Installieren und Konfigurieren von VMware vRealize Orchestrator

vRealize Orchestrator 7.2

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-002396-01

vmware®

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

http://www.vmware.com/de/support/

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

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 Datencentern vertraut sind.

Aktualisierte Informationen

Die Dokumentation *Installieren und Konfigurieren von VMware vRealize Orchestrator* wird mit jeder neuen Version des Produkts oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf für die Dokumentation *Installieren und Konfigurieren von VMware vRealize Orchestrator*.

Revision	Beschreibung
DE-002396-01	■ „Migrieren einer externen vRealize Orchestrator 6.x-Instanz unter Windows auf vRealize Automation 7.2“, auf Seite 74 wurde aktualisiert. ■ „Migrieren einer externen virtuellen vRealize Orchestrator 6.x-Appliance unter Windows auf vRealize Automation 7.2“, auf Seite 76 wurde aktualisiert. ■ „Migrieren einer externen Instanz von vRealize Orchestrator 7.x zu vRealize Automation 7.2“, auf Seite 78 wurde aktualisiert. ■ Kapitel 9, „Konfigurieren des integrierten vRealize Orchestrator-Servers“, auf Seite 81 wurde aktualisiert. ■ Das Handbuch vRealize Orchestrator-Lastausgleich wurde aktualisiert.
DE-002396-00	Erstversion.

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 behandelt die folgenden Themen:

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.

Die folgende Liste präsentiert die wichtigsten Orchestrator-Funktionen.

Persistenz Datenbanken für Produktionsumgebungen werden verwendet, um wichtige Informationen zu speichern, beispielsweise Prozesse, Workflowstatus und Konfigurationsdaten.

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

Die Control Center-Schnittstelle erhöht die administrative Effizienz von vRealize Orchestrator-Instanzen, indem eine zentrale administrative Schnittstelle für Laufzeitvorgänge, Überwachung von Workflows, einheitlichen Protokollzugriff und Konfigurationen sowie Korrelation zwischen der Workflowausführung und Systemressourcen bereitgestellt werden. Der vRealize Orchestrator-Protokollierungsmechanismus ist durch eine zusätzliche Protokolldatei optimiert, die verschiedene Leistungskennzahlen für den Durchsatz der vRealize 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.

Skripterstellungsengine

Die Mozilla Rhino JavaScript-Engine bietet eine Möglichkeit, Bausteine für die Orchestrator-Plattform zu erstellen. Die Skripterstellungsengine 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 einem der Plug-Ins sammeln, sodass Sie veränderte Bedingungen in jeder der integrierten Technologien verarbeiten können.

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 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.

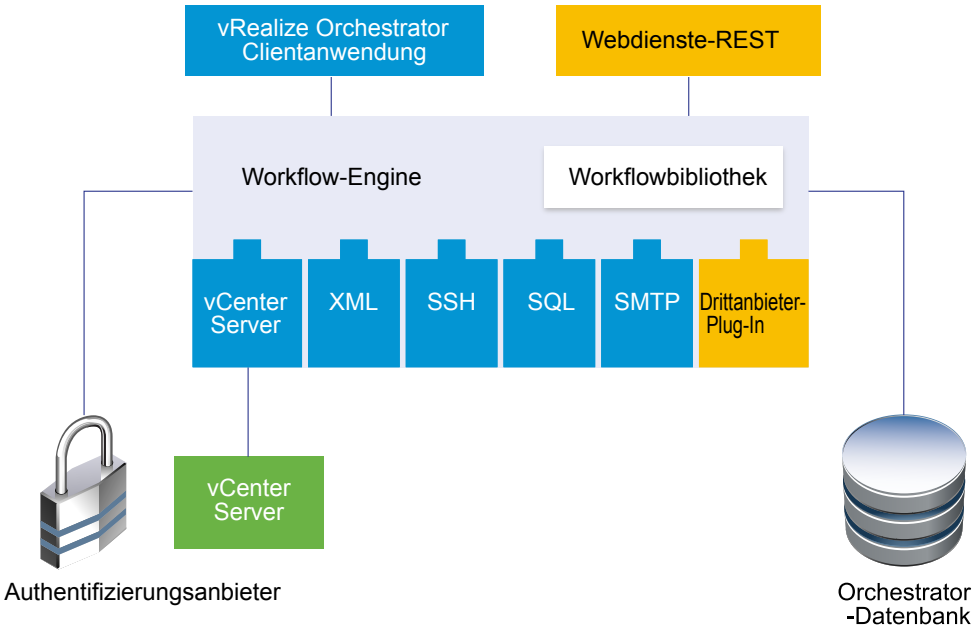
Orchestrator-Architektur

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, damit Sie Aufgaben in den verschiedenen Umgebungen registrieren können, für die das Plug-In verfügbar ist.

Orchestrator bietet auch eine offene Architektur, damit Sie externe Drittanbieteranwendungen in die Orchestrierungsplattform integrieren können. Sie können Workflows mit den Objekten der Plug-In-Technologien ausführen, die Sie selbst definieren. Orchestrator verbindet sich mit einem Authentifizierungsbereitsteller, um Benutzerkonten zu verwalten, und mit einer Datenbank, um Informationen aus den Workflows zu speichern, die unter Orchestrator ausgeführt werden. Sie können auf Orchestrator, die Orchestrator-Workflows und die Objekte, die er über die Orchestrator-Clientschnittstelle bzw. über Webdienste bereitstellt, zugreifen.

Abbildung 1-1. Architektur von VMware vRealize Orchestrator



Orchestrator-Plug-Ins

Plug-Ins ermöglichen die Verwendung von Orchestrator für den Zugriff auf externe Technologien und Anwendungen sowie deren Steuerung. 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 der externen Technologie zugreifen.

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

In Orchestrator steht eine Reihe von Standard-Plug-Ins zur Verfügung, mit deren Hilfe 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 den Funktionsumfang bestehender vRealize Automation-Infrastruktur und Application Services anpassen. Darüber hinaus können Sie mit der offenen Plug-In-Architektur von Orchestrator Plug-Ins für den Zugriff auf andere Anwendungen entwickeln.

Die von VMware entwickelten Orchestrator-Plug-Ins werden als `.vmoapp`-Dateien bereitgestellt. Weitere Informationen zu den von VMware entwickelten und bereitgestellten Orchestrator-Plug-Ins finden Sie unter http://www.vmware.com/support/pubs/vco_plugins_pubs.html. Weitere Informationen zu Orchestrator-Plug-Ins anderer Anbieter finden Sie unter https://solutionexchange.vmware.com/store/vco.

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 behandelt die folgenden Themen:

Hardwareanforderungen der Orchestrator Appliance

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

Die Orchestrator Appliance weist die folgende Hardwarekonfiguration auf:

- 2 CPUs
- 6 GB Arbeitsspeicher
- 17 GB Festplatte

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

Unterstützte Verzeichnisdienste

Wenn Sie planen, einen LDAP-Server zur Authentifizierung zu verwenden, vergewissern Sie sich, dass Sie einen funktionierenden LDAP-Server eingerichtet und konfiguriert haben.

Hinweis Die LDAP-Authentifizierung ist eine veraltete Funktion und wird in zukünftigen Versionen nicht mehr unterstützt.

Orchestrator unterstützt folgende Verzeichnisdiensttypen.

- Windows Server Active Directory
- OpenLDAP

Wichtig Mehrere Domänen in verschiedenen Strukturen mit gegenseitigen Vertrauensbeziehungen werden nicht unterstützt und funktionieren mit Orchestrator nicht. Die Domänenstruktur ist die einzige für Active Directory mit mehreren Domänen unterstützte Konfiguration. Gesamtstruktur-Vertrauensstellung und externe Vertrauensstellungen werden nicht unterstützt.

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, für die Ausführung von Orchestrator optimierte virtuelle Maschine. Die Appliance wird mit vorinstallierter Software geliefert.

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.

Die Standard-LDAP-Konfiguration ist nur für Experiment- und Testzwecke geeignet. Um die Orchestrator Appliance in einer Produktionsumgebung zu verwenden, müssen Sie einen neuen Verzeichnisdienst einrichten und den Orchestrator-Server für den Einsatz mit diesem konfigurieren. Sie können darüber hinaus den Orchestrator-Server für die Authentifizierung über vRealize Automation, vSphere oder vCenter Single Sign-On konfigurieren. Weitere Informationen zum Konfigurieren von externem LDAP oder Single Sign-On finden Sie unter „Wählen des Authentifizierungstyps“, auf Seite 36.

Informationen zum Konfigurieren einer Datenbank für Produktionsumgebungen finden Sie unter „Einrichten der Orchestrator-Datenbank“, auf Seite 22.

Hinweis Die LDAP-Authentifizierung ist eine veraltete Funktion und wird in zukünftigen Versionen nicht mehr unterstützt.

Kennwortanforderungen

Beim Konfigurieren des Root-Kennworts für die Orchestrator Appliance müssen Sie die vordefinierten Kennwortanforderungen einhalten.

Das Root-Kennwort, das Sie bei der Bereitstellung der Orchestrator Appliance mithilfe einer OVF-Vorlage definieren, muss mindestens acht Zeichen umfassen.

Wenn Sie ein lokales Benutzerkennwort über Control Center ändern, wird das neue Kennwort nur akzeptiert, wenn es alle Anforderungen erfüllt.

- Das Kennwort muss mindestens acht Zeichen umfassen.
- Es muss mindestens eine Ziffer enthalten.
- Es muss mindestens einen Großbuchstaben enthalten.
- Es muss mindestens einen Kleinbuchstaben enthalten.
- Es muss mindestens ein Sonderzeichen enthalten.

Hinweis Nicht-ASCII-Zeichen oder erweiterte ASCII-Zeichen werden nicht unterstützt. Solche Zeichen werden zwar eventuell beim Definieren des Kennworts akzeptiert, sie verursachen jedoch Fehler bei Speichervorgängen und beim Verbinden eines Orchestrator-Knotens mit einem Cluster.

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.

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.

Dieses Kapitel behandelt die folgenden Themen:

vCenter Server-Setup

Wenn Sie die Anzahl der vCenter Server-Instanzen in Ihrem Orchestrator-Setup erhöhen, muss Orchestrator mehr Sitzungen verwalten. Jede aktive Sitzung bewirkt Aktivität auf dem entsprechenden vCenter Server, und zu viele aktive Sitzungen können bei mehr als 10 vCenter Server-Verbindungen zu Zeitüberschreitungen in Orchestrator führen.

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 Ihrem Orchestrator-Setup ausführen, wenn Ihr Netzwerk über ausreichend Bandbreite und Latenz verfügt. Wenn Sie ein LAN verwenden, um die Kommunikation zwischen Orchestrator und vCenter Server zu verbessern, ist eine 100-Mb-Leitung zwingend erforderlich.

Authentifizierungsmethoden

Zum Authentifizieren und Verwalten von Benutzerberechtigungen benötigt Orchestrator eine Verbindung zu einem LDAP-Server, zu einem Single Sign-On-Server oder zu vRealize Automation.

Hinweis Die LDAP-Authentifizierung ist eine veraltete Funktion und wird in zukünftigen Versionen nicht mehr unterstützt.

Wenn Sie die Orchestrator Appliance herunterladen und bereitstellen, wird der Orchestrator-Server zum Einsatz mit dem in der Appliance vorinstallierten ApacheDS LDAP-Server vorkonfiguriert. Die standardmäßige In-Process-LDAP-Konfiguration ist nur für Testzwecke geeignet. Um Orchestrator in einer Produktionsumgebung zu verwenden, müssen Sie einen LDAP, einen vCenter Single Sign-On-Server oder eine Verbindung zu vRealize Automation einrichten und Orchestrator für die Nutzung dieser Optionen konfigurieren.

Stellen Sie einen Verbindung zu einem LDAP-Server her, der sich physisch möglichst in der Nähe des Orchestrator-Servers befindet. Dadurch vermeiden Sie lange Reaktionszeiten für LDAP-Anfragen, die sich negativ auf die Systemleistung auswirken. Orchestrator unterstützt Active Directory- und OpenLDAP-Dienste.

Zur Verbesserung der Leistung bei LDAP-Anfragen halten Sie die Suchbasis für Benutzer und Gruppen möglichst eng gefasst. Beschränken Sie die Benutzer auf Zielgruppen, die tatsächlich den Zugriff benötigen, statt das ganze Unternehmen und damit viele Benutzer einzuschließen, die den Zugriff nicht benötigen. Die benötigten Ressourcen sind abhängig von den gewählten Optionen für Datenbank und Verzeichnisdienst. Empfehlungen finden Sie in der Dokumentation für Ihren LDAP-Server.

Um als Authentifizierungsmethode vCenter Single Sign-On verwenden zu können, müssen Sie zunächst vCenter Single Sign-On installieren. Sie müssen den Orchestrator-Server entsprechend konfigurieren, um den installierten und konfigurierten vCenter Single Sign-On-Server nutzen zu können.

Sie können die Single Sign-On-Authentifizierung über vRealize Automation und vSphere mithilfe der Authentifizierungseinstellungen in Control Center nutzen.

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. Um jedoch Orchestrator in einer Produktionsumgebung mit hohem Arbeitsaufkommen verwenden zu können, müssen Sie eine eigene Datenbank einrichten und Orchestrator aus dem Control Center für die Arbeit mit dieser Datenbank konfigurieren.

Orchestrator-Server unterstützt Oracle-, Microsoft SQL Server- und PostgreSQL-Datenbanken.

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“, auf Seite 43.

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 derjenigen, 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 Workflow-Ausführung 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.

Installation und Upgrade von Orchestrator 4

Orchestrator besteht aus einer Server- und einer Clientkomponente.

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

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

Im Orchestrator Control Center können Sie die standardmäßigen Konfigurationseinstellungen für Orchestrator ändern.

Dieses Kapitel behandelt die folgenden Themen:

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 der Orchestrator Appliance“, auf Seite 17.
- Wenn Ihr System isoliert ist und kein Internetzugriff besteht, müssen Sie die `.ova`-Datei für die Appliance von der VMware-Website herunterladen.

Vorgehensweise

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**.

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.

Vorgehensweise

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.

Vorgehensweise

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**.

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.

Vorgehensweise

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**.

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.

Vorgehensweise

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**.

Upgrade von Orchestrator Appliance 5.5.x und höher auf 7.x

vRealize Orchestrator 7.2 unterstützt das direkte Upgrade von Version 5.5.x, 6.0.x, 7.0 und 7.1.

Sie können Ihre vorhandene Orchestrator Appliance über die Schnittstelle zur Verwaltung virtueller Appliances (VAMI) aktualisieren.

Upgrade der Orchestrator Appliance mithilfe des VMware-Standard-Repositorys

Sie können Orchestrator zum Herunterladen des Upgrade-Pakets aus dem VMware-Standard-Repository konfigurieren.

Voraussetzungen

- Unmounten Sie alle Netzwerkdateisysteme. Weitere Informationen finden Sie im *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Erhöhen Sie den Arbeitsspeicher der Orchestrator Appliance auf mindestens 6 GB. Weitere Informationen finden Sie im *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Erstellen Sie einen Snapshot der virtuellen Orchestrator-Maschine. Weitere Informationen finden Sie im *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Wenn Sie eine externe Datenbank verwenden, sichern Sie diese.

- Wenn Sie die vorkonfigurierte PostgreSQL-Datenbank in Orchestrator verwenden, sichern Sie diese mithilfe des Menüs **Datenbank exportieren** in Control Center.

Vorgehensweise

1 Rufen Sie die Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) unter https://*Orchestrator-Server*:5480 auf und melden Sie sich als **`root`** an.

2 Klicken Sie auf der Registerkarte **Update** auf **Einstellungen**.

Das Optionsfeld neben der Option **Standard-Repository verwenden** ist aktiviert.

3 Klicken Sie auf der Seite **Status** auf **Updates überprüfen**.

4 Wenn Updates verfügbar sind, klicken Sie auf **Updates installieren**.

5 Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung von VMware und bestätigen Sie, dass Sie das Update installieren möchten.

6 Starten Sie Orchestrator Appliance neu, um die Aktualisierung abzuschließen.

a Melden Sie sich erneut als **`root`** bei der Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) an.

7 (Optional) Überprüfen Sie auf der Registerkarte **Update**, ob die neueste Version der Orchestrator Appliance erfolgreich installiert wurde.

Damit haben Sie die Orchestrator Appliance aktualisiert.

Weiter

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

Aktualisieren von Orchestrator Appliance mithilfe eines ISO-Images

Sie können Orchestrator zum Herunterladen eines Upgrade-Pakets aus einer ISO-Imagedatei konfigurieren, die sich auf dem CD-ROM-Laufwerk der Appliance befindet.

Voraussetzungen

- Unmounten Sie alle Netzwerkdateisysteme. Weitere Informationen finden Sie im *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Erhöhen Sie den Arbeitsspeicher der Orchestrator Appliance auf mindestens 6 GB. Weitere Informationen finden Sie im *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Erstellen Sie einen Snapshot der virtuellen Orchestrator-Maschine. Weitere Informationen finden Sie im *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Wenn Sie eine externe Datenbank verwenden, sichern Sie diese.
- Wenn Sie die vorkonfigurierte PostgreSQL-Datenbank in Orchestrator verwenden, sichern Sie diese mithilfe des Menüs **Datenbank exportieren** in Control Center.

Vorgehensweise

1 Laden Sie `VMware vRealize Orchestrator Appliance` *`Version`* `.iso Update Repository Archive` von der offiziellen VMware-Downloadseite herunter.

2 Verbinden Sie das CD-ROM-Laufwerk der virtuellen Orchestrator Appliance-Maschine. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.

3 Stellen Sie die ISO-Imagedatei im CD-ROM-Laufwerk der Appliance bereit. Weitere Informationen finden Sie in der Dokumentation zur *Verwaltung virtueller vSphere-Maschinen*.

4 Rufen Sie die Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) unter https://*Orchestrator-Server*:5480 auf und melden Sie sich als **root** an.

5 Klicken Sie auf der Registerkarte **Update** auf **Einstellungen**.

6 Aktivieren Sie das Optionsfeld neben der Option **CD-ROM-Updates verwenden**.

7 Kehren Sie zur Seite **Status** zurück.

Die Version des verfügbaren Upgrades wird angezeigt.

8 Klicken Sie auf **Updates installieren**.

9 Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung von VMware und bestätigen Sie, dass Sie das Update installieren möchten.

10 Starten Sie Orchestrator Appliance neu, um die Aktualisierung abzuschließen.

a Melden Sie sich erneut als **root** bei der Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) an.

11 (Optional) Überprüfen Sie auf der Registerkarte **Update**, ob die neueste Version der Orchestrator Appliance erfolgreich installiert wurde.

Damit haben Sie die Orchestrator Appliance aktualisiert.

Weiter

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

Upgrade von Orchestrator Appliance mithilfe eines angegebenen Repositorys

Sie können Orchestrator für die Verwendung eines lokalen Repositorys konfigurieren, in das Sie das Upgrade-Archiv hochgeladen haben.

Voraussetzungen

- Unmounten Sie alle Netzwerkdateisysteme. Weitere Informationen finden Sie im *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Erhöhen Sie den Arbeitsspeicher der Orchestrator Appliance auf mindestens 6 GB. Weitere Informationen finden Sie im *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Erstellen Sie einen Snapshot der virtuellen Orchestrator-Maschine. Weitere Informationen finden Sie im *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Wenn Sie eine externe Datenbank verwenden, sichern Sie diese.
- Wenn Sie die vorkonfigurierte PostgreSQL-Datenbank in Orchestrator verwenden, sichern Sie diese mithilfe des Menüs **Datenbank exportieren** in Control Center.

Vorgehensweise

1 Bereiten Sie das lokale Repository für Upgrades vor.

a Installieren und konfigurieren Sie einen lokalen Webserver.

b Laden Sie die Datei `VMware-vRO-Appliance-Version-Build-Nummer-updaterepo.zip` von der offiziellen VMware-Downloadseite herunter.

c Extrahieren Sie das `ZIP`-Archiv in das lokale Repository.

2 Rufen Sie die Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) unter https://*Orchestrator-Server*:5480 auf und melden Sie sich als **root** an.

3 Klicken Sie auf der Registerkarte **Update** auf **Einstellungen**.

4 Aktivieren Sie das Optionsfeld neben der Option **Angegebenes Repository verwenden**.

5 Geben Sie die URL-Adresse des lokalen Repositorys an, indem Sie das Verzeichnis `Update_Repo` angeben.

`http://Lokaler_Webserver:Port/build/mts/release/bora-Build-Nummer/publish/exports/Update_Repo`

6 Wenn für das lokale Repository eine Authentifizierung erforderlich ist, geben Sie den Benutzernamen und das Kennwort ein.

7 Klicken Sie auf **Einstellungen speichern**.

8 Klicken Sie auf der Seite **Status** auf **Updates überprüfen**.

9 Wenn Updates verfügbar sind, klicken Sie auf **Updates installieren**.

10 Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung von VMware und bestätigen Sie, dass Sie das Update installieren möchten.

11 Starten Sie Orchestrator Appliance neu, um die Aktualisierung abzuschließen.

   a Melden Sie sich erneut als **root** bei der Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) an.

12 (Optional) Überprüfen Sie auf der Registerkarte **Update**, ob die neueste Version der Orchestrator Appliance erfolgreich installiert wurde.

Damit haben Sie die Orchestrator Appliance aktualisiert.

Weiter

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

Upgrade eines Orchestrator-Clusters 5.5.x und höher auf 7.x

Sie können einen Orchestrator-Cluster auf Version 7.x aktualisieren, indem Sie eine einzelne Instanz aktualisieren und neu installierte Knoten mit Version 7.x mit ihr verbinden.

Voraussetzungen

- Erstellen Sie einen Snapshot aller vRealize Orchestrator-Serverknoten.
- Sichern Sie die gemeinsame Orchestrator-Datenbank.

Vorgehensweise

1 Beenden Sie die Orchestrator-Dienste `vco-server`, `vco-configurator` und `vco-proxy` auf allen Clusterknoten.

2 Aktualisieren Sie nur eine der Orchestrator-Serverinstanzen im Cluster.

   Weitere Informationen finden Sie unter „Upgrade der Orchestrator Appliance mithilfe des VMware-Standard-Repositorys“, auf Seite 28.

3 Starten Sie den Konfigurationsdienst des Orchestrator-Servers, den Sie aktualisiert haben, und melden Sie sich als **root** bei Control Center an.

4 Wechseln Sie zur Seite **Konfiguration überprüfen**, um den Zustand der Systemkomponenten zu überprüfen.

5 Stellen Sie eine neue Orchestrator Appliance für die aktualisierte Version bereit.

6 Konfigurieren Sie den neuen Knoten mit den Netzwerkeinstellungen einer bestehenden Instanz.

7 Verbinden Sie auf der Seite **Verwaltung des Orchestrator-Clusters** in Control Center den neuen Knoten mit dem aktualisierten Knoten im Cluster.

8 Starten Sie die Orchestrator-Server über die Seite **Startoptionen** in Control Center neu, um übereinstimmende Konfigurationsfingerabdrücke für die Knoten zu erhalten.

9 Vergewissern Sie sich, dass der vRealize Orchestrator-Cluster ordnungsgemäß konfiguriert ist, indem Sie die Seite **Konfiguration überprüfen** in Control Center öffnen.

10 (Optional) Führen Sie Schritt 5 bis Schritt 9 für jeden Knoten im Cluster durch.

Damit haben Sie den Orchestrator-Cluster aktualisiert.

Upgrade eines Orchestrator-Clusters 7.0 auf 7.x

Im Cluster werden mehrere Orchestrator-Serverinstanzen gemeinsam ausgeführt. Wenn Sie bereits einen Cluster von Orchestrator-Serverinstanzen eingerichtet haben, können Sie den Cluster auf die neueste Version von Orchestrator aktualisieren, indem Sie seine Knoten aktualisieren.

Vorgehensweise

1 Beenden Sie die Orchestrator-Dienste `vco-server`, `vco-configurator` und `vco-proxy` auf allen Clusterknoten.

2 Aktualisieren Sie eine der Orchestrator-Serverinstanzen im Cluster.

Weitere Informationen finden Sie unter „Upgrade der Orchestrator Appliance mithilfe des VMware-Standard-Repositorys“, auf Seite 28.

3 Starten Sie den Konfigurationsdienst des Orchestrator-Servers, den Sie aktualisiert haben, und melden Sie sich als **`root`** bei Control Center an.

4 Wechseln Sie zur Seite **Konfiguration überprüfen** und überprüfen Sie den Zustand der Systemkomponenten.

5 Aktualisieren Sie alle übrigen Orchestrator-Serverinstanzen im Cluster.

6 Starten Sie die Orchestrator-Server über die Seite **Startoptionen** in Control Center neu, um übereinstimmende Konfigurationsfingerabdrücke für die Knoten zu erhalten.

7 Vergewissern Sie sich, dass der vRealize Orchestrator-Cluster ordnungsgemäß konfiguriert ist, indem Sie die Seite **Konfiguration überprüfen** in Control Center öffnen.

Damit haben Sie den Orchestrator-Cluster aktualisiert.

Konfigurieren von vRealize Orchestrator in Orchestrator Appliance

5

Obwohl Orchestrator Appliance eine vorkonfigurierte, auf Linux basierende virtuelle Maschine ist, müssen Sie das Standard-vCenter Server-Plug-In und die anderen Standard-Orchestrator-Plug-Ins konfigurieren. Gegebenenfalls müssen Sie auch die Orchestrator-Einstellungen ändern.

Wenn Sie Orchestrator Appliance in einer mittleren oder großen Umgebung einsetzen möchten, ändern Sie den Authentifizierungsbereitsteller, um eine optimale Leistung zu gewährleisten.

Hinweis Die LDAP-Authentifizierung ist eine veraltete Funktion und wird in zukünftigen Versionen nicht mehr unterstützt.

Orchestrator Appliance enthält eine vorkonfigurierte PostgreSQL-Datenbank und einen prozessintegrierten ApacheDS LDAP-Server. Die PostgreSQL-Datenbank und der ApacheDS LDAP-Server sind nur lokal aus der Linux-Konsole der virtuellen Appliance zugänglich.

Vorkonfigurierte Software	Standardanwendergruppe oder -benutzer	Kennwort
Vorkonfiguriertes PostgreSQL	Benutzer: vmware	vmware
Prozessintegrierter ApacheDS LDAP-Server	Benutzergruppe: vcoadmins Benutzer: vcoadmin Der Benutzer „admin“ wird standardmäßig als Orchestrator-Administrator eingerichtet.	vcoadmin
Prozessintegrierter ApacheDS LDAP-Server	Benutzergruppe: vcousers Benutzer: vcouser	vcouser

Die vorkonfigurierte PostgreSQL-Datenbank ist bereit für den Produktionseinsatz. Für den Einsatz der Orchestrator-Appliance in einer Produktionsumgebung mit hohem Datenaufkommen ersetzen Sie die vorkonfigurierte PostgreSQL-Datenbank durch eine externe Datenbankinstanz. Weitere Informationen über das Einrichten einer externen Datenbank finden Sie unter „Konfigurieren der Orchestration-Datenbankverbindung“, auf Seite 43.

Der prozessintegrierte ApacheDS LDAP-Server ist nur für Testzwecke geeignet. Für den Einsatz der Orchestrator-Appliance in einer Produktionsumgebung konfigurieren Sie einen Verzeichnisdienst mit externer Unterstützung oder verwenden Sie vRealize Automation, vSphere- und vCenter Single Sign-On-Authentifizierung. Informationen über das Einrichten eines externen Verzeichnisdienstes oder über vRealize Automation-, vSphere- und vCenter Single Sign-On-Authentifizierungsbereitsteller finden Sie unter „Wählen des Authentifizierungstyps“, auf Seite 36.

Dieses Kapitel behandelt die folgenden Themen:

Anmelden beim Control Center

Um den Konfigurationsprozess zu starten, müssen Sie auf das Control Center zugreifen.

Vorgehensweise

1 Greifen Sie auf das Control Center zu, indem Sie in einem Webbrowser zu https://*your_orchestrator_server_IP_or_DNS_name*:8281 gehen und auf **Orchestrator Control Center** klicken bzw. direkt zu https://*your_orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter navigieren.

2 Melden Sie sich mit dem zu Beginn eingerichteten Standardbenutzernamen und Kennwort an.

- Benutzername: **`root`**

  Der Standardbenutzername kann nicht geändert werden.

- Kennwort: *Ihr_Kennwort*

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.

Sie haben sich erfolgreich beim Control Center angemeldet.

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
HTTP-Server-port	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-Server-port	8281	TCP	Endbenutzer-Webbrowser	Orchestrator-Server	Der Zugriffsport für die Startseite von Orchestrator.
HTTPS-Zugriffsport für Webkonfiguration	8283	TCP	Endbenutzer-Webbrowser	Orchestrator-Konfiguration	Der SSL-Zugangsport 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
LDAP	389	TCP	Orchestrator-Server	LDAP-Server	Der Suchport Ihres LDAP-Authentifizierungsservers. **Hinweis** Die LDAP-Authentifizierung ist eine veraltete Funktion und wird in zukünftigen Versionen nicht mehr unterstützt.
LDAP mit SSL	636	TCP	Orchestrator-Server	LDAP-Server	Der Suchport Ihres sicheren LDAP-Authentifizierungsservers.
LDAP mit globalem Katalog	3268	TCP	Orchestrator-Server	Globaler Katalog-Server	Der Port, an den Microsoft Globaler Katalog-Serverabfragen gerichtet sind.
vCenter Single Sign-On-Server	7444	TCP	Orchestrator-Server	vCenter Single Sign-On-Server	Der Port, der für die Kommunikation mit dem vCenter Single Sign-On-Server verwendet wird, wenn Sie die **vCenter Single Sign-On-Authentifizierung (veraltet)** mit vCenter Single Sign-On 5.5 konfigurieren.
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.
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.

Wählen des Authentifizierungstyps

Orchestrator benötigt für eine ordnungsgemäße Funktionsweise und zur Verwaltung von Benutzerberechtigungen eine Authentifizierungsmethode.

Orchestrator unterstützt die folgenden Authentifizierungstypen.

LDAP-Authentifizierung	Orchestrator stellt eine Verbindung zu einem laufenden LDAP-Server her. **Hinweis** Die LDAP-Authentifizierung ist eine veraltete Funktion und wird in zukünftigen Versionen nicht mehr unterstützt.
vRealize Automation-Authentifizierung	Orchestrator wird über die vRealize Automation-Komponentenregistrierung authentifiziert.
vSphere-Authentifizierung	Orchestrator wird über Platform Services Controller authentifiziert.
vCenter Single Sign-On-Authentifizierung (Legacy)	Verwenden Sie diesen Authentifizierungsmodus nur, falls der erforderliche Authentifizierungsanbieter vCenter Single Sign-On 5.5 ist.

Wenn Sie die Orchestrator Appliance herunterladen und bereitstellen, wird der Orchestrator-Server zum Einsatz mit dem in der Appliance vorinstallierten ApacheDS LDAP-Verzeichnisdienst vorkonfiguriert. Wenn Sie Orchestrator jedoch bereits für die Authentifizierung über vRealize Automation, vSphere oder SSO (Legacy) konfiguriert haben, wird die LDAP-Option nicht mehr im Dropdown-Menü **Authentifizierungsmodus** angezeigt.

Wichtig Wenn Sie Orchestrator über den vSphere Web Client zur Verwaltung der vSphere-Bestandslisteobjekte verwenden möchten, müssen Sie Orchestrator für die Verwendung mit demselben Platform Services Controller konfigurieren, mit dem vCenter Server und vSphere Web Client verbunden sind.

Konfigurieren der LDAP-Einstellungen

Sie können Orchestrator so konfigurieren, dass eine Verbindung zu einem laufenden LDAP-Server in Ihrer Infrastruktur zur Benutzerauthentifizierung und zur Verwaltung von Benutzerberechtigungen hergestellt wird.

Hinweis Die LDAP-Authentifizierung ist eine veraltete Funktion und wird in zukünftigen Versionen nicht mehr unterstützt.

Wenn Sie sicheres LDAP über SSL, Windows Server 2008 oder 2012 und Active Directory verwenden, vergewissern Sie sich, dass die Gruppenrichtlinie **Signaturanforderungen für LDAP-Server** auf dem LDAP-Server deaktiviert ist.

Wichtig Mehrere Domänen in verschiedenen Strukturen mit gegenseitigen Vertrauensbeziehungen werden nicht unterstützt und funktionieren mit Orchestrator nicht. Die Domänenstruktur ist die einzige für Active Directory mit mehreren Domänen unterstützte Konfiguration. Gesamtstruktur-Vertrauensstellung und externe Vertrauensstellungen werden nicht unterstützt.

1 Importieren des SSL-Zertifikats für den LDAP-Server auf Seite 37

   Wenn Ihr LDAP-Server SSL nutzt, können Sie die SSL-Zertifikatsdatei in Control Center importieren und eine sichere Verbindung zwischen Orchestrator und LDAP herstellen.

2 Konfigurieren der LDAP-Authentifizierung auf Seite 38

Um Orchestrator mit einer Verzeichnisserverinstanz zu verbinden, müssen Sie den Host, den Port und die Suchbasis des LDAP-Servers angeben, der zum Generieren der Verbindungs-URL verwendet werden soll. Darüber hinaus müssen Sie die Benutzeranmeldedaten sowie die Suchpfade für Benutzer und Gruppen angeben, damit die LDAP-Benutzer sich beim Orchestrator-Client authentifizieren können.

3 Häufige Active Directory LDAP-Fehler auf Seite 40

Wenn eine Fehlermeldung `LDAP:error code 49` auftritt und Sie Probleme bei der Verbindung zu Ihrem LDAP-Authentifizierungsserver feststellen, können Sie überprüfen, welche LDAP-Funktion das Problem ausgelöst hat.

Importieren des SSL-Zertifikats für den LDAP-Server

Wenn Ihr LDAP-Server SSL nutzt, können Sie die SSL-Zertifikatsdatei in Control Center importieren und eine sichere Verbindung zwischen Orchestrator und LDAP herstellen.

Sie können das LDAP-SSL-Zertifikat über die Seite **Zertifikate** im Control Center importieren.

Voraussetzungen

- Wenn Sie LDAP-Server, Windows Server 2008, Windows Server 2012 und Active Directory verwenden, vergewissern Sie sich, dass die Gruppenrichtlinie **Signaturanforderungen für LDAP-Server** auf dem LDAP-Server deaktiviert ist.
- Rufen Sie ein selbstsigniertes oder von einer Zertifizierungsstelle signiertes Zertifikat ab.
- Konfigurieren Sie Ihren LDAP-Server für den SSL-Zugriff. Anweisungen hierfür finden Sie in der Dokumentation für Ihren LDAP-Server.
- Geben Sie explizit das vertrauenswürdige Zertifikat für die ordnungsgemäße SSL-Autorisierung an.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** an.

2 Klicken Sie auf **Zertifikate**.

3 Klicken Sie auf der Registerkarte **Vertrauenswürdige Zertifikate** auf **Importieren**.

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

Option	Aktion
Aus URL oder Proxy-URL importieren	Geben Sie die URL des LDAP-Servers ein: `https://IP–Adresse_Ihres_LDAP–Servers` oder `IP–Adresse_Ihres_LDAP–Servers:Port`
Aus Datei importieren	Rufen Sie die LDAP-SSL-Zertifikatsdatei ab und navigieren Sie, um sie zu importieren.

5 Klicken Sie auf **Importieren**.

Eine Nachricht wird angezeigt, in der bestätigt wird, dass der Import erfolgreich war.

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

Weiter

Beim Generieren der URL für die LDAP-Verbindung sollten Sie im Control Center auf der Seite **Anbieter für Authentifizierung konfigurieren** SSL aktivieren.

Konfigurieren der LDAP-Authentifizierung

Um Orchestrator mit einer Verzeichnisserverinstanz zu verbinden, müssen Sie den Host, den Port und die Suchbasis des LDAP-Servers angeben, der zum Generieren der Verbindungs-URL verwendet werden soll. Darüber hinaus müssen Sie die Benutzeranmeldedaten sowie die Suchpfade für Benutzer und Gruppen angeben, damit die LDAP-Benutzer sich beim Orchestrator-Client authentifizieren können.

Die unterstützten Verzeichnisdienste sind Active Directory über LDAP und Verzeichnisdienste, die auf OpenLDAP basieren.

Hinweis Wenn Sie den LDAP-Server oder den Typ den Verzeichnisdiensts ändern, nachdem Sie Zugriffsrechte für Workflows oder Aktionen für Orchestrator-Objekte zugewiesen haben, müssen Sie diese Berechtigungen zurücksetzen.

Wenn Sie die LDAP-Einstellungen ändern, nachdem Sie benutzerdefinierte Anwendungen konfiguriert haben, die Benutzerdaten sammeln und speichern, werden die LDAP-Authentifizierungseinträge bei Verwendung mit der neuen LDAP-Datenbank ungültig.

Voraussetzungen

Verwenden Sie zum Konfigurieren der LDAP-Authentifizierung die detaillierten Einstellungsinformationen. Weitere Informationen finden Sie unter „LDAP-Authentifizierungseinstellungen“, auf Seite 38.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** an.

2 Klicken Sie auf **Anbieter für Authentifizierung konfigurieren**.

3 Wählen Sie im Dropdown-Menü **Authentifizierungsmodus** die Option **LDAP-Authentifizierung** aus.

4 Wählen Sie im Dropdown-Menü **LDAP-Client** den gewünschten Verzeichnisservertyp.

5 Konfigurieren Sie den LDAP-Server in Ihrer Umgebung.

6 Klicken Sie auf **Änderungen speichern**.

7 Geben Sie unter **Anmeldung testen** Anmeldedaten für einen LDAP-Benutzer ein, um zu testen, ob dieser Benutzer auf den Orchestrator-Client zugreifen kann.

   Das System prüft nach einer erfolgreichen Anmeldung, ob der Benutzer zur Gruppe der Orchestrator-Administratoren gehört.

Weiter

Konfigurieren Sie die Datenbank. Weitere Informationen finden Sie unter „Konfigurieren der Orchestration-Datenbankverbindung“, auf Seite 43.

LDAP-Authentifizierungseinstellungen

Für eine erfolgreiche Verbindung zwischen Orchestrator und dem Verzeichnisserver müssen Sie die LDAP-Authentifizierungseinstellungen passend zu den jeweiligen LDAP-Servereinstellungen konfigurieren.

Tabelle 5-3. LDAP-Authentifizierungsoptionen

Optionen	Beschreibungen
Primärer LDAP-Host	Die IP-Adresse oder der DNS-Name des ersten Hosts, auf dem Control Center Benutzeranmeldedaten überprüft.
Sekundärer LDAP-Host	Die IP-Adresse oder der DNS-Name des Hosts, auf dem Control Center Benutzeranmeldedaten überprüft, falls der primäre LDAP-Host nicht mehr verfügbar ist.

Tabelle 5-3. LDAP-Authentifizierungsoptionen (Fortsetzung)

Optionen	Beschreibungen
Port	Der Wert des Suchports Ihres LDAP-Servers. **Hinweis** Orchestrator unterstützt die hierarchische Domänenstruktur von Active Directory. Falls Ihr Domänencontroller für die Verwendung eines globalen Katalogs konfiguriert ist, müssen Sie Port 3268 wählen. Sie können sich über den Standardport 389 nicht mit einem Global Catalog-Server verbinden.
Root	Der Root-Namespace-Container. Für den Domänennamen *company.org* wäre der Root-Container **`dc=company,dc=org`**. **Hinweis** Zur Verbesserung der Leistung in umfangreichen Dienstverzeichnissen können Sie die Suchbasis einschränken, indem Sie einen bestimmten Container in der Baumstruktur definieren. Sie können etwa **`ou=employees,dc=company,dc=org`** angeben, anstatt das gesamte Verzeichnis zu durchsuchen. Damit gibt der Suchfilter alle Benutzer in der Organisationseinheit für Mitarbeiter zurück. Mit Werten, die Sie in die erforderlichen Textfelder eingeben, wird die folgende LDAP-Verbindungs-URL generiert: `ldap://DomainController:389/ou=employees,dc=company,dc=org`.
SSL verwenden	Wenn diese Option aktiviert ist, wird die Verbindung zwischen Orchestrator und LDAP verschlüsselt. **Hinweis** Wenn Ihr LDAP SSL nutzt, müssen Sie zuerst das SSL-Zertifikat importieren und den Orchestrator-Serverdienst neu starten. Weitere Informationen finden Sie unter „Importieren des SSL-Zertifikats für den LDAP-Server“, auf Seite 37.
Benutzername	Der Name des Benutzerkontos, das über Berechtigungen zum Durchsuchen der Verzeichnisstruktur verfügt. Sie können den Benutzernamen in Active Directory in einem der folgenden Formate angeben: ■ Einfacher Benutzername, z. B.:**`user`** ■ Distinguished Name, z. B.: **`cn=user,ou=employees,dc=company,dc=org`** ■ Prinzipalname, z. B.: **`user@company.org`**
Kennwort	Das Kennwort für das Benutzerkonto, das über Berechtigungen zum Durchsuchen der Verzeichnisstruktur verfügt.
Benutzer-Suchbasis	LDAP-Container oder Organisationseinheit, in denen Orchestrator nach potenziellen Benutzern sucht.
Admin-Gruppe	Die Admin-Gruppe muss eine LDAP-Gruppe sein, für die Sie Orchestrator Administratorrechte gewähren. Beispiel: **`Domain Admins`**.
Zeitüberschreitung bei Anforderung	Wert in Millisekunden, der den Zeitraum bestimmt, während dessen der Orchestrator-Server auf eine Antwort auf eine Anforderung an das Dienstverzeichnis wartet. Kommt es zu einer Zeitüberschreitung, ändern Sie diesen Wert, um zu ermitteln, ob die Zeitüberschreitung im Orchestrator-Server auftritt.
Zeitüberschreitung für Erreichbarkeit des Hosts	Wert in Millisekunden, der die Zeitüberschreitung für die Prüfung der Konnektivität zum Zielhost bestimmt.

Tabelle 5-3. LDAP-Authentifizierungsoptionen (Fortsetzung)

Optionen	Beschreibungen
Links dereferenzieren	Wenn diese Option ausgewählt wird, löst der LDAP-Server Benutzeraliasse für das gesuchte Benutzerobjekt auf.
Filterattribute	Filtert die von der LDAP-Suche zurückgegebenen LDAP-Attribute. Ist dieses Kontrollkästchen aktiviert, läuft die LDAP-Suche schneller ab, da bestimmte Attribute nicht zurückgegeben werden. Sie benötigen jedoch eventuell später einige zusätzliche LDAP-Attribute für die Automatisierung.

Häufige Active Directory LDAP-Fehler

Wenn eine Fehlermeldung `LDAP:error code 49` auftritt und Sie Probleme bei der Verbindung zu Ihrem LDAP-Authentifizierungsserver feststellen, können Sie überprüfen, welche LDAP-Funktion das Problem ausgelöst hat.

Tabelle 5-4. Häufige Active Directory-Authentifizierungsfehler

Fehler	Beschreibung
525	Der Benutzer wurde nicht gefunden.
52e	Die Benutzeranmeldedaten sind ungültig.
530	Eine Anmeldung durch den Benutzer ist gegenwärtig nicht zulässig.
531	Eine Anmeldung durch den Benutzer ist an dieser Workstation nicht zulässig.
532	Das Kennwort ist abgelaufen.
533	Dieses Benutzerkonto wurde deaktiviert.
701	Dieses Benutzerkonto ist abgelaufen.
773	Der Benutzer muss sein Kennwort zurücksetzen.
775	Dieses Benutzerkonto wurde gesperrt.

Authentifizierung von vRealize Automation wird konfiguriert.

Sie können Orchestrator für die Authentifizierung über die Komponentenregistrierung von vRealize Automation konfigurieren.

Voraussetzungen

Installieren und konfigurieren Sie vRealize Automation und stellen Sie sicher, dass Ihr vRealize Automation-Server ausgeführt wird.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** an.

2 Klicken Sie auf **Anbieter für Authentifizierung konfigurieren**.

3 Wählen Sie im Dropdown-Menü **Authentifizierungsmodus** die Option **vRealize Automation** aus.

4 Geben Sie im Textfeld **Hostadresse** die Adresse Ihres vRealize Automation-Hosts ein und klicken Sie auf **Verbinden**.

5 Klicken Sie auf **Zertifikat akzeptieren**.

6 Geben Sie in die Textfelder **Benutzername** und **Kennwort** die Anmeldedaten des vRealize Automation-Administratorkontos ein.

   Das Konto wird nur temporär zum Registrieren oder Entfernen von Orchestrator verwendet.

7 (Optional) Aktivieren Sie das Kontrollkästchen **Lizenzen konfigurieren**.

8 Klicken Sie auf **Registrieren**.

9 Geben Sie in das Textfeld **Standardmandant** die Standarddomäne ein, um einen Benutzer zu authentifizieren, der sich ohne einen Domänennamen anmeldet. Der Standardwert ist **`vsphere.local`**.

10 Geben Sie in das Textfeld **Admin-Gruppe** eine Administratorgruppe ein und klicken Sie auf **Suchen**.

11 Wählen Sie eine Administratorgruppe aus.

12 Klicken Sie auf **Änderungen speichern**.

   Eine Meldung zeigt an, dass die Angaben gespeichert wurden.

Weiter

Damit die Änderungen wirksam werden, starten Sie den Orchestrator-Server auf der Seite „Startoptionen“ im Control Center neu.

Konfigurieren der vCenter Single Sign-On-Einstellungen

VMware vCenter Single Sign-On ist ein Authentifizierungsdienst, der auf vermittelter Authentifizierung basiert. Sie können Orchestrator so konfigurieren, dass eine Verbindung zu einer vCenter Single Sign-On-Instanz erstellt wird, die auf einem Platform Services Controller-Server ausgeführt wird.

Der vCenter Single Sign-On-Server bietet ein Authentifizierungsschnittstelle mit der Bezeichnung Security Token Service (STS). Die Clients senden Authentifizierungsmeldungen an den STS, der die Anmeldedaten des Benutzers mit einer der Identitätsquellen abgleicht. Bei erfolgreicher Authentifizierung erzeugt der STS ein Token.

Der Platform Services Controller enthält die Verwaltungsoberfläche von vCenter Single Sign-On, die Teil von vSphere Web Client ist. Zum Konfigurieren von vCenter Single Sign-On und zum Verwalten der vCenter Single Sign-On-Benutzer und -Gruppen melden Sie sich bei vSphere Web Client als Benutzer mit vCenter Single Sign-On-Administratorrechten an. Dies ist möglicherweise nicht derselbe Benutzer wie der vCenter Server-Administrator. Sie müssen die Anmeldedaten auf der Anmeldeseite von vSphere Web Client angeben. Bei der Authentifizierung können Sie auf das vCenter Single Sign-On-Verwaltungstool zugreifen, um Benutzer zu erstellen und anderen Benutzern Verwaltungsrechte zuzuweisen.

Mithilfe von vSphere Web Client authentifizieren Sie sich bei vCenter Single Sign-On durch Angabe Ihrer Anmeldedaten auf der Anmeldeseite von vSphere Web Client. Sie können dann alle vCenter Server-Instanzen sehen, für die Sie Berechtigungen haben. Nachdem Sie eine Verbindung zu vCenter Server hergestellt haben, ist keine weitere Authentifizierung erforderlich. Welche Aktionen Sie auf Objekte anwenden können, hängt von Ihren vCenter Server-Berechtigungen für diese Objekte ab.

Weitere Informationen zum Platform Services Controller finden Sie unter *vSphere-Sicherheit*.

Stellen Sie nach der Konfiguration von Orchestrator zur Authentifizierung mithilfe von vCenter Single Sign-On sicher, dass Sie den Einsatz mit den vCenter Server-Instanzen konfiguriert haben, die bei dem vSphere Web Client registriert wurden, der dieselbe vCenter Single Sign-On-Instanz verwendet.

Wenn Sie sich beim vSphere Web Client anmelden, kommuniziert das Orchestrator-Web-Plug-In mit dem Orchestrator-Server im Namen des zur Anmeldung verwendeten Benutzerprofils.

Konfigurieren der Authentifizierung über vSphere Platform Services Controller

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

Voraussetzungen

Installieren und konfigurieren Sie VMware vCenter Single Sign-On und stellen Sie sicher, dass Ihr vCenter Single Sign-On-Server ausgeführt wird.

Wichtig Achten Sie darauf, dass die Uhren von Orchestrator-Server und der vCenter Server Appliance synchronisiert sind. Andernfalls können bei vCenter Single Sign-On unverständliche Fehler auftreten.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** an.

2 Klicken Sie auf **Anbieter für Authentifizierung konfigurieren**.

3 Wählen Sie im Dropdown-Menü **Authentifizierungsmodus** die Option **vSphere** aus.

4 Geben Sie im Textfeld **Hostadresse** die Hostadresse Ihres Platform Services Controller ein und klicken Sie auf **Verbinden**.

5 Klicken Sie auf **Zertifikat akzeptieren**.

6 Geben Sie in die Textfelder **Benutzername** und **Kennwort** die Anmeldedaten des vCenter Single Sign-On-Administratorkontos ein.

   Das Konto wird nur temporär zum Registrieren oder Entfernen von Orchestrator verwendet.

7 (Optional) Aktivieren Sie das Kontrollkästchen **Lizenzen konfigurieren**.

8 Klicken Sie auf **Registrieren**.

9 Geben Sie in das Textfeld **Standardmandant** die Standarddomäne ein, um einen Benutzer zu authentifizieren, der sich ohne einen Domänennamen anmeldet. Der Standardwert ist **`vsphere.local`**.

10 Geben Sie in das Textfeld **Admin-Gruppe** eine Administratorgruppe ein und klicken Sie auf **Suchen**.

11 Klicken Sie auf **Änderungen speichern**.

   Eine Meldung zeigt an, dass die Angaben gespeichert wurden.

Sie haben Orchestrator erfolgreich mit vCenter Single Sign-On registriert.

Registrieren von Orchestrator als vCenter Single Sign-On-Lösung (Legacy)

Sie können den Orchestrator-Server mithilfe des Legacy-Authentifizierungsmodus für Single Sign-On im Control Center bei einem vCenter Single Sign-On-Server registrieren. Verwenden Sie die Legacy-Authentifizierung für Single Sign-On nur mit vCenter Server Version 5.5 und den dazugehörigen Update-Releases ab Update 2.

Voraussetzungen

Installieren und konfigurieren Sie VMware vCenter Single Sign-On und stellen Sie sicher, dass Ihr vCenter Single Sign-On-Server ausgeführt wird.

Wichtig Achten Sie darauf, dass die Uhren von Orchestrator-Server und der vCenter Server Appliance synchronisiert sind. Andernfalls können bei vCenter Single Sign-On unverständliche Fehler auftreten.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** an.

2 Klicken Sie auf **Anbieter für Authentifizierung konfigurieren**.

3 Wählen Sie **SSO (Legacy)** aus dem Dropdown-Menü **Authentifizierungsmodus**.

4 Geben Sie im Textfeld **STS-URL** die URL für die Schnittstelle des vCenter Single Sign-On-Tokendienstes ein.

```
https://Ihr_vCenter_Single-Sign-On-Server:7444/sts/STSService/vsphere.local
```

5 Geben Sie im Textfeld **Admin-URL** die URL für die Schnittstelle des vCenter Single Sign-On-Verwaltungsdienstes ein.

```
https://Ihr_vCenter_Single_Sign-On-Server:7444/sso-adminserver/sdk/vsphere.local
```

6 Klicken Sie auf **Verbinden**.

7 Klicken Sie auf **Zertifikat akzeptieren**.

8 Geben Sie in die Textfelder **Benutzername** und **Kennwort** die Anmeldedaten des vCenter Single Sign-On-Administrators ein.

Das Konto wird nur temporär zum Registrieren oder Entfernen von Orchestrator verwendet.

9 Klicken Sie auf **Registrieren**.

10 Geben Sie in das Textfeld **Standardmandant** die Standarddomäne ein, um einen Benutzer zu authentifizieren, der sich ohne einen Domänennamen anmeldet. Der Standardwert ist `vsphere.local`.

11 Geben Sie in das Textfeld **Admin-Gruppe** eine Administratorgruppe ein und klicken Sie auf **Suchen**.

12 Klicken Sie auf **Änderungen speichern**.

Eine Meldung zeigt an, dass die Angaben gespeichert wurden.

Sie haben Orchestrator erfolgreich mit vCenter Single Sign-On registriert.

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“, auf Seite 22. 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.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** 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: `https://Ihre_Datenbank_Server_IP_Adresse` oder `Ihre_Datenbank_Server_IP_Adresse:Port`
Aus Datei importieren	Rufen Sie die Datenbank-SSL-Zertifikatsdatei ab und navigieren Sie zum Import.

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

Weiter

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. Weitere Informationen finden Sie unter „Einrichten der Orchestrator-Datenbank“, auf Seite 22.
- 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 von wesentlicher Bedeutung für eine internationalisierte Umgebung.
- 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“, auf Seite 43.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** 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.

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.
Datenbankname	Der vollständige eindeutige Name Ihrer Datenbank. Der Datenbankname ist im Parameter `SERVICE_NAMES` in der Datei mit den Initialisierungsparametern angegeben. Diese Option ist nur für SQL Server- und PostgreSQL-Datenbanken gültig.
Benutzername	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. Diese Option ist auf alle Datenbanken anwendbar.
Kennwort	Das Kennwort für den Benutzernamen. Diese Option ist auf alle Datenbanken anwendbar.
Instanzname (sofern vorhanden)	Der Name der Datenbankinstanz, die durch den Parameter `INS–TANCE_NAME` in der Datei mit dem Datenbankinitialisierungsparameter identifiziert werden kann. Diese Option ist nur für SQL Server- und Oracle-Datenbanken gültig.

Option	Beschreibung
Domäne	Wenn Sie die Windows-Authentifizierung verwenden möchten, geben Sie den Domänennamen des SQL Servercomputers ein (z. B. *Unternehmen.org*). Wenn Sie die SQL-Authentifizierung verwenden möchten, lassen Sie dieses Textfeld unausgefüllt. Diese Option ist nur für SQL Server gültig und legt fest, ob Sie Windows- oder SQL Server-Authentifizierung verwenden möchten.
Windows-Authentifizierungsmodus (NTLMv2) verwenden	Wählen Sie diese Option aus, um NTLMv2-Antworten bei Verwendung der Windows-Authentifizierung zu senden. Diese Option ist nur für SQL Server gültig.

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

5 Aktualisieren Sie, falls erforderlich, die Tabellenstruktur für Orchestrator.

6 Klicken Sie auf **Änderungen speichern**.

Die Datenbankverbindung wurde erfolgreich konfiguriert.

Exportieren der Orchestrator-Datenbank

Erstellen Sie ein Archiv mit einer vollständigen Sicherung der Serverdatenbank. Die Datenbank lässt sich nur exportieren, wenn es sich um eine PostgreSQL-Datenbank handelt, die unter Linux ausgeführt wird.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** an.

2 Klicken Sie auf **Datenbank exportieren**.

3 Wählen Sie aus, ob Workflowtoken und Protokollereignisse zusammen mit der Datenbank exportiert werden sollen.

4 Klicken Sie auf **Datenbank exportieren**.

Control Center erstellt eine Datei namens `vco-db-dump-`*`databaseName@Hostname`*`.gz` auf dem Computer, auf dem der Orchestrator-Server installiert ist. Sie können diese Datei zum Klonen und Wiederherstellen des 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.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** 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**.

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.

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: `https://IP-Adresse_Ihres_Servers` oder `IP-Adresse:Port_Ihres_Servers`
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“, auf Seite 48.

Erstellen eines selbstsignierten Zertifikats

In der Orchestrator Appliance ist eine 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`.

Option	Beschreibung
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 Domänennamen des Servers, mit dem Orchestrator eine Verbindung über SSL herstellen soll.

Vorgehensweise

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–_oder_DNS–Name:25 –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**.

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 der Orchestrator-Plug-Ins

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

Ändern der Protokollierungsebene für Plug-Ins

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

Installieren eines neuen Plug-Ins

Die Orchestrator-Plug-Ins ermöglichen die Integration anderer Softwareprodukte in Orchestrator-Server. Die Orchestrator Appliance stellt eine Reihe vorinstallierter Plug-Ins bereit, und Sie können darüber hinaus benutzerdefinierte Plug-Ins installieren.

Alle Orchestrator-Plug-Ins werden über Control Center installiert. Dabei können die Dateierweiterungen `.vmoapp` und `.dar` verwendet werden. Eine `.vmoapp`-Datei kann eine Sammlung mehrerer `.dar`-Dateien enthalten und kann als Anwendung installiert werden. Eine `.dar`-Datei hingegen enthält sämtliche zu einem Plug-In gehörigen Ressourcen.

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“, auf Seite 50.

Deinstallieren eines Plug-Ins

Sie können ein Plug-In mit Control Center deaktivieren, aber dadurch wird die Plug-In-Datei nicht aus dem Orchestrator Appliance-Dateisystem entfernt. Um die Plug-In-Datei zu entfernen, müssen Sie sich bei der Orchestrator Appliance anmelden und die Plug-In-Datei manuell entfernen.

Vorgehensweise

1 Löschen Sie das Plug-In aus der Orchestrator Appliance.

   a Melden Sie sich bei der Orchestrator Appliance über SSH als **root** an.

   b Öffnen Sie die Datei `/etc/vco/app-server/plugins/_VSOPluginInstallationVersion.xml` mit einem Texteditor.

   c Löschen Sie die Codezeile, die dem zu entfernenden Plug-In entspricht.

   d Navigieren Sie zum Verzeichnis `/var/lib/vco/app-server/plugins`.

   e Löschen Sie die `.dar`-Archive , die das zu entfernende Plug-In enthalten.

2 Starten Sie die vRealize Orchestrator-Dienste neu.

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

3 Melden Sie sich beim Control Center als **root** an.

4 Prüfen Sie auf der Seite **Plug-Ins verwalten**, ob das Plug-In entfernt wurde.

5 Löschen Sie über den Orchestrator-Client die Pakete und Ordner des Plug-Ins.

   a Melden Sie sich beim Orchestrator-Client an.

   b Wählen Sie im Dropdown-Menü in der oberen linken Ecke die Option **Design** aus.

   c Klicken Sie auf die Ansicht **Pakete**.

   d Klicken Sie mit der rechten Maustaste auf das zu löschende Paket und wählen Sie **Element mit Inhalt löschen**.

   Hinweis Orchestrator-Elemente, die als schreibgeschützt gesperrt sind (z. B. Beispielworkflows in der Standardbibliothek), werden nicht gelöscht.

   e Wählen Sie im Menü **Extras** in der oberen rechten Ecke die Option **Benutzereinstellungen** aus.

   Das Kontextmenü **Einstellungen** wird geöffnet.

   f Wählen Sie auf der Seite **Allgemein** das Kontrollkästchen **Löschen von Ordnern mit Inhalten zulässig** aus.

   Sie können jetzt mit einem einzigen Klick einen gesamten Ordner löschen, einschließlich den Unterordnern und Workflows.

   g Klicken Sie auf die Ansicht **Workflow**.

   h Löschen Sie den Ordner des Plug-Ins, das Sie entfernen möchten.

   i Klicken Sie auf die Ansicht **Aktionen**.

   j Löschen Sie die Aktionsmodule des Plug-Ins, das Sie entfernen möchten.

6 Starten Sie die vRealize Orchestrator-Dienste neu.

Sie haben alle benutzerdefinierten Workflows, Aktionen, Richtlinien, Konfigurationen, Einstellungen und Ressourcen des Plug-Ins entfernt.

Startoptionen für Orchestrator

Auf der Seite **Startoptionen** in Control Center können Sie den Orchestrator-Serverdienst starten, beenden und neu starten.

Der erstmalige Start von Orchestrator kann fünf bis zehn Minuten in Anspruch nehmen, da der Server den Inhalt der Orchestrator-Plug-Ins in den Datenbanktabellen installiert.

Auf der Seite **Startoptionen** wird der Status des `vco-server`-Dienstes angezeigt.

Status	Beschreibung
`WIRD AUSGEFÜHRT`	Der Orchestrator-Serverdienst wurde initialisiert und wird erwartungsgemäß ausgeführt.
`NICHT DEFINIERT`	Der Orchestrator-Server wird gestartet.
`BEENDET`	Der Orchestrator-Serverdienst wird nicht ausgeführt.

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 festzustellen, ob ein Knoten ausgeführt wird, können Sie den REST-API-Dienst für den Betriebszustand unter https://*Ihre_Orchestrator_Server_IP_oder_DNS-Name*:8281/vco/api/healthstatus verwenden und den Status des Knotens überprüfen.

Wichtig Eine Workflow-Entwicklung durch mehrere Benutzer wird in einer geclusterten Umgebung nicht unterstützt. Wenn andere Benutzer die anderen Orchestrator-Knoten innerhalb des Clusters verwenden, um dieselbe Ressource zu ändern, treten Parallelitätsprobleme auf. Um mehrere aktive Orchestrator-Serverknoten in einem Cluster zu verwenden, müssen Sie zuerst die benötigten Workflows entwickeln. Im Anschluss daran können Sie Orchestrator für die Verwendung im Cluster einrichten.

Konfigurieren eines Orchestrator-Clusters

Sie können ein Cluster von Orchestrator-Serverinstanzen erstellen, um die Verfügbarkeit der Orchestrator-Dienste zu verbessern.

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

Voraussetzungen

- Installieren Sie mindestens zwei Orchestrator-Serverinstanzen.
- Konfigurieren Sie die externe Datenbank, die Sie als gemeinsame Datenbank vorgesehen haben, damit diese Verbindungen mit den verschiedenen Orchestrator-Instanzen aufbauen kann.

  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.
- Synchronisieren Sie die Uhren der virtuellen Maschinen, auf denen die Orchestrator-Serverinstanzen installiert sind.

Vorgehensweise

1 Konfigurieren Sie den ersten Orchestrator-Knoten.

   a Melden Sie sich beim Control Center des ersten Orchestrator-Servers als **`root`** an.

   b Beenden Sie den Orchestrator-Serverdienst über die Seite **Startoptionen**.

   c Konfigurieren Sie die Verbindung zur gemeinsamen externen Datenbank. Weitere Informationen finden Sie unter „Konfigurieren der Datenbankverbindung“, auf Seite 44.

   Änderungen der Konfiguration, z. B. bei Zertifikaten, Lizenzen oder dem Authentifizierungsanbieter, müssen nach der Konfiguration der Orchestrator-Instanzen zur Nutzung mit gemeinsam genutzten Datenbanken erfolgen.

   d Konfigurieren Sie den Authentifizierungsanbieter. Weitere Informationen finden Sie unter „Wählen des Authentifizierungstyps“, auf Seite 36.

   e (Optional) Legen Sie eventuell benötigte Systemeigenschaften fest. Informationen hierzu finden Sie unter Kapitel 11, „Festlegen von Systemeigenschaften“, auf Seite 97.

   f (Optional) Öffnen Sie die Seite **Integration der Protokollierung** und konfigurieren Sie Orchestrator für die Verwendung eines Remoteprotokollservers.

g (Optional) Geben Sie auf der Registerkarte **Orchestrator-Knoteneinstellungen** der Seite **Verwaltung des Orchestrator-Clusters** Werte für die Orchestrator-Knoteneinstellungen ein und klicken Sie auf **Speichern**.

Option	Beschreibung
Anzahl der aktiven Knoten	Die maximale Anzahl aktiver Orchestrator-Serverinstanzen im Cluster. Aktive Knoten sind die Orchestrator-Serverinstanzen, die Workflows ausführen und auf Clientanfragen antworten. Wenn ein aktiver Orchestrator-Knoten nicht mehr antwortet, wird er durch eine inaktive Orchestrator-Serverinstanz ersetzt. Der Standardwert für die Anzahl aktiver Orchestrator-Knoten in einem Cluster ist eins.
Taktsignalintervall (in Millisekunden)	Das Zeitintervall in Millisekunden zwischen zwei Netzwerk-Taktsignalen, die ein Orchestrator-Knoten als Betriebssignal sendet. Die Standardeinstellung beträgt 12 Sekunden.
Anzahl der Failover-Taktsignale	Die Anzahl fehlender Taktsignale, bevor ein Orchestrator-Knoten als ausgefallen betrachtet wird. Der Standardwert beträgt zehn Taktsignale.

Das Standardintervall für Zeitüberschreitung beträgt 2 Minuten und entspricht dem Wert des Standard-Taktsignalintervalls multipliziert mit der Anzahl der Standard-Failover-Taktsignale.

h Überprüfen Sie auf der Seite **Konfiguration überprüfen** im Control Center, ob der Knoten ordnungsgemäß konfiguriert ist.

i (Optional) Installieren Sie die externen Plug-Ins.

j Starten Sie den Orchestrator-Serverdienst auf dem ersten Orchestrator-Knoten.

k Vergewissern Sie sich, dass auf der Seite **Startoptionen** die Zeichenfolgen **Aktiver Konfigurationsfingerabdruck** und **Ausstehender Konfigurationsfingerabdruck** übereinstimmen.

Hinweis Sie müssen die Seite **Startoptionen** möglicherweise mehrmals aktualisieren, bis die beiden Zeichenfolgen übereinstimmen.

l (Optional) Konfigurieren Sie die externen Plug-Ins.

2 Konfigurieren Sie das Orchestrator-Cluster.

a Melden Sie sich beim Control Center des zweiten Orchestrator-Servers als `root` an.

b Klicken Sie auf die Registerkarte **Knoten mit Cluster verknüpfen** auf der Seite **Verwaltung des Orchestrator-Clusters**.

c Geben Sie im Textfeld **Hostname** den Hostnamen oder die IP-Adresse der ersten Orchestrator-Serverinstanz ein.

d Geben Sie in den Textfeldern **Benutzername** und **Kennwort** Ihre Control Center-Anmeldedaten ein.

e Klicken Sie auf **Beitreten**.

Die Orchestrator-Instanz klont die Konfiguration des Knotens, mit dem sie verbunden wird.

Sie haben erfolgreich ein Cluster von Orchestrator-Instanzen konfiguriert.

Weiter

Sie können dem Cluster weitere aktive Orchestrator-Serverknoten hinzufügen, indem Sie den Wert im Textfeld **Anzahl der aktiven Knoten** auf der Seite **Verwaltung des Orchestrator-Clusters** ändern.

Überwachen und Synchronisieren eines Orchestrator-Clusters

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

Sie können den Konfigurations-Synchronisierungszustand der Orchestrator-Instanzen, die in einem Cluster verbunden sind, auf der Registerkarte **Orchestrator-Knoteneinstellungen** der Seite **Verwaltung des Orchestrator-Clusters** überprüfen.

Wichtig Control Center meldet den Zustand des lokalen Knotens verglichen mit den anderen Knoten im Cluster.

Konfigurations-Synchronisierungszustand	Lokaler Knoten	Remoteknoten
Synchronisiert	Die Konfiguration des lokalen Knotens ist seit dem letzten Neustart unverändert geblieben.	Die Konfiguration des Remoteknotens stimmt mit der Konfiguration des lokalen Knotens überein.
Der Knoten muss neu gestartet werden	Die Konfiguration des lokalen Knotens wurde geändert oder repliziert und dabei vom Remoteknoten übernommen. Starten Sie den lokalen Knoten neu, um die ausstehende Konfiguration anzuwenden.	Die Konfiguration des Remoteknotens wurde mit dem lokalen Knoten synchronisiert, aber nicht angewendet. Starten Sie den Remoteknoten neu, um die Konfiguration anzuwenden.
Eine Konfigurationssynchronisierung ist erforderlich.	n. z.	Die aktive Konfiguration des Remoteknotens unterscheidet von der aktiven Konfiguration des lokalen Knotens.
Das Control Center des Knotens ist nicht verfügbar.	n. z.	Der Control Center-Dienst (`vco-configurator`) des Remoteknotens wurde angehalten oder ist nicht erreichbar. Der Synchronisierungszustand kann nicht abgerufen werden.
Nicht verfügbar. Lokaler Knoten fehlt	Der lokale Knoten ist nicht in der Liste der Clusterknoten enthalten. Der Synchronisierungszustand kann nicht abgerufen werden.	n. z.

Weitergeben einer Konfiguration und Neustarten von Knoten

Beim Ändern der Konfiguration auf dem lokalen Knoten können Sie mithilfe der Option **Konfiguration weitergeben und Knoten neu starten** aus dem Dropdown-Menü die Konfiguration des lokalen Knotens auf alle anderen Knoten im Cluster kopieren. Wenn Sie die Konfiguration kopieren und die Knoten später neu starten möchten, verwenden Sie die Option **Konfiguration weitergeben**.

Entfernen eines Knotens aus einem Orchestrator-Cluster

Wenn Sie einen Knoten aus einem Cluster entfernen möchten, müssen Sie den Knoten für die Verwendung mit einer Datenbank konfigurieren, die nicht von einem Orchestrator-Cluster verwendet wird.

Hinweis Beim Ändern der Datenbank eines Knotens müssen Sie die Zertifikate und die Lizenz entweder importieren oder neu generieren.

Wenn in Control Center Knoten angezeigt werden, die keinem Cluster mehr angehören, rufen Sie die Seite für die erweiterte **Verwaltung des Orchestrator-Clusters** unter https://*Ihre_Orchestrator_Server_IP_oder_DNS_Name*:8283/vco-controlcenter/#/control-app/ha?remove-nodes auf, um die verbliebenen Datensätze zu entfernen.

Konfigurieren eines Lastausgleichsdiensts

Lastausgleichsdienste verteilen in High Availability-Bereitstellungen die Arbeitslast auf die Server.

Nachdem Sie das Orchestrator-Cluster konfiguriert haben, können Sie einen Lastausgleichsdienst einrichten, um den Datenverkehr auf mehrere Instanzen von vRealize Orchestrator zu verteilen. Weitere Informationen finden Sie unter vRealize Orchestrator-Lastausgleich.

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 Kundenzufriedenheit von VMware (Customer Experience Improvement Program, CEIP) liefert VMware Informationen, die es ermöglichen, VMware-Produkte und -Dienste zu verbessern und Probleme zu beheben. Wenn Sie sich dazu entscheiden, am CEIP teilzunehmen, erfasst VMware in regelmäßigen Abständen technische Informationen zur Art und Weise, wie Sie die Produkte und Dienstleistungen von VMware verwenden, und speichert diese in CEIP-Berichten.

Informationen zu den Daten, die VMware erfasst, und zur Art und Weise, wie diese Daten genutzt werden, finden Sie im VMware CEIP-Portal auf http://www.vmware.com/trustvmware/ceip.html

Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit

Treten Sie dem Programm zur Verbesserung der Benutzerfreundlichkeit über Control Center bei.

Vorgehensweise

1 Melden Sie sich beim Control Center als **root** an und öffnen Sie die Seite **Programm zur Verbesserung der Benutzerfreundlichkeit**.

2 Aktivieren Sie das Kontrollkästchen **Am Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen**, um das CEIP zu aktivieren, oder deaktivieren Sie es, um das Programm zu deaktivieren, und klicken Sie auf **Speichern**.

3 (Optional) Deaktivieren Sie das Kontrollkästchen **Automatische Proxy-Erkennung**, wenn Sie einen Proxy-Host manuell hinzufügen möchten.

6 Verwenden der API-Dienste

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 vertrauenswürdiges 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 auf Seite 57

  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 auf Seite 61

  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.

Vorgehensweise

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“, auf Seite 47.

Vorgehensweise

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

Option	Beschreibung
Vertrauenswürdiges Zertifikat aus Datei importieren	Importiert ein vertrauenswürdiges Zertifikat aus einer Datei.
Vertrauenswürdiges Zertifikat von einer URL importieren	Importiert ein vertrauenswürdiges Zertifikat von einer URL-Adresse.
Vertrauenswürdiges Zertifikat mithilfe eines Proxy-Servers von einer URL importieren	Importiert ein vertrauenswürdiges Zertifikat unter Nutzung eines Proxyservers von einer URL-Adresse.
Vertrauenswürdiges Zertifikat mit Zertifikatalias von einer URL importieren	Importiert ein vertrauenswürdiges 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 „Vertrauenswürdiges 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/workf-
lows/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 *IP_Adresse_oder_DNS_Name:Port* 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.

Vorgehensweise

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.

Vorgehensweise

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/workf-
lows/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/workf-
lows/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.

Vorgehensweise

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

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

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

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

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

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

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

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 behandelt die folgenden Themen:

Erstellen neuer Benutzer in Control Center

Zur Vermeidung potenzieller Sicherheitsprobleme können Sie, anstatt das Root-Kennwort zu ändern, ein neues Benutzerkonto erstellen und ihm jederzeit ein Kennwort zuweisen. Durch das Erstellen dieses neuen Benutzerkontos deaktivieren Sie den Zugriff des Root-Kontos auf Control Center.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** an.

2 Klicken Sie auf der Seite **Einstellungen** auf **Anmeldedaten ändern**.

3 Geben Sie Ihr aktuelles Kennwort in das Textfeld **Altes Kennwort** ein.

4 Geben Sie den neuen Benutzernamen in das Textfeld **Neuer Benutzername** ein.

5 Geben Sie das neue Kennwort in das Textfeld **Neues Kennwort** ein.

6 Geben Sie das neue Kennwort zum Bestätigen erneut ein.

7 Klicken Sie auf **Anmeldedaten ändern**.

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.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** 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**.

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 den geklonten Orchestrator 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.

Voraussetzungen

Halten Sie den Orchestrator-Server über die Seite **Startoptionen** im Control Center an.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** 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.

4 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 Klicken Sie auf **Importieren**.

6 Wählen Sie den Typ der zu importierenden Dateien aus.

   Wichtig Verwenden Sie die Option „Plug-In-Import erzwingen“ nur, wenn alle Plug-Ins mit den neuen Versionen durch frühere Versionen ersetzt werden sollen, die möglicherweise in der exportierten Dateien enthalten sind. Eine Versionsinkompatibilität kann dazu führen, dass die Plug-Ins nicht mehr funktionieren.

7 Klicken Sie auf **Import beenden**.

Eine Meldung, dass die Konfiguration erfolgreich importiert wurde, wird angezeigt. Das neue System repliziert die alte Konfiguration vollständig.

Weiter

- Überprüfen Sie, ob vRealize Orchestrator ordnungsgemäß konfiguriert ist, indem Sie die Seite **Konfiguration überprüfen** in Control Center öffnen.
- Starten Sie den Orchestrator-Server über die Seite **Startoptionen** im Control Center neu, damit die Änderungen wirksam werden.

Migrieren der Orchestrator-Konfiguration

Das Orchestrator-Migrationstool bündelt die Konfigurationseinstellungen, Plug-Ins, Plug-In-Konfigurationen, Zertifikate und Lizenzinformationen in einem Archiv, das in vRealize Orchestrator 7.x importiert werden kann.

Die folgenden Befehlszeilenoptionen können für den Befehl `vro-migrate export` verwendet werden:

Option	Beschreibung
`password`	Festlegen eines Kennworts zum Schutz des exportierten Archivs. Wenn Sie kein Kennwort angeben, ist das Archiv nicht geschützt.
`vroRootPath`	Geben Sie den root-Pfad des vRealize Orchestrator-Servers an.

Migrieren der Orchestrator-Konfiguration von Windows auf eine virtuelle Appliance

Sie können Ihre Windows-Standalone-Konfiguration von Orchestrator 5.5x und 6.x in die Orchestrator Appliance migrieren.

Voraussetzungen

- Beenden Sie den Quell- und den Ziel-Orchestrator-Server.
- Erstellen Sie eine Sicherungskopie der Datenbank des Orchestrator-Quellservers.

Vorgehensweise

1 Laden Sie das Migrationstool vom Orchestrator-Zielserver herunter.

   a Melden Sie sich beim Control Center als **root** an.

   b Öffnen Sie die Seite **Konfiguration exportieren/importieren** und klicken Sie auf die Registerkarte **Konfiguration migrieren**.

   c Laden Sie das Migrationstool wie in der Beschreibung auf der Seite angegeben oder direkt von https://*Orchestrator-Server-IP_oder_DNS-Name*:8283/vco-controlcenter/api/server/migration-tool herunter.

2 Exportieren Sie die Orchestrator-Konfiguration vom Orchestrator-Quellserver.

   a Entpacken Sie das heruntergeladene Archiv und legen Sie den Ordner im Installationsordner von Orchestrator ab.

   Der Standardpfad zum Installationsordner von Orchestrator ist bei einer Installation unter Windows `C:\Programme\VMware\Orchestrator`.

   b Legen Sie die Umgebungsvariable `PATH` fest, wobei Sie den `bin`-Ordner der mit Orchestrator installierten Java-JRE wählen.

   c Navigieren Sie mithilfe der Windows-Befehlszeile zum Ordner `bin` im Installationsordner von Orchestrator.

   Standardmäßig ist der Pfad zum Ordner `bin` `C:\Programme\VMware\Orchestrator\migration-cli\bin`.

   d Führen Sie den Befehl `export` über die Befehlszeile aus.

   ```
   C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
   ```

   Dieser Befehl fasst die Konfigurationsdateien und Plug-Ins von VMware vRealize Orchestrator zu einem Exportarchiv zusammen.

   Das Archiv wird im selben Ordner wie der Ordner `migration-cli` erstellt.

3 Importieren Sie die Konfiguration auf dem Orchestrator-Zielserver.

   a Öffnen Sie im Control Center **Konfiguration exportieren/importieren** und klicken Sie auf die Registerkarte **Konfiguration migrieren**.

   b Klicken Sie auf **Importieren**.

   c Wählen Sie den Typ der zu importierenden Dateien.

   Hinweis

   Wenn die Quell- und Ziel-Orchestrator-Server so konfiguriert sind, dass sie dieselbe externe Datenbank verwenden, lassen Sie das Kontrollkästchen **Datenbankeinstellungen migrieren** leer, um eine Aktualisierung des Datenbankschemas auf die neuere Version zu verhindern. Andernfalls ist die Orchestrator-Quellumgebung nicht mehr funktionsfähig.

   d Klicken Sie auf **Migration beenden**.

4 Wenn die Quell-Instanz von vRealize Orchestrator vRealize Automation als Authentifizierungsanbieter verwendet, importieren Sie das SSL-Zertifikat des vRealize Automation-Servers in den Orchestrator Trust Store und ändern Sie den Lizenzanbieter auf dem Orchestrator-Zielserver.

   a Klicken Sie auf der Seite **Zertifikate** im Control Center auf **Aus URL importieren**.

   b Geben Sie die URL des vRealize Automation-Servers an.

c Wechseln Sie zur Seite **Lizenzierung** im Control Center.

d Wählen Sie aus dem Dropdown-Menü **Lizenzanbieter wählen** die Option **vRA-Lizenz**.

5 Wenn die Quell-Instanz von vRealize Orchestrator **vSphere** oder den **SSO (Legacy)**-Authentifizierungsmodus verwendet, ändern Sie den Lizenzanbieter in **Manuelle Lizenz** und geben Sie den Lizenzschlüssel manuell ein.

Eine Meldung bestätigt, dass die Migration erfolgreich abgeschlossen wurde.

Weiter

- Überprüfen Sie, ob vRealize Orchestrator ordnungsgemäß konfiguriert ist, indem Sie die Seite **Konfiguration überprüfen** in Control Center öffnen.
- Starten Sie den Orchestrator-Server über die Seite **Startoptionen** im Control Center neu, damit die Änderungen wirksam werden.

Migrieren eines Clusters von vRealize Orchestrator 6.x-Instanzen unter Windows zu einem Cluster virtueller vRealize Orchestrator 7.1- oder 7.2-Appliances

Sie können Ihr unter Windows installiertes Cluster von vRealize Orchestrator 6.x-Instanzen zu einem Cluster virtueller vRealize Orchestrator-Appliances der Version 7.1 oder 7.2 migrieren.

Voraussetzungen

- Beenden Sie den Orchestrator-Serverdienst der Orchestrator 6.x-Instanzen im Cluster.
- Sichern Sie die Datenbank des externen Orchestrator-Servers einschließlich des Datenbankschemas.
- Stellen Sie einen Orchestrator-Knoten auf der Zielversion bereit. Weitere Informationen finden Sie unter „Herunterladen und Bereitstellen der Orchestrator Appliance“, auf Seite 25.

Vorgehensweise

1 Laden Sie das Migrationstool vom Orchestrator-Zielserver herunter.

a Melden Sie sich beim Control Center als `root` an.

b Öffnen Sie die Seite **Konfiguration exportieren/importieren** und klicken Sie auf die Registerkarte **Konfiguration migrieren**.

c Laden Sie das Migrationstool wie in der Beschreibung angegeben oder direkt von https://*Orchestrator-Server-IP_oder_DNS-Name*:8283/vco-controlcenter/api/server/migration-tool herunter.

2 Exportieren Sie die Orchestrator-Konfiguration aus einem der Orchestrator-Quellserverknoten.

a Legen Sie die Umgebungsvariable `PATH` fest, wobei Sie den `bin`-Ordner der mit Orchestrator installierten Java-JRE wählen.

b Laden Sie das Migrationstool auf den Windows-Server hoch, auf dem der Quell-Orchestrator installiert ist.

c Entpacken Sie das heruntergeladene Archiv und legen Sie den Ordner im Installationsordner von Orchestrator ab.

Der Standardpfad zum Installationsordner von Orchestrator ist bei einer Installation unter Windows `C:\Programme\VMware\Orchestrator`.

d Führen Sie die Windows-Befehlszeile als Administrator aus und navigieren Sie zum Ordner `bin` im Installationsordner von Orchestrator.

Standardmäßig ist der Pfad zum Ordner `bin` `C:\Programme\VMware\Orchestrator\migration-cli\bin`.

e Führen Sie den Befehl `export` über die Befehlszeile aus.

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

Dieser Befehl fasst die Konfigurationsdateien und Plug-Ins von VMware vRealize Orchestrator zu einem Exportarchiv zusammen.

Das Archiv wird im selben Ordner wie der Ordner `migration-cli` erstellt.

3 Importieren Sie die Konfiguration auf dem Orchestrator-Zielserver.

a Öffnen Sie im Control Center **Konfiguration exportieren/importieren** und klicken Sie auf die Registerkarte **Konfiguration migrieren**.

b Navigieren Sie zur exportierten Konfigurationsdatei und klicken Sie auf **Importieren**.

c Wählen Sie den Typ der zu importierenden Dateien.

Option	Beschreibung
Datenbankeinstellungen migrieren	Verwendet die Datenbank des vRealize Orchestrator 6.x-Clusters.
Plug-Ins migrieren	Migriert alle Plug-Ins, die nicht in der Orchestrator-Plattform enthalten sind.
Legacy-Plug-In-Konfigurationen migrieren	Migriert die Konfiguration der Plug-Ins, die im Ordner *`Orchestrator-Installationsordner`*`\app-server\conf\plugins` gespeichert ist.
Vertrauenswürdige Zertifikate migrieren	Migriert alle Zertifikate aus dem Trust Store des vRealize Orchestrator 6.x-Clusters.

d Klicken Sie auf **Migration beenden**.

Eine Meldung bestätigt, dass die Migration erfolgreich abgeschlossen wurde.

4 Konfigurieren Sie das Orchestrator-Cluster neu.

a Öffnen Sie die Seite für die erweiterte **Verwaltung des Orchestrator-Clusters** unter https://*IP-Adresse_oder_DNS-Name_Ihres_Orchestrator-Servers*:8283/vco-controlcenter/#/control-app/ha?remove-nodes.

b Aktivieren Sie die Kontrollkästchen neben den Orchestrator 6.x-Knoten und klicken Sie auf **Entfernen**.

c Überprüfen Sie auf der Seite **Konfiguration überprüfen** in Control Center, ob Orchestrator ordnungsgemäß konfiguriert ist.

Sie können die Warnung `Orchestrator-Cluster befindet sich im inkonsistenten Zustand` ignorieren. Sie verschwindet, wenn Sie den Orchestrator-Serverdienst starten.

d Wenn ein Lizenzierungsfehler angezeigt wird, konfigurieren Sie einen entsprechenden Anbieter für die Lizenzierung auf der Seite **Lizenzierung** im Control Center.

5 Starten Sie über die Seite **Startoptionen** im Control Center den Orchestrator-Serverdienst des Orchestrator-Zielservers.

a Vergewissern Sie sich, dass auf der Seite **Startoptionen** die Zeichenfolgen **Aktiver Konfigurationsfingerabdruck** und **Ausstehender Konfigurationsfingerabdruck** übereinstimmen.

Hinweis Sie müssen die Seite **Startoptionen** möglicherweise mehrmals aktualisieren, bis die beiden Zeichenfolgen übereinstimmen.

Sie haben erfolgreich ein vRealize Orchestrator 6.x-Cluster zu einem Cluster von virtuellen Orchestrator Appliances der Version 7.1 oder 7.2 migriert.

Weiter

- Melden Sie sich beim Orchestrator-Client an und überprüfen Sie, ob die Konfigurationen aller installierten Plug-Ins korrekt sind.
- Fügen Sie weitere Knoten zum Orchestrator-Zielcluster hinzu. Weitere Informationen finden Sie unter „Konfigurieren eines Orchestrator-Clusters“, auf Seite 52.

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 Skripts 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** in 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

Sie können mithilfe von Control Center ein ZIP-Archiv mit Informationen zur Fehlerbehebung erzeugen, das die Protokolldateien von Konfiguration, Server, Wrapper und Installation enthält.

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

Prüfen der Workflowprotokolle

Sie die können die System- und Serverprotokolle beendeter Workflows rasch prüfen und exportieren, indem Sie die Seite „Workflows überprüfen“ in Control Center aufrufen.

Hinweis Wenn Sie Orchestrator als Bestandteil eines Clusters verwenden, werden die Systemprotokolle nur auf dem Serverknoten gespeichert, auf dem der Workflow gestartet wurde.

Wichtig Protokollinformationen werden vorübergehend gespeichert.

- Systemprotokolle werden in maximal 10 MB großen Dateien gespeichert. Auf jedem Knoten können maximal 5 Protokolldateien gespeichert werden.
- Serverprotokolle verbleiben 15 Tage lang in der Datenbank.

Vorgehensweise

1. Melden Sie sich beim Control Center als **Administrator** an.
2. Klicken Sie auf **Workflows überprüfen**.
3. Klicken Sie auf die Registerkarte **Beendete Workflows**.
4. (Optional) Wählen Sie den Typ der Workflowtoken, die Sie überprüfen möchten, und dann den Datumsbereich und klicken Sie auf **Übernehmen**.
5. (Optional) Sie können anhand des Namens, der ID oder der Token-ID nach einem Workflow suchen.
6. Klicken Sie auf die zu überprüfende Token-ID.

   Die Ansicht für das Ausführungsprotokoll des Workflows wird in Vollbilddarstellung angezeigt.

7 Überprüfen Sie das System- und das Serverprotokoll.

8 (Optional) Klicken Sie auf **Tokenprotokolle exportieren**, um die Workflowtoken-Protokolle in eine `ZIP`-Datei zu exportieren.

Filtern der Orchestrator-Protokolle

Sie können die Orchestrator-Serverprotokolle nach bestimmten Workflowausführungen filtern und Diagnosedaten zur Workflowausführung sammeln.

Die Orchestrator-Protokolle enthalten zahlreiche nützliche Informationen, die Sie in Echtzeit überwachen können. Wenn mehrere Instanzen desselben Workflows gleichzeitig ausgeführt werden, können Sie die einzelnen Workflowausführungen nachverfolgen, indem Sie Diagnosedaten zu jeder Ausführung aus dem Live-Protokoll-Stream von Orchestrator filtern.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** an.

2 Klicken Sie auf **Live-Protokoll-Stream**.

3 Geben Sie die Suchparameter in der Suchleiste ein.

  Sie können Protokolle beispielsweise nach Benutzername, Workflowname, Workflow-ID oder einer Token-ID filtern.

4 (Optional) Wählen Sie **Groß- und Kleinschreibung berücksichtigen** und **Filter (grep)**, um die Suchergebnisse noch weiter zu filtern.

  Durch Auswahl von **Filter (grep)** zeigt der Live-Stream nur noch die Zeilen, die Ihren Suchparametern entsprechen.

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

Weiter

Sie können Tools zur Protokollanalyse von Drittanbietern nutzen, wenn Sie alte Protokolle filtern möchten, die nicht über die Live-Protokoll-Stream-Seite in Control Center verfügbar sind.

Migrieren eines externen Orchestrator-Servers zu vRealize Automation 7.2

8

Sie können einen vorhandenen externen Orchestrator-Server in eine vRealize Orchestrator-Instanz migrieren, die in vRealize Automation eingebettet ist.

Sie können vRealize Orchestrator als externe Serverinstanz bereitstellen und vRealize Automation für die Verwendung mit dieser externen Instanz konfigurieren oder Sie können den vRealize Orchestrator-Server, der in der vRealize Automation Appliance enthalten ist, konfigurieren und verwenden.

Mit der Veröffentlichung von vRealize Automation 7.2 empfiehlt VMware, dass Sie Ihre externe vRealize Orchestrator-Instanz auf den Orchestrator-Server migrieren, der in vRealize Automationintegriert ist. Die Migration von einer externen zu einer eingebetteten Orchestrator-Instanz bietet folgende Vorteile:

- Reduzierung der Gesamtbetriebskosten
- Vereinfachung des Bereitstellungsmodells
- Verbesserung der betrieblichen Effizienz

Hinweis Ziehen Sie in Betracht, die externe vRealize Orchestrator-Instanz in den folgenden Fällen zu verwenden:

- Mehrere Mandanten in der vRealize Automation-Umgebung
- Geografisch verteilte Umgebung
- Bewältigung von Workloads
- Verwendung bestimmter Plug-Ins wie z. B. das Plug-In Site Recovery Manager

Dieses Kapitel behandelt die folgenden Themen:

Migrationsszenarien

Die Migration einer externen vRealize Orchestrator-Instanz auf eine vRealize Automation-Instanz, die in vRealize Orchestrator eingebettet ist, richtet sich nach Ihrer Konfiguration. Es gibt verschiedene Migrationsszenarien basierend darauf, ob der externe Orchestrator-Server Windows-basiert oder eine virtuelle Appliance ist, ob die eingebettete Datenbank oder eine externe Datenbank verwendet wird usw. Sie können den Migrationsprozess mit einem Upgrade von vRealize Orchestrator bzw. vRealize Automation oder beidem kombinieren. In diesem Fall hängt der Migrationsprozess von den Quellversionen der Produkte ab.

Matrix der Migrationsszenarien

Sie können ein Migrationsszenario basierend auf der Quellbereitstellung auswählen.

vRealize Orchestrator-Bereitstellung	vRealize Automation-Bereitstellung	Migrationsszenario
Virtuelle Appli-ancevRealize Orchestrator 6.0.3	vRealize Automation 6.2.3	„Migrieren einer externen virtuellen vRealize Orchestrator 6.x-Appliance unter Windows auf vRealize Automation 7.2“, auf Seite 76
vRealize Orchestrator 6.0.4 unter Windows	vRealize Automation 6.2.4	„Migrieren einer externen vRealize Orchestrator 6.x-Instanz unter Windows auf vRealize Automation 7.2“, auf Seite 74
Virtuelle Appli-ancevRealize Orchestrator 6.0.4	vRealize Automation 6.2.4	„Migrieren einer externen virtuellen vRealize Orchestrator 6.x-Appliance unter Windows auf vRealize Automation 7.2“, auf Seite 76
Virtuelle Appli-ancevRealize Orchestrator 6.0.5	vRealize Automation 6.2.5	„Migrieren einer externen virtuellen vRealize Orchestrator 6.x-Appliance unter Windows auf vRealize Automation 7.2“, auf Seite 76
Virtuelle Appli-ancevRealize Orchestrator 7.0 mit einer externen Oracle 12 c-Datenbank	vRealize Automation 7.0 oder IaaS	„Migrieren einer externen Instanz von vRealize Orchestrator 7.x zu vRealize Automation 7.2“, auf Seite 78
Virtuelle Appliance vRealize Orchestrator 7.0.1 mit einer externen PostgreSQL 9.3.9-Datenbank	vRealize Automation 7.0.1 oder IaaS	„Migrieren einer externen Instanz von vRealize Orchestrator 7.x zu vRealize Automation 7.2“, auf Seite 78
Virtuelle Appliance vRealize Orchestrator 7.1	vRealize Automation 7.1	„Migrieren einer externen Instanz von vRealize Orchestrator 7.x zu vRealize Automation 7.2“, auf Seite 78
Virtuelle Appliance vRealize Orchestrator 7.2	vRealize Automation 7.2	„Migrieren einer externen Instanz von vRealize Orchestrator 7.x zu vRealize Automation 7.2“, auf Seite 78
vRealize Orchestrator 6.0.3 unter Windows	vRealize Automation 6.2.3	„Migrieren der Orchestrator-Konfiguration von Windows auf eine virtuelle Appliance“, auf Seite 65

Migrieren einer externen vRealize Orchestrator 6.x-Instanz unter Windows auf vRealize Automation 7.2

Nach dem Upgrade von vRealize Automation Version 6.x auf Version 7.2 können Sie Ihr vorhandenes externes Orchestrator 6.x, das unter Windows installiert ist, auf den Orchestrator-Server migrieren, der in vRealize Automation 7.2 integriert ist.

Hinweis Wenn Sie eine verteilte vRealize Automation-Umgebung mit mehreren vRealize Automation Appliance-Knoten nutzen, führen Sie den Migrationsvorgang nur auf dem primären vRealize Automation-Knoten aus.

Voraussetzungen

- Aktualisieren Sie vRealize Automation von Version 6.x auf Version 7.2.
- Beenden Sie den Orchestrator-Serverdienst der externen Orchestrator-Instanz.
- Sichern Sie die Datenbank des externen Orchestrator-Servers einschließlich des Datenbankschemas.

Hinweis Wenn Sie vorhaben, bis zur vollständigen Konfiguration der neuen Umgebung die Orchestrator-Quellumgebung zu verwenden, erstellen Sie eine Kopie der Quelldatenbank. Ist dies nicht der Fall, können Sie in der Konfiguration des Orchestrator-Ziels festlegen, dass es dieselbe Datenbank verwendet. Dies führt allerdings dazu, dass die Orchestrator-Quellumgebung nicht mehr funktionsfähig ist, da das Datenbankschema mit der Version des Orchestrator-Ziels aktualisiert wird.

Vorgehensweise

1 Laden Sie das Migrationstool vom Orchestrator-Zielserver herunter.

   a Melden Sie sich bei der vRealize Automation Appliance über SSH als **`root`** an.

   b Laden Sie das Archiv `migration-tool.zip` herunter, das sich im Verzeichnis `/var/lib/vco/downloads` befindet.

2 Exportieren Sie die Orchestrator-Konfiguration vom Orchestrator-Quellserver.

   a Legen Sie die Umgebungsvariable `PATH` fest, wobei Sie den `bin`-Ordner der mit Orchestrator installierten Java-JRE wählen.

   b Laden Sie das Migrationstool auf dem Windows-Server hoch, auf dem der externe Orchestrator-Server installiert ist.

   c Entpacken Sie das heruntergeladene Archiv und legen Sie den Ordner im Installationsordner von Orchestrator ab.

   Der Standardpfad zum Installationsordner von Orchestrator ist bei einer Installation unter Windows `C:\Programme\VMware\Orchestrator`.

   d Führen Sie die Windows-Befehlszeile als Administrator aus und navigieren Sie zum Ordner `bin` im Installationsordner von Orchestrator.

   Standardmäßig ist der Pfad zum Ordner `bin` `C:\Programme\VMware\Orchestrator\migration-cli\bin`.

   e Führen Sie den Befehl `export` über die Befehlszeile aus.

   ```
   C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
   ```

   Dieser Befehl fasst die Konfigurationsdateien und Plug-Ins von VMware vRealize Orchestrator zu einem Exportarchiv zusammen.

   Das Archiv wird im selben Ordner wie der Ordner `migration-cli` erstellt.

3 Migrieren Sie die exportierte Konfiguration auf den Orchestrator-Server, der in vRealize Automation 7.2 integriert ist.

   a Laden Sie die exportierte Konfigurationsdatei in das Verzeichnis `/usr/lib/vco/tools/configuration-cli/bin` von vRealize Automation Appliance hoch.

   b Ändern Sie im Verzeichnis `/usr/lib/vco/tools/configuration-cli/bin` die Zuständigkeit der exportierten Orchestrator-Konfigurationsdatei.

   ```
   chown vco:vco orchestrator-config-export-Orchestrator-IP-Adresse-Datum_Uhrzeit.zip
   ```

   c Importieren Sie die Orchestrator-Konfigurationsdatei in den integrierten vRealize Orchestrator-Server, indem Sie das `vro-configure`-Skript mit dem Befehl `import` ausführen.

   ```
   ./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-Orchestrator-Appliance-IP-Datum_Uhrzeit.zip
   ```

4 Migrieren Sie die Datenbank in die interne PostgreSQL-Datenbank, indem Sie das Skript `vro-configure` mit dem Befehl `db-migrate` ausführen.

   ```
   ./vro-configure.sh db-migrate --sourceJdbcUrl JDBC-Verbindungs-URL --sourceDbUsername Datenbankbenutzer --sourceDbPassword Kennwort_des_Datenbankbenutzers
   ```

   Hinweis Setzen Sie Kennwörter, die Sonderzeichen enthalten, in Anführungszeichen.

   Die *JDBC-Verbindungs-URL* hängt von der Art der Datenbank ab, die Sie verwenden.

   ```
   PostgreSQL: jdbc:postgresql://Host:Port/Datenbankname
   ```

   ```
   MSSQL: jdbc:jtds:sqlserver://Host:Port/Datenbankname\;domain=Domäne
   ```

   ```
   Oracle: jdbc:oracle:thin:@Host:Port:Datenbank
   ```

Damit haben Sie eine externe vRealize Orchestrator 6.x-Instanz unter Windows auf eine vRealize Orchestrator-Instanz migriert, die in vRealize Automation 7.2 eingebettet ist.

Weiter

Richten Sie den integrierten vRealize Orchestrator-Server ein. Siehe Kapitel 9, „Konfigurieren des integrierten vRealize Orchestrator-Servers“, auf Seite 81.

Migrieren einer externen virtuellen vRealize Orchestrator 6.x-Appliance unter Windows auf vRealize Automation 7.2

Nach dem Upgrade von vRealize Automation Version 6.x auf Version 7.2 können Sie Ihre vorhandene externe virtuelle Orchestrator 6.x-Appliance auf den Orchestrator-Server migrieren, der in vRealize Automation 7.2 integriert ist.

Hinweis Wenn Sie eine verteilte vRealize Automation-Umgebung mit mehreren vRealize Automation Appliance-Knoten nutzen, führen Sie den Migrationsvorgang nur auf dem primären vRealize Automation-Knoten aus.

Voraussetzungen

- Aktualisieren Sie vRealize Automation von Version 6.x auf Version 7.2.
- Beenden Sie den Orchestrator Serverdienst und den Control Center-Dienst des externen Orchestrator-Servers.
- Sichern Sie die Datenbank des externen Orchestrator-Servers einschließlich des Datenbankschemas.

Vorgehensweise

1 Laden Sie das Migrationstool vom Orchestrator-Zielserver auf den Orchestrator-Quellserver.

   a Melden Sie sich bei der virtuellen Appliance vRealize Orchestrator 6.x über SSH als **root** an.

   b Führen Sie im Verzeichnis `/var/lib/vco` den Befehl `scp`aus, um das Archiv `migration-tool.zip` herunterzuladen.

   ```
   scp root@vra-va-Hostname.Domäne.Name:/var/lib/vco/downloads/migration-tool.zip ./
   ```

   c Führen Sie den Befehl `unzip` zum Extrahieren des Archivs mit den Migrationstools aus.

   ```
   unzip migration-tool.zip
   ```

2 Exportieren Sie die Orchestrator-Konfiguration vom Orchestrator-Quellserver.

   a Führen Sie im Verzeichnis `/var/lib/vco/migration-cli/bin` den Befehl `export` aus.

   ```
   ./vro-migrate.sh export
   ```

   Dieser Befehl fasst die Konfigurationsdateien und Plug-Ins von VMware vRealize Orchestrator zu einem Exportarchiv zusammen.

   Im Ordner `/var/lib/vco` wird ein Archiv mit dem Dateinamen `orchestrator-config-export-`*`Orchestrator-IP-Adresse-Datum_Uhrzeit`*`.zip` erstellt.

3 Migrieren Sie die exportierte Konfiguration auf den Orchestrator-Server, der in vRealize Automation 7.2 integriert ist.

   a Melden Sie sich bei der vRealize Automation Appliance über SSH als **root** an.

   b Führen Sie im Verzeichnis `/usr/lib/vco/tools/configuration-cli/bin` den Befehl `scp` aus, um das exportierte Konfigurationsarchiv herunterzuladen.

   ```
   scp root@Orchestrator-IP_oder_DNS-Name:/var/lib/vco/orchestrator-config-export-Orchestrator-IP-Adresse-Datum_Uhrzeit.zip ./
   ```

   c Ändern Sie den Besitzer der exportierten Orchestrator-Konfigurationsdatei.

   ```
   chown vco:vco orchestrator-config-export-Orchestrator-IP-Adresse-Datum_Uhrzeit.zip
   ```

   d Beenden Sie den Orchestrator-Serverdienst und den Control Center-Dienst des integrierten vRealize Orchestrator-Servers.

   ```
   service vco-server stop && service vco-configurator stop
   ```

   e Importieren Sie die Orchestrator-Konfigurationsdatei in den integrierten vRealize Orchestrator-Server, indem Sie das `vro-configure`-Skript mit dem Befehl `import` ausführen.

   ```
   ./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSsl-Certificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-Orchestrator-Appliance-IP-Datum_Uhrzeit.zip
   ```

4 Wenn der externe Orchestrator-Server, von dem aus Sie migrieren möchten, die integrierte PostgreSQL-Datenbank verwendet, bearbeiten Sie die Datenbankkonfigurationsdateien.

   a Heben Sie in der Datei `storage/db/pgsql/data/postgresql.conf` die Kommentierung der Zeile `listen_addresses` auf.

   b Legen Sie als Werte für `listen_addresses` Platzhalter (*) fest.

   ```
   listen_addresses ='*'
   ```

c Fügen Sie der Datei `/storage/db/pgsql/data/pg_hba.conf` eine Zeile hinzu.

```
host all all vra-va-Hostname.Domäne.Name/32 md5
```

Hinweis Die Datei `pg_hba.conf` erfordert die Verwendung eines CIDR-Präfixformats anstelle einer IP-Adresse und Subnetzmaske.

d Starten Sie den PostgreSQL-Serverdienst neu.

```
service postgresql restart
```

5 Migrieren Sie die Datenbank in die interne PostgreSQL-Datenbank, indem Sie das Skript `vro-configure` mit dem Befehl `db-migrate` ausführen.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC-Verbindungs-URL --sourceDbUsername Datenbankbenutzer --sourceDbPassword Kennwort_des_Datenbankbenutzers
```

Hinweis Setzen Sie Kennwörter, die Sonderzeichen enthalten, in Anführungszeichen.

Die *JDBC-Verbindungs-URL* hängt von der Art der Datenbank ab, die Sie verwenden.

```
PostgreSQL: jdbc:postgresql://Host:Port/Datenbankname
```

```
MSSQL: jdbc:jtds:sqlserver://Host:Port/Datenbankname\;domain=Domäne
```

```
Oracle: jdbc:oracle:thin:@Host:Port:Datenbank
```

6 Setzen Sie das System auf die Standardkonfiguration der Datei `postgresql.conf` und `pg_hba.conf` zurück.

a Starten Sie den PostgreSQL-Serverdienst neu.

Damit haben Sie eine externe virtuelle vRealize Orchestrator 6.x-Appliance unter Windows auf eine vRealize Orchestrator-Instanz migriert, die in vRealize Automation 7.2 eingebettet ist.

Weiter

Richten Sie den integrierten vRealize Orchestrator-Server ein. Siehe Kapitel 9, „Konfigurieren des integrierten vRealize Orchestrator-Servers“, auf Seite 81.

Migrieren einer externen Instanz von vRealize Orchestrator 7.x zu vRealize Automation 7.2

Sie können die Konfiguration aus Ihrer bestehenden externen Orchestrator-Instanz exportieren und sie in den in vRealize Automation integrierten Orchestrator-Server importieren.

Hinweis Wenn Sie mehrere vRealize Automation Appliance-Knoten nutzen, führen Sie den Migrationsvorgang nur auf dem primären vRealize Automation-Knoten aus.

Voraussetzungen

- Aktualisieren Sie vRealize Automation von Version 6.x auf Version 7.2.
- Beenden Sie den Orchestrator-Serverdienst der externen Orchestrator-Instanz.
- Sichern Sie die Datenbank des externen Orchestrator-Servers einschließlich des Datenbankschemas.

Vorgehensweise

1 Exportieren Sie die Konfiguration aus dem externen Orchestrator-Server.

   a Melden Sie sich beim Control Center des externen Orchestrator-Servers als **root** an.

   b Beenden Sie den Orchestrator-Serverdienst über die Seite **Startoptionen**, um unerwünschte Änderungen an der Datenbank zu vermeiden.

   c Wechseln Sie zur Seite **Konfiguration exportieren/importieren**.

   d Wählen Sie auf der Seite **Konfiguration exportieren** die Optionen **Serverkonfiguration exportieren**, **Paket-Plug-Ins** und **Plug-In-Konfigurationen exportieren**.

2 Migrieren Sie die exportierte Konfiguration in die eingebettete Orchestrator-Instanz.

   a Laden Sie die exportierte Orchestrator-Konfigurationsdatei in das Verzeichnis `/usr/lib/vco/tools/configuration-cli/bin` von vRealize Automation Appliance hoch.

   b Melden Sie sich bei der vRealize Automation Appliance über SSH als **root** an.

   c Beenden Sie den Orchestrator-Serverdienst und den Control Center-Dienst des integrierten vRealize Orchestrator-Servers.

   ```
   service vco-server stop && service vco-configurator stop
   ```

   d Navigieren Sie zum Verzeichnis `/usr/lib/vco/tools/configuration-cli/bin`.

   e Ändern Sie den Besitzer der exportierten Orchestrator-Konfigurationsdatei.

   ```
   chown vco:vco orchestrator-config-export-Orchestrator-Appliance-IP-Datum_Uhrzeit.zip
   ```

   f Importieren Sie die Orchestrator-Konfigurationsdatei in den integrierten vRealize Orchestrator-Server, indem Sie das `vro-configure`-Skript mit dem Befehl `import` ausführen.

   ```
   ./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSsl-Certificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-Orchestrator-Appliance-IP-Datum_Uhrzeit.zip
   ```

3 Migrieren Sie die Datenbank in die interne PostgreSQL-Datenbank, indem Sie das Skript `vro-configure` mit dem Befehl `db-migrate` ausführen.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC-Verbindungs-URL --sourceDbUsername Datenbankbenutzer --sourceDbPassword Kennwort_des_Datenbankbenutzers
```

Hinweis Setzen Sie Kennwörter, die Sonderzeichen enthalten, in Anführungszeichen.

Die *JDBC-Verbindungs-URL* hängt von der Art der Datenbank ab, die Sie verwenden.

```
PostgreSQL: jdbc:postgresql://Host:Port/Datenbankname
```

```
MSSQL: jdbc:jtds:sqlserver://Host:Port/Datenbankname\;domain=Domäne
```

```
Oracle: jdbc:oracle:thin:@Host:Port:Datenbank
```

Damit haben Sie eine externe Orchestrator-Serverinstanz in eine vRealize Orchestrator-Instanz migriert, die in vRealize Automation eingebettet ist.

Weiter

Richten Sie den integrierten vRealize Orchestrator-Server ein. Siehe Kapitel 9, „Konfigurieren des integrierten vRealize Orchestrator-Servers“, auf Seite 81.

Konfigurieren des integrierten vRealize Orchestrator -Servers

9

Nachdem Sie die Konfiguration eines externen Orchestrator-Servers exportiert und in vRealize Automation 7.2 importiert haben, müssen Sie den Orchestrator-Server konfigurieren, der in vRealize Automation integriert ist.

Voraussetzungen

Migrieren Sie die Konfiguration vom externen auf den internen vRealize Orchestrator-Server.

Vorgehensweise

1 Melden Sie sich bei der vRealize Automation Appliance über SSH als **root** an.

2 Starten Sie den Control Center-Dienst des integrierten vRealize Orchestrator-Servers.

```
service vco-configurator start
```

3 Melden Sie sich beim Control Center des integrierten Orchestrator-Servers als **root** an.

Hinweis Wenn Sie von einer externen vRealize Orchestrator 7.2-Instanz migrieren, fahren Sie mit Schritt 8 fort.

4 Wechseln Sie zur Seite für die erweiterte Orchestrator-Verwaltung unter https://*vra-va-Hostname.Domäne.Name*:8283/vco-controlcenter/#/?advanced.

   a Aktualisieren Sie die Browserseite, indem Sie auf die Taste F5 auf der Tastatur drücken.

5 Klicken Sie auf der Seite **Datenbank konfigurieren** auf **Speichern**.

Hinweis Wenn die Schaltfläche **Speichern** nicht aktiv ist, klicken Sie auf **Datenbank aktualisieren** und anschließend auf **Speichern**.

6 Überprüfen Sie auf der Seite **Konfiguration überprüfen** in Control Center, ob Orchestrator ordnungsgemäß konfiguriert ist.

7 Wählen Sie auf der Seite **Lizenzierung** die Option **vRA-Lizenz** aus dem Dropdown-Menü **Lizenzanbieter wählen** aus.

8 Wenn der externe Orchestrator-Server für den Clustermodus konfiguriert wurde, konfigurieren Sie den Orchestrator-Cluster in vRealize Automation neu.

   a Rufen Sie die Seite für die erweiterte **Verwaltung des Orchestrator-Clusters** unter https://*vra-va-Hostname.Domäne.Name*:8283/vco-controlcenter/#/control-app/ha?advanced&remove-nodes auf.

   Hinweis Wenn die Kontrollkästchen zum **Entfernen** neben den bestehenden Knoten im Cluster nicht angezeigt werden, müssen Sie die Browserseite aktualisieren, indem Sie auf der Tastatur die Funktionstaste F5 drücken.

   b Ändern Sie auf der Seite **Orchestrator-Knoteneinstellungen** die **Anzahl der aktiven Knoten** in `10`.

   c Wenn Sie externe Orchestrator-Knoten aus dem Cluster entfernen möchten, aktivieren Sie die Kontrollkästchen neben diesen Knoten und klicken Sie auf **Entfernen**.

   d Wenn Sie die Seite für die erweiterte Verwaltung des Clusters verlassen möchten, entfernen Sie die Zeichenfolge `&remove-nodes` aus der URL und aktualisieren Sie die Browserseite mit der Funktionstaste F5 auf der Tastatur.

   e Prüfen Sie auf der Seite **Konfiguration überprüfen** im Control Center, ob Orchestrator ordnungsgemäß konfiguriert ist.

9 (Optional) Generieren Sie in der Registerkarte **Paketsignaturzertifikat** auf der Seite **Zertifikate** ein neues Paketsignaturzertifikat.

10 (Optional) Ändern Sie die Werte für **Standardmandant** und **Admin-Gruppe** auf der Seite **Anbieter für Authentifizierung konfigurieren**.

11 Starten Sie über die Seite **Startoptionen** den Orchestrator-Serverdienst des integrierten Orchestrator-Servers in vRealize Automation.

12 Stellen Sie sicher, dass der Dienst `vco-server` in der Registerkarte **Dienste** in der Managementkonsole der vRealize Automation Appliance als REGISTRIERT angezeigt wird.

13 Wählen Sie die `vco`-Dienste des externen Orchestrator-Servers aus und klicken Sie auf **Registrierung aufheben**.

Weiter

- Importieren Sie alle vertrauenswürdigen Zertifikate aus dem externen Orchestrator-Server in den Trust Store des integrierten Orchestrator-Servers. Weitere Informationen finden Sie unter „Verwalten von Orchestrator-Zertifikaten“, auf Seite 47.
- Fügen Sie die vRealize Automation-Replikatknoten zum vRealize Automation-Cluster hinzu, um die Orchestrator-Konfiguration zu synchronisieren.
- Aktualisieren Sie den vRealize Orchestrator-Endpoint, um auf den migrierten integrierten Orchestrator-Server zu verweisen.
- Fügen Sie den vRealize Automation-Host und den IaaS-Host zur Bestandsliste des vRealize Automation-Plug-Ins hinzu, indem Sie die Workflows „Einen vRA-Host hinzufügen“ und „Den IaaS-Host eines vRA-Hosts hinzufügen“ ausführen.

Anwendungsfälle für Konfiguration und Fehlerbehebung 10

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 behandelt die folgenden Themen:

Registrieren von Orchestrator als vCenter Server -Erweiterung

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

Vorgehensweise

1. Melden Sie sich beim Orchestrator-Client als Administrator an.
2. Klicken Sie auf die Ansicht **Workflows**.
3. Erweitern Sie in der hierarchischen Liste der Workflows **Bibliothek > vCenter > Konfiguration**.
4. Klicken Sie mit der rechten Maustaste auf den Workflow **vCenter Orchestrator als vCenter Server-Erweiterung registrieren** und wählen Sie **Workflow starten**.
5. Wählen Sie die vCenter Server-Instanz aus, bei der Orchestrator registriert werden soll.
6. Geben Sie https://*Ihre_Orchestrator_Server_IP_oder_DNS-Name*:8281 oder die Dienst-URL des Lastausgleichsdienstes ein, der die Anforderungen an die Orchestrator-Serverknoten weiterleitet.
7. Klicken Sie auf **Senden**.

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.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** 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**.

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 Zertifikatfehler 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 Zertifikatfehler wird rechts in der Adressleiste von Internet Explorer angezeigt.

3 Klicken Sie auf den Zertifikatfehler 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 Zertifikatfehler 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.

Vorgehensweise

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-lighttp restart
```

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

Abbrechen laufender Workflows

Brechen Sie Workflows nur ab, nachdem der Orchestrator-Server angehalten wurde. Andernfalls kann der Vorgang fehlschlagen.

Voraussetzungen

Halten Sie den Orchestrator-Server über die Seite **Startoptionen** im Control Center an.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** 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 alle Token des Workflows abzubrechen. Wenn der Server nicht angehalten wird, werden die Workflowtoken möglicherweise nicht abgebrochen.
Workflow-Ausführungen nach ID abbrechen	Geben Sie alle Token-IDs ein, die Sie abbrechen möchten. Trennen Sie diese durch ein Komma. Wenn der Server nicht angehalten wird, werden die Workflowtoken möglicherweise nicht abgebrochen.
Alle Tokens abbrechen	Alle auf dem Server laufenden Workflows werden abgebrochen. Sie müssen den Server anhalten, um diese Option zu verwenden.

Beim nächsten Start des Servers werden die Workflows auf den Status „Abgebrochen“ gesetzt.

Weiter

Überprüfen Sie auf der Seite **Workflows überprüfen** von Control Center, ob alle Workflows abgebrochen wurden.

Aktivieren von Orchestrator-Server-Debugging

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

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** 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**.

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

Sichern von Orchestrator-Konfiguration und -Elementen

Sie können einen Snapshot Ihrer Orchestrator-Konfiguration anfertigen und diese Konfiguration in eine neue Instanz von Orchestrator importieren, um die Konfiguration zu sichern. Sie können auch Orchestrator-Elemente sichern, die Sie geändert haben.

Wenn Sie Standardworkflows, Aktionen, Richtlinien oder Konfigurationselemente bearbeiten und dann ein Paket mit diesen Elementen mit einer höheren Orchestrator-Version importieren, gehen Ihre Änderungen an den Elementen verloren. Um geänderte und benutzerdefinierte Elemente nach einem Upgrade zu behalten, müssen Sie diese vor dem Upgrade in ein Paket exportieren.

Jede Orchestrator-Serverinstanz hat ein eigenes Zertifikat, und jede vCenter Server-Plug-In-Instanz hat eine eigene ID. Die Zertifikate und die eindeutige ID definieren die Identität von Orchestrator-Server und vCenter Server-Plug-In. Wenn Sie die Orchestrator-Elemente nicht sichern oder die Orchestrator-Konfiguration nicht zur Sicherung exportieren, sollten Sie unbedingt diese Kennungen ändern.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** an.

2 Klicken Sie auf **Konfiguration exportieren/importieren**.

3 Wählen Sie den Typ der zu exportierenden Dateien aus.

4 (Optional) Geben Sie ein Kennwort ein, um die Konfigurationsdatei zu schützen.

   Verwenden Sie das gleiche Kennwort beim Import der Konfiguration.

5 Klicken Sie auf **Exportieren**.

6 Melden Sie sich bei der Orchestrator-Clientanwendung an.

7 Erstellen Sie ein Paket, das alle von Ihnen erstellten oder bearbeiteten Orchestrator-Elemente enthält.

   a Klicken Sie auf die Ansicht **Pakete**.

   b Klicken Sie auf die Menüschaltfläche in der Titelleiste der Paketliste und wählen Sie **Paket hinzufügen**.

   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 auf der Registerkarte **Workflows** die Workflows zum Paket hinzu.

   g (Optional) Fügen Sie Richtlinienvorlagen, Aktionen, Konfigurationselemente, Ressourcenelemente und Plug-Ins zum Paket hinzu.

8 Exportieren Sie das Paket.

   a Klicken Sie mit der rechten Maustaste auf das zu exportierende Paket und wählen Sie **Paket exportieren**.

   b Wählen Sie den gewünschten Speicherort für das Paket aus und klicken Sie auf **Öffnen**.

   c (Optional) Verwenden Sie das zugehörige Zertifikat zum Signieren des Pakets.

   d (Optional) Richten Sie Einschränkungen für das exportierte Paket ein.

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.

f Klicken Sie auf **Speichern**.

9 Importieren Sie die Orchestrator-Konfiguration in die neue Orchestrator-Serverinstanz.

a Melden Sie sich beim Control Center der neuen Orchestrator-Instanz als **Administrator** 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 Klicken Sie auf **Importieren**.

10 Importieren Sie das Paket, das Sie in die neue Orchestrator-Instanz exportiert haben.

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 Ansicht **Pakete**.

d Klicken Sie mit der rechten Maustaste im linken Fensterbereich und wählen Sie **Paket importieren**.

e Navigieren Sie zu dem Paket, das Sie importieren möchten, 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 das importierte Paketelement eine höher Version aufweist als der Server, wird das Element vom System zum Importieren ausgewählt.

g Heben Sie die Auswahl von Elementen auf, die Sie nicht importieren möchten.

Heben Sie beispielsweise die Auswahl benutzerdefinierter Elemente auf, für die höhere Versionen vorhanden sind.

h (Optional) Entfernen Sie die Markierung des Kontrollkästchens **Werte der Konfigurationseinstellungen importieren**, wenn die Attributwerte der Konfigurationseinstellungen 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 überschrieben.
Tags nicht importieren	Es werden keine Tags aus dem Paket importiert.

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

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“, auf Seite 46. 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.

Vorgehensweise

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.

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

Weiter

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“, auf Seite 89.
- 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.

Vorgehensweise

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.

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

Weiter

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.

Vorgehensweise

1 Wählen Sie im vSphere Web Client eine virtuelle Maschine aus, auf der vSphere Replication aktiviert werden soll, und klicken Sie auf **Aktionen > Alle vSphere Replication-Aktionen > Replizierung konfigurieren**.

2 Wählen Sie im Fenster Replizierungstyp die Option **Replizierung auf einen vCenter-Server** aus und klicken Sie auf **Weiter**.

3 Wählen Sie im Fenster Ziel-Site das vCenter für die Wiederherstellungs-Site aus und klicken Sie auf **Weiter**.

4 Wählen Sie im Fenster Replizierungsserver einen vSphere Replication Server aus und klicken Sie auf **Weiter**.

5 Klicken Sie im Fenster Zielspeicherort auf **Bearbeiten**, wählen Sie den Zieldatenspeicher, in dem die replizierten Dateien gespeichert werden sollen, und klicken Sie auf **Weiter**.

6 Lassen Sie die Standardwerte im Fenster Replizierungsoptionen unverändert und klicken Sie auf **Weiter**.

7 Geben Sie im Fenster Wiederherstellungseinstellungen die Zeit für **Recovery Point Objektive (RPO)** und **Zeitpunkt-Instanzen** ein und klicken Sie auf **Weiter**.

8 Überprüfen Sie die Einstellungen im Fenster Bereit zum Abschließen und klicken Sie dann auf **Fertig stellen**.

9 Wiederholen Sie diese Schritte für alle virtuellen Maschinen, auf denen vSphere Replication aktiviert sein muss.

Erstellen von Schutzgruppen

Sie können Schutzgruppen erstellen, damit Site Recovery Manager 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

Vorgehensweise

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.

- 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.

Vorgehensweise

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.

Vorgehensweise

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.

Vorgehensweise

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.

11 Festlegen von Systemeigenschaften

Sie können mit Systemeigenschaften das Standardverhalten von Orchestrator ändern.

Dieses Kapitel behandelt die folgenden Themen:

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.

Vorgehensweise

1. Melden Sie sich beim Control Center als **Administrator** 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.

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 für die Gewährung des Schreibzugriffs auf das Orchestrator-System

Die Datei `js-io-rights.conf` enthält Regeln, die Schreibzugriff auf definierte Verzeichnisse im Dateisystem des Servers gewähren.

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 (`-`), das anzeigt, ob Rechte gewährt oder verweigert werden
- Die Ebene der Rechte: Lesen (`r`), Schreiben (`w`) und Ausführen (`x`)
- Den Pfad, auf den die Rechte angewendet werden sollen

Standardinhalte der Datei js-io-rights.conf

Die Konfigurationsdatei `js-io-rights.conf` in der Orchestrator Appliance enthält standardmäßig die folgenden Inhalte:

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

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

`-rwx /`	Jeglicher Zugriff auf das Dateisystem wird verweigert.
`+rwx /var/run/vco`	Für das Verzeichnis `/var/run/vco` werden Lese-, Schreib- und Ausführungsrechte gewährt.

Regeln in der Datei js-io-rights.conf

Orchestrator löst Zugriffsrechte in der Reihenfolge auf, in der sie in der Datei `js-io-rights.conf` angegeben sind. Jede Zeile kann die vorhergehenden Zeilen außer Kraft setzen.

Wichtig Sie können den Zugriff auf alle Teile des Dateisystems gewähren, indem Sie `+rwx /` in der Datei `js-io-rights.conf` festlegen. Dies bringt jedoch ein hohes Sicherheitsrisiko mit sich.

Festlegen des Dateisystemzugriffs auf dem Server für Workflows und Aktionen

Um die Bereiche des Serverdateisystems zu ändern, auf die Workflows und die 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 Orchestrator-Servers zuzugreifen.

Vorgehensweise

1 Melden Sie sich bei der Orchestrator Appliance-Linux-Konsole als **`root`** an.

2 Navigieren Sie zu `/etc/vco/app-server`.

3 Öffnen Sie die Konfigurationsdatei `js-io-rights.conf` in einem Texteditor.

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

   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.

Sie haben die Zugriffsrechte auf das Dateisystem für Workflows und für die 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.

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** 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.

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`.

Setzten 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.

Vorgehensweise

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 **Administrator** 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.

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
```

Vorgehensweise

1 Melden Sie sich beim Control Center als **Administrator** 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.

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

12 Weitere Schritte

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.

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.

Vorgehensweise

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 Domänennamen 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.

Wenn Sie vRealize Automation, vCenter Single Sign-On oder einen anderen Verzeichnisdienst als Authentifizierungsmethode verwenden, geben Sie die entsprechenden Anmeldedaten ein, um sich beim Orchestrator-Client anzumelden.

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*.

Weiter

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

Index

U

V

W

Z