------|---|-----------------|--|---------------------------------|
| vSphere | vSphere vCloud Suite Standard | Nein | Nein | Nein |
| vSphere | vRealize Automation vRealize Suite Advanced oder Enterprise vCloud Suite Advanced oder Enterprise | Ja | Ja | Ja |
| vRealize Automation | vRealize Automation vRealize Suite Advanced oder Enterprise vCloud Suite Advanced oder Enterprise | Ja | Rollen werden von der vRealize Automation-Instanz verwaltet, die zur Authentifizierung von vRealize Orchestrator verwendet wird. | Ja |

Hinweis vRealize Suite-Standardlizenzen enthalten keine vRealize Automation, daher unterstützen Sie den Zugriff auf vRealize Orchestrator Funktionen nicht.

vRealize Orchestrator-Datenbankverbindung

Der vRealize Orchestrator-Server benötigt eine Datenbank zum Speichern von Daten.

Die bereitgestellte vRealize Orchestrator Appliance enthält eine vorkonfigurierte PostgreSQL-Datenbank, die vom vRealize Orchestrator-Server zum Speichern von Daten verwendet wird.

Die PostgreSQL-Datenbank ist für Benutzer nicht zugänglich.

Zertifikate verwalten

Das Zertifikat wird zu einem bestimmten Server ausgegeben und enthält Informationen über den öffentlichen Schlüssel des Servers. Es ermöglicht Ihnen, alle Elemente zu signieren, die in vRealize Orchestrator erstellt werden, und ihre Authentizität zu garantieren. Wenn der Client ein Element von Ihrem Server erhält, meistens handelt es sich dabei um ein Paket, überprüft der Client Ihre Identität und entscheidet, ob Ihrer Signatur zu trauen ist.

■ Verwalten von vRealize Orchestrator-Zertifikaten

Sie können die vRealize Orchestrator-Zertifikate auf der Seite **Zertifikate** im Control Center von vRealize Orchestrator oder über den vRealize Orchestrator Client mithilfe der getaggtten *ssl_trust_manager*-Workflows verwalten.

Verwalten von vRealize Orchestrator-Zertifikaten

Sie können die vRealize Orchestrator-Zertifikate auf der Seite **Zertifikate** im Control Center von vRealize Orchestrator oder über den vRealize Orchestrator Client mithilfe der getaggten *ssl_trust_manager*-Workflows verwalten.

Importieren eines Zertifikats in den Orchestrator Trust Store

Das Control Center von vRealize Orchestrator nutzt eine sichere Verbindung für die Kommunikation mit vCenter Server, dem Verwaltungssystem für relationale Datenbanken (RDBMS), LDAP, Single Sign-On und anderen Servern. Sie können das erforderliche TLS-Zertifikat über eine URL oder eine PEM-kodierte Datei importieren. Sie müssen jedes Mal, wenn Sie eine TLS-Verbindung zu einer Serverinstanz verwenden möchten, zuerst das entsprechende Zertifikat über die Registerkarte **Vertrauenswürdige Zertifikate** auf der Seite **Zertifikate** und dann das entsprechende TLS-Zertifikat importieren.

Sie können das TLS-Zertifikat in vRealize Orchestrator aus einer URL-Adresse oder aus einer PEM-kodierten Datei laden.

| Option | Beschreibung |
|---|--|
| Aus URL oder Proxy-URL importieren | Die URL des Remoteservers: <code>https://IP-Adresse_Ihres_Servers</code> oder <code>IP-Adresse:Port_Ihres_Servers</code> |
| Aus Datei importieren | Pfad zur PEM-kodierten Zertifikatsdatei. Hinweis Sie können auch ein vertrauenswürdiges Zertifikat importieren, indem Sie den Workflow Vertrauenswürdiges Zertifikat aus einer Datei importieren im vRealize Orchestrator Client ausführen. Die über diesen Workflow importierte Datei muss DER-codiert sein. |

Weitere Informationen zum Importieren eines Zertifikats finden Sie unter [Importieren eines vertrauenswürdigen Zertifikats über Control Center](#).

Paketsignaturzertifikat

Pakete, die aus einem vRealize Orchestrator-Server exportiert werden, werden digital signiert. Sie können ein Zertifikat zum Signieren von Paketen importieren, exportieren oder neu generieren. Paketsignaturzertifikate sind eine Form digitaler Identifikation, die die verschlüsselte Kommunikation sowie eine Signatur für Ihre Orchestrator-Pakete garantiert.

In der vRealize Orchestrator Appliance ist ein Paketsignaturzertifikat enthalten, das automatisch anhand der Netzwerkeinstellungen der Appliance generiert wird. Bei Änderungen an den Netzwerkeinstellungen der Appliance müssen Sie manuell ein neues Paketsignaturzertifikat erstellen. Nachdem Sie ein neues Paketsignaturzertifikat erstellt haben, werden alle Pakete, die Sie in Zukunft exportieren, mit dem neuen Zertifikat signiert.

Generieren eines benutzerdefinierten TLS-Zertifikats für vRealize Orchestrator

Sie können die vRealize Orchestrator Appliance verwenden, um ein neues TLS-Zertifikat für Ihre Umgebung zu generieren oder ein vorhandenes benutzerdefiniertes Zertifikat festzulegen.

In der vRealize Orchestrator Appliance ist ein TLS-Zertifikat (Trusted Layer Security) enthalten, das automatisch anhand der Netzwerkeinstellungen der Appliance generiert wird. Bei Änderungen an den Netzwerkeinstellungen der Appliance müssen Sie manuell ein neues Zertifikat erstellen. Indem Sie eine Zertifikatskette erstellen, können Sie eine verschlüsselte Kommunikation gewährleisten und eine Signatur für Ihre Pakete bereitstellen. Für den Empfänger ist jedoch nicht mit Sicherheit erkennbar, ob das selbstsignierte Paket wirklich von Ihrem Server und nicht von einem Dritten ausgegeben wurde, der vorgibt, Sie zu sein. Um die Identität Ihres Servers nachzuweisen, verwenden Sie ein von einer Zertifizierungsstelle signiertes Zertifikat.

vRealize Orchestrator generiert ein für Ihre Umgebung eindeutiges Serverzertifikat. Der private Schlüssel wird in der `vmo_keystore`-Tabelle der vRealize Orchestrator-Datenbank gespeichert.

Hinweis Informationen zum Konfigurieren Ihrer vRealize Orchestrator Appliance für die Verwendung eines vorhandenen benutzerdefinierten TLS-Zertifikats finden Sie unter [Festlegen eines benutzerdefinierten TLS-Zertifikats für vRealize Orchestrator](#).

Voraussetzungen

Stellen Sie sicher, dass der SSH-Zugriff für die vRealize Orchestrator Appliance aktiviert ist. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren des SSH-Zugriffs auf die vRealize Orchestrator Appliance](#).

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance über SSH als **root** an.
- 2 Führen Sie den Befehl `vracli certificate ingress --generate auto --set stdin` aus.
- 3 Um das benutzerdefinierte Zertifikat auf Ihre vRealize Orchestrator Appliance anzuwenden, führen Sie das Bereitstellungsskript aus.
 - a Gehen Sie zum Verzeichnis `/opt/scripts/`.

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

- b Führen Sie das Skript `./deploy.sh` aus.

Wichtig Unterbrechen Sie das Bereitstellungsskript nicht. Die folgende Meldung wird angezeigt, wenn das Skript ausgeführt wurde:

```
Prelude has been deployed successfully. To access, go to your_orchestrator_address
```

Nächste Schritte

Um zu bestätigen, dass die neue Zertifikatskette angewendet wird, führen Sie den Befehl `vracli certificate ingress --list` aus.

Festlegen eines benutzerdefinierten TLS-Zertifikats für vRealize Orchestrator

Legen Sie ein benutzerdefiniertes TLS-Zertifikat für Ihre vRealize Orchestrator Appliance fest.

In der vRealize Orchestrator Appliance ist ein TLS-Zertifikat (Trusted Layer Security) enthalten, das automatisch anhand der Netzwerkeinstellungen der Appliance generiert wird.

Sie können Ihre vRealize Orchestrator Appliance so konfigurieren, dass ein vorhandenes benutzerdefiniertes TLS-Zertifikat verwendet wird. Sie können das Zertifikat festlegen, indem Sie die entsprechende PEM-Datei von Ihrem lokalen Computer in die vRealize Orchestrator Appliance importieren. Sie können auch Ihr benutzerdefiniertes TLS-Zertifikat festlegen, indem Sie die Zertifikatskette direkt in die vRealize Orchestrator Appliance kopieren. Für beide Verfahren müssen Sie das Skript `./deploy.sh` ausführen, bevor das neue TLS-Zertifikat in Ihrer vRealize Orchestrator-Bereitstellung verwendet werden kann.

Informationen zum Generieren eines neuen benutzerdefinierten TLS-Zertifikats finden Sie unter [Generieren eines benutzerdefinierten TLS-Zertifikats für vRealize Orchestrator](#).

Voraussetzungen

- Stellen Sie sicher, dass der SSH-Zugriff für die vRealize Orchestrator Appliance aktiviert ist. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren des SSH-Zugriffs auf die vRealize Orchestrator Appliance](#).
- Stellen Sie sicher, dass die PEM-Datei mit dem TLS-Zertifikat die folgenden Komponenten in der festgelegten Reihenfolge enthält:
 - a Der private Schlüssel für das Zertifikat.
 - b Das primäre Zertifikat.
 - c Gegebenenfalls das Zwischenzertifikat der Zertifizierungsstelle (CA) oder Zertifikate.
 - d Das Zertifizierungsstellen-Stammzertifikat.

Das TLS-Zertifikat kann beispielsweise folgende Struktur aufweisen:

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

Verfahren

- 1 Legen Sie das Zertifikat fest, indem Sie die PEM-Datei in die vRealize Orchestrator Appliance importieren.

- a Importieren Sie das PEM-Zertifikat von Ihrem lokalen Computer, indem Sie einen Secure-Copy-Befehl (SCP) aus einer SSH-Shell ausführen.

Für Linux können Sie einen Terminal-SCP-Befehl verwenden:

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

Für Windows können Sie einen PuTTY Client-PSCP-Befehl verwenden:

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

- b Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance über SSH als **root** an.
 - c Führen Sie den Befehl `vracli certificate ingress --set your_cert_file.PEM` aus.
- 2 (Optional) Legen Sie das Zertifikat fest, indem Sie die Zertifikatskette direkt in die Appliance kopieren.
 - a Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance über SSH als **root** an.
 - b Führen Sie den Befehl `vracli certificate ingress --set stdin` aus.
 - c Kopieren Sie die Zertifikatskette, fügen Sie sie ein und drücken Sie STRG+D.
- 3 Um das neue TLS-Zertifikat zu übernehmen, führen Sie das Bereitstellungsskript aus.
 - a Gehen Sie zum Verzeichnis `/opt/scripts/`.

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

- b Führen Sie das Skript `./deploy.sh` aus.

Wichtig Unterbrechen Sie das Bereitstellungsskript nicht. Die folgende Meldung wird angezeigt, wenn das Skript ausgeführt wurde:

```
Prelude has been deployed successfully. To access, go to https://your_orchestrator_FQDN
```

Ergebnisse

Sie haben ein benutzerdefiniertes TLS-Zertifikat für Ihre vRealize Orchestrator Appliance festgelegt.

Nächste Schritte

Um zu bestätigen, dass die neue Zertifikatskette angewendet wird, führen Sie den Befehl `vracli certificate ingress --list` aus.

Importieren eines vertrauenswürdigen Zertifikats über Control Center

Um mit anderen Servern sicher kommunizieren zu können, muss der vRealize Orchestrator-Server deren Identität prüfen können. Zu diesem Zweck müssen Sie möglicherweise das TLS-Zertifikat der Remote-Einheit in den vRealize Orchestrator-Trust Store importieren. Um ein Zertifikat als vertrauenswürdig einzustufen, können Sie es in den Trust Store importieren, indem Sie entweder eine Verbindung zu einer bestimmten URL herstellen oder das Zertifikat direkt als PEM-codierte Datei importieren.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Wechseln Sie zur Seite **Zertifikate**.
- 3 Wählen Sie **Vertrauenswürdige Zertifikate** und klicken Sie auf **Importieren**.
- 4 Um das Zertifikat aus einer Datei zu importieren, wählen Sie **Aus PEM-kodierter Datei importieren** aus.
- 5 Navigieren Sie zur Zertifikatsdatei und klicken Sie auf **Importieren**.
- 6 Um das Zertifikat aus einer URL-Adresse zu importieren, wählen Sie **Aus URL importieren** aus.
- 7 Geben Sie die URL-Adresse ein, an der Ihr Zertifikat gespeichert ist, und klicken Sie auf **Importieren**.

Ergebnisse

Sie haben ein Remote-Server-Zertifikat erfolgreich in den vRealize Orchestrator-Trust Store importiert.

Konfigurieren des vRealize Orchestrator-Plug-Ins

Die vRealize Orchestrator Appliance bietet Zugriff auf eine vorinstallierte Bibliothek mit Standard-Plug-Ins. Die standardmäßigen vRealize Orchestrator-Plug-Ins werden über Plug-In-spezifische Workflows konfiguriert, die im vRealize Orchestrator-Client ausgeführt werden.

Die standardmäßigen vRealize Orchestrator-Plug-Ins werden mit Konfigurationsworkflows bereitgestellt. Sie können diese Workflows auf dem vRealize Orchestrator-Client ausführen, um Endpoints für die Verwaltung zu registrieren.

Die Konfigurationsworkflows verfügen über das Tag *configuration*. Um beispielsweise auf Workflows zuzugreifen, die zum Verwalten von AMQP-Brokern und -Abonnements verwendet werden, geben Sie die Tags *AMQP* und *Konfiguration* in das Suchtextfeld der Workflowbibliothek ein.

Verwalten von vRealize Orchestrator-Plug-Ins

Auf der Seite **Plug-Ins verwalten** im Control Center von vRealize Orchestrator können Sie eine Liste aller in vRealize Orchestrator installierten Plug-Ins anzeigen und grundlegende Verwaltungsaktionen ausführen.

Installieren oder Aktualisieren eines Plug-Ins

Die vRealize Orchestrator-Plug-Ins ermöglichen die Integration anderer Softwareprodukte in den vRealize Orchestrator-Server. vRealize Orchestrator enthält eine Reihe von vorinstallierten Standard-Plug-Ins. Sie können die Funktionen der vRealize Orchestrator-Plattform erweitern, indem Sie benutzerdefinierte Plug-Ins installieren.

Sie können Plug-Ins auf der Seite **Plug-Ins verwalten** von vRealize Orchestrator installieren oder aktualisieren. Bei der Dateierweiterung, die verwendet werden kann, handelt es sich um `.vmoapp`.

Weitere Informationen zum Installieren oder Aktualisieren von vRealize Orchestrator-Plug-Ins finden Sie unter [Installieren oder Aktualisieren eines vRealize Orchestrator-Plug-Ins](#).

Ändern der Protokollierungsebene für Plug-Ins

Anstatt die Protokollierungsebene für vRealize Orchestrator zu ändern, können Sie dies lediglich für bestimmte Plug-Ins tun.

Deaktivieren von Plug-Ins

Sie können ein Plug-In deaktivieren, indem Sie die Markierung des Kontrollkästchens **Plug-In aktivieren** neben seinem Namen löschen.

Mit dieser Aktion wird die Plug-In-Datei nicht entfernt. Weitere Informationen zum Deinstallieren eines Plug-Ins in vRealize Orchestrator finden Sie unter [Löschen eines Plug-Ins](#).

Installieren oder Aktualisieren eines vRealize Orchestrator-Plug-Ins

Sie können Plug-Ins von Drittanbietern über das Control Center von vRealize Orchestrator installieren oder aktualisieren.

Voraussetzungen

Laden Sie die `.dar`- oder die `.vmoapp`-Datei des Plug-Ins herunter.

Hinweis Das bevorzugte Dateiformat für vRealize Orchestrator-Plug-Ins ist `.vmoapp`.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Wählen Sie die Seite **Plug-Ins verwalten**.
- 3 Klicken Sie auf **Durchsuchen** und wählen Sie die `.dar`- oder `.vmoapp`-Datei des Plug-Ins aus, das Sie installieren oder aktualisieren möchten.
- 4 Klicken Sie auf **Hochladen**.

- Überprüfen Sie die Plug-In-Informationen, sofern zutreffend, akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Installieren**.

Das Plug-In wird installiert oder aktualisiert und der vRealize Orchestrator-Serverdienst wird neu gestartet.

Nächste Schritte


Überprüfen Sie auf der Seite **Plug-Ins verwalten**, ob dort die richtigen Plug-In-Informationen aufgeführt sind.

Löschen eines Plug-Ins

Sie können Plug-Ins von Drittanbietern über das Control Center von vRealize Orchestrator Appliance löschen.

Hinweis Ab vRealize Orchestrator 8.0 wird das Plug-In-Paket nicht mehr manuell aus dem vRealize Orchestrator Client gelöscht.

Verfahren

- Melden Sie sich beim Control Center als **root** an.
- Wählen Sie **Plug-Ins verwalten** aus.
- Suchen Sie nach dem Plug-In, das Sie löschen möchten, und klicken Sie auf das Symbol Löschen ().
- Bestätigen Sie, dass Sie das Plug-In löschen möchten, und klicken Sie auf **Löschen**.

Ergebnisse

Sie haben das Plug-In aus der vRealize Orchestrator Appliance gelöscht.

vRealize Orchestrator-Hochverfügbarkeit

Um die Verfügbarkeit der vRealize Orchestrator-Dienste zu steigern, starten Sie mehrere Instanzen des vRealize Orchestrator-Servers in einem Cluster mit einer gemeinsamen Datenbank. vRealize Orchestrator wird als einzelne Instanz ausgeführt, bis es für den Einsatz als Bestandteil eines Clusters konfiguriert wird.

Mehrere Instanzen des vRealize Orchestrator-Servers mit identischen Server- und Plug-In-Konfigurationen werden zusammen in einem Cluster eingesetzt und nutzen dieselbe Datenbank.

Alle Instanzen des vRealize Orchestrator-Servers kommunizieren miteinander, indem sie Taktsignale austauschen. Jedes Taktsignal ist ein Zeitstempel, den der Knoten in einem gegebenen Zeitintervall in die gemeinsame Datenbank des Clusters schreibt. Netzwerkprobleme, ein nicht reagierender Datenbankserver oder Überlastung können dazu führen, dass ein vRealize Orchestrator-Clusterknoten nicht mehr reagiert. Wenn eine aktive Instanz des vRealize Orchestrator-Servers keine Taktsignale innerhalb des Standardintervalls für Zeitüberschreitung

sendet, wird angenommen, dass sie nicht reagiert. Das Standardintervall für Zeitüberschreitung entspricht dem Wert des Taktsignalintervalls multipliziert mit der Anzahl der Failover-Taktsignale. Es dient zur Definition eines unzuverlässigen Knotens und kann entsprechend den verfügbaren Ressourcen und der Produktionsauslastung angepasst werden.

Wenn die Verbindung eines vRealize Orchestrator-Knotens zu Datenbank verloren geht, wird er in den Standby-Modus geschaltet und verbleibt in diesem Zustand, bis die Datenbankverbindung wiederhergestellt wird. Die anderen Knoten im Cluster übernehmen die aktiven Aufgaben, indem sie alle unterbrochenen Workflows aus ihren letzten nicht abgeschlossenen Elementen wiederaufnehmen, z. B. skriptfähige Aufgaben oder Workflowaufrufe.

Sie können den Zustand Ihres vRealize Orchestrator-Clusters über die Registerkarte **System** des vRealize Orchestrator Client-Dashboards überwachen. Um das Cluster-Taktsignal, die Anzahl der Failover-Taktsignale und die Anzahl der aktiven Knoten zu konfigurieren, navigieren Sie zur Seite **Verwaltung des Orchestrator-Clusters** des vRealize Orchestrator Control Center.

vRealize Orchestrator-Maximalwerte für die Skalierbarkeit

In der Tabelle für den Skalierbarkeitsgrenzwert werden die empfohlenen Maximalwerte für vRealize Orchestrator 8.x-Bereitstellungen beschrieben.

| Komponente | Skalierungsziele | Weitere Informationen |
|---|-------------------|---|
| Virtuelle Maschinen | 35.000 | |
| vCenter Server-Verbindungen | 10 | Weitere Informationen hierzu finden Sie unter Einrichtung von vCenter Server |
| Aktive Knoten in einem Cluster | 3 | Weitere Informationen hierzu finden Sie unter Konfigurieren eines vRealize Orchestrator-Clusters |
| Gleichzeitig laufende Workflows | 300 pro Knoten | Weitere Informationen hierzu finden Sie unter Konfigurieren der Workflow-Ausführungseigenschaften |
| In der Warteschlange befindliche laufende Workflows | 10.000 pro Knoten | |
| Beibehaltene Workflow-Runs | 100 pro Knoten | |
| Ablauf von Protokollereignissen (in Tagen) | 15 | |

Konfigurieren eines vRealize Orchestrator-Clusters

Sie können Ihre neue vRealize Orchestrator-Bereitstellung so konfigurieren, dass sie in Hochverfügbarkeit ausgeführt wird, indem Sie drei Knoten bereitstellen und als Cluster verbinden.

Ein vRealize Orchestrator-Cluster besteht aus drei vRealize Orchestrator-Instanzen, die eine PostgreSQL-Datenbank gemeinsam nutzen. Die Datenbank des konfigurierten vRealize Orchestrator-Clusters kann nur im asynchronen Modus ausgeführt werden.

Um einen vRealize Orchestrator-Cluster zu erstellen, müssen Sie eine vRealize Orchestrator-Instanz als primären Knoten des Clusters auswählen. Nachdem Sie den primären Knoten konfiguriert haben, fügen Sie ihm die sekundären Knoten hinzu.

Der erstellte vRealize Orchestrator-Cluster ist mit automatischem Failover vorkonfiguriert.

Hinweis Der Ausfall des automatischen Failovers kann zum Verlust von Datenbankdaten führen.

Voraussetzungen

- Laden Sie drei eigenständige vRealize Orchestrator-Instanzen herunter und stellen Sie sie bereit. Weitere Informationen finden Sie unter [Herunterladen und Bereitstellen der vRealize Orchestrator Appliance](#).

Hinweis Die empfohlene Anzahl der Knoten, die zum Erstellen einer vRealize Orchestrator-Clusterumgebung verwendet werden können, ist drei.

- Stellen Sie sicher, dass der SSH-Zugriff für alle vRealize Orchestrator-Knoten aktiviert ist. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren des SSH-Zugriffs auf die vRealize Orchestrator Appliance](#).
- Konfigurieren Sie einen Lastausgleichsserver. Weitere Informationen finden Sie im [Handbuch für den Lastausgleich von VMware vRealize Orchestrator 8.x](#).

Verfahren

1 Konfigurieren Sie den primären Knoten.

- a Melden Sie sich bei der vRealize Orchestrator Appliance-Befehlszeile des primären Knotens über SSH als **root** an.
- b Um den Lastausgleichsserver des Clusters zu konfigurieren, führen Sie den Befehl `vracli load-balancer set load_balancer_FQDN` aus.
- c Melden Sie sich beim Control Center des primären Knotens an und wählen Sie **Hosteinstellungen** aus.
- d Klicken Sie auf **Ändern** und legen Sie die Hostadresse des verbundenen Lastausgleichsservers fest.
- e Konfigurieren Sie den Authentifizierungsanbieter. Weitere Informationen finden Sie unter [Konfigurieren eines eigenständigen vRealize Orchestrator-Servers](#).

2 Verbinden Sie sekundäre Knoten mit dem primären Knoten.

- a Melden Sie sich bei der vRealize Orchestrator Appliance-Befehlszeile des sekundären Knotens über SSH als **root** an.
- b Um den sekundären Knoten mit dem primären Knoten zu verbinden, führen Sie den Befehl `vracli cluster join primary_node_hostname_or_IP` aus.
- c Geben Sie das Root-Kennwort des primären Knotens ein.
- d Wiederholen Sie den Vorgang für einen anderen sekundären Knoten.

- 3 (Optional) Wenn Ihr primärer Knoten ein benutzerdefiniertes Zertifikat verwendet, müssen Sie entweder das Zertifikat in der Appliance festlegen oder ein neues Zertifikat generieren. Weitere Informationen finden Sie unter [Generieren eines benutzerdefinierten TLS-Zertifikats für vRealize Orchestrator](#).

Hinweis Die Datei, die die Zertifikatskette enthält, muss PEM-codiert sein.

- 4 Beenden Sie die Cluster-Bereitstellung.
 - a Melden Sie sich bei der vRealize Orchestrator Appliance-Befehlszeile des primären Knotens über SSH als **root** an.
 - b Um zu bestätigen, dass alle Knoten den Status „Bereit“ aufweisen, führen Sie den Befehl `kubectl -n prelude get nodes` aus.
 - c Führen Sie das Skript `/opt/scripts/deploy.sh` aus und warten Sie, bis die Bereitstellung abgeschlossen ist.

Ergebnisse

Sie haben einen vRealize Orchestrator-Cluster erstellt. Nach dem Erstellen des Clusters können Sie nur über die FQDN-Adresse Ihres Lastausgleichsservers auf Ihre vRealize Orchestrator-Umgebung zugreifen.

Hinweis Da Sie nur mit dem Root-Kennwort des Lastausgleichsdiensts auf das Control Center des Clusters zugreifen können, können Sie die Konfiguration eines Clusterknotens nicht bearbeiten, wenn er über ein anderes Root-Kennwort verfügt. Um die Konfiguration dieses Knotens zu bearbeiten, entfernen Sie ihn aus dem Lastausgleichsdienst, bearbeiten Sie die Konfiguration im Control Center und fügen Sie den Knoten wieder zum Lastausgleichsdienst hinzu.

Nächste Schritte

Um den Status des vRealize Orchestrator-Clusters zu überwachen, melden Sie sich beim vRealize Orchestrator Client an und navigieren Sie zur Registerkarte **System** des Dashboards. Weitere Informationen finden Sie unter [Überwachen eines vRealize Orchestrator-Clusters](#).

Entfernen eines vRealize Orchestrator-Clusterknotens

Sie können vRealize Orchestrator löschen, um Ihre Clusterkapazität zu reduzieren.

Nach dem Entfernen eines Knotens aus dem vRealize Orchestrator-Cluster ist dieser Knoten nicht mehr funktionsfähig. Wenn Sie diesen Knoten erneut verwenden möchten, müssen Sie dessen vRealize Orchestrator Appliance aus vCenter Server löschen und erneut bereitstellen. Weitere Informationen finden Sie unter [Herunterladen und Bereitstellen der vRealize Orchestrator Appliance](#).

Voraussetzungen

Erstellen Sie einen vRealize Orchestrator-Cluster. Weitere Informationen finden Sie unter [Konfigurieren eines vRealize Orchestrator-Clusters](#).

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance des Knotens an, den Sie als **root** entfernen möchten.
- 2 Um den Knoten aus Ihrem vRealize Orchestrator zu entfernen, führen Sie den Befehl `vracli cluster leave` aus.
- 3 Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance eines der verbleibenden Knoten als **root** an.
- 4 Führen Sie den Befehl `kubectl -n prelude get nodes` aus und bestätigen Sie, dass der entfernte Knoten nicht mehr Teil des Clusters ist.

Horizontales Skalieren einer eigenständigen vRealize Orchestrator-Bereitstellung

Sie können die Verfügbarkeit und Skalierbarkeit Ihrer konfigurierten vRealize Orchestrator-Bereitstellung erhöhen, indem Sie sie skalieren.

Voraussetzungen

- Laden Sie eine vRealize Orchestrator-Instanz herunter, stellen Sie sie bereit und konfigurieren Sie sie. Weitere Informationen finden Sie unter [Herunterladen und Bereitstellen der vRealize Orchestrator Appliance](#) und [Konfigurieren eines eigenständigen vRealize Orchestrator-Servers](#).
- Laden Sie zwei zusätzliche vRealize Orchestrator-Instanzen herunter und stellen Sie sie bereit. Weitere Informationen finden Sie unter [Herunterladen und Bereitstellen der vRealize Orchestrator Appliance](#).
- Konfigurieren Sie einen Lastausgleichsserver. Weitere Informationen finden Sie im [Handbuch für den Lastausgleich von VMware vRealize Orchestrator 8.x](#).

Verfahren

- 1 Konfigurieren Sie den primären Knoten.
 - a Melden Sie sich beim Control Center Ihrer konfigurierten vRealize Orchestrator-Bereitstellung als **root** an.
 - b Wählen Sie **Authentifizierungsanbieter konfigurieren** aus und heben Sie die Registrierung Ihres Authentifizierungsanbieters auf.
 - c Wählen Sie **Hosteinstellungen** aus und geben Sie den Hostnamen des Lastausgleichsservers ein.
 - d Wählen Sie **Authentifizierungsanbieter konfigurieren** aus und registrieren Sie Ihren Authentifizierungsanbieter erneut.
 - e Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance der konfigurierten Instanz als **root** an.

- f Um alle Dienste der vRealize Orchestrator-Instanz zu beenden, führen Sie den Befehl `/opt/scripts/deploy.sh --onlyClean` aus.
- g Um den Lastausgleichsdienst festzulegen, führen Sie `vracli load-balancer set load_balancer_FQDN` aus.
- h (Optional) Wenn Ihre vRealize Orchestrator-Instanz ein benutzerdefiniertes Zertifikat verwendet, führen Sie den Befehl `vracli certificate ingress --set your_cert_file.pem` aus.

Hinweis Die Datei, die die Zertifikatskette enthält, muss PEM-codiert sein.

- 2 Verknüpfen Sie sekundäre Knoten mit der konfigurierten Instanz.
 - a Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance des sekundären Knotens als **root** an.
 - b Um den sekundären Knoten mit der konfigurierten Instanz zu verbinden, führen Sie den Befehl `vracli cluster joinprimary_node_hostname_or_IP` aus.
 - c Wiederholen Sie den Vorgang für den anderen sekundären Knoten.
- 3 Beenden Sie den Prozess für die horizontale Skalierung.
 - a Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance der konfigurierten Instanz als **root** an.
 - b Führen Sie `/opt/scripts/deploy.sh` aus und warten Sie, bis das Skript abgeschlossen ist.

Ergebnisse

Sie haben Ihre vRealize Orchestrator-Bereitstellung horizontal skaliert.

Überwachen eines vRealize Orchestrator-Clusters

Sie können Ihren vorhandenen vRealize Orchestrator-Cluster über die Registerkarte **System** des vRealize Orchestrator Client-Dashboards überwachen.

Die empfohlene Methode zur Überwachung der Konfigurationssynchronisierungszustände der vRealize Orchestrator-Instanzen erfolgt über die Registerkarte **System** des vRealize Orchestrator Client-Dashboards.

Hinweis Wenn Sie nicht auf das vRealize Orchestrator Client-Dashboard zugreifen können, können Sie auch die Zustände Ihrer vRealize Orchestrator-Instanzen überwachen, indem Sie den Befehl `kubect1 get pods -n prelude` über die Befehlszeile von vRealize Orchestrator Appliance ausführen.

| Konfigurations-Synchronisierungszustand | Beschreibung |
|--|---|
| WIRD AUSGEFÜHRT | Der vRealize Orchestrator-Dienst ist verfügbar und kann Anforderungen annehmen. |
| STANDBY | <p>Der vRealize Orchestrator-Dienst kann aus folgenden Gründen keine Anforderungen verarbeiten:</p> <ul style="list-style-type: none"> ■ Der Knoten ist Teil eines HA-Clusters (HA = High Availability, Hochverfügbarkeit) und bleibt im Standby-Modus, bis der primäre Knoten ausfällt. ■ Der Dienst kann die Konfigurationsvoraussetzungen – z. B. eine gültige Verbindung zur Datenbank, den Authentifizierungsanbieter und die Lizenz für die vRealize Orchestrator-Instanz – nicht prüfen. |
| Abrufen des Zustandsstatus des Dienstes fehlgeschlagen | Der vRealize Orchestrator-Serverdienst kann nicht kontaktiert werden, da er entweder gestoppt wurde oder ein Netzwerkproblem besteht. |
| Ausstehender Neustart | Control Center erkennt eine Änderung der Konfiguration und der vRealize Orchestrator-Server wird automatisch neu gestartet. |

Konfigurieren des Programms zur Verbesserung der Benutzerfreundlichkeit

Wenn Sie sich für die Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) entscheiden, erhält VMware anonyme Daten zur Verbesserung der Qualität, Zuverlässigkeit und Funktionalität der VMware-Produkte und -Dienste.

Kategorien von Daten, die VMware erhält

Das Programm zur Verbesserung der Benutzerfreundlichkeit von VMware (Customer Experience Improvement Program, CEIP) liefert VMware Informationen, die es VMware ermöglichen, seine Produkte und Dienste zu verbessern und Probleme zu beheben.

Einzelheiten zu den über das CEIP erfassten Daten und warum sie von VMware erhoben werden, finden Sie im „Trust & Assurance Center“ unter <http://www.vmware.com/trustvmware/ceip.html>. Unter [Teilnehmen am Programm zur Verbesserung der Benutzerfreundlichkeit](#) bzw. [Verlassen des Programms](#) finden Sie Informationen, wie Sie am CEIP für dieses Produkt teilnehmen oder es verlassen können.

Teilnehmen am Programm zur Verbesserung der Benutzerfreundlichkeit bzw. Verlassen des Programms

Nehmen Sie am Programm zur Verbesserung der Benutzerfreundlichkeit über die Befehlszeile der vRealize Orchestrator Appliance teil.

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance als **root** an.
- 2 Um am Programm zur Verbesserung der Benutzerfreundlichkeit teilzunehmen, 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 Starten Sie die vRealize Orchestrator-Dienste neu.
 - a Um den Serverdienst neu zu starten, führen Sie den Befehl `kubect1 -n prelude exec -it your_vro_pod-c vco-server-app /bin/bash` aus.
 - b Um den Dienst zu beenden, führen Sie den Befehl `kill 1` aus.
 - c Um den Control Center-Dienst neu zu starten, führen Sie den Befehl `kubect1 -n prelude exec -it your_vro_pod-c vco-controlcenter-app /bin/bash` aus.
 - d Um den Dienst zu beenden, führen Sie den Befehl `kill 1` aus.
- 5 Um das Programm zur Verbesserung der Benutzerfreundlichkeit zu verlassen, führen Sie den Befehl `vracli ceip off` aus.
- 6 Wiederholen Sie die Schritte für den Neustart der Dienste.

Verwenden der vRealize Orchestrator-API-Dienste

6

Neben der Konfiguration von vRealize Orchestrator mithilfe von Control Center können Sie die Konfigurationseinstellungen für vRealize Orchestrator-Server mithilfe der vRealize Orchestrator-REST-API, der Control Center-REST-API oder des Befehlszeilen-Dienstprogramms ändern, die in der Appliance enthalten sind.

Das Konfigurations-Plug-In ist standardmäßig im vRealize Orchestrator-Paket enthalten. Sie können über die vRealize Orchestrator-Workflow-Bibliothek oder die vRealize Orchestrator-REST-API auf die Workflows des Konfigurations-Plug-Ins zugreifen. Mit diesen Workflows können Sie die Einstellungen für vertrauenswürdiges Zertifikat und den Keystore des vRealize Orchestrator-Servers ändern. Informationen zu allen verfügbaren vRealize Orchestrator-REST-API-Dienstaufrufen finden Sie in der Dokumentation zu *vRealize Orchestrator-Server-API* unter https://your_orchestrator_FQDN/vco/api/docs.

■ Verwalten von TLS-Zertifikaten und Keystores mithilfe der REST-API

Neben der Verwaltung von TLS-Zertifikaten mithilfe von Control Center können Sie auch vertrauenswürdige Zertifikate und Keystores verwalten, wenn Sie Workflows über das Konfigurations-Plug-In oder mithilfe der REST-API ausführen.

Verwalten von TLS-Zertifikaten und Keystores mithilfe der REST-API

Neben der Verwaltung von TLS-Zertifikaten mithilfe von Control Center können Sie auch vertrauenswürdige Zertifikate und Keystores verwalten, wenn Sie Workflows über das Konfigurations-Plug-In oder mithilfe der REST-API ausführen.

Das Konfigurations-Plug-In enthält Workflows zum Importieren und Löschen von TLS-Zertifikaten und Keystores. Sie können auf diese Workflows zugreifen, indem Sie zu **Bibliothek > Workflows > SSL Trust Manager** und **Bibliothek > Workflows > Keystores** im vRealize Orchestrator Client navigieren. Sie können diese Workflows auch mithilfe der vRealize Orchestrator-REST-API ausführen.

Die Control Center-REST-API bietet Zugriff auf Ressourcen für die Konfiguration des vRealize Orchestrator-Servers. Sie können die Control Center-REST-API mit Systemen von Drittanbietern verwenden, um die vRealize Orchestrator-Konfiguration zu automatisieren. Der Root-Endpoint der Control Center-RESTAPI ist `https://your_orchestrator_FQDN/vco/api`. Informationen zu allen verfügbaren Dienstaufrufen, die Sie an der Control Center-REST-API vornehmen können, finden Sie in der Dokumentation zur *vRealize Orchestrator Control Center-API* unter `https://your_orchestrator_FQDN/vco-controlcenter/docs`.

Löschen eines TLS-Zertifikats mithilfe der REST-API

Sie können ein TLS-Zertifikat löschen, indem Sie den Workflow zum Löschen eines vertrauenswürdigen Zertifikats des Konfigurations-Plug-Ins ausführen oder indem Sie die REST-API verwenden.

Verfahren

- 1 Stellen Sie eine `GET`-Anforderung an der URL des Workflow-Diensts des Workflows zum Löschen vertrauenswürdiger Zertifikate.

```
GET https://{Orchestrator_Host}:{Port}/vco/api/workflows?conditions=name=Delete trusted certificate
```

- 2 Rufen Sie die Definition des Workflows zum Löschen vertrauenswürdiger Zertifikate ab, indem Sie eine `GET`-Anforderung unter der URL der Definition ausführen.

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

- 3 Führen Sie eine `POST`-Anforderung unter der URL aus, die die Ausführungsobjekte des Workflows zum Löschen vertrauenswürdiger Zertifikate enthält.

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

- 4 Geben Sie den Namen des Zertifikats, das Sie löschen möchten, als Eingabeparameter des Workflows zum Löschen vertrauenswürdiger Zertifikate in einem Ausführungskontextelement im Hauptteil der Anforderung an.

Importieren von TLS-Zertifikaten mithilfe der REST-API

Sie können TLS-Zertifikate mit einem Workflow des Konfigurations-Plug-Ins oder über die REST-API importieren.

Sie können ein vertrauenswürdiges Zertifikat aus einer Datei oder von einer URL importieren. Weitere Informationen hierzu finden Sie unter [Importieren eines vertrauenswürdigen Zertifikats über Control Center](#)

Verfahren

- 1 Führen Sie eine `GET`-Anforderung unter der URL für den Workflowdienst aus.

| Option | Beschreibung |
|---|--|
| Vertrauenswürdigen Zertifikat aus Datei importieren | Importiert ein vertrauenswürdigen Zertifikat aus einer Datei. |
| Vertrauenswürdigen Zertifikat von einer URL importieren | Importiert ein vertrauenswürdigen Zertifikat von einer URL-Adresse. |
| Vertrauenswürdigen Zertifikat mithilfe eines Proxy-Servers von einer URL importieren | Importiert ein vertrauenswürdigen Zertifikat unter Nutzung eines Proxyservers von einer URL-Adresse. |
| Vertrauenswürdigen Zertifikat mit Zertifikatalias von einer URL importieren | Importiert ein vertrauenswürdigen Zertifikat mit einem Zertifikatalias von einer URL-Adresse. |

Führen Sie zum Importieren eines vertrauenswürdigen Zertifikats aus einer Datei die folgende `GET`-Anforderung aus:

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

- 2 Rufen Sie die Definition des Workflows ab, indem Sie eine `GET`-Anforderung unter der URL der Definition ausführen.

Führen Sie zum Abrufen der Definition des Workflows „Vertrauenswürdigen Zertifikat aus Datei importieren“ die folgende `GET`-Anforderung aus:

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

- 3 Führen Sie eine `POST`-Anforderung unter der URL aus, die die Ausführungsobjekte des Workflows enthält.

Führen Sie für den Workflow zum Importieren eines vertrauenswürdigen Zertifikats aus einer Datei die folgende `POST`-Anforderung aus:

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

- 4 Geben Sie in einem Ausführungskontextelement im Hauptteil der Anforderung Werte für die Eingabeparameter des Workflows an.

| Parameter | Beschreibung |
|------------|---|
| cer | Die CER-Datei, aus der das TLS-Zertifikat importiert werden soll. Dieser Parameter ist auf den Workflow zum Importieren eines vertrauenswürdigen Zertifikats aus einer Datei anwendbar. |
| url | Die URL, von der Sie das TLS-Zertifikat importieren möchten. Für Nicht-HTTPS-Dienste wird das Format <i>IP_Adresse_oder_DNS_Name:Port</i> unterstützt. Dieser Parameter ist auf den Workflow zum Importieren eines vertrauenswürdigen Zertifikats von einer URL anwendbar. |

Erstellen eines Keystore mithilfe der REST-API

Sie können einen Keystore mit dem Workflow „Keystore erstellen“ des Konfigurations-Plug-Ins oder über die REST-API hinzufügen.

Verfahren

- 1 Führen Sie eine GET-Anforderung unter der URL für den Workflowdienst des Workflows „Keystore erstellen“ aus.

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

- 2 Rufen Sie die Definition des Workflows ab, indem Sie eine GET-Anforderung unter der URL der Definition ausführen.

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

- 3 Führen Sie eine POST-Anforderung unter der URL aus, die die Ausführungsobjekte des Workflows „Keystore erstellen“ enthält.

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

- 4 Geben Sie den Namen des zu erstellenden Keystore als Eingabeparameter des Workflows „Keystore erstellen“ in einem Ausführungskontext-Element im Hauptteil der Anforderung ein.

Löschen eines Keystore mithilfe der REST-API

Sie können einen Keystore mit dem Workflow „Keystore löschen“ des Konfigurations-Plug-Ins oder über die REST-API löschen.

Verfahren

- 1 Führen Sie eine `GET`-Anforderung unter der URL für den Workflowdienst des Workflows „Keystore löschen“ aus.

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

- 2 Rufen Sie die Definition des Workflows „Keystore löschen“ ab, indem Sie eine `GET`-Anforderung unter der URL der Definition ausführen.

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

- 3 Führen Sie eine `POST`-Anforderung unter der URL aus, die die Ausführungsobjekte des Workflows „Keystore löschen“ enthält.

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

- 4 Geben Sie den Namen des zu löschenden Keystore als Eingabeparameter des Workflows „Keystore löschen“ in einem Ausführungskontextelement im Hauptteil der Anforderung ein.

Hinzufügen eines Schlüssels mithilfe der REST-API

Sie können Schlüssel über das Konfigurations-Plug-In mit dem Workflow „Schlüssel hinzufügen“ oder mithilfe der REST-API hinzufügen.

Verfahren

- 1 Führen Sie eine `GET`-Anforderung unter der URL für den Workflowdienst des Workflows „Schlüssel hinzufügen“ aus.

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

- 2 Rufen Sie die Definition des Workflows „Schlüssel hinzufügen“ ab, indem Sie eine `GET`-Anforderung unter der URL der Definition ausführen.

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

- 3 Führe Sie eine `POST`-Anforderung unter der URL aus, die die Ausführungsobjekte des Workflows „Schlüssel hinzufügen“ enthält.

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

- 4 Geben Sie Keystore, Schlüsselalias, PEM-codierten Schlüssel, Zertifikatkette und Schlüsselkennwort als Eingabeparameter für den Workflow „Schlüssel hinzufügen“ in einem Ausführungskontextelement im Hauptteil der Anforderung ein.

Zusätzliche Konfigurationsoptionen

7

Mit dem Control Center können Sie das Standardverhalten von vRealize Orchestrator ändern.

Dieses Kapitel enthält die folgenden Themen:

- Neukonfigurieren der Authentifizierung
- Konfigurieren der Workflow-Ausführungseigenschaften
- vRealize Orchestrator-Protokolldateien
- Aktivieren der Opentracing- und Wavefront-Erweiterungen
- Aktivieren der Uhrzeitsynchronisierung für vRealize Orchestrator
- Deaktivieren der Uhrzeitsynchronisierung für vRealize Orchestrator
- Konfigurieren von vRealize Orchestrator-Kubernetes-CIDR
- Aktualisieren der DNS-Einstellungen für vRealize Orchestrator

Neukonfigurieren der Authentifizierung

Nachdem Sie die Authentifizierungsmethode während der Erstkonfiguration des Control Center eingerichtet haben, können Sie den Authentifizierungsanbieter oder die konfigurierten Parameter jederzeit ändern.

Ändern des Authentifizierungsanbieters

Wenn Sie den Authentifizierungsmodus oder die Verbindungseinstellungen des Authentifizierungsanbieters ändern möchten, müssen Sie zunächst die Registrierung des bestehenden Authentifizierungsanbieters aufheben.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Klicken Sie auf der Seite **Authentifizierungsanbieter konfigurieren** auf die Schaltfläche **REGISTRIERUNG AUFHEBEN** neben dem Textfeld für die Hostadresse, um die Registrierung des derzeit verwendeten Authentifizierungsanbieters aufzuheben.

Ergebnisse

Sie haben die Registrierung des Authentifizierungsanbieters erfolgreich aufgehoben.

Nächste Schritte

Konfigurieren Sie die Authentifizierung im Control Center neu. Weitere Informationen finden Sie unter [Konfigurieren eines eigenständigen vRealize Orchestrator-Servers](#).

Ändern der Authentifizierungsparameter

Wenn Sie vSphere als Authentifizierungsanbieter im Control Center verwenden, können Sie den Standardmandanten der vRealize Orchestrator-Administratorgruppe ändern.

Voraussetzungen

Konfigurieren Sie vSphere als Authentifizierungsanbieter für Ihre vRealize Orchestrator-Bereitstellung. Weitere Informationen finden Sie unter [Konfigurieren eines eigenständigen vRealize Orchestrator-Servers mit vSphere-Authentifizierung](#).

Hinweis Die vRealize Automation-Authentifizierung enthält diese Parameter nicht.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Wählen Sie **Anbieter für Authentifizierung konfigurieren** aus.
- 3 Klicken Sie auf die Schaltfläche **ÄNDERN** neben dem Textfeld **Standardmandant**.
- 4 Ersetzen Sie den Namen des Mandanten.
- 5 Klicken Sie auf die Schaltfläche **ÄNDERN** neben dem Textfeld **Admin-Gruppe**.

Hinweis Wenn Sie die Administratorgruppe nicht neu konfigurieren, bleibt sie leer, und Sie können nicht mehr auf das Control Center zugreifen.

- 6 Geben Sie den Namen einer Administratorgruppe ein und klicken Sie auf **SUCHEN**.
- 7 Wählen Sie eine Administratorgruppe aus.
- 8 Ändern Sie die Administratorgruppe.
- 9 Um die Bearbeitung der Authentifizierungsparameter abzuschließen, klicken Sie auf **ÄNDERUNGEN SPEICHERN**.

Konfigurieren der Workflow-Ausführungseigenschaften

Sie können standardmäßig 300 Workflows pro Knoten ausführen. Wenn die Anzahl der laufenden Workflows erreicht ist, können 10.000 Workflows in die Warteschlange gestellt werden.

Wenn der vRealize Orchestrator-Knoten mehr als 300 Workflows gleichzeitig ausführen muss, werden die ausstehenden Workflow-Ausführungen in eine Warteschlange gestellt. Wenn die Ausführung eines aktiven Workflows abgeschlossen ist, beginnt die Ausführung des nächsten Workflows in der Warteschlange. Ist die maximale Anzahl von Workflows in der Warteschlange erreicht, schlagen die Ausführungen der folgenden Workflows fehl, bis einer der Workflows aus der Warteschlange ausgeführt wird.

Sie können die Workflow-Ausführungseigenschaften auf der Seite **Erweiterte Optionen** im Control Center konfigurieren.

| Option | Beschreibung |
|---|---|
| Abgesicherten Modus aktivieren | Wenn der abgesicherte Modus aktiviert ist, werden alle laufenden Workflows abgebrochen. Sie werden nicht beim nächsten Start des vRealize Orchestrator-Knotens fortgesetzt. |
| Anzahl gleichzeitig laufender Workflows | Die Anzahl der Workflows, die gleichzeitig ausgeführt werden. Die Standardeinstellung ist 300 Workflows pro Knoten. |
| Maximale Anzahl laufender Workflows in der Warteschlange | Die Anzahl von Workflow-Ausführungsanforderungen, die der vRealize Orchestrator-Server akzeptiert, bevor er nicht mehr verfügbar ist. Die Standardeinstellung ist 10.000 Workflows pro Knoten. |
| Maximale Anzahl gespeicherter Ausführungen pro Workflow | Die maximale Anzahl abgeschlossener Workflow-Durchläufe, die pro Workflow als Verlauf beibehalten werden. Wenn die Anzahl überschritten wird, werden die ältesten Workflow-Runs gelöscht. Die Standardeinstellung ist 100 Ausgeführte pro Workflow. |
| Ablauf von Protokollereignissen (in Tagen) | Anzahl der Tage, die Protokollereignisse in der Datenbank bleiben, bevor sie gelöscht werden. Die Standardeinstellung ist 15 Tage. |

vRealize Orchestrator-Protokolldateien

Der technische Support von VMware fordert routinemäßig Diagnosedaten an, wenn Sie eine Supportanforderung senden. Diese Diagnosedaten enthalten produktspezifische Protokolle und Konfigurationsdateien des Hosts, auf dem das Produkt ausgeführt wird.

vRealize Orchestrator Appliance-Protokolle werden im Verzeichnis `/data/vco/usr/lib/vco/app-server/logs/` gespeichert. Sie exportieren die Protokolle Ihrer vRealize Orchestrator Appliance-Bereitstellung, indem Sie sich bei der Appliance-Befehlszeile anmelden und den Befehl `vracli log-bundle` ausführen. Das generierte Protokollpaket wird im Root-Ordner Ihrer vRealize Orchestrator Appliance gespeichert.

Protokollierungspersistenz

Sie können Informationen in jeder Art von vRealize Orchestrator-Skript protokollieren, z. B. Workflow, Richtlinie oder Aktion. Diese Informationen weisen Typen und Ebenen auf. Der Typ kann entweder persistent oder nicht persistent sein. Die Ebene kann `DEBUG`, `INFO`, `WARN`, `ERROR`, `TRACE` und `FATAL` sein.

Tabelle 7-1. Erstellen persistenter und nicht persistenter Protokolle

| Protokollierungsebene | Persistenter Typ | Nicht persistenter Typ |
|-----------------------|---------------------------------------|------------------------|
| DEBUG | Server.debug("Kurztext", "Langtext"); | System.debug("Text") |
| INFO | Server.log("Kurztext", "Langtext"); | System.log("Text"); |
| WARN | Server.warn("Kurztext", "Langtext"); | System.Warn ("Text"); |
| ERROR | Server.error("Kurztext", "Langtext"); | System.error("Text"); |

Persistente Protokolle

Persistente Protokolle (Serverprotokolle) verfolgen vergangene Workflow-Ausführungsprotokolle und werden in der vRealize Orchestrator-Datenbank gespeichert.

Nicht persistente Protokolle

Wenn Sie ein nicht persistentes Protokoll (Systemprotokoll) zum Erstellen von Skripten verwenden, benachrichtigt der vRealize Orchestrator-Server alle laufenden vRealize Orchestrator-Anwendungen über dieses Protokoll. Diese Informationen werden jedoch nicht in der Datenbank gespeichert. Wenn die Anwendung neu gestartet wird, gehen die Protokollinformationen verloren. Nicht persistente Protokolle werden für Debugging-Zwecke und für Live-Informationen verwendet. Um Systemprotokolle anzuzeigen, müssen Sie eine abgeschlossene Workflow-Ausführung im vRealize Orchestrator Client auswählen und die Registerkarte **Protokolle** auswählen.

Konfiguration der vRealize Orchestrator-Protokolle

Auf der Seite **Protokolle konfigurieren** im Control Center können Sie die benötigte Serverprotokollierungsebene und das Skriptprotokoll festlegen. Wird eines der Protokolle mehrmals täglich generiert, ist es schwierig, die Ursachen von Problemen zu ermitteln.

Die standardmäßige Server- und Skriptprotokollierungsebene ist `INFO`. Änderungen der Protokollierungsebene wirken sich auf alle neuen Meldungen, die der Server in die Protokolle einträgt, sowie auf die Anzahl der aktiven Verbindungen zur Datenbank aus. Die Ausführlichkeit der Protokolle nimmt mit absteigender Reihenfolge ab.

Vorsicht Wählen Sie die Protokollierungsebene `DEBUG` oder `ALL` nur für Debugging-Zwecke. Verwenden Sie diese Einstellungen nicht in Produktionsumgebungen, da sie die Leistung erheblich beeinträchtigen können.

vRealize Orchestrator-Protokolle erstellen

Sie können die Protokolle Ihrer Bereitstellung exportieren, indem Sie sich bei der vRealize Orchestrator Appliance-Befehlszeile als **root** anmelden und den Befehl `vracli log-bundle` ausführen. Das generierte Protokollpaket wird im Root-Ordner der Appliance gespeichert.

Hinweis Wenn Sie über mehrere vRealize Orchestrator-Instanzen in einem Cluster verfügen, enthält das Protokollpaket Protokolle aus allen vRealize Orchestrator-Instanzen im Cluster.

Konfigurieren der Protokollierungsintegration mit vRealize Log Insight

Sie können vRealize Orchestrator so konfigurieren, dass Ihre Protokollierungsinformationen an einen vRealize Log Insight-Server gesendet werden.

Sie können eine Protokollierungsintegration mit einem vRealize Log Insight-Server über die Befehlszeile der vRealize Orchestrator Appliance konfigurieren.

Hinweis Informationen zum Konfigurieren einer Protokollierungsintegration mit einem Remote-Syslog-Server finden Sie unter [Erstellen oder überschreiben einer Syslog-Integration in vRealize Orchestrator](#)

Voraussetzungen

- Konfigurieren Sie Ihren vRealize Log Insight-Server. Weitere Informationen finden Sie in der *vRealize Log Insight-Dokumentation*.
- Stellen Sie sicher, dass Ihre vRealize Log Insight-Version 4.7.1 oder höher ist.

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance als **root** an.
- 2 Um die Protokollierungsintegration mit vRealize Log Insight zu konfigurieren, führen Sie den Befehl `vracli vrli set vRLI_FQDN` aus.

Hinweis Wenn Ihre vRealize Orchestrator-Instanz ein selbstsigniertes Zertifikat verwendet, können Sie die SSL-Authentifizierung deaktivieren, indem Sie das optionale Argument `-k` oder `--insecure` hinzufügen.

Nächste Schritte

Führen Sie den Befehl `vracli vrli -h` aus, um weitere Informationen zu vRealize Log Insight-Konfigurationsoptionen zu erhalten.

Erstellen oder überschreiben einer Syslog-Integration in vRealize Orchestrator

Sie können vRealize Orchestrator so konfigurieren, dass Ihre Protokollierungsinformationen an einen oder mehrere Remote-Syslog-Server gesendet werden.

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

Die Remote-Syslog-Integration in vRealize Orchestrator unterstützt drei Verbindungstypen:

- Über UDP.
- Über TCP ohne TLS.

Hinweis Um eine Syslog-Integration ohne Verwendung von TLS zu erstellen, fügen Sie dem Befehl `vracli remote-syslog set` das Flag `--disable-ssl` hinzu.

- Über TCP mit TLS.

Informationen zum Konfigurieren einer Protokollierungsintegration mit vRealize Log Insight finden Sie unter [Konfigurieren der Protokollierungsintegration mit vRealize Log Insight](#).

Voraussetzungen

Konfigurieren Sie einen oder mehrere Remote-Syslog-Server.

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance als **root** an.
- 2 Um eine Integration mit einem Syslog-Server zu erstellen, führen Sie 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 standardmäßig der Portwert 514 verwendet.

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

- 3 (Optional) Um eine vorhandene Syslog-Integration zu überschreiben, führen Sie `vracli remote-syslog set` aus und legen Sie den Wert für das Flag `-id` auf den Namen der Integration fest, die Sie überschreiben möchten.

Hinweis Standardmäßig fordert die vRealize Orchestrator Appliance Sie auf, das Überschreiben der Syslog-Integration zu bestätigen. Um die Bestätigungsanforderung zu überspringen, fügen Sie das Flag `-f` oder `--force` dem Befehl `vracli remote-syslog set` hinzu.

Nächste Schritte

Um die aktuellen Syslog-Integrationen in der Appliance zu überprüfen, führen Sie den Befehl `vracli remote-syslog` aus.

Löschen einer Syslog-Integration in vRealize Orchestrator

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

Voraussetzungen

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

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance als **root** an.
- 2 Löschen Sie Syslog-Integrationen aus der vRealize Orchestrator Appliance.
 - a Um eine bestimmte Syslog-Integration zu löschen, führen Sie den Befehl `vracli remote-syslog unset -id Integration_name` aus.
 - b Um alle Syslog-Integrationen in der vRealize Orchestrator Appliance zu löschen, führen Sie den Befehl `vracli remote-syslog unset` ohne `-id` aus.

Hinweis Standardmäßig fordert die vRealize Orchestrator Appliance Sie auf, das Löschen aller Syslog-Integrationen zu bestätigen. Um die Bestätigungsanforderung zu überspringen, fügen Sie das Flag `-f` oder `--force` dem Befehl `vracli remote-syslog unset` hinzu.

Aktivieren der Debug-Protokollierung für Kerberos

Sie können Probleme mit dem vRealize Orchestrator-Plug-In beheben, indem Sie die vom Plug-In verwendete Konfigurationsdatei für Kerberos ändern.

Die Konfigurationsdatei für Kerberos befindet sich im Verzeichnis `/data/vco/usr/lib/vco/app-server/conf/` der vRealize Orchestrator Appliance.

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance als **root** an.
- 2 Führen Sie den Befehl `kubect1 -n prelude edit deployment vco-app` aus.
- 3 Suchen und bearbeiten Sie in der Bereitstellungsdatei die Zeichenfolge `-Djava.security.krb5.conf=/usr/lib/vco/app-server/conf/krb5.conf'`.

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

- 4 Speichern Sie die Änderungen und schließen Sie den Dateieditor.
- 5 Führen Sie den Befehl `kubect1 -n prelude get pods` aus.

Warten Sie, bis alle Pods ausgeführt werden.

6 Stellen Sie sicher, dass die Debug-Protokollierung für Kerberos aktiviert ist.

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

Stellen Sie sicher, dass die Protokolle eine ähnliche Meldung enthalten.

```
kubectl -n prelude log vco-app-5c965f9b9d-v8srd -c vco-server-app | grep krb5
12:23:05,417 INFO 011N:75 - Sysprop: java.security.krb5.conf = /usr/lib/vco/app-server/
conf/krb5.conf
12:23:05,421 INFO 011N:75 - Sysprop: sun.security.krb5.debug = true
2019-10-22 12:23:38.521+0000 [Thread-19] INFO {} [011N] Sysprop: java.security.krb5.conf
= /usr/lib/vco/app-server/conf/krb5.conf
2019-10-22 12:23:38.525+0000 [Thread-19] INFO {} [011N] Sysprop: sun.security.krb5.debug =
true
Java config name: /usr/lib/vco/app-server/conf/krb5.conf
EType: sun.security.krb5.internal.crypto.Aes256CtsHmacSha1EType
```

Aktivieren der Opentracing- und Wavefront-Erweiterungen

Die Opentracing- und Wavefront-Erweiterungen für vRealize Orchestrator bieten Tools zum Erfassen von Daten über Ihre vRealize Orchestrator-Umgebung. Sie können diese Daten für die Fehlerbehebung des Systems und der Workflows von vRealize Orchestrator verwenden.

Bevor Sie vRealize Orchestrator für die Verwendung der Opentracing- und Wavefront-Erweiterungen konfigurieren können, müssen Sie diese in der vRealize Orchestrator Appliance aktivieren.

Voraussetzungen

- Stellen Sie sicher, dass der SSH-Dienst für vRealize Orchestrator Appliance aktiviert ist. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren des SSH-Zugriffs auf die vRealize Orchestrator Appliance](#).
- Wenn Sie vorherige Versionen der Opentracing- oder Wavefront-Erweiterungen aktiviert haben, müssen Sie diese entfernen, bevor Sie die aktuelle Version aktivieren. Wenn Sie beispielsweise zuvor Version 8.1.0 der Wavefront-Erweiterung aktiviert haben, müssen Sie den Befehl `rm /data/vco/usr/lib/vco/app-server/extensions/wavefront-8.1.0.jar` ausführen.

Verfahren

- 1 Melden Sie sich bei der vRealize Orchestrator Appliance über SSH als **root** an.
- 2 Um alle verfügbaren Erweiterungen aufzulisten, führen Sie den Befehl `ls /data/vco/usr/lib/vco/app-server/extensions/` aus.
- 3 Führen Sie den folgenden Befehl aus, um die Opentracing-Erweiterung zu aktivieren.

```
mv /data/vco/usr/lib/vco/app-server/extensions/opentracing-8.7.0.jar.inactive /
data/vco/usr/lib/vco/app-server/extensions/opentracing-8.7.0.jar
```

- 4 Führen Sie den folgenden Befehl aus, um die Wavefront-Erweiterung zu aktivieren.

```
mv /data/vco/usr/lib/vco/app-server/extensions/wavefront-8.7.0.jar.inactive /
data/vco/usr/lib/vco/app-server/extensions/wavefront-8.7.0.jar
```

- 5 Melden Sie sich beim Control Center an und bestätigen Sie, dass die Erweiterungen auf der Seite **Erweiterungseigenschaften** angezeigt werden.

Nächste Schritte

Konfigurieren Sie die Opentracing- und Wavefront-Integration mit vRealize Orchestrator auf der Seite **Erweiterungseigenschaften**. Weitere Informationen finden Sie unter [Konfigurieren der Opentracing-Erweiterung](#) und [Konfigurieren der Wavefront-Erweiterung](#).

Konfigurieren der Opentracing-Erweiterung

Die Opentracing-Erweiterung sendet Daten über Workflow-Ausführungen an einen Jaeger-Server. Zu den Daten gehören der Workflow-Status, die Eingabe-/Ausgabeparameter, welcher Benutzer die Workflow-Ausführung initiiert hat, sowie die Workflow-ID-Daten.

Voraussetzungen

- Stellen Sie sicher, dass Opentracing in der vRealize Orchestrator Appliance aktiviert ist. Weitere Informationen finden Sie unter [Aktivieren der Opentracing- und Wavefront-Erweiterungen](#).
- Stellen Sie einen Jaeger-Server für die Verwendung in der Opentracing-Erweiterung bereit. Weitere Informationen finden Sie in der Dokumentation [Erste Schritte Jaeger](#).

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Wählen Sie die Seite **Erweiterungseigenschaften** aus.
- 3 Wählen Sie die Opentracing-Erweiterung aus.
- 4 Geben Sie die Hostadresse und den Port des Jaeger-Servers ein.

Hinweis Fügen Sie zwei Schrägstriche (//) ein, bevor Sie die Serveradresse eingeben.

- 5 Klicken Sie auf **Speichern**.

Ergebnisse

Sie haben die Opentracing -Erweiterung für vRealize Orchestrator konfiguriert.

Nächste Schritte

- Um auf die Jaeger-Benutzeroberfläche zuzugreifen, die die von der Opentracing-Erweiterung erfassten Daten enthält, wechseln Sie zu der während der Konfiguration eingegebenen Hostadresse.
- Wählen Sie unter der Option **Dienst Workflows** aus.

- Um anzugeben, welche Daten angezeigt werden sollen, verwenden Sie die Option **Tags**. Um beispielsweise Daten zu fehlgeschlagenen Workflows anzuzeigen, geben Sie **status=failed** ein.

Konfigurieren der Wavefront-Erweiterung

Verwenden Sie die Wavefront-Erweiterung, um Metrikdaten zu Ihrem vRealize Orchestrator-System und Ihren -Workflows zu erfassen.

Voraussetzungen

- 1 Stellen Sie sicher, dass Wavefront in der vRealize Orchestrator Appliance aktiviert ist. Weitere Informationen finden Sie unter [Aktivieren der Opentracing- und Wavefront-Erweiterungen](#).
- 2 Importieren Sie das Wavefront-Zertifikat:
 - a Melden Sie sich beim vRealize Orchestrator-Control Center als **root** an.
 - b Wählen Sie die Seite **Zertifikate** aus.
 - c Klicken Sie auf das Dropdown-Menü **Importieren** und wählen Sie **Aus URL importieren** aus.
 - d Geben Sie die Wavefront-URL ein und klicken Sie auf **Importieren**.
- 3 Konfigurieren Sie einen Wavefront-Proxy. Weitere Informationen finden Sie unter [Installieren und Verwalten von Wavefront-Proxys](#).

Verfahren

- 1 Melden Sie sich beim vRealize Orchestrator-Control Center als **root** an.
- 2 Wählen Sie die Seite **Erweiterungseigenschaften** aus.
- 3 Wählen Sie die Wavefront-Erweiterung aus.
- 4 Konfigurieren Sie die Wavefront-Eigenschaften.

| Option | Beschreibung |
|---------------|---|
| Proxy | Die Wavefront-Proxyadresse. |
| Host | Optional. Die Wavefront-Hostadresse. |
| Token | Optional. Das Wavefront-API-Token. Weitere Informationen zum Generieren eines Wavefront-API-Tokens finden Sie unter Generieren eines API-Tokens . |
| Präfix | Fügen Sie Präfixbeschriftungen für jede an Wavefront gesendete Metrik hinzu. Präfixbeschriftungen werden durch ein Punktsymbol getrennt. |

- 5 (Optional) Klicken Sie auf **Standard-Dashboard beim nächsten Start senden**.
- 6 Klicken Sie auf **Speichern**.

Ergebnisse

Sie haben die Wavefront-Erweiterung für vRealize Orchestrator konfiguriert.

Nächste Schritte

- Um auf die von Wavefront erfassten Metriken zuzugreifen, greifen Sie auf das Dashboard der während der Konfiguration eingegebenen Adresse zu.
- Um Benachrichtigungen zu bestimmten Ereignissen in Ihrer vRealize Orchestrator-Umgebung zu erhalten, können Sie Wavefront-Warnungen verwenden. Weitere Informationen finden Sie in der [Dokumentation zu Wavefront-Warnungen](#).

Aktivieren der Uhrzeitsynchronisierung für vRealize Orchestrator

Sie können die Uhrzeitsynchronisierung in Ihrer vRealize Orchestrator-Bereitstellung mit der Befehlszeile der vRealize Orchestrator Appliance aktivieren.

Sie können die Uhrzeitsynchronisierung für Ihre eigenständige oder geclusterte vRealize Orchestrator-Bereitstellung mithilfe des NTP-Kommunikationsprotokolls (Network Time Protocol) konfigurieren. vRealize Orchestrator unterstützt zwei NTP-Konfigurationen, die sich gegenseitig ausschließen:

| NTP-Konfiguration | Beschreibung |
|-------------------|---|
| ESXi | <p>Diese Konfiguration kann verwendet werden, wenn der ESXi-Server, der die vRealize Orchestrator Appliance hostet, mit einem NTP-Server synchronisiert ist. Wenn Sie eine geclusterte Bereitstellung verwenden, müssen alle ESXi-Hosts mit einem NTP-Server synchronisiert werden. Weitere Informationen zum Konfigurieren von NTP für ESXi finden Sie unter Konfigurieren von NTP (Network Time Protocol) auf einem ESXi-Host mithilfe des vSphere Web Client.</p> <p>Hinweis Wenn die vRealize Orchestrator-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 Orchestrator-Bereitstellung zu synchronisieren.</p> <p>Hinweis Der systemd-timesyncd-Daemon ist standardmäßig aktiviert, aber ohne NFS-Server konfiguriert. Wenn die vRealize Orchestrator 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 Orchestrator 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 gesetzt 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 die Uhrzeitsynchronisierung für Ihre vRealize Orchestrator-Bereitstellung aktiviert.

Nächste Schritte

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

Deaktivieren der Uhrzeitsynchronisierung für vRealize Orchestrator

Sie können die NTP-Uhrzeitsynchronisierung (Network Time Protocol) in Ihrer vRealize Orchestrator-Bereitstellung mithilfe der Befehlszeile der vRealize Orchestrator Appliance deaktivieren.

Sie können die NTP-Konfiguration Ihrer vRealize Orchestrator Appliance auch auf den Standardzustand zurücksetzen, indem Sie den Befehl `vracli ntp reset` ausführen.

Voraussetzungen

Stellen Sie sicher, dass die Uhrzeitsynchronisierung mit ESXi oder systemd konfiguriert ist. Weitere Informationen finden Sie unter [Aktivieren der Uhrzeitsynchronisierung für vRealize Orchestrator](#).

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance als **root** an.

- 2 Um die Uhrzeitsynchronisierung mit ESXi oder systemd zu deaktivieren, führen Sie den Befehl `vracli ntp disable` aus.
- 3 (Optional) Führen Sie den Befehl `vracli ntp status` aus, um den Status der NTP-Konfiguration zu bestätigen.

Konfigurieren von vRealize Orchestrator-Kubernetes-CIDR

Sie können die CIDR-Subnetzmasken (Classless Inter-domain Routing) von Kubernetes nach der Bereitstellung ändern.

Die vRealize Orchestrator Appliance konfiguriert einen Kubernetes-Cluster und führt ihn aus. Die Pods und Dienste in diesem Cluster werden in separaten IPv4-Subnetzen bereitgestellt, die jeweils durch das interne Cluster-CIDR und das interne Dienst-CIDR dargestellt werden. Die Standardwerte der während der OVF-Bereitstellung festgelegten Subnetzmasken sind:

| Kubernetes network property | Default value | Property description |
|-----------------------------|---------------|---|
| <code>cluster-cidr</code> | 10.244.0.0/22 | Das CIDR, das für Pods verwendet wird, die innerhalb des Kubernetes-Clusters ausgeführt werden. |
| <code>service-cidr</code> | 10.244.4.0/22 | Das CIDR, das für Kubernetes-Dienste verwendet wird, die innerhalb des Kubernetes-Clusters ausgeführt werden. |

Die standardmäßigen CIDR-Netzwerkadressen können zu einem Konflikt mit externen privaten Netzwerken führen, die Sie möglicherweise verwenden. In solchen Szenarien können Sie die Konfiguration dieser CIDR-Werte entweder während oder nach der Bereitstellung Ihrer vRealize Orchestrator Appliance ändern.

Hinweis Informationen zum Ändern der CIDR-Konfiguration während der Bereitstellung der Appliance finden Sie unter [Herunterladen und Bereitstellen der vRealize Orchestrator Appliance](#).

Voraussetzungen

- Stellen Sie sicher, dass die CIDR-Adresswerte mindestens 1.024 Hosts unterstützen.
- Das interne Cluster-CIDR und das interne Dienst-CIDR dürfen nicht denselben Subnetzwert verwenden.
- Der CIDR-Wert für eines der Subnetze darf nicht den Wert enthalten, den Sie zum anderen Subnetz hinzufügen möchten.

Hinweis Beispielsweise kann der `cluster-cidr`-Wert nicht **10.244.4.0/22** **10.244.4.0/24** sein, da auch der Subnetzwert für die `service-cidr`-Eigenschaft enthalten wäre. Jeder Subnetzwert muss separat hinzugefügt werden.

Verfahren

- 1 Melden Sie sich bei der vRealize Orchestrator Appliance als **root** an.

- 2 Führen Sie den Befehl `vracli upgrade exec -y --prepare --profile k8s-subnets` aus.
- 3 Sichern Sie Ihre vRealize Orchestrator-Bereitstellung, indem Sie einen Snapshot der virtuellen Maschine (VM) erstellen. Weitere Informationen finden Sie unter [Erstellen eines Snapshot einer virtuellen Maschine](#).

Vorsicht vRealize Orchestrator 8.x unterstützt derzeit keine Arbeitsspeicher-Snapshots. Bevor Sie den Snapshot Ihrer vRealize Orchestrator-Bereitstellung erstellen, stellen Sie sicher, dass die Option **Snapshot von Zustand des Speichers der virtuellen Maschine** deaktiviert ist.

- 4 Ändern Sie die Werte der Cluster-CIDR- und Dienst-CIDR-Subnetze, indem Sie den Befehl `vracli network k8s-subnets` ausführen.

```
vracli network k8s-subnets --cluster-cidr <CIDR_value> --service-cidr <CIDR_value>
```

- 5 Um den CIDR-Konfigurationsvorgang zu beenden, führen Sie den Befehl `vracli upgrade exec` aus.

Aktualisieren der DNS-Einstellungen für vRealize Orchestrator

Ein Administrator kann die DNS-Einstellungen der vRealize Orchestrator-Bereitstellung mithilfe des Befehls `vracli network dns` aktualisieren.

Voraussetzungen

Stellen Sie sicher, dass der SSH-Dienst für vRealize Orchestrator Appliance aktiviert ist. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren des SSH-Zugriffs auf die vRealize Orchestrator Appliance](#).

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance über SSH als **root** an.

Hinweis Melden Sie sich für geclusterte Bereitstellungen bei der Appliance eines beliebigen Knotens im Cluster an.

- 2 Um neue DNS-Server für Ihre vRealize Orchestrator-Bereitstellung festzulegen, führen Sie den Befehl `vracli network dns set` aus.

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

- 3 Stellen Sie sicher, dass die neuen DNS-Server ordnungsgemäß auf alle vRealize Orchestrator Knoten angewendet werden, indem Sie den Befehl `vracli network dns status` ausführen.

- 4 Um die vRealize Orchestrator-Dienste in Ihrer Bereitstellung zu beenden, führen Sie die folgenden Befehle aus:

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

- 5 Starten Sie die vRealize Orchestrator-Knoten neu und warten Sie, bis sie vollständig gestartet wurden.
- 6 Melden Sie sich über SSH bei der Befehlszeile für jeden vRealize Orchestrator-Knoten an und stellen Sie sicher, dass die neuen DNS-Server in der Datei `/etc/resolve.conf` aufgelistet sind.
- 7 Um die vRealize Orchestrator-Dienste zu starten, führen Sie das Skript `/opt/scripts/deploy.sh` auf einem der Knoten in Ihrer Bereitstellung aus.

Ergebnisse

Die vRealize Orchestrator-DNS-Einstellungen werden wie angegeben geändert.

Anwendungsbeispiele für die Konfiguration und Fehlerbehebung

8

Die Anwendungsbeispiele für die Konfiguration bieten Aufgabenflüsse, die Sie ausführen können, um bestimmte Konfigurationsanforderungen Ihres vRealize Orchestrator-Servers zu erfüllen, sowie Fehlerbehebungsthemen zum Verstehen und Beheben von Problemen.

Dieses Kapitel enthält die folgenden Themen:

- Überprüfen der Build-Nummer des vRealize Orchestrator-Servers
- Konfigurieren des vRealize Orchestrator-Plug-Ins für vSphere Web Client
- Abbrechen laufender Workflows
- Aktivieren des vRealize Orchestrator-Server-Debuggings
- Ändern der Größe der vRealize Orchestrator Appliance-Festplatten
- Skalieren der Heap-Arbeitsspeichergröße des vRealize Orchestrator-Servers
- Notfallwiederherstellung von vRealize Orchestrator mithilfe von Site Recovery Manager

Überprüfen der Build-Nummer des vRealize Orchestrator-Servers

In bestimmten Szenarien müssen Sie möglicherweise die Server-Build-Nummer Ihrer vRealize Orchestrator-Bereitstellung überprüfen.

Sie können Ihre vRealize Orchestrator-Server-Build-Nummer überprüfen, indem Sie zu „https://your_orchestrator_FQDN/vco/api/about“ navigieren. Ihre Server-Build-Nummer wird in den `<ns2:build-number>`-Tags angezeigt.

Die Überprüfung Ihrer Server-Build-Nummer kann in Anwendungsfällen wie der Bereitstellung zusätzlicher Informationen für eine Support-Anfrage nützlich sein, die Sie beim VMware-Support angemeldet haben.

Hinweis Die Build-Nummer des vRealize Orchestrator-Servers unterscheidet sich von der Build-Nummer Ihrer vRealize Orchestrator Appliance. Um die Build-Nummer Ihrer Appliance zu überprüfen, melden Sie sich bei der vRealize Orchestrator Appliance-Befehlszeile an und führen Sie den Befehl `vracli version` aus. Wenn Sie die Build-Nummer der Appliance überprüfen, können Sie feststellen, ob Ihr Upgrade auf die neueste Version von vRealize Orchestrator erfolgreich war.

Konfigurieren des vRealize Orchestrator-Plug-Ins für vSphere Web Client

Um das vRealize Orchestrator-Plug-In für vSphere Web Client zu verwenden, müssen Sie vRealize Orchestrator als Erweiterung von vCenter Server registrieren.

Nachdem Sie den vRealize Orchestrator-Server bei vCenter Single Sign-On registriert und zum Einsatz mit vCenter Server konfiguriert haben, müssen Sie vRealize Orchestrator als Erweiterung von vCenter Server registrieren.

Voraussetzungen

- Vergewissern Sie sich, dass SSH-Zugriff für die vRealize Orchestrator Appliance aktiviert ist. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren des SSH-Zugriffs auf die vRealize Orchestrator Appliance](#).
- Sie müssen vRealize Orchestrator mit vSphere-Authentifizierung auf derselben Plattform Services Controller registrieren, mit dem sich Ihr verwalteter vCenter Server authentifiziert.
- Kopieren Sie die Datei `vco-plugin.zip` in die vRealize Orchestrator Appliance:
 - a Laden Sie die Datei `vco-plugin.zip` vom [VMware Technology Network](#) herunter.
 - b Öffnen Sie einen SSH-Client.

Hinweis Für Linux- oder MacOS-Umgebungen können Sie die Terminal-Befehlszeilenschnittstelle verwenden. Für Windows-Umgebungen können Sie den PuTTY-Client verwenden.

- c Um die Datei `vco-plugin.zip` zu kopieren, führen Sie den Secure-Copy-Befehl aus.

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

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


Verfahren

- 1 Melden Sie sich bei vRealize Orchestrator Client an.
- 2 Navigieren Sie zu **Bibliothek > Workflows**.
- 3 Suchen Sie den Workflow **vCenter Orchestrator als vCenter Server-Erweiterung registrieren** und klicken Sie auf **Ausführen**.
- 4 Wählen Sie die vCenter Server-Instanz aus, bei der vRealize Orchestrator registriert werden soll.
- 5 Geben Sie `https://your_orchestrator_FQDN` oder die Dienst-URL des Lastausgleichsdiensts ein, der die Anforderungen an die vRealize Orchestrator-Serverknoten weiterleitet.
- 6 Klicken Sie auf **Ausführen**.

Abbrechen laufender Workflows

Im Control Center von vRealize Orchestrator können Sie Workflows abbrechen, die nicht ordnungsgemäß abgeschlossen werden.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Klicken Sie auf **Fehlerbehebung**.
- 3 Brechen Sie laufende Workflows ab.

| Option | Beschreibung |
|--|---|
| Alle Workflow-Ausführungen abbrechen | Geben Sie eine Workflow-ID ein, um sämtliche Token für den betreffenden Workflow abubrechen. |
| Workflow-Ausführungen nach ID abbrechen | Geben Sie alle Token-IDs ein, die Sie abbrechen möchten. Trennen Sie die IDs durch ein Komma voneinander. |
| Alle laufenden Workflows abbrechen | Brechen Sie alle laufenden Workflows auf dem Server ab. |

Hinweis Es kann vorkommen, dass Operationen für das Abbrechen von Workflows nach ID nicht erfolgreich sind, da es keine zuverlässige Methode gibt, um den ausgeführten Thread sofort abubrechen.

Ergebnisse

Beim nächsten Serverstart werden die Workflows in einen abgebrochenen Zustand versetzt.

Aktivieren des vRealize Orchestrator-Server-Debuggings

Sie können den vRealize Orchestrator-Server im Debug-Modus starten, um Probleme beim Entwickeln eines Plug-Ins zu debuggen.

Voraussetzungen

Installieren und konfigurieren Sie das Kubernetes-Befehlszeilentool auf Ihrem lokalen Computer. Weitere Informationen finden Sie unter [Installieren und Einrichten von kubectl](#).

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance als **root** an.
- 2 Führen Sie den Befehl `kubectl -n prelude edit deployment vco-app` aus.
- 3 Bearbeiten Sie die YAML-Bereitstellungsdatei, indem Sie eine Debug-Umgebungsvariable für den Container `vco-server-app` hinzufügen. Die Variable muss im Abschnitt `env` des `vco-server-app`-Containers hinzugefügt werden.

```
containers:
  - command:
    ...
    env:
      - name: DEBUG_PORT
        value: "your_desired_debug_port"
    ...
  name: vco-server-app
  ...
```

Hinweis Wenn Sie die Debug-Umgebungsvariable zum Abschnitt `env` hinzufügen, müssen Sie die im vorherigen Beispiel dargestellte YAML-Einrückungsformatierung befolgen.

- 4 Speichern Sie die Änderungen an der Bereitstellungsdatei.
Wenn die Bearbeitung der Bereitstellungsdatei erfolgreich war, erhalten Sie die Meldung `deployment.extensions/vco-app edited`.
- 5 Generieren Sie die Kubernetes-Konfigurationsdatei, indem Sie den Befehl `vracli dev kubeconfig` ausführen.
Da `kubeconfig` eine Entwicklerumgebung ist, werden Sie aufgefordert zu bestätigen, dass Sie fortfahren möchten. Geben Sie **ja** ein, um fortzufahren, oder **nein**, um zu beenden.
- 6 Kopieren Sie den Inhalt der generierten Konfigurationsdatei von `apiVersion: v1` bis einschließlich des Inhalts `client-key-data`.
- 7 Speichern Sie die generierte Kubernetes-Konfigurationsdatei auf Ihrem lokalen Computer.
- 8 Melden Sie sich von der vRealize Orchestrator Appliance ab.

- 9 Beenden Sie die Konfiguration des Debug-Modus auf Ihrem lokalen Computer.
 - a Öffnen Sie eine Befehlszeilen-Shell.
 - b Binden Sie die *KUBECONFIG*-Umgebungsvariable an die gespeicherte Konfigurationsdatei.

Hinweis Dieses Beispiel basiert auf einer Linux-Umgebung.

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

- c Führen Sie den Befehl `kubectl cluster-info` aus, um zu überprüfen, ob die Dienste ausgeführt werden.
- d Um die Konfiguration des Debug-Modus abzuschließen, führen Sie die folgende Kubernetes-API-Anforderung aus.

Hinweis Der Wert der *localhost_debug_port*-Variablen ist der Port, der in Ihrer Remote-Debugging-Konfiguration Ihrer Integrated Development Environment (IDE) festgelegt ist. Der Wert der *vro_debug_port*-Variablen wird in Schritt 3 dieses Verfahrens generiert.

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

Wichtig Geben Sie beim Konfigurieren des Debugging-Tools die DNS- und IP-Einstellungen der lokalen Maschine an, auf der Sie den Befehl für die Portweiterleitung ausgeführt haben.

Ergebnisse

Sie haben das Server-Debugging für Ihre vRealize Orchestrator Appliance konfiguriert.

Ändern der Größe der vRealize Orchestrator Appliance-Festplatten

Sie können die Festplattengröße der vRealize Orchestrator Appliance ändern, indem Sie die Festplattengrößeneinstellungen der virtuellen vRealize Orchestrator Appliance-Maschine in vSphere bearbeiten.

Voraussetzungen

Stellen Sie sicher, dass der SSH-Dienst für vRealize Orchestrator Appliance aktiviert ist. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren des SSH-Zugriffs auf die vRealize Orchestrator Appliance](#).

Verfahren

- 1 Überprüfen Sie den aktuell verfügbaren Festplattenspeicher in der vRealize Orchestrator Appliance.

Hinweis Die vRealize Orchestrator Appliance-Festplatten benötigen mindestens 20 Prozent freien Festplattenspeicher.

- a Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance über SSH als **root** an.
 - b Führen Sie den Befehl `vracli disk-mgr` aus.
- 2 Ändern Sie die Größe der Festplatte der virtuellen vRealize Orchestrator Appliance-Maschine in vSphere.

- a Melden Sie sich beim vSphere Client als **Administrator** an.
 - b Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten** aus.
 - c Erweitern Sie auf der Registerkarte **Virtuelle Hardware** die Option **Festplatte**, um die Einstellungen für Festplatten anzuzeigen und zu ändern, und klicken Sie auf **OK**.

Weitere Informationen zum Ändern der Festplattengröße von virtuellen vSphere-Maschinen finden Sie unter *Ändern der Konfiguration der virtuellen Festplatte in Verwaltung virtueller vSphere-Maschinen*.

- 3 Lösen Sie die automatische Größenänderung im Photon OS aus.
- a Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance über SSH als **root** an.
 - b Führen Sie den Befehl `vracli disk-mgr resize` aus.

Hinweis Sie können den Fortschritt des Vorgangs zum Ändern der Festplattengröße unter `/var/log/vmware/prelude/disk_resize.log` verfolgen.

Sie haben die Größe der vRealize Orchestrator Appliance-Festplatten geändert.

- 4 Stellen Sie sicher, dass der Vorgang zum Ändern der Festplattengröße erfolgreich war, indem Sie den Befehl `disk-mgr` ausführen.

```
vracli disk-mgr
```

Nächste Schritte

Informationen zur Fehlerbehebung bei Problemen mit dem Vorgang zum Ändern der Festplattengröße finden Sie in [KB 79925](#).

Skalieren der Heap-Arbeitsspeichergröße des vRealize Orchestrator-Servers

Sie können die Heap-Arbeitsspeichergröße des vRealize Orchestrator-Servers skalieren, indem Sie ein benutzerdefiniertes Profil erstellen und die Ressourcenmetrikdatei ändern.

Sie können die Heap-Arbeitsspeichergröße des vRealize Orchestrator-Servers anpassen, damit Ihre Orchestrierungsumgebung sich ändernde Arbeitslasten verwalten kann. Beispielsweise können Sie den Heap-Arbeitsspeicher Ihrer vRealize Orchestrator-Bereitstellung erhöhen, wenn Sie vorhaben, mehrere vCenter Server zu verwalten.

Voraussetzungen

- Aktivieren Sie den SSH-Zugriff auf die vRealize Orchestrator Appliance. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren des SSH-Zugriffs auf die vRealize Orchestrator Appliance](#).
- Vergrößern Sie den Arbeitsspeicher der virtuellen Maschine, auf der vRealize Orchestrator bereitgestellt wird, bis zur nächsten geeigneten Erhöhung. Da es wichtig ist, dass ausreichend Arbeitsspeicher für die restlichen Dienste verfügbar bleibt, müssen die vRealize Orchestrator Appliance-Ressourcen zuerst vertikal hochskaliert werden. Wenn beispielsweise der gewünschte Heap-Arbeitsspeicher 7G beträgt, sollte der Arbeitsspeicher für vRealize Orchestrator Appliance um 4G erhöht werden, da der gewünschte Heap-Arbeitsspeicher abzüglich dem Standard-Heap-Wert von 3G 4G beträgt. Informationen dazu, wie Sie den Arbeitsspeicher einer virtuellen Maschine in vSphere erhöhen, finden Sie unter *Ändern der Speicherkonfiguration in Verwaltung virtueller vSphere-Maschinen*.

Verfahren

- 1 Melden Sie sich bei der vRealize Orchestrator Appliance-Befehlszeile über SSH als **root** an.
- 2 Um das benutzerdefinierte Profilverzeichnis und die erforderliche Verzeichnisstruktur zu erstellen, die verwendet wird, wenn das Profil aktiv ist, führen Sie das folgende Skript aus:

[illegible]

- 3 Bearbeiten Sie die Ressourcenmetrikdatei in Ihrem benutzerdefinierten Profil mit den gewünschten Arbeitsspeicherwerten.

```
vi /etc/vmware-prelude/profiles/custom-profile/helm/prelude_vco/90-resources.yaml
```

- 4 Speichern Sie die Änderungen an der Ressourcenmetrikdatei und führen Sie das `deploy.sh`-Skript aus.

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

Ergebnisse

Sie haben die Heap-Arbeitsspeichergröße Ihres vRealize Orchestrator-Servers geändert.

Notfallwiederherstellung von vRealize Orchestrator mithilfe von Site Recovery Manager

Sie müssen Site Recovery Manager konfigurieren, um vRealize Orchestrator zu schützen. Stellen Sie diesen Schutz sicher, indem Sie die allgemeinen Konfigurationsaufgaben für Site Recovery Manager ausführen.

Vorbereiten der Umgebung

Vor dem Konfigurieren von Site Recovery Manager müssen Sie sicherstellen, dass folgende Voraussetzungen erfüllt sind.

- Stellen Sie sicher, dass vSphere 6.0 oder höher auf den geschützten und den für die Wiederherstellung vorgesehenen Sites installiert ist.
- Stellen Sie sicher, dass Sie Site Recovery Manager 8.1 oder höher verwenden.
- Stellen Sie sicher, dass vRealize Orchestrator konfiguriert ist.

Konfigurieren virtueller Maschinen für vSphere Replication

Sie müssen die virtuellen Maschinen für vSphere Replication oder die Array-basierte Replizierung konfigurieren, um Site Recovery Manager nutzen zu können.

Führen Sie folgende Schritte aus, um vSphere Replication auf den benötigten virtuellen Maschinen zu aktivieren.

Verfahren

- 1 Wählen Sie im vSphere Web Client eine virtuelle Maschine aus, auf der vSphere Replication aktiviert werden soll, und klicken Sie auf **Aktionen > Alle vSphere Replication-Aktionen > Replizierung konfigurieren**.
- 2 Wählen Sie im Fenster **Replizierungstyp** die Option **Replizierung auf einen vCenter-Server** aus und klicken Sie auf **Weiter**.

- 3 Wählen Sie im Fenster **Ziel-Site** das vCenter für die Wiederherstellungs-Site aus und klicken Sie auf **Weiter**.
- 4 Wählen Sie im Fenster **Replizierungsserver** einen vSphere Replication Server aus und klicken Sie auf **Weiter**.
- 5 Klicken Sie im Fenster **Zielspeicherort** auf **Bearbeiten**, wählen Sie den Zieldatenspeicher, in dem die replizierten Dateien gespeichert werden sollen, und klicken Sie auf **Weiter**.
- 6 Lassen Sie die Standardwerte im Fenster **Replizierungsoptionen** unverändert und klicken Sie auf **Weiter**.
- 7 Geben Sie im Fenster **Wiederherstellungseinstellungen** die Zeit für **Recovery Point Objektive (RPO)** und **Zeitpunkt-Instanzen** ein und klicken Sie auf **Weiter**.
- 8 Überprüfen Sie die Einstellungen im Fenster **Bereit zum Abschließen** und klicken Sie dann auf **Fertig stellen**.
- 9 Wiederholen Sie diese Schritte für alle virtuellen Maschinen, auf denen vSphere Replication aktiviert sein muss.

Erstellen von Schutzgruppen

Sie können Schutzgruppen erstellen, damit Site Recovery Manager Ihre virtuellen Maschinen schützen kann.

Schutzgruppen können in Ordnern organisiert werden. Auf der Registerkarte **Schutzgruppen** werden die Namen der Schutzgruppen angezeigt. Es wird jedoch nicht angezeigt, in welchem Ordner sie sich befinden. Wenn Sie zwei Schutzgruppen mit demselben Namen in unterschiedlichen Ordnern abgelegt haben, ist es möglicherweise schwer, sie auseinanderzuhalten. Stellen Sie deshalb sicher, dass die Schutzgruppennamen ordnerübergreifend eindeutig sind. In Umgebungen, in denen nicht alle Benutzer über Ansichtsrechte für alle Ordner verfügen, legen Sie keine Schutzgruppen in Ordnern ab, um sicherzustellen, dass die Namen der Schutzgruppen eindeutig sind.

Warten Sie, wenn Sie Schutzgruppen erstellen, um sicherzugehen, dass die Vorgänge erwartungsgemäß abgeschlossen werden. Vergewissern Sie sich, dass Site Recovery Manager die Schutzgruppe erstellt hat und die virtuellen Maschinen in der Gruppe erfolgreich geschützt werden.

Voraussetzungen

Stellen Sie sicher, dass Sie eine der folgenden Aufgaben ausgeführt haben:

- Virtuelle Maschinen wurden in den Datenspeicher einbezogen, für den die Array-basierte Replizierung konfiguriert wurde
- Die Anforderungen in *Voraussetzungen für Speicherrichtlinien-Schutzgruppen* sind erfüllt und die *Einschränkungen für Speicherrichtlinien-Schutzgruppen* im Handbuch *Verwalten von Site Recovery Manager* wurden beachtet
- vSphere Replication wurde auf Ihren virtuellen Maschinen konfiguriert

- Eine Kombination einiger oder aller genannten Punkte.

Verfahren

- 1 Klicken Sie im vSphere Client oder im vSphere Web Client auf **Site-Wiederherstellung > Site-Recovery öffnen**.
- 2 Wählen Sie auf der Registerkarte „Site-Wiederherstellung“ der Startseite ein Site-Paar aus und klicken Sie auf **Details anzeigen**.
- 3 Klicken Sie auf die Registerkarte **Schutzgruppen** und klicken Sie auf **Neu**, um eine Schutzgruppe zu erstellen.
- 4 Geben Sie auf der Seite „Name und Speicherort“ einen Namen und eine Beschreibung für die Schutzgruppe ein, wählen Sie einen Speicherort aus und klicken Sie auf **Weiter**.
- 5 Wählen Sie auf der Seite für den „Schutzgruppentyp“ den Schutzgruppentyp aus und klicken Sie auf **Weiter**.

| Option | Aktion |
|--|--|
| Erstellen einer Schutzgruppe für die Array-basierte Replizierung | Klicken Sie auf Datenspeichergruppen (Array-basierte Replizierung) und wählen Sie ein Array-Paar aus. |
| Eine vSphere Replication-Schutzgruppe erstellen | Klicken Sie auf Einzelne VMs (vSphere Replication) . |
| Erstellen einer Schutzgruppe für Speicherrichtlinien | Klicken Sie auf Speicherrichtlinien (Array-basierte Replizierung) . |

- 6 Wählen Sie Datenspeichergruppen, virtuelle Maschinen oder Speicherrichtlinien aus, um diese der Schutzgruppe hinzuzufügen.

| Option | Aktion |
|---|--|
| Schutzgruppen für Array-basierte Replizierung | Wählen Sie einen Datenspeicher aus und klicken Sie auf Weiter . Wenn Sie eine Datenspeichergruppe auswählen, werden die in der Gruppe enthaltenen virtuellen Maschinen in der Tabelle „Virtuelle Maschinen“ angezeigt. |
| vSphere Replication-Schutzgruppen | Wählen Sie in der Liste virtuelle Maschinen aus und klicken Sie auf Weiter . Nur virtuelle Maschinen, die Sie für vSphere Replication konfiguriert haben und die sich nicht bereits in einer Schutzgruppe befinden, werden in der Liste angezeigt. |
| Speicherrichtlinien-Schutzgruppen | Wählen Sie in der Liste Speicherrichtlinien aus und klicken Sie auf Weiter . |

- 7 Auf der Seite „Wiederherstellungsplan“ können Sie optional die Schutzgruppe zu einem Wiederherstellungsplan hinzufügen.

| Option | Aktion |
|---|---|
| Zu vorhandenem Wiederherstellungsplan hinzufügen | Fügt die Schutzgruppe einem vorhandenen Wiederherstellungsplan hinzu. |
| Zu neuem Wiederherstellungsplan hinzufügen | Fügt die Schutzgruppe zu einem neuen Wiederherstellungsplan hinzu. Wenn Sie diese Option auswählen, müssen Sie einen Namen für den Wiederherstellungsplan eingeben. |
| Jetzt nicht zum Wiederherstellungsplan hinzufügen. | Wählen Sie diese Option aus, wenn Sie die Schutzgruppe nicht zu einem Wiederherstellungsplan hinzufügen möchten. |

- 8 Überprüfen Sie Ihre Einstellungen und klicken Sie auf **Fertig stellen**.

Sie können den Fortschritt bei der Erstellung der Schutzgruppe auf der Registerkarte **Schutzgruppe** überwachen.

- Wenn Site Recovery Manager für die Array-basierte Replizierung und für vSphere Replication-Schutzgruppen erfolgreich Bestandslistenzuordnungen auf die geschützten virtuellen Maschinen angewendet hat, lautet der Schutzstatus der Schutzgruppe *OK*.
- Wenn Site Recovery Manager für Schutzgruppen für Speicherrichtlinien erfolgreich alle der Speicherrichtlinie zugeordneten virtuellen Maschinen geschützt hat, lautet der Status der Schutzgruppe *OK*.
- Wenn Sie für die Array-basierte Replizierung und für vSphere Replication-Schutzgruppen keine Bestandslistenzuordnungen konfiguriert haben oder wenn Site Recovery Manager diese nicht anwenden konnte, lautet der Schutzstatus der Schutzgruppe *Nicht konfiguriert*.
- Wenn Site Recovery Manager für Schutzgruppen für Speicherrichtlinien nicht alle virtuellen Maschinen schützen kann, die der Speicherrichtlinie zugeordnet sind, lautet der Schutzstatus der Schutzgruppe *Nicht konfiguriert*.

Nächste Schritte

Wenn für die Array-basierte Replizierung und für vSphere Replication-Schutzgruppen der Schutzstatus der Schutzgruppen *Nicht konfiguriert* lautet, wenden Sie Bestandslistenzuordnungen auf die virtuellen Maschinen an:

- Informationen zum Anwenden von Bestandslistenzuordnungen für die gesamte Site oder zum Überprüfen, ob bereits festgelegte Bestandslistenzuordnungen gültig sind, finden Sie unter *Konfigurieren von Bestandslistenzuordnungen* im Handbuch *Verwalten von Site Recovery Manager*. Informationen zum Anwenden dieser Zuordnungen auf alle virtuellen Maschinen erhalten Sie unter *Anwenden von Bestandslistenzuordnungen auf alle Mitglieder einer Schutzgruppe* im Handbuch *Verwalten von Site Recovery Manager*.

- Informationen zum Anwenden von Bestandslistenzuordnungen auf jede virtuelle Maschine in der Schutzgruppe einzeln erhalten Sie unter *Konfigurieren von Bestandslistenzuordnungen für eine einzelne virtuelle Maschine in einer Schutzgruppe* im Handbuch *Verwalten von Site Recovery Manager*.

Wenn für Speicherrichtlinien-Schutzgruppen der Schutzstatus der Schutzgruppe *Nicht konfiguriert* lautet, stellen Sie sicher, dass die Anforderungen in *Voraussetzungen für Speicherrichtlinien-Schutzgruppen* erfüllt sind und dass Sie die *Einschränkungen für Schutzgruppen für Speicherrichtlinien* im Handbuch *Verwalten von Site Recovery Manager* beachtet haben.

Erstellen eines Wiederherstellungsplans

Sie erstellen einen Wiederherstellungsplan, um festzulegen, wie Site Recovery Manager virtuelle Maschinen wiederherstellt.

Verfahren

- 1 Klicken Sie im vSphere Client oder im vSphere Web Client auf **Site-Wiederherstellung > Site-Wiederherstellung öffnen**.
- 2 Wählen Sie auf der Registerkarte „Site-Wiederherstellung“ der Startseite ein Site-Paar aus und klicken Sie auf **Details anzeigen**.
- 3 Klicken Sie auf die Registerkarte **Wiederherstellungspläne** und klicken Sie auf **Neu**, um einen Wiederherstellungsplan zu erstellen.
- 4 Geben Sie einen Namen, eine Beschreibung und eine Richtung für diesen Plan ein, wählen Sie einen Ordner aus und klicken Sie dann auf **Weiter**.
- 5 Wählen Sie aus dem Menü den Gruppentyp aus.

| Option | Beschreibung |
|---|---|
| Schutzgruppen für einzelne VMs oder Datenspeichergruppen | Wählen Sie diese Option aus, um einen Wiederherstellungsplan zu erstellen, der Array-basierte Replizierung und vSphere Replication-Schutzgruppen enthält. |
| Speicherrichtlinien-Schutzgruppen | Wählen Sie diese Option aus, um einen Wiederherstellungsplan zu erstellen, der Speicherrichtlinien-Schutzgruppen enthält. Wählen Sie diese Option aus, wenn Sie Stretched Storage verwenden. |

- 6 Wählen Sie eine oder mehrere Schutzgruppen für den Plan aus, der wiederhergestellt werden soll, und klicken Sie auf **Weiter**.
- 7 Wählen Sie im Dropdown-Menü **Testnetzwerk** ein für den Wiederherstellungstest zu verwendendes Netzwerk aus und klicken Sie auf **Weiter**.
Wenn keine Zuordnungen auf Site-Ebene vorhanden sind, erstellt die Standardoption **Zuordnung auf der Site-Ebene verwenden** ein isoliertes Testnetzwerk.
- 8 Überprüfen Sie die zusammengefassten Informationen und klicken Sie auf **Beenden**, um den Wiederherstellungsplan zu erstellen.

Organisieren von Wiederherstellungsplänen in Ordnern

Um den Zugriff verschiedener Benutzer oder Gruppen auf Wiederherstellungspläne zu steuern, können Sie Ihre Wiederherstellungspläne in Ordnern organisieren.

Das Organisieren von Wiederherstellungsplänen in Ordnern ist nützlich, wenn Sie über viele Wiederherstellungspläne verfügen. Sie können den Zugriff auf Wiederherstellungspläne einschränken, indem Sie sie in Ordnern platzieren und den Ordnern für unterschiedliche Benutzer oder Gruppen unterschiedliche Berechtigungen zuweisen. Informationen zum Zuweisen von Berechtigungen zu Ordnern finden Sie unter *Zuweisen von Rollen und Berechtigungen für Site Recovery Manager* im Handbuch *Verwalten von Site Recovery Manager*.

Verfahren

- 1 Wählen Sie auf der Registerkarte **Site-Wiederherstellung** der Startseite ein Site-Paar aus und klicken Sie auf **Details anzeigen**.
- 2 Klicken Sie auf die Registerkarte **Wiederherstellungspläne** und klicken Sie im linken Bereich mit der rechten Maustaste auf **Wiederherstellungspläne** und dann auf **Neuer Ordner**.
- 3 Geben Sie einen Namen für den Ordner ein, den Sie erstellen möchten, und klicken Sie auf **Hinzufügen**.
- 4 Fügen Sie dem Ordner neue oder vorhandene Wiederherstellungspläne hinzu.

| Option | Beschreibung |
|--|--|
| Neuen Wiederherstellungsplan erstellen | Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie Neuer Wiederherstellungsplan . |
| Vorhandenen Wiederherstellungsplan hinzufügen | Klicken Sie mit der rechten Maustaste auf einen Wiederherstellungsplan in der Bestandslistenstruktur und klicken Sie auf Verschieben . Wählen Sie einen Zielordner aus und klicken Sie auf Verschieben . |

Bearbeiten eines Wiederherstellungsplans

Sie können einen Wiederherstellungsplan bearbeiten, um die Eigenschaften, die Sie bei der Erstellung angegeben haben, zu ändern. Sie können Wiederherstellungspläne entweder von der Schutz-Site oder der Wiederherstellungs-Site aus bearbeiten.

Verfahren

- 1 Klicken Sie im vSphere Client oder im vSphere Web Client auf **Site-Wiederherstellung > Site-Wiederherstellung öffnen**.
- 2 Wählen Sie auf der Registerkarte **Site-Wiederherstellung** der Startseite ein Site-Paar aus und klicken Sie auf **Details anzeigen**.
- 3 Klicken Sie auf die Registerkarte **Wiederherstellungspläne**, klicken Sie mit der rechten Maustaste auf einen Wiederherstellungsplan und anschließend auf **Bearbeiten**.

- 4 (Optional) Bearbeiten Sie den Namen und die Beschreibung des Plans und klicken Sie auf **Weiter**.

Sie können die Richtung und den Speicherort des Wiederherstellungsplans nicht ändern.

- 5 (Optional) Wählen Sie eine oder mehrere Schutzgruppen aus oder heben Sie deren Auswahl auf, um sie zum Plan hinzuzufügen bzw. aus dem Plan zu entfernen, und klicken Sie auf **Weiter**.

- 6 (Optional) Wählen Sie im Dropdown-Menü ein anderes Testnetzwerk auf der Wiederherstellungs-Site aus, und klicken Sie dann auf **Weiter**.

- 7 Überprüfen Sie die zusammengefassten Informationen und klicken Sie auf **Beenden**, um die Änderungen in den Wiederherstellungsplan zu übernehmen.

Sie können in der Ansicht **Kürzlich bearbeitete Aufgaben** das Aktualisieren des Plans verfolgen.

Festlegen von Systemeigenschaften

9

Sie können mit Systemeigenschaften das Standardverhalten von Orchestrator ändern.

Dieses Kapitel enthält die folgenden Themen:

- Festlegen des Dateisystemzugriffs auf dem Server für Workflows und Aktionen
- Festlegen des Zugriffs auf Betriebssystembefehle für Workflow und Aktionen
- Setzen von JavaScript-Zugriff auf Java-Klassen
- Festlegen der Eigenschaft für benutzerdefinierte Zeitüberschreitung
- Hinzufügen eines JDBC-Connectors für das vRealize Orchestrator-SQL-Plug-In
- Festlegen einer Eigenschaft für die Verlängerung von Authentifizierungstoken in geplanten Aufgaben oder Richtlinien

Festlegen des Dateisystemzugriffs auf dem Server für Workflows und Aktionen

Workflows und Aktionen haben in vRealize Orchestrator eingeschränkten Zugriff auf bestimmte Dateisystemverzeichnisse. Sie können den Zugriff auf andere Bereiche des Server-Dateisystems erweitern, indem Sie die Konfigurationsdatei `js-io-rights.conf` ändern.

Regeln in der Datei `js-io-rights.conf`, die Schreibzugriff auf das vRealize Orchestrator-System ermöglichen

Die Datei `js-io-rights.conf` enthält Regeln, die Schreibzugriff auf definierte Verzeichnisse im Serverdateisystem zulassen.

Obligatorischer Inhalt der Datei `js-io-rights.conf`

Jede Zeile der Datei `js-io-rights.conf` muss die folgenden Informationen enthalten.

- Ein Pluszeichen (+) oder Minuszeichen (-), um anzugeben, ob Rechte zugelassen oder verweigert werden
- Die Stufen Lesen (r), Schreiben (w) und Ausführen (x) der Rechte

- Den Pfad, auf den die Rechte angewendet werden sollen.

Hinweis Der Root-Ordner für die Datei `js-io-rights.conf` ist immer `/var/run/vco`. Im vRealize Orchestrator Appliance-Dateisystem befindet sich dieser Ordner unter `/data/vco/var/run/vco`. Alle Inhalte mit Zugriff auf das vRealize Orchestrator-Dateisystem müssen unter diesem Root-Ordner zugeordnet werden.

Standardinhalt der Datei `js-io-rights.conf`

Der Standardinhalt der Konfigurationsdatei `js-io-rights.conf` in der Orchestrator Appliance lautet wie folgt:

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

Die ersten beiden Zeilen in der standardmäßigen Konfigurationsdatei `js-io-rights.conf` ermöglichen die folgenden Zugriffsrechte:

-rwx /

Der gesamte Zugriff auf das Dateisystem wird verweigert.

+rwX /var/run/vco

Lese-, Schreib- und Ausführungszugriff sind im Verzeichnis `/var/run/vco` zulässig.

Regeln in der Datei `js-io-rights.conf`

vRealize Orchestrator regelt die Zugriffsrechte in der Reihenfolge, in der sie in der Datei `js-io-rights.conf` aufgeführt werden. Jede Zeile kann die vorherigen Zeilen überschreiben.

Wichtig Sie können den Zugriff auf alle Teile des Dateisystems zulassen, indem Sie `+rwX /` in der Datei `js-io-rights.conf` festlegen. Dies stellt jedoch ein hohes Sicherheitsrisiko dar.

Festlegen des Dateisystemzugriffs auf dem Server für Workflows und Aktionen

Um die Bereiche des Serverdateisystems zu ändern, auf die Workflows und die vRealize Orchestrator-API zugreifen können, bearbeiten Sie die Konfigurationsdatei `js-io-rights.conf`. Die Datei `js-io-rights.conf` wird erstellt, wenn ein Workflow versucht, auf das Dateisystem des vRealize Orchestrator-Servers zuzugreifen.

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance als **root** an.
- 2 Navigieren Sie zum Verzeichnis `/data/vco/var/run/vco/`.

- 3 Öffnen Sie die Konfigurationsdatei `js-io-rights.conf` in einem Texteditor.
- 4 Fügen Sie der Datei `js-io-rights.conf` die benötigten Zeilen hinzu, um den Zugriff auf Bereiche des Dateisystems zuzulassen oder zu verweigern.

Die folgende Zeile verweigert beispielsweise die Ausführungsrechte im Verzeichnis `/data/vco/var/run/vco/noexec`:

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

`/data/vco/var/run/vco/noexec` behält Ausführungsrechte bei, aber `/data/vco/var/run/vco/noexec/bar` nicht. Die Lese- und Schreibrechte für beide Verzeichnisse bleiben erhalten.

Ergebnisse

Sie haben die Zugriffsrechte auf das Dateisystem für Workflows und für die vRealize Orchestrator-API geändert.

Festlegen des Zugriffs auf Betriebssystembefehle für Workflow und Aktionen

Die vRealize Orchestrator-API stellt eine Skripterstellungsklasse, `Command`, bereit, die Befehle im vRealize Orchestrator-Server-Hostbetriebssystem ausführt. Um nicht autorisierten Zugriff auf den Serverhost zu verhindern, haben vRealize Orchestrator-Anwendungen standardmäßig keine Berechtigungen zum Ausführen der Klasse `Command`. Wenn vRealize Orchestrator-Anwendungen Berechtigungen zum Ausführen von Befehlen auf dem Hostbetriebssystem benötigen, können Sie die Skripterstellungsklasse `Command` aktivieren.

Sie gewähren die Berechtigung zur Verwendung der Klasse `Command`, indem Sie eine Systemeigenschaft für die vRealize Orchestrator-Konfiguration festlegen.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Klicken Sie auf **Eigenschaften des Systems**.
- 3 Klicken Sie auf **Neu**.
- 4 Geben Sie im Textfeld **Schlüssel** den Wert `com.vmware.js.allow-local-process` ein.
- 5 Geben Sie im Textfeld **Wert** den Wert `true` ein.
- 6 Geben Sie im Textfeld **Beschreibung** eine Beschreibung der Systemeigenschaft ein.
- 7 Klicken Sie auf **Hinzufügen**.
- 8 Klicken Sie im Popup-Menü auf **Änderungen speichern**.
Eine Meldung zeigt an, dass die Angaben gespeichert wurden.
- 9 Warten Sie, bis der vRealize Orchestrator-Server neu gestartet wird.

Ergebnisse

Damit haben Sie vRealize Orchestrator-Anwendungen die Berechtigung zum Ausführen lokaler Befehle im Betriebssystem des vRealize Orchestrator-Serverhosts gewährt.

Hinweis Indem Sie für die Systemeigenschaft `com.vmware.js.allow-local-process` den Wert `true` festlegen, lassen Sie zu, dass die Skripterstellungsklasse `Command` an beliebiger Stelle im Dateisystem schreibt. Diese Eigenschaft setzt nur jene Zugriffsberechtigungen auf das Dateisystem außer Kraft, die Sie in der Datei `js-io-rights.conf` für die Skripterstellungsklasse `Command` festlegen. Die in der Datei `js-io-rights.conf` festgelegten Zugriffsberechtigungen auf das Dateisystem gelten nach wie vor für alle Skripterstellungsklassen außer `Command`.

Setzen von JavaScript-Zugriff auf Java-Klassen

Standardmäßig beschränkt vRealize Orchestrator den JavaScript-Zugriff auf einen begrenzten Satz von Java-Klassen. Wenn Sie JavaScript-Zugriff auf mehr Java-Klassen benötigen, müssen Sie eine vRealize Orchestrator-Systemeigenschaft festlegen.

Wenn Sie einer JavaScript-Engine den vollen Zugriff auf die Java Virtual Machine (JVM) gestatten, kann dies ein Sicherheitsrisiko bedeuten. Fehlerhaft geschriebene Skripte oder Skripte mit bösartigem Inhalt haben auf alle Systemkomponenten Zugriff, auf die auch der Benutzer Zugriff hat, der den vRealize Orchestrator-Server ausführt. Daher kann die JavaScript-Engine von vRealize Orchestrator standardmäßig nur auf die Klassen im Paket `java.util.*` zugreifen.

Wenn Sie den JavaScript-Zugriff auf Klassen außerhalb des Pakets `java.util.*` benötigen, können Sie in einer Konfigurationsdatei die Java-Pakete auflisten, für die Sie JavaScript-Zugriff gestatten möchten. Sie können die Systemeigenschaft `com.vmware.scripting.rhino-class-shutter-file` so einrichten, dass sie auf diese Datei zeigt.

Verfahren

- 1 Erstellen Sie eine Text Konfigurationsdatei, um die Liste von Java-Paketen zu speichern, auf die Sie den JavaScript-Zugriff gestatten möchten.

Beispiel: Um den JavaScript-Zugriff für alle Klassen im Paket `java.net` und für die Klasse `java.lang.Object` freizugeben, fügen Sie den folgenden Inhalt in die Datei ein.

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

- 2 Geben Sie einen Namen für die Konfigurationsdatei ein.
- 3 Speichern Sie die Konfigurationsdatei in einem Unterverzeichnis von `/data/vco/usr/lib/vco`.

Hinweis Die Konfigurationsdatei kann nicht unter einem anderen Verzeichnis gespeichert werden.

- 4 Melden Sie sich beim Control Center als `root` an.

- 5 Klicken Sie auf **Eigenschaften des Systems**.
- 6 Klicken Sie auf **Neu**.
- 7 Geben Sie im Textfeld **Schlüssel** die Zeichenfolge `com.vmware.scripting.rhino-class-shutter-file` ein.
- 8 Geben Sie im Textfeld **Wert** `vco/usr/lib/vco/ your_configuration_file_subdirectory` ein.
- 9 Geben Sie im Textfeld **Beschreibung** eine Beschreibung der Systemeigenschaft ein.
- 10 Klicken Sie auf **Hinzufügen**.
- 11 Klicken Sie im Popup-Menü auf **Änderungen speichern**.
Eine Meldung zeigt an, dass die Angaben gespeichert wurden.
- 12 Warten Sie, bis der vRealize Orchestrator-Server neu gestartet wird.

Ergebnisse

Die JavaScript-Engine hat Zugriff auf die Java-Klassen, die Sie angegeben haben.

Festlegen der Eigenschaft für benutzerdefinierte Zeitüberschreitung

Wenn vCenter Server überlastet ist, dauert das Zurückgeben der Antwort an den vRealize Orchestrator-Server länger als die standardmäßig festgelegten 20000 Millisekunden. Um dies zu verhindern, müssen Sie die vRealize Orchestrator-Konfigurationsdatei ändern, um den standardmäßigen Zeitüberschreitungszeitraum zu erhöhen.

Wenn der Standard-Zeitüberschreitungszeitraum vor dem Abschluss bestimmter Vorgänge abläuft, enthält das vRealize Orchestrator Server-Protokoll Fehler.

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

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Klicken Sie auf **Eigenschaften des Systems**.
- 3 Klicken Sie auf **Neu**.
- 4 Geben Sie im Textfeld **Schlüssel** die Zeichenfolge `com.vmware.vmo.plugin.vi4.waitUpdatesTimeout` ein.
- 5 Geben Sie im Textfeld **Wert** den neuen Zeitüberschreitungszeitraum in Millisekunden ein.
- 6 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung für die Systemeigenschaft ein.
- 7 Klicken Sie auf **Hinzufügen**.

- 8 Klicken Sie im Popup-Menü auf **Änderungen speichern**.

Eine Meldung zeigt an, dass die Angaben gespeichert wurden.

- 9 Starten Sie den Orchestrator-Server neu.

Ergebnisse

Der festgelegte Wert überschreibt den Standardwert für die Zeitüberschreitung von 20000 Millisekunden.

Hinzufügen eines JDBC-Connectors für das vRealize Orchestrator-SQL-Plug-In

Dieses Beispiel zeigt, wie Sie einen MySQL-Connector für das vRealize Orchestrator-SQL-Plug-In hinzufügen können.

Verfahren

- 1 Fügen Sie der vRealize Orchestrator Appliance die MySQL-Datei „connector.jar“ hinzu.
 - a Melden Sie sich bei der Befehlszeile der vRealize Orchestrator Appliance über SSH als **root** an.
 - b Navigieren Sie zum Verzeichnis `/data/vco/var/run/vco/`.

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

- c Erstellen Sie das Verzeichnis `plugins/SQL/lib/`.

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

- d Kopieren Sie die `connector.jar`-Datei für MySQL von Ihrem lokalen Computer in das Verzeichnis `/data/vco/var/run/vco/plugins/SQL/lib/`, indem Sie einen Secure Copy-Befehl (SCP) ausführen.

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

Hinweis Sie können auch alternative Methoden verwenden, um Ihre `connector.jar`-Datei in die vRealize Orchestrator Appliance zu kopieren, beispielsweise PSCP.

- 2 Fügen Sie dem Control Center die neue MySQL-Eigenschaft hinzu.
 - a Melden Sie sich beim Control Center als **root** an.
 - b Klicken Sie auf **Systemeigenschaften**.
 - c Klicken Sie auf **Neu**.
 - d Geben Sie unter **Schlüssel** die Zeichenfolge `o11n.plugin.SQL.classpath` ein.

- e Geben Sie unter **Wert** die Zeichenfolge `/var/run/vco/plugins/SQL/lib/your_mysql_connector.jar` ein.

Hinweis Das Textfeld „Wert“ kann mehrere JDBC-Connectors enthalten. Jeder JDBC-Connector wird durch ein Semikolon („;“) getrennt. Beispiel:

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

- f (Optional) Geben Sie eine Beschreibung für die MySQL-Systemeigenschaft ein.
- g Klicken Sie auf **Hinzufügen** und warten Sie, bis der vRealize Orchestrator-Server neu gestartet wurde.

Hinweis Speichern Sie die connector.jar-Datei für JDBC nicht in einem anderen Verzeichnis und legen Sie keinen anderen Wert für die Eigenschaft „`o11n.plugin.SQL.classpath`“ fest. Anderenfalls ist der JDBC-Connector für Ihre vRealize Orchestrator-Bereitstellung nicht verfügbar.

Festlegen einer Eigenschaft für die Verlängerung von Authentifizierungstoken in geplanten Aufgaben oder Richtlinien

Verwalten Sie, wie Sie die Verlängerung der in geplanten Aufgaben oder Richtlinien verwendeten Authentifizierungstoken aktivieren können, indem Sie eine Systemeigenschaft festlegen.

Wenn eine geplante Aufgabe von Benutzern ohne Administratorrechte im vRealize Orchestrator Client ohne eine Endzeit konfiguriert wird, läuft das Authentifizierungstoken für den geplanten Workflow acht Stunden nach der angegebenen Startzeit ab. Neben geplanten Aufgaben wird dieses Authentifizierungstoken auch für vRealize Orchestrator-Richtlinien verwendet. Um sicherzustellen, dass die geplanten Workflows oder Richtlinien in der vRealize Orchestrator-Bereitstellung weiterhin ausgeführt werden, können Sie eine Systemeigenschaft im Control Center festlegen.

Hinweis Authentifizierungstoken können nach Ablauf von 90 Tagen nach ihrem ursprünglichen Startdatum nicht mehr verlängert werden.

Voraussetzungen

Stellen Sie sicher, dass Ihre vRealize Orchestrator-Bereitstellung einen vRealize Automation-Authentifizierungsanbieter verwendet oder in vRealize Automation integriert ist. Die Systemeigenschaft `com.vmware.o11n.auth.csp.renewTokens` ist für mit vSphere authentifizierte vRealize Orchestrator-Bereitstellungen nicht verfügbar.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.

- 2 Klicken Sie auf **Systemeigenschaften**.
- 3 Klicken Sie auf **Neu**.
- 4 Geben Sie unter **Schlüssel** Folgendes ein: `com.vmware.o11n.auth.csp.renewTokens`.
- 5 Geben Sie unter **Wert** Folgendes ein: `true`.

Hinweis Bei vRealize Orchestrator-Bereitstellungen in vRealize Automation und vRealize Automation Cloud wird bei Workflows mit langer Laufzeit, die über vRealize Automation gestartet wurden, das Authentifizierungstoken nach seinem Ablauf beschädigt. Das Token läuft acht Stunden nach der angegebenen Startzeit ab.

- 6 (Optional) Geben Sie eine Beschreibung für die neue Systemeigenschaft ein.
- 7 Klicken Sie auf **Hinzufügen** und warten Sie, bis der vRealize Orchestrator-Server neu gestartet wurde.

Wenn Sie vRealize Orchestrator installiert und konfiguriert haben, können Sie vRealize Orchestrator verwenden, um häufig wiederholte Vorgänge im Zusammenhang mit der Verwaltung der virtuellen Umgebung zu automatisieren.

- Melden Sie sich beim vRealize Orchestrator Client an und führen Sie Workflows für die vCenter Server-Bestandslistenobjekte oder andere Objekte aus, auf die vRealize Orchestrator über seine Plug-Ins zugreift. Weitere Informationen finden Sie unter *Verwenden des VMware vRealize Orchestrator Client*.
- Duplizieren und ändern Sie die vRealize Orchestrator-Standard-Workflows und schreiben Sie Ihre eigenen Aktionen und Workflows, um Vorgänge in vCenter Server zu automatisieren.
- Um die Funktionalität der vRealize Orchestrator-Plattform zu erweitern, entwickeln Sie Plug-Ins.
- Verwalten Sie Ihre vRealize Orchestrator-Bestandsliste über mehrere vRealize Orchestrator-Instanzen hinweg mit der Integration eines Remote-Git-Repositorys. Weitere Informationen finden Sie unter *Verwenden des VMware vRealize Orchestrator Client*.
- Führen Sie mithilfe von vSphere Web Client Workflows für Ihre vSphere-Bestandslistenobjekte aus.