

Mandantenfähigkeit in vRealize Orchestrator

vRealize Orchestrator 7.5



vmware®

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

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

Die VMware-Website enthält auch die neuesten Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

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

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

Inhalt

- 1 Mandantenfähigkeit in VMware vRealize Orchestrator 4**
 - [Mandantenfähigkeit in vRealize Orchestrator – Überblick 4](#)
- 2 Aktivieren der Mandantenfähigkeit in vRealize Orchestrator 5**
 - [Aktivieren der vRealize Orchestrator -Mandantenfähigkeit 5](#)
- 3 Mandantenisolierung in vRealize Orchestrator 6**
 - [Isolierung von Zugriffsrechten in einer mandantenfähigen Orchestrator-Umgebung 7](#)
- 4 Vergleich der Orchestrator-Bereitstellung mit einem und mit mehreren Mandanten 9**
- 5 Verwalten älterer benutzerdefinierter Inhalte 10**
 - [Isolieren älterer benutzerdefinierter Inhalte 10](#)

Mandantenfähigkeit in VMware vRealize Orchestrator

1

Mandantenfähigkeit in VMware vRealize Orchestrator enthält allgemeine Informationen zu der in VMware® vRealize Orchestrator 7.4 eingeführten mandantenfähigen Architektur.

Zielgruppe

Diese Informationen richten sich an vRealize Automation-Systemadministratoren, Mandantenadministratoren und Orchestrator-Administratoren.

Mandantenfähigkeit in vRealize Orchestrator – Überblick

vRealize Orchestrator 7.4 führt eine mandantenfähige Architektur ein, in der sich mehrere vRealize Automation-Mandanten eine einzige externe oder eingebettete vRealize Automation-Instanz teilen können.

Ein Mandant ist eine Organisationseinheit in einer vRealize Automation-Bereitstellung. vRealize Orchestrator 7.4 führt eine mandantenfähige Architektur ein, in der sich mehrere vRealize Automation-Mandanten eine einzige externe oder eingebettete vRealize Orchestration-Instanz teilen können. Dies ist die vRealize Automation-Instanz, die Orchestrator als Authentifizierungsanbieter verwendet. Weitere Informationen zur Mandantenfähigkeit in vRealize Automation finden Sie unter *Mandantenfähigkeit und Benutzerrollen in Vorbereiten und Verwenden von Dienst-Blueprints in vRealize Automation*.

Die Funktion für die Mandantenfähigkeit in vRealize Automation ist standardmäßig deaktiviert, um die Abwärtskompatibilität zu gewährleisten und da die Aktivierung das Benutzererlebnis wesentlich verändert. Wenn Sie die Mandantenfähigkeit in vRealize Orchestrator aktivieren, können Sie sie im Anschluss nicht mehr ohne weiteres deaktivieren.

Hinweis Die vRealize Automation-Authentifizierung wird nur unterstützt, wenn die Mandantenfähigkeit aktiviert ist.

Aktivieren der Mandantenfähigkeit in vRealize Orchestrator

2

Sie können die Mandantenfähigkeit nur dann aktivieren, wenn Orchestrator so konfiguriert ist, dass vRealize Automation als Authentifizierungsanbieter verwendet wird. Mandantenfähigkeit ist standardmäßig deaktiviert.

Aktivieren der vRealize Orchestrator -Mandantenfähigkeit

Neue vRealize Orchestrator-Installationen sind für die Ausführung in einem Modus mit einem Mandanten konfiguriert. Wenn Sie Orchestrator in einem Modus mit mehreren Mandanten ausführen möchten, müssen Sie diesen Modus explizit aktivieren.

Hinweis Das Aktivieren der Mandantenfähigkeit ist eine Änderung, die nicht rückgängig gemacht werden kann. Aktivieren Sie die Funktion nicht, wenn Sie ihren Zweck nicht kennen.

Verfahren

- 1 Melden Sie sich bei der Orchestrator Appliance-Linux-Konsole als Root-Benutzer an.
- 2 Beenden Sie den Orchestrator-Serverdienst und den Control Center-Dienst.

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

- 3 Navigieren Sie zum Verzeichnis `/var/lib/vco/tools/configuration-cli/bin`.

```
cd /var/lib/vco/tools/configuration-cli/bin
```

- 4 Um die Funktion der Mandantenfähigkeit zu aktivieren, führen Sie das Skript `vro-configure.sh` aus.

```
./vro-configure.sh enable-multi-tenancy
```

- 5 Starten Sie den Orchestrator-Serverdienst und den Control Center-Dienst.

```
service vco-server start && service vco-configurator start
```

Sie haben die Mandantenfähigkeit in vRealize Orchestrator erfolgreich aktiviert.

Mandantenisolierung in vRealize Orchestrator

3

Die Funktion für die Mandantenfähigkeit von Orchestrator bietet ein gewisses Maß an Isolierung zwischen Mandanten.

Nach der Aktivierung der Mandantenfähigkeit werden die von Orchestrator verwalteten Objekte in einen System-Geltungsbereich und einen mandantenspezifischen Geltungsbereich unterteilt. Zu diesen Objekten zählen Workflows, Aktionen, Pakete, Konfigurationen, Kategorien, Richtlinien, Richtlinienvorlagen, Aufgaben, Workflow-Ausführungen und mehr.

System-Geltungsbereich

Der System-Geltungsbereich ist der semantische Bereich, der all die Orchestrator-Inhalte enthält, die von allen Mandanten gemeinsam genutzt werden. Der Systeminhalt umfasst die folgenden Elemente:

- Alle in den Orchestrator-Standard-Plug-Ins enthaltenen Objekte
- Vor Aktivierung der Mandantenfähigkeit erstellte benutzerdefinierte Objekte
- Vom vRealize Automation-Systemadministrator erstellte Objekte
- Vordefinierte Automatisierungsinhalte (Workflows, Aktionen und sonstige Elemente), die vom Systemmandanten verwaltet werden und für das Lesen und Aufrufen allen systemfremden Mandanten zur Verfügung gestellt werden

Mandanten haben nur Lesezugriff auf diese Inhalte und können keine Objekte des System-Geltungsbereichs erstellen, ändern oder löschen.

Mandantenspezifischer Geltungsbereich

Mandantenspezifische Objekte sind mit dem Mandanten verknüpft, der sie erstellt hat. Zu diesen Objekten zählen Workflows, Aktionen, Richtlinien, Richtlinienvorlagen, Ressourcen usw. Mandanten können selbst erstellte Inhalte bearbeiten oder löschen. Sie können Systeminhalte und ihre eigenen mandantenspezifischen Inhalte ausführen und anzeigen.

Mandanten können Objekte des System-Geltungsbereichs oder von anderen erstellte Objekte nicht anzeigen, bearbeiten oder löschen.

Orchestrator-Plug-Ins in einer Umgebung mit mehreren Mandanten

vRealize Orchestrator 7.4 unterstützt die Mandantenfähigkeit der Orchestrator-Plug-ins und der Objekte des Plug-In-Bestands nicht. Objekte aus dem Plug-In-Bestand gehören zum System-Geltungsbereich.

Hinweis Objekte wie z. B. Endpoints und Bestandselemente, die Sie erstellen, indem Sie Workflows aus der Plug-in-Bibliothek ausführen, sind sichtbar, und alle Mandanten können darauf zugreifen.

Ressourcenzuteilung

Die Ressourcen des Orchestrator-Servers wie z. B. CPU, Arbeitsspeicher, Speicher, Netzwerkbandbreite, Datenbankspeicherplatz, maximale Anzahl der ausgeführten Workflows und Threadpools werden von allen Mandanten gemeinsam genutzt. Wenn einer der Mandanten den Grenzwert der zugeteilten Ressourcen erreicht, sind davon auch alle anderen Mandanten betroffen, die die gleiche Orchestrator-Instanz verwenden.

Sicherheit

Die Sicherheitsisolierung zwischen Mandanten in vRealize Orchestrator 7.4 verwendet die Benutzerrollen Systemadministrator und Mandantenadministrator, die in vRealize Automation definiert sind. Weitere Informationen zu Benutzerrollen in vRealize Automation finden Sie unter *Übersicht über Benutzerrollen in Vorbereiten und Verwenden von Dienst-Blueprints in vRealize Automation*.

Hinweis Der vRealize Automation-Systemadministrator muss Mitglied der Orchestrator-Administratorengruppe sein, die Sie in das Textfeld **Admin-Gruppe** eingeben, wenn Sie den Authentifizierungsanbieter im Control Center konfigurieren.

Benutzerberechtigungen, die vom Orchestrator-Client konfiguriert werden, entsprechen nicht den vRealize Automation-Benutzerrollen. Sie müssen sie explizit für einen bestimmten Benutzer oder eine Gruppe konfigurieren. Weitere Informationen zu Benutzerberechtigungseinstellungen finden Sie unter *Verwenden des VMware vRealize Orchestrator-Clients*.

Isolierung von Zugriffsrechten in einer mandantenfähigen Orchestrator-Umgebung

Wenn die Mandantenfähigkeit aktiviert ist, haben der Systemadministrator und die Mandantenbenutzer unterschiedliche Rechte zum Bearbeiten von Objekten in Orchestrator. Diese Berechtigungen hängen davon ab, ob die Objekte zum System-Geltungsbereich oder zum mandantenspezifischen Geltungsbereich gehören.

Tabelle 3-1. Isolierung zwischen Mandanten

Rolle	Systeminhalt	Inhalte von Mandant A	Inhalte von Mandant B
Systemadministrator	<ul style="list-style-type: none"> ■ Erstellen, Anzeigen, Bearbeiten, Löschen und Wiederherstellen von Objekten des System-Geltungsbereichs ■ Ausführen von System-Workflows ■ Überwachen der vom Systemadministrator gestarteten Workflow-Ausführungen 	<p>Hinweis Wenn ein Systemadministrator in seinem Konto nicht auch gleichzeitig Administrator eines der vorhandenen Mandanten ist, kann er nicht auf mandantenspezifische Inhalte zugreifen oder diese bearbeiten.</p>	
Administrator von Mandant A	<ul style="list-style-type: none"> ■ Anzeigen von Systeminhalten ■ Ausführen von System-Workflows ■ Überwachen von System-Workflows, die von einem beliebigen Benutzer von Mandant A gestartet wurden 	<ul style="list-style-type: none"> ■ Erstellen, Anzeigen, Bearbeiten, Löschen und Wiederherstellen von Objekten, die zu Mandant A gehören ■ Ausführen von Workflows für Mandant A ■ Überwachen der Workflow-Ausführungen für Mandant A, die von einem beliebigen Benutzer von Mandant A gestartet wurden 	Benutzer von Mandant A können nicht auf Objekte zugreifen, die von Benutzern von Mandant B erstellt wurden, mit Ausnahme der Ressourcen, die Benutzer von Mandant B erstellen, indem sie Workflows aus der Plug-In-Bibliothek ausführen.
Administrator von Mandant B	<ul style="list-style-type: none"> ■ Anzeigen von Systeminhalten ■ Ausführen von System-Workflows ■ Überwachen von System-Workflows, die von einem beliebigen Benutzer von Mandant B gestartet wurden 	Benutzer von Mandant B können nicht auf Objekte zugreifen, die von Benutzern von Mandant A erstellt wurden, mit Ausnahme der Ressourcen, die Benutzer von Mandant A erstellen, indem sie Workflows aus der Plug-In-Bibliothek ausführen.	<ul style="list-style-type: none"> ■ Erstellen, Anzeigen, Bearbeiten, Löschen und Wiederherstellen von Objekten, die zu Mandant B gehören ■ Ausführen von Workflows für Mandant B ■ Überwachen der Workflow-Ausführungen für Mandant B, die von einem beliebigen Benutzer von Mandant B gestartet wurden
Lösungsb Benutzer	<ul style="list-style-type: none"> ■ Erstellen, Anzeigen, Bearbeiten, Löschen und Wiederherstellen von Objekten des System-Geltungsbereichs ■ Ausführen von System-Workflows 	<ul style="list-style-type: none"> ■ Erstellen, Anzeigen, Bearbeiten, Löschen und Wiederherstellen von Objekten, die zu Mandant A gehören ■ Ausführen von Workflows für Mandant A 	<ul style="list-style-type: none"> ■ Erstellen, Anzeigen, Bearbeiten, Löschen und Wiederherstellen von Objekten, die zu Mandant B gehören ■ Ausführen von Workflows für Mandant B

Vergleich der Orchestrator-Bereitstellung mit einem und mit mehreren Mandanten

4

Seit Version 7.4 kann in Orchestrator je nach den geschäftlichen Anforderungen zwischen einem Modus mit einem Mandanten oder einem Modus mit mehreren Mandanten gewählt werden.

Einmandantenbereitstellung

Wenn die Mandantenfähigkeit nicht aktiviert ist, läuft Orchestrator im Modus mit einem Mandanten. Dies bedeutet, dass alle Objekte, die die Orchestrator-Inhalte und -Laufzeit bilden, von allen Benutzern gemeinsam genutzt werden. Sie legen verschiedene Berechtigungsebenen für ein Objekt fest, um den Zugriff verschiedener Benutzer oder Benutzergruppen auf dieses Objekt zu begrenzen. Weitere Informationen zu Benutzerberechtigungseinstellungen finden Sie unter *Verwenden des VMware vRealize Orchestrator-Clients*.

Mehrmandantenbereitstellung

Wenn die Mandantenfähigkeit aktiviert ist, sind die mandantenspezifischen Objekte in Orchestrator zwischen den vRealize Automation-Mandanten und von den Objekten des System-Geltungsbereichs isoliert. Mandantenbenutzer können die mandantenspezifischen Inhalte anzeigen, indem sie sich im Orchestrator-Client mit ihrem Benutzernamen, ihrem Kennwort und ihrer Mandanten-ID anmelden.

Hinweis Die Objekte aus der Plug-In-Bestandsliste sind nicht mehrmandantenfähig. Diese Objekte sind Teil des Systembereichs.

Verwalten älterer benutzerdefinierter Inhalte

5

Nachdem Sie die Mandantenfähigkeit in vRealize Orchestrator aktiviert haben, werden alle vorhandenen Objekte zu Objekten des System-Geltungsbereichs.

Ähnlich wie die Objekte und Ressourcen, die in der Orchestrator-Plattform vorkonfiguriert enthalten sind, werden die benutzerdefinierten Objekte, die Sie vor der Aktivierung der Mandantenfähigkeit erstellt haben, unter allen Mandanten im schreibgeschützten Modus geteilt und können nur vom Systemadministrator geändert oder gelöscht werden.

Isolieren älterer benutzerdefinierter Inhalte

Wenn Sie vermeiden möchten, dass die benutzerdefinierten Inhalte zu Inhalten des System-Geltungsbereichs werden, können Sie die benutzerdefinierten Objekte und Ressourcen als Paket exportieren und sie vom Orchestrator-Server löschen, bevor Sie die Mandantenfähigkeit aktivieren. Nach der Aktivierung der Mandantenfähigkeit können Sie diese Objekte in einen bestimmten Mandanten oder in mehrere Mandanten importieren.

Hinweis Sie können dasselbe Paket unabhängig in mehrere Mandanten importieren. Sie können kein Paket, das zum System-Geltungsbereich gehört, in einen Mandanten importieren und Sie können kein Paket mit mandantenspezifischen Inhalten in den System-Geltungsbereich importieren.

Voraussetzungen

Stellen Sie sicher, dass die Mandantenfähigkeit auf Ihrem vRealize Orchestrator 7.4 nicht aktiviert ist.

Verfahren

- 1 Melden Sie sich beim Orchestrator-Client als Administrator an.
- 2 Erstellen Sie ein Paket für den Export.
Siehe [Erstellen eines Pakets](#).
- 3 Exportieren Sie das Paket.
Siehe [Exportieren eines Pakets](#).
- 4 Löschen Sie das exportierte Paket vom Orchestrator-Server.
Siehe [Entfernen eines Pakets](#).

5 Aktivieren Sie die Mandantenfähigkeit.

Siehe [Aktivieren der vRealize Orchestrator-Mandantenfähigkeit](#).

6 Melden Sie sich beim Orchestrator-Client als Mandantenadministrator an, um das Paket in einen bestimmten Mandanten zu importieren.

7 Importieren Sie das Paket.

Siehe [Importieren eines Pakets](#).