

Installieren und Konfigurieren von VMware vRealize Orchestrator

vRealize Orchestrator 7.4

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 © 2008-2018 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise.](#)

Inhalt

Installieren und Konfigurieren von VMware vRealize Orchestrator	6
1 Einführung in VMware vRealize Orchestrator	7
Schüsselfunktionen der Orchestrator-Plattform	7
Benutzertypen für Orchestrator und damit verbundene Verantwortlichkeiten	9
Orchestrator-Architektur	10
Orchestrator-Plug-Ins	11
2 Systemanforderungen für Orchestrator	12
Hardwareanforderungen für die Orchestrator-Appliance	12
Von Orchestrator unterstützte Browser	13
Orchestrator-Datenbankanforderungen	13
In der Orchestrator Appliance enthaltene Software	13
Unterstützungsstufe der Internationalisierung	13
Orchestrator-Netzwerkports	14
3 Einrichten von Orchestrator-Komponenten	17
Einrichtung von vCenter Server	17
Authentifizierungsmethoden	18
Einrichten der Orchestrator-Datenbank	18
4 Installieren von Orchestrator	20
Herunterladen und Bereitstellen der Orchestrator Appliance	20
Einschalten der Orchestrator Appliance und Öffnen der Startseite	22
Ändern des Root-Kennworts	22
Aktivieren und Deaktivieren der SSH-Administratoranmeldung bei der vRealize Orchestrator Appliance	23
Konfigurieren der Netzwerkeinstellungen für die Orchestrator Appliance	23
5 Erstkonfiguration	25
Konfigurieren eines eigenständigen Orchestrator-Servers	25
Konfigurieren eines eigenständigen Orchestrator-Servers mit vRealize Automation-Authentifizierung	25
Konfigurieren eines eigenständigen Orchestrator-Servers mit vSphere-Authentifizierung	27
Orchestrator-Netzwerkports	29
Konfigurieren der Orchestration-Datenbankverbindung	31
Importieren des Datenbank-SSL-Zertifikats	31
Konfigurieren der Datenbankverbindung	32

Exportieren der Orchestrator-Datenbank	34
Importieren einer Orchestrator-Datenbank	35
Zertifikate verwalten	35
Verwalten von Orchestrator-Zertifikaten	36
Konfigurieren der Orchestrator-Plug-Ins	38
Verwalten von vRealize Orchestrator-Plug-Ins	38
Installieren oder Aktualisieren eines vRealize Orchestrator-Plug-Ins	39
Deinstallieren eines Plug-Ins	40
Verfügbarkeit und Skalierbarkeit von Orchestrator	41
Konfigurieren eines Orchestrator-Clusters	42
Überwachen eines Orchestrator-Clusters	45
Konfigurieren des Programms zur Verbesserung der Kundenzufriedenheit	45
Kategorien von Daten, die VMware erhält	46
Am Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen	46
6 Verwenden der API-Dienste	47
Verwalten von SSL-Zertifikaten mithilfe der REST-API	47
Löschen von SSL-Zertifikaten mithilfe der REST-API	48
Importieren von SSL-Zertifikaten mithilfe der REST-API	48
Erstellen eines Keystore mithilfe der REST-API	50
Löschen eines Keystore mithilfe der REST-API	50
Hinzufügen eines Schlüssels mithilfe der REST-API	51
Automatisieren der Orchestrator-Konfiguration mithilfe der Control Center-REST-API	52
7 Zusätzliche Konfigurationsoptionen	53
Neukonfigurieren der Authentifizierung	53
Ändern des Authentifizierungsanbieters	53
Ändern der Authentifizierungsparameter	54
Exportieren der Orchestrator-Konfiguration	55
Importieren der Orchestrator-Konfiguration	56
Konfigurieren der Workflow-Ausführungseigenschaften	57
Orchestrator-Protokolldateien	57
Persistenz von Protokollen	58
Konfiguration der Orchestrator-Protokolle	59
Filtern der Orchestrator-Protokolle	59
Hinzufügen von Netzwerkkarten (NICs)	60
Konfigurieren von statischen Routen	61
8 Anwendungsfälle für Konfiguration und Fehlerbehebung	63
Konfigurieren des vRealize Orchestrator-Plug-Ins für vSphere Web Client	63
Aufheben der Registrierung der Orchestrator-Authentifizierung	64

Ändern von SSL-Zertifikaten	65
Hinzufügen eines Zertifikats zum Local Store	65
Ändern des Zertifikats der Orchestrator Appliance-Management-Site	66
Abbrechen laufender Workflows	67
Aktivieren von Orchestrator-Server-Debugging	67
Sichern der Konfiguration und Elemente von Orchestrator	68
Sichern und Wiederherstellen vRealize Orchestrator	71
Sichern von vRealize Orchestrator	71
Wiederherstellen einer vRealize Orchestrator-Instanz	73
Notfallwiederherstellung von Orchestrator mithilfe von Site Recovery Manager	74
Konfigurieren virtueller Maschinen für vSphere Replication	74
Erstellen von Schutzgruppen	75
Erstellen eines Wiederherstellungsplans	76
Organisieren von Wiederherstellungsplänen in Ordnern	77
Bearbeiten eines Wiederherstellungsplans	78

9 Festlegen von Systemeigenschaften 79

Deaktivieren des Zugriffs auf den Orchestrator-Client für Nichtadministratoren	79
Festlegen des Dateisystemzugriffs auf dem Server für Workflows und Aktionen	80
Regeln in der Datei „js-io-rights.conf“, die Schreibzugriff auf das Orchestrator-System ermöglichen	80
Festlegen des Dateisystemzugriffs auf dem Server für Workflows und Aktionen	81
Festlegen des Zugriffs auf Betriebssystembefehle für Workflow und Aktionen	82
Setzen von JavaScript-Zugriff auf Java-Klassen	83
Festlegen der Eigenschaft für benutzerdefinierte Zeitüberschreitung	84

10 Weitere Schritte 86

Anmelden beim Orchestrator-Client über die Webkonsole der Orchestrator Appliance	86
--	----

Installieren und Konfigurieren von VMware vRealize Orchestrator

Unter *Installieren und Konfigurieren von VMware vRealize Orchestrator* finden Sie Informationen und Anleitungen zum Installieren, Aktualisieren und Konfigurieren 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 Datacentern 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](#)
- [Benutzertypen für Orchestrator und damit verbundene Verantwortlichkeiten](#)
- [Orchestrator-Architektur](#)
- [Orchestrator-Plug-Ins](#)

Schlüsselfunktionen der Orchestrator-Plattform

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

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 Orchestrator-Konfiguration werden in hochwertigen Datenbanken gespeichert.

Zentrale Verwaltung

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, einheitlichen Protokollzugriff und Konfigurationen sowie Korrelation zwischen der Workflow-Ausführung und Systemressourcen bereitgestellt werden. Der Orchestrator-Protokollierungsmechanismus ist durch eine zusätzliche Protokolldatei optimiert, die verschiedene Leistungskennzahlen für den Durchsatz der Orchestrator-Engine sammelt.

Versionierung

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

Skripterstellungseengine

Die Mozilla Rhino JavaScript-Engine bietet eine Möglichkeit, Bausteine für die Orchestrator-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 Orchestrator bereitgestellt werden
- Benutzerdefinierte Bausteine, die vom Kunden erstellt werden
- Objekte, die Orchestrator 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 Orchestrator-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.

Monitoring-Client

Überwachen Sie Orchestrator-Prozesse mithilfe des Monitoring-Clients, der als Web-Benutzerschnittstelle zur Verfügung gestellt wird. Sie können diese Informationen zur Fehlerbehebung der Orchestrator-Prozesse verwenden.

Entwicklung und Ressourcen

Die 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 Orchestrator-REST-API für das Senden von Anforderungen an den Orchestrator-Server.

Sicherheit

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
- Secure Sockets Layer (SSL), um verschlüsselte Kommunikation zwischen dem Desktop-Client und dem Server sowie den HTTPS-Zugriff auf den Web-Frontend 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 verwenden denselben Chiffreschlüssel.

Benutzertypen für Orchestrator und damit verbundene Verantwortlichkeiten

Orchestrator stellt verschiedene Tools und Schnittstellen basierend auf den spezifischen Verantwortungen der globalen Benutzerrollen bereit. In Orchestrator können Sie Benutzer mit umfassenden Rechten haben, die Teil der Administratorgruppe (Administratoren) sind, und Benutzer mit beschränkten Rechten, die nicht Teil der Administratorengruppe sind (Endbenutzer).

Benutzer mit vollen Rechten

Orchestrator-Administratoren und Entwickler haben gleiche administrative Rechte, die aber im Bereich der Verantwortung aufgeteilt sind.

Administratoren

Diese Rolle hat vollen Zugriff auf alle Orchestrator-Plattformfunktionen. Administrative Basisverantwortlichkeiten umfassen folgende Elemente:

- Installieren und Konfigurieren von Orchestrator
- Verwalten von Zugriffsrechten für Orchestrator und Anwendungen
- Importieren und Exportieren von Paketen
- Ausführen von Workflows und Planen von Aufgaben
- Verwaltung der Versionskontrolle für importierte Elemente
- Erstellen neuer Workflows und Plug-Ins

Entwickler

Dieser Benutzertyp hat vollen Zugriff auf alle Orchestrator-Plattformfunktionen. Entwickler erhalten Zugriff auf die Orchestrator-Clientschnittstelle und haben folgende Verantwortlichkeiten:

- Erstellen von Anwendungen zur Erweiterung der Orchestrator-Plattformfunktionen
- Automatische Verarbeitung durch Anpassung bestehender Workflows und Erstellen neuer Workflows und Plug-Ins

Benutzer mit beschränkten Rechten

Endbenutzer

Endbenutzer können Workflows und Richtlinien ausführen und planen, die Administratoren oder Entwickler im Orchestrator-Client verfügbar machen.

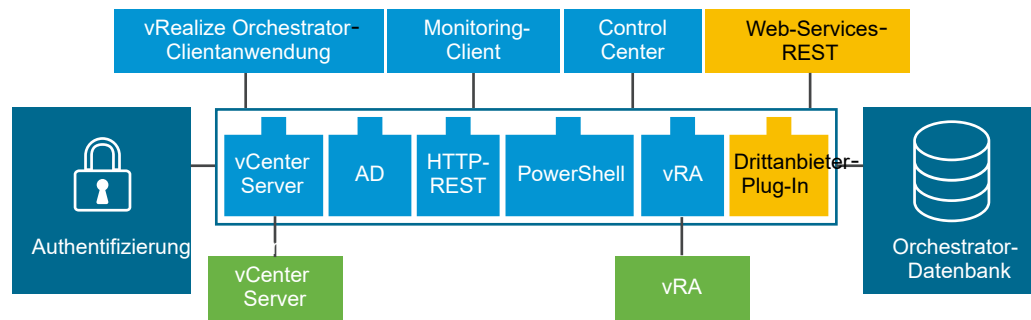
Orchestrator-Architektur

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 Orchestrator über eine Serie von Plug-Ins zugreift.

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

Zudem bietet 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. Orchestrator verbindet sich mit einem Authentifizierungsanbieter, um Benutzerkonten zu verwalten, und mit einer Datenbank, um Informationen aus den Workflows zu speichern, die unter Orchestrator ausgeführt werden. Der Zugriff auf Orchestrator, die damit bereitgestellten Objekte sowie die Orchestrator-Workflows ist über die Orchestrator-Clientschnittstelle oder über Webdienste möglich. Die Überwachung und Konfiguration der Orchestrator-Workflows und -Dienste erfolgen über den Monitoring-Client und Control Center.

Abbildung 1-1. Architektur von VMware vRealize Orchestrator



Orchestrator-Plug-Ins

Plug-Ins ermöglichen Ihnen den Zugriff auf und die Steuerung von externen Technologien und Anwendungen über Orchestrator. Indem Sie eine externe Technologie in einem 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.

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 vRealize Automation-Infrastruktur und Anwendungsdienste anpassen. Darüber hinaus können Sie mit der offenen Plug-In-Architektur von Orchestrator Plug-Ins für den Zugriff auf andere Anwendungen entwickeln.

Von VMware entwickelte Orchestrator-Plug-Ins werden als .vmoapp-Dateien verteilt. Weitere Informationen zu den von VMware entwickelten und verteilten Orchestrator-Plug-Ins finden Sie unter [Externe vRealize Orchestrator-Plug-Ins](#). Weitere Informationen zu Orchestrator-Plug-Ins von Drittanbietern finden Sie unter [VMware Solution Exchange](#).

Systemanforderungen für Orchestrator

2

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

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

Dieses Kapitel enthält die folgenden Themen:

- [Hardwareanforderungen für die Orchestrator-Appliance](#)
- [Von Orchestrator unterstützte Browser](#)
- [Orchestrator-Datenbankanforderungen](#)
- [In der Orchestrator Appliance enthaltene Software](#)
- [Unterstützungsstufe der Internationalisierung](#)
- [Orchestrator-Netzwerkports](#)

Hardwareanforderungen für die Orchestrator-Appliance

Die Orchestrator Appliance ist eine vorkonfigurierte Linux-basierte virtuelle Maschine. Stellen Sie vor der Bereitstellung der Appliance sicher, dass Ihr System die Mindestanforderungen an die Hardware erfüllt.

Für die Orchestrator Appliance gelten die folgenden Hardwareanforderungen:

- 2 CPUs
- 6 GB Arbeitsspeicher
- 17 GB Festplattenspeicher

Verringern Sie die Standardgröße des Arbeitsspeichers nicht, da der Orchestrator-Server mindestens 2 GB freien Arbeitsspeicher benötigt.

Von Orchestrator unterstützte Browser

Control Center erfordert einen Webbrowser.

Sie müssen zum Verbinden mit Control Center einen der folgenden Browser verwenden.

- Microsoft Internet Explorer 10 oder höher
- Mozilla Firefox
- Google Chrome

Orchestrator-Datenbankanforderungen

Der Orchestrator-Server benötigt eine Datenbank. Die vorkonfigurierte Orchestrator PostgreSQL-Datenbank ist bereit für den Produktionseinsatz. Sie können je nach Ihrer Umgebung auch eine externe Datenbank verwenden.

Eine Liste der unterstützten Datenbankversionen finden Sie in der [VMware-Produkt-Interoperabilitätsmatrix](#).

In der Orchestrator Appliance enthaltene Software

Die Orchestrator Appliance ist eine vorkonfigurierte virtuelle Maschine, die für die Ausführung von Orchestrator optimiert ist. Die Appliance wird mit vorinstallierter Software verteilt.

Das Orchestrator Appliance-Paket enthält die folgende Software:

- SUSE Linux Enterprise Server 11 Update 3 für VMware, 64-Bit-Edition
- PostgreSQL
- Orchestrator

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

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

Informationen zum Konfigurieren einer Datenbank für Produktionsumgebungen finden Sie unter [Einrichten der Orchestrator-Datenbank](#).

Unterstützungsstufe der Internationalisierung

Das Orchestrator Control Center umfasst Ländereinstellungen für Spanisch, Französisch, Deutsch, Chinesisch (traditionell), Chinesisch (vereinfacht), Koreanisch und Japanisch. Der Orchestrator-Client unterstützt die Internationalisierungsstufe 1.

Unterstützung für Nicht-ASCII-Zeichen in Orchestrator

Obwohl der Orchestrator-Client nicht lokalisiert ist, kann die Software auch auf einem nicht englischsprachigen Betriebssystem ausgeführt werden und unterstützt Text mit Nicht-ASCII-Zeichen.

Tabelle 2-1. Unterstützung für Nicht-ASCII-Zeichen in der grafischen Benutzeroberfläche von Orchestrator

Unterstützung für Nicht-ASCII-Zeichen				
Orchestrator-Element	Beschreibungsfeld	Namensfeld	Eingabe- und Ausgabeparameter	Attribute
Aktion	Ja	Nein	Nein	Nein
Ordner	Ja	Ja	-	-
Konfigurationselement	Ja	Ja	-	Nein
Paket	Ja	Ja	-	-
Richtlinie	Ja	Ja	-	-
Richtlinienvorlage	Ja	Ja	-	-
Ressourcenelement	Ja	Ja	-	-
Workflow	Ja	Ja	Nein	Nein
Anzeigegruppe und Eingabeschritt in Workflowpräsentation	Ja	Ja	-	-

Unterstützung für Nicht-ASCII-Zeichen für Oracle-Datenbanken

Um Zeichen im richtigen Format in einer Oracle-Datenbank zu speichern, legen Sie den Parameter NLS_CHARACTER_SET auf AL32UTF8 fest, bevor Sie die Datenbankverbindung konfigurieren und die Tabellenstruktur einrichten. Diese Einstellung ist für eine internationalisierte Umgebung von wesentlicher Bedeutung.

Orchestrator-Netzwerkports

Orchestrator benutzt spezifische Ports zur Kommunikation mit den anderen Systemen. Die Ports werden mit einem Standardwert eingerichtet, der nicht geändert werden kann.

Standardkonfigurationsports

Zu Bereitstellung des Orchestrator-Dienstes müssen Sie Standardports einrichten und Ihre Firewall so konfigurieren, dass ankommende TCP-Verbindungen zugelassen werden.

Hinweis Andere Ports können erforderlich sein, wenn Sie benutzerdefinierte Plug-Ins verwenden.

Tabelle 2-2. VMware vRealize Orchestrator Standardkonfigurationsports

Port	Zahl	Protokoll	Quelle	Ziel	Beschreibung
Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI)	5480	TCP			Der Zugriffspunkt für die Schnittstelle mit den Systemeinstellungen der Appliance.
HTTP-Serverport	8280	TCP	Endbenutzer-Webbrowser	Orchestrator-Server	Die Anforderungen, die an den Standard-HTTP-Webport 8280 von Orchestrator gesendet wurden, werden an den Standard-HTTPS-Webport 8281 umgeleitet.
HTTPS-Serverport	8281	TCP	Endbenutzer-Webbrowser	Orchestrator-Server	Der Zugriffspunkt für die Startseite von Orchestrator.
HTTPS-Zugriffspunkt für Webkonfiguration	8283	TCP	Endbenutzer-Webbrowser	Orchestrator-Konfiguration	Der SSL-Zugangspunkt zur Webschnittstelle der Orchestrator-Konfiguration.

Externe Kommunikationsports

Sie müssen Ihre Firewall so konfigurieren, dass abgehende Verbindungen zulässig sind und Orchestrator mit externen Diensten kommunizieren kann.

Tabelle 2-3. VMware vRealize Orchestrator Externe Kommunikationsports

Port	Zahl	Protokoll	Quelle	Ziel	Beschreibung
SQL Server	1433	TCP	Orchestrator-Server	Microsoft SQL Server	Der Port, der für die Kommunikation mit den Microsoft SQL Server-Instanzen verwendet wird, die als Orchestrator-Datenbank konfiguriert wurden.
PostgreSQL	5432	TCP	Orchestrator-Server	PostgreSQL Server	Der Port, der für die Kommunikation mit dem PostgreSQL Server verwendet wird, der als Orchestrator-Datenbank konfiguriert wurde.
Oracle	1521	TCP	Orchestrator-Server	Oracle DB Server	Der Port, der für die Kommunikation mit dem Oracle Datenbankserver verwendet wird, der als Orchestrator-Datenbank konfiguriert wurde.

Tabelle 2-3. VMware vRealize Orchestrator Externe Kommunikationsports (Fortsetzung)

Port	Zahl	Protokoll	Quelle	Ziel	Beschreibung
SMTP-Server-Port	25	TCP	Orchestrator-Server	SMTP-Server	Der für E-Mail-Benachrichtigungen verwendete Port.
vCenter Server API-Port	443	TCP	Orchestrator-Server	vCenter Server	Der vCenter Server-API-Kommunikationsport, der von Orchestrator verwendet wird, um Informationen über die virtuelle Infrastruktur und die virtuellen Maschinen von registrierten vCenter Server-Instanzen zu erhalten.

Einrichten von Orchestrator-Komponenten

3

Wenn Sie die Orchestrator Appliance herunterladen und bereitstellen, wird der Orchestrator-Server vorkonfiguriert. Der Dienst wird nach der Bereitstellung automatisch gestartet.

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

- Installieren und konfigurieren Sie eine Datenbank und konfigurieren Sie Orchestrator für die Verbindung mit ihr.
- Installieren und konfigurieren Sie einen Authentifizierungsanbieter und konfigurieren Sie Orchestrator für die Verwendung mit ihm.
- Installieren und konfigurieren Sie einen Lastausgleichsserver. Legen Sie in seiner Konfiguration fest, dass er die Arbeitslast auf zwei oder mehr Orchestrator-Server verteilt.

Dieses Kapitel enthält die folgenden Themen:

- [Einrichtung von vCenter Server](#)
- [Authentifizierungsmethoden](#)
- [Einrichten der Orchestrator-Datenbank](#)

Einrichtung von vCenter Server

Eine Erhöhung der Anzahl an vCenter Server-Instanzen in der Orchestrator-Einrichtung bedeutet auch, dass Orchestrator mehr Sitzungen verwalten muss. Zu viele aktive Sitzungen können zu Zeitüberschreitungen in 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 Sie können mehrere vCenter Server-Instanzen auf verschiedenen virtuellen Maschinen in Ihrer Orchestrator-Einrichtung ausführen, sofern Ihr Netzwerk über ausreichend Bandbreite verfügt und angemessene Latenzzeiten bieten kann. Wenn Sie ein LAN verwenden, um die Kommunikation zwischen Orchestrator und vCenter Server zu verbessern, ist eine Leitung mit 100 Mbit/s unerlässlich.

Authentifizierungsmethoden

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

Wenn Sie die Orchestrator Appliance herunterladen und bereitstellen, müssen Sie eine Verbindung mit vRealize Automation oder vSphere einrichten.

Einrichten der Orchestrator-Datenbank

Orchestrator erfordert eine Datenbank zum Speichern von Workflows und Aktionen.

Wenn Sie die Orchestrator Appliance herunterladen und bereitstellen, wird der Orchestrator-Server zum Einsatz mit der in der Appliance verteilten PostgreSQL-Datenbank vorkonfiguriert. Die Standardkonfiguration der Orchestrator Appliance-Datenbank ist bereit für den Einsatz in Produktionssystemen.

Für eine externe vRealize Orchestrator-Instanz empfiehlt VMware die Verwendung einer externen PostgreSQL-, Microsoft SQL Server- oder Oracle-Datenbank.

Wenn vRealize Orchestrator in vRealize Automation integriert ist, empfiehlt VMware die Verwendung der in die vRealize Automation-Appliance eingebettete PostgreSQL-Datenbank.

Hinweis Die Microsoft SQL Server- und die Oracle-Datenbank sind veraltet und werden in künftigen Versionen entfernt. Bis dahin werden die Microsoft SQL Server- und die Oracle-Datenbank vollständig unterstützt. Nach dem Entfernen dieser Datenbanken werden Tools für die Migration von Daten zur Postgres-Datenbank bereitgestellt.

Der gemeinsame Workflow für das Einrichten der Orchestrator-Datenbank besteht aus folgenden Schritten:

- 1 Erstellen Sie eine Datenbank. Weitere Informationen zum Erstellen einer Datenbank finden Sie in der Dokumentation Ihres Datenbankherstellers.
- 2 Aktivieren Sie die Remoteverbindungen für die Datenbank.
- 3 Konfigurieren Sie die Datenbankverbindungsparameter. Weitere Informationen finden Sie unter [Konfigurieren der Orchestration-Datenbankverbindung](#).

Wenn Sie planen, einen Orchestrator-Cluster einzurichten, müssen Sie die Datenbank so konfigurieren, dass sie mehrere Verbindungen akzeptiert. Damit kann sie Verbindungen von verschiedenen Orchestrator-Serverinstanzen im Cluster akzeptieren.

Die Konfiguration der Datenbank kann die Leistung von Orchestrator beeinflussen. Installieren Sie die Datenbank auf einer anderen Maschine als der, auf der der Orchestrator-Server installiert ist. Mit diesem Ansatz ist sichergestellt, dass die JVM und der Datenbankserver nicht dieselbe CPU, denselben Arbeitsspeicher und dasselbe E/A-System verwenden.

Der Standort der Datenbank ist wichtig, weil fast jede Aktivität auf dem Orchestrator-Server Vorgänge in der Datenbank auslöst. Zur Vermeidung von Latenz in der Datenbankverbindung richten Sie eine Verbindung zu dem Datenbankserver ein, der geografisch dem Orchestrator-Server am nächsten und in einem Netzwerk mit der besten verfügbaren Bandbreite liegt.

Die Größe der Orchestrator-Datenbank variiert je nach der Konfiguration und der Art, wie Workflowtoken verarbeitet werden. Weisen Sie rund 50 KB für jedes vCenter Server-Objekt und 4 KB für jede Workflowausführung zu.

Vorsicht Vergewissern Sie sich, dass mindestens 1 GB Festplattenspeicher auf der Maschine verfügbar ist, auf der die Orchestrator-Datenbank installiert ist.

Unzureichender Festplattenspeicher kann dazu führen, dass der Orchestrator-Server und der Client nicht ordnungsgemäß funktionieren.

Installieren von Orchestrator

4

Orchestrator besteht aus einer Server- und einer Clientkomponente.

Der installierbare Orchestrator-Client kann auf Maschinen mit Windows, Linux und Mac (jeweils mit 64 Bit) ausgeführt werden.

Um Orchestrator zu verwenden, müssen Sie den Orchestrator-Serverdienst und anschließend den Orchestrator-Client starten.

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

Dieses Kapitel enthält die folgenden Themen:

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

Herunterladen und Bereitstellen der Orchestrator Appliance

Laden Sie eine Orchestrator Appliance herunter und installieren Sie sie, indem Sie sie über eine Vorlage bereitstellen.

Voraussetzungen

- Stellen Sie sicher, dass vCenter Server installiert ist und ausgeführt wird.
- Stellen Sie sicher, dass der Host, auf dem Sie die Appliance bereitstellen, die Mindestanforderungen für die Hardware erfüllt. Weitere Informationen finden Sie unter [Hardwareanforderungen für die 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 im vSphere Web Client ein Bestandslistenobjekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, z. B. Datencenter, 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 Überprüfen Sie Details der OVF-Vorlage und klicken Sie auf **Weiter**.
- 6 Akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 7 Geben Sie den Namen und den Speicherort der bereitgestellten Appliance an und klicken Sie auf **Weiter**.
- 8 Wählen Sie einen Host, ein Cluster, einen Ressourcenpool oder eine vApp als Ziel für die Ausführung der Appliance aus und klicken Sie auf **Weiter**.
- 9 Wählen Sie ein Format, in dem Sie die virtuelle Festplatte und den Speicher der Appliance speichern 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 Wählen Sie die Optionen aus, die Sie aktivieren möchten, und richten Sie das anfängliche Kennwort für das Root-Benutzerkonto ein.

Das anfängliche Kennwort muss mindestens acht Zeichen umfassen.

Wichtig Das Kennwort für das Root-Konto der Orchestrator Appliance läuft nach 365 Tagen ab. Sie können die Ablaufzeit für ein Konto erhöhen, indem Sie sich als Root-Benutzer bei der Orchestrator Appliance anmelden und dann `passwd -x number_of_days name_of_account` ausführen. Wenn Sie die Laufzeit des Root-Kennworts für die Orchestrator Appliance auf „unendlich“ erhöhen möchten, führen Sie `passwd -x 99999 root` aus.

- 11 (Optional) Konfigurieren Sie die Netzwerkeinstellungen und klicken Sie auf **Weiter**.

Die Orchestrator Appliance verwendet standardmäßig DHCP. Sie können diese Einstellung ändern und über die Webkonsole der Appliance eine statische IP-Adresse zuweisen.

- 12 Überprüfen Sie die Angaben auf der Seite „Bereit zum Abschließen“ und klicken Sie auf **Fertig stellen**.

Ergebnisse

Die Orchestrator Appliance wurde bereitgestellt.

Einschalten der Orchestrator Appliance und Öffnen der Startseite

Um die Orchestrator Appliance zu verwenden, müssen Sie sie zunächst einschalten und eine IP-Adresse für die virtuelle Appliance abrufen.

Verfahren

- 1 Melden Sie sich bei als Administrator beim vSphere Web Client an.
- 2 Klicken Sie mit der rechten Maustaste auf Orchestrator Appliance und wählen Sie **Stromversorgung > Einschalten**.
- 3 Auf der Registerkarte **Übersicht** ist die Orchestrator Appliance IP-Adresse angegeben.
- 4 Navigieren Sie in einem Webbrowser zu der IP-Adresse Ihrer virtuellen Orchestrator Appliance-Maschine.

`http://orchestrator_appliance_ip`

Ändern des Root-Kennworts

Aus Sicherheitsgründen können Sie das Root-Kennwort von Orchestrator Appliance ändern.

Wichtig Das Kennwort für das Root-Konto der Orchestrator Appliance läuft nach 365 Tagen ab. Sie können die Ablaufzeit für ein Konto erhöhen, indem Sie sich als Root-Benutzer bei der Orchestrator Appliance anmelden und dann `passwd -x number_of_days name_of_account` ausführen. Wenn Sie die Laufzeit des Root-Kennworts für die Orchestrator Appliance auf „unendlich“ erhöhen möchten, führen Sie den Befehl `passwd -x 99999 root` aus.

Voraussetzungen

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

Verfahren

- 1 Navigieren Sie in einem Webbrowser zu `https://orchestrator_appliance_ip:5480`.
- 2 Geben Sie den Benutzernamen und das Kennwort für die Appliance ein.
- 3 Klicken Sie auf die Registerkarte **Admin**.
- 4 Geben Sie das aktuelle Root-Kennwort in das Textfeld **Aktuelles Administratorkennwort** ein.
- 5 Geben Sie das neue Kennwort in die Textfelder **Neues Administratorkennwort** und **Neues Administratorkennwort erneut eingeben** ein.
- 6 Klicken Sie auf **Kennwort ändern**.

Ergebnisse

Sie haben das Kennwort des Linux-Root-Benutzers der Orchestrator Appliance erfolgreich geändert.

Aktivieren und Deaktivieren der SSH-Administratoranmeldung bei der vRealize Orchestrator Appliance

Sie können die Möglichkeit einer Anmeldung über SSH bei Orchestrator Appliance als Root aktivieren bzw. deaktivieren.

Voraussetzungen

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

Verfahren

- 1 Navigieren Sie in einem Webbrowser zu `https://orchestrator_appliance_ip:5480`.
- 2 Melden Sie sich als „root“ an.
- 3 Wählen Sie auf der Registerkarte **Admin** die Option **SSH-Dienst aktivieren**, um den SSH-Dienst von Orchestrator zu aktivieren.
- 4 (Optional) Klicken Sie auf **SSH-Administratoranmeldung aktiviert**, um die Anmeldung bei Orchestrator Appliance als Root über SSH zuzulassen.
- 5 Klicken Sie auf **Einstellungen speichern**.

Ergebnisse

Der **SSH-Status** wird als *Wird ausgeführt* angezeigt.

Konfigurieren der Netzwerkeinstellungen für die Orchestrator Appliance

Konfigurieren Sie die Netzwerkeinstellungen der Orchestrator Appliance, um eine statische IP-Adresse zuzuweisen und die Proxy-Einstellungen zu definieren.

Voraussetzungen

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

Verfahren

- 1 Navigieren Sie in einem Webbrowser zu `https://orchestrator_appliance_ip:5480`.
- 2 Melden Sie sich als „root“ an.
- 3 Klicken Sie auf der Registerkarte **Netzwerk** auf **Adresse**.

- 4 Wählen Sie die Methode aus, über die die Appliance die Einstellungen der IP-Adresse erhält.

Option	Beschreibung
DHCP	Erhält IP-Einstellungen von einem DHCP-Server. Dies ist die Standardeinstellung.
Statisch	Verwendet statische IP-Einstellungen. Geben Sie die IP-Adresse, die Netzmaske und das Gateway ein.

Abhängig von Ihren Netzwerkeinstellungen müssen Sie möglicherweise einen Adresstypen auswählen (IPv4 oder IPv6).

- 5 (Optional) Geben Sie die notwendigen Informationen zur Netzwerkkonfiguration ein.
- 6 Klicken Sie auf **Einstellungen speichern**.
- 7 (Optional) Nehmen Sie die Proxy-Einstellungen vor und klicken Sie auf **Einstellungen speichern**.

Erstkonfiguration

5

Bevor Sie mit der Automatisierung von Aufgaben und der Verwaltung von Systemen und Anwendungen mit Orchestrator beginnen, müssen Sie Orchestrator für die Verwendung eines externen Authentifizierungsanbieters konfigurieren und den verschiedenen Benutzern Rollen zuweisen. Sie können auch eine externe Datenbank einrichten, von einer Zertifizierungsstelle signierte Zertifikate importieren, Plug-Ins installieren oder die Konfiguration der Standardprotokolle ändern.

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren eines eigenständigen Orchestrator-Servers](#)
- [Orchestrator-Netzwerkports](#)
- [Konfigurieren der Orchestration-Datenbankverbindung](#)
- [Zertifikate verwalten](#)
- [Konfigurieren der Orchestrator-Plug-Ins](#)
- [Verfügbarkeit und Skalierbarkeit von Orchestrator](#)
- [Konfigurieren des Programms zur Verbesserung der Kundenzufriedenheit](#)

Konfigurieren eines eigenständigen Orchestrator-Servers

Bei der Orchestrator Appliance handelt es sich zwar um eine vorkonfigurierte Linux-basierte virtuelle Maschine, Sie müssen aber dennoch die Schritte im Konfigurationsassistenten ausführen, bevor Sie auf das Control Center von Orchestrator zugreifen.

Konfigurieren eines eigenständigen Orchestrator-Servers mit vRealize Automation-Authentifizierung

Um die Orchestrator Appliance für die Verwendung vorzubereiten, müssen Sie Hosteinstellungen und den Authentifizierungsanbieter konfigurieren. Sie können Orchestrator für die Authentifizierung über die Komponentenregistrierung von vRealize Automation konfigurieren.

Voraussetzungen

- Laden Sie die neueste Version der vRealize Orchestrator Appliance herunter und stellen Sie diese bereit. Siehe [Herunterladen und Bereitstellen der Orchestrator Appliance](#).
- Installieren und konfigurieren Sie vRealize Automation und stellen Sie sicher, dass Ihr vRealize Automation-Server ausgeführt wird. Weitere Informationen finden Sie in der vRealize Automation-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 in der Dokumentation zum vRealize Orchestrator-Lastausgleich.
- Richten Sie die externe Datenbank ein, die Sie als gemeinsame Datenbank vorgesehen haben, damit diese Verbindungen mit den verschiedenen Orchestrator-Instanzen aufbauen kann.

Verfahren

- 1 Rufen Sie das Control Center auf, um den Konfigurationsassistenten zu starten.
 - a Navigieren Sie zu `https://IP_oder_DNS-Name_Ihres_Orchestrator-Servers:8283/vco-controlcenter`.
 - b Melden Sie sich als **root** mit dem Kennwort an, das Sie bei der OVA-Bereitstellung eingegeben haben.
- 2 Wählen Sie den Bereitstellungstyp **Standalone-Orchestrator** aus.

Durch die Auswahl dieses Typs konfigurieren Sie einen Orchestrator-Einzelknoten oder den ersten Orchestrator-Knoten eines Clusters.
- 3 Klicken Sie auf **ÄNDERN**, um den Namen des Hosts zu konfigurieren, auf dem Control Center aufgerufen werden kann.

Hinweis Wenn Sie im Begriff sind, einen Orchestrator-Cluster zu konfigurieren, geben Sie den Hostnamen des virtuellen Lastausgleichsservers ein.

- 4 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**.
 - c Klicken Sie auf **Zertifikat akzeptieren**.

- d Geben Sie in die Textfelder **Benutzername** und **Kennwort** die Anmeldedaten des Benutzerkontos ein, das für die SSO-Verbindung in vRealize Automation konfiguriert ist. Klicken Sie auf **REGISTRIEREN**.

Standardmäßig wird das SSO-Konto **administrator** 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\vcadmins**

- f Doppelklicken Sie in der Liste der Gruppen auf den Namen der Gruppe, um sie auszuwählen.

- g Klicken Sie auf **ÄNDERUNGEN SPEICHERN**.

Der erfolgreiche Speichervorgang wird in einer Meldung bestätigt, und Sie werden an die Hauptansicht des Control Center umgeleitet.

- 5 (Optional) Konfigurieren Sie den Orchestrator-Knoten für die Verwendung einer externen gemeinsam genutzten Datenbank. Weitere Informationen finden Sie unter [Konfigurieren der Datenbankverbindung](#).

Ergebnisse

Sie haben die Control Center-Konfiguration erfolgreich abgeschlossen.

Nächste Schritte

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

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

Konfigurieren eines eigenständigen Orchestrator-Servers mit vSphere-Authentifizierung

Sie registrieren den 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. Siehe [Herunterladen und Bereitstellen der 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 in der Dokumentation zum vRealize Orchestrator-Lastausgleich.
- Richten Sie die externe Datenbank ein, die Sie als gemeinsame Datenbank vorgesehen haben, damit diese Verbindungen mit den verschiedenen Orchestrator-Instanzen aufbauen kann.

Verfahren

- 1 Rufen Sie das Control Center auf, um den Konfigurationsassistenten zu starten.

- a Navigieren Sie zu `https://IP_oder_DNS-Name_Ihres_Orchestrator-Servers:8283/vco-controlcenter`.
- b Melden Sie sich als **root** mit dem Kennwort an, das Sie bei der OVA-Bereitstellung eingegeben haben.

- 2 Wählen Sie den Bereitstellungstyp **Standalone-Orchestrator** aus.

Durch die Auswahl dieses Typs konfigurieren Sie einen Orchestrator-Einzelknoten oder den ersten Orchestrator-Knoten eines Clusters.

- 3 Klicken Sie auf **ÄNDERN**, um den Namen des Hosts zu konfigurieren, auf dem Control Center aufgerufen werden kann.

Hinweis Wenn Sie im Begriff sind, einen Orchestrator-Cluster zu konfigurieren, geben Sie den Hostnamen des virtuellen Lastausgleichsservers ein.

- 4 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 Domänennamen 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 alle Platform Services Controller-Zertifikate, die die gleiche vCenter Single Sign-On-Domäne nutzen, manuell in Orchestrator importieren.

- c Klicken Sie auf **Zertifikat akzeptieren**.

- d Geben Sie in die Textfelder **Benutzername** und **Kennwort** 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 Doppelklicken Sie in der Liste der Gruppen auf den Namen der Gruppe, um sie auszuwählen.

- g Klicken Sie auf **ÄNDERUNGEN SPEICHERN**.

Der erfolgreiche Speichervorgang wird in einer Meldung bestätigt, und Sie werden an die Hauptansicht des Control Center umgeleitet.

- 5 (Optional) Konfigurieren Sie den Orchestrator-Knoten für die Verwendung einer externen gemeinsam genutzten Datenbank. Weitere Informationen finden Sie unter [Konfigurieren der Datenbankverbindung](#).

Ergebnisse

Sie haben die Control Center-Konfiguration 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 Orchestrator-Server automatisch nach 2 Minuten neu gestartet. Wenn Sie die Konfiguration unmittelbar nach Abschluss des Prozesses überprüfen, kann es vorkommen, dass ein ungültiger Konfigurationsstatus zurückgegeben wird.

Orchestrator-Netzwerkports

Orchestrator benutzt spezifische Ports zur Kommunikation mit den anderen Systemen. Die Ports werden mit einem Standardwert eingerichtet, der nicht geändert werden kann.

Standardkonfigurationsports

Zu Bereitstellung des Orchestrator-Dienstes müssen Sie Standardports einrichten und Ihre Firewall so konfigurieren, dass ankommende TCP-Verbindungen zugelassen werden.

Hinweis Andere Ports können erforderlich sein, wenn Sie benutzerdefinierte Plug-Ins verwenden.

Tabelle 5-1. VMware vRealize Orchestrator Standardkonfigurationsports

Port	Zahl	Protokoll	Quelle	Ziel	Beschreibung
Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI)	5480	TCP			Der Zugriffspunkt für die Schnittstelle mit den Systemeinstellungen der Appliance.
HTTP-Serverport	8280	TCP	Endbenutzer-Webbrowser	Orchestrator-Server	Die Anforderungen, die an den Standard-HTTP-Webport 8280 von Orchestrator gesendet wurden, werden an den Standard-HTTPS-Webport 8281 umgeleitet.
HTTPS-Serverport	8281	TCP	Endbenutzer-Webbrowser	Orchestrator-Server	Der Zugriffspunkt für die Startseite von Orchestrator.
HTTPS-Zugriffspunkt für Webkonfiguration	8283	TCP	Endbenutzer-Webbrowser	Orchestrator-Konfiguration	Der SSL-Zugangspunkt zur Webschnittstelle der Orchestrator-Konfiguration.

Externe Kommunikationsports

Sie müssen Ihre Firewall so konfigurieren, dass abgehende Verbindungen zulässig sind und Orchestrator mit externen Diensten kommunizieren kann.

Tabelle 5-2. VMware vRealize Orchestrator Externe Kommunikationsports

Port	Zahl	Protokoll	Quelle	Ziel	Beschreibung
SQL Server	1433	TCP	Orchestrator-Server	Microsoft SQL Server	Der Port, der für die Kommunikation mit den Microsoft SQL Server-Instanzen verwendet wird, die als Orchestrator-Datenbank konfiguriert wurden.
PostgreSQL	5432	TCP	Orchestrator-Server	PostgreSQL Server	Der Port, der für die Kommunikation mit dem PostgreSQL Server verwendet wird, der als Orchestrator-Datenbank konfiguriert wurde.

Tabelle 5-2. VMware vRealize Orchestrator Externe Kommunikationsports (Fortsetzung)

Port	Zahl	Protokoll	Quelle	Ziel	Beschreibung
Oracle	1521	TCP	Orchestrator-Server	Oracle DB Server	Der Port, der für die Kommunikation mit dem Oracle Datenbankserver verwendet wird, der als Orchestrator-Datenbank konfiguriert wurde.
SMTP-Server-Port	25	TCP	Orchestrator-Server	SMTP-Server	Der für E-Mail-Benachrichtigungen verwendete Port.
vCenter Server API-Port	443	TCP	Orchestrator-Server	vCenter Server	Der vCenter Server-API-Kommunikationsport, der von Orchestrator verwendet wird, um Informationen über die virtuelle Infrastruktur und die virtuellen Maschinen von registrierten vCenter Server-Instanzen zu erhalten.

Konfigurieren der Orchestration-Datenbankverbindung

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

Wenn Sie die Orchestrator Appliance herunterladen und bereitstellen, wird der Orchestrator-Server zum Einsatz mit der in der Appliance vorinstallierten PostgreSQL-Datenbank konfiguriert.

Die vorkonfigurierte Orchestrator PostgreSQL-Datenbank ist bereit für den Produktionseinsatz. Um eine bessere Leistung in einer Produktionsumgebung mit hoher Last zu erreichen, installieren Sie ein separates Managementsystem für relationale Datenbanken (RDBMS) und erstellen eine Datenbank für Orchestrator. Weitere Informationen zum Erstellen von Datenbanken für Orchestrator finden Sie unter [Einrichten der Orchestrator-Datenbank](#). Damit Sie die externe Datenbank mit Orchestrator verwenden können, müssen Sie diese für Remoteverbindungen konfigurieren.

Importieren des Datenbank-SSL-Zertifikats

Wenn Ihre Datenbank SSL nutzt, müssen Sie die SSL-Zertifikatsdatei in Control Center importieren und eine sichere Verbindung zwischen Orchestrator und der Datenbank herstellen.

Voraussetzungen

- Konfigurieren Sie Ihre Datenbank für den SSL-Zugriff. Anweisungen finden Sie in der Dokumentation Ihrer Datenbank.
- Rufen Sie ein selbstsigniertes oder von einer Zertifizierungsstelle signiertes Zertifikat ab.
- Geben Sie explizit das vertrauenswürdige Zertifikat für die ordnungsgemäße SSL-Autorisierung an.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Klicken Sie auf **Zertifikate**.
- 3 Klicken Sie auf der Registerkarte **Vertrauenswürdige Zertifikate** auf **Importieren**.

4 Laden Sie das Datenbank-SSL-Zertifikat von einer URL oder aus einer Datei.

Option	Aktion
Aus URL oder Proxy-URL importieren	Geben Sie die URL des Datenbankservers ein: <i>https://Ihre_Datenbank_Server_IP_Adresse</i> oder <i>Ihre_Datenbank_Server_IP_Adresse:Port</i>
Aus Datei importieren	Rufen Sie die Datenbank-SSL-Zertifikatsdatei ab und navigieren Sie zum Import.

Ergebnisse

Das importierte Zertifikat wird in der Liste „Vertrauenswürdige SSL-Zertifikate“ angezeigt. Die sichere Verbindung zwischen Orchestrator und Ihrer Datenbank ist aktiviert.

Nächste Schritte

Wenn Sie die Datenbankverbindung konfigurieren, müssen Sie in Control Center auf der Seite **Datenbank konfigurieren** SSL aktivieren.

Konfigurieren der Datenbankverbindung

Wenn Sie eine Verbindung zur Orchestrator-Datenbank herstellen möchten, müssen Sie die Parameter für die Datenbankverbindung festlegen.

Voraussetzungen

- Richten Sie eine neue Datenbank zur Verwendung mit dem Orchestrator-Server ein. Siehe [Einrichten der Orchestrator-Datenbank](#).
- Wenn Sie eine SQL Server-Datenbank nutzen, die für die Verwendung dynamischer Ports konfiguriert ist, überprüfen Sie, ob der SQL Server Browser-Dienst ausgeführt wird.
- Zur Vermeidung von Deadlocks bei der Übertragung müssen Sie bei Nutzung der Microsoft SQL Server-Datenbank die Datenbankoptionen ALLOW_SNAPSHOT_ISOLATION und READ_COMMITTED_SNAPSHOT aktivieren.
- Wenn Ihre Microsoft SQL Server-Datenbank dynamische Ports verwendet, stellen Sie sicher, dass der SQL Server Browser ausgeführt wird.
- Um bei der Verwendung der Oracle-Datenbank den Fehler ORA-01450 zu vermeiden, überprüfen Sie, ob Sie die Größe des Datenbankblocks ordnungsgemäß konfiguriert haben. Die erforderliche Mindestgröße hängt von der Größe des Blocks ab, der vom Index Ihrer Oracle-Datenbank verwendet wird.
- Um Zeichen im richtigen Format in einer Oracle-Datenbank zu speichern, legen Sie den Parameter NLS_CHARACTER_SET auf AL32UTF8 fest, bevor Sie die Datenbankverbindung konfigurieren und die Tabellenstruktur einrichten. Diese Einstellung ist für eine internationalisierte Umgebung von wesentlicher Bedeutung.

- Wenn Sie Orchestrator für die Kommunikation mit der Datenbank über eine sichere Verbindung konfigurieren möchten, müssen Sie das SSL-Zertifikat für die Datenbank importieren. Weitere Informationen finden Sie unter [Importieren des Datenbank-SSL-Zertifikats](#).

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Klicken Sie auf **Datenbank konfigurieren**.
- 3 Wählen Sie im Dropdown-Menü **Datenbanktyp** den Datenbanktyp aus, den der Orchestrator-Server verwenden soll.

Option	Beschreibung
Oracle	Konfiguriert Orchestrator für das Arbeiten mit einer Oracle-Datenbankinstanz.
SQL Server	Konfiguriert Orchestrator für das Arbeiten mit einer Microsoft SQL Server-Datenbankinstanz.
PostgreSQL	Konfiguriert Orchestrator für das Arbeiten mit einer PostgreSQL-Datenbankinstanz.
In-Process-Datenbank DerbyDB	Konfiguriert Orchestrator für das Arbeiten mit der In-Process-Datenbank DerbyDB.
	Hinweis Sie dürfen DerbyDB nicht verwenden.

Hinweis Die Microsoft SQL Server- und die Oracle-Datenbank sind veraltet und werden in künftigen Versionen entfernt. Bis dahin werden die Microsoft SQL Server- und die Oracle-Datenbank vollständig unterstützt. Nach dem Entfernen dieser Datenbanken werden Tools für die Migration von Daten zur Postgres-Datenbank bereitgestellt.

- 4 Geben Sie die Parameter für die Datenbankverbindung ein und klicken Sie auf **Änderungen speichern**.

Option	Beschreibung
Serveradresse	Die IP-Adresse oder der DNS-Name des Datenbankservers. Diese Option ist auf alle Datenbanken anwendbar.
Port	Der Port des Datenbankservers wird für die Kommunikation mit Ihrer Datenbank verwendet. Diese Option ist auf alle Datenbanken anwendbar.
SSL verwenden	Wählen Sie SSL verwenden aus, um eine SSL-Verbindung zur Datenbank zu verwenden. Wenn Sie diese Option verwenden möchten, müssen Sie das SSL-Zertifikat der Datenbank in Orchestrator importieren. Diese Option ist auf alle Datenbanken anwendbar.

Option	Beschreibung
Datenbankname	<p>Der vollständige eindeutige Name Ihrer Datenbank. Der Datenbankname ist im Parameter SERVICE_NAMES in der Datei mit den Initialisierungsparametern angegeben.</p> <p>Diese Option ist nur für SQL Server- und PostgreSQL-Datenbanken gültig.</p>
Benutzername	<p>Der Benutzername, mit dem Orchestrator eine Verbindung zur ausgewählten Datenbank herstellt und sie bedient. Der von Ihnen ausgewählte Name muss ein gültiger Benutzer in der Zieldatenbank mit db_owner-Rechten sein.</p> <p>Diese Option ist auf alle Datenbanken anwendbar.</p> <p>Hinweis Der Standardbenutzername für die vorkonfigurierte PostgreSQL-Datenbank lautet vmware.</p>
Kennwort	<p>Das Kennwort für den Benutzernamen.</p> <p>Diese Option ist auf alle Datenbanken anwendbar.</p> <p>Hinweis Das Standardkennwort für die vorkonfigurierte PostgreSQL-Datenbank lautet vmware.</p>
Instanzname (sofern vorhanden)	<p>Der Name der Datenbankinstanz, die durch den Parameter INSTANCE_NAME in der Datei mit dem Datenbankinitialisierungsparameter identifiziert werden kann.</p> <p>Diese Option ist nur für SQL Server- und Oracle-Datenbanken gültig.</p>
Domäne	<p>Wenn Sie die Windows-Authentifizierung verwenden möchten, geben Sie den Domänennamen des SQL Servercomputers ein (z. B. <i>Unternehmen.org</i>). Wenn Sie die SQL-Authentifizierung verwenden möchten, lassen Sie dieses Textfeld unausgefüllt.</p> <p>Diese Option ist nur für SQL Server gültig und legt fest, ob Sie Windows- oder SQL Server-Authentifizierung verwenden möchten.</p>
Windows-Authentifizierungsmodus (NTLMv2) verwenden	<p>Wählen Sie diese Option aus, um NTLMv2-Antworten bei Verwendung der Windows-Authentifizierung zu senden.</p> <p>Diese Option ist nur für SQL Server gültig.</p>

Wenn die angegebenen Parameter richtig sind, wird eine Meldung angezeigt, dass die Verbindung zur Datenbank erfolgreich hergestellt wurde.

5 Aktualisieren Sie bei Bedarf die Tabellenstruktur für Orchestrator.

6 Klicken Sie auf **Änderungen speichern**.

Ergebnisse

Die Datenbankverbindung wurde erfolgreich konfiguriert.

Exportieren der Orchestrator-Datenbank

Erstellen Sie ein Archiv mit einer vollständigen Sicherung der Serverdatenbank. Sie können nur eine PostgreSQL-Datenbank exportieren.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Klicken Sie auf **Datenbank exportieren**.
- 3 Wählen Sie, welche Elemente Sie exportieren möchten.
- 4 Klicken Sie auf **Datenbank exportieren**.

Ergebnisse

Control Center erstellt die Datei `vco-db-dump-Datenbankname@Hostname.gz` auf dem System, auf dem Sie die Orchestrator Appliance installiert haben. Sie können diese Datei zum Klonen der Datenbank und zum Wiederherstellen des Orchestrator-Systems nutzen.

Importieren einer Orchestrator-Datenbank

Sie können eine zuvor exportierte Datenbank nach einer Neuinstallation von Orchestrator oder einem Systemausfall importieren.

Voraussetzungen

Die neue Orchestrator-Datenbank muss leer sein.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Klicken Sie auf **Datenbank importieren**.
- 3 Navigieren Sie zu der `.gz`-Datei, die Sie aus Ihrer vorherigen Installation exportiert haben.
- 4 Klicken Sie auf **Datenbank importieren**.

Ergebnisse

Eine Meldung, dass die Datenbank erfolgreich importiert wurde, wird angezeigt. Das neue System übernimmt die Datenbank des alten Systems.

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 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.

Wichtig Sie können das Serverzertifikat nicht ändern, wenn Orchestrator die prozessintegrierte Apache Derby-Datenbank verwendet.

■ [Verwalten von Orchestrator-Zertifikaten](#)

Sie können die Orchestrator-Zertifikate über die Seite **Zertifikate** in Control Center oder über den Orchestrator-Client verwalten, indem Sie die Workflows für SSL-Trust-Manager aus der Workflowkategorie „Konfiguration“ verwenden.

Verwalten von Orchestrator-Zertifikaten

Sie können die Orchestrator-Zertifikate über die Seite **Zertifikate** in Control Center oder über den Orchestrator-Client verwalten, indem Sie die Workflows für SSL-Trust-Manager aus der Workflowkategorie „Konfiguration“ verwenden.

Importieren eines Zertifikats in den Orchestrator Trust Store

Control Center 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 SSL-Zertifikat über eine URL oder eine PEM-kodierte Datei importieren. Sie müssen jedes Mal, wenn Sie eine SSL-Verbindung zu einer Serverinstanz verwenden möchten, zuerst das entsprechende Zertifikat über die Registerkarte

Vertrauenswürdige Zertifikate auf der Seite **Zertifikate** und dann das entsprechende SSL-Zertifikat importieren.

Sie können das SSL-Zertifikat in Orchestrator von 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. Weitere Informationen zum Importieren einer PEM-kodierten Zertifikatsdatei finden Sie unter Importieren eines vertrauenswürdigen Zertifikats über Control Center .

Erstellen eines selbstsignierten Zertifikats

In der Orchestrator Appliance ist ein selbstsigniertes Zertifikat enthalten, das automatisch anhand der Netzwerkeinstellungen der Appliance generiert wird. Bei Änderungen an den Netzwerkeinstellungen der Appliance müssen Sie manuell ein neues selbstsigniertes Zertifikat erstellen. Indem Sie ein selbstsigniertes Zertifikat 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.

Ein selbstsigniertes Zertifikat können Sie auf der Registerkarte **Orchestrator-Server-SSL-Zertifikat** auf der Seite **Zertifikate** in Control Center erstellen.

Option	Beschreibung
Signaturalgorithmus	Verschlüsselungsalgorithmus zum Generieren einer digitalen Signatur.
Allgemeiner Name	Hostname des Orchestrator-Servers.
Organisation	Name Ihrer Organisation. Beispiel: VMware .
Organisationseinheit	Name Ihrer Organisationseinheit. Beispiel: Forschung und Entwicklung .
Ländercode	Abkürzung des Ländercodes. Beispiel: US .

Orchestrator generiert ein für Ihre Umgebung eindeutiges Serverzertifikat. Die Details für den öffentlichen Schlüssel des Zertifikats werden auf der Registerkarte **Orchestrator-Server-SSL-Zertifikat** angezeigt. Der private Schlüssel wird in der vmo_keystore-Tabelle der Orchestrator-Datenbank gespeichert.

Importieren eines Orchestrator-Server-SSL-Zertifikats

vRealize Orchestrator nutzt ein SSL-Zertifikat, um sich während der sicheren Kommunikation für Clients und Remoteserver auszuweisen. In Orchestrator ist standardmäßig ein selbstsigniertes SSL-Zertifikat enthalten, das automatisch anhand der Netzwerkeinstellungen der Appliance generiert wird. Um Fehler im Zusammenhang mit der Vertrauenswürdigkeit des Zertifikats zu vermeiden, können Sie ein von einer Zertifizierungsstelle signiertes SSL-Zertifikat importieren.

Sie müssen das von einer Zertifizierungsstelle signierte Zertifikat als PEM-kodierte Datei importieren, die den öffentlichen und den privaten Schlüssel enthält.

Paketsignaturzertifikat

Pakete, die aus einem 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 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.

Hinweis In der Orchestrator Appliance ist ein selbstsigniertes Paketsignaturzertifikat enthalten, das automatisch bei der anfänglichen Konfiguration von Orchestrator generiert wird. Sie können das Paketsignaturzertifikat ändern. Danach werden alle Pakete, die Sie in Zukunft senden, mit dem neuen Zertifikat signiert.

Importieren eines vertrauenswürdigen Zertifikats über Control Center

Um mit anderen Servern sicher kommunizieren zu können, muss der Orchestrator-Server deren Identität prüfen können. Zu diesem Zweck müssen Sie möglicherweise das SSL-Zertifikat der

Remote-Einheit in den 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.

Voraussetzungen

Suchen Sie den vollqualifizierten Domännennamen des Servers, mit dem Orchestrator eine Verbindung über SSL herstellen soll.

Verfahren

- 1 Melden Sie sich bei der Orchestrator Appliance über SSH als **root** an.
- 2 Führen Sie einen Befehl zum Abrufen des Zertifikats des Remote-Servers aus.

```
openssl s_client -connect Host-oder_DNA-Name:Sicherer_Port
```

- a Wenn Sie einen unverschlüsselten Port verwenden, verwenden Sie **starttls** und das erforderliche Protokoll mit dem Befehl **openssl**.

```
openssl s_client -connect host_or_dns_name:port -starttls smtp
```

- 3 Kopieren Sie den Text vom Tag -----BEGIN CERTIFICATE----- bis zum Tag -----END CERTIFICATE----- in einen Texteditor und speichern Sie ihn als Datei.
- 4 Melden Sie sich beim Control Center als **root** an.
- 5 Wechseln Sie zur Seite **Zertifikate**.
- 6 Klicken Sie in der Registerkarte **Vertrauenswürdige Zertifikate** auf **Importieren** und wählen Sie die Option **Aus PEM-kodierter Datei importieren**.
- 7 Navigieren Sie zur Zertifikatsdatei und klicken Sie auf **Importieren**.

Ergebnisse

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

Konfigurieren der Orchestrator-Plug-Ins

Die Standard-Plug-Ins von Orchestrator werden nur durch Workflows konfiguriert.

Um eines der Orchestrator-Plug-Ins zu konfigurieren, müssen Sie einen bestimmten Workflow des Orchestrator-Clients verwenden.

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.

Ändern der Protokollierungsebene für Plug-Ins

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

Installieren oder Aktualisieren eines neuen Plug-Ins

Die vRealize Orchestrator-Plug-Ins ermöglichen die Integration anderer Softwareprodukte in den vRealize Orchestrator-Server. Die vRealize Orchestrator Appliance enthält einen Satz vorinstallierter Plug-Ins. Sie können auch 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. Dabei können die Dateierweiterungen `.vmoapp` und `.dar` verwendet werden. Eine `.vmoapp`-Datei kann eine Sammlung mehrerer `.dar`-Dateien enthalten und als Anwendung installiert werden. Eine `.dar`-Datei enthält alle Ressourcen, die einem Plug-In zugeordnet sind.

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

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

Deaktivieren von Plug-Ins

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

Mit dieser Aktion wird die Plug-In-Datei nicht entfernt. Weitere Informationen zum Deinstallieren eines Plug-Ins in Orchestrator finden Sie unter [Deinstallieren 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**.

- 5 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.

Deinstallieren eines Plug-Ins

Sie können das Control Center verwenden, um ein Plug-In zu löschen. Mit dieser Aktion wird jedoch nicht der gesamte Inhalt aus ihrer vRealize Orchestrator-Umgebung gelöscht. Nachdem Sie das-Plug-In aus dem Control Center gelöscht haben, müssen Sie die zugehörigen Plug-In-Pakete und Ordner aus dem vRealize Orchestrator-Client löschen.

Verfahren

- 1 Löschen Sie das Plug-In aus dem Orchestrator Control Center.
 - a Melden Sie sich beim Control Center als **root** an.
 - b Wählen Sie **Plug-Ins verwalten** aus.
 - c Suchen Sie nach dem Plug-In, das Sie löschen möchten, und klicken Sie auf das Löschesymbol.
 - d Klicken Sie auf **Löschen**.
- 2 Löschen der Plug-In-Pakete und Ordner aus dem vRealize Orchestrator-Client
 - a Melden Sie sich beim vRealize Orchestrator-Client an.
 - b Wählen Sie im Dropdown-Menü in der oberen linken Ecke die Option **Design** aus.
 - c Wählen Sie die Registerkarte **Pakete** aus.
 - d Klicken Sie mit der rechten Maustaste auf das zu löschende Paket und wählen Sie **Element mit Inhalt löschen**.

Hinweis Wählen Sie zum Löschen aller Plug-Ins, einschließlich freigegebener benutzerdefinierter Inhalte, **Alle löschen** aus. Um benutzerdefinierte Inhalte, die das Plug-In-Paket mit anderen vRealize Orchestrator-Objekten gemeinsam nutzt, beizubehalten, wählen Sie **Gemeinsam genutzt beibehalten** aus. vRealize Orchestrator-Inhalte, die im schreibgeschützten Zustand gesperrt sind, wie z. B. Workflows in der Standardbibliothek, werden nicht gelöscht, unabhängig davon, welche Option ausgewählt ist.

- e Wählen Sie die Registerkarte **Workflow** aus.
- f Erweitern Sie die Workflowbibliothek und löschen Sie den Ordner des Plug-Ins, das Sie entfernen möchten.

- g Wählen Sie die Registerkarte **Aktionen** aus.
- h Löschen Sie die Aktionsmodule des Plug-Ins, das Sie entfernen möchten.

3 Starten Sie die vRealize Orchestrator-Dienste neu.

```
service vco-configurator restart && service vco-server restart
```

Ergebnisse

Sie haben das Plug-In und seinen Inhalt in Ihrer vRealize Orchestrator-Umgebung deinstalliert.

Verfügbarkeit und Skalierbarkeit von Orchestrator

Um die Verfügbarkeit der Orchestrator-Dienste zu steigern, starten Sie mehrere Instanzen des 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.

Orchestrator-Cluster

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

Alle Instanzen des 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 kann dazu führen, dass ein Orchestrator-Clusterknoten nicht mehr reagiert. Wenn eine aktive Instanz des 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 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.

Orchestrator stellt kein integriertes Tool zum Überwachen des Clusterstatus und Senden von Failover-Benachrichtigungen bereit. Sie können den Clusterstatus mithilfe einer externen Komponente überwachen, etwa einem Lastausgleichsdienst. Um zu prüfen, ob ein Knoten ausgeführt wird, können Sie den REST-API-Dienst für den Systemzustand unter <https://>

IP_oder_DNS-Name_Ihres_Orchestrator-Servers:8281/vco/api/healthstatus aufrufen und den Status des Knotens prüfen. Mit dem unter *https://IP_oder_DNS-Name_Ihres_Orchestrator-Servers:8283/vco-controlcenter/docs/* verfügbaren Dienst können Sie den Status des Control Center überwachen.

Konfigurieren eines Orchestrator-Clusters

Wenn Sie die Orchestrator-Dienste skalieren und Orchestrator im Hochverfügbarkeitsmodus verwenden möchten, können Sie einen Cluster mit zwei oder mehr Orchestrator-Instanzen erstellen.

Hinweis Beim Konfigurieren eines NTP-Servers für Ihre geclusterte vRealize Orchestrator-Umgebung müssen Sie die IP-Adresse des NTP-Servers verwenden. Die Verwendung des vollqualifizierten Domännennamens des NTP-Servers kann zu einem Zeitüberschreitungsfehler führen.

Konfigurieren eines aus Orchestrator-Instanzen bestehenden Clusters mit vRealize Automation-Authentifizierung

Um einen Cluster zu bilden, können Sie eine einzelne Orchestrator-Instanz für die Verwendung von vRealize Automation als Authentifizierungsanbieter konfigurieren und andere Orchestrator-Knoten damit verbinden.

Ein Orchestrator-Cluster besteht aus mindestens zwei Orchestrator-Serverinstanzen, die sich eine Datenbank teilen.

Voraussetzungen

- Konfigurieren Sie einen eigenständigen Orchestrator-Serverknoten. Siehe [Konfigurieren eines eigenständigen Orchestrator-Servers mit vRealize Automation-Authentifizierung](#).
- Synchronisieren Sie die Uhren der virtuellen Maschinen, auf denen die Orchestrator-Serverinstanzen installiert sind.
- Richten Sie einen Lastausgleichsdienst ein, um den Datenverkehr auf mehrere Instanzen von vRealize Orchestrator zu verteilen. Entsprechende Informationen finden Sie in der Dokumentation zum vRealize Orchestrator-Lastausgleich.

Verfahren

- 1 Rufen Sie zum Starten des Konfigurationsassistenten das Control Center des Knotens auf, den Sie dem Cluster hinzufügen möchten.
 - a Navigieren Sie zu *https://IP_oder_DNS-Name_Ihres_Orchestrator-Servers:8283/vco-controlcenter*.
 - b Melden Sie sich als **root** mit dem Kennwort an, das Sie bei der OVA-Bereitstellung eingegeben haben.

- 2 Wählen Sie den Bereitstellungstyp **Orchestrator-Cluster** aus.

Durch die Auswahl dieses Typs fügen Sie den Knoten einem vorhandenen Orchestrator-Cluster hinzu.

- 3 Geben Sie in das Textfeld **Hostname** den Hostnamen oder die IP-Adresse der ersten Orchestrator-Serverinstanz ein.

Hinweis Hierbei muss es sich um die lokale IP-Adresse oder den Hostnamen der Orchestrator-Instanz handeln, der Sie den Cluster hinzufügen möchten. Verwenden Sie keine Lastausgleichsadresse.

- 4 Geben Sie in die Textfelder **Benutzername** und **Kennwort** die Anmeldedaten des Root-Benutzers für die erste Orchestrator-Serverinstanz ein.

- 5 Klicken Sie auf **Beitreten**.

Die Orchestrator-Instanz kloniert die Konfiguration des Knotens, mit dem sie verbunden wird, und wird automatisch neu gestartet.

Hinweis Die an die einzelnen Orchestrator-Knoten im Cluster gestellten Anforderungen werden vom Lastausgleichsserver verwaltet. Daher können Sie nicht mehr gesondert auf die verschiedenen Control Center zugreifen.

Ergebnisse

Sie haben erfolgreich ein Cluster von Orchestrator-Instanzen konfiguriert.

Nächste Schritte

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

Hinweis Nach der Konfiguration der Clusterinstanz wird der Orchestrator-Server automatisch nach 2 Minuten neu gestartet. Wenn Sie die Konfiguration unmittelbar nach Abschluss des Prozesses überprüfen, kann es vorkommen, dass ein ungültiger Clusterstatus zurückgegeben wird.

Konfigurieren eines aus Orchestrator-Instanzen bestehenden Clusters mit vSphere-Authentifizierung

Um einen Cluster zu bilden, können Sie eine einzelne Orchestrator-Instanz für die Verwendung von vCenter Single Sign-On als Authentifizierungsanbieter konfigurieren und andere Orchestrator-Knoten damit verbinden.

Ein Orchestrator-Cluster besteht aus mindestens zwei Orchestrator-Serverinstanzen, die sich eine Datenbank teilen.

Voraussetzungen

- Konfigurieren Sie einen eigenständigen Orchestrator-Serverknoten. Siehe [Konfigurieren eines eigenständigen Orchestrator-Servers mit vSphere-Authentifizierung](#).
- Synchronisieren Sie die Uhren der virtuellen Maschinen, auf denen die Orchestrator-Serverinstanzen installiert sind.
- Richten Sie einen Lastausgleichsdienst ein, um den Datenverkehr auf mehrere Instanzen von vRealize Orchestrator zu verteilen. Entsprechende Informationen finden Sie in der Dokumentation zum vRealize Orchestrator-Lastausgleich.

Verfahren

- 1 Rufen Sie zum Starten des Konfigurationsassistenten das Control Center des Knotens auf, den Sie dem Cluster hinzufügen möchten.
 - a Navigieren Sie zu `https://IP_oder_DNS-Name_Ihres_Orchestrator-Servers:8283/vco-controlcenter`.
 - b Melden Sie sich als **root** mit dem Kennwort an, das Sie bei der OVA-Bereitstellung eingegeben haben.

- 2 Wählen Sie den Bereitstellungstyp **Orchestrator-Cluster** aus.

Durch die Auswahl dieses Typs fügen Sie den Knoten einem vorhandenen Orchestrator-Cluster hinzu.

- 3 Geben Sie in das Textfeld **Hostname** den Hostnamen oder die IP-Adresse der ersten Orchestrator-Serverinstanz ein.

Hinweis Hierbei muss es sich um die lokale IP-Adresse oder den Hostnamen der Orchestrator-Instanz handeln, der Sie den Cluster hinzufügen möchten. Verwenden Sie keine Lastausgleichsadresse.

- 4 Geben Sie in die Textfelder **Benutzername** und **Kennwort** die Anmeldedaten des Root-Benutzers für die erste Orchestrator-Serverinstanz ein.

- 5 Klicken Sie auf **Beitreten**.

Die Orchestrator-Instanz kloniert die Konfiguration des Knotens, mit dem sie verbunden wird, und wird automatisch neu gestartet.

Hinweis Die an die einzelnen Orchestrator-Knoten im Cluster gestellten Anforderungen werden vom Lastausgleichsserver verwaltet. Daher können Sie nicht mehr gesondert auf die verschiedenen Control Center zugreifen.

Ergebnisse

Sie haben erfolgreich ein Cluster von Orchestrator-Instanzen konfiguriert.

Nächste Schritte

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

Hinweis Nach der Konfiguration der Clusterinstanz wird der Orchestrator-Server automatisch nach 2 Minuten neu gestartet. Wenn Sie die Konfiguration unmittelbar nach Abschluss des Prozesses überprüfen, kann es vorkommen, dass ein ungültiger Clusterstatus zurückgegeben wird.

Überwachen eines Orchestrator-Clusters

Nachdem Sie einen Cluster erstellt haben, können Sie die Zustände der Clusterknoten überwachen und weitere Maßnahmen ergreifen, damit die Knoten stets synchron sind.

Über die Registerkarte **Orchestrator-Knoteneinstellungen** auf der Seite **Orchestrator-Clusterverwaltung** in Control Center können Sie die Synchronisierungszustände der Konfiguration von Orchestrator-Instanzen überwachen, die in einem Cluster verbunden sind.

Konfigurations-Synchronisierungszustand	Beschreibung
WIRD AUSGEFÜHRT	Der Orchestrator-Dienst ist verfügbar und kann Anforderungen annehmen.
STANDBY	<p>Der 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 Orchestrator-Instanz – nicht prüfen.
Abrufen des Zustandsstatus des Dienstes fehlgeschlagen	Der Orchestrator-Dienst kann nicht kontaktiert werden, da er entweder gestoppt wurde oder ein Netzwerkproblem besteht.
Ausstehender Neustart	Control Center erkennt eine Änderung der Konfiguration und der Orchestrator-Server wird automatisch neu gestartet.

Konfigurieren des Programms zur Verbesserung der Kundenzufriedenheit

Wenn Sie sich zur Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit entscheiden, erhält VMware anonyme Informationen, mit deren Hilfe die Qualität, Zuverlässigkeit und Funktionalität der Produkte und Dienste von VMware verbessert werden kann.

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 [Am Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen](#) finden Sie Informationen, wie Sie dem CEIP beitreten oder aus dem CEIP austreten können.

Am Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen

Nehmen Sie am Programm zur Verbesserung der Benutzerfreundlichkeit im Control Center teil.

Verfahren

- 1 Melden Sie sich als **root** beim Control Center an und öffnen Sie die Seite **Programm zur Verbesserung der Benutzerfreundlichkeit**.
- 2 Wählen Sie das Kontrollkästchen **Am Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen** aus, um das Programm zu aktivieren, bzw. heben Sie die Auswahl des Kontrollkästchens auf, wenn Sie es deaktivieren möchten. Klicken Sie anschließend auf **Speichern**.
- 3 (Optional) Heben Sie die Auswahl des Kontrollkästchens für die **Automatische Proxy-Erkennung** auf, wenn Sie einen Proxy-Host manuell hinzufügen möchten.

Verwenden der API-Dienste

6

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

Das Konfigurations-Plug-In ist im Standardumfang des Orchestrator-Pakets enthalten. Sie können über die Orchestrator-Workflowbibliothek oder die Orchestrator-REST-API auf die Workflows des Konfigurations-Plug-Ins zugreifen. Mit diesen Workflows können Sie die Einstellungen für vertrauenswürdige Zertifikat und die Keystore des Orchestrator-Servers ändern. Informationen zu allen verfügbaren Orchestrator-REST-API-Dienstaufrufen finden Sie in der Dokumentation *Orchestrator-REST-API-Referenz* unter https://Orchestrator_Server_IP_oder_DNS_Name:8281/vco/api/docs.

- **Verwalten von SSL-Zertifikaten und Keystores mithilfe der REST-API**

Außer der Verwaltung von SSL-Zertifikaten über Control Center können Sie auch vertrauenswürdige Zertifikate und Keystores verwalten, wenn Sie Workflows über das Konfigurations-Plug-In ausführen oder indem Sie die REST-API verwenden.

- **Automatisieren der Orchestrator-Konfiguration mithilfe der Control Center-REST-API**

Die Control Center-REST-API bietet Zugriff auf die Ressourcen zum Konfigurieren des Orchestrator-Servers. Sie können die Orchestrator-Konfiguration mithilfe der Control Center-REST-API und Drittanbietersystemen automatisieren.

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

Außer der Verwaltung von SSL-Zertifikaten über Control Center können Sie auch vertrauenswürdige Zertifikate und Keystores verwalten, wenn Sie Workflows über das Konfigurations-Plug-In ausführen oder indem Sie die REST-API verwenden.

Das Konfigurations-Plug-In enthält Workflows zum Importieren und Löschen von SSL-Zertifikaten und Keystores. Um auf diese Workflows zuzugreifen, navigieren Sie in der Ansicht „Workflows“ des Orchestrator-Clients zu **Bibliothek > Konfiguration > SSL-Trust-Manager** und **Bibliothek > Konfiguration > Keystores**. Sie können diese Workflows auch mithilfe der Orchestrator-REST-API ausführen.

Löschen von SSL-Zertifikaten mithilfe der REST-API

Sie können ein SSL-Zertifikat mit dem Workflow „Vertrauenswürdiges Zertifikat 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 „Vertrauenswürdiges Zertifikat löschen“ aus.

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

- 2 Rufen Sie die Definition des Workflows „Vertrauenswürdiges Zertifikat löschen“ 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 „Vertrauenswürdiges Zertifikat löschen“ enthält.

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

- 4 Geben Sie den Namen des zu löschenden Zertifikats als Eingabeparameter des Workflows „Vertrauenswürdiges Zertifikat löschen“ in einem Ausführungskontext-Element im Hauptteil der Anforderung ein.

Importieren von SSL-Zertifikaten mithilfe der REST-API

Sie können SSL-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. Informationen zum Importieren von Zertifikaten in Orchestrator mithilfe von Control Center finden Sie unter [Verwalten von Orchestrator-Zertifikaten](#).

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 SSL-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 SSL-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 Führen 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.

Automatisieren der Orchestrator-Konfiguration mithilfe der Control Center-REST-API

Die Control Center-REST-API bietet Zugriff auf die Ressourcen zum Konfigurieren des Orchestrator-Servers. Sie können die Orchestrator-Konfiguration mithilfe der Control Center-REST-API und Drittanbietersystemen automatisieren.

Der Root-Endpoint der Control Center-REST-API ist `https://Orchestrator_Server_IP_oder_DNS_Name:8283/vco-controlcenter/api`. Informationen zu allen verfügbaren Dienstaufrufen mit der Control Center-REST-API finden Sie in der Dokumentation *Control Center-REST-API-Referenz* unter `https://Orchestrator_Server_IP_oder_DNS_Name:8283/vco-controlcenter/docs`.

Befehlszeilen-Dienstprogramm

Sie können das Befehlszeilen-Dienstprogramm von Orchestrator nutzen, um die Konfiguration von Orchestrator zu automatisieren.

Sie können auf das Befehlszeilen-Dienstprogramm zugreifen, indem Sie sich bei der Orchestrator Appliance über SSH als Root anmelden. Das Dienstprogramm befindet sich unter `/var/lib/vco/tools/configuration-cli/bin`. Zur Anzeige der verfügbaren Konfigurationsoptionen führen Sie `./vro-configure.sh --help` aus.

Zusätzliche Konfigurationsoptionen

7

Sie können mit Control Center das Standardverhalten von Orchestrator ändern.

Dieses Kapitel enthält die folgenden Themen:

- [Neukonfigurieren der Authentifizierung](#)
- [Exportieren der Orchestrator-Konfiguration](#)
- [Importieren der Orchestrator-Konfiguration](#)
- [Konfigurieren der Workflow-Ausführungseigenschaften](#)
- [Orchestrator-Protokolldateien](#)
- [Hinzufügen von Netzwerkkarten \(NICs\)](#)
- [Konfigurieren von statischen Routen](#)

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.

Voraussetzungen

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.

- 3 Klicken Sie im Abschnitt **IDENTITÄTSDIENST** auf **REGISTRIERUNG AUFHEBEN**, um die Anmeldedaten für den Server zu löschen.

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 Orchestrator-Servers mit vRealize Automation-Authentifizierung](#) oder [Konfigurieren eines eigenständigen Orchestrator-Servers mit vSphere-Authentifizierung](#).

Ändern der Authentifizierungsparameter

Wenn Sie vRealize Automation als Authentifizierungsanbieter im Control Center verwenden, müssen Sie möglicherweise den Standardmandanten der Orchestrator-Administratorgruppe ändern. Bei Verwendung der vSphere-Authentifizierung können Sie die Administratorgruppe ändern.

Voraussetzungen

- Melden Sie sich beim Control Center als **Administrator** an.
- Wählen Sie den Authentifizierungsmodus aus und konfigurieren Sie die Verbindungseinstellungen des Authentifizierungsanbieters.

Verfahren

- 1 Ändern Sie den Standardmandanten.

Hinweis Sie können den Standardmandanten nur im vRealize Automation-Authentifizierungsmodus ändern.

- a Klicken Sie auf der Seite **Anbieter für Authentifizierung konfigurieren** im Control Center auf die Schaltfläche **ÄNDERN** neben dem Textfeld **Standardmandant**.
- b Ersetzen Sie im Textfeld den Namen des vorhandenen Standardmandanten durch den Namen des gewünschten Mandanten.
- c 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.

- d Geben Sie den Namen einer Administratorgruppe ein und klicken Sie auf **SUCHEN**.

- e Doppelklicken Sie in der Liste der Gruppen auf den Namen der Gruppe, um sie auszuwählen.

- f Klicken Sie auf **ÄNDERUNGEN SPEICHERN**.

Sie werden beim Control Center abgemeldet und an den Single Sign-On-Anmeldebildschirm umgeleitet.

2 Ändern Sie die Administratorgruppe.

- a Klicken Sie auf die Schaltfläche **ÄNDERN** neben dem Textfeld **Admin-Gruppe**.
- b Geben Sie den Namen einer Administratorgruppe ein und klicken Sie auf **SUCHEN**.
- c Doppelklicken Sie in der Liste der Gruppen auf den Namen der Gruppe, um sie auszuwählen.
- d Klicken Sie auf **ÄNDERUNGEN SPEICHERN**.

Sie werden beim Control Center abgemeldet und an den Single Sign-On-Anmeldebildschirm umgeleitet.

Exportieren der Orchestrator-Konfiguration

Control Center bietet einen Mechanismus zum Exportieren der Orchestrator-Konfigurationseinstellungen in eine lokale Datei. Damit können Sie jederzeit einen Snapshot Ihrer Systemkonfiguration erstellen und diese Konfiguration in eine neue Instanz von Orchestrator importieren.

Sie sollten Ihre Konfigurationseinstellungen regelmäßig exportieren und speichern, insbesondere beim Vornehmen von Änderungen, Durchführen von Wartungsaufgaben oder Aktualisieren des Systems.

Wichtig Bewahren Sie die Datei mit der exportierten Konfiguration sicher auf, da sie vertrauliche administrative Informationen enthält.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Klicken Sie auf **Konfiguration exportieren/importieren**.
- 3 Wählen Sie den Typ der zu exportierenden Dateien aus.

Hinweis Wenn Sie **Plug-In-Konfigurationen exportieren** auswählen und die Plug-In-Konfigurationen verschlüsselte Eigenschaften enthalten, müssen Sie auch **Serverkonfiguration exportieren** auswählen, um die Daten beim Importieren zu verschlüsseln.

- 4 (Optional) Geben Sie ein Kennwort ein, um die Konfigurationsdatei zu schützen.
Verwenden Sie das gleiche Kennwort beim späteren Import der Konfiguration.

5 Klicken Sie auf **Exportieren**.

Ergebnisse

Orchestrator erstellt die Datei `orchestrator-config-export-hostname-dateReference.zip`, die auf Ihren lokalen Computer heruntergeladen wird. Sie können diese Datei zum Klonen oder Wiederherstellen des Systems nutzen.

Hinweis Wenn Sie sich für das Klonen der Orchestrator-Instanz entscheiden, dürfen Sie die Datenbankeinstellungen nicht in die geklonte Orchestrator-Instanz importieren. Sie müssen stattdessen eine Verbindung zu einer anderen externen Datenbank konfigurieren.

Importieren der Orchestrator-Konfiguration

Sie können eine zuvor exportierte Systemkonfiguration nach einer Neuinstallation von Orchestrator oder einem Systemausfall wiederherstellen.

Wenn Sie den Importvorgang verwenden, um die Orchestrator-Konfiguration zu klonen, wird die vCenter Server-Plug-In-Konfiguration ungültig und funktioniert nicht, weil eine neue vCenter Server-Plug-In-ID generiert wird.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Klicken Sie auf **Konfiguration exportieren/importieren** und navigieren Sie zur Registerkarte **Konfiguration importieren**.
- 3 Navigieren Sie zu der `.zip`-Datei, die Sie aus Ihrer vorherigen Installation exportiert haben.

Hinweis Die Standardsyntax für die exportierte Konfigurationsdatei lautet `orchestrator-config-export-Hostname-Exportdatum_Exportzeit.zip`

- 4 (Optional) Geben Sie das Kennwort ein, das Sie beim Exportieren der Konfiguration verwendet haben.

Dieser Schritt ist nicht erforderlich, wenn Sie die Konfiguration nicht mit einem Kennwort exportiert haben.

- 5 Wählen Sie den Importtyp aus:

Option	Beschreibung
Eingebettet	Migriert zu einer Orchestrator-Instanz, die in vRealize Automation eingebettet ist.
Extern	Migriert zu einer externen Orchestrator-Instanz.
Replikat	Repliziert die bestehende Orchestrator-Instanz.

- 6 Klicken Sie auf **Importieren**.

Ergebnisse

Das neue System repliziert die alte Konfiguration basierend auf dem ausgewählten Importtyp. Der Orchestrator-Serverdienst wird automatisch neu gestartet.

Nächste Schritte

Stellen Sie auf der Seite **Konfiguration validieren** in Control Center sicher, dass Orchestrator ordnungsgemäß konfiguriert ist.

Konfigurieren der Workflow-Ausführungseigenschaften

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

Wenn der Orchestrator-Knoten mehr als 300 Workflows gleichzeitig ausführen muss, werden die ausstehenden Workflowausführungen 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.

Auf der Seite **Erweiterte Optionen** in Control Center können Sie die Workflow-Ausführungseigenschaften konfigurieren.

Option	Beschreibung
Abgesicherten Modus aktivieren	Wenn der abgesicherte Modus aktiviert ist, werden alle laufenden Workflows abgebrochen. Sie werden nicht beim nächsten Start des Orchestrator-Knotens fortgesetzt.
Anzahl gleichzeitig laufender Workflows	Die maximale Anzahl von Workflows auf Orchestrator-Knoten, die gleichzeitig ausgeführt werden können.
Maximale Anzahl laufender Workflows in der Warteschlange	Die Anzahl von Workflow-Ausführungsanforderungen, die der Orchestrator-Knoten akzeptiert, bevor er nicht mehr verfügbar ist.
Maximale Anzahl gespeicherter Ausführungen pro Workflow	Die maximale Anzahl abgeschlossener Workflow-Ausführungen, die pro Workflow im Verlauf auf einem Cluster gespeichert werden. Wenn diese Anzahl überschritten wird, werden die ältesten Workflow-Ausführungen gelöscht.
Ablauf von Protokollereignissen (in Tagen)	Anzahl der Tage, die Protokollereignisse für den Cluster in der Datenbank bleiben, bevor sie gelöscht werden.

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.

Sie können ein ZIP-Paket mit den Konfigurations- und Protokolldateien von Orchestrator aus dem Menü **Protokolle exportieren** in Control Center herunterladen.

Tabelle 7-1. Liste der Orchestrator-Protokolldateien

File Name	Speicherort	Beschreibung
scripting.log	/var/log/vco/app-server	Enthält Skriptprotokollmeldungen für Workflows und Aktionen. Verwenden Sie die Datei scripting.log zur Unterscheidung von Workflowausführungen und Aktionsausführungen von normalen Orchestrator-Vorgängen. Diese Informationen sind auch in der Datei server.log enthalten.
server.log	/var/log/vco/app-server	Enthält Informationen zu sämtlichen Aktivitäten auf dem Orchestrator-Server. Analysieren Sie die Datei server.log zum Debuggen von Orchestrator oder beliebiger auf Orchestrator ausgeführter Anwendungen.
metrics.log	/var/log/vco/app-server	Enthält Laufzeitinformationen zum Server. Diese Informationen werden der Protokolldatei in Abständen von fünf Minuten hinzugefügt.
localhost_access_log.txt	/var/log/vco/app-server	Dies ist das HTTP-Anforderungsprotokoll des Servers.
localhost_access_log.Datum.txt	/var/log/vco/configuration	Dies ist das HTTP-Anforderungsprotokoll des Control Center-Dienstes.
controlcenter.log	/var/log/vco/configuration	Die Protokolldatei des Control Center-Dienstes.

Persistenz von Protokollen

Sie können Informationen in Orchestrator-Skripts beliebiger Art protokollieren, z. B. in Workflows, Richtlinien oder Aktionen. Für diese Informationen stehen Typen und Ebenen zur Verfügung. Typen können persistente oder nicht persistente sein. Die möglichen Ebenen sind DEBUG, INFO, WARN, ERROR, TRACE und FATAL.

Tabelle 7-2. Erstellen von persistenten und nicht persistenten Protokollen

Protokollierungsebene	Persistenter Typ	Nicht persistenter Typ
DEBUG	Server.debug("short text", "long text");	System.debug("text")
INFO	Server.log("short text", "long text");	System.log("text");
WARN	Server.warn("short text", "long text");	System.warn("text");
ERROR	Server.error("short text", "long text");	System.error("text");

Persistente Protokolle

Persistente Protokolle (Serverprotokolle) verfolgen Protokolle zu früheren Workflowausführungen und werden in der Orchestrator-Datenbank gespeichert. Um Serverprotokolle anzuzeigen, müssen Sie einen Workflow, eine abgeschlossene Workflowausführung oder eine Richtlinie auswählen und auf die Registerkarte **Ereignisse** im Orchestrator-Client klicken.

Nicht persistente Protokolle

Wenn Sie ein nicht persistentes Protokoll (Systemprotokoll) zum Erstellen von Skripten verwenden, benachrichtigt der Orchestrator-Server alle laufenden Orchestrator-Anwendungen über dieses Protokoll, diese Informationen werden jedoch nicht in der Datenbank gespeichert. Beim Neustart der Anwendung gehen die Protokollinformationen verloren. Nicht persistente Protokolle werden zum Debuggen und für Live-Informationen verwendet. Um Systemprotokolle anzuzeigen, müssen Sie eine abgeschlossene Workflowausführung im Orchestrator-Client auswählen und auf der Registerkarte **Schema** auf **Protokolle** klicken.

Konfiguration der 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.

Einstellungen für Protokollrotation

Um ein übermäßiges Anwachsen des Serverprotokolls zu vermeiden, definieren Sie die maximale Dateigröße und -anzahl des Serverprotokolls durch Anpassung der Werte in den Textfeldern **Max. Dateianzahl** und **Max. Dateigröße (MB)**.

Exportieren von Orchestrator-Protokolldateien

Auf der Seite **Protokolle exportieren** im Control Center können Sie ein ZIP-Archiv mit Fehlerbehebungsinformationen generieren, das Konfigurations-, Server-, Wrapper- und Installationsprotokolldateien enthält.

Die Protokollinformationen sind in einem ZIP-Archiv mit dem Namen `vco-logs-Datum_Uhrzeit.zip` gespeichert.

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

Filtern der Orchestrator-Protokolle

Sie können die Orchestrator-Serverprotokolle für eine bestimmte Workflowausführung filtern und Diagnosedaten zur Ausführung des Workflows erfassen.

Die Orchestrator-Protokolle enthalten viele nützliche Informationen, die Sie in Echtzeit überwachen können. Wenn mehrere Instanzen desselben Workflows gleichzeitig ausgeführt werden, können Sie die verschiedenen Workflowausführungen durch Filtern der Diagnosedaten zu den einzelnen Ausführungen im Live-Protokoll-Stream von Orchestrator verfolgen.

Hinweis Falls ein Cluster mehrere Orchestrator-Instanzen enthält, zeigt der Live-Protokoll-Stream nur die Protokolle des lokalen Orchestrator-Knotens an.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Klicken Sie auf **Live-Protokoll-Stream**.
- 3 Geben Sie in der Suchleiste Ihre Suchparameter ein.

Sie können die Protokolle beispielsweise nach Benutzernamen, Workflownamen, Workflow-IDs oder Token-IDs filtern.
- 4 (Optional) Wählen Sie **Groß-/Kleinschreibung beachten** und **Filtern (grep)** aus, um die Suchergebnisse noch engmaschiger zu filtern.

Die Auswahl von **Filtern (grep)** bewirkt, dass der Live-Stream nur die Zeilen anzeigt, die Ihren Suchparametern entsprechen.

Ergebnisse

Der Live-Protokoll-Stream von Orchestrator wird Ihren Suchparametern entsprechend gefiltert.

Nächste Schritte

Sie können Protokollanalysetools von Drittanbietern verwenden, wenn Sie alte Protokolle filtern möchten, die nicht über die Seite **Live-Protokoll-Stream** im Control Center zugänglich sind.

Hinzufügen von Netzwerkkarten (NICs)

vRealize Orchestrator unterstützt mehrere Netzwerkkarten (NICs). Nach der Installation können Sie der Orchestrator Appliance NICs hinzufügen.

Voraussetzungen

Installieren Sie vRealize Orchestrator vollständig in Ihrer vCenter Server-Umgebung.

Verfahren

- 1 Fügen Sie in vCenter Server jeder vRealize Orchestrator Appliance NICs hinzu.
 - a Klicken Sie mit der rechten Maustaste auf die Appliance und wählen Sie **Einstellungen bearbeiten** aus.
 - b Fügen Sie VMXNET3-NICs hinzu.
 - c Wenn die Appliance eingeschaltet ist, starten Sie sie neu.

- 2 Melden Sie sich als Root-Benutzer bei der Verwaltungsschnittstelle der vRealize Orchestrator Appliance an.

`https://Orchestrator_Appliance-IP:5480`

- 3 Wählen Sie **Netzwerk** aus und stellen Sie sicher, dass mehrere Netzwerkkarten verfügbar sind.
- 4 Wählen Sie die **Adresse** aus, und konfigurieren Sie die IP-Adresse für die Netzwerkkarten.

Tabelle 7-3. Beispiel für NIC-Konfiguration

Einstellung	Wert
IPv4-Adresstyp	Statisch
IPv4-Adresse	172.22.0.2
Netzmaske	255.255.255.0

- 5 Klicken Sie auf **Einstellungen speichern**.

Konfigurieren von statischen Routen

Wenn Sie Netzwerkkarten (NICs) zu einer vRealize Orchestrator-Installation hinzufügen und statische Routen benötigen, öffnen Sie eine Eingabeaufforderungssitzung, um diese zu konfigurieren.

Voraussetzungen

Fügen Sie den vRealize Orchestrator Appliances mehrere Netzwerkkarten hinzu.

Verfahren

- 1 Melden Sie sich als Root-Benutzer bei der Befehlszeile der vRealize Orchestrator Appliance an.
- 2 Öffnen Sie die Routendatei in einem Texteditor.

`/etc/sysconfig/network/routes`

- 3 Suchen Sie die Zeile `default` für das Standard-Gateway, ändern Sie diese aber nicht.

Hinweis Verwenden Sie in Fällen, in denen das Standard-Gateway geändert werden muss, stattdessen die vRealize Orchestrator-Verwaltungsschnittstelle.

- 4 Fügen Sie unterhalb der Zeile `default` neue Zeilen für statische Routen hinzu. Beispiel:

```
default 10.10.10.1 - -
172.30.30.0 192.168.100.1 255.255.255.0 eth0
192.168.210.0 192.168.230.1 255.255.255.0 eth2
```

- 5 Speichern und schließen Sie die Routendatei.
- 6 Starten Sie die Appliance neu.

- 7 Wiederholen Sie den Vorgang in HA-Clustern für jede Appliance.

Anwendungsfälle für Konfiguration und Fehlerbehebung

8

Sie können den Orchestrator-Server zum Einsatz mit der vCenter Server Appliance konfigurieren. Sie können außerdem Plug-Ins von Orchestrator deinstallieren oder die selbstsignierten Zertifikate ändern.

Die Anwendungsfälle für die Konfiguration bieten Taskflows, die Sie nutzen können, um bestimmte Konfigurationsanforderungen Ihres Orchestrator-Servers zu erfüllen. Sie helfen zudem bei der Fehlerbeseitigung, indem Sie das Verständnis von Problemen verbessern und Lösungen bieten, wo eine Problemumgehung möglich ist.

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren des vRealize Orchestrator-Plug-Ins für vSphere Web Client](#)
- [Aufheben der Registrierung der Orchestrator-Authentifizierung](#)
- [Ändern von SSL-Zertifikaten](#)
- [Abbrechen laufender Workflows](#)
- [Aktivieren von Orchestrator-Server-Debugging](#)
- [Sichern der Konfiguration und Elemente von Orchestrator](#)
- [Sichern und Wiederherstellen vRealize Orchestrator](#)
- [Notfallwiederherstellung von Orchestrator mithilfe von Site Recovery Manager](#)

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

Sie müssen vRealize Orchestrator mit vSphere-Authentifizierung auf demselben Platform Services Controller registrieren, mit dem sich Ihr verwalteter vCenter Server authentifiziert.

Verfahren

- 1 Melden Sie sich beim 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 (Optional) Geben Sie `https://your_orchestrator_hostname:8281` oder die Dienst-URL des Lastausgleichsdiensts ein, der die Anforderungen an die vRealize Orchestrator-Serverknoten weiterleitet.
- 6 Klicken Sie auf **Ausführen**.

Aufheben der Registrierung der Orchestrator-Authentifizierung

Sie können die Registrierung von Orchestrator als Single Sign-On-Lösung auf der Seite „Anbieter für Authentifizierung konfigurieren“ in Control Center aufheben.

Wenn Sie die Authentifizierung von Orchestrator vCenter Single Sign-On oder vRealize Automation neu konfigurieren möchten, müssen Sie zunächst die Registrierung der Orchestrator-Authentifizierung aufheben.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Klicken Sie auf **Anbieter für Authentifizierung konfigurieren**.
- 3 Klicken Sie auf **Registrierung aufheben**.
- 4 (Optional) Geben Sie Ihre Anmeldedaten ein, wenn Sie Registrierungsdaten vom Identity Server löschen möchten.
- 5 Klicken Sie im Bereich **Identitätsdienst** auf **Registrierung aufheben**.

Ergebnisse

Damit haben Sie die Registrierung Ihrer Orchestrator-Serverinstanz aufgehoben.

Ändern von SSL-Zertifikaten

In der Standardeinstellung verwendet der Orchestrator-Server ein selbstsigniertes SSL-Zertifikat, um über eine Remoteverbindung mit dem Orchestrator-Client zu kommunizieren. Sie können das SSL-Zertifikat ersetzen, wenn beispielsweise die Sicherheitsrichtlinien Ihres Unternehmens die Verwendung eigener SSL-Zertifikate vorschreiben.

Wenn Sie versuchen, Orchestrator über eine vertrauenswürdige SSL-Internetverbindung zu nutzen und Control Center in einem Webbrowser öffnen, erhalten Sie bei Verwendung von Mozilla Firefox eine Warnung, dass die Verbindung nicht vertrauenswürdig ist, und bei Verwendung von Internet Explorer, dass Probleme mit dem Sicherheitszertifikat der Website festgestellt wurden.

Nach Klicken auf **Laden dieser Website fortsetzen (nicht empfohlen)** wird auch nach Importieren des SSL-Zertifikats in den vertrauenswürdigen Speicher weiterhin die rote Benachrichtigung zum Zertifikatsfehler in der Adressleiste des Webbrowsers angezeigt. Sie können mit Orchestrator im Webbrowser arbeiten, es kann jedoch bei Drittanbietersystemen beim Zugriff auf die API über HTTPS zu Problemen kommen.

Sie erhalten möglicherweise auch eine Zertifikatwarnung, wenn Sie den Orchestrator-Client starten und versuchen, eine SSL-Verbindung mit dem Orchestrator-Server herzustellen.

Sie können das Problem lösen, indem Sie ein von einer kommerziellen Zertifizierungsstelle (Certification Authority, CA) signiertes Zertifikat installieren. Um keine Zertifikatwarnungen mehr vom Orchestrator-Client zu erhalten, fügen Sie Ihr Root-CA-Zertifikat dem Orchestrator-Keystore auf jenem Computer hinzu, auf dem der Orchestrator-Client installiert ist.

Hinzufügen eines Zertifikats zum Local Store

Nachdem Sie ein Zertifikat von einer Zertifizierungsstelle erhalten haben, müssen Sie das Zertifikat dem lokalen Speicher hinzufügen, um ohne Zertifikatswarnungen und Fehlermeldungen mit Control Center arbeiten zu können.

Dieser Workflow beschreibt das Hinzufügen von Zertifikaten zu Ihrem lokalen Speicher unter Verwendung von Internet Explorer.

- 1 Öffnen Sie Internet Explorer und navigieren Sie zu `https://Orchestrator_Server_IP_oder_DNS_Name:8283/`.
- 2 Klicken Sie nach Aufforderung auf **Laden dieser Website fortsetzen (nicht empfohlen)**.
Der Zertifikatsfehler wird rechts in der Adressleiste von Internet Explorer angezeigt.
- 3 Klicken Sie auf den Zertifikatsfehler und wählen Sie **Zertifikate anzeigen**.
- 4 Klicken Sie auf **Zertifikat installieren**.
- 5 Klicken Sie auf der Willkommensseite des **Zertifikatimport-Assistenten** auf **Weiter**.
- 6 Im Fenster **Zertifikatspeicher** wählen Sie **Alle Zertifikate in folgendem Speicher speichern**.

- 7 Durchsuchen Sie die Auswahl und wählen Sie **Vertrauenswürdige Stammzertifizierungsstellen**.
- 8 Beenden Sie den Assistenten und starten Sie Internet Explorer neu.
- 9 Navigieren Sie über Ihre SSL-Verbindung zum Orchestrator-Server.

Sie erhalten nun keine Warnungen mehr und es wird kein Zertifikatsfehler in der Adressleiste angezeigt.

Andere Anwendungen und Systeme wie VMware Service Manager müssen über eine SSL-Verbindung auf die Orchestrator-REST-APIs zugreifen.

Ändern des Zertifikats der Orchestrator Appliance-Management-Site

Die Orchestrator Appliance verwendet Light HTTPd zum Ausführen der eigenen Verwaltungswebsite. Sie können das SSL-Zertifikat der Verwaltungswebsite der Orchestrator Appliance ersetzen, wenn beispielsweise die Sicherheitsrichtlinien Ihres Unternehmens die Verwendung eigener SSL-Zertifikate vorschreiben.

Voraussetzungen

Standardmäßig sind das SSL-Zertifikat von Orchestrator Appliance und der Privatschlüssel in einer PEM-Datei im Verzeichnis `/opt/vmware/etc/lighttpd/server.pem` gespeichert. Speichern Sie beim Installieren eines neuen Zertifikats Ihr neues SSL-Zertifikat und den privaten Schlüssel aus dem Java-Keystore in einer PEM-Datei.

Verfahren

- 1 Melden Sie sich bei der Orchestrator Appliance-Linux-Konsole als Root-Benutzer an.
- 2 Suchen Sie die Datei `/opt/vmware/etc/lighttpd/lighttpd.conf` und öffnen Sie diese in einem Editor.
- 3 Navigieren Sie zu folgender Zeile:

```
#### SSL engine
ssl.engine = "enable"
ssl.pemfile = "/opt/vmware/etc/lighttpd/server.pem"
```

- 4 Ändern Sie die `ssl.pemfile`-Attribute, sodass diese auf die PEM-Datei verweisen, die Ihr neues SSL-Zertifikat und den privaten Schlüssel enthält.
- 5 Speichern Sie die Datei `lighttpd.conf`.
- 6 Führen Sie folgenden Befehl aus, um den Light HTTPd-Server neu zu starten.

```
service vami-lighttpd restart
```

Ergebnisse

Sie haben das Zertifikats der Orchestrator Appliance-Management-Site erfolgreich geändert.

Abbrechen laufender Workflows

In Control Center 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 abzubrechen.
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 abzubrechen.

Ergebnisse

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

Nächste Schritte

Vergewissern Sie sich auf der Seite **Workflows überprüfen** in Control Center, dass die Workflows abgebrochen werden.

Aktivieren von Orchestrator-Server-Debugging

Sie können den Orchestrator-Server im Debug-Modus starten, um Probleme beim Entwickeln von Plug-Ins zu lösen.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Klicken Sie auf **Orchestrator-Debugging**.
- 3 Klicken Sie auf **Debuggen aktivieren**.
- 4 (Optional) Geben Sie einen Port ein, der sich vom Standardport unterscheidet.

5 (Optional) Klicken Sie auf **Anhalten**.

Bei Auswahl dieser Option müssen Sie einen Debugger anhängen, bevor Sie den Orchestrator-Server starten.

6 Klicken Sie auf **Speichern**.

7 Öffnen Sie die Seite „Startoptionen“ im Control Center und klicken Sie auf **Neu starten**.

Ergebnisse

Der Orchestrator-Server wird beim Start angehalten, bis Sie einen Remote-Java-Debugger mit dem festgelegten Port verbinden.

Sichern der Konfiguration und Elemente von Orchestrator

Sichern Sie Ihre benutzerdefinierte Serverkonfiguration und Ihre benutzerdefinierten Workflow-Elemente von Orchestrator, um sicherzustellen, dass sie von anderen Orchestrator-Instanzen wiederverwendet werden können.

Wenn Sie Standard-Workflows, Aktionen, Richtlinien oder Konfigurationselemente bearbeiten und danach ein Paket mit den gleichen Elementen und einer höheren Orchestrator-Versionsnummer importieren, gehen Ihre Änderungen an den Elementen verloren. Sie können den Verlust von benutzerdefinierten Workflows und sonstigen Elementen verhindern, indem Sie diese vor dem Upgrade Ihrer Orchestrator-Instanz exportieren.

Jede Orchestrator-Serverinstanz verfügt über eindeutige Zertifikate, und jede vCenter Server-Plug-In-Instanz besitzt eine eindeutige ID. Die Zertifikate und die eindeutige ID definieren die Identität des Orchestrator-Servers und vCenter Server-Plug-Ins. Wenn Sie die Orchestrator-Elemente nicht sichern bzw. die Orchestrator-Konfiguration nicht zu Sicherungszwecken exportieren, müssen Sie diese Kennungen unbedingt ändern.

Voraussetzungen

Stellen Sie eine neue Orchestrator-Serverinstanz bereit und konfigurieren Sie diese. Weitere Informationen finden Sie unter [Konfigurieren eines eigenständigen Orchestrator-Servers](#).

Verfahren

1 Exportieren Sie die Orchestrator-Konfiguration.

- a Melden Sie sich beim Control Center als **root** an.
- b Klicken Sie auf **Konfiguration exportieren/importieren**.
- c Wählen Sie die Typen der zu exportierenden Dateien aus.
- d (Optional) Schützen Sie die Konfigurationsdatei durch Eingabe eines Kennworts.
Verwenden Sie das gleiche Kennwort beim Import der Konfiguration.
- e Klicken Sie auf **Exportieren**.

2 Melden Sie sich bei der Orchestrator-Clientanwendung an.

3 Erstellen Sie ein Paket mit allen Orchestrator-Elementen, die Sie erstellt oder bearbeitet haben.

- a Klicken Sie unter der Ansicht **Verwalten** auf die Registerkarte **Pakete**.
- b Klicken Sie in der Titelleiste der Paketliste auf die Menüschaltfläche und wählen Sie **Paket hinzufügen** aus.
- c Geben Sie einen Namen für das neue Paket ein und klicken Sie auf **OK**.
Die Syntax für Paketnamen ist *Domäne.Ihr_Unternehmen.Ordner.Paketname*
Beispiel: `com.vmware.meinOrdner.meinPaket`.
- d Klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie **Bearbeiten**.
- e Fügen Sie auf der Registerkarte **Allgemein** eine Beschreibung des Pakets hinzu.
- f Fügen Sie dem Paket auf der Registerkarte **Workflows** die Workflows hinzu.
- g (Optional) Fügen Sie dem Paket Richtlinienvorlagen, Aktionen, Konfigurationselemente, Ressourcenelemente, Zugriffsrechte und Plug-Ins hinzu.
- h Klicken Sie auf **Speichern und schließen**.

4 Exportieren Sie das Paket.

- a Klicken Sie mit der rechten Maustaste auf das zu exportierende Paket und wählen Sie **Paket exportieren** aus.
- b Navigieren Sie zu dem gewünschten Speicherort für das Paket und wählen Sie diesen aus.
- c (Optional) Signieren Sie das Paket mit dem entsprechenden Zertifikat.
- d (Optional) Legen Sie Einschränkungen für das exportierte Paket fest.
- e (Optional) Zur Anwendung von Einschränkungen für den Inhalt des exportierten Pakets entfernen Sie die Markierung der entsprechenden Optionen.

Option	Beschreibung
Versionsverlauf exportieren	Der Versionsverlauf eines Pakets wird nicht exportiert.
Werte der Konfigurationseinstellungen exportieren	Die Attributwerte der Konfigurationselemente im Paket werden nicht exportiert.
Globale Tags exportieren	Die globalen Tags im Paket werden nicht exportiert.

Hinweis Die Option **Werte der SecureString-Konfigurationseinstellungen exportieren** ist standardmäßig deaktiviert. Der Export dieser Konfigurationseinstellungen kann zu einem Sicherheitsproblem führen. Verwenden Sie diese Funktion mit Bedacht.

- f Klicken Sie auf **Speichern**.

- 5 Importieren Sie die zuvor exportierte Orchestrator-Konfiguration in die neue Orchestrator-Serverinstanz.
 - a Melden Sie sich beim Control Center der neuen Orchestrator-Instanz als **root** an.
 - b Klicken Sie auf **Konfiguration exportieren/importieren** und navigieren Sie zur Registerkarte **Konfiguration importieren**.
 - c Wählen Sie die aus der vorherigen Installation exportierte ZIP-Datei aus.
 - d Geben Sie das beim Exportieren der Konfiguration verwendete Kennwort ein.
Dieser Schritt ist nicht erforderlich, wenn Sie kein Kennwort angegeben haben.
 - e Wählen Sie den Importtyp aus.
 - f Klicken Sie auf **Importieren**.
- 6 Importieren Sie das von Ihnen zuvor exportierte Paket in die neue Orchestrator-Instanz.
 - a Melden Sie sich bei der Orchestrator-Clientanwendung der neuen Orchestrator-Instanz an.
 - b Wählen Sie im Dropdown-Menü im Orchestrator-Client **Verwalten** aus.
 - c Klicken Sie auf die Registerkarte **Pakete**.
 - d Klicken Sie in der Titelleiste der Paketliste auf die Menüschaltfläche und wählen Sie **Paket importieren** aus.
 - e Navigieren Sie zu dem Paket, das Sie importieren möchten, wählen Sie es aus und klicken Sie auf **Öffnen**.
Es werden Zertifikatinformationen zum Export angezeigt.
 - f Überprüfen Sie die Importinformationen des Pakets und wählen Sie **Importieren** oder **Importieren und Anbieter vertrauen**.
Die Ansicht „Paket importieren“ wird angezeigt. Falls die Version des importierten Paketelements eine höhere Version aufweist als diejenige auf dem Server, wird das Element automatisch vom System zum Importieren ausgewählt.
 - g Wählen Sie die zu importierenden Elemente aus.

Hinweis Heben Sie die Auswahl von benutzerdefinierten Elementen auf, für die höhere Versionen vorhanden sind.

 - h (Optional) Entfernen Sie die Markierung des Kontrollkästchens **Werte der Konfigurationseinstellungen importieren**, wenn die Attributwerte der Konfigurationselemente des Pakets nicht importiert werden sollen.

- i Wählen Sie im Dropdown-Menü aus, ob die Tags aus dem Paket importiert werden sollen.

Option	Beschreibung
Tags importieren aber vorhandene Werte behalten	Die Tags aus dem Paket werden importiert, ohne die vorhandenen Tagwerte zu überschreiben.
Tags importieren und vorhandene Werte überschreiben	Die Tags aus dem Paket werden importiert, und ihre Werte werden überschrieben.
Tags nicht importieren	Es werden keine Tags aus dem Paket importiert.

- j Klicken Sie auf **Ausgewählte Elemente importieren**.

Ergebnisse

Sie haben die Orchestrator-Konfiguration und -Elemente erfolgreich gesichert.

Sichern und Wiederherstellen vRealize Orchestrator

Sie können mit vSphere Data Protection virtuelle Maschinen (VMs), die eine vRealize Orchestrator-Instanz enthalten, sichern und wiederherstellen.

vSphere Data Protection ist eine VMware-Lösung für vSphere-Umgebungen zur Sicherung auf einem Datenträger und zur Wiederherstellung. vSphere Data Protection ist vollständig integriert in vCenter Server. Mit vSphere Data Protection können Sie Sicherungsaufträge verwalten und an deduplizierten Zielspeicherorten sichern. Nach der Bereitstellung und Konfiguration von vSphere Data Protection können Sie auf vSphere Data Protection zugreifen, indem Sie über die vSphere Web Client-Schnittstelle die Auswahl, Planung, Konfiguration sowie die Verwaltung von Sicherungen und die Wiederherstellung von virtuellen Maschinen ausführen. Bei der Sicherung erstellt vSphere Data Protection einen Snapshot der stillgelegten virtuellen Maschine. Die Deduplizierung wird bei jedem Sicherungsvorgang automatisch durchgeführt.

Informationen zu Bereitstellung und Konfiguration von vSphere Data Protection finden Sie in der Dokumentation *vSphere Data Protection-Verwaltung*.

Sichern von vRealize Orchestrator

Sie können Ihre Instanz von vRealize Orchestrator als virtuelle Maschine sichern.

Sie können Ihre Datenbank vor der vollständigen Sicherung der VM exportieren. Informationen zum Exportieren der Datenbank finden Sie unter [Exportieren der Orchestrator-Datenbank](#). Wenn vRealize Orchestrator und die externe Datenbank sich auf unterschiedlichen Maschinen befinden, müssen Sie die Datenbank separat sichern.

Hinweis Um sicherzustellen, dass alle Komponenten einer VM innerhalb desselben Produkts zusammen gesichert werden, speichern Sie die VMs Ihrer vRealize Orchestrator-Umgebung im selben vCenter Server-Ordner und erstellen Sie einen Auftrag für eine Sicherungsrichtlinie für diesen Ordner.

Voraussetzungen

- Überprüfen Sie, ob die vSphere Data Protection-Appliance bereitgestellt und konfiguriert wurde. Informationen zur Bereitstellung und Konfiguration von vSphere Data Protection finden Sie in der Dokumentation *vSphere Data Protection-Verwaltung*.
- Melden Sie sich über den vSphere Web Client bei der vCenter Server-Instanz an, die Ihre Umgebung verwaltet. Melden Sie sich als derselbe Benutzer mit Administratorrechten an, der bei der Konfiguration von vSphere Data Protection verwendet wurde.

Verfahren

- 1 Klicken Sie auf der vSphere Web Client-Startseite auf **vSphere Data Protection**.
- 2 Wählen Sie Ihre vSphere Data Protection-Appliance aus dem Dropdown-Menü **VDP-Appliance** und klicken Sie auf **Verbinden**.
- 3 Klicken Sie auf der Registerkarte **Erste Schritte** auf **Sicherungsauftrag erstellen**.
- 4 Klicken Sie auf **Gast-Images**, um Ihre vRealize Orchestrator-Instanz zu sichern, und klicken Sie auf **Weiter**.
- 5 Wählen Sie **Vollständiges Image**, um die gesamte virtuelle Maschine zu sichern, und klicken Sie auf **Weiter**.
- 6 Erweitern Sie die Baumstruktur **Virtuelle Maschinen** und aktivieren Sie das Kontrollkästchen für Ihre vRealize Orchestrator VM.
- 7 Folgen Sie den Anweisungen zum Festlegen des Sicherungszeitplans, der Aufbewahrungsrichtlinie und des Namens für den Sicherungsauftrag.

Weitere Informationen zum Sichern und Wiederherstellen virtueller Maschinen finden Sie in der Dokumentation zur *vSphere Data Protection-Verwaltung*.

Ihr Sicherungsauftrag wird in der Liste der Sicherungsaufträge auf der Registerkarte **Sicherung** angezeigt.

- 8 (Optional) Öffnen Sie die Registerkarte **Sicherung**, wählen Sie Ihren Sicherungsauftrag aus und klicken Sie auf **Jetzt sichern**, um vRealize Orchestrator zu sichern.

Hinweis Stattdessen können Sie auch warten, bis die Sicherung automatisch gemäß dem von Ihnen festgelegten Zeitplan gestartet wird.

Der Sicherungsprozess wird auf der Seite **Kürzlich bearbeitete Aufgaben** angezeigt.

Ergebnisse

Das Image Ihrer virtuellen Maschine wird in der Liste der Sicherungen auf der Registerkarte **Wiederherstellen** angezeigt.

Nächste Schritte

Öffnen Sie die Registerkarte **Wiederherstellen** und vergewissern Sie sich, dass das Image Ihrer VM in der Sicherungsliste angezeigt wird.

Wiederherstellen einer vRealize Orchestrator-Instanz

Sie können eine vRealize Orchestrator-Instanz an ihrem Originalspeicherort oder unter einem anderen Speicherort auf demselben vCenter Server wiederherstellen.

Wenn vRealize Orchestrator und die externe Datenbank auf verschiedenen Maschinen laufen, müssen Sie zuerst die Datenbank und dann die vRealize Orchestrator-VM wiederherstellen.

Voraussetzungen

- Überprüfen Sie, ob die vSphere Data Protection-Appliance bereitgestellt und konfiguriert wurde. Informationen zur Bereitstellung und Konfiguration von vSphere Data Protection finden Sie in der Dokumentation *vSphere Data Protection-Verwaltung*.
- Sichern Sie Ihre vRealize Orchestrator-Instanz. Weitere Informationen finden Sie unter [Sichern von vRealize Orchestrator](#).
- Melden Sie sich über den vSphere Web Client bei der vCenter Server-Instanz an, die Ihre Umgebung verwaltet. Melden Sie sich als derselbe Benutzer mit Administratorrechten an, der bei der Konfiguration von vSphere Data Protection verwendet wurde.

Verfahren

- 1 Klicken Sie auf der vSphere Web Client-Startseite auf **vSphere Data Protection**.
- 2 Wählen Sie Ihre vSphere Data Protection-Appliance im Dropdown-Menü **VDP-Appliance** und klicken Sie auf **Verbinden**.
- 3 Öffnen Sie die Registerkarte **Wiederherstellen**.
- 4 Wählen Sie aus der Liste der Sicherungsaufträge die vRealize Orchestrator-Sicherung, die Sie wiederherstellen möchten.

Hinweis Falls mehrere VMs vorhanden sind, müssen Sie diese gleichzeitig wiederherstellen, damit sie synchron bleiben.

- 5 Um die vRealize Orchestrator-Instanz auf demselben vCenter Server wiederherzustellen, klicken Sie auf das Symbol **Wiederherstellen** und folgen Sie den Anweisungen, um den Speicherort auf dem vCenter Server festzulegen, unter dem Sie vRealize Orchestrator wiederherstellen möchten.

Sie dürfen nicht **Einschalten** wählen, da die Appliance die Komponente ist, die zuletzt eingeschaltet werden muss. Informationen zum Sichern und Wiederherstellen einer virtuellen Maschine finden Sie in der Dokumentation zur *vSphere Data Protection-Verwaltung*.

Eine Meldung wird angezeigt, die bestätigt, dass die Wiederherstellung gestartet wurde.

- 6 (Optional) Schalten Sie die Datenbankhosts ein, sofern dies externe Hosts sind, und stellen Sie die Konfiguration des Lastausgleichsdienstes wieder her.
- 7 Schalten Sie die vRealize Orchestrator-Appliance ein.

Ergebnisse

Die wiederhergestellte vRealize Orchestrator-VM wird in der vCenter Server-Bestandsliste angezeigt.

Nächste Schritte

Überprüfen Sie, ob vRealize Orchestrator ordnungsgemäß konfiguriert ist, indem Sie die Seite **Konfiguration überprüfen** in Control Center öffnen.

Notfallwiederherstellung von 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 5.5 auf den geschützten und den für die Wiederherstellung vorgesehenen Sites installiert ist.
- Stellen Sie sicher, dass Sie Site Recovery Manager 5.8. 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 Objektiv (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 die virtuellen Maschinen schützen kann.

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
- vSphere Replication wurde auf den virtuellen Maschinen konfiguriert
- Eine Kombination einiger oder aller genannten Punkte

Verfahren

- 1 Wählen Sie im vSphere Web Client **Site-Wiederherstellung** > **Schutzgruppen** aus.
- 2 Klicken Sie auf die Registerkarte **Objekte** und anschließend auf das Symbol zum Erstellen von Schutzgruppen.
- 3 Wählen Sie auf der Seite für den Schutzgruppentyp die Schutz-Site und den Replizierungstyp aus und klicken Sie auf **Weiter**.

Option	Aktion
Array-basierte Replizierungsgruppen	Wählen Sie Array-basierte Replizierung (ABR) und dann ein Array-Paar aus.
vSphere Replication-Schutzgruppe	Wählen Sie vSphere Replication aus.

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

Option	Aktion
Schutzgruppen für Array-basierte Replizierung	Wählen Sie einen Datenspeicher aus und klicken Sie auf Weiter .
vSphere Replication-Schutzgruppen	Wählen Sie in der Liste virtuelle Maschinen aus und klicken Sie auf Weiter .

Wenn Sie vSphere Replication-Schutzgruppen erstellen, werden nur für vSphere Replication konfigurierte virtuelle Maschinen angezeigt, die nicht bereits in Schutzgruppen sind.

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

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

Ergebnisse

- Wenn Site Recovery Manager erfolgreich Bestandslistenzuordnungen auf die geschützten virtuellen Maschinen angewendet hat, lautet der Status der Schutzgruppe „OK“.
- Wenn Site Recovery Manager erfolgreich alle von der Speicherrichtlinie erfassten virtuellen Maschinen geschützt hat, lautet der Status der Schutzgruppe „OK“.

Erstellen eines Wiederherstellungsplans

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

Verfahren

- 1 Wählen Sie im vSphere Web Client **Site-Wiederherstellung** > **Wiederherstellungspläne** aus.
- 2 Klicken Sie auf die Registerkarte **Objekte** auf das Symbol zum Erstellen eines Wiederherstellungsplans.
- 3 Geben Sie einen Namen und eine Beschreibung für diesen Plan ein, wählen Sie einen Ordner aus und klicken Sie dann auf **Weiter**.
- 4 Wählen Sie die Wiederherstellungs-Site aus und klicken Sie auf **Weiter**.
- 5 Wählen Sie aus dem Menü den Gruppentyp aus.

Option	Beschreibung
VM-Schutzgruppen	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.

Die Standardeinstellung ist **VM-Schutzgruppen**.

Hinweis Bei Nutzung von Stretched Storage wählen Sie **Speicherrichtlinien-Schutzgruppen** als Gruppentyp aus.

- 6 Wählen Sie eine oder mehrere Schutzgruppen für den Plan aus, der wiederhergestellt werden soll, und klicken Sie auf **Weiter**.
- 7 Klicken Sie auf den Wert **Testnetzwerk**, wählen Sie ein für den Wiederherstellungstest zu verwendendes Netzwerk aus und klicken Sie auf **Weiter**.

Die Standardoption ist das automatische Erstellen eines isolierten Netzwerks.

- 8 Überprüfen Sie die zusammengefassten Informationen und klicken Sie auf **Beenden**, um den Wiederherstellungsplan zu erstellen.

Organisieren von Wiederherstellungsplänen in Ordnern

Sie können Ordner erstellen, um Wiederherstellungspläne zu organisieren.

Das Organisieren von Wiederherstellungsplänen in Ordnern ist sinnvoll, wenn zahlreiche Wiederherstellungspläne vorhanden sind. Sie können den Zugriff auf Wiederherstellungspläne einschränken, indem Sie sie in Ordnern ablegen und diesen unterschiedliche Berechtigungen für verschiedene Benutzer oder Gruppen zuweisen.

Verfahren

- 1 Klicken Sie auf der Startseite des vSphere Web Client auf **Site Recovery**.
- 2 Erweitern Sie **Bestandslistenstruktur** und klicken Sie auf **Wiederherstellungspläne**.
- 3 Wählen Sie die Registerkarte **Verwandte Objekte** und klicken Sie auf **Ordner**.
- 4 Klicken Sie auf das Symbol **Ordner erstellen**, geben Sie den Namen des zu erstellenden Ordners ein und klicken Sie auf **OK**.
- 5 Fügen Sie dem Ordner neue oder bestehenden Wiederherstellungspläne hinzu.

Option	Beschreibung
Erstellen eines neuen Wiederherstellungsplans	Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie Wiederherstellungsplan erstellen .
Hinzufügen eines bestehenden Wiederherstellungsplans	Ziehen Sie Wiederherstellungspläne aus der Bestandslistenstruktur in den Ordner und legen Sie sie dort ab.

- 6 (Optional) Um einen Ordner umzubenennen oder zu löschen, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Ordner umbenennen** bzw. **Ordner löschen**.

Sie können einen Ordner nur löschen, wenn er leer ist.

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 Wählen Sie im vSphere Web Client **Site-Wiederherstellung** > **Wiederherstellungspläne** aus.
- 2 Klicken Sie mit der rechten Maustaste auf einen Wiederherstellungsplan und wählen Sie **Plan bearbeiten** aus.

Sie können einen Plan auch bearbeiten, indem Sie auf das Symbol **Wiederherstellungsplan bearbeiten** in der Ansicht **Wiederherstellungsschritte** auf der Registerkarte **Überwachen** klicken.

- 3 (Optional) Ändern Sie den Namen und die Beschreibung des Plans im Textfeld **Wiederherstellungsplanname** und klicken Sie auf **Weiter**.
- 4 Klicken Sie auf der Seite „Wiederherstellungs-Site“ auf **Weiter**.
Sie können die Wiederherstellungs-Site 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) Klicken Sie auf das Testnetzwerk, um ein anderes Testnetzwerk auf der Wiederherstellungs-Site auszuwählen, 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:

- Deaktivieren des Zugriffs auf den Orchestrator-Client für Nichtadministratoren
- 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

Deaktivieren des Zugriffs auf den Orchestrator-Client für Nichtadministratoren

Sie können den Orchestrator-Server so konfigurieren, dass nur Mitgliedern der Orchestrator-Administratorgruppe Zugriff auf den Orchestrator-Client gewährt wird.

In der Standardeinstellung können alle Benutzer mit Ausführungsberechtigung eine Verbindung zum Orchestrator-Client aufbauen. Sie können den Zugriff auf den Orchestrator-Client jedoch auf Orchestrator-Administratoren beschränken, indem Sie eine Systemeigenschaft für die Orchestrator-Konfiguration einrichten.

Wichtig Wenn keine Eigenschaft eingerichtet wurde oder diese auf „false“ gesetzt wurde, können alle Benutzer auf den Orchestrator-Client zugreifen.

Verfahren

- 1 Melden Sie sich beim Control Center als **root** an.
- 2 Klicken Sie auf **Systemeigenschaften**.
- 3 Klicken Sie auf das Symbol **Hinzufügen** (+).
- 4 Geben Sie im Textfeld **Schlüssel** Folgendes ein: **com.vmware.o11n.smart-client-disabled**.
- 5 Geben Sie im Textfeld **Wert** Folgendes ein: **true**.

- 6 (Optional) Geben Sie in das Textfeld **Beschreibung** Folgendes ein:
Verbindung zum Orchestrator-Client deaktivieren.
- 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

Sie haben den Zugriff auf den Orchestrator-Client für alle Benutzer mit Ausnahme der Mitglieder der Orchestrator-Administratorgruppe deaktiviert.

Festlegen des Dateisystemzugriffs auf dem Server für Workflows und Aktionen

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

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

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

Wichtig Bevor Sie die Datei `js-io-rights.conf` verwenden, müssen Sie den Control Center-Dienst von vRealize Orchestrator beenden. Andernfalls wird die Datei `js-io-rights.conf` auf ihre Standardkonfiguration zurückgesetzt. Weitere Informationen finden Sie unter [Festlegen des Dateisystemzugriffs auf dem Server für Workflows und Aktionen](#).

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

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
```



```
-rwx /etc/vco/app-server/security/
+rx /etc/vco
+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`

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 Linux-Konsole der vRealize Orchestrator Appliance als **root** an.
- 2 Starten Sie den vRealize Orchestrator-Systemsteuerungsdienst.

```
service vco-configurator stop
```

- 3 Navigieren Sie zu `/etc/vco/app-server`.
- 4 Öffnen Sie die Konfigurationsdatei `js-io-rights.conf` in einem Texteditor.
- 5 Fügen Sie der Datei `js-io-rights.conf` die erforderlichen Zeilen hinzu.

So werden beispielsweise mit der folgenden Zeile die Ausführungsrechte im Verzeichnis `/Pfad_zu_Ordner/noexec` verweigert:

```
-x /Pfad_zu_Ordner/noexec
```

Die Ausführungsrechte für `/Pfad_zu_Ordner/noexec` bleiben erhalten, diejenigen für `/Pfad_zu_Ordner/noexec/bar` hingegen nicht. Die Lese- und Schreibrechte für beide Verzeichnisse bleiben erhalten.

- 6 Führen Sie zum Anwenden der Änderungen den folgenden Befehl aus.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh sync-local
```

- 7 Starten Sie den vRealize Orchestrator-Control Center-Dienst.

```
service vco-configurator start
```

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 Orchestrator-API stellt eine Skripterstellungsklasse, `Command`, bereit, die Befehle im Orchestrator-Server-Hostbetriebssystem durchführt. Um nicht autorisierten Zugriff auf den Orchestrator-Serverhost zu verhindern, haben Orchestrator-Anwendungen standardmäßig keine Berechtigungen zum Ausführen der Klasse `Command`. Wenn 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 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 das Symbol **Hinzufügen** (+).
- 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 Starten Sie den Orchestrator-Server neu.

Ergebnisse

Damit haben Sie Orchestrator-Anwendungen die Berechtigung zum Ausführen lokaler Befehle im Betriebssystem des 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 schränkt Orchestrator den JavaScript-Zugriff auf einen begrenzten Satz von Java-Klassen. Wenn Sie JavaScript-Zugriff auf mehr Java-Klassen benötigen, müssen Sie eine Orchestrator-Systemeigenschaft festlegen, um diesen Zugriff zuzulassen.

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 Orchestrator-Server betreibt. Daher kann die Orchestrator JavaScript-Engine 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 Speichern Sie die Konfigurationsdatei mit einem geeigneten Namen und an einem geeigneten Speicherort.
- 3 Melden Sie sich beim Control Center als **root** an.
- 4 Klicken Sie auf **Eigenschaften des Systems**.
- 5 Klicken Sie auf das Symbol **Hinzufügen** (+).

- 6 Geben Sie im Textfeld **Schlüssel** die Zeichenfolge `com.vmware.scripting.rhino-class-shutter-file` ein.
- 7 Geben Sie im Textfeld **Wert** den Pfad zu Ihrer Konfigurationsdatei ein.
- 8 Geben Sie im Textfeld **Beschreibung** eine Beschreibung für die Systemeigenschaft ein.
- 9 Klicken Sie auf **Hinzufügen**.
- 10 Klicken Sie im Popup-Menü auf **Änderungen speichern**.
Eine Meldung zeigt an, dass die Angaben gespeichert wurden.
- 11 Starten Sie den Orchestrator-Server neu.

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, nimmt die Rückgabe der Antwort an den Orchestrator-Server mehr Zeit in Anspruch als die standardmäßig festgelegten 20000 Millisekunden. Um dies zu vermeiden, müssen Sie die Konfigurationsdatei für Orchestrator bearbeiten und das standardmäßige Zeitüberschreitungslimit vergrößern.

Wenn das Standard-Zeitlimit überschritten wird, bevor bestimmte Vorgänge abgeschlossen sind, werden im Protokoll für den Orchestrator-Server Fehler aufgezeichnet.

```
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 **Systemeigenschaften**.
- 3 Klicken Sie auf das Symbol **Hinzufügen** ()
- 4 Geben Sie im Textfeld **Schlüssel** Folgendes ein:
`com.vmware.vmo.plugin.vi4.waitUpdatesTimeout`.
- 5 Geben Sie im Textfeld **Wert** das neue Zeitlimit 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.

Wenn Sie vRealize Orchestrator installiert und konfiguriert haben, können Sie mithilfe von Orchestrator häufig verwendete Prozesse zur Verwaltung der virtuellen Umgebung automatisieren.

- Melden Sie sich beim Orchestrator-Client an, führen Sie Workflows für die vCenter Server-Bestandslistenobjekte oder andere Objekte aus, auf die Orchestrator über seine Plug-Ins zugreift, und planen Sie solche Workflows. Weitere Informationen finden Sie unter *Verwenden des VMware vRealize Orchestrator-Clients*.
- Duplizieren und ändern Sie die Standardworkflows von Orchestrator und erstellen Sie eigene Aktionen und Workflows, um Vorgänge in vCenter Server zu automatisieren.
- Entwickeln Sie Plug-Ins und Webdienste, um die Orchestrator-Plattform zu erweitern.
- Führen Sie mithilfe des vSphere Web Client Workflows für Ihre vSphere-Bestandslistenobjekte aus.

Dieses Kapitel enthält die folgenden Themen:

- [Anmelden beim Orchestrator-Client über die Webkonsole der Orchestrator Appliance](#)

Anmelden beim Orchestrator-Client über die Webkonsole der Orchestrator Appliance

Zum Ausführen allgemeiner Verwaltungsaufgaben oder zum Bearbeiten und Erstellen von Workflows müssen Sie sich bei der Schnittstelle des Orchestrator-Clients anmelden.

Die Orchestrator-Client-Schnittstelle ist für Entwickler mit Administratorrechten vorgesehen, die Workflows, Aktionen und andere benutzerdefinierte Elemente entwickeln möchten.

Wichtig Achten Sie darauf, dass die Uhren der Orchestrator Appliance und der Orchestrator-Client-Maschine synchronisiert sind.

Voraussetzungen

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

- Installieren Sie 64-Bit-Java auf der Workstation, auf der Sie den Orchestrator-Client ausführen werden.

Hinweis 32-Bit-Java wird nicht unterstützt.

Verfahren

- 1 Navigieren Sie in einem Webbrowser zu der IP-Adresse Ihrer virtuellen Orchestrator Appliance-Maschine.

`http://orchestrator_appliance_ip`

- 2 Klicken Sie auf **Orchestrator-Client starten**.

- 3 Geben Sie die IP oder den Domännennamen der Orchestrator Appliance in das Textfeld **Hostname** ein.

Die IP-Adresse der Orchestrator Appliance wird standardmäßig angezeigt.

- 4 Melden Sie sich mit dem Benutzernamen und dem Kennwort für den Orchestrator-Client an.

Je nachdem, ob Sie vRealize Automation oder vSphere als Authentifizierungsanbieter verwenden, geben Sie die entsprechenden Anmeldedaten ein, um sich im Orchestrator-Client anzumelden.

Wenn auf Ihrem Orchestrator 7.4 die Mandantenfähigkeit aktiviert ist, geben Sie den Benutzernamen, das Kennwort und die Mandanten-ID des jeweiligen Systemadministrators oder Mandantenadministrators ein.

- 5 Wählen Sie im Fenster **Sicherheitswarnung** eine Option zum Behandeln der Zertifikatwarnung aus.

Der Orchestrator-Client kommuniziert mit dem Orchestrator-Server unter Verwendung eines SSL-Zertifikats. Eine vertrauenswürdige Zertifizierungsstelle signiert das Zertifikat nicht bei der Installation. Sie erhalten eine Zertifikatwarnung jedes Mal, wenn Sie eine Verbindung zum Orchestrator-Server herstellen.

Option	Beschreibung
Ignorieren	Setzen Sie den Vorgang unter Verwendung des aktuellen SSL-Zertifikats fort. Die Warnmeldung wird erneut angezeigt, wenn Sie die Verbindung zum selben Orchestrator-Server erneut herstellen, oder wenn Sie versuchen, einen Workflow mit einem Orchestrator-Remoteserver zu synchronisieren.
Abbrechen	Schließen Sie das Fenster und beenden Sie den Anmeldevorgang.
Dieses Zertifikat installieren und keine Sicherheitswarnungen für dieses mehr anzeigen.	Wählen Sie dieses Kontrollkästchen und klicken Sie auf Ignorieren , um das Zertifikat zu installieren und um den Empfang von Sicherheitswarnungen zu beenden.

Sie können das SSL-Standardzertifikat durch ein von einer Zertifizierungsstelle signiertes Zertifikat ersetzen. Weitere Informationen zum Ersetzen von SSL-Zertifikaten finden Sie unter *Installieren und Konfigurieren von VMware vRealize Orchestrator*.

Nächste Schritte

Sie können ein Paket importieren, Workflows starten oder Rechte für den Root-Zugriff auf dem System festlegen.