

# Konfigurieren von vRealize Automation

vRealize Automation 7.1



vmware®

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

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

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

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://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](http://www.vmware.com/de)

# Inhalt

Konfigurieren von vRealize Automation 7

Aktualisierte Informationen 8

## 1 Externe Vorbereitungen für die Bereitstellung 9

- Vorbereiten Ihrer Umgebung für die Verwaltung durch vRealize Automation 9
  - Checkliste für das Vorbereiten der NSX -Netzwerk- und -Sicherheitskonfiguration 11
  - Checkliste zum Vorbereiten der Unterstützung eines externen IPAM-Anbieters 14
  - Vorbereiten Ihrer vCloud Director -Umgebung für vRealize Automation 17
  - Vorbereiten Ihrer vCloud Air -Umgebung für vRealize Automation 17
  - Vorbereiten Ihrer Amazon AWS -Umgebung 18
  - Vorbereiten von Netzwerk- und Sicherheitsfunktionen für Red Hat OpenStack 24
  - Vorbereiten Ihrer SCVMM -Umgebung 25
- Vorbereiten für Maschinenbereitstellung 25
  - Auswählen einer vorzubereitenden Methode zur Maschinenbereitstellung 26
  - Checkliste für die Ausführung von Visual Basic-Skripts während der Bereitstellung 29
  - Verwenden des vRealize Automation -Gast-Agent bei der Bereitstellung 31
  - Checkliste für das Vorbereiten für die Bereitstellung durch Klonen 39
  - Vorbereiten für die vCloud Air - und vCloud Director -Bereitstellung 55
  - Vorbereiten für die Linux Kickstart-Bereitstellung 56
  - Vorbereiten für SCCM -Bereitstellung 59
  - Vorbereiten für die WIM-Bereitstellung 60
  - Vorbereiten für die Image-Bereitstellung der virtuellen Maschine 71
  - Vorbereiten für die Bereitstellung von Amazon-System-Images 71
  - Szenario: Vorbereiten von vSphere -Ressourcen für Maschinenbereitstellung in Rainpole 74
- Vorbereiten für Software -Bereitstellung 77
  - Vorbereiten der Bereitstellung von Maschinen mit Software 78
  - Szenario: Vorbereiten einer vSphere CentOS-Vorlage für Klonmaschinen- und Softwarekomponenten-Blueprints 83
  - Szenario: Vorbereiten auf den Import des vSphere -Beispielanwendungs-Blueprints „Dukes Bank“ 87

## 2 Konfigurieren der Mandanteneinstellungen 93

- Auswählen der Verzeichnisverwaltungs-Konfigurationsoptionen 94
  - Verzeichnisverwaltung – Übersicht 95
  - Konfigurieren der Verzeichnisverwaltung zum Erstellen eines Active Directory-Links 99
  - Verwalten von Benutzerattributen, die aus Active Directory synchronisieren 114
  - Verwalten von Konnektoren 115

Hinzufügen einer Konnektormaschine zu einer Domäne	116
Informationen über die Auswahl von Domänencontrollern	117
Verwalten von Zugriffsrichtlinien	121
Integrieren alternativer Benutzerauthentifizierungsprodukte in die Verzeichnisverwaltung	127
Szenario: Konfigurieren eines Active Directory-Links für hochverfügbare vRealize Automation -Bereitstellung	150
Konfigurieren der Smartcard-Authentifizierung für vRealize Automation	152
Generieren eines Konnektor-Aktivierungstokens	154
Bereitstellen der Connector-OVA-Datei	154
Konfigurieren der Connector-Einstellungen	156
Anwenden einer öffentlichen Zertifizierungsstelle	157
Erstellen eines Arbeitsbereichs-Identitätsanbieter	159
Konfigurieren der Zertifikatauthentifizierung und Konfigurieren der Regeln für Standardzugriffsrichtlinien	159
Erstellen eines Links für Active Directory mit mehreren Domänen oder mit mehreren Gesamtstrukturen	160
Konfigurieren von Gruppen und Benutzerrollen	163
Zuweisen von Rollen zu Directory-Benutzern oder -Gruppen Rollen zuweisen	163
Erstellen einer benutzerdefinierten Gruppe	164
Erstellen einer Business-Gruppe	165
Fehlerbehebung bei Leistungsbeeinträchtigungen bei der Anzeige von Gruppenmitgliedern	168
Szenario: Konfigurieren des Standardmandanten für Rainpole	168
Szenario: Erstellen von lokalen Benutzerkonten für Rainpole	169
Szenario: Verbinden des Active Directory Ihres Unternehmens mit vRealize Automation für Rainpole	170
Szenario: Konfigurieren von Branding für den Standardmandanten für Rainpole	172
Szenario: Erstellen einer benutzerdefinierten Gruppe für Ihre Rainpole-Architekten	173
Szenario: Zuweisen von IaaS-Administratorrechten zu Ihrer benutzerdefinierten Gruppe von Rainpole-Architekten	174
Erstellen weiterer Mandanten	174
Angaben von Mandanteninformationen	175
Konfigurieren von lokalen Benutzern	176
Ernennen von Administratoren	176
Löschen eines Mandanten	177
Konfigurieren des benutzerdefinierten Brandings	178
Benutzerdefiniertes Branding für die Anmeldeseite des Mandanten	178
Benutzerdefiniertes Branding für Mandantenanwendungen	179
Checkliste für die Konfiguration von Benachrichtigungen	180
Konfigurieren globaler E-Mail-Server für Benachrichtigungen	183
Hinzufügen eines mandantenspezifischen Postausgangsservers	185
Hinzufügen eines mandantenspezifischen Posteingangsservers	186
Überschreiben eines Standard-Ausgangs-E-Mail-Servers des Systems	187

Überschreiben eines Standard-Eingangs-E-Mail-Servers des Systems	188
Zurücksetzen von Systemstandard-E-Mail-Servern	189
Konfigurieren der Benachrichtigungen	190
Anpassen des Datums für E-Mail-Benachrichtigungen wegen des Ablaufs von Maschinen	190
Konfigurieren von Vorlagen für automatische IaaS-E-Mails	191
Abonnieren von Benachrichtigungen	191
Erstellen einer benutzerdefinierten RDP-Datei zur Unterstützung von RDP-Verbindungen für bereitgestellte Maschinen	192
Szenario: Hinzufügen von Datacenter-Standorten für regionsübergreifende Bereitstellungen	192
Konfigurieren von vRealize Orchestrator und Plug-ins	193
Konfigurieren des standardmäßigen Workflow-Ordners für einen Mandanten	194
Konfigurieren eines externen vRealize Orchestrator -Servers	195
Anmelden bei der Konfigurationsschnittstelle von vRealize Orchestrator	196
Anmelden beim vRealize Orchestrator -Client	197

### 3 Konfigurieren von Ressourcen 199

Checkliste für die Konfiguration von IaaS-Ressourcen	199
Speichern von Benutzeranmeldedaten	200
Auswählen eines Endpoint-Szenarios	202
Erstellen einer Fabric-Gruppe	222
Konfigurieren von Maschinenpräfixen	222
Verwalten von Schlüsselpaaren	223
Erstellen eines Netzwerkprofils	225
Konfigurieren von Reservierungen und Reservierungsrichtlinien	243
Szenario: Konfigurieren von IaaS-Ressourcen für Rainpole	285
Szenario: Anwenden eines Standorts auf eine Computing-Ressource für regionsübergreifende Bereitstellungen	290
Checkliste für die Implementierung einer vRealize Automation -Bereitstellung mithilfe eines externen IPAM-Anbieters.	291
Konfigurieren von XaaS -Ressourcen	292
Konfigurieren des Active Directory-Plug-Ins als Endpoint	292
Konfigurieren des HTTP-REST-Plug-Ins als Endpoint	294
Konfigurieren des PowerShell-Plug-ins als Endpoint	296
Konfigurieren des SOAP-Plug-Ins als Endpoint	297
Konfigurieren des vCenter Server -Plug-ins als Endpoint	299
Installieren zusätzlicher Plug-Ins auf dem vRealize Orchestrator -Standardserver	301
Arbeiten mit Active Directory-Richtlinien	301
Erstellen und Anwenden von Active Directory-Richtlinien	302

### 4 Bereitstellen von bedarfsgesteuerten Diensten für Benutzer 306

Entwerfen von Blueprints	306
--------------------------	-----

Exportieren und Importieren von Blueprints	308
Szenario: Importieren der vSphere -Beispielanwendung „Dukes Bank“ und Konfigurieren für Ihre Umgebung	309
Szenario: Testen der Beispielanwendung „Dukes Bank“	313
Erstellen Ihrer Design-Bibliothek	315
Entwerfen von Maschinen-Blueprints	317
Entwerfen von Maschinen-Blueprints mit NSX -Netzwerk und -Sicherheit	361
Entwerfen von Software -Komponenten	379
Erstellen von XaaS -Blueprints und -Ressourcenaktionen	399
Veröffentlichen eines Blueprints	454
Erstellen zusammengesetzter Blueprints	455
Grundlegendes zum Verhalten von verschachtelten Blueprints	457
Auswählen einer Maschinenkomponente, die Software komponenten unterstützt	460
Erstellen von Eigenschaftsbindungen zwischen Blueprint-Komponenten	461
Erstellen expliziter Abhängigkeiten und Steuern der Bereitstellungsreihenfolge	462
Szenario: Zusammenfügen und Testen eines Blueprints zur Bereitstellung von MySQL auf Rainpole-verknüpften Klon-Maschinen	463
Verwalten des Servicekatalogs	467
Checkliste für die Konfiguration des Servicekatalogs	468
Erstellen eines Diensts	469
Arbeiten mit Katalogelementen und Aktionen	472
Erstellen von Berechtigungen	475
Arbeiten mit Genehmigungsrichtlinien	483
Szenario: Konfigurieren des Katalogs für Rainpole-Architekten zum Testen von Blueprints	506
Szenario: Testen der Rainpole-CentOS-Maschine	509
Szenario: Den Anwendungs-Blueprint vom Typ „CentOS mit MySQL“ im Servicekatalog verfügbar machen	511
Szenario: Erstellen und Anwenden von CentOS with MySQL-Genehmigungsrichtlinien	515

# Konfigurieren von vRealize Automation

*Konfigurieren von vRealize Automation* enthält Informationen zum Konfigurieren von vRealize Automation und Ihren externen Umgebungen, um Vorbereitungen für die Bereitstellung und das Katalogmanagement von vRealize Automation zu treffen.

Informationen zu unterstützten Integrationen finden Sie unter <https://www.vmware.com/pdf/vrealize-automation-71-support-matrix.pdf>.

## Zielgruppe

Diese Informationen sind für IT-Experten bestimmt, die für die Konfiguration der vRealize Automation-Umgebung zuständig sind, sowie für Infrastrukturadministratoren, die für die Vorbereitung von Komponenten in ihrer bestehenden Infrastruktur für die Verwendung bei der Bereitstellung von vRealize Automation zuständig sind. Diese Informationen wurden für erfahrene Windows- und Linux-Systemadministratoren verfasst, die mit der Technologie virtueller Maschinen und den Vorgängen von Datacentern vertraut sind.

## VMware Technical Publications – Glossar

VMware Technical Publications enthält ein Glossar mit Begriffen, die Ihnen möglicherweise unbekannt sind. Definitionen von Begriffen, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter <http://www.vmware.com/support/pubs>.

# Aktualisierte Informationen

*Konfigurieren von vRealize Automation* wird mit jeder Produktversion oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf für *Konfigurieren von vRealize Automation*.

Revision	Beschreibung
DE-002076-04	<ul style="list-style-type: none"><li>■ <a href="#">Installieren des Gast-Agents auf einer Windows-Referenzmaschine</a> wurde aktualisiert.</li><li>■ <a href="#">Vorbereiten einer Windows-Referenzmaschine für die Unterstützung von Software</a> wurde aktualisiert.</li><li>■ <a href="#">Vorbereiten einer Linux-Referenzmaschine für die Unterstützung von Software</a> wurde aktualisiert.</li><li>■ <a href="#">Erstellen einer Active Directory-Richtlinie</a> wurde aktualisiert.</li></ul>
DE-002076-03	<a href="#">Angaben von Mandanteninformationen</a> wurde ein Hinweis hinzugefügt, der angibt, dass in Mandanten-URLs nur Kleinbuchstaben zulässig sind.
DE-002076-02	<ul style="list-style-type: none"><li>■ <a href="#">Vorbereiten für die vCloud Air- und vCloud Director-Bereitstellung</a> wurde aktualisiert.</li><li>■ <a href="#">Erstellen eines vCloud Director-Endpoints</a> wurde aktualisiert.</li><li>■ <a href="#">Exportieren und Importieren von Blueprints</a> wurde aktualisiert.</li><li>■ <a href="#">vSphere-Maschinenkomponenteneinstellungen</a> wurde aktualisiert.</li></ul>
DE-002076-01	<ul style="list-style-type: none"><li>■ <a href="#">Löschen eines Mandanten</a> wurde hinzugefügt.</li><li>■ <a href="#">Einstellungen für Amazon-Maschinenkomponenten</a> wurde aktualisiert.</li><li>■ <a href="#">Fehlerbehebung bei Blueprints für Klone und verknüpfte Klone</a> wurde aktualisiert.</li></ul>
DE-002076-00	Erste 7.1-Version.



# Externe Vorbereitungen für die Bereitstellung

1

Möglicherweise müssen Sie einige Elemente außerhalb von vRealize Automation erstellen oder vorbereiten, um die Bereitstellung von Katalogelementen zu unterstützen. Wenn Sie beispielsweise ein Katalogelement für die Bereitstellung einer Klonmaschine zur Verfügung stellen möchten, müssen Sie eine Vorlage auf Ihrem Hypervisor erstellen, von der Sie klonen können.



Dieses Kapitel behandelt die folgenden Themen:

- [Vorbereiten Ihrer Umgebung für die Verwaltung durch vRealize Automation](#)
- [Vorbereiten für Maschinenbereitstellung](#)
- [Vorbereiten für Software-Bereitstellung](#)





## Vorbereiten Ihrer Umgebung für die Verwaltung durch vRealize Automation

Abhängig von Ihrer Integrationsplattform müssen Sie möglicherweise einige Konfigurationsänderungen vornehmen, bevor Sie Ihre Umgebung der Verwaltung durch vRealize Automation unterstellen oder bestimmte Funktionen nutzen können.

**Tabelle 1-1. Vorbereiten Ihrer Umgebung für die Integration von vRealize Automation**

Umgebung	Vorbereitungen
 NSX	Wenn Sie NSX nutzen möchten, um Netzwerk- und Sicherheitsfunktionen von mit vRealize Automation bereitgestellten Maschinen verwalten zu können, bereiten Sie Ihre NSX-Instanz für die Integration vor. Siehe <a href="#">Checkliste für das Vorbereiten der NSX-Netzwerk- und -Sicherheitskonfiguration</a> .
 vCloud Director	Installieren und konfigurieren Sie Ihre vCloud Director-Instanz, richten Sie Ihre vSphere- und Cloud-Ressourcen ein und legen Sie entsprechende Anmeldedaten fest bzw. erstellen Sie diese, um vRealize Automation den Zugriff auf Ihre vCloud Director-Umgebung zu gewähren. Siehe <a href="#">Vorbereiten Ihrer vCloud Director-Umgebung für vRealize Automation</a> .

**Tabelle 1-1. Vorbereiten Ihrer Umgebung für die Integration von vRealize Automation (Fortsetzung)**

Umgebung	Vorbereitungen
 vCloud Air	Registrieren Sie sich für das vCloud Air-Konto, richten Sie Ihre vCloud Air-Umgebung ein und legen Sie entsprechende Anmeldedaten fest bzw. erstellen Sie diese, um vRealize Automation den Zugriff auf Ihre Umgebung zu gewähren. Siehe <a href="#">Vorbereiten für die vCloud Air- und vCloud Director-Bereitstellung</a> .
 Amazon AWS	Bereiten Sie Elemente und Benutzerrollen in der Amazon AWS-Umgebung für die Verwendung in vRealize Automation vor und begreifen Sie, wie Amazon AWS-Funktionen vRealize Automation-Funktionen zugeordnet werden. Siehe <a href="#">Vorbereiten Ihrer Amazon AWS-Umgebung</a> .
 Red Hat OpenStack	Wenn Sie Red Hat OpenStack nutzen möchten, um Netzwerk- und Sicherheitsfunktionen von mit vRealize Automation bereitgestellten Maschinen verwalten zu können, bereiten Sie Ihre Red Hat OpenStack-Instanz für die Integration vor. Siehe <a href="#">Vorbereiten von Netzwerk- und Sicherheitsfunktionen für Red Hat OpenStack</a> .
 SCVMM	Konfigurieren Sie den Speicher und das Netzwerk und machen Sie sich mit den Einschränkungen bei der Namensgebung von Vorlagen- und Hardwareprofilen vertraut. Siehe <a href="#">Vorbereiten Ihrer SCVMM-Umgebung</a> .
Externe IPAM-Anbieter	Registrieren Sie ein externes IPAM-Anbieterpaket oder Plug-In, führen Sie die Konfigurationsworkflows aus und registrieren Sie die IPAM-Lösung als neuen vRealize Automation-Endpoint. Siehe <a href="#">Checkliste zum Vorbereiten der Unterstützung eines externen IPAM-Anbieters</a> .
Alle übrigen Umgebungen	Sie müssen keine Änderungen an Ihrer Umgebung vornehmen. Sie können mit der Vorbereitung der Maschinenbereitstellung beginnen, indem Sie Vorlagen, Startumgebungen oder Maschinen-Images erstellen. Siehe <a href="#">Vorbereiten für Maschinenbereitstellung</a> .

## Checkliste für das Vorbereiten der NSX -Netzwerk- und -Sicherheitskonfiguration

Sie können die Optionen für NSX-Netzwerk und -Sicherheit in vRealize Automation erst dann verwenden, wenn Sie die externe NSX-Netzwerk- und -Sicherheitsumgebung konfiguriert haben, die Sie verwenden möchten.

Ein Großteil des vRealize Automation-Supports für die Netzwerk- und Sicherheitskonfiguration, die Sie in Blueprints und Reservierungen angeben, wird extern konfiguriert und für vRealize Automation zur Verfügung gestellt, nachdem die Datenerfassung auf den Computing-Ressourcen ausgeführt wurde.

Weitere Informationen zu den verfügbaren Netzwerk- und Konfigurationsoptionen, die Sie für vRealize Automation konfigurieren können, finden Sie unter [Konfigurieren der Einstellungen für Netzwerk- und Sicherheitskomponenten](#).

**Tabelle 1-2. Checkliste zum Vorbereiten von NSX -Netzwerk und -Sicherheit**

Aufgabe	Speicherort	Details
<input type="checkbox"/> Installieren und konfigurieren Sie das NSX-Plug-In.	Installieren Sie das NSX-Plug-In in vRealize Orchestrator.	Einzelheiten finden Sie unter <a href="#">Installieren des NSX-Plug-Ins auf vRealize Orchestrator</a> und im <i>NSX-Administratorhandbuch</i> .
<input type="checkbox"/> Konfigurieren Sie NSX-Netzwerkeinstellungen, einschließlich Einstellungen für Gateway und Transportzone.	Konfigurieren Sie Netzwerkeinstellungen in NSX.	Informationen dazu finden Sie im <i>NSX-Administratorhandbuch</i> .
<input type="checkbox"/> Erstellen Sie NSX-Sicherheitsrichtlinien-, -Tags und -Gruppen.	Konfigurieren Sie Sicherheitseinstellungen in NSX.	Informationen dazu finden Sie im <i>NSX-Administratorhandbuch</i> .
<input type="checkbox"/> Konfigurieren Sie NSX-Lastausgleichsdienst-Einstellungen.	Konfigurieren Sie einen NSX-Lastausgleichsdienst für vRealize Automation.	Informationen dazu finden Sie im <i>NSX-Administratorhandbuch</i> . Weitere Informationen finden Sie auch unter „Benutzerdefinierte Eigenschaften für Netzwerke“ in <i>Referenz für benutzerdefinierte Eigenschaften</i> .

## Installieren des NSX -Plug-Ins auf vRealize Orchestrator

Um das NSX-Plug-In zu installieren, müssen Sie die vRealize Orchestrator-Installationsdatei herunterladen, mit der vRealize Orchestrator-Konfigurationsschnittstelle die Plug-In-Datei hochladen und das Plug-In auf einem vRealize Orchestrator-Server installieren.

---

**Hinweis** Wenn Sie eine eingebettete vRealize Orchestrator-Instanz verwenden, die ein installiertes NSX-Plug-In enthält, müssen Sie die folgenden Plug-In-Installationsschritte nicht durchführen, da das NSX-Plug-In bereits installiert ist.

---

Allgemeine Informationen zum Plug-In-Update und zur Fehlerbehebung finden Sie in der vRealize Orchestrator-Dokumentation unter [https://www.vmware.com/support/pubs/orchestrator\\_pubs.html](https://www.vmware.com/support/pubs/orchestrator_pubs.html).

### Voraussetzungen

- Stellen Sie sicher, dass Sie eine unterstützte vRealize Orchestrator-Instanz ausführen.  
Informationen zum Einrichten von vRealize Orchestrator finden Sie unter *Installieren und Konfigurieren von VMware vRealize Orchestrator*.
- Stellen Sie sicher, dass Sie über Anmeldedaten für ein Konto mit der Berechtigung zum Installieren von vRealize Orchestrator-Plug-Ins und zum Authentifizieren durch vCenter Single Sign-On verfügen.
- Stellen Sie sicher, dass Sie die richtige Version des NSX-Plug-Ins installiert haben. Siehe *Übersicht über die Unterstützung von vRealize Automation*.
- Stellen Sie sicher, dass Sie den vRealize Orchestrator-Client installiert haben und dass Sie sich mit Administratoranmeldedaten anmelden können.

### Vorgehensweise

- 1 Laden Sie die Plug-In-Datei in einen Speicherort herunter, der vom vRealize Orchestrator-Server aus erreichbar ist.  
  
Das Namensformat der Plug-In-Installationsdatei, mit entsprechenden Versionswerten, ist `o11nplug-in-nsx-1.n.n.vmoapp`. Plug-In-Installationsdateien für das Netzwerk- und Sicherheitsprodukt NSX sind über die Downloadwebsite für VMware-Produkte unter <http://vmware.com/web/vmware/downloads> verfügbar.
- 2 Öffnen Sie einen Browser und starten Sie die vRealize Orchestrator-Konfigurationsschnittstelle.  
Ein Beispiel des URL-Formats ist `https://orchestrator_server.com:8283`.
- 3 Klicken Sie auf **Plug-Ins** im linken Fensterbereich und scrollen Sie nach unten in den Bereich für das Installieren des neuen Plug-Ins.
- 4 Browsen Sie im Textfeld **Plug-In-Datei** zur Plug-In-Installationsdatei und klicken Sie auf **Hochladen und installieren**.  
  
Die Datei muss das `.vmoapp`-Format aufweisen.

- 5 Bei Eingabeaufforderung akzeptieren Sie die Lizenzvereinbarung im Bereich für das Installieren eines Plug-Ins.
- 6 Bestätigen Sie im Abschnitt für den Installationsstatus der aktivierten Plug-Ins, dass der richtige NSX-Plug-In-Name angegeben ist.

Versionsinformationen finden Sie unter *Übersicht über die Unterstützung von vRealize Automation*.

Der Status Plug-in wird beim nächsten Serverstart installiert wird angezeigt.

- 7 Starten Sie den vRealize Orchestrator-Server-Dienst neu.
- 8 Starten Sie die vRealize Orchestrator-Konfigurationsschnittstelle neu.
- 9 Klicken Sie auf **Plug-Ins** und stellen Sie sicher, dass sich der Status zu Installation OK geändert hat.
- 10 Starten Sie die vRealize Orchestrator-Client-Anwendung und navigieren Sie mit der Registerkarte **Workflow** durch die Bibliothek zum Ordner NSX.

Sie können die Workflows durchsuchen, die das NSX-Plug-In bereitstellt.

#### Weiter

Erstellen Sie einen vRealize Orchestrator-Endpoint in vRealize Automation, um ihn zum Ausführen von Workflows zu verwenden. Siehe [Erstellen eines vRealize Orchestrator-Endpoints](#).

## Ausführen eines vRealize Orchestrator - und NSX -Sicherheitsworkflows

Vor der Verwendung der NSX-Sicherheitsrichtlinienfunktionen von vRealize Automation muss ein Administrator den Workflow Enable security policy support for overlapping subnets in vRealize Orchestrator ausführen.

Der Workflow für die Unterstützung der Sicherheitsrichtlinie für überlappende Subnetze ist anwendbar auf NSX-Endpoints der Version 6.1 und höher. Führen Sie diesen Workflow nur einmal aus, um die Unterstützung zu aktivieren.

#### Voraussetzungen

- Stellen Sie sicher, dass ein vSphere-Endpoint mit einem NSX-Endpoint registriert ist. Siehe [Erstellen eines vSphere-Endpoints](#).
- Melden Sie sich beim vRealize Orchestrator-Client als Administrator an.
- Vergewissern Sie sich, dass Sie den vRO-Workflow Create NSX endpoint ausgeführt haben.

#### Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Workflow** und wählen Sie **NSX > NSX-Workflows für VCAC** aus.
- 2 Führen Sie den Workflow **NSX-Endpoint erstellen** aus und beantworten Sie die Eingabeaufforderungen.
- 3 Führen Sie den Workflow **Unterstützung der Sicherheitsrichtlinie für überlappende Subnetze** aus.

#### 4 Wählen Sie den NSX-Endpoint als Eingabeparameter für den Workflow aus.

Verwenden Sie die IP-Adresse, die Sie beim Erstellen des vSphere-Endpoints angegeben haben, um eine NSX-Instanz zu registrieren.

Nachdem Sie diesen Workflow ausgeführt haben, werden die in der Sicherheitsrichtlinie definierten Distributed Firewall-Regeln nur auf die virtuellen Netzwerkkarten (vNICs) der Sicherheitsgruppenmitglieder angewendet, auf die diese Sicherheitsrichtlinie angewendet wird.

#### Weiter

Wenden Sie die entsprechenden Sicherheitsfunktionen für den Blueprint an.

## Checkliste zum Vorbereiten der Unterstützung eines externen IPAM-Anbieters

Sie können IP-Adressen und -Bereiche für die Verwendung in einer Netzwerkprofildefinition von einem unterstützten externen IPAM-Anbieter wie z. B. Infoblox beziehen.

Vor der Verwendung eines externen IPAM-Anbieter-Endpoints in einem vRealize Automation-Netzwerkprofil müssen Sie ein vRealize Orchestrator-IPAM-Anbieterpaket herunterladen oder anderweitig beziehen, das Paket importieren und erforderliche Workflows in vRealize Orchestrator ausführen sowie die IPAM-Lösung als vRealize Automation-Endpoint in vRealize Orchestrator registrieren.

Eine Übersicht über den Vorgang zum Bereitstellen eines möglichen IP-Adressbereichs mithilfe eines externen IPAM-Anbieters finden Sie unter [Checkliste für die Implementierung einer vRealize Automation-Bereitstellung mithilfe eines externen IPAM-Anbieters..](#)

**Tabelle 1-3. Checkliste zum Vorbereiten der Unterstützung eines externen IPAM-Anbieters**

Aufgabe	Speicherort	Details
<input type="checkbox"/> Unterstütztes vRealize Orchestrator-Plug-In für den externen IPAM-Anbieter beziehen und importieren.	Laden Sie das IPAM-Anbieterpaket (z. B. Infoblox IPAM) vom VMware Solution Exchange herunter und importieren Sie das Paket in vRealize Orchestrator.  Wenn VMware Solution Exchange ( <a href="https://solutionexchange.vmware.com/store/category_groups/cloud-management">https://solutionexchange.vmware.com/store/category_groups/cloud-management</a> ) das benötigte IPAM-Anbieterpaket nicht enthält, können Sie mithilfe des SDKs des IPAM-Lösungsanbieters und der zugehörigen Dokumentation Ihr eigenes Paket erstellen.	Siehe <a href="#">Abrufen und Importieren des externen IPAM-Anbieterpakets in vRealize Orchestrator</a> .
<input type="checkbox"/> Die erforderlichen Konfigurationsworkflows ausführen und die externe IPAM-Lösung als vRealize Automation-Endpoint registrieren.	Führen Sie die vRealize Orchestrator-Konfigurationsworkflows aus und registrieren Sie den Endpoint-Typ des IPAM-Anbieters in vRealize Orchestrator.	Siehe <a href="#">Ausführen des Workflows zum Registrieren des Infoblox-IPAM-Endpoint-Typs in vRealize Orchestrator</a> .

## Abrufen und Importieren des externen IPAM-Anbieterpakets in vRealize Orchestrator

Um die Definition und Verwendung eines Endpoints für den externen IPAM-Anbieter vorzubereiten, müssen Sie zunächst das externe IPAM-Anbieterpaket abrufen und das Paket in vRealize Orchestrator importieren.

Sie können ein vorhandenes Drittanbieterpaket für das IP-Adressmanagement herunterladen und verwenden, wie beispielsweise Infoblox IPAM. Darüber hinaus können Sie mithilfe eines von VMware bereitgestellten SDK und der SDK-Begleitdokumentation Ihr eigenes Paket erstellen, beispielsweise ein Paket für die Verwendung mit Bluecat IPAM. In diesem Beispiel wird das IPAM-Paket Infoblox verwendet.

Nachdem Sie das externe IPAM-Anbieterpaket abgerufen und in vRealize Orchestrator importiert haben, führen Sie die erforderlichen Workflows aus und registrieren Sie den IPAM-Endpoint-Typ.

Weitere Informationen zum Importieren von Paketen und zum Ausführen von vRealize Orchestrator-Workflows finden Sie unter *Verwenden des VMware vRealize Orchestrator-Clients*. Weitere Informationen zum Erweitern von vRealize Automation mit vRealize Orchestrator-Paketen und -Workflows finden Sie unter *Lebenszyklus-Erweiterbarkeit*.

### Voraussetzungen

- Melden Sie sich bei vRealize Orchestrator mit Administratorrechten an, um ein vRealize Orchestrator-Paket zu importieren, konfigurieren und registrieren.

### Vorgehensweise

- 1 Öffnen Sie die VMware Solution Exchange-Website unter [https://solutionexchange.vmware.com/store/category\\_groups/cloud-management](https://solutionexchange.vmware.com/store/category_groups/cloud-management).
- 2 Wählen Sie **Cloud Management Marketplace** aus.
- 3 Suchen Sie das gewünschte Plug-In oder Paket und laden Sie es herunter, wie beispielsweise Infoblox VIPAM Plug-in.
- 4 Klicken Sie in vRealize Orchestrator auf die Registerkarte **Administrator** und klicken Sie auf **Paket importieren**.
- 5 Wählen Sie das Paket oder Plug-In aus, beispielsweise das Infoblox IPAM-Plug-In.
- 6 Wählen Sie alle Workflows und Artefakte aus und klicken Sie auf **Ausgewählte Elemente importieren**.

### Weiter

[Ausführen des Workflows zum Registrieren des Infoblox-IPAM-Endpoint-Typs in vRealize Orchestrator.](#)

## Ausführen des Workflows zum Registrieren des Infoblox-IPAM-Endpoint-Typs in vRealize Orchestrator

Führen Sie den Registrierungsworkflow in vRealize Orchestrator aus, um für die vRealize Automation die Verwendung des externen IPAM-Anbieters zu unterstützen und den Infoblox-IPAM-Endpoint-Typ für die Verwendung in vRealize Automation zu registrieren.

Für die Registrierung von IPAM-Endpoint-Typen in vRealize Orchestrator werden Sie zur Eingabe von vRA-Administratoranmeldedaten für vRealize Automation aufgefordert. T

Weitere Informationen zum Importieren von Paketen und zum Ausführen von vRealize Orchestrator-Workflows finden Sie unter *Verwenden des VMware vRealize Orchestrator-Clients*. Weitere Informationen zum Erweitern von vRealize Automation mit vRealize Orchestrator-Paketen und -Workflows finden Sie unter *Lebenszyklus-Erweiterbarkeit*.

### Voraussetzungen

- [Abrufen und Importieren des externen IPAM-Anbieterpakets in vRealize Orchestrator](#)
- Vergewissern Sie sich, dass Sie bei vRealize Orchestrator mit vRealize Automation mit der Berechtigung zum Ausführen von Workflows angemeldet sind.
- Halten Sie Ihre IaaS-Administratoranmeldedaten für vRealize Automation für die Eingabe bereit.

### Vorgehensweise

- 1 Klicken Sie in vRealize Orchestrator auf die Registerkarte **Design**, wählen Sie **Administrator > Bibliothek** und dann **IPAM Service Package SDK** aus.

Jedes IPAM-Anbieterpaket weist einen eindeutigen Namen auf und enthält spezielle Workflows. Die Workflownamen können zwischen den verschiedenen Anbieterpaketen ähnlich sein. Der Speicherort der Workflows in vRealize Orchestrator kann davon abweichen und ist vom Anbieter abhängig.

- 2 Führen Sie den Registrierungsworkflow **Register IPAM Endpoint** aus und geben Sie den IPAM-Infoblox-Endpoint-Typ an.
- 3 Geben Sie bei der Eingabeaufforderung für vRealize Automation-Anmeldedaten Ihre IaaS-Administratoranmeldedaten für vRealize Automation ein.

Das Paket registriert InfoBlox als neuen IPAM-Endpoint-Typ im vRealize Automation-Endpoint-Dienst und stellt den Endpoint-Typ beim Definieren von Endpoints in vRealize Automation zur Verfügung.

### Weiter

Nun können Sie einen IPAM-Infoblox-Endpoint-Typ in vRealize Automation erstellen. Siehe [Erstellen eines Endpoints für externen IPAM-Anbieter](#).



## **Vorbereiten Ihrer vCloud Director -Umgebung für vRealize Automation**

Bevor Sie vCloud Director in vRealize Automation integrieren können, müssen Sie Ihre vCloud Director-Instanz installieren und konfigurieren, Ihre vSphere- und Cloud-Ressourcen einrichten und entsprechende Anmeldedaten festlegen oder erstellen, um vRealize Automation den Zugriff auf Ihre vCloud Director-Umgebung zu gewähren.

### **Vorbereiten Ihrer Umgebung**

Konfigurieren Sie Ihre vSphere-Ressourcen und Cloud-Ressourcen, einschließlich der virtuellen Datacenter und Netzwerke. Weitere Informationen finden Sie in der Dokumentation zu vCloud Director.

### **Für die Integration erforderliche Anmeldedaten**

Erstellen oder identifizieren Sie Anmeldedaten entweder für einen Organisationsadministrator oder einen Systemadministrator, die Ihre vRealize Automation-IaaS-Administratoren verwenden können, damit Ihre vCloud Director-Umgebung als Endpoint von vRealize Automation verwaltet wird.

### **Überlegungen zu Benutzerrollen**

vCloud Director-Benutzerrollen in einer Organisation müssen nicht mit den Rollen in vRealize Automation-Business-Gruppen übereinstimmen. Wenn das Benutzerkonto in vCloud Director nicht vorhanden ist, führt vCloud Director einen Suchvorgang im zugewiesenen LDAP oder Active Directory durch und erstellt das Benutzerkonto, wenn der Benutzer in der Identitätsquelle vorhanden ist. Wenn das Benutzerkonto nicht erstellt werden kann, wird eine Warnung protokolliert, aber der Bereitstellungsvorgang schlägt nicht fehl. Die bereitgestellte Maschine wird dann dem Konto zugewiesen, das zum Konfigurieren des vCloud Director-Endpoints verwendet wurde.

Weitere Informationen zur Benutzerverwaltung in vCloud Director finden Sie in der vCloud Director-Dokumentation.

## **Vorbereiten Ihrer vCloud Air -Umgebung für vRealize Automation**

Bevor Sie vCloud Air in vRealize Automation integrieren, müssen Sie sich für das vCloud Air-Konto registrieren, Ihre vCloud Air-Umgebung einrichten und entsprechende Anmeldedaten festlegen oder erstellen, um vRealize Automation den Zugriff auf Ihre Umgebung zu gewähren.

### **Vorbereiten Ihrer Umgebung**

Konfigurieren Sie Ihre Umgebung gemäß den Anweisungen in der Dokumentation zu vCloud Air.

### **Für die Integration erforderliche Anmeldedaten**

Erstellen oder identifizieren Sie Anmeldedaten entweder für einen Virtual Infrastructure-Administrator oder einen Kontoadministrator, die Ihre vRealize Automation-IaaS-Administratoren verwenden können, damit Ihre vCloud Air-Umgebung als Endpoint von vRealize Automation verwaltet wird.

## Überlegungen zu Benutzerrollen

vCloud Air-Benutzerrollen in einer Organisation müssen nicht mit den Rollen in vRealize Automation-Business-Gruppen übereinstimmen. Weitere Informationen zur Benutzerverwaltung in vCloud Air finden Sie in der vCloud Air-Dokumentation.

## Vorbereiten Ihrer Amazon AWS -Umgebung

Bereiten Sie Elemente und Benutzerrollen in Ihrer Amazon AWS-Umgebung vor, bereiten Sie Amazon AWS für die Kommunikation mit dem Gast-Agent und dem Software-Bootstrap-Agent vor und informieren Sie sich, wie Amazon AWS-Funktionen vRealize Automation-Funktionen zugeordnet werden.

### Für vRealize Automation erforderliche Amazon AWS -Benutzerrollen und -Anmeldedaten

Für die Verwaltung Ihrer Umgebung müssen Sie Anmeldedaten in Amazon AWS mit den erforderlichen Berechtigungen für vRealize Automation konfigurieren.

Sie benötigen bestimmte Amazon-Zugriffsrechte, um Maschinen mithilfe von vRealize Automation erfolgreich bereitzustellen.

- Rollen- und Berechtigungsautorisierung in Amazon Web Services

Mit der Hauptbenutzerrolle in AWS erhält ein(e) AWS Directory Services-Benutzer/Gruppe den Vollzugriff auf AWS-Dienste und -Ressourcen.

Sie benötigen keine AWS-Anmeldedaten, um einen AWS-Endpoint in vRealize Automation zu erstellen. vRealize Automation erwartet jedoch, dass der AWS-Benutzer, der ein Amazon-Maschinen-Image erstellt, über die Hauptbenutzerrolle verfügt.

- Anmeldedaten für die Authentifizierung in Amazon Web Services

Mit der AWS-Hauptbenutzerrolle können AWS Identity and Access Management (IAM)-Benutzer und -Gruppen nicht verwaltet werden. Für die Verwaltung von IAM-Benutzern und -Gruppen benötigen Sie Anmeldedaten als AWS-Administrator mit Vollzugriff.

vRealize Automation erfordert Zugriffsschlüssel als Endpoint-Anmeldedaten und unterstützt keine Benutzernamen und Kennwörter. Für den Abruf des erforderlichen Zugriffsschlüssels zum Erstellen des Amazon-Endpoints muss der Hauptbenutzer entweder einen Schlüssel von einem Benutzer anfordern, der über Anmeldedaten als AWS-Administrator mit Vollzugriff verfügt, oder es muss zusätzlich die Richtlinie für einen AWS-Administrator mit Vollzugriff konfiguriert werden.

Weitere Informationen zum Aktivieren von Richtlinien und Rollen finden Sie im Abschnitt *AWS Identity and Access Management (IAM)* der Produktdokumentation zu Amazon Web Services.

## **Konfigurieren der Erlaubnis zur Kommunikation zwischen Amazon AWS die Kommunikation mit dem dem Software -Bootstrap-Agent und dem -Gast-Agent erlauben**

Falls Sie Anwendungs-Blueprints bereitstellen möchten, die Software enthalten, oder die Möglichkeit haben möchten, bereitgestellte Maschinen mithilfe des Gast-Agents weiter anzupassen, müssen Sie die Konnektivität zwischen Ihrer Amazon AWS-Umgebung, in der Ihre Maschinen bereitgestellt werden, und Ihrer vRealize Automation-Umgebung, in der die Agents Pakete herunterladen und Anweisungen erhalten, aktivieren.

Wenn Sie vRealize Automation zur Bereitstellung von Amazon AWS-Maschinen mit dem vRealize Automation-Gast-Agent und dem Software-Bootstrap-Agent verwenden, müssen Sie die Netzwerk-zu-Amazon-VPC-Konnektivität einrichten, damit Ihre bereitgestellten Maschinen zur Anpassung Ihrer Maschinen an vRealize Automation zurück kommunizieren können.

Weitere Informationen zu den Konnektivitätsoptionen von Amazon AWS VPC finden Sie in der Dokumentation zu Amazon AWS.

## **Verwenden von optionalen Amazon-Funktionen**

vRealize Automation unterstützt mehrere Amazon-Funktionen, z. B. Amazon Virtual Private Cloud, elastische Lastausgleichsdienste, elastische IP-Adressen und elastische Blockspeicherung.

### **Verwenden von Amazon-Sicherheitsgruppen**

Geben Sie beim Erstellen einer Amazon-Reservierung mindestens eine Sicherheitsgruppe an. Jede verfügbare Region erfordert mindestens eine angegebene Sicherheitsgruppe.

Eine Sicherheitsgruppe dient als Firewall, um den Zugriff auf die Maschine zu kontrollieren. Jede Region enthält zumindest die Standardsicherheitsgruppe. Mithilfe der Amazon Web Services Management Console können Administratoren zusätzliche Sicherheitsgruppen erstellen, Ports für Microsoft Remote Desktop Protocol oder SSH konfigurieren und ein virtuelles privates Netzwerk für ein Amazon VPN einrichten.

Bei der Erstellung einer Amazon-Reservierung oder Konfiguration einer Maschinenkomponente im Blueprint können Sie aus einer Liste Sicherheitsgruppen auswählen, die für die Region des angegebenen Amazon-Kontos verfügbar sind. Sicherheitsgruppen werden während der Datenerfassung importiert.

Weitere Informationen zur Erstellung und Verwendung von Sicherheitsgruppen in Amazon Web Services finden Sie in der Dokumentation zu Amazon.

### **Grundlegende Informationen zu Amazon Web Services-Regionen**

Jedes Amazon Web Services-Konto wird durch einen Cloud-Endpoint repräsentiert. Beim Erstellen eines Amazon Elastic Cloud Computing-Endpoints in vRealize Automation werden Regionen als Computing-Ressourcen erfasst. Nachdem der IaaS-Administrator Computing-Ressourcen für eine Business-Gruppe ausgewählt hat, erfolgt die automatische Erfassung von Bestandslisten- und Statusdaten.

Bei der Erfassung von Bestandslistendaten, die automatisch einmal täglich erfolgt, werden Daten für eine Computing-Ressource erfasst, wie beispielsweise folgende Daten:

- Elastische IP-Adressen
- Elastische Lastausgleichsmodule
- Elastic Block-Speichervolumes

Statusdaten werden standardmäßig alle 15 Minuten automatisch erfasst. Es werden Informationen zum Status der verwalteten Instanzen gesammelt. Hierbei handelt es sich um von vRealize Automation erstellte Instanzen. Nachstehend finden Sie Beispiele für Statusdaten:

- Windows-Kennwörter
- Status von Maschinen in Lastausgleichsdiensten
- Elastische IP-Adressen

Ein Fabric-Administrator kann die Erfassung von Bestandslisten- und Statusdaten starten und die Erfassung von Bestandslisten- und Statusdaten deaktivieren oder deren Häufigkeit ändern.

### Verwenden von Amazon Virtual Private Cloud

Mit Amazon Virtual Private Cloud können Sie Instanzen von Amazon-Maschinen in einem privaten Abschnitt der Amazon Web Services-Cloud bereitstellen.

Benutzer von Amazon Web Services können Amazon VPC zum Entwerfen einer virtuellen Netzwerktopologie entsprechend ihren Spezifikationen verwenden. Sie können eine Amazon VPC in vRealize Automation zuweisen. vRealize Automation verfolgt jedoch nicht die Kosten für die Verwendung der Amazon VPC.

Wenn Sie eine Bereitstellung mithilfe von Amazon VPC durchführen, erwartet vRealize Automation ein VPC-Subnetz, von dem Amazon eine primäre IP-Adresse abrufen kann. Diese Adresse ist so lange statisch, bis die Instanz beendet wird. Sie können den elastischen IP-Pool auch verwenden, um einer Instanz in vRealize Automation eine elastische IP-Adresse anzuhängen. Dadurch könnte der Benutzer dieselbe IP-Adresse behalten, wenn er Instanzen in Amazon Web Services kontinuierlich bereitstellt und entfernt.

Verwenden Sie die AWS Management Console, um die folgenden Elemente zu erstellen:

- Eine Amazon VPC, einschließlich Internet-Gateways, Routing-Tabellen, Sicherheitsgruppen und Subnetzen sowie verfügbaren IP-Adressen.
- Ein Amazon Virtual Private Network, wenn sich Benutzer außerhalb der AWS Management Console bei Instanzen von Amazon-Maschinen anmelden müssen.

vRealize Automation-Benutzer können die folgenden Aufgaben beim Arbeiten mit einer Amazon VPC ausführen:

- Ein Fabric-Administrator kann einer Cloud-Reservierung eine Amazon VPC zuweisen. Siehe [Erstellen einer Amazon-Reservierung](#).
- Ein Maschinenbesitzer kann einer Amazon VPC die Instanz einer Amazon-Maschine zuweisen.

Weitere Informationen zur Erstellung einer Amazon VPC finden Sie in der Dokumentation zu Amazon Web Services.

### **Verwenden von elastischen Lastausgleichsdiensten für Amazon Web Services**

Elastische Lastausgleichsdienste verteilen eingehenden Anwendungsdatenverkehr über Amazon Web Services-Instanzen hinweg. Mit dem Amazon-Lastausgleich können Sie Fault Tolerance und Leistung verbessern.

Amazon stellt Maschinen, die mit Amazon EC2-Blueprints bereitgestellt wurden, einen elastischen Lastausgleich zur Verfügung.

Der elastische Lastausgleichsdienst muss in Amazon Web Services, Amazon Virtual Private Network und am Speicherort der Bereitstellung verfügbar sein. Wenn ein Lastausgleichsdienst beispielsweise in us-east-1c verfügbar ist und der Speicherort der Maschine us-east-1b ist, kann die Maschine den Lastausgleichsdienst nicht verwenden.

Durch vRealize Automation werden elastische Lastausgleichsdienste weder erstellt, noch verwaltet oder überwacht.

Informationen zum Erstellen eines elastischen Amazon-Lastausgleichsdiensts mithilfe der Amazon Web Services Management Console finden Sie in der Amazon Web Services-Dokumentation.

### **Verwenden von elastischen IP-Adressen für Amazon Web Services**

Durch die Verwendung einer elastischen IP-Adresse können Sie ein schnelles Failover auf eine andere Maschine in einer dynamischen Amazon Web Services-Cloud-Umgebung durchführen. In vRealize Automation ist die elastische IP-Adresse für alle Business-Gruppen verfügbar, die über Rechte auf die Region verfügen.

Ein Administrator kann Ihrem Amazon Web Services-Konto elastische IP-Adressen mithilfe der AWS Management Console zuweisen. Es sind zwei Gruppen von elastischen IP-Adressen in jeder angegebenen Region vorhanden, ein Bereich für Nicht-Amazon VPC-Instanzen und ein anderer Bereich für Amazon VPCs. Wenn Sie Adressen nur in einer Nicht-Amazon VPC-Region zuweisen, sind die Adressen in einer Amazon VPC nicht verfügbar. Dies trifft umgekehrt ebenfalls zu. Wenn Sie Adressen nur in einer Amazon VPC zuweisen, sind die Adressen in einer Nicht-Amazon VPC-Region nicht verfügbar.

Die elastische IP-Adresse ist Ihrem Amazon Web Services-Konto zugeordnet, nicht einer bestimmten Maschine. Die Adresse kann jedoch nur von jeweils einer Maschine genutzt werden. Die Adresse bleibt mit Ihrem Amazon Web Services-Konto verknüpft, bis Sie sie freigeben möchten. Sie können sie freigeben, um sie einer bestimmten Maschineninstanz zuzuordnen.

Ein IaaS-Architekt kann während der Bereitstellung eine benutzerdefinierte Eigenschaft zu einem Blueprint hinzufügen, um Maschinen eine elastische IP-Adresse zuzuweisen. Maschinenbesitzer und Administratoren können die den Maschinen zugewiesenen elastischen IP-Adressen anzeigen, und Maschinenbesitzer oder Administratoren mit der Berechtigung zur Bearbeitung von Maschinen können nach der Bereitstellung eine elastische IP-Adresse zuweisen. Wenn die Adresse jedoch bereits mit einer Maschineninstanz verknüpft ist und die Maschine einen Teil der Amazon Virtual Private Cloud-Bereitstellung darstellt, führt Amazon die Zuweisung nicht durch.

Weitere Informationen zum Erstellen und Verwenden elastischer IP-Adressen von Amazon finden Sie in der Dokumentation zu Amazon Web Services.

### Verwenden von elastischen Blockspeichern für Amazon Web Services

Mit der elastischen Blockspeicherung von Amazon können Speichervolumes auf Blockebene mit einer Amazon-Maschineninstanz und Amazon Virtual Private Cloud verwendet werden. Das Speichervolume kann über die Lebensdauer der verknüpften Amazon-Maschineninstanz hinaus in der Amazon Web Services-Cloud-Umgebung erhalten bleiben.

Wenn Sie ein elastisches Blockspeichervolume von Amazon in Verbindung mit vRealize Automation verwenden, gelten die folgenden Einschränkungen:

- Sie können bei der Bereitstellung einer Maschineninstanz kein vorhandenes elastisches Blockspeichervolume anhängen. Wenn Sie jedoch ein neues Volume erstellen und gleichzeitig mehr als eine Maschine anfordern, wird das Volume erstellt und an jede Instanz angehängt. Wenn Sie beispielsweise ein als „volume\_1“ benanntes Volume erstellen und drei Maschinen anfordern, wird das Volume für jede Maschine erstellt. Es werden drei als „volume\_1“ benannte Volumes erstellt und je eines an die Maschinen angehängt. Jedes Volume verfügt über eine eindeutige Volume-ID. Jedes Volume weist dieselbe Größe auf und befindet sich am selben Speicherort.
- Das Volume muss denselben Betriebssystemtyp aufweisen und sich am selben Speicherort befinden wie die Maschine, an die es angehängt wird.
- vRealize Automation verwaltet nicht das primäre Volume einer auf elastische Blockspeicherung gestützten Instanz.

Weitere Informationen zu elastischer Blockspeicherung von Amazon und deren Aktivierung mit Amazon Web Services Management Console finden Sie in der Dokumentation zu Amazon Web Services.

### Szenario: Konfigurieren der VPC-Konnektivität zwischen Netzwerk und Amazon für eine Proof-of-Concept-Umgebung

Als mit der Einrichtung einer Proof-of-Concept-Umgebung zur Evaluierung von vRealize Automation beauftragter IT-Experte möchten Sie die Netzwerk-zu-Amazon-VPC-Konnektivität temporär zur Unterstützung der Software-Funktion von vRealize Automation konfigurieren.

Die Netzwerk-zu-Amazon-VPC-Verbindung ist nur erforderlich, wenn Sie den Gast-Agent zum Anpassen der bereitgestellten Maschinen verwenden möchten, oder wenn Sie Software-Komponenten in Ihre Blueprints einschließen möchten. Für eine Produktionsumgebung konfigurieren Sie diese Konnektivität offiziell durch Amazon Web Services. Da Sie jedoch in einer Proof-of-Concept-Umgebung arbeiten, möchten Sie stattdessen eine temporäre Netzwerk-zu-Amazon-VPC-Konnektivität konfigurieren. Sie erstellen den SSH-Tunnel und konfigurieren dann eine Amazon-Reservierung in vRealize Automation zwecks Weiterleitung durch Ihren Tunnel.

#### Voraussetzungen

- Installieren Sie vRealize Automation und führen Sie eine vollständige Konfiguration aus. Siehe *Installieren und Konfigurieren von vRealize Automation für das Rainpole-Szenario*.

- Erstellen Sie eine Amazon AWS-Sicherheitsgruppe namens „TunnelGroup“ und konfigurieren Sie sie so, dass der Zugriff auf Port 22 zulässig ist.
- Erstellen oder bestimmen Sie eine CentOS-Maschine in der Amazon AWS-Sicherheitsgruppe „TunnelGroup“ und notieren Sie die folgenden Konfigurationseinstellungen:
  - Anmeldedaten des Administratorbenutzers, zum Beispiel *root*.
  - Öffentliche IP-Adresse.
  - Private IP-Adresse.
- Erstellen oder bestimmen Sie eine CentOS-Maschine im gleichen lokalen Netzwerk wie Ihre vRealize Automation-Installation.
- Installieren Sie OpenSSH SSHD Server auf beiden Tunnelmaschinen.

### Vorgehensweise

- 1 Melden Sie sich bei Ihrer Amazon AWS-Tunnelmaschine als Root-Benutzer (oder ähnlich) an.
- 2 Deaktivieren Sie iptables.

```
# service iptables save
# service iptables stop
# chkconfig iptables off
```

- 3 Bearbeiten Sie `/etc/ssh/sshd_config`, um `AllowTCPForwarding` und `GatewayPorts` zu aktivieren.
- 4 Starten Sie den Dienst neu.

```
/etc/init.d/sshd restart
```

- 5 Melden Sie sich bei der CentOS-Maschine im gleichen lokalen Netzwerk wie Ihre vRealize Automation-Installation als Root-Benutzer an.
- 6 Rufen Sie den SSH-Tunnel zwischen der Maschine im lokalen Netzwerk und der Amazon AWS-Tunnelmaschine auf.

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" \
-R 1442:vRealize_automation_appliance_fqdn:5480 \
-R 1443:vRealize_automation_appliance_fqdn:443 \
-R 1444:manager_service_fqdn:443 \
Benutzer der Amazon-Tunnelmaschine@Öffentliche IP-Adresse der Amazon-Tunnelmaschine
```

Sie haben die Portweiterleitung konfiguriert, damit Ihre Amazon AWS-Tunnelmaschine auf vRealize Automation-Ressourcen zugreifen kann. Ihr SSH-Tunnel funktioniert jedoch erst, wenn Sie eine Amazon-Reservierung zwecks Weiterleitung durch den Tunnel konfiguriert haben

**Weiter**

- 1 Installieren Sie den Software-Bootstrap-Agent und den Gast-Agent auf einer Windows- oder Linux-Referenzmaschine, um ein Amazon-Maschinen-Image zu erstellen, das die IaaS-Architekten zum Erstellen von Blueprints verwenden können. Siehe [Vorbereiten für Software-Bereitstellung](#).
- 2 Konfigurieren Sie Ihre Amazon-Reservierung in vRealize Automation zwecks Weiterleitung durch Ihren SSH-Tunnel. Siehe [Szenario: Erstellen einer Amazon-Reservierung für eine Proof-of-Concept-Umgebung](#).

## Vorbereiten von Netzwerk- und Sicherheitsfunktionen für Red Hat OpenStack

vRealize Automation unterstützt mehrere Funktionen in OpenStack, z. B. Sicherheitsgruppen und dynamische IP-Adressen. Machen Sie sich mit der Funktionsweise dieser Funktionen mit vRealize Automation vertraut und konfigurieren Sie sie in Ihrer Umgebung.

### Verwenden von OpenStack-Sicherheitsgruppen

Mithilfe von Sicherheitsgruppen können Sie Regeln zur Steuerung des Netzwerkdatenverkehrs von bestimmten Ports angeben.

Sie können beim Erstellen einer Reservierung und auch auf der Blueprint-Arbeitsfläche Sicherheitsgruppen angeben. Sie können auch beim Anfordern einer Maschine Sicherheitsgruppen angeben.

Sicherheitsgruppen werden während der Datenerfassung importiert.

Jede verfügbare Region erfordert mindestens eine angegebene Sicherheitsgruppe. Wenn Sie eine Reservierung erstellen, werden die in dieser Region verfügbaren Sicherheitsgruppen angezeigt. Jede Region enthält zumindest die Standardsicherheitsgruppe.

Zusätzliche Sicherheitsgruppen müssen in der Quellressource verwaltet werden. Weitere Informationen zur Verwaltung von Sicherheitsgruppen für die verschiedenen Maschinen finden Sie in der OpenStack-Dokumentation.

### Verwenden von Pool-IP-Adressen mit OpenStack

Sie können einer virtuellen Instanz in OpenStack Pool-IP-Adressen zuweisen.

Um die Zuweisung von Pool-IP-Adressen zu aktivieren, müssen Sie die IP-Weiterleitung konfigurieren und einen IP-Adressenpool in Red Hat OpenStack erstellen. Weitere Informationen finden Sie in der Dokumentation zu Red Hat OpenStack.

Sie müssen Maschinenbesitzern die Berechtigung für die Aktionen „Pool-IP-Adresse zuweisen“ und „Pool-IP-Adresse zurücknehmen“ zuweisen. Der berechtigte Benutzer kann dann einer bereitgestellten Maschine über die externen Netzwerke, die mit der Maschine verbunden sind, eine Pool-IP-Adresse zuweisen, indem er im IP-Adressenpool eine verfügbare Adresse auswählt. Nachdem einer Maschine eine Pool-IP-Adresse zugewiesen wurde, kann ein Benutzer von vRealize Automation die Option „Pool-IP-Adresse zurücknehmen“ auswählen, um die aktuell zugewiesenen Pool-IP-Adressen anzuzeigen und eine Adresse für eine Maschine zurückzunehmen.



## Vorbereiten Ihrer SCVMM -Umgebung

Bevor Sie mit der Erstellung von SCVMM-Vorlagen und -Hardwareprofilen für die Verwendung bei Maschinenbereitstellung in vRealize Automation beginnen, müssen Sie die Einschränkungen bei der Namensgebung von Vorlagen- und Hardwareprofilnamen verstehen sowie SCVMM-Netzwerk- und Speichereinstellungen konfigurieren.

### Benennung von Vorlagen und Hardwareprofilen

Aufgrund der von SCVMM und vRealize Automation verwendeten Benennungskonventionen für Vorlagen und Hardwareprofile dürfen die Namen Ihrer Vorlagen und Hardwareprofile nicht mit den Wörtern „temporär“ und „Profil“ beginnen. Die folgenden Wörter beispielsweise werden während der Datenerfassung ignoriert:

- TemporäreVorlage
- Temporäre Vorlage
- TemporäresProfil
- Temporäres Profil
- Profil

### Erforderliche Netzwerkkonfiguration für SCVMM -Cluster

Da SCVMM-Cluster virtuelle Netzwerke nur für vRealize Automation verfügbar machen, benötigen Sie eine 1:1-Beziehung zwischen dem virtuellen und dem logischen Netzwerk. Mithilfe der SCVMM-Konsole ordnen Sie jedes logische Netzwerk einem virtuellen Netzwerk zu und konfigurieren Ihren SCVMM-Cluster, um über das virtuelle Netzwerk auf Maschinen zugreifen zu können.

### Erforderliche Speicherkonfiguration für SCVMM -Cluster

vRealize Automation erfasst auf SCVMM-Hyper-V-Clustern Daten und führt Bereitstellungen nur auf gemeinsam genutzten Volumes durch. Mithilfe der SCVMM-Konsole konfigurieren Sie Ihre Cluster für die Verwendung von gemeinsam genutzten Ressourcenvolumes für Speicher.

### Erforderliche Speicherkonfiguration für eigenständige SCVMM -Hosts

vRealize Automation erfasst für eigenständige SCVMM-Hosts Daten und führt Bereitstellungen auf dem Standardpfad der virtuellen Maschine durch. Mithilfe der SCVMM-Konsole konfigurieren Sie Standardpfade von virtuellen Maschinen für Ihre eigenständigen Hosts.

## Vorbereiten für Maschinenbereitstellung

In Abhängigkeit von Ihrer Umgebung und Ihrer Methode der Maschinenbereitstellung müssen Sie möglicherweise Elemente außerhalb von vRealize Automation konfigurieren. Beispielsweise müssen Sie möglicherweise Maschinenvorlagen oder Maschinen-Images konfigurieren. Darüber hinaus müssen Sie möglicherweise NSX-Einstellungen konfigurieren oder vRealize Orchestrator-Workflows ausführen.

## Auswählen einer vorzubereitenden Methode zur Maschinenbereitstellung

Bei den meisten Methoden zur Maschinenbereitstellung müssen einige Elemente außerhalb von vRealize Automation vorbereitet werden.

**Tabelle 1-4. Auswählen einer vorzubereitenden Methode zur Maschinenbereitstellung**

Szenario	Unterstützter End-point	Agent-Unterstützung	Bereitstellungsmethode	Vorbereitungen vor der Bereitstellung
vRealize Automation so konfigurieren, dass benutzerdefinierte Visual Basic-Skripts als zusätzliche Schritte im Lebenszyklus der Maschine vor oder nach der Bereitstellung der Maschine ausgeführt werden. Beispielsweise könnten Sie mithilfe eines Skripts vor der Bereitstellung Zertifikate oder Sicherheitstoken vor der Bereitstellung generieren und dann mithilfe eines Skripts nach der Bereitstellung die Zertifikate und Token nach der Bereitstellung der Maschine verwenden.	Visual Basic-Skripts können Sie mit jedem unterstützten Endpoint außer Amazon AWS ausführen.	Hängt von der von Ihnen gewählten Bereitstellungsmethode ab.	Als zusätzlicher Schritt in jeder Bereitstellungsmethode unterstützt, aber Visual Basic-Skripts können nicht zusammen mit Amazon AWS-Maschinen verwendet werden.	<a href="#">Checkliste für die Ausführung von Visual Basic-Skripts während der Bereitstellung</a>
Anwendungs-Blueprints bereitstellen, die die Installations-, Konfigurations- und Lebenszyklusverwaltung von Middleware- und Anwendungsbereitstellungskomponenten wie Oracle, MySQL, WAR und Datenbankschemata automatisieren.	<ul style="list-style-type: none"> <li>■ vSphere</li> <li>■ vCloud Air</li> <li>■ vCloud Director</li> <li>■ Amazon AWS</li> </ul>	<ul style="list-style-type: none"> <li>■ (Erforderlich) Gast-Agent</li> <li>■ (Erforderlich) Software-Bootstrap-Agent und Gast-Agent</li> </ul>	<ul style="list-style-type: none"> <li>■ Klonen</li> <li>■ Klon (für vCloud Air oder vCloud Director)</li> <li>■ Verknüpfter Klon</li> <li>■ Amazon-Maschinen-Image</li> </ul>	Um Software-Komponenten in Ihren Blueprints verwenden zu können, müssen Sie eine Bereitstellungsmethode vorbereiten, die den Gast-Agent und den Software-Bootstrap-Agent unterstützt. Weitere Informationen zur Vorbereitung für Software finden Sie unter <a href="#">Vorbereiten für Software-Bereitstellung</a> .
Weiteres Anpassen von Maschinen nach der Bereitstellung mithilfe des Gast-Agent.	Alle virtuellen Endpoints und Amazon AWS.	<ul style="list-style-type: none"> <li>■ (Erforderlich) Gast-Agent</li> <li>■ (Optional) Software-Bootstrap-Agent und Gast-Agent</li> </ul>	Wird für alle Bereitstellungsmethoden außer VM-Image unterstützt.	Um Maschinen nach der Bereitstellung anpassen zu können, müssen Sie eine Bereitstellungsmethode auswählen, die den Gast-Agent unterstützt. Weitere Informationen zum Gast-Agent finden Sie unter <a href="#">Verwenden des vRealize Automation-Gast-Agent bei der Bereitstellung</a> .

**Tabelle 1-4. Auswählen einer vorzubereitenden Methode zur Maschinenbereitstellung (Fortsetzung)**

Szenario	Unterstützter End-point	Agent-Unterstützung	Bereitstellungsmethode	Vorbereitungen vor der Bereitstellung
Stellen Sie Maschinen ohne Gastbetriebssystem bereit. Sie können nach der Bereitstellung ein Betriebssystem installieren.	Alle VM-Endpoints.	Nicht unterstützt	Einfach	Keine Vorbereitungen vor der Bereitstellung außerhalb von vRealize Automation erforderlich.
Stellen Sie eine speicher-effiziente Kopie einer virtuellen Maschine bereit, einen so genannten verknüpften Klon. Verknüpfte Klone basieren auf einem Snapshot einer VM und verwenden eine Kette von Delta-Datenträgern zum Nachverfolgen von Unterschieden von einer übergeordneten Maschine.	vSphere	<ul style="list-style-type: none"> <li>■ (Optional) Gast-Agent</li> <li>■ (Optional) Software-Bootstrap-Agent und Gast-Agent</li> </ul>	Verknüpfter Klon	<p>Es muss eine virtuelle vSphere-Maschine vorhanden sein.</p> <p>Wenn Software unterstützt werden soll, müssen Sie den Gast-Agent und den Software-Bootstrap-Agent auf der Maschine, die Sie klonen möchten, installieren.</p>
Stellen Sie eine speicher-effiziente Kopie einer virtuellen Maschine durch Verwendung der Net App FlexClone-Technologie bereit.	vSphere	(Optional) Gast-Agent	NetApp FlexClone	<a href="#">Checkliste für das Vorbereiten für die Bereitstellung durch Klonen</a>
Stellen Sie Maschinen durch Klonen von einem Vorlagenobjekt bereit, das von einer vorhandenen Windows- oder Linux-Maschine erstellt wurde, der so genannten Referenzmaschine, und von einem Anpassungsobjekt.	<ul style="list-style-type: none"> <li>■ vSphere</li> <li>■ KVM (RHEV)</li> <li>■ SCVMM</li> </ul>	<ul style="list-style-type: none"> <li>■ (Optional) Gast-Agent</li> <li>■ (Nur für vSphere optional) Software-Bootstrap-Agent und Gast-Agent</li> </ul>	Klonen	<p>Siehe <a href="#">Checkliste für das Vorbereiten für die Bereitstellung durch Klonen</a>.</p> <p>Wenn Software unterstützt werden soll, müssen Sie den Gast-Agent und den Software-Bootstrap-Agent auf der vSphere-Maschine, die Sie klonen möchten, installieren.</p>
Bereitstellen von vCloud Air- oder vCloud Director-Maschinen anhand einer Vorlage und eines Anpassungsobjekts.	<ul style="list-style-type: none"> <li>■ vCloud Air</li> <li>■ vCloud Director</li> </ul>	<ul style="list-style-type: none"> <li>■ (Optional) Gast-Agent</li> <li>■ (Optional) Software-Bootstrap-Agent und Gast-Agent</li> </ul>	Klonen von vCloud Air oder vCloud Director	<p>Siehe <a href="#">Vorbereiten für die vCloud Air- und vCloud Director-Bereitstellung</a>.</p> <p>Wenn Software unterstützt werden soll, müssen Sie eine Vorlage erstellen, die den Gast-Agent und den Software-Bootstrap-Agent enthält. Konfigurieren Sie für vCloud Air die Netzwerkverbindung zwischen Ihrer vRealize Automation-Umgebung und Ihrer vCloud Air-Umgebung.</p>

**Tabelle 1-4. Auswählen einer vorzubereitenden Methode zur Maschinenbereitstellung (Fortsetzung)**

Szenario	Unterstützter End-point	Agent-Unterstützung	Bereitstellungsmethode	Vorbereitungen vor der Bereitstellung
Stellen Sie eine Maschine durch Starten von einem ISO-Image bereit. Verwenden Sie dabei eine Kickstart- oder AutoYaST-Konfigurationsdatei und ein Linux-Distributions-Image zum Installieren des Betriebssystems auf der Maschine.	<ul style="list-style-type: none"> <li>■ Alle virtuellen Endpoints</li> <li>■ Red Hat Open-Stack</li> </ul>	Der Gast-Agent wird im Rahmen der Vorbereitungsanweisungen installiert.	Linux Kickstart	<a href="#">Vorbereiten für die Linux Kickstart-Bereitstellung</a>
Stellen Sie eine Maschine bereit und geben Sie die Steuerung an eine SCCM-Aufgabensequenz zum Starten von einem ISO-Image weiter, stellen Sie ein Windows-Betriebssystem bereit und installieren Sie den vRealize Automation-Gast-Agent.	Alle VM-Endpoints.	Der Gast-Agent wird im Rahmen der Vorbereitungsanweisungen installiert.	SCCM	<a href="#">Vorbereiten für SCCM-Bereitstellung</a>
Stellen Sie eine Maschine durch Starten in eine WinPE-Umgebung bereit und durch Installieren eines Betriebssystems unter Verwendung eines WIM-Images (Windows Imaging Format) einer vorhandenen Windows-Referenzmaschine.	<ul style="list-style-type: none"> <li>■ Alle virtuellen Endpoints</li> <li>■ Red Hat Open-Stack</li> </ul>	<p>Gast-Agent ist erforderlich. Sie können PEBuilder zum Erstellen eines WinPE-Images verwenden, das den Gast-Agent enthält. Sie können das WinPE-Image unter Verwendung einer anderen Methode erstellen, aber Sie müssen den Gast-Agent manuell einfügen.</p>	WIM	<a href="#">Vorbereiten für die WIM-Bereitstellung</a>

**Tabelle 1-4. Auswählen einer vorzubereitenden Methode zur Maschinenbereitstellung (Fortsetzung)**

Szenario	Unterstützter End-point	Agent-Unterstützung	Bereitstellungsmethode	Vorbereitungen vor der Bereitstellung
Starten Sie eine Instanz von einem VM-Image.	Red Hat OpenStack	Nicht unterstützt	VM-Image	Siehe <a href="#">Vorbereiten für die Image-Bereitstellung der virtuellen Maschine</a> .
Starten Sie eine Instanz von einem Amazon-System-Image.	Amazon AWS	<ul style="list-style-type: none"> <li>■ (Optional) Gast-Agent</li> <li>■ (Optional) Software-Bootstrap-Agent und Gast-Agent</li> </ul>	Amazon-Maschinen-Image	<p>Amazon-Maschinen-Images und -Instanztypen müssen mit Ihrem Amazon AWS-Konto verknüpft werden.</p> <p>Wenn Software unterstützt werden soll, müssen Sie ein Amazon-Maschinen-Image erstellen, das den Gast-Agent und den Software-Bootstrap-Agent enthält, und die Netzwerk-zu-VPC-Konnektivität zwischen Ihrer Amazon AWS-Umgebung und Ihrer vRealize Automation-Umgebung konfigurieren.</p>

## Checkliste für die Ausführung von Visual Basic-Skripts während der Bereitstellung

Sie können vRealize Automation so konfigurieren, dass Ihre benutzerdefinierten Visual Basic-Skripts als zusätzliche Schritte im Lebenszyklus der Maschine vor oder nach der Bereitstellung der Maschine ausgeführt werden. Beispielsweise könnten Sie mithilfe eines Skripts vor der Bereitstellung Zertifikate oder Sicherheitstoken vor der Bereitstellung generieren und dann mithilfe eines Skripts nach der Bereitstellung die Zertifikate und Token nach der Bereitstellung der Maschine verwenden. Visual Basic-Skripts können mit jeder Bereitstellungsmethode ausgeführt werden, aber Visual Basic-Skripts können nicht zusammen mit Amazon AWS-Maschinen verwendet werden.

**Tabelle 1-5. Checkliste für die Ausführung von Visual Basic-Skripts während der Bereitstellung**

Aufgabe	Speicherort	Details
<input type="checkbox"/> Installieren und konfigurieren Sie den EPI-Agent für Visual Basic-Skripts.	In der Regel der Manager Service-Host	Siehe <i>Installieren von vRealize Automation 7.1</i> .
<input type="checkbox"/> Erstellen Sie Ihre Visual Basic-Skripts.	Die Maschine, auf der der EPI-Agent installiert ist	<p>vRealize Automation enthält das Visual Basic-Beispielskript <code>PrePostProvisioningExample.vbs</code> im Unterverzeichnis <code>Scripts</code> des EPI-Agent-Installationsverzeichnisses. Dieses Skript enthält eine Kopfzeile zum Laden aller Argumente in ein Wörterbuch, einen Textkörper zur Eingabe von Funktionen sowie eine Fußzeile zum Zurückgeben von aktualisierten benutzerdefinierten Eigenschaften an vRealize Automation.</p> <p>Beim Ausführen eines Visual Basic-Skripts übergibt der EPI-Agent alle benutzerdefinierten Maschineneigenschaften als Argumente an das Skript. Um aktualisierte Eigenschaftswerte an vRealize Automation zurückzugeben, platzieren Sie diese Eigenschaften in einem Wörterbuch und rufen Sie eine Funktion von vRealize Automation auf.</p>
<input type="checkbox"/> Sammeln Sie die erforderlichen Informationen, um Ihre Skripts in Blueprints einzubeziehen.	<p>Erfassen von Informationen und Übertragen an Ihre Infrastrukturarchitekten</p> <p><b>Hinweis</b> Ein Fabric-Administrator kann eine Eigenschaftsgruppe durch Verwendung der Eigenschaftensätze <code>ExternalPreProvisioningVbScript</code> und <code>ExternalPostProvisioningVbScript</code> erstellen, um diese erforderlichen Informationen bereitzustellen. Auf diese Weise können Blueprint-Architekten diese Informationen richtig zu ihren Blueprints hinzufügen.</p>	<ul style="list-style-type: none"> <li>Der vollständige Pfad zum Visual Basic-Skript, einschließlich Dateiname und Erweiterung. Zum Beispiel <code>%System Drive%Programme (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs</code>.</li> <li>Um ein Skript vor der Bereitstellung auszuführen, weisen Sie die Infrastrukturarchitekten an, den vollständigen Pfad zum Skript als Wert der benutzerdefinierten Eigenschaft <code>ExternalPreProvisioningVbScript</code> einzugeben. Zum Ausführen eines Skripts nach der Bereitstellung müssen sie die benutzerdefinierte Eigenschaft <code>ExternalPostProvisioningVbScript</code> verwenden.</li> </ul>

## Verwenden des vRealize Automation -Gast-Agent bei der Bereitstellung

Sie können den Gast-Agent auf Referenzmaschinen installieren, um eine Maschine nach der Bereitstellung weiter anzupassen. Sie können die reservierten benutzerdefinierten Eigenschaften des Gast-Agent verwenden, um allgemeine Anpassungen wie z. B. das Hinzufügen und Formatieren von Festplatten durchzuführen. Sie können aber auch Ihre eigenen benutzerdefinierten Skripts für den Gast-Agent erstellen, die dann im Gastbetriebssystem einer bereitgestellten Maschine ausgeführt werden.

Wenn die Bereitstellung abgeschlossen ist und die Anpassungsspezifikation (sofern angegeben) ausgeführt wird, erstellt der Gast-Agent eine XML-Datei, die alle benutzerdefinierten Eigenschaften der bereitgestellten Maschine enthält `c:\VRMGuestAgent\site\workitem.xml`, führt alle Aufgaben durch, die dem ihm durch die benutzerdefinierten Eigenschaften des Gast-Agent zugewiesen wurden, und löscht sich anschließend selbst von der bereitgestellten Maschine.

Sie können Ihre eigenen benutzerdefinierten Skripts für den Gast-Agent zur Ausführung auf bereitgestellten Maschinen schreiben und benutzerdefinierte Eigenschaften auf dem Maschinen-Blueprint verwenden, um den Speicherort dieser Skripts sowie die Reihenfolge ihrer Ausführung festzulegen. Sie können benutzerdefinierte Eigenschaften auf dem Maschinen-Blueprint auch dazu verwenden, benutzerdefinierte Eigenschaftswerte als Parameter an Ihre Skripts weiterzugeben.

Verwenden Sie z. B. den Gast-Agent, um die folgenden Anpassungen auf bereitgestellten Maschinen vorzunehmen:

- Ändern der IP-Adresse
- Ändern oder Formatieren von Laufwerken
- Ausführen von Sicherheitsskripts
- Initialisieren eines weiteren Agents, z. B. Puppet oder Chef

Sie können auch eine verschlüsselte Zeichenfolge als benutzerdefinierte Eigenschaft in einem Befehlszeilenargument bereitstellen. Auf diese Weise können Sie verschlüsselte Informationen speichern, die der Gast-Agent entschlüsseln und als gültiges Befehlszeilenargument interpretieren kann.

Ihre benutzerdefinierten Skripts müssen nicht lokal auf der Maschine installiert werden. Solange die bereitgestellte Maschine über Netzwerkzugriff auf den Skriptspeicherort verfügt, kann der Gast-Agent auf die Skripts zugreifen und sie ausführen. Dies führt zu geringeren Wartungskosten, da Sie Ihre Skripts aktualisieren können, ohne dazu Ihre gesamten Vorlagen neu erstellen zu müssen.

Wenn Sie den Gast-Agent zur Ausführung benutzerdefinierter Skripts auf bereitgestellten Maschinen installieren möchten, müssen Ihre Blueprints die entsprechenden benutzerdefinierten Eigenschaften des Gast-Agents enthalten. Wenn Sie beispielsweise den Gast-Agent auf einer Vorlage zum Klonen installieren, ein benutzerdefiniertes Skript erstellen, das die IP-Adresse der bereitgestellten Maschine ändert, und das Skript an einem gemeinsam genutzten Speicherort ablegen, müssen Sie eine Anzahl von benutzerdefinierten Eigenschaften in Ihren Blueprint einbeziehen.

**Tabelle 1-6. Benutzerdefinierte Eigenschaften für das Ändern von IP-Adressen auf einer bereitgestellten Maschine mithilfe eines Gast-Agents**

Benutzerdefinierte Eigenschaft	Beschreibung
VirtualMachine.Admin.UseGuestAgent	Setzen Sie den Wert auf <b>true</b> , um den Gast-Agent beim Start der bereitgestellten Maschine zu initialisieren.
VirtualMachine.Customize.WaitComplete	Legen Sie diese Eigenschaft auf „True“ fest, um zu verhindern, dass der Bereitstellungsworkflow Arbeitselemente an den Gast-Agent sendet, bevor alle Anpassungen abgeschlossen wurden.



**Tabelle 1-6. Benutzerdefinierte Eigenschaften für das Ändern von IP-Adressen auf einer bereitgestellten Maschine mithilfe eines Gast-Agents (Fortsetzung)**

Benutzerdefinierte Eigenschaft	Beschreibung
VirtualMachine.SoftwareN.ScriptPath	<p data-bbox="810 300 1412 420">Gibt den vollständigen Pfad zum Installationsskript einer Anwendung an. Bei dem Pfad muss es sich um einen gültigen absoluten Pfad wie er im Gastbetriebssystem angezeigt wird handeln und er muss den Namen der Skriptdatei enthalten.</p> <p data-bbox="810 432 1412 709">Sie können benutzerdefinierte Eigenschaftswerte als Parameter an das Skript übergeben, indem Sie <i>{CustomPropertyName}</i> in der Pfadzeichenfolge einfügen. Angenommen, Sie haben eine benutzerdefinierte Eigenschaft <i>ActivationKey</i> mit dem Wert 1234. In diesem Fall lautet der Skriptpfad <i>D:\InstallApp.bat -key {ActivationKey}</i>. Der Gast-Agent führt den Befehl <i>D:\InstallApp.bat -key 1234</i> aus. Ihre Skriptdatei kann dann so programmiert werden, dass dieser Wert akzeptiert und verwendet wird.</p> <p data-bbox="810 722 1412 783">Fügen Sie <i>{Owner}</i> ein, um den Namen des Maschinenbesitzers an das Skript zu übergeben.</p> <p data-bbox="810 795 1412 915">Sie können auch benutzerdefinierte Eigenschaftswerte als Parameter an das Skript weitergeben, indem Sie <i>{YourCustomProperty}</i> in die Pfadzeichenfolge einfügen. Wenn Sie beispielsweise den</p> <p data-bbox="810 928 1412 1047">Wert <i>\\vra-scripts.mycompany.com\scripts\changeIP.bat</i> eingeben, wird das Skript <i>changeIP.bat</i> von einem gemeinsam genutzten Speicherort ausgeführt. Wenn Sie jedoch den</p> <p data-bbox="810 1060 1412 1234">Wert <i>\\vra-scripts.mycompany.com\scripts\changeIP.bat {VirtualMachine.Network0.Address}</i> eingeben, wird das Skript für die Änderung der IP-Adresse ausgeführt, aber auch der Wert der Eigenschaft <i>VirtualMachine.Network0.Address</i> als Parameter an das Skript weitergegeben.</p>
VirtualMachine.ScriptPath.Decrypt	<p data-bbox="810 1260 1412 1409">Ermöglicht vRealize Automation das Abrufen einer verschlüsselten Zeichenfolge, die als ordnungsgemäß formatierte benutzerdefinierte Eigenschaftsanweisung <i>VirtualMachine.SoftwareN.ScriptPath</i> an die zugewiesene Befehlszeile übergeben wird.</p> <p data-bbox="810 1421 1412 1701">Sie können eine verschlüsselte Zeichenfolge wie beispielsweise Ihr Kennwort als benutzerdefinierte Eigenschaft in einem Befehlszeilenargument bereitstellen. Auf diese Weise können Sie verschlüsselte Informationen speichern, die der Gast-Agent entschlüsseln und als gültiges Befehlszeilenargument interpretieren kann. Beispielsweise ist die benutzerdefinierte Eigenschaftszeichenfolge <i>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat Kennwort</i> nicht sicher, da sie ein tatsächliches Kennwort enthält.</p> <p data-bbox="810 1713 1412 1833">Zum Entschlüsseln des Kennworts können Sie eine benutzerdefinierte vRealize Automation-Eigenschaft erstellen, wie beispielsweise <i>MyPassword = password</i>, und die Verschlüsselung durch Aktivieren des verfügbaren Kontrollkästchens akti-</p>

**Tabelle 1-6. Benutzerdefinierte Eigenschaften für das Ändern von IP-Adressen auf einer bereitgestellten Maschine mithilfe eines Gast-Agents (Fortsetzung)**

Benutzerdefinierte Eigenschaft	Beschreibung
	<p>vieren. Der Gast-Agent entschlüsselt den Eintrag <b>[MyPassword]</b> in den Wert in der benutzerdefinierten Eigenschaft <b>MyPassword</b> und führt das Skript als <code>c:\dosomething.bat password</code> aus.</p> <ul style="list-style-type: none"> <li>■ Erstellen Sie die benutzerdefinierte Eigenschaft <b>MyPassword = Kennwort</b>, wobei <i>Kennwort</i> der Wert Ihres tatsächlichen Kennworts ist. Aktivieren Sie die Verschlüsselung durch Aktivieren des verfügbaren Kontrollkästchens.</li> <li>■ Legen Sie die benutzerdefinierte Eigenschaft <b>VirtualMachine.ScriptPath.Decrypt</b> als <b>VirtualMachine.ScriptPath.Decrypt = true</b> fest.</li> <li>■ Legen Sie die benutzerdefinierte Eigenschaft <b>VirtualMachine.Software0.ScriptPath</b> als <b>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat [MyPassword]</b> fest.</li> </ul> <p>Wenn Sie <b>VirtualMachine.ScriptPath.Decrypt</b> auf „False“ festlegen oder die benutzerdefinierte Eigenschaft <b>VirtualMachine.ScriptPath.Decrypt</b> nicht erstellen, wird die Zeichenfolge in den eckigen Klammern ([ und ]) nicht entschlüsselt.</p>

Weitere Informationen zu benutzerdefinierten Eigenschaften, die Sie mit dem Gast-Agent verwenden können, finden Sie unter *Referenz für benutzerdefinierte Eigenschaften*.

## Installieren des Gast-Agents auf einer Linux-Referenzmaschine

Installieren Sie den Linux-Gast-Agent auf Ihren Referenzmaschinen zum weiteren Anpassen der Maschinen nach der Bereitstellung.

### Voraussetzungen

- Bestimmen oder erstellen Sie die Referenzmaschine.
- Die heruntergeladenen Gast-Agent-Dateien enthalten beide Paketformate `tar.gz` und `RPM`. Wenn das Betriebssystem `tar.gz`- oder `RPM`-Dateien nicht installieren kann, konvertieren Sie die Installationsdateien mit einem Konvertierungstool in Ihr bevorzugtes Paketformat.

### Vorgehensweise

- 1 Navigieren Sie zur Installationsseite für die vCloud Automation Center Appliance-Managementkonsole.  
Beispielsweise „`https://vcac-hostname.domain.name:5480/installer/`“.
- 2 Laden Sie die Linux-Gast-Agent-Pakete herunter und speichern Sie sie.
- 3 Entpacken Sie die Datei `LinuxGuestAgentPkgs`.

- 4 Installieren Sie das Gast-Agent-Paket, das dem Gastbetriebssystem entspricht, das Sie bei der Bereitstellung bereitstellen.

- a Navigieren Sie zum Unterverzeichnis `LinuxGuestAgentPkgs` für das Gastbetriebssystem.
- b Suchen Sie Ihr bevorzugtes Paketformat oder konvertieren Sie ein Paket in Ihr bevorzugtes Paketformat.
- c Installieren Sie das Gast-Agent-Paket auf Ihrer Referenzmaschine.

Um beispielsweise die Dateien aus dem RPM-Paket zu installieren, führen Sie `rpm -i gu-gent-7.0.0-012715.x86_64.rpm` aus.

- 5 Konfigurieren Sie den Gast-Agent zum Kommunizieren mit dem Manager Service durch Ausführen von `installgugent.sh Manager_Service_Hostname_fqdn:portnumber ssl platform`.

Die Standardportnummer für den Manager Service ist 443. Zulässige Plattformwerte sind `ec2`, `vcd`, `vca` und `vsphere`.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichsdienst verwenden</b>	<p>Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts von Manager Service ein. Beispiel:</p> <pre>cd /usr/share/gugent ./installgugent.sh load_balancer_manager_service.mycompany.com:443 ssl ec2</pre>
<b>Wenn Sie keinen Lastausgleichsdienst verwenden</b>	<p>Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Manager Service-Maschine ein. Beispiel:</p> <pre>cd /usr/share/gugent ./installgugent.sh manager_service_machine.mycompany.com:443 ssl vsphere</pre>

- 6 Wenn bereitgestellte Maschinen nicht schon so konfiguriert sind, dass sie dem SSL-Zertifikat von Manager Service vertrauen, müssen Sie die `cert.pem`-Datei auf der Referenzmaschine installieren, um die Vertrauensstellung herzustellen.

- Rufen Sie das `cert.pem`-Zertifikat ab und installieren Sie die Datei auf der Referenzmaschine manuell. Das ist die sicherste Vorgehensweise.
- Sie können aber auch einfach die Verbindung zum Lastausgleichsdiensts von Manager Service oder zur Manager Service-Maschine herstellen und das `cert.pem`-Zertifikat herunterladen.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	<p>Führen Sie als Root-Benutzer auf der Referenzmaschine den folgenden Befehl aus:</p> <pre>echo   openssl s_client -connect <i>manager_service_load_balancer.mycompany.com:443</i>   sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' &gt; cert.pem</pre>
Wenn Sie keinen Lastausgleichsdienst verwenden	<p>Führen Sie als Root-Benutzer auf der Referenzmaschine den folgenden Befehl aus:</p> <pre>echo   openssl s_client -connect <i>manager_service_machine.mycompany.com:443</i>   sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' &gt; cert.pem</pre>

- 7 Wenn Sie den Gast-Agent auf einem Ubuntu-Betriebssystem installieren, erstellen Sie symbolische Verknüpfungen für freigegebene Objekte, indem Sie einen der folgenden Befehlssätze ausführen.

Option	Beschreibung
64-Bit-Systeme	<pre>cd /lib/x86_64-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>
32-Bit-Systeme	<pre>cd /lib/i386-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>

## Weiter

Konvertieren Sie Ihre Referenzmaschine in eine Vorlage zum Klonen, ein Amazon-System-Image oder einen Snapshot, die/das/den Ihre IaaS-Architekten beim Erstellen von Blueprints verwenden können.

## Installieren des Gast-Agents auf einer Windows-Referenzmaschine

Installieren Sie den Windows-Gast-Agent auf einer Windows-Referenzmaschine zur Ausführung als Windows-Dienst und um die weitere Anpassung von Maschinen zu ermöglichen.

### Voraussetzungen

- Bestimmen oder erstellen Sie die Referenzmaschine.

- Wenn Sie die sicherste Methode für eine vertrauenswürdige Kommunikation zwischen dem Gast-Agent und Ihrer Manager Service-Maschine festlegen möchten, rufen Sie das SSL-Zertifikat im PEM-Format von Ihrer Manager Service-Maschine ab. Weitere Informationen zum Festlegen von Vertrauen für den Gast-Agent finden Sie unter [Konfigurieren des Vertrauensverhältnisses zu einem Server für den Windows-Gast-Agent](#).

### Vorgehensweise

- 1 Navigieren Sie zur Installationsseite für die vCloud Automation Center Appliance-Managementkonsole.

Beispielsweise „<https://vcac-hostname.domain.name:5480/installer/>“.

- 2 Klicken Sie auf dieser Seite im Abschnitt für die Installation der vRealize Automation-Komponente auf **Gast- und Software-Agents**.

Beispiel: <https://va-hostname.domain.com/software/index.html>.

Die Seite **Installationsprogramme für Gast- und Software-Agents** wird mit Links zu verfügbaren Downloads geöffnet.

- 3 Laden Sie die Installationsdatei für den Windows-Gast-Agent herunter und speichern Sie sie auf dem Laufwerk C Ihrer Referenzmaschine.

- Dateien für den Windows-Gast-Agent (**32-Bit**)

- Dateien für den Windows-Gast-Agent (**64-Bit**)

- 4 Installieren Sie den Gast-Agent auf der Referenzmaschine.

- a Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie **Eigenschaften** aus.

- b Klicken Sie auf **Allgemein**.

- c Klicken Sie auf **Blockierung aufheben**.

- d Extrahieren Sie die Dateien.

Dadurch wird das Verzeichnis C:\VRMGuestAgent erstellt. Benennen Sie dieses Verzeichnis nicht um.

- 5 Konfigurieren Sie den Gast-Agent zum Kommunizieren mit dem Manager Service.

- a Öffnen Sie eine Eingabeaufforderung mit erweiterten Berechtigungen.

- b Navigieren Sie zu C:\VRMGuestAgent.

- c Konfigurieren Sie die vertrauenswürdige Kommunikation zwischen dem Gast-Agent und Ihrer Manager Service-Maschine.

Option	Beschreibung
<b>Lassen Sie zu, dass der Gast-Agent der ersten Maschine vertraut, mit der er verbunden wird.</b>	Es ist keine Konfiguration erforderlich.
<b>Installieren Sie die vertrauenswürdige PEM-Datei manuell.</b>	Speichern Sie die PEM-Datei der Manager Service-Maschine im Verzeichnis C:\VRMGuestAgent\.

- d Führen Sie `win-service -i -h Manager_Service_Hostname_fdqn:portnumber -p ssl` aus. Die Standardportnummer für den Manager Service ist 443.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts von Manager Service ein. Beispielsweise <code>win-service -i -h load_balancer_manager_service.mycompany.com:443 -p ssl</code> .
<b>Wenn Sie keinen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Manager Service-Maschine ein. Beispielsweise <code>win-service -i -h manager_service_machine.mycompany.com:443 -p ssl</code> .
<b>Wenn Sie ein Amazon-System-Image vorbereiten</b>	Sie müssen angeben, dass Sie Amazon verwenden. Beispielsweise <code>win-service -i -h manager_service_machine.mycompany.com:443:443 -p ssl -c ec2</code>

Der Name des Windows-Diensts lautet VCACGuestAgentService. Das Installationsprotokoll VCAC-GuestAgentService.log finden Sie unter C:\VRMGuestAgent.

## Weiter

Konvertieren Sie Ihre Referenzmaschine in eine Vorlage zum Klonen, ein Amazon-Maschinen-Image oder einen Snapshot, welche Ihre IaaS-Architekten beim Erstellen von Blueprints verwenden können.

## Konfigurieren des Vertrauensverhältnisses zu einem Server für den Windows-Gast-Agent

Die sicherste Methode ist die manuelle Installation der vertrauenswürdigen PEM-Datei für jede Vorlage, die den Gast-Agent verwendet. Sie können aber auch erlauben, dass der Gast-Agent der ersten Maschine vertraut, mit der eine Verbindung hergestellt wird.

Die Installation der PEM-Datei für den vertrauenswürdigen Server in jeder Vorlage, die den Gast-Agent verwendet, ist die sicherste Methode. Aus Sicherheitsgründen sucht der Gast-Agent nicht nach einem Zertifikat, wenn bereits eine PEM-Datei im Verzeichnis VRMGuestAgent vorhanden ist. Wenn die Serverzertifikate geändert werden, müssen Sie Ihre Vorlagen unter Verwendung der neuen PEM-Dateien manuell neu erstellen.

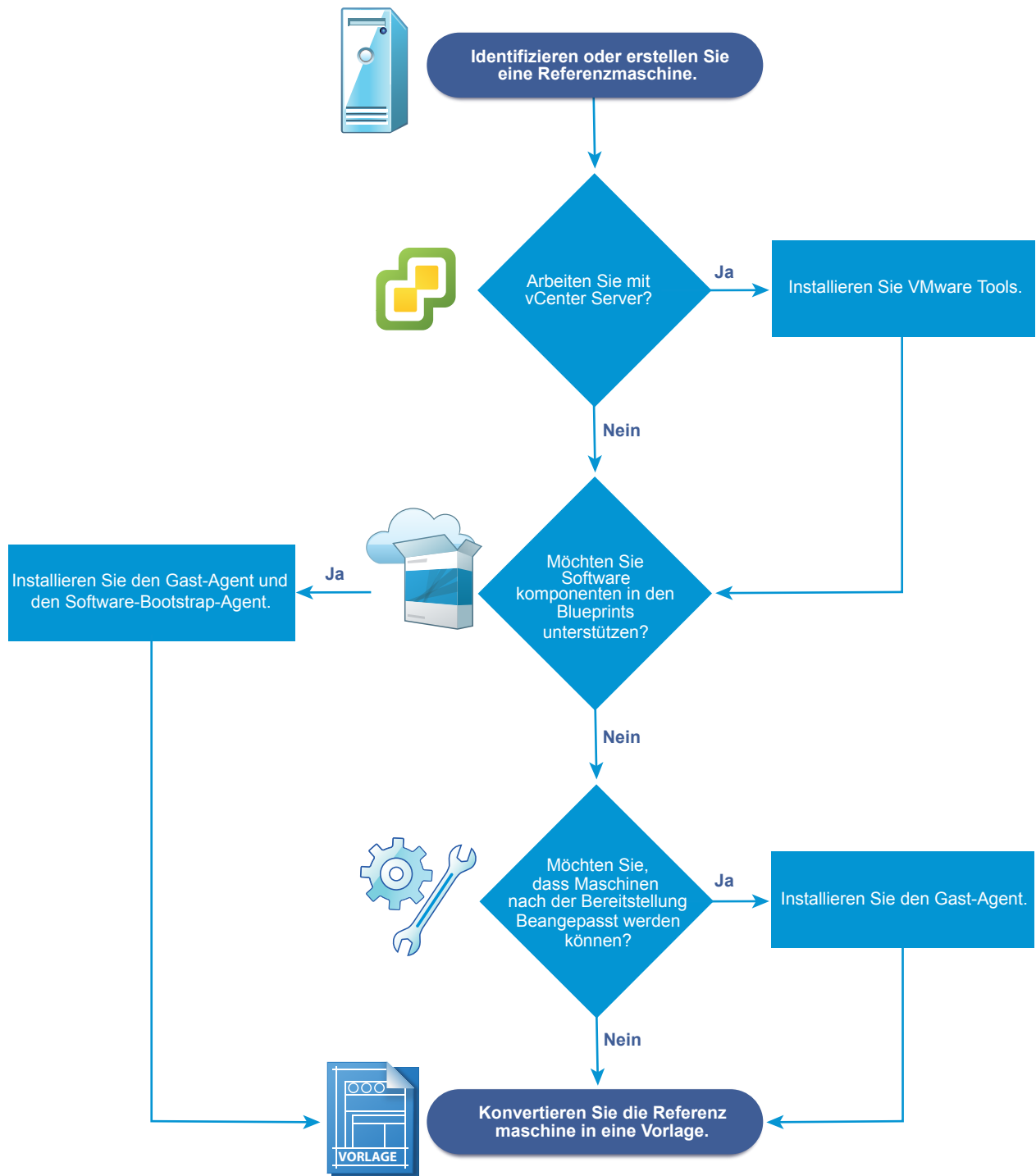
Sie können auch den Gast-Agent so konfigurieren, dass die vertrauenswürdige PEM-Datei bei der ersten Verwendung aufgefüllt wird. Dies ist zwar nicht so sicher wie die manuelle Installation der PEM-Dateien für jede Vorlage, allerdings flexibler für Umgebungen, in denen möglicherweise eine einzige Vorlage für mehrere Server verwendet wird. Damit der Gast-Agent dem ersten Server, mit dem eine Verbindung hergestellt wird, vertraut, erstellen Sie eine Vorlage ohne PEM-Dateien im Verzeichnis VRMGuestAgent. Der

Gast-Agent füllt die PEM-Datei auf, wenn erstmalig eine Verbindung mit einem Server hergestellt wird. Die Vorlage vertraut immer dem ersten System, mit dem eine Verbindung hergestellt wird. Aus Sicherheitsgründen sucht der Gast-Agent nicht nach einem Zertifikat, wenn bereits eine PEM-Datei im Verzeichnis VRMGuestAgent vorhanden ist. Wenn das Serverzertifikat geändert wird, müssen Sie die PEM-Datei aus dem Verzeichnis VRMGuestAgent entfernen. Der Gast-Agent installiert die neue PEM-Datei, wenn das nächste Mal eine Verbindung mit dem Server hergestellt wird.

## **Checkliste für das Vorbereiten für die Bereitstellung durch Klonen**

Sie müssen einige Vorbereitungen außerhalb von vRealize Automation für das Erstellen der Vorlage und der Anpassungsobjekte durchführen, die zum Klonen von Linux- und Windows-VMs verwendet werden.

Beim Klonen ist eine Vorlage erforderlich, von der geklont wird. Diese wird von einer Referenzmaschine erstellt.



Wenn Sie eine Windows-Maschine durch Klonen bereitstellen, können Sie die bereitgestellte Maschine zu einer Active Directory-Domäne nur wie folgt hinzufügen: Verwenden Sie die Anpassungsspezifikation von vCenter Server oder fügen Sie ein Profil für das Gastbetriebssystem mit Ihrer SCVMM-Vorlage hinzu. Maschinen, die durch Klonen bereitgestellt werden, können bei der Bereitstellung nicht in einem Active Directory-Container positioniert werden. Dies muss manuell nach der Bereitstellung ausgeführt werden.



**Tabelle 1-7. Checkliste für das Vorbereiten für die Bereitstellung durch Klonen**

Aufgabe	Speicherort	Details
<input type="checkbox"/> Bestimmen oder erstellen Sie die Referenzmaschine.	Hypervisor	Informieren Sie sich in der von Ihrem Hypervisor bereitgestellten Dokumentation.
<input type="checkbox"/> (Optional) Wenn Ihre Klonvorlage Software-Komponenten unterstützen soll, installieren Sie den vRealize Automation-Gast-Agent und den Software-Bootstrap-Agent auf Ihrer Referenzmaschine.	Referenzmaschine	Weitere Informationen zu Windows-Referenzmaschinen finden Sie unter <a href="#">Vorbereiten einer Windows-Referenzmaschine für die Unterstützung von Software</a> .  Weitere Informationen zu Linux-Referenzmaschinen finden Sie unter <a href="#">Vorbereiten einer Linux-Referenzmaschine für die Unterstützung von Software</a> .
<input type="checkbox"/> (Optional) Wenn Ihre Klonvorlage keine Software-Komponenten unterstützen muss, Sie aber die Möglichkeit haben möchten, bereitgestellte Maschinen anzupassen, installieren Sie den vRealize Automation-Gast-Agent auf Ihrer Referenzmaschine.	Referenzmaschine	Siehe <a href="#">Verwenden des vRealize Automation-Gast-Agent bei der Bereitstellung</a> .
<input type="checkbox"/> Wenn Sie in einer vCenter Server-Umgebung arbeiten, installieren Sie VMware Tools auf der Referenzmaschine.	vCenter Server	Weitere Informationen finden Sie in der VMware Tools-Dokumentation.
<input type="checkbox"/> Verwenden Sie die Referenzmaschine zum Erstellen einer Vorlage für das Klonen.	Hypervisor	Die Referenzmaschine kann ein- oder ausgeschaltet sein. Wenn Sie in vCenter Server klonen, können Sie eine Referenzmaschine direkt verwenden, ohne eine Vorlage zu erstellen.  Informieren Sie sich in der von Ihrem Hypervisor bereitgestellten Dokumentation.
<input type="checkbox"/> Erstellen Sie das Anpassungsobjekt zum Konfigurieren von geklonten Maschinen, indem Informationen zum Dienstprogramm für die Systemvorbereitung oder eine Linux-Anpassung angewendet werden.	Hypervisor	Wenn Sie für Linux klonen, können Sie den Linux-Gast-Agent installieren und externe Anpassungsskripts bereitstellen, anstatt ein Anpassungsobjekt zu erstellen. Wenn Sie mit vCenter Server klonen, müssen Sie die Anpassungsspezifikation als das Anpassungsobjekt bereitstellen.  Informieren Sie sich in der von Ihrem Hypervisor bereitgestellten Dokumentation.
<input type="checkbox"/> Erfassen Sie die Informationen, die zum Erstellen von Blueprints erforderlich sind, die Ihre Vorlage klonen.	Erfassen Sie Informationen und übertragen Sie sie an Ihre IaaS-Architekturen.	Siehe <a href="#">Arbeitsblatt zur virtuellen Bereitstellung durch Klonen</a> .

## Arbeitsblatt zur virtuellen Bereitstellung durch Klonen

Füllen Sie das Wissenstransfer-Arbeitsblatt aus, um Informationen zu Vorlage, Anpassungen und benutzerdefinierten Eigenschaften zu erfassen, die zum Erstellen von Klon-Blueprints für die in Ihrer Umgebung vorbereiteten Vorlagen erforderlich sind. Nicht alle diese Informationen sind für jede Implementierung erforderlich. Verwenden Sie dieses Arbeitsblatt als Leitfaden, oder kopieren Sie die Arbeitsblatttabellen und fügen sie zur Bearbeitung in ein Textverarbeitungstool ein.

## Erforderliche Vorlagen- und Reservierungsinformationen

**Tabelle 1-8. Arbeitsblatt für Vorlagen- und Reservierungsinformationen**

Erforderliche Informationen	Mein Wert	Details
Vorlagenname		
Reservierungen, in denen die Vorlage verfügbar ist, bzw. anwendbare Reservierungsrichtlinie		Um Fehler bei der Bereitstellung zu vermeiden, stellen Sie sicher, dass die Vorlage in allen Reservierungen verfügbar ist, oder erstellen Sie Reservierungsrichtlinien, mit denen Architekten den Blueprint auf Reservierungen beschränken können, für die die Vorlage verfügbar ist.
(nur vSphere) Klontyp, der für diese Vorlage angefordert wird		<ul style="list-style-type: none"> <li>■ Klonen</li> <li>■ Verknüpfter Klon</li> <li>■ NetApp FlexClone</li> </ul>
Name der Anpassungsspezifikation (erforderlich für das Klonen mit statischen IP-Adressen)		Sie können keine Anpassungen von Windows-Maschinen ohne ein Anpassungsspezifikationsobjekt durchführen.
(nur SCVMM) ISO-Name		
(nur SCVMM) Virtuelle Festplatte		
(nur SCVMM) Hardwareprofil zum Anhängen an bereitgestellte Maschinen		

## Erforderliche Eigenschaftsgruppen

Sie können die Abschnitte mit Informationen zu benutzerdefinierten Eigenschaften des Arbeitsblatts ausfüllen oder Eigenschaftsgruppen erstellen und Architekten auffordern, Ihre Eigenschaftsgruppen anstelle zahlreicher einzelner benutzerdefinierter Eigenschaften ihren Blueprints hinzuzufügen.

## Erforderliches vCenter Server -Betriebssystem

Sie müssen die benutzerdefinierte Eigenschaft des Gastbetriebssystems für die vCenter Server-Bereitstellung angeben.

**Tabelle 1-9. vCenter Server -Betriebssystem**

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
VMware.VirtualCenter.Operating-System		Gibt die Version des vCenter Server-Gastbetriebssystems (VirtualMachine-GuestOsIdentifizier) an, mit der vCenter Server die Maschine erstellt. Diese Betriebssystemversion muss mit der Betriebssystemversion übereinstimmen, die auf der bereitgestellten Maschine installiert werden soll. Administratoren können Eigenschaftsgruppen mithilfe mehrerer Eigenschaftensätze erstellen, wie beispielsweise VMware[OS_Version]Properties. Diese Eigenschaftensätze sind vordefiniert und enthalten die korrekten Werte für VMware.VirtualCenter.OperatingSystem. Diese Eigenschaft dient für die virtuelle Bereitstellung.

### Visual Basic-Skriptinformationen

Wenn Sie vRealize Automation für die Ausführung Ihrer benutzerdefinierten Visual Basic-Skripts als zusätzliche Schritte im Maschinenlebenszyklus konfiguriert haben, müssen Sie Informationen zu den Skripten im Blueprint einschließen.

**Hinweis** Ein Fabric-Administrator kann eine Eigenschaftsgruppe durch Verwendung der Eigenschaftensätze ExternalPreProvisioningVbScript und ExternalPostProvisioningVbScript erstellen, um diese erforderlichen Informationen bereitzustellen. Auf diese Weise können Blueprint-Architekten diese Informationen richtig zu ihren Blueprints hinzufügen.

**Tabelle 1-10. Visual Basic-Skriptinformationen**

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
ExternalPreProvisioningVbScript		Führen Sie ein Skript vor der Bereitstellung aus. Geben Sie den vollständigen Pfad zum Skript an, einschließlich Dateiname und Erweiterung. <i>%System Drive %Programme (x86)\VMware\vCAC Agents\EPI_Agents\Scripts\Send-Email.vbs</i> .
ExternalPostProvisioningVbScript		Führen Sie ein Skript nach der Bereitstellung aus. Geben Sie den vollständigen Pfad zum Skript an, einschließlich Dateiname und Erweiterung. <i>%System Drive %Programme (x86)\VMware\vCAC Agents\EPI_Agents\Scripts\Send-Email.vbs</i>

## Informationen zum Linux-Gast-Agent-Anpassungsskript

Wenn Sie die Linux-Vorlage für die Verwendung des Gast-Agents zur Ausführung von Anpassungsskripts konfiguriert haben, müssen Sie Informationen zu den Skripten in den Blueprint einschließen.

**Tabelle 1-11. Arbeitsblatt für Informationen zum Linux-Gast-Agent-Anpassungsskript**

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
Linux.ExternalScript.Name		Gibt den Namen eines optionalen Anpassungsskripts an, wie beispielsweise <code>config.sh</code> , das der Linux-Gast-Agent nach der Installation des Betriebssystems ausführt. Diese Eigenschaft ist für über Vorlagen geklonte Linux-Maschinen verfügbar, auf denen der Linux-Agent installiert ist.  Wenn Sie ein externes Skript angeben, müssen Sie auch mithilfe der Eigenschaften <code>Linux.ExternalScript.LocationType</code> und <code>Linux.ExternalScript.ScriptPath</code> dessen Speicherort definieren.
Linux.ExternalScript.LocationType		Gibt den Speicherorttyp des in der Eigenschaft <code>Linux.ExternalScript.ScriptName</code> benannten Anpassungsskripts an. Mögliche Werte sind „local“ oder „nfs“.  Darüber hinaus müssen Sie mit der Eigenschaft <code>Linux.ExternalScript.ScriptPath</code> den Skriptenspeicherort angeben. Wenn der Speicherorttyp „nfs“ lautet, sollten Sie auch die Eigenschaft <code>Linux.ExternalScript.Server</code> verwenden.
Linux.ExternalScript.Server		Gibt den Namen des NFS-Servers an, wie beispielsweise „lab-ad.lab.local“, auf dem das in <code>Linux.ExternalScript.ScriptName</code> angegebene externe Linux-Anpassungsskript gespeichert ist.
Linux.ExternalScript.Path		Gibt den lokalen Pfad zum Linux-Anpassungsskript oder den Exportpfad zur Linux-Anpassung auf dem NFS-Server an. Dieser Wert muss mit einem Schrägstrich beginnen und darf den Dateinamen nicht enthalten, wie beispielsweise <code>/scripts/linux/config.sh</code> .

## Weitere benutzerdefinierte Gast-Agent-Eigenschaften

Wenn Sie den Gast-Agent auf Ihrer Referenzmaschine installiert haben, können Sie benutzerdefinierte Eigenschaften verwenden, um Maschinen nach der Bereitstellung weiter anzupassen.

**Tabelle 1-12. Arbeitsblatt für benutzerdefinierte Eigenschaften zum Anpassen geklonter Maschinen mit einem Gast-Agent**

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
VirtualMachine.Admin.AddOwnerToAdmins		Legen Sie diese Eigenschaft auf „True“ (Standardwert) fest, um den Besitzer der Maschine, gemäß der Eigenschaft VirtualMachine.Admin.Owner, zur lokalen Administratorengruppe auf der Maschine hinzuzufügen.
VirtualMachine.Admin.AllowLogin		Legen Sie diese Eigenschaft auf „True“ (Standardwert) fest, um den Maschinenbesitzer zur Gruppe der lokalen Remotedesktopbenutzer, gemäß der Eigenschaft VirtualMachine.Admin.Owner, hinzuzufügen.
VirtualMachine.Admin.UseGuestAgent		Wenn der Gast-Agent als Dienst in einer Vorlage für das Klonen installiert ist, legen Sie diese Eigenschaft im Maschinen-Blueprint auf „True“ fest, um den Gast-Agent-Dienst auf Maschinen, die anhand dieser Vorlage geklont werden, zu aktivieren. Beim Starten der Maschine wird der Gast-Agent-Dienst gestartet. Legen Sie diese Eigenschaft auf „False“ fest, um den Gast-Agent zu deaktivieren. Mit der Einstellung „False“ verwendet der erweiterte Klon-Workflow den Gast-Agent nicht für Aufgaben des Gastbetriebssystems, wodurch dessen Funktionalität auf VMwareClone-Workflow reduziert wird. Wenn diese Option nicht angegeben ist oder auf einen anderen Wert als „False“ festgelegt ist, sendet der erweiterte Klon-Workflow Arbeitselemente an den Gast-Agent.
VirtualMachine.DiskN.Active		Legen Sie diese Eigenschaft auf „True“ (Standardwert) fest, um anzugeben, dass die Festplatte <i>N</i> der Maschine aktiv ist. Legen Sie diese Eigenschaft auf „False“ fest, um anzugeben, dass die Festplatte <i>N</i> der Maschine nicht aktiv ist.

**Tabelle 1-12. Arbeitsblatt für benutzerdefinierte Eigenschaften zum Anpassen geklonter Maschinen mit einem Gast-Agent (Fortsetzung)**

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
VirtualMachine.DiskN.Size		Definiert die Größe der Festplatte <i>N</i> in GB. Um beispielsweise eine Größe von 150 GB für die Festplatte G festzulegen, definieren Sie die benutzerdefinierte Eigenschaft VirtualMachine.Disk0.Size und geben den Wert „150“ ein. Festplatten müssen sequenziell nummeriert werden. Standardmäßig weist eine Maschine eine Festplatte auf, auf die mit VirtualMachine.Disk0.Size verwiesen wird. Dabei wird die Größe durch den Speicherwert im Blueprint angegeben, über den die Maschine bereitgestellt wird. Der Speicherwert in der Blueprint-Benutzeroberfläche überschreibt den Wert in der Eigenschaft VirtualMachine.Disk0.Size. Die Eigenschaft VirtualMachine.Disk0.Size ist aufgrund ihrer Beziehung mit der Speicheroption im Blueprint nicht als benutzerdefinierte Eigenschaft verfügbar. Durch Angabe von VirtualMachine.Disk1.Size, VirtualMachine.Disk2.Size usw. können weitere Festplatten hinzugefügt werden. VirtualMachine.Admin.TotalDiskUsage stellt stets die Summe der Eigenschaften .DiskN.Size zuzüglich der zugeordneten Größe für VMware.Memory.Reservation dar.
VirtualMachine.DiskN.Label		Gibt die Bezeichnung für die Festplatte <i>N</i> einer Maschine an. Für die Festplattenbezeichnung sind maximal 32 Zeichen zulässig. Festplatten müssen sequenziell nummeriert werden. Bei Verwendung in Verbindung mit einem Gast-Agent wird hiermit die Bezeichnung der Festplatte <i>N</i> einer Maschine im Gastbetriebssystem angegeben.

**Tabelle 1-12. Arbeitsblatt für benutzerdefinierte Eigenschaften zum Anpassen geklonter Maschinen mit einem Gast-Agent (Fortsetzung)**

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
VirtualMachine.DiskN.Letter		Gibt den Laufwerkbuchstaben oder Einhängpunkt der Festplatte N einer Maschine an. Der Standardwert ist C. Um beispielsweise den Buchstaben D für die Festplatte 1 anzugeben, definieren Sie die benutzerdefinierte Eigenschaft als VirtualMachine.Disk1.Letter und geben Sie den Wert „D“ ein. Festplatten müssen sequenziell nummeriert werden. Bei Verwendung in Verbindung mit einem Gast-Agent gibt dieser Wert den Laufwerkbuchstaben oder Einhängpunkt an, unter dem die zusätzliche Festplatte N vom Gast-Agent im Gastbetriebssystem gemountet wird.
VirtualMachine.Admin.Customize-GuestOSDelay		Gibt an, wie lange nach Abschluss der Anpassung gewartet werden soll, bevor die Anpassung des Gastbetriebssystems gestartet wird. Für diesen Wert ist das Format HH:MM:SS erforderlich. Wenn dieser Wert nicht festgelegt wird, wird der Standardwert von einer Minute (00:01:00) verwendet. Wenn Sie diese benutzerdefinierte Eigenschaft nicht angeben, schlägt die Bereitstellung möglicherweise fehl, falls die virtuelle Maschine neu gestartet wird, bevor Arbeitselemente des Gast-Agents abgeschlossen sind.
VirtualMachine.Customize.Wait-Complete		Legen Sie diese Eigenschaft auf „True“ fest, um zu verhindern, dass der Bereitstellungsworkflow Arbeitselemente an den Gast-Agent sendet, bevor alle Anpassungen abgeschlossen wurden.
VirtualMachine.SoftwareN.Name		Gibt den beschreibenden Namen der Softwareanwendung N oder eines Skripts an, die bzw. das während der Bereitstellung installiert oder ausgeführt werden soll. Dies ist eine optionale und rein informative Eigenschaft. Sie hat keine echte Funktion für den erweiterten Klon-Workflow oder den Gast-Agent, ist aber hilfreich für die benutzerdefinierte Softwareauswahl in einer Benutzeroberfläche oder für Berichte zur Softwarenutzung.

**Tabelle 1-12. Arbeitsblatt für benutzerdefinierte Eigenschaften zum Anpassen geklonter Maschinen mit einem Gast-Agent (Fortsetzung)**

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
VirtualMachine.SoftwareN.Script-Path		<p>Gibt den vollständigen Pfad zum Installationskript einer Anwendung an. Bei dem Pfad muss es sich um einen gültigen absoluten Pfad wie er im Gastbetriebssystem angezeigt wird handeln und er muss den Namen der Skriptdatei enthalten.</p> <p>Sie können benutzerdefinierte Eigenschaftswerte als Parameter an das Skript übergeben, indem Sie <i>{CustomPropertyName}</i> in der Pfadzeichenfolge einfügen. Angenommen, Sie haben eine benutzerdefinierte Eigenschaft <i>ActivationKey</i> mit dem Wert 1234. In diesem Fall lautet der Skriptpfad <code>D:\InstallApp.bat -key {ActivationKey}</code>. Der Gast-Agent führt den Befehl <code>D:\InstallApp.bat -key 1234</code> aus. Ihre Skriptdatei kann dann so programmiert werden, dass dieser Wert akzeptiert und verwendet wird.</p>
VirtualMachine.SoftwareN.ISOName		<p>Gibt den Pfad und den Dateinamen der ISO-Datei in Bezug auf das Stammverzeichnis des Datenspeichers an. Das Format lautet <i>/Ordnername/Unterordnername/Dateiname.iso</i>. Wenn kein Wert angegeben wird, wird das ISO-Image nicht gemountet.</p>
VirtualMachine.SoftwareN.ISOLocation		<p>Gibt den Speicherpfad an, der die ISO-Imagedatei enthält, die von der Anwendung oder dem Skript verwendet werden soll. Formatieren Sie den in der Hostreservierung angezeigten Pfad, wie beispielsweise <code>netapp-1:it_nfs_1</code>. Wenn kein Wert angegeben wird, wird das ISO-Image nicht gemountet.</p>

## Benutzerdefinierte Netzwerkeigenschaften

Wenn Sie keine Integration in NSX vornehmen, können Sie dennoch eine Konfiguration für bestimmte Netzwerkgeräte auf einer Maschine angeben, indem Sie benutzerdefinierte Eigenschaften verwenden.



**Tabelle 1-13. Konfiguration benutzerdefinierter Eigenschaften für Netzwerke**

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
<code>VirtualMachine.NetworkN.Address</code>		Gibt die IP-Adresse des Netzwerkgeräts <i>N</i> in einer mit einer statischen IP-Adresse bereitgestellten Maschine an.
<code>VirtualMachine.NetworkN.MacAddressType</code>		<p>Gibt an, ob die MAC-Adresse des Netzwerkgeräts <i>N</i> generiert wird („generated“) oder benutzerdefiniert („static“) ist. Diese Eigenschaft ist für das Klonen verfügbar.</p> <p>Der Standardwert lautet „generated“. Mit dem Wert „static“ müssen Sie auch <code>VirtualMachine.NetworkN.MacAddress</code> verwenden, um die MAC-Adresse anzugeben.</p> <p>Die benutzerdefinierten Eigenschaften <code>VirtualMachine.NetworkN</code> gelten speziell für einzelne Blueprints und Maschinen. Wenn eine Maschine angefordert wird, erfolgt die Zuteilung der Netzwerk- und IP-Adresse vor der Zuweisung der Maschine zu einer Reservierung. Es ist nicht garantiert, dass Blueprints einer bestimmten Reservierung zugeteilt werden, weshalb Sie diese Eigenschaft nicht für eine Reservierung verwenden sollten.</p>

**Tabelle 1-13. Konfiguration benutzerdefinierter Eigenschaften für Netzwerke (Fortsetzung)**

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
VirtualMachine.NetworkN.MacAddress		<p>Gibt die MAC-Adresse des Netzwerkgeräts <i>N</i> an. Diese Eigenschaft ist für das Klonen verfügbar.</p> <p>Wenn VirtualMachine.NetworkN.MacAddressType den Wert „generated“ hat, enthält diese Eigenschaft die generierte Adresse.</p> <p>Wenn VirtualMachine.NetworkN.MacAddressType den Wert „static“ hat, enthält diese Eigenschaft die MAC-Adresse. Für virtuelle Maschinen, die auf ESX Server-Hosts bereitgestellt werden, muss die Adresse innerhalb des von VMware angegebenen Bereichs liegen. Weitere Informationen finden Sie in der vSphere-Dokumentation.</p> <p>Die benutzerdefinierten Eigenschaften VirtualMachine.Network<i>N</i> gelten speziell für einzelne Blueprints und Maschinen. Wenn eine Maschine angefordert wird, erfolgt die Zuteilung der Netzwerk- und IP-Adresse vor der Zuweisung der Maschine zu einer Reservierung. Es ist nicht garantiert, dass Blueprints einer bestimmten Reservierung zugeteilt werden, weshalb Sie diese Eigenschaft nicht für eine Reservierung verwenden sollten.</p>

**Tabelle 1-13. Konfiguration benutzerdefinierter Eigenschaften für Netzwerke (Fortsetzung)**

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
<code>VirtualMachine.NetworkN.Name</code>		<p>Gibt den Namen des Netzwerks an, mit dem eine Verbindung hergestellt werden soll. Beispielsweise das Netzwerkgerät <i>N</i>, mit dem eine Maschine verbunden wird. Dies entspricht einer Netzwerkkarte (Network Interface Card, NIC).</p> <p>Standardmäßig wird ein Netzwerk aus den in der Reservierung verfügbaren Netzwerkpfaden zugewiesen, in denen die Maschine bereitgestellt wird. Siehe auch <code>VirtualMachine.NetworkN.AddressType</code>.</p> <p>Sie können sicherstellen, dass ein Netzwerkgerät mit einem bestimmten Netzwerk verbunden wird, indem Sie für diese Eigenschaft den Namen eines Netzwerks in einer verfügbaren Reservierung festlegen. Wenn Sie beispielsweise als Eigenschaften <i>N</i>= 0 und 1 festlegen, erhalten Sie zwei NICs und deren zugewiesenen Wert, vorausgesetzt das Netzwerk ist in der zugeordneten Reservierung ausgewählt.</p> <p>Die benutzerdefinierten Eigenschaften <code>VirtualMachine.NetworkN</code> gelten speziell für Blueprints und Maschinen. Wenn eine Maschine angefordert wird, erfolgt die Zuteilung der Netzwerk- und IP-Adresse vor der Zuweisung der Maschine zu einer Reservierung. Es ist nicht garantiert, dass Blueprints einer bestimmten Reservierung zugeteilt werden, weshalb Sie diese Eigenschaft nicht für eine Reservierung verwenden sollten.</p> <p>Sie können diese Eigenschaft zu einer vCloud Air- oder vCloud Director-Maschinenkomponente in einem Blueprint hinzufügen.</p>

**Tabelle 1-13. Konfiguration benutzerdefinierter Eigenschaften für Netzwerke (Fortsetzung)**

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
VirtualMachine.NetworkN.PortID		<p>Gibt die für das Netzwerkgerät <i>N</i> zu verwendende Port-ID an, wenn eine dvPort-Gruppe mit einem vSphere Distributed Switch verwendet wird.</p> <p>Die benutzerdefinierten Eigenschaften VirtualMachine.NetworkN gelten speziell für einzelne Blueprints und Maschinen. Wenn eine Maschine angefordert wird, erfolgt die Zuteilung der Netzwerk- und IP-Adresse vor der Zuweisung der Maschine zu einer Reservierung. Es ist nicht garantiert, dass Blueprints einer bestimmten Reservierung zugeteilt werden, weshalb Sie diese Eigenschaft nicht für eine Reservierung verwenden sollten.</p>
VirtualMachine.NetworkN.ProfileName		<p>Gibt den Namen eines Netzwerkprofils an, aus dem dem Netzwerkgerät <i>N</i> eine statische IP-Adresse zugewiesen werden soll oder aus dem der statische IP-Adressbereich bezogen werden soll, der dem Netzwerkgerät <i>N</i> einer geklonten Maschine zugewiesen werden kann. Dabei steht <i>N</i>=0 für das erste Gerät, 1 für das zweite Gerät usw.</p> <p>Wenn Sie die Eigenschaft VirtualMachine.NetworkN.ProfileName verwenden, wird mithilfe des Netzwerkprofils, auf das verwiesen wird, eine IP-Adresse zugeteilt. Die bereitgestellte Maschine wird jedoch jedem in der Reservierung ausgewählten Netzwerk mithilfe der Round-Robin-Methode hinzugefügt.</p>

**Tabelle 1-13. Konfiguration benutzerdefinierter Eigenschaften für Netzwerke (Fortsetzung)**

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
<ul style="list-style-type: none"> <li>■ VirtualMachine.Net-workN.SubnetMask</li> <li>■ VirtualMachine.NetworkN.Gateway</li> <li>■ VirtualMachine.Net-workN.PrimaryDns</li> <li>■ VirtualMachine.NetworkN.SecondaryDns</li> <li>■ VirtualMachine.Net-workN.PrimaryWins</li> <li>■ VirtualMachine.NetworkN.SecondaryWins</li> <li>■ VirtualMachine.Net-workN.DnsSuffix</li> <li>■ VirtualMachine.Net-workN.DnsSearchSuffixes</li> </ul>		<p>Durch Anfügen eines Namens können Sie mehrere Versionen einer benutzerdefinierten Eigenschaft erstellen. Beispielsweise werden mit den folgenden Eigenschaften Lastausgleichspools aufgelistet, die zur allgemeinen Verwendung und für Maschinen mit hohen, mäßigen und niedrigen Leistungsanforderungen eingerichtet sind:</p> <ul style="list-style-type: none"> <li>■ VCNS.LoadBalancerEdgePool.Names</li> <li>■ VCNS.LoadBalancerEdgePool.Names.moderate</li> <li>■ VCNS.LoadBalancerEdgePool.Names.high</li> <li>■ VCNS.LoadBalancerEdgePool.Names.low</li> </ul> <p>Konfiguriert Attribute des in VirtualMachine.NetworkN.ProfileName angegebenen Netzwerkprofils.</p>
VCNS.LoadBalancerEdgePool.Names.name		<p>Gibt die vCloud Networking and Security-Lastausgleichspools an, denen die virtuelle Maschine während der Bereitstellung zugewiesen wird. Die virtuelle Maschine wird allen Dienstports von allen angegebenen Pools zugewiesen. Bei dem Wert handelt es sich um einen <i>Edge/Pool</i>-Namen oder eine durch Kommas getrennte Liste von <i>Edge/Pool</i>-Namen. Bei Namen wird die Groß- und Kleinschreibung berücksichtigt.</p> <p>Durch Anfügen eines Namens können Sie mehrere Versionen einer benutzerdefinierten Eigenschaft erstellen. Beispielsweise werden mit den folgenden Eigenschaften Lastausgleichspools aufgelistet, die zur allgemeinen Verwendung und für Maschinen mit hohen, mäßigen und niedrigen Leistungsanforderungen eingerichtet sind:</p> <ul style="list-style-type: none"> <li>■ VCNS.LoadBalancerEdgePool.Names</li> <li>■ VCNS.LoadBalancerEdgePool.Names.moderate</li> <li>■ VCNS.LoadBalancerEdgePool.Names.high</li> <li>■ VCNS.LoadBalancerEdgePool.Names.low</li> </ul>

**Tabelle 1-13. Konfiguration benutzerdefinierter Eigenschaften für Netzwerke (Fortsetzung)**

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
VCNS.SecurityGroup.Names.name		<p>Gibt die vCloud Networking and Security-Sicherheitsgruppe(n) an, der bzw. denen die virtuelle Maschine während der Bereitstellung zugewiesen wird. Bei dem Wert handelt es sich um einen Sicherheitsgruppennamen oder eine durch Kommas getrennte Liste von Sicherheitsgruppennamen. Bei Namen wird die Groß- und Kleinschreibung berücksichtigt.</p> <p>Durch Anfügen eines Namens können Sie mehrere Versionen der Eigenschaft erstellen, die separat oder kombiniert verwendet werden können. Beispielsweise können mit den folgenden Eigenschaften Sicherheitsgruppen aufgelistet werden, die zur allgemeinen Verwendung, für die Vertriebsmitarbeiter und für den Support gedacht sind:</p> <ul style="list-style-type: none"> <li>■ VCNS.SecurityGroup.Names</li> <li>■ VCNS.SecurityGroup.Names.sales</li> <li>■ VCNS.SecurityGroup.Names.support</li> </ul>
VCNS.SecurityTag.Names.name		<p>Gibt das vCloud Networking and Security-Sicherheitstag bzw. die -Sicherheitstags an, dem bzw. denen die virtuelle Maschine während der Bereitstellung zugeordnet wird. Bei dem Wert handelt es sich um einen Sicherheits-Tag-Namen oder eine durch Kommas getrennte Liste von Sicherheits-Tag-Namen. Bei Namen wird die Groß- und Kleinschreibung berücksichtigt.</p> <p>Durch Anfügen eines Namens können Sie mehrere Versionen der Eigenschaft erstellen, die separat oder kombiniert verwendet werden können. Beispielsweise können mit den folgenden Eigenschaften Sicherheits-Tags aufgelistet werden, die zur allgemeinen Verwendung, für die Vertriebsmitarbeiter und für den Support gedacht sind:</p> <ul style="list-style-type: none"> <li>■ VCNS.SecurityTag.Names</li> <li>■ VCNS.SecurityTag.Names.sales</li> <li>■ VCNS.SecurityTag.Names.support</li> </ul>

## Vorbereiten für die vCloud Air - und vCloud Director - Bereitstellung

Um die Bereitstellung von vCloud Air- und vCloud Director-Maschinen unter Verwendung von vRealize Automation vorzubereiten, müssen Sie das virtuelle Datacenter der Organisation mit Vorlagen und Anpassungsobjekten konfigurieren.

Um vCloud Air- und vCloud Director-Ressourcen unter Verwendung von vRealize Automation bereitzustellen, erfordert die Organisation eine Vorlage zum Klonen, die aus mindestens einer Maschinenressource besteht.

Vorlagen, die für Organisationen freizugeben sind, müssen öffentlich sein. Nur reservierte Vorlagen sind für vRealize Automation als Klon-Quelle verfügbar.

---

**Hinweis** Wenn Sie durch Klonen von einer Vorlage einen Blueprint erstellen, wird der eindeutige Bezeichner dieser Vorlage dem Blueprint zugeordnet. Wenn der Blueprint im vRealize Automation-Katalog veröffentlicht und in den Vorgängen für die Bereitstellung und Datenerfassung verwendet wird, wird die zugeordnete Vorlage erkannt. Wenn Sie die Vorlage in vCloud Air oder vCloud Director löschen, schlägt die nachfolgende vRealize Automation-Bereitstellung und -Datenerfassung fehl, da die zugeordnete Vorlage nicht mehr vorhanden ist. Anstatt eine Vorlage zu löschen und neu zu erstellen, um beispielsweise eine aktualisierte Version hochzuladen, ersetzen Sie die Vorlage unter Verwendung des Vorgangs zum Ersetzen von Vorlagen für vCloud Air vCloud Director. Durch das Verwenden von vCloud Air oder vCloud Director zum Ersetzen der Vorlage (statt Löschen und Neuerstellen der Vorlage) wird der eindeutige Bezeichner der Vorlage nicht verändert und ermöglicht, dass die Bereitstellung und Datenerfassung weiterhin funktionieren.

---

vRealize Automation setzt voraus, dass der veröffentlichte Katalog für alle vCloud Director-Organisationen freigegeben ist. Die Datenerfassung schlägt fehl, wenn der veröffentlichte Katalog nicht für alle vCloud Director-Organisationen freigegeben ist.

Der folgende Überblick zeigt die Schritte, die Sie ausführen müssen, bevor vRA zum Erstellen von Endpoints und Definieren von Reservierungen und Blueprints verwendet wird. Weitere Informationen zu diesen administrativen Aufgaben finden Sie in der Produktdokumentation zu vCloud Air und vCloud Director.

- 1 Erstellen Sie in vCloud Air oder vCloud Director eine Vorlage zum Klonen und fügen Sie sie zum Organisationskatalog hinzu.
- 2 Verwenden Sie in vCloud Air oder vCloud Director die Vorlage zum Angeben von benutzerdefinierten Einstellungen wie z. B. Kennwörter, Domäne und Skripts für das Gastbetriebssystem auf jeder Maschine.

Sie können vRealize Automation zum Überschreiben einiger dieser Einstellungen verwenden.

Die Anpassung kann je nach Gastbetriebssystem der Ressource variieren.

- 3 Konfigurieren Sie in vCloud Air oder vCloud Director den Katalog, der für alle in der Organisation freigegeben wird.

Konfigurieren Sie in vCloud Air oder vCloud Director den Kontoadministratorzugriff auf zutreffende Organisationen, damit alle Benutzer und Gruppen in der Organisation Zugriff auf den Katalog haben. Ohne diese Freigabebezeichnung werden die Katalogvorlagen Endpoint- oder Blueprint-Architekten in vRealize Automation nicht angezeigt.

- 4 Erfassen Sie die folgenden Informationen, damit Sie sie zu Blueprints hinzufügen können:
  - Name der vCloud Air- oder vCloud Director-Vorlage.
  - Menge des für die Vorlage angegebenen Gesamtspeichers

## Vorbereiten für die Linux Kickstart-Bereitstellung

Die Linux Kickstart-Bereitstellung verwendet eine Konfigurationsdatei zum Automatisieren einer Linux-Installation auf einer neu bereitgestellten Maschine. Zum Vorbereiten für die Bereitstellung müssen Sie ein startbares ISO-Image und eine Kickstart- oder AutoYaST-Konfigurationsdatei erstellen.

Im Folgenden finden Sie eine grobe Übersicht über die erforderlichen Schritte für die Vorbereitung für die Linux Kickstart-Bereitstellung:

- 1 Stellen Sie sicher, dass ein DHCP-Server auf dem Netzwerk verfügbar ist. vRealize Automation kann Maschinen nicht durch die Verwendung von Linux Kickstart-Bereitstellung bereitstellen, es sei denn, DHCP ist verfügbar.
- 2 Bereiten Sie die Konfigurationsdatei vor. In der Konfigurationsdatei müssen Sie die Speicherorte des vRealize Automation-Servers und des Linux-Agent-Installationspakets angeben. Siehe [Vorbereiten der Konfigurationsbeispieldatei für Linux Kickstart](#).
- 3 Bearbeiten Sie die Datei `isolinux/isolinux.cfg` oder `loader/isolinux.cfg`, um den Namen und den Speicherort der Konfigurationsdatei und der entsprechenden Linux-Verteilungsquelle anzugeben.
- 4 Erstellen Sie das Boot-ISO-Image und speichern Sie es in dem für Ihre Virtualisierungsplattform erforderlichen Speicherort. Informationen über den erforderlichen Speicherort finden Sie in der von Ihrem Hypervisor bereitgestellten Dokumentation.
- 5 (Optional) Fügen Sie Anpassungsskripts hinzu.
  - a Informationen zum Angeben von Anpassungsskripts nach erfolgter Installation in der Konfigurationsdatei finden Sie unter [Angaben von benutzerdefinierten Skripten in einer kickstart-/autoYaST-Konfigurationsdatei](#).
  - b Informationen zum Aufrufen von Visual Basic-Skripten in Blueprints finden Sie unter [Checkliste für die Ausführung von Visual Basic-Skripten während der Bereitstellung](#).
- 6 Erfassen Sie die folgenden Informationen, damit Blueprint-Architekten sie zu ihren Blueprints hinzufügen können:
  - a Der Name und der Speicherort des ISO-Images.



- b Für vCenter Server-Integrationen die Version des vCenter Server-Gastbetriebssystems, mit der vCenter Server die Maschine erstellt.

**Hinweis** Sie können eine Eigenschaftsgruppe mit dem Eigenschaftensatz `BootIsoProperties` erstellen, um die erforderlichen ISO-Informationen hinzuzufügen. So können diese Informationen auf Blueprints ordnungsgemäß hinzugefügt werden.

## Vorbereiten der Konfigurationsbeispieldatei für Linux Kickstart

vRealize Automation stellt Beispielkonfigurationsdateien bereit, die Sie zum Anpassen an Ihre Anforderungen ändern und bearbeiten können. Es sind mehrere Änderungen erforderlich, damit die Dateien verwendbar sind.

### Vorgehensweise

- 1 Navigieren Sie zur Installationsseite für die vCloud Automation Center Appliance-Managementkonsole.  
Beispielsweise „`https://vcac-hostname.domain.name:5480/installer/`“.
- 2 Laden Sie die Linux-Gast-Agent-Pakete herunter und speichern Sie sie.
- 3 Entpacken Sie die Datei `LinuxGuestAgentPkgs`.
- 4 Navigieren Sie zur Datei `LinuxGuestAgentPkgs` und suchen Sie nach dem entsprechenden Unterverzeichnis für das Gastbetriebssystem, das Sie bei der Bereitstellung verwenden.
- 5 Öffnen Sie die Datei `sample-https.cfg`.
- 6 Ersetzen Sie alle Instanzen der Zeichenfolge `host=dcac.example.net` durch die IP-Adresse oder den vollqualifizierten Domännennamen und die Portnummer für den vRealize Automation-Serverhost.

Plattform	Erforderliches Format
vSphere ESXi	IP-Adresse, beispielsweise: <code>--host=172.20.9.59</code>
vSphere ESX	IP-Adresse, beispielsweise: <code>--host=172.20.9.58</code>
SUSE 10	IP-Adresse, beispielsweise: <code>--host=172.20.9.57</code>
Alle anderen	FQDN, beispielsweise: <code>--host=mycompany-host1.mycompany.local:443</code>

- 7 Suchen Sie jede Instanz von `gugent.rpm` oder `gugent.tar.gz` und ersetzen Sie die URL `rpm.example.net` durch den Speicherort des Gast-Agent-Pakets.

Beispiel:

```
rpm -i nfs:172.20.9.59/suseagent/gugent.rpm
```

- 8 Speichern Sie die Datei an einem Speicherort, der für neu bereitgestellte Maschinen zugreifbar ist.

## Angeben von benutzerdefinierten Skripts in einer kickstart-/autoYaST-Konfigurationsdatei

Sie können die Konfigurationsdatei ändern, um benutzerdefinierte Skripts auf neu bereitgestellte Maschinen zu kopieren oder zu installieren. Der Linux-Agent führt die Skripts an der angegebenen Stelle im Workflow aus.

Ihr Skript kann auf alle Dateien `./properties.xml` in den Verzeichnissen `/usr/share/gugent/site/workitem` verwenden.

### Voraussetzungen

- Bereiten Sie eine Kickstart- bzw. autoYaST-Konfigurationsdatei vor. Siehe [Vorbereiten der Konfigurationsbeispieldatei für Linux Kickstart](#).
- Ihr Skript muss bei einem Fehler einen Wert ungleich Null zurückgeben, um einen Fehler bei der Maschinenbereitstellung zu verhindern.

### Vorgehensweise

- 1 Erstellen Sie das Skript oder geben Sie eines an, das Sie verwenden möchten.
- 2 Speichern Sie das Skript als *NN\_scriptname*.  
  
*NN* stellt eine Zahl mit zwei Ziffern dar. Skripts werden der Reihe nach ausgeführt, beginnend mit dem niedrigsten. Wenn zwei Skripts dieselbe Zahl aufweisen, wird die alphabetische Reihenfolge verwendet, basierend auf *scriptname*.
- 3 Sorgen Sie dafür, dass Ihr Skript ausgeführt werden kann.
- 4 Suchen Sie für Ihre kickstart- bzw. autoYaST-Konfigurationsdatei den Abschnitt nach der Installation.  
  
In kickstart wird dies durch `%post` gekennzeichnet. In autoYaST wird dies durch `post-scripts` gekennzeichnet.
- 5 Ändern Sie für die Konfigurationsdatei den Abschnitt nach der Installation, sodass Sie Ihr Skript in das Verzeichnis `/usr/share/gugent/site/workitem` Ihrer Wahl kopieren oder installieren können.  
  
Benutzerdefinierte Skripts werden normalerweise für virtual kickstart/autoYaST mit den Arbeitselementen SetupOS (für das Erstellen von Bereitstellungen) und CustomizeOS (für das Klonen von Bereitstellungen) ausgeführt, aber Sie können die Skripts an jeder beliebigen Stelle im Workflow ausführen.

Sie können z. B. die Konfigurationsdatei ändern, um das Skript `11_addusers.sh` in das Verzeichnis `/usr/share/gugent/site/SetupOS` auf eine neu bereitgestellte Maschine kopieren zu können. Verwenden Sie dazu den folgenden Befehl:

```
cp nfs:172.20.9.59/linuxscripts/11_addusers.sh /usr/share/gugent/site/SetupOS
```

Der Linux-Agent führt das Skript in der Reihenfolge aus, die durch das Arbeitselemente-Verzeichnis und den Namen der Skriptdatei festgelegt ist.

## Vorbereiten für SCCM -Bereitstellung

vRealize Automation startet eine neu bereitgestellte Maschine von einem ISO-Image und gibt dann die Steuerung an die angegebene SCCM-Aufgabensequenz weiter.

Die SCCM-Bereitstellung wird für die Bereitstellung von Windows-Betriebssystemen unterstützt. Linux wird nicht unterstützt. Softwareverteilung und -aktualisierungen werden nicht unterstützt.

Das Folgende ist eine grobe Übersicht über die erforderlichen Schritte für die Vorbereitung für die SCCM-Bereitstellung:

- 1 Wenden Sie sich an Ihren Netzwerkadministrator, um sicherzustellen, dass die folgenden Netzwerkbedingungen erfüllt sind:
  - Die Kommunikation mit SCCM erfordert den NetBios-Namen des SCCM-Servers. Mindestens ein Distributed Execution Manager (DEM) muss den vollqualifizierten Namen des SCCM-Servers zu seinem NetBios-Namen auflösen können.
  - Der SCCM-Server und der vRealize Automation-Server müssen sich im selben Netzwerk befinden und für einander verfügbar sein.
- 2 Erstellen Sie ein Softwarepaket, das den vRealize Automation-Gast-Agent enthält. Siehe [Erstellen eines Softwarepakets für die SCCM-Bereitstellung](#).
- 3 Erstellen Sie in SCCM die gewünschte Aufgabensequenz für die Bereitstellung der Maschine. Im abschließenden Schritt müssen Sie das erstellte Softwarepaket, das den vRealize Automation-Gast-Agent enthält, installieren. Informationen zum Erstellen von Aufgabensequenzen und Installieren von Softwarepaketen finden Sie in der SCCM-Dokumentation.
- 4 Erstellen Sie ein Zero Touch-Boot-ISO-Image für die Aufgabensequenz. Standardmäßig erstellt SCCM ein Light Touch-Boot-ISO-Image. Informationen zum Konfigurieren von SCCM für Zero Touch-ISO-Images finden Sie in der SCCM-Dokumentation.
- 5 Kopieren Sie das ISO-Image in den für Ihre Virtualisierungsplattform erforderlichen Speicherort. Wenn Sie den entsprechenden Speicherort nicht kennen, informieren Sie sich in der von Ihrem Hypervisor bereitgestellten Dokumentation.
- 6 Erfassen Sie die folgenden Informationen, damit Blueprint-Architekten sie zu ihren Blueprints hinzufügen können:
  - a Der Name der Sammlung, die die Aufgabensequenz enthält.
  - b Der vollqualifizierte Domänenname des SCCM-Servers, auf dem sich die Sammlung, in der die Sequenz enthalten ist, befindet.
  - c Der Standortcode des SCCM-Servers.
  - d Anmeldedaten auf Administratorebene für den SCCM-Server.

- e (Optional) Für SCVMMIntegrationen ISO, die virtuelle Festplatte oder das Hardwareprofil zum Anhängen an die bereitgestellten Maschinen.

---

**Hinweis** Sie können eine Eigenschaftsgruppe mit dem Eigenschaftensatz SCCMProvisioningProperties erstellen, um all diese erforderlichen Informationen hinzuzufügen. So können die Informationen auf Blueprints einfacher hinzugefügt werden.

---

## Erstellen eines Softwarepakets für die SCCM -Bereitstellung

Der abschließende Schritt in der SCCM-Aufgabenabfolge ist die Installation eines Softwarepakets, das den vRealize Automation-Gast-Agent beinhaltet.

### Vorgehensweise

- 1 Navigieren Sie zur Installationsseite für die vCloud Automation Center Appliance-Managementkonsole.  
  
Beispielsweise „<https://vcac-hostname.domain.name:5480/installer/>“.
- 2 Laden Sie die Dateien für den Windows-Gast-Agent herunter und speichern Sie sie.
  - Dateien für den Windows-Gast-Agent (**32-Bit**)
  - Dateien für den Windows-Gast-Agent (**64-Bit**)
- 3 Extrahieren Sie die Dateien für den Windows-Gast-Agent in einen für SCCM verfügbaren Speicherort.
- 4 Erstellen Sie anhand der Definitionsdatei SCCMPackageDefinitionFile.sms ein Softwarepaket.
- 5 Stellen Sie das Softwarepaket für Ihren Verteilungspunkt zur Verfügung.
- 6 Wählen Sie den Inhalt der extrahierten Dateien für den Windows-Gast-Agent als Quelldateien aus.

## Vorbereiten für die WIM-Bereitstellung

Stellen Sie eine Maschine durch Starten in einer WinPE-Umgebung bereit und installieren Sie anschließend ein Betriebssystem unter Verwendung eines WIM-Images (Windows Imaging File Format) einer vorhandenen Windows-Referenzmaschine.

Im Folgenden finden Sie einen allgemeinen Überblick über die Schritte, die für die Vorbereitung der WIM-Bereitstellung erforderlich sind:

- 1 Identifizieren oder erstellen Sie den Bereitstellungsbereich. Dies sollte ein Netzwerkverzeichnis sein, das als ein UNC-Pfad angegeben oder als ein Netzlaufwerk durch die Referenzmaschine gemountet werden kann, das System, auf dem Sie das WinPE-Image erstellen, und der Virtualisierungshost, auf dem Maschinen bereitgestellt werden.
- 2 Stellen Sie sicher, dass im Netzwerk ein DHCP-Server verfügbar ist. vRealize Automation kann keine Maschinen unter Verwendung eines WIM-Images bereitstellen, es sei denn, DHCP ist verfügbar.

- 3 Identifizieren oder erstellen Sie die Referenzmaschine innerhalb der Virtualisierungsplattform, die Sie für die Bereitstellung verwenden möchten. Weitere Informationen zu den vRealize Automation-Anforderungen finden Sie unter [Anforderungen der Referenzmaschine für die WIM-Bereitstellung](#). Informationen zum Erstellen einer Referenzmaschine finden Sie in der von Ihrem Hypervisor bereitgestellten Dokumentation.
- 4 Bereiten Sie unter Verwendung von System Preparation Utility for Windows das Betriebssystem der Maschine für die Bereitstellung vor. Siehe [SysPrep-Anforderungen an die Referenzmaschine](#).
- 5 Erstellen Sie das WIM-Image der Referenzmaschine. Fügen Sie keine Leerzeichen in den Namen der WIM-Image-Datei ein, da sonst die Bereitstellung fehlschlägt.
- 6 Erstellen Sie ein WinPE-Image, das den vRealize Automation-Gast-Agent enthält. Sie können den vRealize Automation PEBuilder zum Erstellen eines WinPE-Images verwenden, das den Gast-Agent enthält.

- [Installieren von PEBuilder](#).
- (Optional) Erstellen Sie beliebige benutzerdefinierte Skripts, die Sie zur Anpassung bereitgestellter Maschinen verwenden möchten, und legen Sie sie im entsprechenden Arbeitselementverzeichnis der PEBuilder-Installation ab. Siehe [Angaben von benutzerdefinierten Skripten in der PEBuilder-WinPE](#).
- Wenn Sie VirtIO für Netzwerk- oder Speicherschnittstellen verwenden, müssen Sie sicherstellen, dass die notwendigen Treiber im WinPE-Image und im WIM-Image enthalten sind. Siehe [Vorbereiten für die WIM-Bereitstellung mit VirtIO-Treibern](#).
- [Erstellen eines WinPE-Images mithilfe von PEBuilder](#).

Sie können das WinPE-Image unter Verwendung einer anderen Methode erstellen, aber Sie müssen den vRealize Automation-Gast-Agent manuell einfügen. Siehe [Manuelles Einfügen des Gast-Agent in ein WinPE-Image](#).

- 7 Legen Sie das WinPE-Image in dem von der Virtualisierungsplattform benötigten Speicherort ab. Wenn Sie den Speicherort nicht kennen, informieren Sie sich in der von Ihrem Hypervisor bereitgestellten Dokumentation.
- 8 Erfassen Sie die folgenden Informationen, damit Sie sie zum Blueprint hinzufügen können:
  - a Der Name und der Speicherort des WinPE-ISO-Images.
  - b Der Name der WIM-Datei, der UNC-Pfad zur WIM-Datei und der verwendete Index zum Extrahieren des gewünschten Images aus der WIM-Datei.
  - c Der Benutzername und das Kennwort, unter denen der WIM-Image-Pfad einem Netzwerklaufwerk auf der bereitgestellten Maschine zugeordnet wird.
  - d (Optional) Wenn Sie den Laufwerksbuchstaben K (Standard) nicht akzeptieren möchten, dem der WIM-Image-Pfad auf der bereitgestellten Maschine zugeordnet ist.
  - e Für vCenter Server-Integrationen die Version des vCenter Server-Gastbetriebssystems, mit der vCenter Server die Maschine erstellt.

- f (Optional) Für SCVMM-Integrationen ISO, die virtuelle Festplatte oder das Hardwareprofil zum Anhängen an die bereitgestellten Maschinen.

---

**Hinweis** Sie können eine Eigenschaftsgruppe mit allen diesen erforderlichen Informationen erstellen. Unter Verwendung einer Eigenschaftsgruppe ist es einfacher, alle Informationen korrekt in Blueprints hinzuzufügen.

---

## Anforderungen der Referenzmaschine für die WIM-Bereitstellung

Die WIM-Bereitstellung umfasst das Erstellen eines WIM-Images aus einer Referenzmaschine. Die Referenzmaschine muss Mindestanforderungen für das WIM-Image erfüllen, damit sie für die Bereitstellung in vRealize Automation funktioniert.

Im Folgenden finden Sie eine grobe Übersicht über die Schritte für die Vorbereitung einer Referenzmaschine:

- 1 Wenn das Betriebssystem auf der Referenzmaschine Windows Server 2008 R2, Windows Server 2012, Windows 7 oder Windows 8 ist, erstellt die Standardinstallation eine kleine Partition auf der Festplatte des Systems zusätzlich zur Hauptpartition. vRealize Automation unterstützt nicht die Verwendung von WIM-Images, die auf solchen mehrfach partitionierten Referenzmaschinen erstellt wurden. Sie müssen diese Partition beim Installationsvorgang löschen.
- 2 Installieren Sie NET 4.5 und Windows Automated Installation Kit (AIK) für Windows 7 (einschließlich WinPE 3.0) auf der Referenzmaschine.
- 3 Wenn das Betriebssystem der Referenzmaschine Windows Server 2003 oder Windows XP ist, setzen Sie das Administratorkennwort auf die Leeroption zurück. (Es gibt kein Kennwort.)
- 4 (Optional) Wenn Sie die XenDesktop-Integration aktivieren möchten, installieren und konfigurieren Sie einen Citrix Virtual Desktop Agent.
- 5 (Optional) Ein WMI-Agent (Windows Management Instrumentation, Windows-Verwaltungsinstrumentation) ist für das Erfassen bestimmter Daten aus einer Windows-Maschine erforderlich, die von vRealize Automation verwaltet wird, beispielsweise der Active Directory-Status eines Maschinenbesitzers. Um eine erfolgreiche Verwaltung von Windows-Maschinen sicherzustellen, müssen Sie einen WMI-Agent (normalerweise auf dem Manager Service-Host) installieren und den Agent für die Erfassung von Daten aus Windows-Maschinen aktivieren. Siehe *Installieren von vRealize Automation 7.1*.

## SysPrep-Anforderungen an die Referenzmaschine

Eine SysPrep-Antwortdatei enthält mehrere erforderliche Einstellungen, die für die WIM-Bereitstellung verwendet werden.

**Tabelle 1-14. Erforderliche SysPrep-Einstellungen für Windows Server- oder Windows XP-Referenzmaschine**

GuiUnattended-Einstellungen	Wert
AutoLogon	Ja
AutoLogonCount	1

**Tabelle 1-14. Erforderliche SysPrep-Einstellungen für Windows Server- oder Windows XP-Referenzmaschine (Fortsetzung)**

GuiUnattended-Einstellungen	Wert
AutoLogonUsername	<i>Benutzername</i> ( <i>Benutzername</i> und <i>Kennwort</i> sind die Anmeldedaten, die für die automatische Anmeldung verwendet werden, wenn die neu bereitgestellte Maschine im Gastbetriebssystem gestartet wird. In der Regel wird „Administrator“ verwendet.)
AutoLogonPassword	<i>Kennwort</i> entspricht AutoLogonUsername.

**Tabelle 1-15. Erforderliche SysPrep-Einstellungen für Referenzmaschinen, die nicht Windows Server 2003 oder Windows XP verwenden:**

AutoLogon-Einstellungen	Wert
Enabled	Ja
LogonCount	1
Username	<i>Benutzername</i> ( <i>Benutzername</i> und <i>Kennwort</i> sind die Anmeldedaten, die für die automatische Anmeldung verwendet werden, wenn die neu bereitgestellte Maschine im Gastbetriebssystem gestartet wird. In der Regel wird „Administrator“ verwendet.)
Password	<i>Kennwort</i> ( <i>Benutzername</i> und <i>Kennwort</i> sind die Anmeldedaten, die für die automatische Anmeldung verwendet werden, wenn die neu bereitgestellte Maschine im Gastbetriebssystem gestartet wird. In der Regel wird „Administrator“ verwendet.)  <b>Hinweis</b> Für Referenzmaschinen, die eine neuere Windows-Plattform als Windows Server 2003/Windows XP verwenden, müssen Sie das Kennwort für die automatische Anmeldung mithilfe der benutzerdefinierten Eigenschaft Sysprep.GuiUnattended.AdminPassword festlegen. Dies können Sie auf bequeme Weise sicherstellen, indem Sie eine Eigenschaftsgruppe erstellen, die diese benutzerdefinierte Eigenschaft enthält, sodass Mandantenadministratoren und Business-Gruppenmanager diese Informationen ordnungsgemäß ihren Blueprints hinzufügen können.

## Installieren von PEBuilder

Das PEBuilder-Tool, das von vRealize Automation bereitgestellt wird, bietet eine einfache Möglichkeit zum Hinzufügen des vRealize Automation-Gast-Agents in Ihre WinPE-Images.

PEBuilder verfügt über einen 32-Bit-Gast-Agent. Wenn Sie Befehle ausführen müssen, die 64-Bit-spezifisch sind, installieren Sie PEBuilder und rufen Sie dann die 64-Bit-Dateien von der Datei Gugen-Zipx64.zip ab.

Installieren Sie PEBuilder in einem Standort, wo Sie auf die Staging-Umgebung zugreifen können.

## Voraussetzungen

- Installieren Sie NET Framework 4.5.
- Windows Automated Installation Kit (AIK) für Windows 7 (einschließlich WinPE 3.0) ist installiert.

## Vorgehensweise

- 1 Navigieren Sie zur Installationsseite für die vCloud Automation Center Appliance-Managementkonsole.  
  
Beispielsweise „<https://vcac-hostname.domain.name:5480/installer/>“.
- 2 Laden Sie den PEBuilder herunter.
- 3 (Optional) Laden Sie das Windows-64-Bit-Gast-Agent-Paket herunter, wenn Sie den Windows-64-Bit-Gast-Agent in WinPE hinzufügen möchten anstatt den Windows-32-Bit-Gast-Agent.
- 4 Führen Sie vCAC-WinPEBuilder-Setup.exe aus.
- 5 Befolgen Sie die Anleitungen zum Installieren von PEBuilder.
- 6 (Optional) Ersetzen Sie die Windows-32-Bit-Gast-Agent-Dateien, die sich in \PE Builder\Plugins\VRM Agent\VRMGuestAgent befinden, mit den 64-Bit-Dateien, um den 64-Bit-Agent in WinPE hinzuzufügen.

Sie können mit PEBuilder ein WinPE für die Verwendung in einer WIM-Bereitstellung erstellen.

## Angeben von benutzerdefinierten Skripts in der PEBuilder-WinPE

Sie können PEBuilder zur Anpassung von Maschinen verwenden, indem Sie benutzerdefinierte bat-Skripte an angegebenen Stellen im Bereitstellungsworkflow ausführen.

## Voraussetzungen

[Installieren von PEBuilder.](#)

## Vorgehensweise

- 1 Erstellen Sie das bat-Skript oder geben Sie eines an, das Sie verwenden möchten.  
  
Ihr Skript muss bei einem Fehler einen Wert ungleich Null zurückgeben, um einen Fehler bei der Maschinenbereitstellung zu verhindern.
- 2 Speichern Sie das Skript als *NN\_scriptname*.  
  
*NN* stellt eine Zahl mit zwei Ziffern dar. Skripts werden der Reihe nach ausgeführt, beginnend mit dem niedrigsten. Wenn zwei Skripts dieselbe Zahl aufweisen, wird die alphabetische Reihenfolge verwendet, basierend auf *scriptname*.
- 3 Sorgen Sie dafür, dass Ihr Skript ausgeführt werden kann.



- Legen Sie die Skripts im Arbeitselemente-Unterverzeichnis ab, das der Stelle im Bereitstellungswork-flow entspricht, an der Sie das Skript ausführen möchten.

Zum Beispiel: C:\Programme (x86)\VMware\vRA\PE Builder\Plugins\VRM Agent\VRMGuest-Agent\site\SetupOS.

Der Agent führt das Skript in der Reihenfolge aus, die durch das Arbeitselemente-Verzeichnis und den Namen der Skriptdatei festgelegt ist.

## Vorbereiten für die WIM-Bereitstellung mit VirtIO-Treibern

Wenn Sie VirtIO für Netzwerk- oder Speicherschnittstellen verwenden, müssen Sie sicherstellen, dass die notwendigen Treiber im WinPE-Image und im WIM-Image enthalten sind. VirtIO bietet allgemein eine bessere Leistung bei der Bereitstellung mit KVM (RHEV).

Windows-Treiber für VirtIO sind Teil der Red Hat Enterprise Virtualization und befinden sich im Verzeichnis /usr/share/virtio-win des Dateisystems von Red Hat Enterprise Virtualization Manager. Die Treiber sind auch in den Gasttools von Red Hat Enterprise Virtualization enthalten, die sich unter /usr/share/rhev-guest-tools-iso/rhev-tools-setup.iso befinden.

So wird die WIM-basierte Bereitstellung mit VirtIO-Treibern aktiviert (grobe Übersicht):

- Erstellen Sie ein WIM-Image von einer Windows-Referenzmaschine mit den installierten VirtIO-Treibern oder legen Sie die Treiber in ein vorhandenes WIM-Image ein.
- Kopieren Sie vor dem Erstellen eines WinPE-Images die VirtIO-Treiberdateien in das Unterverzeichnis Plug-Ins des PEBuilder-Installationsverzeichnisses oder legen Sie die Treiber in ein WinPE-Image ein, das durch andere Methoden erstellt wurde.
- Laden Sie das WinPE-Image ISO auf die ISO-Speicherdomänen von Red Hat Enterprise Virtualization unter Verwendung des rhvm-iso-uploader-Befehls hoch. Weitere Informationen zum Verwalten von ISO-Images in RHEV finden Sie in der Red Hat-Dokumentation.
- Erstellen Sie einen KVM (RHEV)-Blueprint für die WIM-Bereitstellung und wählen Sie die WinPE-ISO-Option aus. Die benutzerdefinierte Eigenschaft VirtualMachine.Admin.DiskInterfaceType muss mit dem Wert **VirtIO** enthalten sein. Ein Fabric-Administrator kann diese Informationen in einer Eigenschaftsgruppe für die Aufnahme in Blueprints hinzufügen.

Die benutzerdefinierten Eigenschaften Image.ISO.Location und Image.ISO.Name werden nicht für KVM (RHEV)-Blueprints verwendet.

## Erstellen eines WinPE-Images mithilfe von PEBuilder

Verwenden Sie das PEBuilder-Tool, das im Lieferumfang von vRealize Automation enthalten ist, um eine WinPE-ISO-Datei zu erstellen, die den vRealize Automation-Gast-Agent beinhaltet.

### Voraussetzungen

- [Installieren von PEBuilder](#).
- (Optional) Konfigurieren Sie PEBuilder so, dass der Windows-64-Bit-Gast-Agent anstelle des Windows-32-Bit-Gast-Agents in Ihrem WinPE-Image verwendet wird. Siehe [Installieren von PEBuilder](#).

- (Optional) Fügen Sie Drittanbieter-Plug-Ins, die Sie dem WinPE-Image hinzufügen möchten, im Unterverzeichnis PlugIns des Installationsverzeichnisses von PEBuilder hinzu.
- (Optional) [Angaben von benutzerdefinierten Skripts in der PEBuilder-WinPE.](#)

### Vorgehensweise

- 1 Führen Sie PEBuilder aus.
- 2 Geben Sie Informationen zum IaaS Manager Service-Host ein.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichsdienst verwenden</b>	<ol style="list-style-type: none"> <li>a Geben Sie in das Textfeld <b>vCAC-Hostname</b> den vollqualifizierten Domänennamen des Lastausgleichsdiensts für den IaaS Manager Service ein. Beispielsweise <b>manager_service_LB.mycompany.com</b>.</li> <li>b Geben Sie in das Textfeld <b>vCAC-Port</b> die Portnummer des Lastausgleichsdiensts für den IaaS Manager Service ein. Beispielsweise <b>443</b>.</li> </ol>
<b>Wenn Sie keinen Lastausgleichsdienst verwenden</b>	<ol style="list-style-type: none"> <li>a Geben Sie in das Textfeld <b>vCAC-Hostname</b> den vollqualifizierten Domänennamen der IaaS Manager Service-Maschine ein. Beispielsweise <b>manager_service.mycompany.com</b>.</li> <li>b Geben Sie in das Textfeld <b>vCAC-Port</b> die Portnummer für die IaaS Manager Service-Maschine ein. Beispielsweise <b>443</b>.</li> </ol>

- 3 Geben Sie den Pfad zum PEBuilder-Plug-Ins-Verzeichnis ein.

Dieser Pfad ist abhängig von dem bei der Installation angegebenen Installationsverzeichnis. Standardmäßig lautet dieser Pfad C:\Programme (x86)\VMware\vCAC\PE Builder\PlugIns.

- 4 Geben Sie in das Textfeld **ISO-Ausgabepfad** den Ausgabepfad für die ISO-Datei ein, die Sie erstellen.

Dieser Speicherort sollte sich in dem von Ihnen vorbereiteten Staging-Bereich befinden.

- 5 Klicken Sie auf **Datei > Erweitert**.

**Hinweis** Die Einstellungen für **WinPE-Architektur** oder **Protokoll** sollten Sie nicht ändern.

- 6 Aktivieren Sie das Kontrollkästchen **vCAC-Gast-Agent in WinPE-ISO einbeziehen**.
- 7 Klicken Sie auf **OK**.
- 8 Klicken Sie auf **Erstellen**.

### Weiter

Platzieren Sie das WinPE-Image in dem für Ihre Integrationsplattform erforderlichen Speicherort. In der Begleitdokumentation zu Ihrer Plattform finden Sie weitere Informationen hierzu, falls Sie diesen Speicherort nicht kennen.

Wenn Sie HP iLO-Maschinen bereitstellen, platzieren Sie das WinPE-Image in einem Speicherort mit Webzugriff. Für Dell iDRAC-Maschinen platzieren Sie das Image in einem Speicherort, das für NFS oder CIFS verfügbar ist. Notieren Sie sich die Adresse.

## Manuelles Einfügen des Gast-Agent in ein WinPE-Image

Sie müssen für das Erstellen der WinPE den vRealize Automation PEBuilder nicht verwenden. Wenn Sie jedoch nicht den PEBuilder verwenden, müssen Sie den vRealize Automation-Gast-Agent manuell in das WinPE-Image einfügen.

### Voraussetzungen

- Wählen Sie ein Windows-System aus, von dem aus der vorbereitete Stagingbereich zugreifbar ist und auf dem .NET 4.5 und Windows Automated Installation Kit (AIK) für Windows 7 (einschließlich WinPE 3.0) installiert sind.
- Erstellen Sie ein WinPE.

### Vorgehensweise

#### 1 Installieren des Gast-Agents in einem WinPE

Wenn Sie den vRealize Automation PEBuilder nicht zum Erstellen des WinPE verwenden möchten, müssen Sie PEBuilder installieren, um die Gast-Agent-Dateien manuell in das WinPE-Image zu kopieren.

#### 2 Konfigurieren der Datei „doagent.bat“

Für den Fall, dass Sie den vRealize Automation PEBuilder nicht verwenden möchten, müssen Sie die Datei `doagent.bat` manuell konfigurieren.

#### 3 Konfigurieren der Datei „doagentc.bat“

Für den Fall, dass Sie den vRealize Automation PEBuilder nicht verwenden möchten, müssen Sie die Datei `doagentc.bat` manuell konfigurieren.

#### 4 Konfigurieren der Gast-Agent-Eigenschaftendateien

Für den Fall, dass Sie den vRealize Automation PEBuilder nicht verwenden möchten, müssen Sie die Gast-Agent-Eigenschaftendateien manuell konfigurieren.

### Vorgehensweise

#### 1 Installieren des Gast-Agents in einem WinPE.

#### 2 Konfigurieren der Datei „doagent.bat“.

#### 3 Konfigurieren der Datei „doagentc.bat“.

#### 4 Konfigurieren der Gast-Agent-Eigenschaftendateien.

### Installieren des Gast-Agents in einem WinPE

Wenn Sie den vRealize Automation PEBuilder nicht zum Erstellen des WinPE verwenden möchten, müssen Sie PEBuilder installieren, um die Gast-Agent-Dateien manuell in das WinPE-Image zu kopieren.

PEBuilder verfügt über einen 32-Bit-Gast-Agent. Wenn Sie Befehle ausführen müssen, die 64-Bit-spezifisch sind, installieren Sie PEBuilder und rufen Sie dann die 64-Bit-Dateien von der Datei `Gugent-Zipx64.zip` ab.

## Voraussetzungen

- Wählen Sie ein Windows-System aus, von dem aus der vorbereitete Stagingbereich zugreifbar ist und auf dem .NET 4.5 und Windows Automated Installation Kit (AIK) für Windows 7 (einschließlich WinPE 3.0) installiert sind.
- Erstellen Sie ein WinPE.

## Vorgehensweise

- 1 Navigieren Sie zur Installationsseite für die vCloud Automation Center Appliance-Managementkonsole.

Beispielsweise „<https://vcac-hostname.domain.name:5480/installer/>“.

- 2 Laden Sie den PEBuilder herunter.
- 3 (Optional) Laden Sie das Windows-64-Bit-Gast-Agent-Paket herunter, wenn Sie den Windows-64-Bit-Gast-Agent in WinPE hinzufügen möchten anstatt den Windows-32-Bit-Gast-Agent.
- 4 Führen Sie vCAC-WinPEBuilder-Setup.exe aus.
- 5 Heben Sie die Auswahl von **Plug-Ins** und **PEBuilder** auf.
- 6 Erweitern Sie **Plug-Ins** und wählen Sie **VRMAgent** aus.
- 7 Folgen Sie den Eingabeaufforderungen, um die Installation abzuschließen.
- 8 (Optional) Ersetzen Sie nach Abschluss der Installation die Windows-32-Bit-Gast-Agent-Dateien, die sich in \PE Builder\Plugins\VRM Agent\VRMGuestAgent befinden, mit den 64-Bit-Dateien, um den 64-Bit-Agent in WinPE hinzuzufügen.
- 9 Kopieren Sie den Inhalt von %SystemDrive%\Programdateien (x86)\VMware\PE Builder\Plugins\VRM Agent\VRMGuestAgent in einen neuen Speicherort innerhalb des WinPE-Images.

Beispiel: C:\Programme (x86)\VMware\PE Builder\Plugins\VRM Agent\VRMGuestAgent.

## Weiter

[Konfigurieren der Datei „doagent.bat“.](#)

## Konfigurieren der Datei „doagent.bat“

Für den Fall, dass Sie den vRealize Automation PEBuilder nicht verwenden möchten, müssen Sie die Datei doagent.bat manuell konfigurieren.

## Voraussetzungen

[Installieren des Gast-Agents in einem WinPE.](#)

## Vorgehensweise

- 1 Navigieren Sie zum Verzeichnis VRMGuestAgent in Ihrem WinPE-Image.

Beispiel: C:\Programme (x86)\VMware\PE Builder\Plugins\VRM Agent\VRMGuestAgent.

- 2 Erstellen Sie eine Kopie der Datei doagent-template.bat und benennen Sie sie doagent.bat.

- 3 Öffnen Sie `doagent.bat` in einem Texteditor.
- 4 Ersetzen Sie alle Instanzen der Zeichenfolge `#Dcac Hostname#` durch den vollqualifizierten Domännennamen und die Portnummer des IaaS Manager Service-Hosts.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und den Port des Lastausgleichsdiensts für den IaaS Manager Service ein. Beispiel:  <code>manager_service_LB.mycompany.com:443</code>
<b>Wenn Sie keinen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und den Port der Maschine, auf der der IaaS Manager Service installiert ist, ein. Beispiel:  <code>manager_service.mycompany.com:443</code>

- 5 Ersetzen Sie alle Instanzen der Zeichenfolge `#Protocol#` durch die Zeichenfolge `/ssl`.
- 6 Ersetzen Sie alle Instanzen der Zeichenfolge `#Comment#` durch `REM` (auf `REM` muss ein nachfolgendes Leerzeichen folgen).
- 7 (Optional) Wenn Sie selbstsignierte Zertifikate verwenden, heben Sie die Auskommentierung des `openssl`-Befehls auf.

```
echo QUIT | c:\VRMGuestAgent\bin\openssl s_client -connect
```

- 8 Speichern und schließen Sie die Datei.
- 9 Bearbeiten Sie das Skript `Startnet.cmd` für Ihre WinPE-Instanz, um die Datei `doagent.bat` als benutzerdefiniertes Skript einzufügen.

## Weiter

[Konfigurieren der Datei „doagentc.bat“.](#)

### Konfigurieren der Datei „doagentc.bat“

Für den Fall, dass Sie den vRealize Automation PEBuilder nicht verwenden möchten, müssen Sie die Datei `doagentc.bat` manuell konfigurieren.

## Voraussetzungen

[Konfigurieren der Datei „doagent.bat“.](#)

## Vorgehensweise

- 1 Navigieren Sie zum Verzeichnis `VRMGuestAgent` in Ihrem WinPE-Image.  
Beispiel: `C:\Programme (x86)\VMware\PE Builder\Plugins\VRM Agent\VRMGuestAgent`.
- 2 Erstellen Sie eine Kopie der Datei `doagentsvc-template.bat` und benennen Sie sie `doagentc.bat`.
- 3 Öffnen Sie `doagentc.bat` in einem Texteditor.

- 4 Entfernen Sie alle Instanzen der Zeichenfolge #Comment#.
- 5 Ersetzen Sie alle Instanzen der Zeichenfolge #Dcac Hostname# durch den vollqualifizierten Domännennamen und die Portnummer des Manager Service-Hosts.

Der Standardport für den Manager Service lautet 443.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und den Port des Lastausgleichsdiensts für den Manager Service ein. Beispiel:  <code>load_balancer_manager_service.mycompany.com:443</code>
<b>Wenn Sie keinen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und den Port des Manager Service ein. Beispiel:  <code>manager_service.mycompany.com:443</code>

- 6 Ersetzen Sie alle Instanzen der Zeichenfolge #errorlevel# durch das Zeichen 1.
- 7 Ersetzen Sie alle Instanzen der Zeichenfolge #Protocol# durch die Zeichenfolge /ssl.
- 8 Speichern und schließen Sie die Datei.

#### Weiter

[Konfigurieren der Gast-Agent-Eigenschaftendateien.](#)

### Konfigurieren der Gast-Agent-Eigenschaftendateien

Für den Fall, dass Sie den vRealize Automation PEBuilder nicht verwenden möchten, müssen Sie die Gast-Agent-Eigenschaftendateien manuell konfigurieren.

#### Voraussetzungen

[Konfigurieren der Datei „doagentc.bat“.](#)

#### Vorgehensweise

- 1 Navigieren Sie zum Verzeichnis VRMGuestAgent in Ihrem WinPE-Image.  
Beispiel: C:\Programme (x86)\VMware\PE Builder\Plugins\VRM Agent\VRMGuestAgent.
- 2 Erstellen Sie eine Kopie der Datei gugent.properties und benennen Sie sie gugent.properties.template.
- 3 Erstellen Sie eine Kopie der Datei gugent.properties.template und benennen Sie sie gugentc.properties.
- 4 Öffnen Sie gugent.properties in einem Texteditor.
- 5 Ersetzen Sie alle Instanzen der Zeichenfolge GuestAgent.log durch die Zeichenfolge X:/VRMGuestAgent/GuestAgent.log.
- 6 Speichern und schließen Sie die Datei.
- 7 Öffnen Sie gugentc.properties in einem Texteditor.

- 8 Ersetzen Sie alle Instanzen der Zeichenfolge `GuestAgent.log` durch die Zeichenfolge `C:/VRMGuestAgent/GuestAgent.log`.
- 9 Speichern und schließen Sie die Datei.

## Vorbereiten für die Image-Bereitstellung der virtuellen Maschine

Bevor Sie Instanzen mit OpenStack bereitstellen, müssen VM-Images und -Typen im OpenStack-Anbieter konfiguriert werden.

### Virtuelle Maschinen-Images

Sie können ein virtuelles Maschinen-Image aus der Liste der verfügbaren Images auswählen, wenn Sie Blueprints für OpenStack-Ressourcen erstellen.

Ein virtuelles Maschinen-Image ist eine Vorlage, die eine Softwarekonfiguration enthält, einschließlich eines Betriebssystems. Virtuelle Maschinen-Images werden vom OpenStack-Anbieter verwaltet und während der Datenerfassung importiert.

Wenn ein in einem Blueprint verwendetes Image später vom OpenStack-Anbieter gelöscht wird, wird es auch vom Blueprint entfernt. Wenn alle Images von einem Blueprint entfernt wurden, wird der Blueprint deaktiviert und kann so lange nicht mehr für Maschinenanforderungen verwendet werden, bis er bearbeitet und mindestens ein Image hinzugefügt wurde.

### OpenStack-Typen

Sie können beim Erstellen von OpenStack-Blueprints mindestens einen Typen auswählen.

OpenStack-Typen sind virtuelle Hardwarevorlagen, die die Spezifikationen der Maschinenressourcen für in OpenStack bereitgestellte Instanzen definieren. Typen werden durch den OpenStack-Anbieter verwaltet und während der Datenerfassung importiert.

vRealize Automation unterstützt mehrere OpenStack-Typen. Aktuelle Informationen zur Unterstützung von OpenStack-Typen finden Sie in der *Übersicht über die Unterstützung von vRealize Automation* unter <https://www.vmware.com/support/pubs/vcac-pubs.html>.

## Vorbereiten für die Bereitstellung von Amazon-System-Images

Bereiten Sie Ihre Amazon-Maschinen-Images und Instanztypen für die Bereitstellung in vRealize Automation vor.

### Grundlegendes zu Amazon-Maschinen-Images

Beim Erstellen von Amazon-Maschinen-Blueprints können Sie ein Amazon-Maschinen-Image aus einer Liste mit verfügbaren Images auswählen.

Ein Amazon-Maschinen-Image ist eine Vorlage, die eine Softwarekonfiguration einschließlich eines Betriebssystems enthält. Sie werden über Amazon Web Services-Konten verwaltet. vRealize Automation verwaltet die Instanztypen, die für die Bereitstellung verfügbar sind.

Das Amazon-Maschinen-Image und der Instanztyp müssen in einer Amazon-Region verfügbar sein. Es sind nicht alle Instanztypen in allen Regionen verfügbar.

Sie können ein von Amazon Web Services bereitgestelltes Amazon-Maschinen-Image, eine Benutzercommunity oder die AWS-Marketplace-Website auswählen. Sie können auch Ihre eigenen Amazon-Maschinen-Images erstellen und optional freigeben. Ein einzelnes Amazon-Maschinen-Image kann zum Starten einer Instanz oder vieler Instanzen verwendet werden.

Die folgenden Überlegungen gelten für Amazon-Maschinen-Images in den Amazon Web Services-Konten, aus denen Sie Cloud-Maschinen bereitstellen:

- Jeder Blueprint muss ein Amazon-Maschinen-Image angeben.  
Ein privates Amazon-Maschinen-Image steht einem bestimmten Konto und all seinen Regionen zur Verfügung. Ein öffentliches Amazon-Maschinen-Image steht allen Konten zur Verfügung, aber nur einer bestimmten Region in jedem Konto.
- Wurde der Blueprint erstellt, wird das angegebene Amazon-Maschinen-Image aus Regionen ausgewählt, für die Daten erfasst wurden. Wenn mehrere Amazon Web Services-Konten verfügbar sind, muss der Business-Gruppenmanager über Rechte für alle privaten Amazon-Maschinen-Images verfügen. Die Region des Amazon-Maschinen-Images und der Standort des angegebenen Benutzers beschränken Bereitstellungsanforderungen auf Reservierungen, die mit der entsprechenden Region und dem entsprechenden Standort übereinstimmen.
- Verteilen Sie mit Reservierungen und Richtlinien Amazon-Maschinen-Images in Ihren Amazon Web Services-Konten. Beschränken Sie mit Richtlinien die Bereitstellung aus einem Blueprint in einen bestimmten Satz von Reservierungen.
- vRealize Automation kann keine Benutzerkonten in einer Cloud-Maschine erstellen. Wenn sich ein Maschinenbesitzer zum ersten Mal bei einer Cloud-Maschine anmeldet, muss er sich als ein Administrator anmelden und seine vRealize Automation-Benutzeranmeldedaten hinzufügen, oder ein Administrator muss dies für ihn übernehmen. Er kann sich dann mithilfe seiner vRealize Automation-Benutzeranmeldedaten anmelden.

Wenn das Amazon-Maschinen-Image das Administratorkennwort bei jedem Start erstellt, zeigt die Seite zum Bearbeiten des Maschinendatensatzes das Kennwort an. Ist dies nicht der Fall, finden Sie das Kennwort im Amazon Web Services-Konto. Sie können alle Amazon-Maschinen-Images so konfigurieren, dass das Administratorkennwort bei jedem Start erstellt wird. Sie können auch Informationen zum Administratorkennwort bereitstellen, um Benutzer zu unterstützen, die Maschinen für andere Benutzer bereitstellen.

- Um Microsoft Windows-WMI-Remoteanforderungen (Windows Management Instrumentation, Windows-Verwaltungsinstrumentation) auf Cloud-Maschinen zu erlauben, die in Amazon Web Services-Konten bereitgestellt werden, aktivieren Sie einen Microsoft WinRM-Agent (Windows Remote Management, Windows-Remoteverwaltung) zum Erfassen von mit vRealize Automation verwalteten Windows-Maschinen. Siehe *Installieren von vRealize Automation 7.1*.
- Ein privates Amazon-Maschinen-Image kann über Mandanten hinweg angezeigt werden.

Informationen hierzu finden Sie unter dem Abschnitt *Amazon-Maschinen-Images (AMI)* in der Amazon-Dokumentation.



## Grundlegendes zu Amazon-Instanztypen

Beim Erstellen von Amazon EC2-Blueprints wählt ein IaaS-Architekt einen oder mehrere Amazon-Instanztypen aus. Ein IaaS-Administrator kann Instanztypen hinzufügen oder entfernen, um die Wahlmöglichkeiten zu steuern, die den Architekten zur Verfügung stehen.

Eine Amazon EC2-Instanz ist ein virtueller Server, der Anwendungen in Amazon Web Services ausführen kann. Instanzen werden aus einem Amazon-Maschinen-Image erstellt und indem ein geeigneter Instanztyp ausgewählt wird.

Um eine Maschine in einem Amazon Web Services-Konto bereitzustellen, wird ein Instanztyp auf das angegebene Amazon-Maschinen-Image angewendet. Die verfügbaren Instanztypen werden aufgelistet, wenn Architekten den Amazon EC2-Blueprint erstellen. Architekten wählen einen oder mehrere Instanztypen aus. Diese Instanztypen stehen Benutzern dann als Optionen zur Verfügung, wenn sie die Bereitstellung einer Maschine anfordern. Die Instanztypen müssen in der festgelegten Region unterstützt werden.

Weitere Informationen finden Sie unter den Abschnitten *Auswählen der Instanztypen* und *Amazon-EC2-Instanz-Details* in der Amazon-Dokumentation.

## Hinzufügen eines Amazon-Instanztyps

Mit vRealize Automation werden mehrere Instanztypen für die Verwendung mit Amazon-Blueprints zur Verfügung gestellt. Ein Administrator kann Instanztypen hinzufügen und entfernen.

Die von IaaS-Administratoren verwalteten Maschineninstanztypen stehen Blueprint-Architekten zur Verfügung, wenn sie einen Amazon-Blueprint erstellen oder bearbeiten. Amazon-Maschinen-Images und Instanztypen werden durch das Amazon Web Services-Produkt zur Verfügung gestellt.

### Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **IaaS-Administrator** an.

### Vorgehensweise

- 1 Klicken Sie auf **Infrastruktur > Administration > Instanztypen**.
- 2 Klicken Sie auf **Neuer Instanztyp**.
- 3 Fügen Sie einen neuen Instanztyp hinzu und geben Sie die folgenden Parameter an.

Informationen über die verfügbaren Amazon-Instanztypen und die Einstellungswerte, die Sie für diese Parameter angeben können, sind in der Amazon Web Services-Dokumentation in *EC2-Instance-Typen - Amazon Web Services (AWS)* unter „aws.amazon.com/ec2“ und *Instance Types* (Instanztypen) unter „docs.aws.amazon.com“ verfügbar.

- Name
- API-Name
- Name des Typs
- Name des E/A-Leistungsindikators
- CPUs

- Arbeitsspeicher (GB)
- Speicher (GB)
- Einheiten berechnen

4 Klicken Sie auf das Symbol **Speichern** (✓).

Wenn IaaS-Architekten Amazon Web Services-Blueprints erstellen, können sie Ihre benutzerdefinierten Instanztypen verwenden.

#### Weiter

Fügen Sie die Computing-Ressourcen von Ihrem Endpoint zu einer Fabric-Gruppe hinzu. Siehe [Erstellen einer Fabric-Gruppe](#).

## Szenario: Vorbereiten von vSphere -Ressourcen für Maschinenbereitstellung in Rainpole

Als der Administrator von vSphere, der Vorlagen für vRealize Automation erstellt, möchten Sie den vSphere Web Client verwenden, um das Klonen von CentOS-Maschinen in vRealize Automation vorzubereiten.



Sie möchten eine vorhandene CentOS-Referenzmaschine in eine vSphere-Vorlage konvertieren, sodass Sie und Ihre Rainpole-Architekten Blueprints für das Klonen von CentOS-Maschinen in vRealize Automation erstellen können. Um Konflikte zu vermeiden, die aus der Bereitstellung von mehreren virtuellen Maschinen mit identischen Einstellungen entstehen können, möchten Sie auch eine allgemeine Anpassungsspezifikation erstellen, mit der Sie und Ihre Architekten Klon-Blueprints für Linux-Vorlagen erstellen können.

#### Vorgehensweise

##### 1 Szenario: Konvertieren einer CentOS-Referenzmaschine in eine Vorlage für Rainpole

Mithilfe des vSphere Client konvertieren Sie Ihre vorhandene CentOS-Referenzmaschine in eine vSphere-Vorlage für die vRealize Automation-IaaS-Architekten, die als Grundlage für deren Klon-Blueprints dient.

##### 2 Szenario: Erstellen einer Anpassungsspezifikation für das Klonen von Maschinen in Rainpole

Mit dem vSphere Client können Sie eine Standard-Anpassungsspezifikation erstellen, die Ihre vRealize Automation-IaaS-Architekten beim Erstellen von Klon-Blueprints für Linux-Maschinen verwenden können.

## Szenario: Konvertieren einer CentOS-Referenzmaschine in eine Vorlage für Rainpole

Mithilfe des vSphere Client konvertieren Sie Ihre vorhandene CentOS-Referenzmaschine in eine vSphere-Vorlage für die vRealize Automation-IaaS-Architekten, die als Grundlage für deren Klon-Blueprints dient.

### Vorgehensweise

- 1 Melden Sie sich an Ihrer Referenzmaschine als Root-Benutzer an und bereiten Sie die Maschine zum Konvertieren vor.

- a Entfernen Sie udev-Persistenzregeln.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- b Aktivieren Sie bei von dieser Vorlage geklonten Maschinen eigene eindeutige Bezeichner.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- c Fahren Sie die Maschine herunter.

```
shutdown -h now
```

- 2 Melden Sie sich beim vSphere Web Client als Administrator an.
- 3 Klicken Sie auf die Registerkarte **VM-Optionen**.
- 4 Klicken Sie mit der rechten Maustaste auf Ihre Referenzmaschine und wählen Sie **Einstellungen bearbeiten**.
- 5 Geben Sie **Rainpole\_centos\_63\_x86** in das Textfeld **VM-Name** ein.
- 6 Selbst wenn Ihre Referenzmaschine über ein CentOS-Gastbetriebssystem verfügt, wählen Sie aus dem Dropdown-Menü **Version des Gastbetriebssystems** die Option **Red Hat Enterprise Linux 6 (64-Bit)** aus.

Wenn Sie CentOS auswählen, funktionieren Ihre Vorlage und Anpassungsspezifikation möglicherweise nicht wie erwartet.

- 7 Klicken Sie im vSphere Web Client mit der rechten Maustaste auf die Referenzmaschine **Rainpole\_centos\_63\_x86** und wählen Sie **Vorlage > In Vorlage konvertieren** aus.

vCenter Server markiert Ihre Referenzmaschine „Rainpole\_centos\_63\_x86“ als Vorlage und zeigt die Aufgabe im Fensterbereich „Kürzlich bearbeitete Aufgaben“ an.

## Weiter

Um Konflikte zu vermeiden, die aus der Bereitstellung von mehreren virtuellen Maschinen mit identischen Einstellungen entstehen können, erstellen Sie eine allgemeine Anpassungsspezifikation, mit der Sie und Ihre Rainpole-Architekten Klon-Blueprints für Linux-Vorlagen erstellen können.

## Szenario: Erstellen einer Anpassungsspezifikation für das Klonen von Maschinen in Rainpole

Mit dem vSphere Client können Sie eine Standard-Anpassungsspezifikation erstellen, die Ihre vRealize Automation-laaS-Architekten beim Erstellen von Klon-Blueprints für Linux-Maschinen verwenden können.

### Vorgehensweise

- 1 Klicken Sie auf der Startseite auf **Anpassungsspezifikations-Manager**, um den Assistenten zu öffnen.
- 2 Klicken Sie auf das Symbol **Neu**.
- 3 Geben Sie Eigenschaften an.
  - a Wählen Sie **Linux** aus dem Dropdown-Menü **Ziel-VM-Betriebssystem** aus.
  - b Geben Sie **Linux** im Textfeld **Name der Anpassungsspezifikation** ein.
  - c Geben Sie **Rainpole Linux Klonen mit vRealize Automation** in das Textfeld **Beschreibung** ein.
  - d Klicken Sie auf **Weiter**.
- 4 Legen Sie den Computernamen fest.
  - a Wählen Sie **Den Namen der virtuellen Maschine verwenden** aus.
  - b Geben Sie die Domäne, in der geklonte Maschinen bereitgestellt werden, in das Textfeld **Domänenname** ein.  
Beispiel: **rainpole.local**.
  - c Klicken Sie auf **Weiter**.
- 5 Konfigurieren Sie Einstellungen für die Zeitzone.
- 6 Klicken Sie auf **Weiter**.
- 7 Wählen Sie **Standardnetzwerkeinstellungen für das Gastbetriebssystem verwenden und DHCP an allen Netzwerkschnittstellen aktivieren**.
- 8 Folgen Sie den Eingabeaufforderungen, um die noch erforderlichen Informationen einzugeben.
- 9 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Auswahl und klicken Sie auf **Beenden**.

Sie verfügen über eine allgemeine Anpassungsspezifikation, die Sie zum Erstellen von Blueprints zum Klonen von Linux-Maschinen verwenden können.

## Weiter

Melden Sie sich bei der vRealize Automation-Konsole als Konfigurationsadministrator an, den Sie während der Installation erstellt haben, und fordern Sie die Katalogelemente für die schnelle Einrichtung Ihrer Proof-of-Concept-Umgebung an.

## Vorbereiten für Software -Bereitstellung

Verwenden Sie Software für die Bereitstellung von Anwendungen und Middleware im Rahmen des vRealize Automation-Bereitstellungsprozesses für vSphere-, vCloud Director-, vCloud Air- und Amazon AWS-Maschinen.

Sie können Software auf Maschinen bereitstellen, wenn Ihr Blueprint Software unterstützt und wenn Sie den Gast-Agent und den Software-Bootstrap-Agent auf Ihren Referenzmaschinen installieren, bevor Sie sie in Vorlagen, Snapshots oder Amazon-Maschinen-Images konvertieren.

**Tabelle 1-16. Bereitstellungsmethoden, die Software unterstützen**

Maschinentyp	Bereitstellungsmethode	Erforderliche Vorbereitung
vSphere	Klonen	Ein Klon-Blueprint stellt eine vollständige und unabhängige virtuelle Maschine basierend auf der vCenter Server-Vorlage für virtuelle Maschinen bereit. Wenn Ihre Vorlagen zum Klonen Software-Komponenten unterstützen sollen, installieren Sie den Gast-Agent und den Software-Bootstrap-Agent auf Ihrer Referenzmaschine, während Sie eine Vorlage zum Klonen vorbereiten. Siehe <a href="#">Checkliste für das Vorbereiten für die Bereitstellung durch Klonen</a> .
vSphere	Verknüpfter Klon	Ein verknüpfter Klon-Blueprint stellt eine speicherplatzeffiziente Kopie einer vSphere-Maschine basierend auf einem Snapshot bereit. Dabei wird eine Kette von Delta-Festplatten verwendet, um Unterschiede zur übergeordneten Maschine zu verfolgen. Wenn Ihre verknüpften Klon-Blueprints Software-Komponenten unterstützen sollen, installieren Sie den Gast-Agent und den Software-Bootstrap-Agent auf der Maschine, bevor Sie den Snapshot erstellen.  Wenn Ihre Snapshot-Maschine von einer Vorlage geklont wurde, die Software unterstützt, sind die erforderlichen Agents bereits installiert.
vCloud Director	Klonen	Ein Klon-Blueprint stellt eine vollständige und unabhängige virtuelle Maschine basierend auf der vCenter Server-Vorlage für virtuelle Maschinen bereit. Wenn Ihre Vorlagen zum Klonen Software-Komponenten unterstützen sollen, installieren Sie den Gast-Agent und den Software-Bootstrap-Agent auf Ihrer Referenzmaschine, während Sie eine Vorlage zum Klonen vorbereiten. Siehe <a href="#">Checkliste für das Vorbereiten für die Bereitstellung durch Klonen</a> .

**Tabelle 1-16. Bereitstellungsmethoden, die Software unterstützen (Fortsetzung)**

Maschinentyp	Bereitstellungsmethode	Erforderliche Vorbereitung
vCloud Air	Klonen	Ein Klon-Blueprint stellt eine vollständige und unabhängige virtuelle Maschine basierend auf der vCenter Server-Vorlage für virtuelle Maschinen bereit. Wenn Ihre Vorlagen zum Klonen Software-Komponenten unterstützen sollen, installieren Sie den Gast-Agent und den Software-Bootstrap-Agent auf Ihrer Referenzmaschine, während Sie eine Vorlage zum Klonen vorbereiten. Siehe <a href="#">Checkliste für das Vorbereiten für die Bereitstellung durch Klonen</a> .
Amazon AWS	Amazon-Maschinen-Image	Ein Amazon-Maschinen-Image ist eine Vorlage, die eine Softwarekonfiguration einschließlich eines Betriebssystems enthält. Wenn Sie ein Amazon-Maschinen-Image erstellen möchten, das Software unterstützt, stellen Sie eine Verbindung zu einer laufenden Amazon AWS-Instanz her, die ein EBS-Volume als Root-Gerät verwendet. Installieren Sie den Gast-Agent und Software-Bootstrap-Agent auf der Referenzmaschine, und erstellen Sie dann ein Amazon-Maschinen-Image von Ihrer Instanz. Anweisungen zum Erstellen von Amazon EBS-gestützten AMIs finden Sie in der Amazon AWS-Dokumentation.  Damit der Gast-Agent und der Software-Bootstrap-Agent auf bereitgestellten Maschinen funktionieren, müssen Sie Netzwerk-zu-VPC-Konnektivität konfigurieren.

## Vorbereiten der Bereitstellung von Maschinen mit Software

Zur Unterstützung von Software-Komponenten müssen Sie den Gast-Agent und den Software-Bootstrap-Agent auf Ihrer Referenzmaschine installieren, bevor Sie die Konvertierung in eine Vorlage zum Klonen durchführen, ein Amazon-Maschinen-Image erstellen oder einen Snapshot erstellen.

### Vorbereiten einer Windows-Referenzmaschine für die Unterstützung von Software

Sie installieren die unterstützte Java-Laufzeitumgebung, den Gast-Agent und den Software-Bootstrap-Agent auf Ihrer Windows-Referenzmaschine, um eine Vorlage, einen Snapshot oder eine Amazon-Maschineninstanz zu erstellen, die bzw. der Software-Komponenten unterstützt.

Software unterstützt die Skripterstellung mit Windows CMD und PowerShell 2.0.

**Wichtig** Da der Startvorgang nicht unterbrochen werden darf, ist die virtuelle Maschine so zu konfigurieren, dass der Startvorgang der virtuellen Maschine vor der letztendlichen Anmeldeaufforderung des Betriebssystems in keinem Fall angehalten wird. Stellen Sie z. B. sicher, dass keine Prozesse oder Skripte Benutzereingaben anfordern, wenn die virtuelle Maschine gestartet wird.

#### Voraussetzungen

- Identifizieren oder erstellen Sie eine Referenzmaschine.
- Falls Sie zuvor den Gast-Agent oder den Software-Bootstrap-Agent auf dieser Maschine installiert haben, entfernen Sie die Agents und Laufzeitprotokolle. Siehe [Aktualisieren von vorhandenen VM-Vorlagen in vRealize Automation](#).

- Wenn Sie zur Fehlerbehebung oder aus einem anderen Grund Remotezugriff auf den Windows-Remotedesktop der virtuellen Maschine benötigen, installieren Sie die Remotedesktopdienste (RDS) für Windows.
- Vergewissern Sie sich, dass alle Artefakte der Netzwerkkonfiguration aus den Netzwerkkonfigurationsdateien entfernt wurden.
- Wenn Sie die sicherste Methode für eine vertrauenswürdige Kommunikation zwischen dem Gast-Agent und Ihrer Manager Service-Maschine festlegen möchten, rufen Sie das SSL-Zertifikat im PEM-Format von Ihrer Manager Service-Maschine ab. Informationen zum Installieren eines Gast-Agents auf einer Windows-Maschine finden Sie unter [Installieren des Gast-Agents auf einer Windows-Referenzmaschine](#). Weitere Informationen zum Festlegen von Vertrauen für den Gast-Agent finden Sie unter [Konfigurieren des Vertrauensverhältnisses zu einem Server für den Windows-Gast-Agent](#).

### Vorgehensweise

- 1 Melden Sie sich an Ihrer Windows-Referenzmaschine als Windows-Administrator an und öffnen Sie eine Eingabeaufforderung.
- 2 Laden Sie die unterstützte Java-Laufzeitumgebung unter [https://vRealize\\_VA\\_Hostname\\_fqdn/software/index.html](https://vRealize_VA_Hostname_fqdn/software/index.html) herunter und installieren Sie sie.
  - a Laden Sie die ZIP-Datei [https://vRealize\\_VA\\_Hostname\\_fqdn/software/download/jre-version-win64.zip](https://vRealize_VA_Hostname_fqdn/software/download/jre-version-win64.zip) für die Java SE-Laufzeitumgebung herunter.
  - b Erstellen Sie den Ordner `c:\opt\vmware-jre` und entpacken Sie die JRE-ZIP-Datei in diesen Ordner.
  - c Öffnen Sie ein Eingabeaufforderungsfenster und geben Sie zur Überprüfung der Installation `c:\opt\vmware-jre\bin\java -version` ein.  
Es wird die installierte Java-Version angegeben.
- 3 Laden Sie den vRealize Automation-Gast-Agent unter [https://vRealize\\_VA\\_Hostname\\_fqdn/software/index.html](https://vRealize_VA_Hostname_fqdn/software/index.html) herunter und installieren Sie ihn.
  - a Laden Sie die Datei `GugentZip_version` auf Laufwerk C: auf der Referenzmaschine herunter.  
Wählen Sie in Abhängigkeit von Ihrem Betriebssystem `GuestAgentInstaller.exe` (32-Bit) oder `GuestAgentInstaller_x64.exe` (64 Bit) aus.
  - b Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie **Eigenschaften** aus.
  - c Klicken Sie auf **Allgemein**.
  - d Klicken Sie auf **Blockierung aufheben**.
  - e Extrahieren Sie die Dateien nach `C:\`.  
Dadurch wird das Verzeichnis `C:\VRMGuestAgent` erstellt. Benennen Sie dieses Verzeichnis nicht um.

#### 4 Konfigurieren Sie den Gast-Agent zum Kommunizieren mit dem Manager Service.

- a Öffnen Sie eine Eingabeaufforderung mit erweiterten Berechtigungen.
- b Navigieren Sie zu `C:\VRMGuestAgent`.
- c Konfigurieren Sie die vertrauenswürdige Kommunikation zwischen dem Gast-Agent und Ihrer Manager Service-Maschine.

Option	Beschreibung
<b>Lassen Sie zu, dass der Gast-Agent der ersten Maschine vertraut, mit der er verbunden wird.</b>	Es ist keine Konfiguration erforderlich.
<b>Installieren Sie die vertrauenswürdige PEM-Datei manuell.</b>	Speichern Sie die PEM-Datei der Manager Service-Maschine im Verzeichnis <code>C:\VRMGuestAgent\</code> .

- d Führen Sie den folgenden Befehl aus: `win service -i -h Manager_Service_Hostname_fqdn:portnumber -p ssl`.

Die Standardportnummer für den Manager Service ist 443.

Option	Beschreibung
<b>Wenn Sie einen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer des Lastausgleichsdiensts von Manager Service ein. Beispielsweise <code>win service -i -h load_balancer_manager_service.mycompany.com:443 -p ssl</code> .
<b>Wenn Sie keinen Lastausgleichsdienst verwenden</b>	Geben Sie den vollqualifizierten Domännennamen und die Portnummer der Manager Service-Maschine ein. Beispielsweise <code>win service -i -h manager_service_machine.mycompany.com:443 -p ssl</code> .
<b>Wenn Sie ein Amazon-System-Image vorbereiten</b>	Sie müssen angeben, dass Sie Amazon verwenden. Beispielsweise <code>win service -i -h manager_service_machine.mycompany.com:443:443 -p ssl -c ec2</code>

#### 5 Laden Sie die Software-Agent-Bootstrap-Datei unter [https://vRealize\\_VA\\_Hostname\\_fqdn/software/index.html](https://vRealize_VA_Hostname_fqdn/software/index.html) herunter.

- a Laden Sie die Software-Bootstrap-Agent-Datei [https://vRealize\\_VA\\_Hostname\\_fqdn/software/download/vmware-vra-software-agent-bootstrap-windows\\_version.zip](https://vRealize_VA_Hostname_fqdn/software/download/vmware-vra-software-agent-bootstrap-windows_version.zip) herunter.
- b Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie **Eigenschaften** aus.
- c Klicken Sie auf **Allgemein**.
- d Klicken Sie auf **Blockierung aufheben**.

**Wichtig** Wenn Sie diese Windows-Sicherheitsfunktion nicht deaktivieren, können Sie die Agent Bootstrap-Datei für Software nicht verwenden.

- e Entpacken Sie die Datei `vmware-vra-software-agent-bootstrap-windows_version.zip` in den Ordner `c:\temp`.



## 6 Installieren Sie den Software-Bootstrap-Agent.

- a Öffnen Sie eine Windows CMD-Konsole und navigieren Sie zum Ordner `c:\temp`.
- b Geben Sie den Befehl zur Installation von Agent Bootstrap ein.

```
install.bat password=Password managerServiceHost=manager_service_machine.mycompany.com manager-
ServicePort=443 httpsMode=true cloudProvider=ec2|vca|vcd|vsphere
```

Die Standardportnummer für den Manager Service ist 443. Zulässige Werte für `cloudprovider` sind `ec2`, `vca`, `vcd` und `vsphere`. Das Skript `install.bat` erstellt ein Benutzerkonto mit dem Namen „darwin“ für den Software-Bootstrap-Agent und verwendet das von Ihnen im Installationsbefehl festgelegte Kennwort. Das von Ihnen festgelegte *Kennwort* muss den Anforderungen für Windows-Kennwörter genügen.

Falls die Installation aufgrund einer .NET-Abhängigkeit fehlschlägt, finden Sie im folgenden Artikel weitere Informationen: <https://technet.microsoft.com/en-us/library/dn482071.aspx>

## 7 Stellen Sie sicher, dass der Benutzer **darwin** vorhanden ist.

- a Geben Sie an der Eingabeaufforderung `lusrmgr.msc` ein.
- b Stellen Sie sicher, dass der Benutzer **darwin\_user** vorhanden ist und zur Administratorgruppe gehört.
- c Konfigurieren Sie das Kennwort so, dass es nie abläuft.

Die Einstellung sorgt dafür, dass nach 30 Tagen die Vorlage weiterhin verwendbar bleibt.

Wenn dieser Benutzer nicht verfügbar ist, vergewissern Sie sich, dass das Windows-Serverkennwort korrekt ist.

## 8 Fahren Sie die virtuelle Windows-Maschine herunter.

### Weiter

Konvertieren Sie Ihre Referenzmaschine in eine Vorlage zum Klonen, ein Amazon-Maschinen-Image oder einen Snapshot, welche Ihre IaaS-Architekten beim Erstellen von Blueprints verwenden können.

## Vorbereiten einer Linux-Referenzmaschine für die Unterstützung von Software

Mithilfe eines einzelnen Skripts installieren Sie die unterstützte Java-Laufzeitumgebung, den Gast-Agent und den Software-Bootstrap-Agent auf Ihrer Linux-Referenzmaschine, um eine Vorlage, einen Snapshot oder eine Amazon-Maschineninstanz zu erstellen, die bzw. der Software-Komponenten unterstützt.

Software unterstützt Skripting mit Bash.

---

**Wichtig** Da der Startvorgang nicht unterbrochen werden darf, ist die virtuelle Maschine so zu konfigurieren, dass der Startvorgang der virtuellen Maschine vor der letztendlichen Anmeldeaufforderung des Betriebssystems in keinem Fall angehalten wird. Stellen Sie z. B. sicher, dass keine Prozesse oder Skripte Benutzereingaben anfordern, wenn die virtuelle Maschine gestartet wird.

---

## Voraussetzungen

- Identifizieren oder erstellen Sie eine Linux-Referenzmaschine und vergewissern Sie sich, dass in Abhängigkeit von Ihrem Linux-Betriebssystem die folgenden Befehle verfügbar sind:
  - `yum` oder `apt-get`
  - `wget` oder `curl`
  - `python`
  - `dmidecode` gemäß den Anforderungen von Cloud-Anbietern
  - Allgemeine Anforderungen wie beispielsweise `sed`, `awk`, `perl`, `chkconfig`, `unzip` und `grep` in Abhängigkeit von Ihrer Linux-Distribution

Verwandte Informationen zu den Voraussetzungen für Linux finden Sie im Skript `prepare_vra_template.sh`.

- Wenn Sie planen, zu Fehlerbehebungs Zwecken oder aus anderen Gründen mit Linux `ssh`-Protokollierung `remote` auf die virtuelle Maschine zuzugreifen, installieren Sie den OpenSSH-Server und -Client für Linux.
- Entfernen Sie die Artefakte der Netzwerkkonfiguration aus den Netzwerkkonfigurationsdateien.

## Vorgehensweise

- 1 Melden Sie sich an Ihrer Referenzmaschine als Root-Benutzer an.
- 2 Laden Sie das Installationsskript aus der vRealize Automation-Appliance herunter.

```
wget https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

Wenn in Ihrer Umgebung selbst signierte Zertifikate verwendet werden, müssen Sie möglicherweise die `wget`-Option `--no-check-certificate` verwenden. Beispiel:

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

- 3 Sorgen Sie dafür, dass das Skript `prepare_vra_template.sh` ausgeführt werden kann.

```
chmod +x prepare_vra_template.sh
```

- 4 Führen Sie das Installationsprogramm-Skript `prepare_vra_template.sh` aus.

```
./prepare_vra_template.sh
```

Sie können den Hilfebefehl `./prepare_vra_template.sh --help` ausführen, um Informationen zu nicht interaktiven Optionen und erwarteten Werten zu erhalten.

## 5 Folgen Sie den Eingabeaufforderungen, um die Installation abzuschließen.

Wenn die Installation erfolgreich abgeschlossen wurde, wird eine Bestätigungsmeldung angezeigt. Werden in der Konsole eine Fehlermeldung und Protokolle angezeigt, beheben Sie die Fehler und führen Sie das Installationsprogramm-Skript erneut aus.

## 6 Schalten Sie die Linux-VM aus.

Das Skript entfernt vorherige Installationen des Software-Bootstrap-Agents und installiert die unterstützten Versionen der Java-Laufzeitumgebung, den Gast-Agent und den Software-Bootstrap-Agent.

### Weiter

Wandeln Sie auf dem Hypervisor oder dem Cloud-Anbieter Ihre Referenzmaschine in eine Vorlage, einen Snapshot oder ein Amazon Machine Image um, die Ihre Infrastruktur-Architekten beim Erstellen von Blueprints verwenden können.

## Aktualisieren von vorhandenen VM-Vorlagen in vRealize Automation

Wenn Sie Ihre Vorlagen, Amazon-System-Images oder Snapshots für die neueste Version des Windows Software-Bootstrap-Agents aktualisieren oder wenn Sie manuell auf den neuesten Linux Software-Bootstrap-Agent aktualisieren, anstatt das Skript `prepare_vra_template.sh` zu verwenden, müssen Sie vorhandene Versionen entfernen und Protokolle löschen.

### Linux

Für Linux-Referenzmaschinen wird durch Ausführen des Skripts `prepare_vra_template.sh` der Agent zurückgesetzt und alle Protokolle werden entfernt, bevor die Neuinstallation durchgeführt wird. Wenn Sie jedoch manuell installieren möchten, müssen Sie sich als Root-Benutzer bei der Referenzmaschine anmelden und den Befehl zum Zurücksetzen und Entfernen der Artefakte ausführen.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

### Windows

Für Windows-Referenzmaschinen entfernen Sie den vorhandenen Software-Agent-Bootstrap und den vRealize Automation 6.0-Gast-Agent (oder höher) und löschen vorhandene Laufzeitprotokolldateien. Führen Sie in einem PowerShell-Befehlsfenster die Befehle zum Entfernen des Agents und der Artefakte aus.

```
c:\opt\vmware-appdirector\agent-bootstrap\agent_bootstrap_removal.bat
c:\opt\vmware-appdirector\agent-bootstrap\agent_reset.bat
```

## Szenario: Vorbereiten einer vSphere CentOS-Vorlage für Klonmaschinen- und Softwarekomponenten-Blueprints

Als vCenter Server-Administrator möchten Sie eine vSphere-Vorlage vorbereiten, mit der Ihre vRealize Automation-Architekten Linux CentOS-Maschinen klonen können. Wenn Sie sicherstellen möchten, dass Ihre Vorlage Blueprints mit Softwarekomponenten unterstützt, installieren Sie den Gast-Agent und den Software-Bootstrap-Agent, bevor Sie Ihre Referenzmaschine in eine Vorlage konvertieren.

## Voraussetzungen

- Identifizieren oder erstellen Sie eine Linux CentOS-Referenzmaschine, auf der VMware Tools installiert ist. Schließen Sie mindestens einen Netzwerkadapter zur Unterstützung der Internetkonnektivität ein, falls Blueprint-Architekten diese Funktion nicht auf der Blueprint-Ebene hinzufügen. Weitere Informationen zum Erstellen virtueller Maschinen erhalten Sie in der Dokumentation zu vSphere.
- Zum Konvertieren einer virtuellen Maschine in eine Vorlage müssen Sie mit einem vCenter Server verbunden sein. Das Erstellen von Vorlagen ist nicht möglich, wenn der vSphere-Client direkt mit einem vSphere ESXi-Host verbunden ist.

## Vorgehensweise

### 1 [Szenario: Vorbereiten der Referenzmaschine auf Anpassungen des Gast-Agent und Softwarekomponenten](#)

Damit Ihre Vorlage Softwarekomponenten unterstützen kann, installieren Sie den Software-Bootstrap-Agent und den dafür vorausgesetzten Gast-Agent auf Ihrer Referenzmaschine. Die Agents stellen sicher, dass vRealize Automation-Architekten, die Ihre Vorlage verwenden, Softwarekomponenten in ihre Blueprints aufnehmen können.

### 2 [Szenario: Konvertieren einer CentOS-Referenzmaschine in eine Vorlage](#)

Nachdem Sie den Gast-Agenten und den Software-Bootstrap-Agenten auf Ihrer Referenzmaschine installiert haben, wandeln Sie Ihre Referenzmaschine in eine Vorlage um, die vRealize Automation-Architekten zum Erstellen von Klonmaschinen-Blueprints verwenden können.

### 3 [Szenario: Erstellen einer Anpassungsspezifikation für das Klonen mit vSphere](#)

Erstellen Sie eine Anpassungsspezifikation für Ihre Blueprint-Architekten zur Verwendung mit Ihrer `cpb_centos_63_x84`-Vorlage.

Sie haben eine Vorlage und Anpassungsspezifikation anhand Ihrer Referenzmaschine erstellt, mit deren Hilfe Blueprint-Architekten vRealize Automation-Blueprints erstellen können, mit denen Linux CentOS-Maschinen geklont werden. Sie haben den Software-Bootstrap-Agent und den Gast-Agent auf Ihrer Referenzmaschine installiert. Deshalb können Architekten mithilfe Ihrer Vorlage ausgefeilte Katalogelement-Blueprints erstellen, die Softwarekomponenten oder Gast-Agent-Anpassungen wie beispielsweise das Ausführen von Skripten oder das Formatieren von Festplatten beinhalten. Da Sie VMware Tools installiert haben, können Architekten und Katalogadministratoren Benutzern das Ausführen von Aktionen für Maschinen erlauben, wie beispielsweise das Ausführen einer Neukonfiguration oder eines Neustarts und das Erstellen von Snapshots.

## Weiter

Nach der Konfiguration von Benutzern, Gruppen und Ressourcen für vRealize Automation können Sie mithilfe Ihrer Vorlage und Anpassungsspezifikation einen Maschinen-Blueprint für das Klonen erstellen. Siehe [Szenario: Erstellen eines vSphere CentOS-Blueprints zum Klonen in Rainpole](#).

## Szenario: Vorbereiten der Referenzmaschine auf Anpassungen des Gast-Agent und Softwarekomponenten

Damit Ihre Vorlage Softwarekomponenten unterstützen kann, installieren Sie den Software-Bootstrap-Agent und den dafür vorausgesetzten Gast-Agent auf Ihrer Referenzmaschine. Die Agents stellen sicher, dass vRealize Automation-Architekten, die Ihre Vorlage verwenden, Softwarekomponenten in ihre Blueprints aufnehmen können.

Zur Vereinfachung des Vorgangs laden Sie ein vRealize Automation-Skript herunter, das beide Agents installiert, anstatt separate Pakete herunterzuladen und zu installieren.

Das Skript stellt auch eine Verbindung zur Manager Service-Instanz her und lädt das SSL-Zertifikat herunter, das ein Vertrauensverhältnis zwischen dem Manager Service und den anhand der Vorlage bereitgestellten Maschinen einrichtet. Beachten Sie, dass das Herunterladen des Zertifikats seitens des Skripts weniger sicher ist als ein manuelles Abrufen und Installieren des SSL-Zertifikats für den Manager Service auf Ihrer Referenzmaschine in `/usr/share/gugent/cert.pem`.

### Vorgehensweise

- 1 Rufen Sie in Ihrem Webbrowser folgende URL auf:  
`https://vrealize-automation-appliance-FQDN/software/index.html`
- 2 Speichern Sie das Skript `prepare_vra_template.sh` auf Ihrer Referenzmaschine.
- 3 Machen Sie auf Ihrer Referenzmaschine die Datei `prepare_vra_template.sh` ausführbar.

```
chmod +x prepare_vra_template.sh
```

- 4 Führen Sie `prepare_vra_template.sh` aus.

```
./prepare_vra_template.sh
```

- 5 Folgen Sie den Anweisungen am Bildschirm.

Wenn Sie nicht interaktive Informationen zu Optionen und Werten benötigen, geben Sie `./prepare_vra_template.sh --help` ein.

Bei Abschluss der Installation wird eine Bestätigungsmeldung angezeigt. Wenn Fehlermeldungen und Protokolle angezeigt werden, beheben Sie die Probleme und führen Sie das Skript erneut aus.

## Szenario: Konvertieren einer CentOS-Referenzmaschine in eine Vorlage

Nachdem Sie den Gast-Agenten und den Software-Bootstrap-Agenten auf Ihrer Referenzmaschine installiert haben, wandeln Sie Ihre Referenzmaschine in eine Vorlage um, die vRealize Automation-Architekten zum Erstellen von Klonmaschinen-Blueprints verwenden können.

Nachdem Ihre Referenzmaschine in eine Vorlage konvertiert wurde, können Sie die Vorlage weder bearbeiten noch einschalten. Sie müssen sie erst wieder in eine virtuelle Maschine zurückkonvertieren.

## Vorgehensweise

- 1 Melden Sie sich an Ihrer Referenzmaschine als Root-Benutzer an und bereiten Sie die Maschine zum Konvertieren vor.

- a Entfernen Sie udev-Persistenzregeln.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- b Aktivieren Sie bei von dieser Vorlage geklonten Maschinen eigene eindeutige Bezeichner.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- c Wenn Sie die Referenzmaschine nach der Installation des Software-Bootstrap-Agent neu gestartet oder neu konfiguriert haben, setzen Sie den Agent zurück.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- d Fahren Sie die Maschine herunter.

```
shutdown -h now
```

- 2 Melden Sie sich beim vSphere Web Client als Administrator an.
- 3 Klicken Sie mit der rechten Maustaste auf Ihre Referenzmaschine und wählen Sie **Einstellungen bearbeiten**.
- 4 Geben Sie **cpb\_centos\_63\_x84** im Textfeld **VM-Name** ein.
- 5 Selbst wenn Ihre Referenzmaschine über ein CentOS-Gastbetriebssystem verfügt, wählen Sie aus dem Dropdown-Menü **Version des Gastbetriebssystems** die Option **Red Hat Enterprise Linux 6 (64-Bit)** aus.

Wenn Sie CentOS auswählen, funktionieren Ihre Vorlage und Anpassungsspezifikation möglicherweise nicht wie erwartet.

- 6 Klicken Sie im vSphere Web Client mit der rechten Maustaste auf Ihre Referenzmaschine und wählen Sie **Vorlage > In Vorlage konvertieren**.

vCenter Server markiert Ihre Referenzmaschine „cpb\_centos\_63\_x84“ als Vorlage und zeigt die Aufgabe im Fensterbereich „Kürzlich bearbeitete Aufgaben“ an. Wenn Ihre vSphere-Umgebung bereits von vRealize Automation verwaltet wird, wird Ihre Vorlage während der nächsten automatisierten Datenerfassung erkannt. Wenn Sie vRealize Automation noch nicht konfiguriert haben, wird die Vorlage während dieses Vorgangs erfasst.

## Szenario: Erstellen einer Anpassungsspezifikation für das Klonen mit vSphere

Erstellen Sie eine Anpassungsspezifikation für Ihre Blueprint-Architekten zur Verwendung mit Ihrer cpb\_centos\_63\_x84-Vorlage.

## Vorgehensweise

- 1 Melden Sie sich beim vSphere Web Client als Administrator an.
- 2 Klicken Sie auf der Startseite auf **Anpassungsspezifikations-Manager**, um den Assistenten zu öffnen.
- 3 Klicken Sie auf das Symbol **Neu**.
- 4 Klicken Sie auf das Symbol **Neu**.
- 5 Geben Sie Eigenschaften an.
  - a Wählen Sie **Linux** aus dem Dropdown-Menü **Ziel-VM-Betriebssystem** aus.
  - b Geben Sie **Customspecs** im Textfeld **Name der Anpassungsspezifikation** ein.
  - c Geben Sie **cpb\_centos\_63\_x84 Klonen mit vRealize Automation** in das Textfeld **Beschreibung** ein.
  - d Klicken Sie auf **Weiter**.
- 6 Legen Sie den Computernamen fest.
  - a Wählen Sie **Den Namen der virtuellen Maschine verwenden** aus.
  - b Geben Sie die Domäne, in der geklonte Maschinen bereitgestellt werden, in das Textfeld **Domänenname** ein.
  - c Klicken Sie auf **Weiter**.
- 7 Konfigurieren Sie Einstellungen für die Zeitzone.
- 8 Klicken Sie auf **Weiter**.
- 9 Wählen Sie **Standardnetzwerkeinstellungen für das Gastbetriebssystem verwenden und DHCP an allen Netzwerkschnittstellen aktivieren**.

Fabric-Administratoren und Infrastruktur-Architekten handhaben Netzwerkeinstellungen für bereitgestellte Maschinen, indem sie Netzwerkprofile in vRealize Automation erstellen und verwenden.
- 10 Folgen Sie den Eingabeaufforderungen, um die noch erforderlichen Informationen einzugeben.
- 11 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Auswahl und klicken Sie auf **Beenden**.

## Szenario: Vorbereiten auf den Import des vSphere - Beispielanwendungs-Blueprints „Dukes Bank“

Als vCenter Server-Administrator möchten Sie eine vSphere CentOS 6.x-Linux-Vorlage und -Anpassungsspezifikation vorbereiten, die Sie für die Bereitstellung der vRealize Automation-Beispielanwendung „Dukes Bank“ verwenden können.

Wenn Sie sicherstellen möchten, dass Ihre Vorlage die Softwarekomponenten der Beispielanwendung unterstützt, installieren Sie den Gast-Agent und den Software-Bootstrap-Agent auf Ihrer Linux-Referenzmaschine, bevor Sie die Konvertierung in eine Vorlage und Erstellung einer Anpassungsspezifikation durchführen. Sie deaktivieren SELinux auf Ihrer Referenzmaschine, um sicherzustellen, dass Ihre Vorlage die in der Beispielanwendung „Dukes Bank“ verwendete spezielle Implementierung von MySQL unterstützt.

### Voraussetzungen

- Installieren Sie vRealize Automation und führen Sie eine vollständige Konfiguration aus. Siehe *Installieren und Konfigurieren von vRealize Automation für das Rainpole-Szenario*.
- Identifizieren oder erstellen Sie eine CentOS 6.x-Linux-Referenzmaschine, auf der VMware Tools installiert ist. Weitere Informationen zum Erstellen virtueller Maschinen erhalten Sie in der Dokumentation zu vSphere.
- Zum Konvertieren einer virtuellen Maschine in eine Vorlage müssen Sie mit einem vCenter Server verbunden sein. Das Erstellen von Vorlagen ist nicht möglich, wenn der vSphere-Client direkt mit einem vSphere ESXi-Host verbunden ist.

### Vorgehensweise

#### 1 Szenario: Vorbereiten der Referenzmaschine auf die vSphere-Beispielanwendung „Dukes Bank“

Wenn Ihre Vorlage die Beispielanwendung „Dukes Bank“ unterstützen soll, müssen Sie sowohl den Gast-Agent als auch den Software-Bootstrap-Agent auf Ihrer Referenzmaschine installieren, sodass vRealize Automation die Softwarekomponenten bereitstellen kann. Zur Vereinfachung des Prozesses laden Sie ein vRealize Automation-Skript, mit dem sowohl der Gast-Agent als auch der Software-Bootstrap-Agent installiert wird, herunter und führen dieses aus. Auf diese Weise müssen Sie die Pakete nicht separat herunterladen und installieren.

#### 2 Szenario: Konvertieren einer Referenzmaschine in eine Vorlage für die vSphere-Anwendung „Dukes Bank“

Nachdem Sie den Gast-Agent und den Software-Bootstrap-Agent auf Ihrer Referenzmaschine installiert haben, deaktivieren Sie SELinux, um sicherzustellen, dass Ihre Vorlage die Implementierung von MySQL in der Beispielanwendung „Dukes Bank“ unterstützt. Sie wandeln Ihre Referenzmaschine in eine Vorlage um, die zum Bereitstellen der vSphere-Beispielanwendung „Dukes Bank“ verwendet werden kann.

#### 3 Szenario: Erstellen einer Anpassungsspezifikation für das Klonen der Maschinen der vSphere-Beispielanwendung „Dukes Bank“

Sie erstellen eine Anpassungsspezifikation zur Verwendung mit Ihrer Vorlage der „Dukes Bank“-Maschine.

Sie haben eine Vorlage und Anpassungsspezifikation anhand Ihrer Referenzmaschine erstellt, die die vRealize Automation-Beispielanwendung „Dukes Bank“ unterstützt.



## Szenario: Vorbereiten der Referenzmaschine auf die vSphere - Beispielanwendung „Dukes Bank“

Wenn Ihre Vorlage die Beispielanwendung „Dukes Bank“ unterstützen soll, müssen Sie sowohl den Gast-Agent als auch den Software-Bootstrap-Agent auf Ihrer Referenzmaschine installieren, sodass vRealize Automation die Softwarekomponenten bereitstellen kann. Zur Vereinfachung des Prozesses laden Sie ein vRealize Automation-Skript, mit dem sowohl der Gast-Agent als auch der Software-Bootstrap-Agent installiert wird, herunter und führen dieses aus. Auf diese Weise müssen Sie die Pakete nicht separat herunterladen und installieren.

### Vorgehensweise

- 1 Melden Sie sich an Ihrer Referenzmaschine als Root-Benutzer an.
- 2 Laden Sie das Installationsskript aus der vRealize Automation-Appliance herunter.

```
wget https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

Wenn in Ihrer Umgebung selbst signierte Zertifikate verwendet werden, müssen Sie möglicherweise die wget-Option `--no-check-certificate` verwenden. Beispiel:

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

- 3 Sorgen Sie dafür, dass das Skript `prepare_vra_template.sh` ausgeführt werden kann.

```
chmod +x prepare_vra_template.sh
```

- 4 Führen Sie das Installationsprogramm-Skript `prepare_vra_template.sh` aus.

```
./prepare_vra_template.sh
```

Sie können den Hilfebefehl `./prepare_vra_template.sh --help` ausführen, um Informationen zu nicht interaktiven Optionen und erwarteten Werten zu erhalten.

- 5 Folgen Sie den Eingabeaufforderungen, um die Installation abzuschließen.

Wenn die Installation erfolgreich abgeschlossen wurde, wird eine Bestätigungsmeldung angezeigt. Werden in der Konsole eine Fehlermeldung und Protokolle angezeigt, beheben Sie die Fehler und führen Sie das Installationsprogramm-Skript erneut aus.

Sie haben den Software-Bootstrap-Agent und dessen Voraussetzung, den Gast-Agent, installiert, um sicherzustellen, dass die Beispielanwendung „Dukes Bank“ Softwarekomponenten erfolgreich bereitstellt. Durch das Skript wurde auch eine Verbindung zu Ihrer Manager Service-Instanz hergestellt sowie das SSL-Zertifikat heruntergeladen, um ein Vertrauensverhältnis zwischen dem Manager Service und den an-

hand Ihrer Vorlage bereitgestellten Maschinen einzurichten. Es ist jedoch eine sicherere Vorgehensweise, wenn Sie das Manager Service-SSL-Zertifikat abrufen und manuell auf Ihrer Referenzmaschine in `/usr/share/gugent/cert.pem` installieren. Sie können dieses Zertifikat nun auch manuell ersetzen, wenn der Sicherheit eine hohe Priorität beigemessen wird.

## Szenario: Konvertieren einer Referenzmaschine in eine Vorlage für die vSphere -Anwendung „Dukes Bank“

Nachdem Sie den Gast-Agent und den Software-Bootstrap-Agent auf Ihrer Referenzmaschine installiert haben, deaktivieren Sie SELinux, um sicherzustellen, dass Ihre Vorlage die Implementierung von MySQL in der Beispielanwendung „Dukes Bank“ unterstützt. Sie wandeln Ihre Referenzmaschine in eine Vorlage um, die zum Bereitstellen der vSphere-Beispielanwendung „Dukes Bank“ verwendet werden kann.

Nachdem Ihre Referenzmaschine in eine Vorlage konvertiert wurde, können Sie die Vorlage weder bearbeiten noch einschalten. Sie müssen sie erst wieder in eine virtuelle Maschine zurückkonvertieren.

### Vorgehensweise

- 1 Melden Sie sich an Ihrer Referenzmaschine als Root-Benutzer an.

- a Bearbeiten Sie die Datei `/etc/selinux/config`, um SELinux zu deaktivieren.

```
SELINUX=disabled
```

Wenn Sie SELinux nicht deaktivieren, funktioniert die MySQL-Softwarekomponente der Beispielanwendung „Dukes Bank“ möglicherweise nicht wie erwartet.

- b Entfernen Sie udev-Persistenzregeln.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- c Aktivieren Sie bei von dieser Vorlage geklonten Maschinen eigene eindeutige Bezeichner.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- d Wenn Sie die Referenzmaschine nach der Installation des Software-Bootstrap-Agent neu gestartet oder neu konfiguriert haben, setzen Sie den Agent zurück.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- e Fahren Sie die Maschine herunter.

```
shutdown -h now
```

- 2 Melden Sie sich beim vSphere Web Client als Administrator an.
- 3 Klicken Sie mit der rechten Maustaste auf Ihre Referenzmaschine und wählen Sie **Einstellungen bearbeiten**.
- 4 Im Textfeld **VM-Name** geben Sie **dukes\_bank\_template** ein.

- 5 Wenn Ihre Referenzmaschine über ein CentOS-Gastbetriebssystem verfügt, wählen Sie aus dem Dropdown-Menü **Version des Gastbetriebssystems** die Option **Red Hat Enterprise Linux 6 (64-Bit)** aus.

Wenn Sie CentOS auswählen, funktionieren Ihre Vorlage und Anpassungsspezifikation möglicherweise nicht wie erwartet.

- 6 Klicken Sie auf **OK**.
- 7 Klicken Sie im vSphere Web Client mit der rechten Maustaste auf Ihre Referenzmaschine und wählen Sie **Vorlage > In Vorlage konvertieren**.

vCenter Server markiert Ihre Referenzmaschine „dukes\_bank\_template“ als Vorlage und zeigt die Aufgabe im Fensterbereich „Kürzlich bearbeitete Aufgaben“ an. Wenn Ihre vSphere-Umgebung bereits von vRealize Automation verwaltet wird, wird Ihre Vorlage während der nächsten automatisierten Datenerfassung erkannt. Wenn Sie vRealize Automation noch nicht konfiguriert haben, wird die Vorlage während dieses Vorgangs erfasst.

## Szenario: Erstellen einer Anpassungsspezifikation für das Klonen der Maschinen der vSphere -Beispielanwendung „Dukes Bank“

Sie erstellen eine Anpassungsspezifikation zur Verwendung mit Ihrer Vorlage der „Dukes Bank“-Maschine.

### Vorgehensweise

- 1 Melden Sie sich beim vSphere Web Client als Administrator an.
- 2 Klicken Sie auf der Startseite auf **Anpassungsspezifikations-Manager**, um den Assistenten zu öffnen.
- 3 Klicken Sie auf das Symbol **Neu**.
- 4 Geben Sie Eigenschaften an.
  - a Wählen Sie **Linux** aus dem Dropdown-Menü **Ziel-VM-Betriebssystem** aus.
  - b Geben Sie **Customspecs\_sample** im Textfeld **Name der Anpassungsspezifikation** ein.
  - c Geben Sie **Dukes Bank-Anpassungsspezifikation** im Textfeld **Beschreibung** ein.
  - d Klicken Sie auf **Weiter**.
- 5 Legen Sie den Computernamen fest.
  - a Wählen Sie **Den Namen der virtuellen Maschine verwenden** aus.
  - b Geben Sie die Domäne, auf der Sie die Beispielanwendung „Dukes Bank“ bereitstellen möchten, im Textfeld **Domänenname** ein.
  - c Klicken Sie auf **Weiter**.
- 6 Konfigurieren Sie Einstellungen für die Zeitzone.
- 7 Klicken Sie auf **Weiter**.

- 8 Wählen Sie **Standardnetzwerkeinstellungen für das Gastbetriebssystem verwenden und DHCP an allen Netzwerkschnittstellen aktivieren**.

Fabric-Administratoren und Infrastruktur-Architekten handhaben Netzwerkeinstellungen für bereitgestellte Maschinen, indem sie Netzwerkprofile in vRealize Automation erstellen und verwenden.

- 9 Folgen Sie den Eingabeaufforderungen, um die noch erforderlichen Informationen einzugeben.
- 10 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Auswahl und klicken Sie auf **Beenden**.

Sie haben eine Vorlage und Anpassungsspezifikation erstellt, die Sie zur Bereitstellung der Beispielanwendung „Dukes Bank“ verwenden können.

#### Weiter

- 1 Erstellen Sie ein externes Netzwerkprofil zum Bereitstellen eines Gateways und eines Bereichs von IP-Adressen. Siehe [Erstellen eines externen Netzwerkprofils mithilfe eines externen IPAM-Anbieters](#).
- 2 Ordnen Sie Ihr externes Netzwerkprofil zu Ihrer vSphere-Reservierung zu. Siehe [Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer](#). Die Beispielanwendung kann ohne ein externes Netzwerkprofil nicht erfolgreich bereitgestellt werden.
- 3 Importieren Sie die Beispielanwendung „Dukes Bank“ in Ihre Umgebung. Siehe [Szenario: Importieren der vSphere-Beispielanwendung „Dukes Bank“ und Konfigurieren für Ihre Umgebung](#).

# Konfigurieren der Mandanteneinstellungen

## 2

Mandantenadministratoren konfigurieren Mandanteneinstellungen, wie zum Beispiel die Benutzerauthentifizierung, und verwalten Benutzerrollen und Business-Gruppen. Systemadministratoren und Mandantenadministratoren konfigurieren Optionen, wie zum Beispiel E-Mail-Server zur Verarbeitung von Benachrichtigungen und das Branding für die vRealize Automation-Konsole.

Sie können die Checkliste für die Konfiguration von Mandanteneinstellungen verwenden, um eine allgemeine Übersicht über die Abfolge der Schritte zu erhalten, die für die Konfiguration von Mandanteneinstellungen erforderlich sind.

**Tabelle 2-1. Checkliste für die Konfiguration von Mandanteneinstellungen**

Aufgabe	vRealize Automation-Rolle	Details
<input type="checkbox"/> Erstellen von Benutzerkonten und Zuweisen eines Mandantenadministrators.	Systemadministrator	Ein Beispiel zum Erstellen von lokalen Benutzerkonten finden Sie unter <a href="#">Szenario: Erstellen von lokalen Benutzerkonten für Rainpole</a> .
<input type="checkbox"/> Konfigurieren der Verzeichnisverwaltung zum Einrichten der Mandanten-Identitätsverwaltung und für den Zugriff auf Steuerungseinstellungen.	Mandantenadministrator	<a href="#">Auswählen der Verzeichnisverwaltungs-Konfigurationsoptionen</a>
<input type="checkbox"/> Erstellen von Business-Gruppen und benutzerdefinierten Gruppen und Erteilen von Zugriffsrechten für Benutzer auf die vRealize Automation-Konsole.	Mandantenadministrator	<a href="#">Konfigurieren von Gruppen und Benutzerrollen</a>
<input type="checkbox"/> (Optional) Erstellen von zusätzlichen Mandanten, sodass Benutzer auf die entsprechenden Anwendungen und Ressourcen zugreifen können, die sie zum Abschließen ihrer zugewiesenen Aufgaben benötigen.	Systemadministrator	<a href="#">Erstellen weiterer Mandanten</a>
<input type="checkbox"/> (Optional) Konfigurieren von benutzerdefiniertem Branding auf den Anmeldeseiten von Mandanten und auf Anwendungsseiten der vRealize Automation-Konsole.	<ul style="list-style-type: none"><li>■ Systemadministrator</li><li>■ Mandantenadministrator</li></ul>	<a href="#">Konfigurieren des benutzerdefinierten Brandings</a>
<input type="checkbox"/> (Optional) Konfigurieren von vRealize Automation, so dass Benachrichtigungen an Benutzer gesendet werden, wenn bestimmte Ereignisse auftreten.	<ul style="list-style-type: none"><li>■ Systemadministrator</li><li>■ Mandantenadministrator</li></ul>	<a href="#">Checkliste für die Konfiguration von Benachrichtigungen</a>

**Tabelle 2-1. Checkliste für die Konfiguration von Mandanteneinstellungen (Fortsetzung)**

Aufgabe	vRealize Automation-Rolle	Details
<input type="checkbox"/> (Optional) Konfigurieren von vRealize Orchestrator zur Unterstützung von XaaS und weiteren Optionen zur Erweiterbarkeit.	<ul style="list-style-type: none"> <li>■ Systemadministrator</li> <li>■ Mandantenadministrator</li> </ul>	<a href="#">Konfigurieren von vRealize Orchestrator und Plug-ins</a>
<input type="checkbox"/> (Optional) Erstellen einer benutzerdefinierten Remote-desktop-Protokolldatei, die von IaaS-Architekten in Blueprints zum Konfigurieren von RDP-Einstellungen verwendet wird.	Systemadministrator	<a href="#">Erstellen einer benutzerdefinierten RDP-Datei zur Unterstützung von RDP-Verbindungen für bereitgestellte Maschinen</a>
<input type="checkbox"/> (Optional) Definieren von Datacenter-Standorten, die Ihre Fabric-Administratoren und IaaS-Architekten nutzen können, um Benutzern zu erlauben, einen geeigneten Standort für die Bereitstellung auszuwählen, wenn sie Maschinen anfordern.	Systemadministrator	Ein Beispiel über das Hinzufügen von Datacenter-Standorten finden Sie unter <a href="#">Szenario: Hinzufügen von Datacenter-Standorten für regionsübergreifende Bereitstellungen</a> .

Dieses Kapitel behandelt die folgenden Themen:

- [Auswählen der Verzeichnisverwaltungs-Konfigurationsoptionen](#)
- [Szenario: Konfigurieren eines Active Directory-Links für hochverfügbare vRealize Automation-Bereitstellung](#)
- [Konfigurieren der Smartcard-Authentifizierung für vRealize Automation](#)
- [Erstellen eines Links für Active Directory mit mehreren Domänen oder mit mehreren Gesamtstrukturen](#)
- [Konfigurieren von Gruppen und Benutzerrollen](#)
- [Szenario: Konfigurieren des Standardmandanten für Rainpole](#)
- [Erstellen weiterer Mandanten](#)
- [Löschen eines Mandanten](#)
- [Konfigurieren des benutzerdefinierten Brandings](#)
- [Checkliste für die Konfiguration von Benachrichtigungen](#)
- [Erstellen einer benutzerdefinierten RDP-Datei zur Unterstützung von RDP-Verbindungen für bereitgestellte Maschinen](#)
- [Szenario: Hinzufügen von Datacenter-Standorten für regionsübergreifende Bereitstellungen](#)
- [Konfigurieren von vRealize Orchestrator und Plug-ins](#)

## Auswählen der Verzeichnisverwaltungs-Konfigurationsoptionen

Sie können mithilfe der Funktionen der vRealize Automation-Verzeichnisverwaltung einen Active Directory-Link Ihren Benutzerauthentifizierungs-Anforderungen gemäß konfigurieren.

Die Verzeichnisverwaltung bietet viele Optionen zur Unterstützung einer in hohem Maße angepassten Benutzerauthentifizierung.

**Tabelle 2-2. Auswählen der Verzeichnisverwaltungs-Konfigurationsoptionen**

Konfigurationsoption	Prozedur
Konfigurieren eines Links zu Active Directory.	<ol style="list-style-type: none"> <li>1 Konfigurieren eines Links zu Active Directory. Siehe <a href="#">Konfigurieren eines Links zu Active Directory</a>.</li> <li>2 Wenn Sie vRealize Automation für Hochverfügbarkeit konfiguriert haben, finden Sie weitere Informationen unter <a href="#">Verzeichnisverwaltung für Hochverfügbarkeit konfigurieren</a>.</li> </ol>
(Optional) Erhöhen der Sicherheit eines auf Benutzer-ID und Kennwort basierenden Verzeichnis-Links durch Konfiguration einer bidirektionalen Integration mit Active Directory-Verbindungsdiensten.	<a href="#">Konfigurieren einer bidirektionalen Vertrauensstellung zwischen vRealize Automation und Active Directory</a>
(Optional) Hinzufügen von Benutzern und Gruppen zu einem vorhandenen Active Directory-Link.	<a href="#">Benutzer oder Gruppen zu einer Active Directory-Verbindung hinzufügen.</a>
(Optional) Bearbeiten der Standardrichtlinie, um benutzerdefinierte Regeln für einen Active Directory-Link anzuwenden.	<a href="#">Verwalten der Benutzerzugriffsrichtlinie.</a>
(Optional) Konfigurieren von Netzwerkbereichen, um die IP-Adressen einzuschränken, über die die Benutzer sich beim System anmelden können, und Verwalten von Anmeldebeschränkungen (Zeitüberschreitung, Anzahl der Anmeldeversuche vor einer Kontosperrung).	<a href="#">Hinzufügen oder Bearbeiten eines Netzwerkbereichs.</a>

## Verzeichnisverwaltung – Übersicht

Mandantenadministratoren können die Mandantenidentitätsverwaltung und die Zugriffssteuerungseinstellungen mithilfe der Verzeichnisverwaltungsoptionen in der vRealize Automation-Anwendungskonsolle konfigurieren.

Sie können die folgenden Einstellungen über die Registerkarte **Administration > Verzeichnisverwaltung** verwalten.

**Tabelle 2-3. Verzeichnisverwaltung – Einstellungen**

Einstellung	Beschreibung
Verzeichnisse	<p>Auf der Seite „Verzeichnisse“ können Sie Active Directory-Links zur Unterstützung der Authentifizierung und Autorisierung des vRealize Automation-Mandantenbenutzers erstellen und verwalten. Sie können ein oder mehrere Verzeichnisse erstellen und diese Verzeichnisse mit Ihrer Active Directory-Bereitstellung synchronisieren. Auf dieser Seite werden die Anzahl der mit dem Verzeichnis synchronisierten Gruppen und Benutzer sowie die letzte Synchronisierungszeit angezeigt. Klicken Sie auf <b>Jetzt synchronisieren</b>, um die Verzeichnissynchronisierung manuell zu starten.</p> <p>Siehe <a href="#">Konfigurieren der Verzeichnisverwaltung zum Erstellen eines Active Directory-Links</a>.</p> <p>Wenn Sie auf ein Verzeichnis und dann auf die Schaltfläche <b>Synchronisierungseinstellungen</b> klicken, können Sie die Synchronisierungseinstellungen bearbeiten, zur Seite „Identitätsanbieter“ navigieren und das Synchronisierungsprotokoll anzeigen.</p> <p>Auf der Seite mit den Verzeichnis-Synchronisierungseinstellungen können Sie die Synchronisierungshäufigkeit planen, die Liste der Domänen anzeigen, die diesem Verzeichnis zugeordnet sind, die Liste der zugeordneten Attribute ändern, die Liste der Benutzer und Gruppen für die Synchronisierung aktualisieren sowie die Schutzmaßnahmenziele festlegen.</p>
Konnektoren	<p>Auf der Seite „Konnektoren“ sind bereitgestellte Konnektoren für Ihr Unternehmensnetzwerk aufgeführt. Ein Konnektor synchronisiert Benutzer- und Gruppendaten zwischen Active Directory und dem Verzeichnisverwaltungsdienst. Wenn er als Identitätsanbieter verwendet wird, authentifiziert er Benutzer für den Dienst. Jede vRealize Automation-Appliance enthält standardmäßig einen Konnektor. Siehe <a href="#">Verwalten von Konnektoren</a>.</p>
Benutzerattribute	<p>Die Seite „Benutzerattribute“ enthält eine Liste der Standardbenutzerattribute, die im Verzeichnis synchronisiert werden. Sie können weitere Attribute hinzufügen, die Sie Active Directory-Attributen zuordnen können. Siehe <a href="#">Auswahl der mit dem Verzeichnis zu synchronisierenden Attribute</a>.</p>
Netzwerkbereiche	<p>Auf dieser Seite sind die Netzwerkbereiche aufgeführt, die für Ihr System konfiguriert sind. Sie konfigurieren einen Netzwerkbereich, um den Benutzerzugriff über die angegebenen IP-Adressen zuzulassen. Sie können weitere Netzwerkbereiche hinzufügen und vorhandene Bereiche bearbeiten. Siehe <a href="#">Hinzufügen oder Bearbeiten eines Netzwerkbereichs</a>.</p>
Identitätsanbieter	<p>Auf der Seite „Identitätsanbieter“ sind die Identitätsanbieter aufgeführt, die in Ihrem System zur Verfügung stehen. vRealize Automation-Systeme enthalten einen Konnektor, der als standardmäßiger Identitätsanbieter dient und für viele Benutzeranforderungen ausreichend ist. Sie können externe Identitätsanbieter-Instanzen hinzufügen oder eine Kombination von Connector und externen Identitätsanbietern verwenden.</p> <p>Siehe <a href="#">Konfigurieren einer Identitätsanbieter-Instanz</a>.</p>
Richtlinien	<p>Die Seite „Richtlinien“ enthält die Standardzugriffsrichtlinie sowie andere von Ihnen erstellte Zugriffsrichtlinien für Web-Anwendungen. Bei Richtlinien handelt es sich um Regeln, mit denen Kriterien angegeben werden, die erfüllt werden müssen, damit Benutzer auf ihre Anwendungsportale zugreifen oder Webanwendungen starten können, die für sie aktiviert sind. Die Standardrichtlinie dürfte für die meisten vRealize Automation-Bereitstellungen passend sein. Sie können die Richtlinie jedoch bei Bedarf bearbeiten. Siehe <a href="#">Verwalten der Benutzerzugriffsrichtlinie</a>.</p>

## Wichtige Konzepte zu Active Directory

Diverse Konzepte im Zusammenhang mit Active Directory sind ein integraler Bestandteil des Verständnisses der Integration der Directories Management in Ihre Active Directory-Umgebungen.



## Connector

Die Dienstkomponekte Connector erfüllt die folgenden Funktionen.

- Synchronisierung von Benutzer- und Gruppendaten aus Ihrem Active Directory oder LDAP-Verzeichnis mit dem Dienst.
- Authentifizierung der Benutzer gegenüber dem Dienst bei Verwendung als Identitätsanbieter.

Der Connector ist der Standardidentitätsanbieter. Informationen zu den von Connector unterstützten Authentifizierungsmethoden finden Sie unter *Administration von VMware Identity Manager*. Sie können auch externe Identitätsanbieter, die das Protokoll SAML 2.0 unterstützen, verwenden. Verwenden Sie einen externen Identitätsanbieter für einen Authentifizierungstyp, der vom Connector nicht unterstützt wird, oder für einen vom Connector unterstützten Authentifizierungstyp, wenn der externe Identitätsanbieter aufgrund der Sicherheitsrichtlinie des Unternehmens zu bevorzugen ist.

---

**Hinweis** Wenn Sie Dritt-Identitätsanbieter verwenden, können Sie entweder den Connector zum Synchronisieren von Benutzer- und Gruppendaten konfigurieren oder die Just-in-Time-Benutzerbereitstellung konfigurieren. Im Abschnitt „Just-in-Time-Benutzerbereitstellung“ des Handbuchs *Administration von VMware Identity Manager* finden Sie dazu weitere Informationen.

---



---

**Hinweis** Selbst bei Verwendung eines externen Identitätsanbieters müssen Sie den Connector zum Synchronisieren von Benutzer- und Gruppendaten konfigurieren.

---

## Verzeichnis

Der Directories Management-Dienst hat ein eigenes Verzeichnis-Konzept entsprechend dem Active Directory oder LDAP-Verzeichnis in Ihrer Umgebung. Dieses Verzeichnis verwendet Attribute zur Definition von Benutzern und Gruppen.

- Active Directory
  - Active Directory über LDAP Erstellen Sie diesen Verzeichnistyp, wenn Sie eine Verbindung mit einer Active Directory-Umgebung mit einer Domäne herstellen möchten. Beim Verzeichnistyp „Active Directory über LDAP“ verwendet der Connector eine einfache Bind-Authentifizierung zum Herstellen der Verbindung mit Active Directory.
  - Active Directory, integrierte Windows-Authentifizierung. Erstellen Sie diesen Verzeichnistyp, wenn Sie eine Verbindung mit einer Active Directory-Umgebung mit mehreren Domänen oder mehreren Gesamtstrukturen herstellen möchten. Der Connector stellt die Verbindung mit Active Directory unter Verwendung der integrierten Windows-Authentifizierung her.

Typ und Anzahl der Verzeichnisse, die Sie erstellen, hängen von der Active Directory-Umgebung ab, z. B. ob nur eine Domäne oder mehrere Domänen vorhanden sind, und vom Typ des zwischen den Domänen vorhandenen Vertrauensverhältnisses. In den meisten Umgebungen erstellen Sie ein Verzeichnis.

- LDAP-Verzeichnis

Der Dienst hat keinen direkten Zugriff auf Ihr Active Directory oder LDAP-Verzeichnis. Nur der Connector hat einen direkten Zugriff. Daher können Sie jedes im Dienst erstellte Verzeichnis mit einer Connector-Instanz verknüpfen.

## Worker

Wenn Sie ein Verzeichnis mit einer Connector-Instanz verknüpfen, dann erstellt der Connector für das verknüpfte Verzeichnis eine Partition, die als Worker bezeichnet wird. Einer Connector-Instanz können mehrere Worker zugeordnet sein. Jeder Worker fungiert als Identitätsanbieter. Sie definieren und konfigurieren die Authentifizierungsmethoden für jeden Worker getrennt.

Der Connector synchronisiert die Benutzer- und Gruppendaten zwischen Ihrem Active Directory oder LDAP-Verzeichnis und dem Dienst über mindestens einen Worker.

---

**Wichtig** Eine Connector-Instanz kann nicht mit zwei Workern des Active Directory, des Typs mit integrierter Windows-Authentifizierung verknüpft sein.

---

## Active Directory-Umgebungen

Sie können den Dienst in eine Active Directory-Umgebung integrieren, die aus einer einzelnen Active Directory-Domäne, mehreren Domänen in einer einzelnen Active Directory-Gesamtstruktur oder mehreren Domänen in mehreren Active Directory-Gesamtstrukturen besteht.

### Active Directory-Umgebung mit einer einzelnen Domäne

Eine einzelne Active Directory-Bereitstellung ermöglicht Ihnen die Synchronisierung von Benutzern und Gruppen aus einer einzelnen Active Directory-Domäne heraus.

Siehe [Konfigurieren eines Links zu Active Directory](#). Wenn Sie dem Dienst ein Verzeichnis hinzufügen, wählen Sie für diese Umgebung die Option „Active Directory über LDAP“.

### Active Directory-Umgebung mit mehreren Domänen in einer einzelnen Gesamtstruktur

Die Active Directory-Bereitstellung mit mehreren Domänen in einer einzelnen Gesamtstruktur ermöglicht Ihnen die Synchronisierung von Benutzern und Gruppen aus mehreren Active Directory-Domänen in einer einzelnen Gesamtstruktur heraus.

Sie können den Dienst für diese Active Directory-Umgebung als Active Directory-Verzeichnistyp mit einer einzelnen Struktur und integrierter Windows-Authentifizierung oder stattdessen als mit der globalen Katalogoption konfigurierten Verzeichnistyp „Active Directory über LDAP“ konfigurieren.

- Empfohlen wird die Erstellung des Active Directory-Verzeichnistyps mit einer einzelnen Struktur und integrierter Windows-Authentifizierung.

Siehe [Konfigurieren eines Links zu Active Directory](#). Wenn Sie ein Verzeichnis für diese Umgebung hinzufügen, wählen Sie die Option „Active Directory (integrierte Windows-Authentifizierung)“.

## Active Directory-Umgebung mit mehreren Gesamtstrukturen und Vertrauensbeziehungen

Eine Active Directory-Bereitstellung mit mehreren Gesamtstrukturen und Vertrauensbeziehungen ermöglicht Ihnen die Synchronisierung von Benutzern und Gruppen aus mehreren Active Directory-Domänen in Gesamtstrukturen heraus, bei denen zwischen den Domänen gegenseitige Vertrauensbeziehungen bestehen.

Siehe [Konfigurieren eines Links zu Active Directory](#). Wenn Sie ein Verzeichnis für diese Umgebung hinzufügen, wählen Sie die Option „Active Directory (integrierte Windows-Authentifizierung)“.

## Active Directory-Umgebung mit mehreren Gesamtstrukturen, aber ohne Vertrauensbeziehungen

Eine Active Directory-Bereitstellung mit mehreren Gesamtstrukturen, aber ohne Vertrauensbeziehungen ermöglicht Ihnen die Synchronisierung von Benutzern und Gruppen aus mehreren Active Directory-Domänen in mehreren Gesamtstrukturen heraus, bei denen zwischen den Domänen keine gegenseitigen Vertrauensbeziehungen bestehen. In dieser Umgebung erstellen Sie im Dienst mehrere Verzeichnisse und zwar ein Verzeichnis für jede Gesamtstruktur.

Siehe [Konfigurieren eines Links zu Active Directory](#). Welchen Typ von Verzeichnissen Sie im Dienst erstellen, hängt von der Gesamtstruktur ab. Bei Gesamtstrukturen mit mehreren Domänen wählen Sie die Option „Active Directory (integrierte Windows-Authentifizierung)“. Bei einer Gesamtstruktur mit einer einzelnen Domäne wählen Sie die Option „Active Directory über LDAP“.

## Konfigurieren der Verzeichnisverwaltung zum Erstellen eines Active Directory-Links

Nach der Erstellung von vRealize Automation-Mandanten müssen Sie sich bei der Systemkonsole als Mandantenadministrator anmelden und einen Active Directory-Link erstellen, um die Benutzerauthentifizierung zu unterstützen.

### Konfigurieren eines Links zu Active Directory

Sie müssen über die Funktion Directories Management einen Link zu Active Directory konfigurieren, um die Benutzerauthentifizierung für alle Mandanten zu unterstützen und die mit dem Directories Management-Verzeichnis zu synchronisierenden Benutzer und Gruppen auszuwählen.

Für Active Directory gibt es zwei Kommunikationsprotokolle: Active Directory über LDAP und Active Directory (Integrierte Windows-Authentifizierung). Das Protokoll „Active Directory über LDAP“ unterstützt standardmäßig die DNS-Dienstidentifizierungssuche. Mit Active Directory (Integrierte Windows-Authentifizierung) können Sie die Domäne, der beigetreten werden soll, konfigurieren. Active Directory über LDAP ist für die Bereitstellung einzelner Domänen geeignet. Verwenden Sie „Active Directory (Integrierte Windows-Authentifizierung)“ für alle Bereitstellungen mit mehreren Domänen und mehreren Gesamtstrukturen.

Nachdem Sie ein Kommunikationsprotokoll ausgewählt haben, können Sie die Domänen angeben, die mit der Active Directory-Konfiguration verwendet werden sollen, und dann die Benutzer und Gruppen auswählen, die mit der angegebenen Konfiguration synchronisiert werden sollen.

## Voraussetzungen

- Installierter Connector mit aktiviertem Aktivierungscode.
- Auf der Seite „Benutzerattribute“ können Sie die erforderlichen Standardattribute auswählen und zusätzliche Attribute hinzufügen. Siehe [Auswahl der mit dem Verzeichnis zu synchronisierenden Attribute](#).
- Liste der Active Directory-Gruppen und -Benutzer, die aus Active Directory synchronisiert werden sollen.
- Für Active Directory über LDAP gehören zu den erforderlichen Informationen der Basis-DN, der Bind-DN und das Bind-DN-Kennwort.
- Für die integrierte Windows-Authentifizierung von Active Directory werden die Bind-Benutzer-UPN-Adresse und das entsprechende Kennwort benötigt.
- Wenn auf Active Directory über SSL zugegriffen wird, ist eine Kopie des SSL-Zertifikats erforderlich.
- Verfügen Sie über eine Active Directory-Umgebung (Integrierte Windows-Authentifizierung), in der mehrere Gesamtstrukturen konfiguriert sind, und enthält die lokale Domänengruppe Mitglieder aus Domänen in unterschiedlichen Gesamtstrukturen, müssen Sie sicherstellen, dass der Bind-DN-Benutzer der Administratorgruppe der Domäne hinzugefügt wurde, die die lokale Domänengruppe enthält. Wenn Sie diesen Schritt nicht durchführen, fehlen diese Mitglieder in der lokalen Domänengruppe.
- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

## Vorgehensweise

- 1 Wählen Sie **Administration > Verwaltung der Verzeichnisse > Verzeichnisse** aus.
- 2 Klicken Sie auf **Verzeichnis hinzufügen**.
- 3 Geben Sie auf der Seite „Verzeichnis hinzufügen“ im Textfeld **Verzeichnisname** die IP-Adresse für den Active Directory-Server an.
- 4 Wählen Sie über die Optionsfelder unter dem Textfeld **Verzeichnisname** das geeignete Active Directory-Kommunikationsprotokoll aus.

Option	Beschreibung
Windows-Authentifizierung	Wählen Sie <b>Active Directory (Integrierte Windows-Authentifizierung)</b> aus.
LDAP	Wählen Sie <b>Active Directory über LDAP</b> aus.

- 5 Konfigurieren Sie den Connector, der Benutzer aus dem Active Directory mit dem VMware Directories Management-Verzeichnis im Abschnitt „Verzeichnissynchronisierung und Authentifizierung“ synchronisiert.

Option	Beschreibung
<b>Synchronisierungs-Connector</b>	Wählen Sie den gewünschten Connector aus, der für Ihr System verwendet werden soll. Jede vRealize Automation-Appliance enthält einen Standard-Connector. Wenden Sie sich an Ihren Systemadministrator, falls Sie Hilfe bei der Auswahl des geeigneten Connectors benötigen.
<b>Authentifizierung</b>	Klicken Sie auf das entsprechende Optionsfeld, um anzugeben, ob der ausgewählte Connector auch Authentifizierung durchführt.
<b>Verzeichnissuchattribut</b>	Geben Sie das gewünschte Kontoattribut ein, das den Benutzernamen enthält.

- 6 Geben Sie die entsprechenden Informationen im Textfeld „Server-Speicherort“ ein, falls Sie „Active Directory über LDAP“ ausgewählt haben, bzw. in die Felder von „Domänenbeitrittsdetails“, falls Sie Active Directory (Integrierte Windows-Authentifizierung) ausgewählt haben.

Option	Beschreibung
<b>Serverspeicherort - Wird bei Auswahl von „Active Directory über LDAP“ angezeigt</b>	<ul style="list-style-type: none"> <li>■ Wenn Sie die DNS-Dienstidentifizierung für die Suche nach Active Directory-Domänen verwenden, behalten Sie die Aktivierung des Kontrollkästchens <b>Dieses Verzeichnis unterstützt die DNS-Dienstidentifizierung</b> bei.</li> <li>■ Falls das angegebene Active Directory keine DNS-Dienstidentifizierungssuche verwendet, deaktivieren Sie in den Server-Speicherort-Feldern das Kontrollkästchen neben <b>Dieses Verzeichnis unterstützt die DNS-Dienstidentifizierung</b> und geben Sie den Hostnamen und die Portnummer für Active Directory ein.</li> <li>■ Wenn Active Directory Zugriff über SSL benötigt, aktivieren Sie unter der Überschrift „Zertifikate“ das Kontrollkästchen <b>Für dieses Verzeichnis müssen alle Verbindungen SSL verwenden</b> und stellen Sie das Active Directory-SSL-Zertifikat bereit.</li> </ul>
<b>Domänenbeitrittsdetails – Wird bei Auswahl von „Active Directory (Integrierte Windows-Authentifizierung)“ angezeigt.</b>	Geben Sie die entsprechenden Anmeldedaten ein in den Textfeldern <b>Domänenname</b> , <b>Benutzername des Domänenadministrators</b> und <b>Kennwort des Domänenadministrators</b> ein.

- 7 Geben Sie im Abschnitt „Bind-Benutzerdetails“ die entsprechenden Anmeldeinformationen ein, um die Verzeichnissynchronisierung zu erleichtern.

Für Active Directory über LDAP:

Option	Beschreibung
<b>Basis-DN</b>	Geben Sie den Basis-Distinguished-Name für die Suche ein. Beispiel: <b>cn=users,dc=corp,dc=local.</b>
<b>Bind-DN</b>	Geben Sie den Bind-Distinguished-Name ein. Beispiel: <b>cn=fritz infra,cn=users,dc=corp,dc=local</b>

Für Active Directory (Integrierte Windows-Authentifizierung):

Option	Beschreibung
<b>Bind-Benutzer-UPN</b>	Geben Sie den User Principal Name (Benutzername des Prinzipals) des Benutzers ein, der die Domäne authentifizieren kann. Beispiel: Benutzername@example.com.
<b>Bind-DN-Kennwort</b>	Geben Sie das Bind-Benutzerkennwort ein.

- 8 Klicken Sie auf **Verbindung testen**, um die Verbindung zum konfigurierten Verzeichnis zu testen.

Diese Schaltfläche wird nicht angezeigt, wenn Sie „Active Directory (Integrierte Windows-Authentifizierung)“ ausgewählt haben.

- 9 Klicken Sie auf **Speichern und weiter**.

Die Seite „Domänen auswählen“ mit der Liste der Domänen wird angezeigt.

- 10 Überprüfen und aktualisieren Sie die für die Active Directory-Verbindung aufgelisteten Domänen.

- Bei Verwendung von „Active Directory (integrierte Windows-Authentifizierung)“ wählen Sie die Domänen aus, die dieser Active Directory-Verbindung zugeordnet werden sollen.
- Bei Verwendung von „Active Directory über LDAP“ werden die verfügbaren Domänen mit einem Häkchen aufgeführt.


**Hinweis** Wenn Sie nach der Verzeichniserstellung eine Domäne mit Vertrauensbeziehung hinzufügen, erkennt der Dienst nicht automatisch die neue Domäne mit Vertrauensbeziehung. Damit der Dienst die Domäne erkennen kann, muss der Connector die Domäne verlassen und ihr dann erneut beitreten. Wenn der Connector erneut der Domäne beitrifft, wird die Domäne mit Vertrauensbeziehung in der Liste angezeigt.

- 11 Klicken Sie auf **Weiter**.

- 12 Stellen Sie sicher, dass die Attributnamen des Directories Management-Verzeichnisses den richtigen Active Directory-Attributen zugeordnet sind.

Wenn die Verzeichnisattributnamen nicht ordnungsgemäß zugeordnet wurden, wählen Sie das richtige Active Directory-Attribut aus dem Dropdown-Menü aus.

- 13 Klicken Sie auf **Weiter**.

- 14 Klicken Sie auf , um die Gruppen auszuwählen, die aus Active Directory mit dem Verzeichnis synchronisiert werden sollen.


Enthält eine aus Active Directory hinzugefügte Gruppe Mitglieder, die nicht in der Benutzerliste enthalten sind, werden sie hinzugefügt.


---

**Hinweis** Das Directories Management-Benutzerauthentifizierungssystem importiert beim Hinzufügen von Gruppen und Benutzern Daten aus Active Directory, und die Geschwindigkeit des Systems wird durch Active Directory-Funktionen eingeschränkt. Je nach Anzahl der hinzuzufügenden Gruppen und Benutzer können Importvorgänge daher eventuell viel Zeit in Anspruch nehmen. Beschränken Sie, um diesen eventuell auftretenden Verzögerungen oder Problemen entgegenzuwirken, die Anzahl der Gruppen und Benutzer auf jene, die für den Betrieb von vRealize Automation erforderlich sind. Falls sich Ihre Systemleistung verringert oder Fehler auftreten, schließen Sie alle nicht benötigten Anwendungen und stellen Sie sicher, dass Ihr System Active Directory die erforderliche Arbeitsspeicherzuteilung zugeteilt hat. Wenn das Problem weiterhin besteht, erhöhen Sie die Arbeitsspeicherzuteilung für Active Directory nach Bedarf. Bei Systemen mit einer großen Anzahl von Benutzern und Gruppen muss möglicherweise die Arbeitsspeicherzuteilung für Active Directory auf bis zu 24 GB erhöht werden.

---

- 15 Klicken Sie auf **Weiter**.

- 16 Klicken Sie auf , um weitere Benutzer hinzuzufügen. Geben Sie diese beispielsweise im Format **CN=Benutzername,CN=Benutzer,OU=MeineEinheit,DC=MeineFirma,DC=com** ein.

Klicken Sie zum Ausschließen von Benutzern auf , um einen Filter zum Ausschluss bestimmter Benutzertypen zu erstellen. Dazu wählen Sie das Benutzerattribut für den Filter, die Abfragerregel und den Wert aus.

- 17 Klicken Sie auf **Weiter**.

- 18 Überprüfen Sie die Seite, um sehen, wie viele Benutzer und Gruppen mit dem Verzeichnis synchronisiert werden.

Wenn Sie die Zusammenstellung der Benutzer und Gruppen ändern möchten, klicken Sie auf die Optionen zum Bearbeiten.

- 19 Um die Synchronisierung mit dem Verzeichnis zu starten, klicken Sie auf **An Workspace weitergeben**.

Die Verbindung zu Active Directory-Server ist abgeschlossen und die ausgewählten Benutzer und Gruppen werden dem Verzeichnis hinzugefügt.

## Weiter

Wenn Ihre vRealize Automation-Umgebung für Hochverfügbarkeit konfiguriert ist, müssen Sie die Verzeichnisverwaltung speziell für Hochverfügbarkeit konfigurieren. Siehe [Verzeichnisverwaltung für Hochverfügbarkeit konfigurieren](#).

- Richten Sie Authentifizierungsmethoden ein. Nachdem Benutzer und Gruppen mit dem Verzeichnis synchronisiert wurden, können Sie zusätzliche Authentifizierungsmethoden für den Connector konfigurieren, falls dieser auch zur Authentifizierung verwendet wird. Wenn ein externer Identitätsanbieter zur Authentifizierung verwendet wird, konfigurieren Sie diesen Identitätsanbieter im Connector.
- Überprüfen Sie die Standardzugriffsrichtlinie. Die Standardzugriffsrichtlinie wird so konfiguriert, dass alle Appliances in allen Netzwerkbereichen auf den Webbrowser zugreifen können, wobei ein Sitzungs-Timeout von acht Stunden bzw. der Zugriff auf eine Client-App innerhalb eines Sitzungs-Timeout von 2160 Stunden (90 Tagen) festgelegt wird. Sie können die Standardzugriffsrichtlinie ändern. Wenn Sie Web-Anwendungen dem Katalog hinzufügen, können Sie zudem neue Standardzugriffsrichtlinien erstellen.
- Wenden Sie das benutzerdefinierte Branding auf die Verwaltungskonsole, die Benutzerportalseiten und den Anmeldebildschirm an.

## Verzeichnisverwaltung für Hochverfügbarkeit konfigurieren

Sie können mithilfe der Verzeichnisverwaltung eine hochverfügbare Active Directory-Verbindung in vRealize Automation konfigurieren.

Jede vRealize Automation-Appliance enthält einen Connector, der die Benutzerauthentifizierung unterstützt, jedoch ist in der Regel nur ein Connector zum Ausführen der Verzeichnissynchronisierung konfiguriert. Es spielt keine Rolle, welchen Connector Sie als Synchronisierungs-Connector auswählen. Damit die Verzeichnisverwaltung mit Hochverfügbarkeit unterstützt wird, müssen Sie einen zweiten Connector konfigurieren, der Ihrer zweiten vRealize Automation-Appliance entspricht. Dieser verbindet sich mit Ihrem Identitätsanbieter und verweist auf dasselbe Active Directory. Fällt eine Appliance aus, wird bei dieser Konfiguration die Verwaltung der Benutzerauthentifizierung von der anderen Appliance übernommen.

In einer hochverfügbaren Umgebung müssen alle Knoten dieselbe Gruppe von Active Directories, Benutzern, Authentifizierungsmethoden usw. bedienen. Am einfachsten wird dies dadurch erreicht, dass der Identitätsanbieter zum Cluster heraufgestuft wird, indem der Lastausgleichsdienst-Host als der Identitätsanbieter-Host eingerichtet wird. Mit dieser Konfiguration werden alle Authentifizierungsanforderungen an den Lastausgleichsdienst gerichtet, der diese dann an einen der Connectors weiterleitet.

## Voraussetzungen

- Konfigurieren Sie Ihre vRealize Automation-Bereitstellung mit mindestens zwei Instanzen der vRealize Automation-Appliance.
- Installieren Sie vRealize Automation im Enterprise-Modus für den Betrieb in einer einzelnen Domäne mit zwei Instanzen der vRealize Automation-Appliance.
- Installieren und konfigurieren Sie einen geeigneten Lastausgleichsdienst für Ihre vRealize Automation-Bereitstellung.



- Konfigurieren Sie die Mandanten und die Verzeichnisverwaltung mit einem der in den installierten Instanzen der vRealize Automation-Appliance enthaltenen Connectors. Informationen zur Mandantenkonfiguration finden Sie unter [Kapitel 2 Konfigurieren der Mandanteneinstellungen](#).

### Vorgehensweise

- 1 Melden Sie sich beim Lastausgleichsdienst für Ihre vRealize Automation-Bereitstellung als Mandantenadministrator an.  
Die Lastausgleichsdienst-URL lautet `<load balancer address>/vcac/org/tenant_name`.
- 2 Wählen Sie **Administration > Verzeichnisverwaltung > Identitätsanbieter** aus.
- 3 Klicken Sie auf den Identitätsanbieter, der gerade für Ihr System verwendet wird.  
Das vorhandene Verzeichnis und der vorhandene Connector, die die grundlegende Identitätsverwaltung für Ihr System bereitstellen, werden angezeigt.
- 4 Klicken Sie auf der Seite „Identitätsanbieter-Eigenschaften“ auf die Dropdown-Liste **Connector hinzufügen** und wählen Sie den Connector, der Ihrer sekundären vRealize Automation-Appliance entspricht.
- 5 Geben Sie das entsprechende Kennwort im Textfeld **Bind-DN-Kennwort** ein, das nach Auswahl des Connectors angezeigt wird.
- 6 Klicken Sie auf **Connector hinzufügen**.
- 7 Der Haupt-Connector wird standardmäßig im Textfeld **IdP-Hostname** angezeigt. Ändern Sie den Hostnamen in der Weise, dass er auf den Lastausgleichsdienst verweist.

## Konfigurieren einer bidirektionalen Vertrauensstellung zwischen vRealize Automation und Active Directory

Sie können die Systemsicherheit einer grundlegenden vRealize Automation Active Directory-Verbindung verbessern, indem Sie eine bidirektionale Vertrauensstellung zwischen Ihrem Identitätsanbieter und den Active Directory-Verbunddiensten konfigurieren.

Um eine bidirektionale Vertrauensstellung zwischen vRealize Automation und Active Directory zu konfigurieren, müssen Sie einen benutzerdefinierten Identitätsanbieter erstellen und diesem die Active Directory-Metadaten hinzufügen. Außerdem müssen Sie die von Ihrer vRealize Automation-Bereitstellung verwendete Standardrichtlinie ändern. Schließlich müssen Sie Active Directory so konfigurieren, dass Ihr Identitätsanbieter erkannt wird.

### Voraussetzungen

- Stellen Sie sicher, dass Sie Mandanten für Ihre vRealize Automation-Bereitstellung konfiguriert haben, um einen entsprechenden Active Directory-Link einzurichten, um eine grundlegende Benutzer-ID- und Kennwortauthentifizierung von Active Directory zu unterstützen.
- Active Directory ist für die Verwendung in Ihrem Netzwerk installiert und konfiguriert.
- Besorgen Sie sich die Metadaten der Active Directory-Verbunddienste (ADFS).
- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

## Vorgehensweise

- 1 Besorgen Sie sich die Datei mit den Federation-Metadaten.

Sie können diese Datei über <https://servername.domain/FederationMetadata/2007-06/FederationMetadata.xml> herunterladen.

- 2 Suchen Sie nach der Wort-Abmeldung und bearbeiten Sie den Speicherort für jede Instanz, um auf <https://servername.domain/adfs/ls/logout.aspx> zu verweisen.

Beispielsweise die Folgende:

```
SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://servername.domain/adfs/ls/ "/>
```

Muss folgendermaßen geändert werden:

```
SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://servername.domain/adfs/ls/logout.aspx"/>
```

- 3 Erstellen Sie einen neuen Identitätsanbieter für Ihre Bereitstellung.
  - a Wählen Sie **Administration > Verzeichnisverwaltung > Identitätsanbieter** aus.
  - b Klicken Sie auf **Identitätsanbieter hinzufügen** und füllen Sie die Felder entsprechend aus.

Option	Beschreibung
<b>Name des Identitätsanbieters</b>	Einen Namen für den neuen Identitätsanbieter eingeben
<b>Metadaten des Identitätsanbieters (URI oder XML)</b>	Fügen Sie die Inhalte der Metadatendatei der Active Directory-Verbindungsdienste hier ein.
<b>Richtlinien für Namen-ID in SAML-Anforderung (optional)</b>	Geben Sie bei Bedarf einen Namen für die SAML-Anforderung der Identitätsrichtlinien ein.
<b>Benutzer</b>	Wählen Sie die Domains aus, auf die Benutzer Zugriff haben sollen.
<b>IDP-Metadaten verarbeiten</b>	Klicken Sie, um die hinzugefügte Metadatendatei zu verarbeiten.
<b>Netzwerk</b>	Wählen Sie die Netzwerkbereiche aus, auf die Benutzer Zugriff haben sollen.
<b>Authentifizierungsmethoden</b>	Geben Sie einen Namen für die Authentifizierungsmethode ein, die von diesem Identitätsanbieter verwendet wird.
<b>SAML-Kontext</b>	Wählen Sie für das System den entsprechenden Kontext aus.
<b>SAML-Signaturzertifikat</b>	Klicken Sie auf den Link neben der SAML-Metadatenüberschrift, um die Metadaten der Verzeichnisverwaltung herunterzuladen.

- c Speichern Sie die Datei mit den Metadaten der Verzeichnisverwaltung als `sp.xml`.
  - d Klicken Sie auf **Hinzufügen**.

#### 4 Fügen Sie der Standardrichtlinie eine Regel hinzu.

- a Wählen Sie **Administration > Verzeichnisverwaltung > Richtlinien** aus.
- b Klicken Sie auf den Namen der Standardrichtlinie.
- c Klicken Sie auf das „+“-Symbol unter der Überschrift **Richtlinienregeln**, um eine neue Regel hinzuzufügen.

Erstellen Sie mithilfe der Felder auf der Seite „Richtlinienregel hinzufügen“ eine Regel, die die für einen bestimmten Netzwerkbereich und ein bestimmtes Netzwerkgerät jeweils zu verwendende primäre und sekundäre Authentifizierungsmethode festlegt.

Wenn beispielsweise der Netzwerkbereich des Benutzers **Mein Computer** ist und der Benutzer auf Inhalte über **Alle Gerätetypen** zugreifen muss, dann muss sich der Benutzer in einer normalen Bereitstellung unter Verwendung der folgenden Methode authentifizieren:

**ADFS-Benutzername und Kennwort.**

- d Klicken Sie auf **Speichern**, um Ihre Richtlinienaktualisierungen zu speichern.
  - e Ziehen Sie die neue Regel auf der Seite „Standardrichtlinie“ in den oberen Bereich der Tabelle, damit diese Vorrang vor anderen vorhandenen Regeln hat.
- #### 5 Richten Sie mit der Verwaltungskonsolle der Active Directory-Verbunddienste oder einem anderen geeigneten Tool eine Vertrauensstellung für vertrauende Seiten mithilfe des vRealize Automation-Identitätsanbieters ein.

Um diese Vertrauensstellung einzurichten, müssen Sie die zuvor heruntergeladenen Metadaten der Verzeichnisverwaltung importieren. Weitere Informationen zum Konfigurieren von Active Directory-Verbunddiensten für bidirektionale Vertrauensstellungen finden Sie in der Dokumentation zu Microsoft Active Directory. Im Rahmen dieses Vorgangs sind folgende Schritte auszuführen:

- Richten Sie eine Vertrauensstellung für vertrauende Seiten ein. Beim Einrichten dieser Vertrauensstellung müssen Sie die zuvor kopierte und gespeicherte XML-Datei mit den Metadaten des Dienstanbieters für VMware Identity Provider importieren.
- Erstellen Sie eine Beanspruchungsregel, die die aus LDAP abgerufenen Attribute in der „Attribute abrufen“-Regel in das gewünschte SAML-Format umwandeln. Nach Erstellen der Regel müssen Sie diese bearbeiten, indem Sie folgenden Text hinzufügen:

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
= c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "vmwareidentity.domain.com");
```

## Konfigurieren eines SAML-Verbunds zwischen Directories Management und SSO2

Zur Unterstützung der einmaligen Anmeldung können Sie einen SAML-Verbund zwischen vRealize Automation Directories Management und Systemen, die SSO2 nutzen, einrichten.

Stellen Sie einen Verbund zwischen Directories Management und SSO2 her, indem Sie eine SAML-Verbindung zwischen den beiden Seiten erstellen. Der einzige gegenwärtig unterstützte End-to-End-Flow ist jener, in dem SSO2 als Identitätsanbieter (IdP) und Directories Management als Dienstanbieter (SP) fungiert.

Für die SSO2-Benutzerauthentifizierung muss dasselbe Konto sowohl in Directories Management als auch in SSO2 vorhanden sein. Mindestens der Benutzerprinzipalname (User Principal Name, UPN) des Benutzers muss an beiden Enden übereinstimmen. Andere Attribute können abweichen, da sie zur Identifizierung des SAML-Objekts benötigt werden.

Für lokale Benutzer in SSO2, wie beispielsweise `admin@vsphere.local`, müssen auch in Directories Management entsprechende Konten vorhanden sein, wobei mindestens der UPN des Benutzers übereinstimmen muss. Erstellen Sie diese Konten manuell oder unter Verwendung eines Skripts mithilfe der APIs von Directories Management zum Erstellen lokaler Benutzer.

Das Einrichten von SAML zwischen SSO2 und Directories Management erfordert auch eine Konfiguration der Verzeichnisverwaltungs- und SSO-Komponenten.

**Tabelle 2-4. Komponentenkongfiguration für SAML-Verbund**

Komponente	Konfiguration
Verzeichnisverwaltung	Konfigurieren Sie SSO2 als einen externen Identitätsanbieter in Directories Management und aktualisieren Sie die Standardauthentifizierungsrichtlinie. Sie können ein automatisiertes Skript zum Einrichten von Directories Management erstellen.
SSO2-Komponente	Konfigurieren Sie Directories Management als einen Dienstanbieter, indem Sie die Directories Management-Datei <code>sp.xml</code> importieren. Diese Datei ermöglicht es Ihnen, SSO2 so zu konfigurieren, dass Directories Management als der Dienstanbieter (SP) verwendet wird.

### Voraussetzungen

- Konfigurieren Sie Mandanten für Ihre vRealize Automation-Bereitstellung. Siehe [Erstellen weiterer Mandanten](#).
- Richten Sie eine entsprechende Active Directory-Verbindung ein, um die einfache Active Directory-Authentifizierung mit Benutzer-ID und Kennwort zu unterstützen.
- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

### Vorgehensweise

- 1 Laden Sie die SSO2-Identitätsanbieter-Metadaten über die SSO2-Benutzeroberfläche herunter.
  - a Melden Sie sich unter `https://<cloudvm-hostname>/` als Administrator bei vCenter an.
  - b Klicken Sie auf den Link **Bei vSphere Web Client anmelden**.
  - c Wählen Sie im linken Navigationsfenster **Administration > Single Sign On > Konfiguration** aus.

- d Klicken Sie neben den Metadaten für Ihre SAML-Dienstanbieter-Überschrift auf **Download**.

Der Download der `vsphere.local.xml`-Datei sollte beginnen.

- e Kopieren Sie den Inhalt der `vsphere.local.xml`-Datei.

## 2 Erstellen Sie auf der Seite für die Identitätsanbieter der vRealize Automation-Verzeichnisverwaltung einen neuen Identitätsanbieter.

- a Melden Sie sich bei vRealize Automation als **Mandantenadministrator** an.
- b Wählen Sie **Administration > Verzeichnisverwaltung > Identitätsanbieter** aus.
- c Klicken Sie auf **Identitätsanbieter hinzufügen** und geben Sie die Konfigurationsinformationen ein.

Option	Aktion
<b>Name des Identitätsanbieters</b>	Geben Sie einen Namen für den neuen Identitätsanbieter ein.
<b>Identitätsanbieter-Metadaten (URI oder XML) (Textfeld)</b>	Fügen Sie den Inhalt Ihrer SSO2-Metadaten-Datei <code>idp.xml</code> in das Textfeld ein und klicken Sie auf <b>IDP-Metadaten verarbeiten</b> .
<b>Richtlinien für Namen-ID in SAML-Anforderung (optional)</b>	Geben Sie <code>http://schemas.xmlsoap.org/claims/UPN</code> .
<b>Benutzer</b>	Wählen Sie die Domains aus, auf die Benutzer Zugriff haben sollen.
<b>Netzwerk</b>	Wählen Sie die Netzwerkbereiche aus, auf die Benutzer Zugriff haben sollen. Wenn Sie Benutzer über IP-Adressen authentifizieren möchten, wählen Sie <b>Alle Bereiche</b> aus.
<b>Authentifizierungsmethoden</b>	Geben Sie einen Namen für die Authentifizierungsmethode ein. Verwenden Sie dann das Dropdown-Menü <b>SAML-Kontext</b> auf der rechten Seite, um <code>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</code> die Authentifizierungsmethode zuzuordnen.
<b>SAML-Signaturzertifikat</b>	Klicken Sie auf den Link neben der SAML-Metadatenüberschrift, um die Metadaten der Verzeichnisverwaltung herunterzuladen.

- d Speichern Sie die Datei mit den Metadaten der Verzeichnisverwaltung als `sp.xml`.

- e Klicken Sie auf **Hinzufügen**.

## 3 Aktualisieren Sie auf der Seite mit den Richtlinien für die Verzeichnisverwaltung die entsprechende Authentifizierungsrichtlinie so, dass eine Umleitung zum externen SSO2-Identitätsanbieter erfolgt.

- a Wählen Sie **Administration > Verzeichnisverwaltung > Richtlinien** aus.
- b Klicken Sie auf den Namen der Standardrichtlinie.
- c Klicken Sie unter der Überschrift **Richtlinienregeln** auf die Authentifizierungsmethode, um die vorhandene Authentifizierungsregel zu bearbeiten.
- d Ändern Sie auf der Seite „Richtlinie bearbeiten“ die Authentifizierungsmethode und wählen Sie anstelle der Kennwortmethode die gewünschte Methode.

In diesem Fall sollte die Methode SSO2 sein.

- e Klicken Sie auf **Speichern**, um Ihre Richtlinienaktualisierungen zu speichern.

- 4 Wählen Sie im linken Navigationsbereich **Administration > Single Sign-On > Konfiguration** aus und klicken Sie auf **Aktualisieren**, um die Datei `sp.xml` nach vSphere hochzuladen.

## Benutzer oder Gruppen zu einer Active Directory-Verbindung hinzufügen

Sie können Benutzer oder Gruppen zu einer vorhandenen Active Directory-Verbindung hinzufügen.

Das Verzeichnisverwaltung-Benutzerauthentifizierungssystem der Verzeichnisverwaltung importiert beim Hinzufügen von Gruppen und Benutzern Daten aus Active Directory, und die Geschwindigkeit des Systems wird durch Active Directory-Funktionen eingeschränkt. Je nach Anzahl der hinzuzufügenden Gruppen und Benutzer können Importvorgänge daher eventuell viel Zeit in Anspruch nehmen. Beschränken Sie, um diesen eventuell auftretenden Verzögerungen oder Problemen entgegenzuwirken, die Anzahl der Gruppen und Benutzer auf jene, die für den Betrieb von vRealize Automation erforderlich sind. Falls sich die Leistung verringert oder Fehler auftreten, schließen Sie alle nicht benötigten Anwendungen und stellen Sie sicher, dass Active Directory die erforderliche Arbeitsspeichermenge von Ihrer Bereitstellung zugewiesen wurde. Wenn das Problem weiterhin besteht, erhöhen Sie die Arbeitsspeicherzuteilung für Active Directory nach Bedarf. Bei Bereitstellungen mit einer großen Anzahl von Benutzern und Gruppen muss möglicherweise die Arbeitsspeicherzuteilung für Active Directory auf bis zu 24 GB erhöht werden.

Beim Ausführen eines Synchronisierungsvorgangs für eine vRealize Automation-Bereitstellung mit vielen Benutzern und Gruppen kann eine Verzögerung auftreten, wenn die Meldung *Synchronisierung läuft* angezeigt wird, bevor die Details des Synchronisierungsprotokolls angezeigt werden. Auch kann sich der Zeitstempel der Protokolldatei von der Zeit unterscheiden, die vom System für den Abschluss des Synchronisierungsvorgangs angegeben wird.

---

**Hinweis** Sie können einen Synchronisierungsvorgang nicht mehr abbrechen, nachdem er initiiert wurde.

---

### Voraussetzungen

- Installierter Connector mit aktiviertem Aktivierungscode. Auf der Seite „Benutzerattribute“ können Sie die erforderlichen Standardattribute auswählen und zusätzliche Attribute hinzufügen.
- Liste der Active Directory-Gruppen und -Benutzer, die aus Active Directory synchronisiert werden sollen.
- Für Active Directory über LDAP gehören zu den erforderlichen Informationen der Basis-DN, der Bind-DN und das Bind-DN-Kennwort.
- Für die integrierte Windows-Authentifizierung von Active Directory werden die Bind-Benutzer-UPN-Adresse und das entsprechende Kennwort benötigt.
- Wenn auf Active Directory über SSL zugegriffen wird, ist eine Kopie des SSL-Zertifikats erforderlich.
- Verfügen Sie über eine Active Directory-Umgebung mit integrierter Windows-Authentifizierung, in der mehrere Gesamtstrukturen konfiguriert sind, und enthält die lokale Domänengruppe Mitglieder aus Domänen in unterschiedlichen Gesamtstrukturen, müssen Sie sicherstellen, dass der Bind-DN-Benutzer der Administratorgruppe der Domäne hinzugefügt wurde, die die lokale Domänengruppe enthält. Wird dies versäumt, fehlen diese Benutzer in der lokalen Domänengruppe.
- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

## Vorgehensweise

- 1 Wählen Sie **Administration > Verwaltung der Verzeichnisse > Verzeichnisse** aus.
- 2 Klicken Sie auf den gewünschten Verzeichnisnamen.
- 3 Klicken Sie auf **Synchronisierungseinstellungen**, um ein Dialogfeld mit Synchronisierungsoptionen zu öffnen.
- 4 Klicken Sie je nachdem, ob Sie die Benutzerkonfiguration oder die Gruppenkonfiguration ändern möchten, auf das entsprechende Symbol.

So bearbeiten Sie die Gruppenkonfiguration:

- Zum Hinzufügen von Gruppen klicken Sie auf das Symbol **+**, um eine neue Zeile für Gruppen-DN-Definitionen hinzuzufügen, und geben Sie den entsprechenden Gruppen-DN ein.
- Um eine Gruppen-DN-Definition zu löschen, klicken Sie beim gewünschten Gruppen-DN auf das Symbol **x**.

So bearbeiten Sie die Benutzerkonfiguration:

- ◆ Zum Hinzufügen von Benutzern klicken Sie auf das Symbol **+**, um eine neue Zeile für eine Benutzer-DN-Definition hinzuzufügen, und geben Sie den entsprechenden Benutzer-DN ein.

Um eine Benutzer-DN-Definition zu löschen, klicken Sie beim gewünschten Benutzer-DN auf das Symbol **x**.

- 5 Klicken Sie auf **Speichern**, um Ihre Änderungen ohne Synchronisierung zu speichern und so die Aktualisierungen sofort vorzunehmen, oder klicken Sie auf **Speichern und Synchronisieren**, um Ihre Änderungen zu speichern und eine Synchronisierung vorzunehmen, um Ihre Aktualisierungen sofort zu implementieren.

## Auswahl der mit dem Verzeichnis zu synchronisierenden Attribute

Wenn Sie das Directories Management-Verzeichnis für die Synchronisierung mit Active Directory einrichten, geben Sie die Benutzerattribute an, die mit dem Verzeichnis synchronisiert werden sollen. Bevor Sie das Verzeichnis einrichten, können Sie auf der Seite „Benutzerattribute“ angeben, welche Standardattribute erforderlich sind, und auf Wunsch zusätzliche Attribute definieren, die Sie den Active Directory-Attributen zuordnen möchten.

Wenn Sie die Seite „Benutzerattribute“ vor der Erstellung des Verzeichnisses konfigurieren, können Sie die erforderlichen Standardattribute ändern, Attribute als erforderlich markieren und benutzerdefinierte Attribute hinzufügen.

Eine Liste der standardmäßig zugeordneten Attribute finden Sie unter [Verwalten von Benutzerattributen, die aus Active Directory synchronisieren](#).

Nachdem das Verzeichnis erstellt worden ist, können Sie erforderliche Attribute als nicht erforderlich festlegen und benutzerdefinierte Attribute löschen. Sie können ein vorhandenes Attribut allerdings nicht als erforderliches Attribut definieren.

Wenn Sie nach der Erstellung des Verzeichnisses weitere Attribute hinzufügen, die mit dem Verzeichnis synchronisiert werden sollen, dann öffnen Sie die Seite „Zugeordnete Attribute“ des Verzeichnisses und ordnen diese Attribute den gewünschten Active Directory-Attributen zu.

### Vorgehensweise

- 1 Melden Sie sich als System- oder Mandantenadministrator bei vRealize Automation an.
- 2 Klicken Sie auf die Registerkarte „Administration“.
- 3 Wählen Sie **Verzeichnisverwaltung > Benutzerattribute** aus.
- 4 Prüfen Sie im Abschnitt „Standardattribute“ die Liste der erforderlichen Attribute und nehmen Sie die erforderlichen Änderungen vor, um die erforderlichen Attribute festzulegen.
- 5 Im Abschnitt „Attribute“ fügen Sie der Liste den Attributnamen des Directories Management-Verzeichnisses hinzu.
- 6 Klicken Sie auf **Speichern**.  
Der Standardattributstatus wird aktualisiert und die von Ihnen hinzugefügten Attribute werden der Liste „Zugeordnete Attribute“ des Verzeichnisses hinzugefügt.
- 7 Gehen Sie nach Erstellung des Verzeichnisses zur Seite „Identitätsquellen“ und wählen Sie das Verzeichnis aus.
- 8 Klicken Sie auf **Synchronisierungseinstellungen > Zugeordnete Attribute**.
- 9 Im Dropdown-Menü für die hinzugefügten Attribute wählen Sie das Active Directory-Attribut für die Zuordnung aus.
- 10 Klicken Sie auf **Speichern**.

Das Verzeichnis wird bei der nächsten Synchronisierung mit Active Directory aktualisiert.

### Der Verzeichnisverwaltung Arbeitsspeicher hinzufügen

Sie müssen Directories Management möglicherweise zusätzlichen Arbeitsspeicher zuteilen, wenn Sie Active Directory-Verbindungen haben, die eine große Anzahl von Benutzern oder Gruppen enthalten.

Standardmäßig sind dem Directories Management-Dienst 4 GB Arbeitsspeicher zugeteilt. Dies ist für viele zahlreiche kleine bis mittlere Bereitstellungen ausreichend. Wenn Sie eine Active Directory-Verbindung haben, die eine große Anzahl von Benutzern oder Gruppen verwendet, müssen Sie diese Arbeitsspeicherzuteilung möglicherweise erhöhen. Eine Erhöhung der Arbeitsspeicherzuteilung ist bei Systemen mit mehr als 100.000 Benutzern, jeweils in 30 Gruppen und bei insgesamt 750 Gruppen, angebracht. Für diese Systeme empfiehlt VMware eine Erhöhung der Directories Management-Arbeitsspeicherzuteilung auf 6 GB.

Die Berechnung des Arbeitsspeichers für die Verzeichnisverwaltung erfolgt auf der Grundlage der Gesamtgröße des der vRealize Automation-Appliance zugeteilten Arbeitsspeichers. In der folgenden Tabelle werden die Arbeitsspeicherzuteilungen für die entsprechenden Komponenten aufgeführt.



**Tabelle 2-5. Arbeitsspeicherzuteilung für die vRealize Automation-Appliance**

Arbeitsspeicher der virtuellen Appliance	Arbeitsspeicher für den vRA-Dienst	Arbeitsspeicher für den vIDM-Dienst
18 GB	3,3 GB	4 GB
24 GB	4,9 GB	6 GB
30 GB	7,4 GB	9,1 GB

**Hinweis** Bei diesen Zuteilungen wird davon ausgegangen, dass alle Standarddienste auf der virtuellen Appliance aktiviert sind und ausgeführt werden. Sie können variieren, wenn bestimmte Dienste beendet werden.

#### Voraussetzungen

- In Ihrer vRealize Automation-Bereitstellung ist eine geeignete Active Directory-Verbindung konfiguriert und funktionsbereit.

#### Vorgehensweise

1 Stoppen Sie jede Maschine, auf der vRealize Automation-Appliance ausgeführt wird.

2 Erhöhen Sie auf jeder Maschine die Arbeitsspeicherzuteilung für die virtuelle Appliance.

Bei Verwendung der Standard-Arbeitsspeicherzuteilung von 18 GB empfiehlt VMware eine Erhöhung der Arbeitsspeicherzuteilung auf 24 GB.

3 Starten Sie die vRealize Automation-Appliance-Maschinen neu.

### Erstellen einer Domänenhost-Suchdatei, um DNS-Dienstspeicherort-Suchvorgänge (SRV) außer Kraft zu setzen

Wenn Sie die integrierte Windows-Authentifizierung aktivieren, wird die Verzeichniskonfiguration so geändert, dass das Feld „DNS-Dienstspeicherort“ aktiviert wird. Bei der Connector-Dienstspeicherort-Suche wird die Site nicht berücksichtigt. Um die zufällige DC-Auswahl außer Kraft zu setzen, können Sie eine Datei namens `domain_krb.properties` erstellen und die Domäne den Hostwerten hinzufügen, die Vorrang vor der SRV-Suche haben.

#### Vorgehensweise

1 Melden Sie sich an der `appliance-va`-Befehlszeile als Benutzer mit Root-Berechtigungen an.

2 Ändern Sie die Verzeichnisse in `/usr/local/horizon/conf` und erstellen Sie eine Datei mit dem Namen `domain_krb.properties`.

3 Bearbeiten Sie die Datei „`domain_krb.properties`“ und fügen Sie die Liste der Domänen zu den Hostwerten hinzu. Fügen Sie die Informationen als `<AD Domain>=<host:port>`, `<host2:port2>`, `<host2:port2>` hinzu.

Geben Sie die Liste z. B. als `example.com=examplehost.com:636`, `examplehost2.example.com:389` ein.

- 4 Ändern Sie den Besitzer der Datei „domain\_krb.properties“ in „horizon“ und gruppieren Sie unter „www“. Geben Sie **chown horizon:www /usr/local/horizon/conf/domain\_krb.properties** ein.
- 5 Starten Sie den Dienst neu. Geben Sie **service horizon-workspace restart** ein.

## Verwalten von Benutzerattributen, die aus Active Directory synchronisieren

Auf der Seite „Benutzerattribute“ der Verzeichnisverwaltung sind die Benutzerattribute aufgeführt, die mit Ihrer Active Directory-Verbindung synchronisiert werden.

Änderungen, die auf der Seite „Benutzerattribute“ vorgenommen und gespeichert wurden, werden der Seite „Zugeordnete Attribute“ im Directories Management-Verzeichnis hinzugefügt. Bei der nächsten Synchronisierung mit Active Directory werden die Attributänderungen im Verzeichnis aktualisiert.

Die Seite „Benutzerattribute“ zeigt die Standardverzeichnisattribute an, die den Active Directory-Attributen zugeordnet werden können. Sie wählen die erforderlichen Attribute aus und können weitere Active Directory-Attribute hinzufügen, die mit dem Verzeichnis synchronisiert werden sollen.

**Tabelle 2-6. Standardzuordnung von Verzeichnisattributen zu Active Directory-Attributen**

Verzeichnisattributname	Standardzuordnung zu Active Directory-Attribut
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
Domäne	canonicalName. Fügt den vollqualifizierten Domänennamen des Objekts ein.
deaktiviert (externer Benutzer deaktiviert)	userAccountControl. Mit UF_Account_Disable gekennzeichnet Wenn ein Konto deaktiviert ist, können sich Benutzer nicht mehr anmelden, um auf ihre Anwendungen und Ressourcen zuzugreifen. Die Ressourcen, zu deren Nutzung die Benutzer berechtigt sind, werden nicht aus dem Konto entfernt. Wenn die Markierung vom Konto entfernt wird, können sich Benutzer daher anmelden und auf die Ressourcen zugreifen, für die sie Berechtigungen haben.
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName

Die Seite „Benutzerattribute“ zeigt die Standardverzeichnisattribute an, die den Active Directory-Attributen zugeordnet werden können. Sie wählen die erforderlichen Attribute aus und können weitere Active Directory-Attribute hinzufügen, die mit dem Verzeichnis synchronisiert werden sollen.

**Tabelle 2-7. Standardzuordnung von Verzeichnisattributen zu Active Directory-Attributen**

Verzeichnisattributname	Standardzuordnung zu Active Directory-Attribut
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
Domäne	canonicalName. Fügt den vollqualifizierten Domänennamen des Objekts ein.
deaktiviert (externer Benutzer deaktiviert)	userAccountControl. Mit UF_Account_Disable gekennzeichnet Wenn ein Konto deaktiviert ist, können sich Benutzer nicht mehr anmelden, um auf ihre Anwendungen und Ressourcen zuzugreifen. Die Ressourcen, zu deren Nutzung die Benutzer berechtigt sind, werden nicht aus dem Konto entfernt. Wenn die Markierung vom Konto entfernt wird, können sich Benutzer daher anmelden und auf die Ressourcen zugreifen, für die sie Berechtigungen haben.
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName

## Verwalten von Konnektoren

Auf der Seite „Konnektoren“ sind bereitgestellte Konnektoren für Ihr Unternehmensnetzwerk aufgeführt. Ein Konnektor synchronisiert Benutzer- und Gruppendaten zwischen Active Directory und dem Verzeichnisverwaltungsdienst. Wenn er als Identitätsanbieter verwendet wird, authentifiziert er Benutzer für den Dienst.

In vRealize Automation enthält jede vRealize Automation-Appliance-Appliance ihren eigenen Konnektor. Diese Konnektoren sind für die meisten Bereitstellungen geeignet.

Wenn Sie ein Verzeichnis mit einer Konnektorinstanz verknüpfen, dann erstellt der Konnektor für das verknüpfte Verzeichnis eine Partition, die als Worker bezeichnet wird. Einer Konnektorinstanz können mehrere Worker zugeordnet sein. Jeder Worker fungiert als Identitätsanbieter. Der Connector synchronisiert die Benutzer- und Gruppendaten zwischen Active Directory und dem Dienst über mindestens einen Worker. Sie definieren und konfigurieren Authentifizierungsmethoden pro Worker.

Auf der Seite „Konnektoren“ können Sie verschiedene Aspekte eines Active Directory-Links verwalten. Diese Seite enthält eine Tabelle und verschiedene Schaltflächen, über die Sie diverse Verwaltungsaufgaben durchführen können.

- Wählen Sie in der Spalte „Worker“ einen Worker, um die Konnektordetails anzuzeigen, und navigieren Sie zur Seite „Authentifizierungsadapter“, um den Status der verfügbaren Authentifizierungsmethoden zu betrachten. Informationen zur Authentifizierung finden Sie unter [Integrieren alternativer Benutzerauthentifizierungsprodukte in die Verzeichnisverwaltung](#).

- Wählen Sie in der Spalte „Identitätsanbieter“ den Identitätsanbieter aus, den Sie anzeigen, bearbeiten oder deaktivieren möchten. Siehe [Konfigurieren einer Identitätsanbieter-Instanz](#).
- Greifen Sie über die Spalte „Zugeordnetes Verzeichnis“ auf das Verzeichnis zu, das diesem Worker zugeordnet ist.
- Klicken Sie auf **Domäne beitreten**, um den Konnektor in eine bestimmte Active Directory-Domäne aufzunehmen. Wenn Sie z. B. die Kerberos-Authentifizierung konfigurieren, müssen Sie der Active Directory-Domäne beitreten, welche die Benutzer enthält, oder eine Vertrauensbeziehung mit den Domänen haben, welche die Benutzer enthalten.
- Wird ein Verzeichnis mit einer Active Directory-Umgebung mit integrierter Windows-Authentifizierung konfiguriert, dann tritt der Konnektor der Domäne entsprechend den Konfigurationsdetails bei.

## Hinzufügen einer Konnektormaschine zu einer Domäne

In einigen Fällen müssen Sie möglicherweise eine Maschine, in der ein Verzeichnisverwaltungskonnektor enthalten ist, zu einer Domäne hinzufügen.

Bei „Active Directory über LDAP“-Verzeichnissen können Sie einer Domäne beitreten, nachdem Sie das Verzeichnis erstellt haben. Bei Verzeichnissen vom Typ „Active Directory“ (integrierte Windows-Authentifizierung) wird der Konnektor automatisch der Domäne hinzugefügt, wenn Sie das Verzeichnis erstellen. In beiden Fällen müssen Sie die entsprechenden Anmeldedaten eingeben.

Um einer Domäne beizutreten, benötigen Sie Active Directory-Anmeldedaten, die über Rechte zum Beitritt des Computers zu einer AD-Domäne besitzen. Dies wird in Active Directory mit den folgenden Rechten konfiguriert:

- Erstellen von Computerobjekten
- Löschen von Computerobjekten

Wenn Sie einer Domäne beitreten, wird im Standardspeicherort von Active Directory ein Computerobjekt erstellt.

Wenn Sie keine Rechte zum Hinzufügen einer Domäne besitzen oder wenn die Unternehmensrichtlinie einen benutzerdefinierten Speicherort für das Computerobjekt verlangt, müssen Sie Ihren Administrator bitten, das Objekt zu erstellen und anschließend die Konnektormaschine der Domäne hinzuzufügen.

### Vorgehensweise

- 1 Bitten Sie Ihren Active Directory-Administrator, ein Computerobjekt an einem Speicherort in Active Directory zu erstellen, den Ihre Unternehmensrichtlinie vorsieht. Sie müssen den Hostnamen des Connectors angeben. Stellen Sie sicher, dass ein vollqualifizierter Domänenname angegeben wird, z. B. `server.beispiel.de`.

Sie können den Hostnamen in der Verwaltungskonsolle auf der Seite „Konnektoren“ in der Spalte „Hostname“ anzeigen. Wählen Sie **Administration > Verzeichnisverwaltung > Konnektoren** aus.

- 2 Klicken Sie nach der Erstellung des Computerobjekts auf der Seite „Konnektoren“ auf **Domäne beitreten**, um die Domäne mit einem Domänenbenutzerkonto, das in Verzeichnisverwaltung verfügbar ist, hinzuzufügen.

## Informationen über die Auswahl von Domänencontrollern

Die Datei `domain_krb.properties` legt fest, welche Domänencontroller für die Verzeichnisse verwendet werden, deren DNS-Dienstspeicherort(SRV-Einträge)-Suche aktiviert ist. Sie enthält eine Liste von Domänencontrollern für jede Domäne. Der Connector erstellt anfänglich die Datei und Sie müssen diese in der Folge warten. Die Datei überschreibt die DNS-Dienstspeicherort(SRV)-Suche.

Bei folgenden Verzeichnistypen ist die DNS-Dienstspeicherort-Suche aktiviert.

- „Active Directory über LDAP“ mit der ausgewählten Option **Dieses Verzeichnis unterstützt den DNS-Dienstspeicherort**
- Active Directory (integrierte Windows-Authentifizierung) mit dauerhaft aktivierter DNS-Dienstspeicherort-Suche

Wenn Sie zuerst ein Verzeichnis erstellen, dessen DNS-Dienstspeicherort-Suche aktiviert ist, wird die Datei `domain_krb.properties` automatisch im Verzeichnis `/usr/local/horizon/conf` der virtuellen Maschine erstellt und mit den Domänencontrollern für jede Domäne automatisch aufgefüllt. Zum Auffüllen der Datei versucht der Connector Domänencontroller zu ermitteln, die sich in derselben Site wie der Connector befinden. Dann wählt er jene beiden aus, die erreichbar sind und am schnellsten antworten.

Wenn Sie weitere Verzeichnisse erstellen, deren DNS-Dienstspeicherort-Suche aktiviert ist, oder neue Domänen einem Verzeichnis mit integrierter Windows-Authentifizierung hinzufügen, werden der Datei diese neuen Domänen und eine Liste ihrer Domänencontroller hinzugefügt.

Sie können die Standardauswahl durch Bearbeiten der Datei `domain_krb.properties` jederzeit überschreiben. Zeigen Sie als Best Practice nach dem Erstellen eines Verzeichnisses die Datei `domain_krb.properties` an und prüfen Sie, ob die aufgeführten Domänencontroller für Ihre Konfiguration optimal sind. Bei einer globalen Active Directory-Bereitstellung mit vielen Domänencontrollern an verschiedenen geografischen Standorten empfiehlt es sich, einen Domänencontroller zu verwenden, der sich in unmittelbarer Nähe des Connectors befindet. So stellen Sie eine schnelle Kommunikation mit Active Directory sicher.

Sie müssen darüber hinaus die Datei manuell im Hinblick auf die anderen Änderungen aktualisieren. Beachten Sie die nachfolgend aufgeführten Regeln.

- Die Datei `domain_krb.properties` wird in der virtuellen Maschine erstellt, die den Connector enthält. In einer typischen Bereitstellung ohne zusätzlich bereitgestellte Connectoren wird die Datei im Directories Management-Dienst der virtuellen Maschine angelegt. Wenn Sie für das Verzeichnis einen zusätzlichen Connector verwenden, wird die Datei im Connector der virtuellen Maschine erstellt. Eine virtuelle Maschine kann immer nur über eine Datei `domain_krb.properties` verfügen.
- Die Datei wird erstellt und für jede Domäne mit Domänencontrollern aufgefüllt, wenn Sie das Verzeichnis mit aktivierter DNS-Dienstspeicherort-Suche erstmalig erstellen.
- Die Domänencontroller für jede Domäne werden in der Reihenfolge ihrer Priorität aufgelistet. Für die Herstellung einer Verbindung mit Active Directory versucht der Connector den ersten Domänencontroller in der Liste zu verwenden. Ist dieser nicht erreichbar, versucht er es mit dem zweiten und so weiter.

- Die Datei wird nur aktualisiert, wenn Sie ein neues Verzeichnis mit aktivierter DNS-Dienstspeicherort-Suche erstellen oder wenn Sie eine Domäne einem Verzeichnis mit integrierter Windows-Authentifizierung hinzufügen. Die neue Domäne und eine Liste der zugehörigen Domänencontroller werden der Datei hinzugefügt.

Hinweis: Wenn bereits ein Eintrag für eine Domäne vorhanden ist, wird die Datei nicht aktualisiert. Wenn Sie beispielsweise ein Verzeichnis erstellt und dann wieder gelöscht haben, bleibt der Originaldomäneneintrag in der Datei bestehen und wird nicht aktualisiert.

- Auch in anderen Szenarien wird die Datei nicht automatisch aktualisiert. Beispiel: Wenn Sie ein Verzeichnis löschen, wird der Domäneneintrag nicht aus der Datei entfernt.
- Wenn ein in der Datei aufgelisteter Domänencontroller nicht erreichbar ist, bearbeiten Sie die Datei und entfernen Sie diesen.
- Wenn Sie einen Domäneneintrag manuell hinzufügen oder bearbeiten, werden Ihre Änderungen nicht überschrieben.

## Auswahl von Domänencontrollern für das automatische Auffüllen der Datei „domain\_krb.properties“

Zum automatischen Auffüllen der Datei `domain_krb.properties` werden die Domänencontroller zunächst durch die Auswahl des Subnetzes festgelegt, in dem sich der Connector befindet (basierend auf der IP-Adresse und Netzmaske). Dann wird mit der Konfiguration von Active Directory die Site dieses Subnetzes anhand der Liste der Domänencontroller für diese Site identifiziert. Es werden die beiden Domänencontroller ausgewählt, die am schnellsten antworten.

Zur Ermittlung der nächstliegenden Domänencontroller müssen für VMware Identity Manager folgende Voraussetzungen erfüllt sein.

- Das Subnetz des Connectors muss in der Konfiguration von Active Directory enthalten sein, oder in der Datei `runtime-config.properties` muss ein Subnetz angegeben sein.

Das Subnetz wird zur Bestimmung des Standorts verwendet.

- Die Konfiguration von Active Directory muss auf die Site abgestimmt sein.

Wenn das Subnetz nicht identifiziert werden kann oder Ihre Active Directory-Konfiguration nicht Site-bezogen erfolgt ist, sucht die DNS-Dienstspeicherort-Suche nach Domänencontrollern. Die Datei wird dann mit den wenigen Domänencontrollern aufgefüllt, die erreichbar sind. Beachten Sie, dass sich diese Domänencontroller eventuell nicht an derselben geografischen Position wie der Connector befinden. Dies kann zu Verzögerungen oder Zeitüberschreitungen bei der Kommunikation mit Active Directory führen. In diesem Fall sollten Sie die Datei `domain_krb.properties` manuell bearbeiten und die richtigen Domänencontroller für die einzelnen Domänen festlegen.

## Beispiel für Datei „domain\_krb.properties“

```
example.com=host1.example.com:389,host2.example.com:389
```

### ■ Überschreiben der Standard-Subnetzauswahl

Für das automatische Auffüllen der Datei `domain_krb.properties` versucht der Connector die Domänencontroller zu finden, die sich in derselben Site befinden, um die Latenz zwischen Connector und Active Directory möglichst gering zu halten.

### ■ Bearbeiten der Datei „domain\_krb.properties“

Die Datei `/usr/local/horizon/conf/domain_krb.properties` legt die Domänencontroller für die Verzeichnisse fest, deren DNS-Dienstspeicherort-Suche aktiviert ist. Sie können die Datei jederzeit bearbeiten und die Liste der Domänencontroller ändern sowie Domäneneinträge hinzufügen oder löschen. Ihre Änderungen werden nicht überschrieben.

### ■ Fehlerbehebung in „domain\_krb.properties“

Mit diesen Informationen können Sie Fehler in der Datei `domain_krb.properties` beheben.

## Überschreiben der Standard-Subnetzauswahl

Für das automatische Auffüllen der Datei `domain_krb.properties` versucht der Connector die Domänencontroller zu finden, die sich in derselben Site befinden, um die Latenz zwischen Connector und Active Directory möglichst gering zu halten.

Für die Suche nach der Site verwendet der Connector das Subnetz, in dem er sich befindet, basierend auf seiner IP-Adresse und Netzmaske. Dann verwendet er die Active Directory-Konfiguration zur Identifizierung der Site für dieses Subnetz. Wenn sich das Subnetz der virtuellen Maschine nicht in Active Directory befindet oder wenn Sie die automatische Subnetzauswahl überschreiben möchten, können Sie ein Subnetz in der Datei `runtime-config.properties` angeben.

### Vorgehensweise

- 1 Melden Sie sich bei der virtuellen Directories Management-Maschine als Root-Benutzer an.

---

**Hinweis** Wenn Sie für das Verzeichnis einen zusätzlichen Connector verwenden, melden Sie sich bei der virtuellen Maschine des Connectors an.

---

- 2 Bearbeiten Sie die Datei `/usr/local/horizon/conf/runtime-config.properties` und fügen Sie das folgende Attribut hinzu.

**`siteaware.subnet.override=subnet`**

wobei *subnet* ein Subnetz für jene Site darstellt, deren Domänencontroller Sie verwenden möchten.  
Beispiel:

**`siteaware.subnet.override=10.100.0.0/20`**

- 3 Speichern und schließen Sie die Datei.
- 4 Starten Sie den Dienst neu.

`service horizon-workspace restart`

## Bearbeiten der Datei „domain\_krb.properties“

Die Datei `/usr/local/horizon/conf/domain_krb.properties` legt die Domänencontroller für die Verzeichnisse fest, deren DNS-Dienstspeicherort-Suche aktiviert ist. Sie können die Datei jederzeit bearbeiten und die Liste der Domänencontroller ändern sowie Domäneneinträge hinzufügen oder löschen. Ihre Änderungen werden nicht überschrieben.

Die Datei wird erstmalig erstellt und dann automatisch vom Connector aufgefüllt. Sie müssen sie in einigen Szenarien manuell aktualisieren.

- Wenn die standardmäßig ausgewählten Domänencontroller für Ihre Konfiguration nicht optimal sind, bearbeiten Sie die Datei und legen Sie die Domänencontroller fest, die verwendet werden sollen.
- Wenn Sie ein Verzeichnis löschen, löschen Sie auch den zugehörigen Domäneneintrag aus der Datei.
- Wenn Domänencontroller in der Datei nicht erreichbar sind, entfernen Sie diese.

Siehe auch [Informationen über die Auswahl von Domänencontrollern](#).

### Vorgehensweise

- 1 Melden Sie sich bei der virtuellen Directories Management-Maschine als Root-Benutzer an.

---

**Hinweis** Wenn Sie für das Verzeichnis einen zusätzlichen Connector verwenden, melden Sie sich bei der virtuellen Maschine des Connectors an.

---

- 2 Ändern Sie die Verzeichnisse in `/usr/local/horizon/conf`.
- 3 Bearbeiten Sie die Datei `domain_krb.properties` und fügen Sie die Liste der Domänen den Hostwerten hinzu bzw. bearbeiten Sie diese.

Verwenden Sie folgendes Format:

*Domäne=Host:Port,Host2:Port,Host3:Port*

Beispiel:

`example.com=examplehost1.example.com:389,examplehost2.example.com:389`

Listen Sie die Domänencontroller in der Reihenfolge ihrer Priorität auf. Für die Herstellung einer Verbindung mit Active Directory versucht der Connector den ersten Domänencontroller in der Liste zu verwenden. Ist dieser nicht erreichbar, versucht er es mit dem zweiten und so weiter.

---

**Wichtig** Domänennamen müssen in Kleinbuchstaben eingegeben werden.

---

- 4 Ändern Sie den Besitzer der Datei `domain_krb.properties` in Horizon und gruppieren Sie mit dem folgenden Befehl unter `www`:

```
chown horizon:www /usr/local/horizon/conf/domain_krb.properties
```

- 5 Starten Sie den Dienst neu.

```
service horizon-workspace restart
```



## Fehlerbehebung in „domain\_krb.properties“

Mit diesen Informationen können Sie Fehler in der Datei `domain_krb.properties` beheben.

### Fehler „Domänenauflösungsfehler“

Wenn die Datei `domain_krb.properties` bereits einen Eintrag für eine Domäne enthält und Sie versuchen, ein neues Verzeichnis mit einem Typ zu erstellen, der nicht derselbe Typ ist wie die Domäne, tritt der „Domänenauflösungsfehler“ auf. Sie müssen dann die Datei `domain_krb.properties` bearbeiten und den Domäneneintrag manuell entfernen, ehe Sie ein neues Verzeichnis erstellen.

### Domänencontroller sind nicht erreichbar

Sobald ein Domäneneintrag in der Datei `domain_krb.properties` hinzugefügt wurde, wird dieser nicht mehr automatisch aktualisiert. Wenn Domänencontroller, die in der Datei aufgeführt sind, nicht mehr erreichbar sind, müssen Sie die Datei manuell bearbeiten und diese entfernen.

## Verwalten von Zugriffsrichtlinien

Die Directories Management-Richtlinien sind ein Regelsatz mit Kriterien, die von Benutzern erfüllt werden müssen, damit diese auf ihr App-Portal zugreifen oder bestimmte Web-Anwendungen starten können.

Die Regel wird als Bestandteil einer Richtlinie erstellt. Jede Richtlinie in einer Regel kann die folgenden Informationen angeben.

- Der Netzwerkbereich, von wo aus Benutzer sich anmelden dürfen, z. B. von innerhalb oder von außerhalb des Unternehmensnetzwerks.
- Der Gerätetyp, der über diese Richtlinie Zugriff erhält.
- Reihenfolge der Anwendung aktivierter Authentifizierungsmethoden.
- Anzahl der Stunden, für die die Authentifizierung gültig ist.
- Benutzerdefinierte Meldung über eine Zugriffsverweigerung.

---

**Hinweis** Die Richtlinien steuern nicht die Dauer einer Web-Anwendungssitzung. Sie steuern, wie viel Zeit Benutzern zum Starten einer Web-Anwendung zur Verfügung steht.

---

Der Directories Management-Dienst enthält eine Standardrichtlinie, die Sie bearbeiten können. Diese Richtlinie steuert den Zugriff auf den Dienst insgesamt. Siehe [Anwenden der Standardzugriffsrichtlinie](#). Um den Zugriff auf bestimmte Web-Anwendungen zu steuern, können Sie zusätzliche Richtlinien erstellen. Wenn Sie einer Web-Anwendung keine Richtlinie zuweisen, wird die Standardrichtlinie verwendet.

## Konfigurieren von Einstellungen für die Zugriffsrichtlinie

Eine Richtlinie enthält eine oder mehrere Zugriffsregeln. Jede Regel besteht aus Einstellungen, die Sie zur Verwaltung des Benutzerzugriffs auf deren Anwendungsportale als Ganzes oder auf bestimmte Webanwendungen konfigurieren können.

## Netzwerkbereich

Für jede Regel legen Sie die Benutzerbasis fest, indem Sie einen Netzwerkbereich angeben. Ein Netzwerkbereich besteht aus mindestens einem IP-Adressenbereich. Vor der Konfiguration der Richtlinienätze für den Zugriff erstellen Sie auf der Seite „Einrichten“ > „Netzwerkbereiche“ der Registerkarte „Identitäts- und Zugriffsmanagement“ die Netzwerkbereiche.

## Gerätetyp

Wählen Sie den Gerätetyp aus, den die Regel verwalten soll. Zu den Clienttypen gehören Webbrowser, Identity Manager-Client-Anwendung, iOS, Android und „Alle Gerätetypen“.

## Authentifizierungsmethoden

Legen Sie die Priorität der Authentifizierungsmethoden für die Richtlinienregel fest. Die Authentifizierungsmethoden werden in der Reihenfolge angewendet, in der sie aufgeführt sind. Die ersten Identitätsanbieter-Instanzen, die die Authentifizierungsmethode und Netzwerkbereichskonfiguration der Richtlinie erfüllen, werden ausgewählt und die Benutzerauthentifizierungsanforderung zur Authentifizierung an die Identitätsanbieter-Instanz weitergeleitet. Wenn die Authentifizierung scheitert, wird die nächste Authentifizierungsmethode in der Liste ausgewählt. Wenn die Zertifikatsauthentifizierung verwendet wird, muss diese an oberster Stelle der Liste stehen.

Sie können die Regeln für die Zugriffsrichtlinie so konfigurieren, dass Benutzer Anmeldedaten über zwei Authentifizierungsmethoden eingeben müssen, bevor sie sich anmelden können. Wenn eine oder beide Authentifizierungsmethoden scheitern und gleichzeitig Fallback-Methoden konfiguriert wurden, werden Benutzer zur Eingabe ihrer Anmeldedaten für die nächsten konfigurierten Authentifizierungsmethoden aufgefordert. Die beiden nachfolgend aufgeführten Szenarien beschreiben die Funktionsweise der Authentifizierungsverkettung.

- Im ersten Szenario wird die Regel der Zugriffsrichtlinie so konfiguriert, dass Benutzer sich mit ihrem Kennwort und mit ihren Kerberos-Anmeldedaten authentifizieren müssen. Für die Fallback-Authentifizierung sollen das Kennwort und die RADIUS-Anmeldedaten erforderlich sein. Ein Benutzer gibt das Kennwort korrekt ein, aber nicht die richtigen Kerberos-Anmeldedaten zur Authentifizierung. Da der Benutzer das korrekte Kennwort eingegeben hat, fordert die Fallback-Authentifizierung nur die RADIUS-Anmeldedaten an. Der Benutzer muss also das Kennwort nicht erneut eingeben.
- Auch im zweiten Szenario wird die Regel der Zugriffsrichtlinie so konfiguriert, dass Benutzer sich mit ihrem Kennwort und mit ihren Kerberos-Anmeldedaten authentifizieren müssen. Für die Fallback-Authentifizierung sollen allerdings die RSA SecurID und ein RADIUS erforderlich sein. Ein Benutzer gibt das Kennwort korrekt ein, aber nicht die richtigen Kerberos-Anmeldedaten zur Authentifizierung. Die Fallback-Authentifizierung fordert sowohl die Anmeldedaten für RSA SecurID als auch für RADIUS zur Authentifizierung an.

## Dauer der Authentifizierungssitzung

Für jede Regel legen Sie die für diese Authentifizierung gültige Dauer fest. Dieser Wert bestimmt, wie viel Zeit den Benutzern seit ihrem letzten Authentifizierungsereignis maximal für den Zugriff auf ihr Portal oder zum Starten einer bestimmten Web-Anwendung zur Verfügung steht. Mit einem Wert von 4 in einer Web-Anwendungsregel werden beispielsweise für die Benutzer vier Stunden zum Starten der Web-Anwendung bereitgestellt, sofern sie kein weiteres Authentifizierungsereignis initiieren, das den Zeitwert erhöht.

## Benutzerdefinierte Meldung zu einer Zugriffsverweigerung

Wenn Benutzer versuchen, sich anzumelden, und dies aufgrund ungültiger Anmeldedaten, falscher Konfiguration oder von Systemfehlern nicht möglich ist, wird eine Meldung über eine Zugriffsverweigerung angezeigt. Die Standardmeldung lautet:

Der Zugriff wurde verweigert, da keine gültigen Authentifizierungsmethoden gefunden wurden.

Sie haben die Möglichkeit, für jede Regel der Zugriffsrichtlinie eine benutzerdefinierte Meldung festzulegen, die Vorrang vor der Standardmeldung hat. Die benutzerdefinierte Meldung kann einen Text und einen Link für den Aufruf einer Aktionsmeldung enthalten. Beispielsweise kann in einer Richtlinienregel für von Ihnen verwaltete mobile Geräte im Falle der Anmeldung eines Benutzers von einem nicht angemeldeten Gerät die folgende benutzerdefinierte Fehlermeldung angezeigt werden:

Bitte melden Sie Ihr Gerät durch Anklicken des Links am Ende dieser Meldung für den Zugriff auf die Unternehmensressourcen an. Sollte Ihr Gerät bereits angemeldet sein, kontaktieren Sie den Support.

## Beispiel für Standardrichtlinie

Die folgende Richtlinie dient als Beispiel dafür, wie Sie die Standardrichtlinie zur Steuerung des Zugriffs auf das App-Portal konfigurieren können. Siehe [Verwalten der Benutzerzugriffsrichtlinie](#).

Die Richtlinienregeln werden in der aufgeführten Reihenfolge ausgewertet. Sie können durch Versetzen der Regel mittels „Drag-and-Drop“ die Richtlinienreihenfolge im Abschnitt „Richtlinienregeln“ verändern.

Im folgenden Anwendungsfall gilt das Richtlinienbeispiel für alle Anwendungen.

STANDARDRICHTLINIE

\* Name der Richtlinie: default\_access\_policy\_set

Beschreibung: Default access policy set

Gültig für: Alle Anwendungen

Richtlinienregeln

Sie können für den Zugriff auf diese Webanwendungen eine Liste mit Regeln erstellen. Für jede Regel wählen Sie den IP-Netzwerkbereich, den Typ der Geräte, die auf die Anwendungen zugreifen sollen, die Methoden sowie die Authentifizierungsreihenfolge und die maximale Anzahl an Stunden, für die die Benutzer die Anwendung vor einer erneuten Authentifizierung verwenden können.

Netzwerkbereich	Gerätetyp	Authentifizierungsmethode	Erneut authentifizieren	
ALLE BEREICHE	Web-Browser	Password	8 Stunde(n)	✗ +
ALLE BEREICHE	Identity Manager-Client-Anwendung	Password	2160 Stunde(n)	✗ +

Speichern Abbrechen

- Für das interne Netzwerk (Interner Netzwerkbereich) sind für die Regel zwei Authentifizierungsmethoden konfiguriert, Kerberos- und Kennwortauthentifizierung als Fallback-Methode. Um auf das App-Portal von einem internen Netzwerk aus zuzugreifen, versucht der Dienst, Benutzer zuerst mit der Kerberos-Authentifizierung zu authentifizieren, da diese als erste Authentifizierungsmethode in der Regel aufgeführt ist. Schlägt diese fehl, werden die Benutzer zur Eingabe ihres Active Directory-Kennworts aufgefordert. Benutzer melden sich mit einem Browser an und haben dann im Rahmen einer Acht-Stunden-Sitzung Zugriff auf ihre Benutzerportale.
  - Für den Zugriff vom externen Netzwerk aus (Alle Bereiche) wurde nur eine Authentifizierungsmethode konfiguriert, RSA SecurID. D. h., Benutzer müssen sich für den Zugriff auf das App-Portal von einem externen Netzwerk aus mit SecurID anmelden. Benutzer melden sich mit einem Browser an und haben dann im Rahmen einer Vier-Stunden-Sitzung Zugriff auf ihre App-Portale.
- Wenn ein Benutzer auf eine Ressource (mit Ausnahme von Web-Anwendungen, für die eine Richtlinie für spezifische Web-Anwendungen gilt) zuzugreifen versucht, gilt die Standardrichtlinie für den Portalzugriff.

So entspricht beispielsweise die Zeit für erneute Authentifizierung derartiger Ressourcen der Zeit für erneute Authentifizierung der Standard-Zugriffsrichtlinienregel. Wenn die Zeit für einen Benutzer, der sich beim Anwendungsportal anmeldet, gemäß der Standard-Zugriffsrichtlinienregel acht Stunden beträgt und der Benutzer während der Sitzung versucht, eine Ressource zu starten, wird die Anwendung gestartet, ohne den Benutzer zur erneuten Authentifizierung aufzufordern.


## Verwalten von Richtlinien für spezifische Web-Anwendungen

Wenn Sie Ihrem Katalog Web-Anwendungen hinzufügen, können Sie Web-Anwendungs-spezifische Richtlinien erstellen. Beispielsweise können Sie eine Richtlinie mit Regeln für eine Web-Anwendung erstellen, in der festgelegt ist, welche IP-Adressen Zugriff auf die Anwendung haben, welche Authentifizierungsmethoden diese verwenden und nach welchem Intervall eine erneute Authentifizierung erforderlich ist.

Der folgende Richtlinie für spezifische Web-Anwendungen ist ein Beispiel für eine Richtlinie, die Sie erstellen können, um den Zugriff auf spezifische Web-Anwendungen zu steuern.

### Beispiel 1: Strenge Web-Anwendungs-spezifische Richtlinie

In diesem Beispiel wird eine neue Richtlinie erstellt und einer vertraulichen Web-Anwendung zugeordnet.



**Sensitive Web Application**  
 To be applied to Web application that should have limited access.

Richtlinie löschen

**Name der Richtlinie\***

**Beschreibung**

**Gültig für**

Wählen Sie in Ihrem Katalog die Anwendungen aus, für die diese Richtlinie gilt.

Anwendungen bearbeiten

**Richtlinienregeln**  
 Sie können für den Zugriff auf diese Anwendungen eine Liste mit Regeln erstellen. Wählen Sie für jede Regel den IP-Netzwerkbereich, den Typ der Geräte, die auf die Anwendungen zugreifen sollen, die Methoden sowie die Authentifizierungsreihenfolge und die maximale Anzahl an Stunden, für die die Benutzer die Anwendung vor einer erneuten Authentifizierung verwenden können.

Netzwerkbereich	Gerätetyp	Authentifizierung...	Erneut authenti...	Gruppen	
Internal Network	Web-Browser	Zuerst folgende Aktion durchführen: Kerberos und 1 weitere(r) Fallback(s)...	8 Stunde(n)	Alle Benutzer	✗ +
ALLE BEREICHE	Web-Browser	Securid	4 Stunde(n)	Alle Benutzer	✗ +

Speichern

Abbrechen

- 1 Für den Zugriff auf den Dienst von einem Standort außerhalb des Unternehmensnetzwerks muss sich der Benutzer mit RSA SecurID anmelden. Der Benutzer meldet sich mit einem Browser an und hat jetzt für eine vierstündige Sitzung Zugriff auf das Apps-Portal, entsprechend den Einstellungen in der Standardzugriffsregel.
- 2 Nach vier Stunden versucht der Benutzer, eine Web-Anwendung zu starten, für die die Richtlinie für vertrauliche Web-Anwendungen angewendet wird.
- 3 Der Dienst prüft die Regeln der Richtlinie und wendet die Richtlinie mit dem Netzwerkbereich „ALLE BEREICHE“ an, da die Benutzeranforderung von einem Webbrowser und aus dem Netzwerkbereich „ALLE BEREICHE“ kommt.

Der Benutzer meldet sich mit der Authentifizierungsmethode RSA SecurID an, aber die Sitzung ist gerade abgelaufen. Der Benutzer wird zur erneuten Authentifizierung umgeleitet. Mit der erneuten Authentifizierung kann der Benutzer eine weitere vierstündige Sitzung beginnen und die Anwendung nun starten. Für die nächsten vier Stunden kann der Benutzer die Anwendung weiterhin starten, ohne sich erneut authentifizieren zu müssen.

## Beispiel 2: Strengere Web-Anwendungs-spezifische Richtlinie

Um für besonders vertrauliche Web-Anwendungen eine strengere Regel anzuwenden, können Sie eine erneute Authentifizierung mit SecurID auf jedem Gerät nach einer Stunde anfordern. Im Folgenden finden Sie ein Beispiel, wie dieser Regeltyp einer Zugriffsrichtlinie implementiert werden kann.

- 1 Der Benutzer meldet sich innerhalb des Unternehmensnetzwerks mit der Kennwort-Authentifizierungsmethode an.

Der Benutzer hat nun acht Stunden Zugriff auf das Apps-Portal, wie in Beispiel 1 eingerichtet.

- 2 Der Benutzer versucht daraufhin sofort, eine Web-Anwendung zu starten, auf die die Richtlinienregel aus Beispiel 2 angewendet wird. Für diese Richtlinienregel ist die RSA SecurID-Authentifizierung erforderlich.
- 3 Der Benutzer wird zu einem Identitätsanbieter umgeleitet, der die RSA SecurID-Authentifizierung vorsieht.
- 4 Nachdem sich der Benutzer erfolgreich angemeldet hat, startet der Dienst die Anwendung und speichert das Authentifizierungsereignis.

Der Benutzer kann diese Anwendung noch eine Stunde lang erneut starten. Nach einer Stunde wird er jedoch aufgefordert, sich erneut zu authentifizieren, wie durch die Regel vorgeschrieben.

## Verwalten der Benutzerzugriffsrichtlinie

vRealize Automation enthält eine Standard-Benutzerzugriffsrichtlinie, die Sie in vorliegender Form verwenden oder nach Bedarf zur Verwaltung des Mandantenzugriffs auf Anwendungen bearbeiten können.

vRealize Automation enthält eine Standard-Benutzerzugriffsrichtlinie und Sie können keine neuen Richtlinien hinzufügen. Sie können die vorhandene Richtlinie bearbeiten, um Richtlinien hinzuzufügen.

### Voraussetzungen

- Wählen Sie die geeigneten Identitätsanbieter für Ihre Bereitstellung aus oder konfigurieren Sie diese. Siehe [Konfigurieren einer Identitätsanbieter-Instanz](#).
- Konfigurieren Sie die geeigneten Netzwerkbereiche für Ihre Bereitstellung. Siehe [Hinzufügen oder Bearbeiten eines Netzwerkbereichs](#).
- Konfigurieren Sie die geeigneten Authentifizierungsmethoden für Ihre Bereitstellung. Siehe [Integrieren alternativer Benutzerauthentifizierungsprodukte in die Verzeichnisverwaltung](#).
- Wenn Sie die Standardrichtlinie bearbeiten möchten (um den Benutzerzugriff auf den Dienst insgesamt zu steuern), konfigurieren Sie diese, bevor Sie Web-Anwendungsspezifische Richtlinien erstellen.
- Fügen Sie Web-Anwendungen zum Katalog hinzu. Sie können erst dann eine Richtlinie hinzufügen, wenn die Web-Anwendungen auf der Seite „Katalog“ aufgeführt werden.
- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Richtlinien** aus.
- 2 Klicken Sie auf **Richtlinie bearbeiten**, um eine neue Richtlinie hinzuzufügen.
- 3 Fügen Sie in den entsprechenden Textfeldern einen Namen und eine Beschreibung der Richtlinie ein.
- 4 Im Abschnitt „Gültig für“ klicken Sie auf **Auswählen** und in der daraufhin angezeigten Seite wählen Sie die Web-Anwendung aus, die mit dieser Richtlinie verbunden ist.

- 5 Im Abschnitt „Richtlinienregeln“ klicken Sie auf das **+**-Zeichen, um eine Regel hinzuzufügen.

Die Seite „Richtlinienregel hinzufügen“ wird angezeigt.

- a Wählen Sie einen Netzwerkbereich aus, auf den diese Regel angewendet werden soll.
- b Wählen Sie den Gerätetyp aus, der für diese Regel auf die Web-Anwendung zugreifen können soll.
- c Wählen Sie die Authentifizierungsmethoden in der Reihenfolge aus, in der die Methoden angewendet werden sollen.
- d Geben Sie die Anzahl von Stunden ein, über die eine Web-Anwendungssitzung geöffnet bleiben soll.
- e Klicken Sie auf **Speichern**.

- 6 Konfigurieren Sie weitere Regeln nach Bedarf.

- 7 Klicken Sie auf **Speichern**.

## Integrieren alternativer Benutzerauthentifizierungsprodukte in die Verzeichnisverwaltung

Bei der Erstkonfiguration der Verzeichnisverwaltung werden in der Regel die in Ihrer vorhandenen vRealize Automation-Infrastruktur enthaltenen Konnektoren verwendet, um eine Active Directory-Verbindung für eine auf Benutzer-ID und Kennwort basierende Authentifizierung und Verwaltung zu erstellen. Die Verzeichnisverwaltung lässt sich aber auch in andere Authentifizierungslösungen wie Kerberos oder RSA SecurID integrieren.

Die Identitätsanbieter-Instanz können die Directories Management Connector-Instanz, externe Identitätsanbieter-Instanzen oder eine Kombination von beidem sein.

Von der Identitätsanbieter-Instanz, die Sie mit dem Directories Management-Dienst verwenden, wird eine Verbundautorität im Netzwerk erstellt, die über SAML 2.0-Annahmen mit dem Dienst kommuniziert.

Bei der erstmaligen Bereitstellung des Directories Management-Diensts ist der Connector der anfängliche Identitätsanbieter für den Dienst. Ihre vorhandene Active Directory-Infrastruktur wird für die Benutzerauthentifizierung und -verwaltung verwendet.

Die folgenden Authentifizierungsmethoden werden unterstützt: Sie können diese Authentifizierungsmethoden in der Verwaltungskonsole konfigurieren.

**Tabelle 2-8. Von der Verzeichnisverwaltung unterstützte Authentifizierungstypen**

Authentifizierungstypen	Beschreibung
Kennwort (lokale Bereitstellung)	Wenn Sie nach der Konfiguration von Active Directory keine weiteren Konfigurationen vornehmen, unterstützt Directories Management die Kennwortauthentifizierung von Active Directory. Diese Methode authentifiziert Benutzer direkt anhand des Active Directory.
Kerberos für Desktops	Die Kerberos-Authentifizierung ermöglicht Domänenbenutzern den SSO-Zugang (mit einmaliger Anmeldung) zu ihrem App-Portal. Nach der Anmeldung beim Netzwerk müssen sich die Benutzer nicht erneut anmelden.

**Tabelle 2-8. Von der Verzeichnisverwaltung unterstützte Authentifizierungstypen (Fortsetzung)**

Authentifizierungstypen	Beschreibung
Zertifikat (lokale Bereitstellung)	<p>Die zertifikatbasierte Authentifizierung kann so konfiguriert werden, dass Clients sich mithilfe von Zertifikaten auf Desktops und mobilen Geräten authentifizieren oder einen Smartcard-Adapter für die Authentifizierung verwenden können.</p> <p>Die zertifikatbasierte Authentifizierung basiert auf etwas, was der Benutzer besitzt und auf etwas, was die Person weiß. Ein X.509-Zertifikat verwendet den Standard der Public Key Infrastructure (PKI), um zu überprüfen, ob ein im Zertifikat enthaltener öffentlicher Schlüssel dem Benutzer gehört.</p>
RSA SecurID (lokale Bereitstellung)	Wenn die RSA SecurID-Authentifizierung konfiguriert ist, wird Directories Management als Authentifizierungsagent im RSA SecurID-Server konfiguriert. Bei der RSA SecurID-Authentifizierung müssen die Benutzer ein Token-basiertes Authentifizierungssystem verwenden. RSA SecurID ist eine Authentifizierungsmethode für Benutzer, die von außerhalb des Unternehmensnetzwerks auf Directories Management zugreifen.
RADIUS (lokale Bereitstellung)	Die RADIUS-Authentifizierung bietet Zwei-Faktor-Authentifizierungsoptionen. Sie richten den RADIUS-Server ein, auf den der Directories Management-Dienst zugreifen kann. Wenn sich die Benutzer mit ihrem Benutzernamen und dem Passcode anmelden, wird eine Zugriffsanfrage für die Authentifizierung an den RADIUS-Server übermittelt.
Adaptive RSA-Authentifizierung (lokale Bereitstellung)	Die RSA-Authentifizierung bietet eine stärkere Mehr-Faktoren-Authentifizierung als die einfache Authentifizierung bei Active Directory mit Benutzername und Kennwort. Wenn „Adaptive RSA-Authentifizierung“ aktiviert ist, werden die in der Risikorichtlinie angegebenen Risikoindikatoren in der Anwendung „RSA Policy Management“ eingerichtet. Zur Ermittlung der erforderlichen Authentifizierungsaufforderungen wird die Directories Management-Dienstkonfiguration der adaptiven Authentifizierung verwendet.
Mobile SSO (für iOS)	Die Authentifizierung Mobile SSO für iOS wird zur SSO-Authentifizierung (mit einmaliger Anmeldung) für von AirWatch verwaltete iOS-Geräte verwendet. Die Authentifizierung Mobile SSO (für iOS) verwendet ein Schlüsselverteilungscenter (Key Distribution Center, KDC), das zum Directories Management-Dienst gehört. Vor dem Aktivieren dieser Authentifizierungsmethode müssen Sie den KDC-Dienst im VMware Identity Manager-Dienst starten.
Mobile SSO (für Android)	Die Authentifizierung Mobile SSO für Android wird zur SSO-Authentifizierung (mit einmaliger Anmeldung) für von AirWatch verwaltete Android-Geräte verwendet. Zum Abrufen des Zertifikats von AirWatch für die Authentifizierung wird ein Proxydienst zwischen dem Directories Management-Dienst und AirWatch eingerichtet.
Kennwort (AirWatch Connector)	Zur Benutzerkennwort-Authentifizierung kann der AirWatch Cloud Connector in den Directories Management-Dienst integriert werden. Sie können den Directories Management-Dienst so konfigurieren, dass Benutzer aus dem AirWatch-Verzeichnis synchronisiert werden.

Benutzer werden auf Basis der Authentifizierungsmethoden, der Standardregeln der Zugriffsrichtlinie, der Netzwerkbereiche und der von Ihnen konfigurierten Identitätsanbieter-Instanz authentifiziert. Nach dem Konfigurieren der Authentifizierungsmethoden können Sie Regeln für die Zugriffsrichtlinie erstellen, die die nach Gerätetyp zu verwendenden Authentifizierungsmethoden angeben.



## Konfigurieren von SecurID für Directories Management

Wenn Sie den RSA SecurID-Server konfigurieren, müssen Sie die Informationen des Directories Management -Dienstes als Authentifizierungs-Agent auf dem RSA SecurID-Server hinzufügen und die RSA SecurID-Serverinformationen im Directories Management -Dienst konfigurieren.

Wenn Sie SecurID konfigurieren, um zusätzliche Sicherheit zu bieten, müssen Sie sicherstellen, dass Ihr Netzwerk für Ihre Directories Management-Bereitstellung richtig konfiguriert ist. Insbesondere müssen Sie sich für SecurID vergewissern, ob der richtige Port geöffnet ist, damit Benutzer außerhalb Ihres Netzwerks über SecurID authentifiziert werden können.

Nach der Ausführung des Directories Management-Setup-Assistenten und der Konfiguration Ihrer Active Directory-Verbindung verfügen Sie über die erforderlichen Informationen zur Vorbereitung des RSA SecurID-Servers. Nach dem Vorbereiten des RSA SecurID-Servers für Directories Management müssen Sie SecurID in der Verwaltungskonsole aktivieren.

### ■ Vorbereiten des RSA SecurID-Servers

Der RSA SecurID-Server muss mit Informationen über die Directories Management -Appliance als Authentifizierungs-Agent konfiguriert werden. Die erforderlichen Informationen sind der Hostname und die IP-Adressen für Netzwerkschnittstellen.

### ■ Konfigurieren der RSA SecurID-Authentifizierung

Nachdem die Verzeichnisverwaltung als Authentifizierungsagent auf dem RSA SecurID-Server konfiguriert wurde, müssen Sie dem Connector die RSA SecurID-Konfigurationsinformationen hinzufügen.

## Vorbereiten des RSA SecurID-Servers

Der RSA SecurID-Server muss mit Informationen über die Directories Management -Appliance als Authentifizierungs-Agent konfiguriert werden. Die erforderlichen Informationen sind der Hostname und die IP-Adressen für Netzwerkschnittstellen.

### Voraussetzungen

- Stellen Sie sicher, dass eine der folgenden Versionen von RSA Authentication Manager im Unternehmensnetzwerk installiert und funktionsbereit ist: RSA AM 6.1.2, 7.1 SP2 und höher oder 8.0 und höher. Der Directories Management -Server verwendet AuthSDK\_Java\_v8.1.1.312.06\_03\_11\_03\_16\_51 (Agent API 8.1 SP1), das nur die vorhergehenden Versionen von RSA Authentication Manager (RSA SecurID-Server) unterstützt. Weitere Informationen zum Installieren und Konfigurieren von RSA Authentication Manager (RSA SecurID-Server) finden Sie in der RSA-Dokumentation.

## Vorgehensweise

- 1 Fügen Sie den Directories Management auf einer unterstützten Version des RSA SecurID-Servers als Authentifizierungs-Agent hinzu. Geben Sie die folgenden Informationen ein.

Option	Beschreibung
<b>Hostname</b>	Hostname von Directories Management.
<b>IP-Adresse</b>	IP-Adresse von Directories Management.
<b>Alternative IP-Adresse</b>	Wird Datenverkehr vom Connector über ein NAT-Gerät (Network Address Translation, Netzwerkadressübersetzung) an den RSA SecurID-Server geleitet, geben Sie die private IP-Adresse der Appliance ein.

- 2 Laden Sie die komprimierte Konfigurationsdatei herunter, und extrahieren Sie die Datei `sdconf.rec`. Diese Datei müssen Sie später beim Konfigurieren der RSA SecurID in Directories Management hochladen.

## Weiter

Wechseln Sie zur Verwaltungskonsole und zu den Setup-Seiten der Registerkarte „Identitäts- und Zugriffsmanagement“, wählen Sie den Connector aus und konfigurieren Sie auf der Seite „Authentifizierungsadapter“ die SecurID.

## Konfigurieren der RSA SecurID-Authentifizierung

Nachdem die Verzeichnisverwaltung als Authentifizierungsagent auf dem RSA SecurID-Server konfiguriert wurde, müssen Sie dem Connector die RSA SecurID-Konfigurationsinformationen hinzufügen.

## Voraussetzungen

- Vergewissern Sie sich, dass der RSA Authentication Manager (der RSA SecurID-Server) installiert und richtig konfiguriert ist.
- Laden Sie die komprimierte Datei vom RSA SecurID-Server herunter, und extrahieren Sie die Serverkonfigurationsdatei.

## Vorgehensweise

- 1 Navigieren Sie als Mandantenadministrator zu **Administration > Verzeichnisverwaltung > Konnektoren**.
- 2 Wählen Sie auf der Seite „Konnektoren“ den Worker-Link für den Connector aus, der für RSA-SecurID konfiguriert wird.
- 3 Klicken Sie auf **Authentifizierungsadapter** und dann auf **SecurIDIdpAdapter**.  
Sie werden auf die Anmeldeseite des Identity Managers umgeleitet.
- 4 Auf der Seite „Authentifizierungsadapter“ klicken Sie in der Zeile SecurIDIdpAdapter auf **Bearbeiten**.
- 5 Konfigurieren Sie die SecurID-Seite „Authentifizierungsadapter“.

Beim Konfigurieren der Seite SecurID werden die auf dem RSA SecurID-Server verwendeten Informationen und generierten Dateien benötigt.

Option	Aktion
Name	Der Name ist erforderlich. Der Standardname lautet „SecurIDIdpAdapter“. Sie können diese Angaben ändern.
SecurID aktivieren	Aktivieren Sie dieses Kontrollkästchen, um die SecurID-Authentifizierung zu aktivieren.
Anzahl der zulässigen Authentifizierungsversuche	Geben Sie die maximal zulässige Anzahl fehlgeschlagener Anmeldungen mit dem RSA SecurID-Token ein. Die Standardeinstellung lautet fünf Versuche.
Connector-Adresse	Geben Sie die IP-Adresse der Connector-Instanz ein. Der eingegebene Wert muss mit dem Wert übereinstimmen, den Sie beim Hinzufügen der Connector-Appliance als Authentifizierungs-Agent zum RSA SecurID-Server verwendet haben. Wenn auf Ihrem RSA SecurID-Server unter der Eingabe „Alternative IP-Adresse“ ein Wert zugewiesen wurde, geben Sie diesen Wert als Connector-IP-Adresse ein. Wenn keine alternative IP-Adresse zugewiesen wurde, geben Sie den Wert ein, der der Eingabe „IP-Adresse“ zugewiesen wurde.
IP-Adresse des Agent	Geben Sie den für <b>IP-Adresse</b> auf dem RSA SecurID-Server festgelegten Wert ein.
Serverkonfiguration	Laden Sie die RSA SecurID-Serverkonfigurationsdatei hoch. Zuerst müssen Sie die komprimierte Datei vom RSA SecurID-Server herunterladen und die Serverkonfigurationsdatei (standardmäßig sdconf.rec benannt) extrahieren.
Knoten-Secret	Wenn Sie das Feld für das Knoten-Secret leer lassen, kann dieses automatisch generiert werden. Es empfiehlt sich, die Knoten-Secret-Datei auf dem RSA SecurID-Server zu löschen und bewusst nicht hochzuladen. Stellen Sie sicher, dass die Knoten-Secret-Datei auf dem RSA SecurID-Server immer mit der Knoten-Secret-Datei auf der Server-Connector-Instanz identisch ist. Wenn Sie das Knoten-Secret an einem Speicherort ändern, nehmen Sie die Änderung auch an dem anderen Speicherort vor.

## 6 Klicken Sie auf **Speichern**.

### Weiter

Fügen Sie der Standardzugriffsrichtlinie die Authentifizierungsmethode hinzu. Navigieren Sie zu **Administration > Verzeichnisverwaltung > Richtlinien** und klicken Sie auf **Standardrichtlinie bearbeiten**, um die Standardrichtlinienregeln so zu bearbeiten, dass die SecurID-Authentifizierungsmethode der Regel in der richtigen Authentifizierungsreihenfolge hinzugefügt wird.

## Konfigurieren von RADIUS für Directories Management

Sie können Directories Management so konfigurieren, dass die Benutzer die RADIUS-Authentifizierung verwenden müssen (Remote Authentication Dial-In User Service). Sie können die Informationen des RADIUS-Servers im Directories Management-Dienst konfigurieren.

Der RADIUS-Support bietet eine große Anzahl alternativer Zwei-Faktor-Authentifizierungsoptionen, die auf Token basieren. Da Zwei-Faktor-Authentifizierungslösungen wie RADIUS auf separaten Servern installierte Authentication Manager verwenden, muss der RADIUS-Server konfiguriert und für den Identity Manager-Dienst zugänglich sein.

Wenn sich die Benutzer bei ihrem „Meine Apps“-Portal anmelden und die RADIUS-Authentifizierung aktiviert ist, wird ein besonderes Anmeldedialogfeld im Browser angezeigt. Die Benutzer geben den Benutzernamen und Passcode der RADIUS-Authentifizierung in das Anmeldedialogfeld ein. Wenn der RADIUS-Server eine Zugriffsherausforderung (Access Challenge) ausgibt, zeigt der Identity Manager-Dienst ein Dialogfeld mit der Aufforderung zur Eingabe einer zweiten Kennung an. Zurzeit ist der Support für RADIUS-Herausforderungen auf die Aufforderung zur Texteingabe beschränkt.

Nachdem ein Benutzer die Anmeldedaten in das Dialogfeld eingegeben hat, kann der RADIUS-Server eine SMS-Textnachricht oder eine E-Mail oder einen Text mithilfe anderer Out-of-Band-Mechanismen mit einem Code an das Mobiltelefon des Benutzers senden. Der Benutzer kann diesen Text und Code in das Anmeldedialogfeld eingeben, um die Authentifizierung abzuschließen.

Wenn der RADIUS-Server die Möglichkeit zum Importieren von Benutzern aus Active Directory bietet, werden die Endbenutzer möglicherweise erst aufgefordert, ihre Anmeldedaten für Active Directory einzugeben, bevor sie nach dem Benutzernamen und Passcode für die RADIUS-Authentifizierung gefragt werden.

### **Vorbereiten des RADIUS-Servers**

Richten Sie den RADIUS-Server ein und konfigurieren Sie ihn dann so, dass er RADIUS-Anfragen vom Directories Management-Dienst akzeptiert.

Informationen zum Einrichten des RADIUS-Servers finden Sie in den Einrichtungs-Handbüchern Ihres RADIUS-Händlers. Notieren Sie die RADIUS-Konfigurationsinformationen, da Sie diese Informationen verwenden, wenn Sie RADIUS im Dienst konfigurieren. Den Typ der RADIUS-Informationen, die zum Konfigurieren von Directories Management erforderlich sind, finden Sie unter [Konfigurieren der RADIUS-Authentifizierung in der Verzeichnisverwaltung](#).

Sie können einen sekundären Radiusauthentifizierungsserver einrichten, der für die Hochverfügbarkeit verwendet wird. Wenn der primäre RADIUS-Server nicht innerhalb des für die RADIUS-Authentifizierung konfigurierten Server-Timeouts antwortet, wird die Anfrage an den sekundären Server weitergeleitet. Wenn der primäre Server nicht antwortet, erhält der sekundäre Server alle zukünftigen Authentifizierungsanfragen.

### **Konfigurieren der RADIUS-Authentifizierung in der Verzeichnisverwaltung**

RADIUS-Software wird auf einem Authentication Manager-Server aktiviert. Folgen Sie der Konfigurationsdokumentation des Lieferanten für die RADIUS-Authentifizierung.

#### **Voraussetzungen**

Installieren und konfigurieren Sie die RADIUS-Software auf einem Authentifizierungsmanagerserver. Folgen Sie der Konfigurationsdokumentation des Lieferanten für die RADIUS-Authentifizierung.

Wenn Sie RADIUS in dem Dienst konfigurieren möchten, benötigen Sie die folgenden Informationen des RADIUS-Servers.

- IP-Adresse oder DNS-Name des RADIUS-Servers.
- Portnummern der Authentifizierung. Der Authentifizierungsport ist normalerweise 1812.

- Authentifizierungstyp. Zu den Authentifizierungstypen zählen PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP1, MSCHAP2 (Microsoft Challenge Handshake Authentication Protocol, Version 1 und 2).
- Der gemeinsame geheime Schlüssel von RADIUS, der für die Verschlüsselung und Entschlüsselung in RADIUS-Protokollmeldungen verwendet wird.
- Spezielle Zeitüberschreitungs- und Wiederholungswerte, die für die RADIUS-Authentifizierung erforderlich sind.
- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Konnektoren** aus.
- 2 Wählen Sie auf der Seite „Connectors“ den Worker-Link für den Connector aus, der für die RADIUS-Authentifizierung konfiguriert wird.
- 3 Klicken Sie auf **Authentifizierungsadapter** und dann auf **RadiusAuthAdapter**.  
Sie werden auf die Anmeldeseite des Identity Managers umgeleitet.
- 4 Klicken Sie auf **Bearbeiten**, um diese Felder auf der Seite „Authentifizierungsadapter“ zu konfigurieren.

Option	Aktion
Name	Der Name ist erforderlich. Der Standardname lautet „RadiusAuthAdapter“. Sie können diese Angaben ändern.
Aktivieren des Radiusadapters	Aktivieren Sie dieses Kontrollkästchen, um die RADIUS-Authentifizierung zu aktivieren.
Anzahl der zulässigen Authentifizierungsversuche	Geben Sie die maximale Anzahl fehlgeschlagener Anmeldeversuche ein, bei denen Sie RADIUS für die Anmeldung verwendet haben. Die Standardeinstellung lautet fünf Versuche.
Anzahl der Versuche beim Radius-Server.	Geben Sie die Gesamtanzahl der Wiederholungsversuche an. Wenn der primäre Server nicht antwortet, wartet der Dienst die konfigurierte Zeit, bevor er es erneut versucht.
Hostname/Adresse des Radius-Servers.	Geben Sie den Hostnamen oder die IP-Adresse des RADIUS-Servers ein.
Authentifizierungsport	Geben Sie die Nummer des Radius-Authentifizierungsports ein. Dies ist normalerweise 1812.
Accounting-Port	Geben Sie für die Portnummer 0 ein. Der Accounting-Port wird zurzeit nicht verwendet.
Authentifizierungstyp	Geben Sie das vom RADIUS-Server unterstützte Authentifizierungsprotokoll ein. Entweder PAP, CHAP, MSCHAP1 ODER MSCHAP2.

Option	Aktion
Gemeinsamer geheimer Schlüssel	Geben Sie den gemeinsamen geheimen Schlüssel ein, der zwischen dem RADIUS-Server und dem VMware Identity Manager-Dienst wird.
Server-Time-out in Sekunden	Geben Sie den Timeout des RADIUS-Servers in Sekunden ein, nach dem eine Wiederholung gesendet wird, wenn der RADIUS-Server nicht antwortet.
Realm-Präfix	(Optional) Die Position des Benutzerkontos wird „Realm“ genannt. Wenn Sie einen Realm-Präfix-String angeben, wird der String am Anfang des Benutzernamens platziert, wenn der Name an den RADIUS-Server gesendet wird. Wenn der Benutzername beispielsweise mit „jdoe“ angegeben wird und das Realm-Präfix DOMAIN-A\ angegeben wird, wird der Benutzername DOMAIN-A\jdoe an den RADIUS-Server gesendet. Wenn Sie diese Felder nicht konfigurieren, wird nur der eingegebene Benutzername gesendet.
Realm-Suffix	(Optional) Wenn Sie ein Realm-Suffix angeben, wird dieser am Ende des Benutzernamens platziert. Wenn das Suffix z. B. @myco.com ist, wird der Benutzername jdoe@myco.com an den RADIUS-Server gesendet.
Kennphrasen-hinweis der Anmeldeseite	Geben Sie den Textstring ein, der in der Meldung auf der Anmeldeseite des Benutzers angezeigt werden soll und die Benutzer auffordert, den richtigen Radius-Passcode einzugeben. Wenn dieses Feld z. B. mit <b>AD-Kennwort zuerst und dann SMS-Passcode konfiguriert wird, steht in der Meldung der Anmeldeseite Geben Sie zuerst Ihr AD-Kennwort und dann den SMS-Passcode ein.</b> Der Standardtextstring ist <b>RADIUS-Passcode</b> .

- 5 Sie können für die Hochverfügbarkeit einen zweiten RADIUS-Server aktivieren.

Konfigurieren Sie den sekundären Server wie in Schritt 4 beschrieben.

- 6 Klicken Sie auf **Speichern**.

#### Weiter

Fügen Sie der Standardzugriffsrichtlinie die RADIUS-Authentifizierungsmethode hinzu. Wählen Sie **Administration > Verzeichnisverwaltung > Richtlinien** aus und klicken Sie auf **Standardrichtlinie bearbeiten**, um die Standardrichtlinienregeln so zu bearbeiten, dass die RADIUS-Authentifizierungsmethode der Regel in der richtigen Authentifizierungsreihenfolge hinzugefügt wird.

## Konfigurieren eines Zertifikats oder Smartcard-Adapters zur Verwendung mit Directories Management

Sie können die x509-Zertifikatauthentifizierung so konfigurieren, dass Clients sich mithilfe von Zertifikaten auf Desktops und mobilen Geräten authentifizieren oder einen Smartcard-Adapter für die Authentifizierung verwenden können. Die zertifikatbasierte Authentifizierung beruht auf etwas, was der Benutzer besitzt (dem privaten Schlüssel oder der Smartcard) und auf etwas, was die Person weiß (dem Kennwort für den privaten Schlüssel oder der PIN der Smartcard). Ein X.509-Zertifikat verwendet den Standard der Public Key Infrastructure (PKI), um zu überprüfen, ob ein im Zertifikat enthaltener öffentlicher Schlüssel dem Benutzer gehört. Bei der Smartcard-Authentifizierung legen Benutzer die Smartcard in den Computer ein und geben eine PIN ein.

Die Smartcard-Zertifikate werden in den lokalen Zertifikatspeicher des Benutzercomputers kopiert. Die Zertifikate im lokalen Zertifikatspeicher sind für alle Browser auf diesem Benutzercomputer verfügbar (mit einigen Ausnahmen) und stehen deshalb einer Directories Management-Instanz im Browser zur Verfügung.

- **Verwenden des Benutzer-Prinzipalnamens für die Zertifikatauthentifizierung**

Sie können die Zertifikatzuordnung in Active Directory verwenden. Zertifikat- und Smartcard-Anmeldungen verwenden für die Überprüfung der Benutzerkonten den Benutzer-Prinzipalnamen (UPN, User Principal Name) von Active Directory. Die Active Directory-Konten von Benutzern, die sich im Directories Management-Dienst authentifizieren möchten, müssen über einen gültigen UPN verfügen, der dem UPN im Zertifikat entspricht.

- **Zertifizierungsstelle für die Authentifizierung erforderlich**

Um Anmeldungen mit der Zertifikatauthentifizierung zu ermöglichen, müssen Root-Zertifikate und Zwischen-Zertifikate in Directories Management hochgeladen werden.

- **Verwenden der Zertifikatsperrüberprüfung**

Sie können die Zertifikatsperrüberprüfung konfigurieren, um zu verhindern, dass sich Benutzer authentifizieren, deren Benutzerzertifikate gesperrt sind. Zertifikate werden oft gesperrt, wenn ein Benutzer eine Organisation verlässt, eine Smartcard verliert oder die Abteilung wechselt.

- **Konfigurieren der Zertifikatsauthentifizierung für die Verzeichnisverwaltung**

Die Zertifikatsauthentifizierung lässt sich über die Verzeichnisverwaltungs-Funktion der vRealize Automation-Verwaltungskonsolle aktivieren und konfigurieren.

## **Verwenden des Benutzer-Prinzipalnamens für die Zertifikatauthentifizierung**

Sie können die Zertifikatzuordnung in Active Directory verwenden. Zertifikat- und Smartcard-Anmeldungen verwenden für die Überprüfung der Benutzerkonten den Benutzer-Prinzipalnamen (UPN, User Principal Name) von Active Directory. Die Active Directory-Konten von Benutzern, die sich im Directories Management-Dienst authentifizieren möchten, müssen über einen gültigen UPN verfügen, der dem UPN im Zertifikat entspricht.

Sie können Directories Management für die Verwendung einer E-Mail-Adresse zur Überprüfung des Benutzerkontos konfigurieren, wenn der UPN nicht im Zertifikat vorhanden ist.

Sie haben auch die Möglichkeit, die Verwendung eines alternativen UPN-Typs zu aktivieren.

## **Zertifizierungsstelle für die Authentifizierung erforderlich**

Um Anmeldungen mit der Zertifikatauthentifizierung zu ermöglichen, müssen Root-Zertifikate und Zwischen-Zertifikate in Directories Management hochgeladen werden.

Die Zertifikate werden in den lokalen Zertifikatspeicher des Benutzercomputers kopiert. Die Zertifikate im lokalen Zertifikatspeicher sind für alle Browser auf diesem Benutzercomputer verfügbar (mit einigen Ausnahmen) und stehen deshalb einer Directories Management-Instanz im Browser zur Verfügung.

Für die Smartcard-Authentifizierung gilt: wenn ein Benutzer eine Verbindung mit einer Directories Management-Instanz initiiert, sendet der Directories Management-Dienst eine Liste vertrauenswürdiger Zertifizierungsstellen an den Browser. Der Browser vergleicht die Liste vertrauenswürdiger Zertifizierungsstellen mit den verfügbaren Benutzerzertifikaten, wählt ein passendes Zertifikat aus und fordert den Benutzer dann zur Eingabe einer Smartcard-PIN auf. Sind mehrere gültige Benutzerzertifikate verfügbar, wird der Benutzer zur Auswahl eines Zertifikats aufgefordert.

Wenn ein Benutzer nicht authentifiziert werden kann, sind die Root- und Zwischen-CAs eventuell nicht korrekt eingerichtet worden oder der Dienst wurde nach dem Hochladen der Root- und Zwischen-CAs auf den Server nicht neu gestartet. In diesem Fall kann der Browser die installierten Zertifikate nicht anzeigen und der Benutzer das korrekte Zertifikat nicht auswählen, so dass die Authentifizierung des Zertifikats scheitert.

### **Verwenden der Zertifikatsperrüberprüfung**

Sie können die Zertifikatsperrüberprüfung konfigurieren, um zu verhindern, dass sich Benutzer authentifizieren, deren Benutzerzertifikate gesperrt sind. Zertifikate werden oft gesperrt, wenn ein Benutzer eine Organisation verlässt, eine Smartcard verliert oder die Abteilung wechselt.

Es wird sowohl eine Zertifikatsperrüberprüfung mit Zertifikatsperrlisten (CRL, Certificate Revocation Lists) als auch mit dem Online Certificate Status Protocol (OCSP) unterstützt. Eine CRL ist eine Liste gesperrter Zertifikate, die von der ausgebenden Zertifizierungsstelle veröffentlicht wurde. Bei OCSP handelt es sich um ein Zertifikatsüberprüfungsprotokoll zur Ermittlung des Sperrstatus eines Zertifikats.

Sie können die Zertifikatsperrüberprüfung an der Administratorkonsole unter Connector > Authentifizierungsadapter > CertificateAuthAdapter bei der Konfiguration der Zertifikatauthentifizierung konfigurieren.

Sie können CRL und OCSP in der derselben Zertifikat-Authentifizierungsadapter-Konfiguration festlegen. Wenn Sie beide Arten der Zertifikatsperrüberprüfung konfiguriert haben und das Kontrollkästchen „CRL im Falle eines OCSP-Fehlers verwenden“ aktiviert ist, wird OCSP zuerst überprüft und bei einem Scheitern die Sperrüberprüfung an CRL weitergegeben. Beachten Sie, dass umgekehrt bei einem Scheitern der CRL-Überprüfung die Sperrüberprüfung nicht an OCSP zurückgegeben wird.

### **Anmelden mit der CRL-Überprüfung**

Bei aktivierter Zertifikatsperre wertet der Directories Management -Server eine CRL-Liste zur Ermittlung des Sperrstatus eines Benutzerzertifikats aus.

Ist ein Zertifikat gesperrt, kann die Authentifizierung mit dem Zertifikat nicht durchgeführt werden.

### **Anmelden mit der OCSP-Zertifikatsüberprüfung**

Ist eine Sperrüberprüfung mittels Certificate Status Protocol (OCSP) konfiguriert, sendet der Directories Management eine Anforderung an den OCSP-Antwortdienst, um den Sperrstatus eines bestimmten Benutzerzertifikats zu ermitteln. Der Directories Management -Server überprüft mit dem OCSP-Anmeldezertifikat, ob die Antworten vom OCSP-Antwortdienst authentisch sind.

Wenn das Zertifikat gesperrt ist, scheitert die Authentifizierung.

Bei der Konfiguration der Authentifizierung kann festgelegt werden, dass diese an die CRL-Überprüfung weitergegeben wird, wenn keine Antwort vom OCSP-Antwortdienst erfolgt oder die Antwort ungültig ist.



## Konfigurieren der Zertifikatsauthentifizierung für die Verzeichnisverwaltung

Die Zertifikatsauthentifizierung lässt sich über die Verzeichnisverwaltungs-Funktion der vRealize Automation-Verwaltungskonsolle aktivieren und konfigurieren.

### Voraussetzungen

- Abrufen des Root-Zertifikats und der Zwischen-Zertifikate von der Zertifizierungsstelle (CA), die die Zertifikate der Benutzer signiert hat.
- (Optional) Eine OID-Liste (Objektkennungsliste) der gültigen Zertifikatsrichtlinien für die Zertifikatsauthentifizierung.
- Für Sperrprüfungen: den Datei-Speicherort der Zertifikatswiderrufsliste und die URL des OCSP-Servers.
- (Optional) Speicherort des OCSP-Antwortsignaturzertifikats.
- Inhalt des Zustimmungsf formulars, wenn vor der Authentifizierung ein Zustimmungsf formular angezeigt werden muss.

### Vorgehensweise

- 1 Navigieren Sie als Mandantenadministrator zu **Administration > Verzeichnisverwaltung > Konnektoren**.
- 2 Wählen Sie auf der Seite „Konnektoren“ den Worker-Link für den Connector aus, der konfiguriert wird.
- 3 Klicken Sie auf **Authentifizierungsadapter** und dann auf **CertificateAuthAdapter**.  
Sie werden auf die Anmeldeseite des Identity Managers umgeleitet.
- 4 Konfigurieren Sie die Seite „Zertifikat-Authentifizierungsadapter“.

**Hinweis** Mit einem Sternchen wird angezeigt, dass die Informationen erforderlich sind.

Option	Beschreibung
<b>*Name</b>	Der Name ist erforderlich. Der Standardname lautet „CertificateAuthAdapter“. Sie können diesen Namen ändern.
<b>Zertifikatsadapter aktivieren</b>	Aktivieren Sie das Kontrollkästchen, um die Zertifikatauthentifizierung zu aktivieren.
<b>*Root- und Zwischen-CA-Zertifikate</b>	Wählen Sie die hochzuladenden Zertifikatsdateien aus. Sie können mehrere Root- und Zwischen-CA-Zertifikate auswählen, die im DER- oder PEM-Format codiert sind.
<b>Hochgeladene CA-Zertifikate</b>	Die hochgeladenen Zertifikatsdateien sind im Abschnitt „Hochgeladene CA-Zertifikate“ des Formulars aufgeführt.
<b>E-Mail verwenden, wenn kein UPN im Zertifikat vorhanden ist</b>	Wenn der Benutzer-Prinzipalname (User Principal Name, UPN) nicht im Zertifikat vorhanden ist, aktivieren Sie dieses Kontrollkästchen, um das Attribut „emailAddress“ als Erweiterung des Alternativen Antragstellernamens für die Validierung der Benutzerkonten zu verwenden.

Option	Beschreibung
<b>Zertifikatsrichtlinien wurden akzeptiert</b>	Erstellen Sie eine Liste mit Objektkennungen, die in den Erweiterungen der Zertifikatsrichtlinien akzeptiert werden. Geben Sie die Objekt-ID-Nummern (OID) für die Zertifikatsausstellungsrichtlinie ein. Klicken Sie auf <b>Weiteren Wert hinzufügen</b> , um weitere OIDs hinzuzufügen.
<b>Zertifikatssperrung aktivieren</b>	Aktivieren Sie das Kontrollkästchen, um die Zertifikatssperrüberprüfung zu aktivieren. Durch die Zertifikatssperrüberprüfung wird verhindert, dass sich Benutzer authentifizieren können, die über gesperrte Zertifikate verfügen.
<b>CRL von Zertifikaten verwenden</b>	Aktivieren Sie das Kontrollkästchen, um die von der Zertifizierungsstelle veröffentlichte Zertifikatssperrliste (CRL, Certificate Revocation Lists) zu verwenden, um den Status eines Zertifikats (gesperrt oder nicht gesperrt) zu validieren.
<b>CRL-Speicherort</b>	Geben Sie den Serverdateipfad oder den lokalen Dateipfad ein, von dem die CRL geladen werden kann.
<b>OCSP-Sperrung aktivieren</b>	Aktivieren Sie das Kontrollkästchen, um das Zertifikatvalidierungsprotokoll „Online Certificate Status Protocol (OCSP)“ zu verwenden, um den Sperrstatus des Zertifikats zu erfahren.
<b>CRL im Falle eines OCSP-Fehlers verwenden</b>	Wenn Sie CRL und OCSP konfigurieren. Sie markieren dieses Kontrollkästchen für die Verwendung von CRL, wenn die OCSP-Prüfung nicht verfügbar ist.
<b>OCSP-Nonce senden</b>	Aktivieren Sie dieses Kontrollkästchen, wenn Sie den eindeutigen Bezeichner der OCSP-Anfrage in der Antwort übermitteln möchten.
<b>OCSP-URL</b>	Wenn Sie OCSP-Widerruf aktiviert haben, geben Sie die OCSP-Serveradresse für die Widerrufsprüfung ein.
<b>Signaturzertifikat des OCSP-Antwortdienstes</b>	Geben Sie den Pfad des OCSP-Zertifikats für den Antwortdienst: <i>/path/to/file.cer</i> ein.
<b>Zustimmungsformular vor der Authentifizierung aktivieren</b>	Aktivieren Sie dieses Kontrollkästchen, um eine Seite mit einem Zustimmungsformular anzuzeigen, bevor sich die Benutzer mit der Zertifikatauthentifizierung bei ihrem „Meine Apps“-Portal anmelden.
<b>Inhalt des Zustimmungsformulars</b>	Geben Sie hier den Text ein, der im Zustimmungsformular angezeigt werden soll.

## 5 Klicken Sie auf **Speichern**.

### Weiter

- Fügen Sie die Zertifikatsauthentifizierungsmethode der Standardzugriffsrichtlinie hinzu. Navigieren Sie zu **Administration > Verzeichnisverwaltung > Richtlinien** und klicken Sie auf **Standardrichtlinie bearbeiten**, um die Standardrichtlinienregeln zu bearbeiten, und auf „Zertifikat hinzufügen“, um diese zur ersten Authentifizierungsmethode für die Standardrichtlinie zu machen. Das Zertifikat muss die erste in der Richtlinienregel aufgeführte Authentifizierungsmethode sein, andernfalls schlägt die Zertifikatauthentifizierung fehl.
- Wenn die Zertifikatauthentifizierung konfiguriert ist und die Service-Appliance hinter dem Lastenausgleichsdienst eingerichtet ist, müssen Sie sicherstellen, dass der Directories Management Connector mit SSL-Durchleitung am Lastenausgleichsdienst konfiguriert ist, d.h. SSL darf nicht im Lastenausgleichsdienst beendet werden. Diese Konfiguration stellt sicher, dass das SSL-Handshake zwischen Connector und Client stattfindet, damit das Zertifikat an den Connector übergeben wird.

## Konfigurieren einer externen Identitätsanbieter-Instanz zum Authentifizieren von Benutzern

Sie können einen externen Identitätsanbieter für die Authentifizierung von Benutzern im Directories Management-Dienst konfigurieren.

Führen Sie folgende Schritte aus, bevor Sie die Verwaltungskonsole verwenden, um eine externe Identitätsanbieter-Instanz hinzuzufügen.

- Vergewissern Sie sich, dass die externen Instanzen SAML 2.0-konform sind und dass der Dienst die externe Instanz erreichen kann.
- Beziehen Sie die geeigneten Metadateninformation für die externe Instanz, die Sie beim Konfigurieren des Identitätsanbieters in der Verwaltungskonsole hinzufügen müssen. Die Metadateninformationen, die Sie von der externen Instanz erhalten, sind entweder die URL zu den Metadaten oder die Metadaten selbst.

### Konfigurieren einer Identitätsanbieter-Instanz

vRealize Automation enthält eine Identitätsanbieter-Standardinstanz. Benutzer können bei Bedarf weitere Identitätsanbieter erstellen.

vRealize Automation enthält einen Standard-Identitätsanbieter. In den meisten Fällen werden die Kundenbedürfnisse mit dem Standardanbieter ausreichend abgedeckt. Wenn Sie eine bereits vorhandene Identitätsverwaltungslösung für Unternehmen verwenden, können Sie jedoch einen benutzerdefinierten Identitätsanbieter so einrichten, dass die Benutzer zu Ihrer vorhandenen Identitätslösung umgeleitet werden.

#### Voraussetzungen

- Konfigurieren Sie die Netzwerkbereiche, an die Sie diese Identitätsanbieter-Instanz zur Authentifizierung weiterleiten möchten. Siehe [Hinzufügen oder Bearbeiten eines Netzwerkbereichs](#).
- Zugriff auf das externe Metadatendokument. Es kann sich dabei um die URL zu den Metadaten oder die eigentlichen Metadaten handeln.
- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

#### Vorgehensweise

- 1 Navigieren Sie zu **Administration > Verzeichnisverwaltung > Identitätsanbieter**.

Auf der Seite werden alle konfigurierten Identitätsanbieter angezeigt.

- 2 Klicken Sie auf **Identitätsanbieter hinzufügen** und bearbeiten Sie die Einstellungen für die Identitätsanbieter-Instanz.

Formularelement	Beschreibung
Name des Identitätsanbieters	Geben Sie einen Namen für diese Identitätsanbieter-Instanz ein.
SAML-Metadaten	<p>Fügen Sie das IDPs XML-basierte Metadatendokument Dritter hinzu, um Vertrauen zum Identitätsanbieter aufzubauen.</p> <ol style="list-style-type: none"> <li>1 Geben Sie die SAML-Metadaten-URL oder den xml-Inhalt in das Textfeld ein.</li> <li>2 Klicken Sie auf <b>IDP-Metadaten verarbeiten</b>. Die von IdP unterstützten Formate der Namens-ID werden aus den Metadaten extrahiert und der Tabelle mit den Formaten der Namens-ID hinzugefügt.</li> <li>3 Wählen Sie in der Spalte mit dem Wert der Namens-ID das Benutzerattribut des Dienstes aus, das den angezeigten ID-Formaten zugeordnet werden soll. Sie können benutzerdefinierte externe Namens-ID-Formate hinzufügen und den Benutzerattributwerten im Dienst zuordnen.</li> <li>4 (Optional) Wählen Sie das Zeichenfolgenformat für den NameIDPolicy-Antwortbezeichner aus.</li> </ol>
Benutzer	Wählen Sie die Directories Management-Verzeichnisse der Benutzer aus, die sich mit diesem Identitätsanbieter authentifizieren können.
Netzwerk	<p>Die im Dienst konfigurierten vorhandenen Netzwerkbereiche werden aufgeführt.</p> <p>Wählen Sie die Netzwerkbereiche der Benutzer anhand ihrer IP-Adressen aus, die Sie zu dieser Identitätsanbieter-Instanz für die Authentifizierung umleiten möchten.</p>
Authentifizierungsmethoden	Fügen Sie die Authentifizierungsmethoden hinzu, die vom externen Identitätsanbieter unterstützt werden. Wählen Sie die SAML-Authentifizierungskontextklasse aus, welche die Authentifizierungsmethode unterstützt.
SAML-Signaturzertifikat	Klicken Sie auf <b>Metadaten des Dienstanbieters</b> , um die URL zur Metadaten-URL des Directories Management SAML-Dienstanbieters anzuzeigen. Kopieren und speichern Sie die URL. Diese URL wird konfiguriert, wenn Sie die SAML-Assertion im Identitätsanbieter Dritter so bearbeiten, dass Directories Management-Benutzer zugeordnet werden können.
Hostname	Geben Sie, wenn das Feld <b>Hostname</b> angezeigt wird, den Namen des Hosts an, auf den der Identitätsanbieter zur Authentifizierung umgeleitet wird. Wenn Sie einen anderen Nicht-Standardport als 443 verwenden, können Sie dies als Hostname:Port einstellen. Beispiel: my-co.example.com:8443.

- 3 Klicken Sie auf **Hinzufügen**.

#### Weiter

- Kopieren und speichern Sie die Directories Management-Dienstanbieter-Metadaten, die zum Konfigurieren der externen Identitätsanbieter-Instanz erforderlich sind. Diese Metadaten sind entweder im Abschnitt „SAML-Signierungszertifikat“ oder auf der Seite „Identitätsanbieter“ verfügbar.
- Fügen Sie die Authentifizierungsmethode der Standardrichtlinie für Dienste hinzu.

Informationen zum Hinzufügen und zum Anpassen von Ressourcen, die Sie dem Katalog hinzufügen, finden Sie im Handbuch *Einrichten von Ressourcen in Directories Management*.

## Verwalten der auf Benutzer anzuwendenden Authentifizierungsmethoden

Der Directories Management-Dienst versucht, Benutzer basierend auf den Authentifizierungsmethoden, der Standardzugriffsrichtlinie, den Netzwerkbereichen und den Identitätsanbieter-Instanzen, die Sie konfiguriert haben, zu authentifizieren.

Wenn Benutzer versuchen, sich anzumelden, wertet der Dienst die Regeln der Standardzugriffsrichtlinie aus, um die anzuwendende Regel in der Richtlinie auszuwählen. Die Authentifizierungsmethoden werden in der Reihenfolge angewendet, in der sie in der Regel aufgeführt sind. Die erste Identitätsanbieter-Instanz, die die Anforderungen an die Authentifizierungsmethode und den Netzwerkbereich der Regel erfüllt, wird ausgewählt und die Benutzerauthentifizierungsanforderung zur Authentifizierung an die Identitätsanbieter-Instanz weitergeleitet. Wenn die Authentifizierung scheitert, wird die nächste in der Regel konfigurierte Authentifizierungsmethode ausgewählt.

Sie können Regeln hinzufügen, die die Authentifizierungsmethoden festlegen, die von den Gerätetypen oder den Gerätetypen und dem spezifischen Netzwerkbereich verwendet werden müssen. Beispiel: Sie konfigurieren eine Regel, die festlegt, dass Benutzer für die Anmeldung von iOS-Geräten aus einem bestimmten Netzwerk zur Authentifizierung RSA SecurID verwenden müssen. Darüber hinaus können Sie eine weitere Regel erstellen, die verlangt, dass sich alle Gerätetypen, die sich über eine interne Netzwerk-IP-Adresse anmelden, mit ihrem Kennwort authentifizieren müssen.

### Hinzufügen oder Bearbeiten eines Netzwerkbereichs

Die Netzwerkbereiche lassen sich verwalten, um die IP-Adressen zu definieren, von denen aus sich die Benutzer über einen Active Directory-Link anmelden können. Sie fügen die von Ihnen erstellten Netzwerkbereiche bestimmten Identitätsanbieter-Instanzen und Zugriffsrichtlinien hinzu.

Auf der Basis Ihrer Netzwerktopologie definieren Sie Netzwerkbereiche für Ihre Directories Management-Bereitstellung.

Ein Netzwerkbereich, genannt ALLE BEREICHE, wird standardmäßig erstellt. Dieser Netzwerkbereich enthält alle im Internet verfügbaren IP-Adressen, d. h. 0.0.0.0 bis 255.255.255.255. Selbst wenn Ihre Bereitstellung eine einzige Identitätsanbieter-Instanz enthält, können Sie den IP-Adressbereich ändern und weitere Bereiche hinzufügen, um bestimmte IP-Adressen im Standardnetzwerkbereich ein- oder auszuschließen. Sie können andere Netzwerkbereiche mit bestimmten IP-Adressen erstellen, die Sie für bestimmte Verwendungszwecke anwenden können.

---

**Hinweis** Der Name des Standardnetzwerkbereichs („ALLE BEREICHE“) und seine Beschreibung („ein Netzwerk für alle Bereiche“) können bearbeitet werden. Sie können den Namen und die Beschreibung bearbeiten, und beispielsweise den Text in einer anderen Sprache anzeigen, indem Sie auf der Seite „Netzwerkbereiche“ auf den Namen des betreffenden Netzwerkbereichs klicken.

---

### Voraussetzungen

- Sie haben Mandanten für Ihre vRealize Automation-Bereitstellung konfiguriert und einen geeigneten Active Directory-Link zur Unterstützung der Standardauthentifizierung von Active Directory-Benutzer-ID und -Kennwort eingerichtet.
- Active Directory ist für die Verwendung in Ihrem Netzwerk installiert und konfiguriert.

- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Netzwerkbereiche** aus.
- 2 Bearbeiten Sie einen vorhandenen Netzwerkbereich oder fügen Sie einen neuen Netzwerkbereich hinzu.

Option	Beschreibung
<b>Vorhandenen Bereich bearbeiten</b>	Klicken Sie zum Bearbeiten auf den Namen des Netzwerkbereichs.
<b>Bereich hinzufügen</b>	Klicken Sie auf <b>Netzwerkbereich hinzufügen</b> , um einen neuen Bereich hinzuzufügen.

- 3 Füllen Sie das Formular aus.

Formularelement	Beschreibung
Name	Geben Sie einen Namen für den Netzwerkbereich ein.
Beschreibung	Geben Sie eine Beschreibung für den Netzwerkbereich ein.
View-Pods	Die Option „View-Pods“ wird nur angezeigt, wenn das View-Modul aktiviert ist. Host der Client-Zugriffs-URL Geben Sie die korrekte Horizon Client-Zugriffs-URL für den Netzwerkbereich ein. Client-Zugriffsport Geben Sie den korrekten Horizon Client-Zugriffsport für den Netzwerkbereich ein.
IP-Bereiche	Bearbeiten Sie IP-Bereiche oder fügen Sie IP-Bereiche hinzu, bis alle gewünschten IP-Adressen ein- und alle unerwünschten IP-Adressen ausgeschlossen sind.

### Weiter

- Verknüpfen Sie die einzelnen Netzwerkbereiche jeweils mit einer Identitätsanbieter-Instanz.
- Weisen Sie Netzwerkbereiche entsprechend Zugriffsrichtlinienregeln zu. Siehe [Konfigurieren von Einstellungen für die Zugriffsrichtlinie](#).

### Auswahl der mit dem Verzeichnis zu synchronisierenden Attribute

Wenn Sie das Directories Management-Verzeichnis für die Synchronisierung mit Active Directory einrichten, geben Sie die Benutzerattribute an, die mit dem Verzeichnis synchronisiert werden sollen. Bevor Sie das Verzeichnis einrichten, können Sie auf der Seite „Benutzerattribute“ angeben, welche Standardattribute erforderlich sind, und auf Wunsch zusätzliche Attribute definieren, die Sie den Active Directory-Attributen zuordnen möchten.

Wenn Sie die Seite „Benutzerattribute“ vor der Erstellung des Verzeichnisses konfigurieren, können Sie die erforderlichen Standardattribute ändern, Attribute als erforderlich markieren und benutzerdefinierte Attribute hinzufügen.

Eine Liste der standardmäßig zugeordneten Attribute finden Sie unter [Verwalten von Benutzerattributen, die aus Active Directory synchronisieren](#).

Nachdem das Verzeichnis erstellt worden ist, können Sie erforderliche Attribute als nicht erforderlich festlegen und benutzerdefinierte Attribute löschen. Sie können ein vorhandenes Attribut allerdings nicht als erforderliches Attribut definieren.

Wenn Sie nach der Erstellung des Verzeichnisses weitere Attribute hinzufügen, die mit dem Verzeichnis synchronisiert werden sollen, dann öffnen Sie die Seite „Zugeordnete Attribute“ des Verzeichnisses und ordnen diese Attribute den gewünschten Active Directory-Attributen zu.

### Vorgehensweise

- 1 Melden Sie sich als System- oder Mandantenadministrator bei vRealize Automation an.
- 2 Klicken Sie auf die Registerkarte „Administration“.
- 3 Wählen Sie **Verzeichnisverwaltung > Benutzerattribute** aus.
- 4 Prüfen Sie im Abschnitt „Standardattribute“ die Liste der erforderlichen Attribute und nehmen Sie die erforderlichen Änderungen vor, um die erforderlichen Attribute festzulegen.
- 5 Im Abschnitt „Attribute“ fügen Sie der Liste den Attributnamen des Directories Management-Verzeichnisses hinzu.
- 6 Klicken Sie auf **Speichern**.  
  
Der Standardattributstatus wird aktualisiert und die von Ihnen hinzugefügten Attribute werden der Liste „Zugeordnete Attribute“ des Verzeichnisses hinzugefügt.
- 7 Gehen Sie nach Erstellung des Verzeichnisses zur Seite „Identitätsquellen“ und wählen Sie das Verzeichnis aus.
- 8 Klicken Sie auf **Synchronisierungseinstellungen > Zugeordnete Attribute**.
- 9 Im Dropdown-Menü für die hinzugefügten Attribute wählen Sie das Active Directory-Attribut für die Zuordnung aus.
- 10 Klicken Sie auf **Speichern**.

Das Verzeichnis wird bei der nächsten Synchronisierung mit Active Directory aktualisiert.

### Anwenden der Standardzugriffsrichtlinie

Der Directories Management-Dienst enthält eine Standardzugriffsrichtlinie, die den Zugriff der Benutzer auf ihre Apps-Portale steuert. Sie können diese Richtlinie bearbeiten, um die Richtlinienregeln nach Bedarf zu ändern.

Wenn Sie andere Authentifizierungsmethoden als die Kennwortauthentifizierung aktivieren möchten, müssen Sie die Standardrichtlinie bearbeiten und die aktive Authentifizierungsmethode den Richtlinienregeln hinzufügen.

Jede Regel in der Standardzugriffsrichtlinie erfordert, dass eine Reihe von Kriterien erfüllt ist, bevor dem Benutzer Zugriff auf das Apps-Portal gewährt wird. Sie geben einen Netzwerkbereich an, wählen den Benutzertyp aus, der auf den Inhalt zugreifen kann, und wählen die zu verwendenden Authentifizierungsmethoden aus. Siehe [Verwalten von Zugriffsrichtlinien](#).

Die Anzahl der Benutzeranmeldungsversuche, die der Dienst mit einer gegebenen Authentifizierungsmethode unternimmt, ist unterschiedlich. Der Dienst führt nur einen Authentifizierungsversuch für Kerberos oder die Zertifikatauthentifizierung durch. Wenn der Benutzer in diesem Versuch nicht erfolgreich angemeldet werden kann, wird ein neuer Versuch mit der nächsten Authentifizierungsmethode in der Liste durchgeführt. Die maximale Anzahl fehlgeschlagener Anmeldeversuche mit Active Directory-Kennwort und RSA SecurID-Authentifizierung beträgt standardmäßig fünf. Wenn der Benutzer fünf fehlgeschlagene Anmeldeversuche unternommen hat, versucht der Dienst, den Benutzer mit der nächsten Authentifizierungsmethode in der Liste anzumelden. Nachdem alle Authentifizierungsmethoden angewendet wurden, gibt der Dienst eine Fehlermeldung aus.

## Anwenden von Authentifizierungsmethoden auf Richtlinienregeln

In den Standardrichtlinienregeln ist nur die Kennwortauthentifizierungsmethode konfiguriert. Sie müssen die Richtlinienregeln bearbeiten, um andere konfigurierte Authentifizierungsmethoden auszuwählen und die Reihenfolge festzulegen, in der die Authentifizierungsmethoden zur Authentifizierung verwendet werden sollen.

### Voraussetzungen

Aktivieren und konfigurieren Sie die von Ihrer Organisation unterstützten Authentifizierungsmethoden. Siehe [Integrieren alternativer Benutzerauthentifizierungsprodukte in die Verzeichnisverwaltung](#).

### Vorgehensweise

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Richtlinien** aus.
- 2 Klicken Sie zur Bearbeitung auf die Standardzugriffsrichtlinie.
- 3 Um eine Seite für eine Richtlinienregel zur Bearbeitung zu öffnen, klicken Sie auf den Authentifizierungsnamen in der Spalte „Authentifizierungsmethode“. Um eine neue Richtlinienregel hinzuzufügen, klicken Sie auf das Symbol +.
  - a Stellen Sie sicher, dass der Netzwerkbereich korrekt ist. Wenn Sie eine neue Regel hinzufügen, wählen Sie den Netzwerkbereich für diese Richtlinienregel aus.
  - b Wählen Sie den Gerätetyp, den diese Regel verwaltet, aus dem Dropdown-Menü **und der Benutzer versucht, auf Inhalte zuzugreifen von...** aus.
  - c Konfigurieren Sie die Authentifizierungsreihenfolge. Im Dropdown-Menü **muss der Benutzer die Authentifizierung mit der folgenden Methode durchführen** wählen Sie die Authentifizierungsmethode aus, die zuerst angewendet werden soll.  
  
Damit Benutzer für die Authentifizierung zwei Authentifizierungsmethoden verwenden müssen, klicken Sie auf + und geben Sie eine zweite Authentifizierungsmethode ein.
  - d (Optional) Um zusätzliche Authentifizierungsmethoden zu konfigurieren für den Fall, dass die erste Authentifizierung fehlschlägt, wählen Sie eine weitere aktivierte Authentifizierungsmethode aus dem nächsten Dropdown-Menü aus.

Sie können einer Regel mehrere Fallback-Authentifizierungsmethoden hinzufügen.



- e Im Textfeld für den Wert **Erneute Authentifizierung nach:** geben Sie die Anzahl der Stunden ein, nach denen Benutzer sich erneut authentifizieren müssen.
- f (Optional) Erstellen Sie eine benutzerdefinierte Meldung über einen verweigerten Zugriff, die beim Scheitern der Authentifizierung angezeigt wird. Es stehen Ihnen dabei bis zu 4000 Zeichen zur Verfügung. Das entspricht etwa 650 Wörtern. Wenn Sie Benutzer auf eine andere Seite weiterleiten möchten, fügen Sie im Feld **Link-URL** den URL-Link hinzu. Im Textfeld **Link-Text** geben Sie den Text ein, der für den Link angezeigt werden soll. Wird dieses Feld leer gelassen, wird das Wort Fortfahren angezeigt.
- g Klicken Sie auf **Speichern**.

#### 4 Klicken Sie auf **Speichern**.

##### Richtlinienregel bearbeiten

Ist der Netzwerkbereich eines Benutzers... ALLE BEREICHE

und der Benutzer versucht, auf Inhalte zuzugreifen von... Web-Browser

muss der Benutzer die Authentifizierung mit der folgenden Methode durchführen...

Password und

Wenn die vorangegangene Authentifizierungsmethode fehlschlägt, daan:

-Authentifizierungsmethode auswählen- Nur

+ Fallback-Methode(n)

Erneute Authentifizierung nach: 8 Stunden

#### 5 Klicken Sie auf **Speichern** und auf der Richtlinienseite erneut auf **Speichern**.

## Konfigurieren von Kerberos für Directories Management

Die Kerberos-Authentifizierung bietet Benutzern, die erfolgreich an ihrer Active Directory-Domäne angemeldet sind, ohne weitere Anmeldungsaufforderungen Zugriff auf ihr Apps-Portal. Sie aktivieren die Windows-Authentifizierung, um mit dem Kerberos-Protokoll gesicherte Interaktionen zwischen den Browsern der Benutzer und dem Directories Management-Dienst zuzulassen. Sie müssen keine direkte Konfiguration von Active Directory vornehmen, um die Kerberos-Funktion in Ihrer Bereitstellung nutzen zu können.

Aktuell können Interaktionen zwischen dem Browser eines Benutzers und dem Dienst nur in Windows-Betriebssystemen durch Kerberos authentifiziert werden. Für den Zugriff auf den Dienst von anderen Betriebssystemen wird die Kerberos-Authentifizierung nicht genutzt.

### ■ Konfigurieren der Kerberos-Authentifizierung

Wenn Sie den Directories Management-Dienst für die Bereitstellung der Kerberos-Authentifizierung konfigurieren möchten, müssen Sie der Domäne beitreten und die Kerberos-Authentifizierung im Directories Management-Connector aktivieren.

### ■ Konfigurieren von Internet Explorer für den Zugriff auf die Webschnittstelle

Wenn Kerberos für Ihre Bereitstellung konfiguriert ist und Sie Benutzern Zugriff auf die Webschnittstelle über Internet Explorer gewähren möchten, müssen Sie den Internet Explorer-Browser konfigurieren.

### ■ Konfigurieren von Firefox für den Zugriff auf die Webschnittstelle

Wenn Kerberos für Ihre Bereitstellung konfiguriert ist und Sie Benutzern Zugriff auf die Webschnittstelle über Firefox gewähren möchten, müssen Sie den Firefox-Browser konfigurieren.

### ■ Konfigurieren von Chrome für den Zugriff auf die Webschnittstelle

Wenn Kerberos für Ihre Bereitstellung konfiguriert ist und Sie Benutzern Zugriff auf die Webschnittstelle über Chrome gewähren möchten, müssen Sie den Chrome-Browser konfigurieren.

## Konfigurieren der Kerberos-Authentifizierung

Wenn Sie den Directories Management-Dienst für die Bereitstellung der Kerberos-Authentifizierung konfigurieren möchten, müssen Sie der Domäne beitreten und die Kerberos-Authentifizierung im Directories Management-Connector aktivieren.

### Vorgehensweise

- 1 Navigieren Sie als Mandantenadministrator zu **Administration > Verzeichnisverwaltung > Konnektoren**.
- 2 Auf der Seite „Connectors“ klicken Sie bei dem Connector, der für die Kerberos-Authentifizierung konfiguriert ist, auf **Domäne beitreten**.
- 3 Geben Sie auf der Seite „Domäne beitreten“ die Informationen für die Active Directory-Domäne ein.

Option	Beschreibung
Domäne	Geben Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) des Active Directory ein. Der eingegebene Domänenname muss der Windows-Domäne entsprechen, in der sich der Connector-Server befindet.
Domänenbenutzer	Geben Sie den Benutzernamen eines Kontos in Active Directory ein, das über die erforderlichen Berechtigungen verfügt, um mit Systemen einer Active Directory-Domäne beizutreten.
Domänenkennwort	Geben Sie das entsprechende Kennwort für AD-Benutzername ein. Dieses Kennwort wird von Directories Management nicht gespeichert

Klicken Sie auf **Speichern**.

Die Seite „Domäne beitreten“ wird aktualisiert und es wird eine Meldung angezeigt, dass Sie der Domäne beigetreten sind.

- 4 Klicken Sie in der Spalte „Mitarbeiter“ für den Connector auf **Authentifizierungsadapter**.
- 5 Wählen Sie **KerberosIdpAdapter**

Sie werden auf die Anmeldeseite des Identity Managers umgeleitet.

- 6 Klicken Sie in der Zeile „KerberosIdpAdapter“ auf **Bearbeiten** und konfigurieren Sie die Seite „Kerberos-Authentifizierung“.

Option	Beschreibung
Name	Der Name ist erforderlich. Der Standardname lautet „KerberosIdpAdapter“. Sie können diese Angaben ändern.
Verzeichnis-UID-Attribut	Geben Sie das Kontoattribut ein, das den Benutzernamen enthält.
Windows-Authentifizierung aktivieren	Wählen Sie diese Option, um die Authentifizierungsinteraktionen von zwischen dem Browser des Benutzers und Directories Management zu erweitern.
NTLM aktivieren	Wählen Sie diese Option, um die protokollbasierte Authentifizierung des NT LAN Manager (NTLM) nur dann zu aktivieren, wenn Ihre Active Directory-Infrastruktur auf der NTLM-Authentifizierung basiert.
Umleitung aktivieren	Aktivieren Sie diese Option, wenn Kerberos für Round-Robin-DNS und Lastausgleichsdienste nicht unterstützt wird. Authentifizierungsanforderungen werden zu „Hostnamen umleiten“ umgeleitet. Wenn dieses Kontrollkästchen ausgewählt ist, geben Sie den Namen des Umleitungshosts in das Textfeld <b>Hostnamen umleiten</b> ein. Meist ist dies der Hostname des Dienstes.

- 7 Klicken Sie auf **Speichern**.

#### Weiter

Fügen Sie der Standardzugriffsrichtlinie die Authentifizierungsmethode hinzu. Navigieren Sie zu **Administration > Verzeichnisverwaltung > Richtlinien** und klicken Sie auf **Standardrichtlinie bearbeiten**, um die Standardrichtlinienregeln so zu bearbeiten, dass die Kerberos-Authentifizierungsmethode der Regel in der richtigen Authentifizierungsreihenfolge hinzugefügt wird.

#### Konfigurieren von Internet Explorer für den Zugriff auf die Webschnittstelle

Wenn Kerberos für Ihre Bereitstellung konfiguriert ist und Sie Benutzern Zugriff auf die Webschnittstelle über Internet Explorer gewähren möchten, müssen Sie den Internet Explorer-Browser konfigurieren.

Die Kerberos-Authentifizierung funktioniert für Directories Management auf Windows-Betriebssystemen.

**Hinweis** Implementieren Sie diese auf Kerberos bezogenen Schritte nicht auf anderen Betriebssystemen.

#### Voraussetzungen

Konfigurieren Sie Internet Explorer für jeden Benutzer oder geben Sie den Benutzern die entsprechenden Anweisungen, nachdem Sie Kerberos konfiguriert haben.

#### Vorgehensweise

- 1 Stellen Sie sicher, dass Sie bei Windows als Domänenbenutzer angemeldet sind.
- 2 Aktivieren Sie in Internet Explorer die automatische Anmeldung.
  - a Wählen Sie **Extras > Internetoptionen > Sicherheit** aus.
  - b Klicken Sie auf **Stufe anpassen**.

- c Aktivieren Sie **Automatisches Anmelden nur in der Intranetzone**.
  - d Klicken Sie auf **OK**.
- 3 Stellen Sie sicher, dass diese Instanz der virtuellen Connector-Appliance Teil der lokalen Intranetzone ist.
- a Verwenden Sie Internet Explorer für den Zugriff auf die Directories Management -Anmeldungs-URL unter *https://myconnectorhost.domain/authenticate/*.
  - b Die Zone wird unten rechts in der Statusleiste des Browserfensters angezeigt.  
Wenn die Zone das lokale Intranet ist, ist die Internet Explorer-Konfiguration fertig gestellt.
- 4 Wenn die Zone nicht das lokale Intranet ist, fügen Sie die Directories Management -Anmeldungs-URL der Internetzone hinzu.
- a Wählen Sie **Extras > Internetoptionen > Sicherheit > Lokales Intranet > Sites** aus.
  - b Aktivieren Sie **Intranet automatisch ermitteln**.  
War diese Option nicht aktiviert, reicht diese Aktivierung möglicherweise aus, um zur Intranetzone hinzuzufügen.
  - c (Optional) Wenn Sie **Intranet automatisch ermitteln** aktiviert haben, klicken Sie mehrmals auf **OK**, bis alle Dialogfelder geschlossen sind.
  - d Klicken Sie im Dialogfeld Lokales Intranet auf **Erweitert**.  
Ein zweites Dialogfeld mit dem Namen Lokales Intranet wird angezeigt.
  - e Geben Sie die Directories Management-URL in das Textfeld **Diese Website zur Zone hinzufügen** ein.  
*https://myconnectorhost.domain/authenticate/*
  - f Klicken Sie auf **Hinzufügen > Schließen > OK**.
- 5 Vergewissern Sie sich, dass Internet Explorer berechtigt ist, die Windows-Authentifizierung an die vertrauenswürdige Site zu übergeben.
- a Klicken Sie im Dialogfeld Internetoptionen auf die Registerkarte **Erweitert**.
  - b Aktivieren Sie **Integrierte Windows-Authentifizierung aktivieren**.  
Diese Option wird erst nach dem Neustarten von Internet Explorer wirksam.
  - c Klicken Sie auf **OK**.
- 6 Melden Sie sich an der Webschnittstelle an, um den Zugriff zu prüfen.  
Wenn die Kerberos-Authentifizierung erfolgreich ist, gelangen Sie über die Test-URL zur Webschnittstelle

Das Kerberos-Protokoll sichert alle Interaktionen zwischen dieser Internet Explorer-Browserinstanz und Directories Management ab. Die Benutzer können sich nun per Single Sign On-Zugriff an ihrem „Meine Apps“-Portal anmelden.

## Konfigurieren von Firefox für den Zugriff auf die Webschnittstelle

Wenn Kerberos für Ihre Bereitstellung konfiguriert ist und Sie Benutzern Zugriff auf die Webschnittstelle über Firefox gewähren möchten, müssen Sie den Firefox-Browser konfigurieren.

Die Kerberos-Authentifizierung funktioniert für Directories Management auf Windows-Betriebssystemen.

### Voraussetzungen

Konfigurieren Sie Firefox für jeden Benutzer, oder geben Sie den Benutzern die entsprechenden Anweisungen, nachdem Sie Kerberos konfiguriert haben.

### Vorgehensweise

- 1 Geben Sie in das URL-Textfeld von Firefox `about:config` ein, um auf die erweiterten Einstellungen zuzugreifen.
- 2 Klicken Sie **Ich werde vorsichtig sein, versprochen!**.
- 3 Doppelklicken Sie in der Spalte Einstellungsname auf **network.negotiate-auth.trusted-uris**.
- 4 Geben Sie Ihre Directories Management -URL in das Textfeld ein.  
*`https://myconnectorhost.domain.com`*
- 5 Klicken Sie auf **OK**.
- 6 Doppelklicken Sie in der Spalte Einstellungsname auf **network.negotiate-auth.delegation-uris**.
- 7 Geben Sie Ihre Directories Management-URL in das Textfeld ein.  
*`https://myconnectorhost.domain.com/authenticate/`*
- 8 Klicken Sie auf **OK**.
- 9 Testen Sie die Kerberos-Funktionalität mit einem Firefox-Browser, indem Sie sich bei der -Anmelde-URL anmelden. Zum Beispiel: *`https://myconnectorhost.domain.com/authenticate/`*.

Wenn die Kerberos-Authentifizierung erfolgreich ist, gelangen Sie über die Test-URL zur Webschnittstelle.

Das Kerberos-Protokoll sichert alle Interaktionen zwischen dieser Firefox-Browserinstanz und Directories Management ab. Die Benutzer können sich nun per Single Sign On-Zugriff an ihrem „Meine Apps“-Portal anmelden.

## Konfigurieren von Chrome für den Zugriff auf die Webschnittstelle

Wenn Kerberos für Ihre Bereitstellung konfiguriert ist und Sie Benutzern Zugriff auf die Webschnittstelle über Chrome gewähren möchten, müssen Sie den Chrome-Browser konfigurieren.

Die Kerberos-Authentifizierung funktioniert für Directories Management auf Windows-Betriebssystemen.

---

**Hinweis** Implementieren Sie diese auf Kerberos bezogenen Schritte nicht auf anderen Betriebssystemen.

---

## Voraussetzungen

- Konfigurieren Sie Kerberos.
- Da Chrome die Internet Explorer-Konfiguration zur Aktivierung der Kerberos-Authentifizierung verwendet, müssen Sie die Internet Explorer-Konfiguration für Chrome freigeben. In der Google-Dokumentation finden Sie Informationen zum Konfigurieren von Chrome für Kerberos-Authentifizierung.

## Vorgehensweise

- 1 Testen Sie die Kerberos-Funktionalität unter Verwendung von Chrome.
- 2 Melden Sie sich bei Directories Management unter <https://myconnectorhost.domain.com/authenticate/> an.

Wenn die Kerberos-Authentifizierung erfolgreich ist, gelangen Sie über die Test-URL zur Webschnittstelle.

Wenn alle erforderlichen Kerberos-Konfigurationseinstellungen korrekt sind, sichert das entsprechende Protokoll (Kerberos) alle Interaktionen zwischen Chrome-Browserinstanzen und Directories Management ab. Die Benutzer können sich per Single Sign On-Zugriff an ihrem „Meine Apps“-Portal anmelden.

## Szenario: Konfigurieren eines Active Directory-Links für hochverfügbare vRealize Automation -Bereitstellung

Als Mandantenadministrator können Sie eine Active Directory über LDAP-Verbindung zur Unterstützung der Benutzerauthentifizierung für Ihre hochverfügbare vRealize Automation-Bereitstellung konfigurieren.

Jede vRealize Automation-Appliance enthält einen Connector, der die Benutzerauthentifizierung unterstützt, jedoch ist in der Regel nur ein Connector zum Ausführen der Verzeichnissynchronisierung konfiguriert. Es spielt keine Rolle, welchen Connector Sie als Synchronisierungs-Connector auswählen. Damit die Verzeichnisverwaltung mit Hochverfügbarkeit unterstützt wird, müssen Sie einen zweiten Connector konfigurieren, der Ihrer zweiten vRealize Automation-Appliance entspricht. Dieser verbindet sich mit Ihrem Identitätsanbieter und verweist auf dasselbe Active Directory. Fällt eine Appliance aus, wird bei dieser Konfiguration die Verwaltung der Benutzerauthentifizierung von der anderen Appliance übernommen.

In einer hochverfügbaren Umgebung müssen alle Knoten dieselbe Gruppe von Active Directories, Benutzern, Authentifizierungsmethoden usw. bedienen. Am einfachsten wird dies dadurch erreicht, dass der Identitätsanbieter zum Cluster heraufgestuft wird, indem der Lastausgleichsdienst-Host als der Identitätsanbieter-Host eingerichtet wird. Mit dieser Konfiguration werden alle Authentifizierungsanforderungen an den Lastausgleichsdienst gerichtet, der diese dann an einen der Connectors weiterleitet.

## Voraussetzungen

- Installieren Sie eine verteilte vRealize Automation-Bereitstellung mit den entsprechenden Lastausgleichsdiensten. Siehe *Installieren von vRealize Automation 7.1*.
- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

## Vorgehensweise

- 1 Wählen Sie **Administration > Verwaltung der Verzeichnisse > Verzeichnisse** aus.
- 2 Klicken Sie auf **Verzeichnis hinzufügen**.
- 3 Geben Sie die jeweiligen Active Directory-Kontoeinstellungen ein und akzeptieren Sie die Standardoptionen.

Option	Beispieleingabe
<b>Verzeichnisname</b>	Fügen Sie die IP-Adresse des Active Directory-Domänennamens hinzu.
<b>Synchronisierungs-Connector</b>	Jede vRealize Automation-Appliance enthält einen Connector. Sie können alle verfügbaren Connectoren verwenden.
<b>Basis-DN</b>	Geben Sie den definierten Namen (DN, Distinguished Name) des Startpunkts für Verzeichnisserversuchen ein. Beispiel: <b>cn=users,dc=corp,dc=local</b> .
<b>Bind-DN</b>	Geben Sie den vollständigen definierten Namen (DN, Distinguished Name), einschließlich des allgemeinen Namens (Common Name, CN), eines Active Directory-Benutzerkontos mit Berechtigungen zum Suchen von Benutzern ein. Beispiel: <b>cn=config_admin infra,cn=users,dc=corp,dc=local</b> .
<b>Bind-DN-Kennwort</b>	Geben Sie das Active Directory-Kennwort für das Konto ein, das nach Benutzern suchen kann.

- 4 Klicken Sie auf **Verbindung testen**, um die Verbindung zum konfigurierten Verzeichnis zu testen.  
Wenn die Verbindung fehlschlägt, überprüfen Sie Ihre Einträge in allen Feldern und wenden Sie sich ggf. an den Systemadministrator.
- 5 Klicken Sie auf **Speichern und weiter**.  
Die Seite „Domänen auswählen“ mit der Liste der Domänen wird angezeigt.
- 6 Behalten Sie die Auswahl der Standarddomäne bei und klicken Sie auf **Weiter**.
- 7 Überprüfen Sie, ob die Attributnamen den richtigen Active Directory-Attributen zugeordnet sind. Ist dies nicht der Fall, wählen Sie das erforderliche Active Directory-Attribut aus dem Dropdown-Menü aus. Klicken Sie auf **Weiter**.
- 8 Wählen Sie die Gruppen und Benutzer aus, die synchronisiert werden sollen.
  - a Klicken Sie auf das Symbol **Hinzufügen (+)**.
  - b Geben Sie die Benutzerdomäne ein und klicken Sie auf **Gruppen suchen**.  
Beispiel: **cn=users,dc=corp,dc=local**.
  - c Aktivieren Sie das Kontrollkästchen **Alle auswählen**.
  - d Klicken Sie auf **Auswählen**.
  - e Klicken Sie auf **Weiter**.

- f Klicken Sie auf **+**, um weitere Benutzer hinzuzufügen. Geben Sie diese beispielsweise im Format **CN=Benutzername,CN=Benutzer,OU=MeineEinheit,DC=MeineFirma,DC=com** ein.

Um Benutzer auszuschließen, klicken Sie auf **+**, um einen Filter für den Ausschluss bestimmter Benutzertypen zu erstellen. Dazu wählen Sie das Benutzerattribut für den Filter, die Abfragerregel und den Wert aus.

- g Klicken Sie auf **Weiter**.

- 9 Überprüfen Sie auf der Seite, wie viele Benutzer und Gruppen mit dem Verzeichnis synchronisiert werden, und klicken Sie auf **Verzeichnis synchronisieren**.

Für die Verzeichnissynchronisierung wird einige Zeit benötigt. Der Prozess wird jedoch im Hintergrund ausgeführt und Sie können Ihre Arbeit fortsetzen.

- 10 Konfigurieren Sie einen zweiten Connector zwecks Unterstützung von Hochverfügbarkeit.

- a Melden Sie sich beim Lastausgleichsdienst für Ihre vRealize Automation-Bereitstellung als Mandantenadministrator an.

Die Lastausgleichsdienst-URL lautet *load balancer address/vcac/org/tenant\_name*.

- b Wählen Sie **Administration > Verzeichnisverwaltung > Identitätsanbieter** aus.

- c Klicken Sie auf den Identitätsanbieter, der derzeit für Ihr System verwendet wird.

Das vorhandene Verzeichnis und der vorhandene Connector, die die grundlegende Identitätsverwaltung für Ihr System bereitstellen, werden angezeigt.

- d Klicken Sie in der Dropdown-Liste auf **Connector hinzufügen** und wählen Sie den Connector aus, der Ihrer zweiten vRealize Automation-Appliance entspricht.

- e Geben Sie das entsprechende Kennwort in das Textfeld **Bind-DN-Kennwort** ein, das nach Auswahl des Connectors angezeigt wird.

- f Klicken Sie auf **Connector hinzufügen**.

- g Ändern Sie den Hostnamen in der Weise, dass er auf den Lastausgleichsdienst verweist.

Sie haben das Active Directory Ihres Unternehmens mit vRealize Automation verbunden und die Verzeichnisverwaltung für Hochverfügbarkeit konfiguriert.

### Weiter

Zur Erhöhung der Sicherheit können Sie ein bidirektionales Vertrauensverhältnis zwischen Ihrem Identitätsanbieter und Ihrem Active Directory konfigurieren. Siehe [Konfigurieren einer bidirektionalen Vertrauensstellung zwischen vRealize Automation und Active Directory](#).

## Konfigurieren der Smartcard-Authentifizierung für vRealize Automation

Als Systemadministrator müssen Sie die Smartcard-Authentifizierung für die vRealize Automation-Bereitstellung mit Verzeichnisverwaltung konfigurieren.



Mit Verzeichnisverwaltung werden mehrere Identitätsanbieter und Konnektor-Cluster für jedes konfigurierte Active Directory unterstützt. Sie können für die Verwendung der Smartcard-Authentifizierung entweder einen einzelnen externen Konnektor oder einen Konnektor-Cluster mit einem entsprechenden Identitätsanbieter hinter einem Lastausgleichsdienst, der SSL-Passthrough zulässt, einrichten.

Es stehen verschiedene Optionen für die Zertifikatkonfiguration für die Verwendung mit der Smartcard-Authentifizierung zur Verfügung. Siehe [Konfigurieren eines Zertifikats oder Smartcard-Adapters zur Verwendung mit Directories Management](#).

### Voraussetzungen

- Konfigurieren Sie eine entsprechende Active Directory-Verbindung für die Verwendung mit der vRealize Automation-Bereitstellung.
- Laden Sie die OVA-Datei herunter, die für die Konfiguration eines Konnektors aus [VMware vRealize Automation Tools und SDK](#) erforderlich ist.
- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

### Vorgehensweise

#### 1 Generieren eines Konnektor-Aktivierungstokens

Generieren Sie einen Aktivierungscode für den neuen Konnektor in der vRealize Automation-Konsole. Stellen Sie erst danach die virtuelle Konnektor-Appliance für die Verwendung für die Smartcard-Authentifizierung bereit. Der Aktivierungscode wird zur Einrichtung der Kommunikation zwischen Verzeichnisverwaltung und dem Konnektor verwendet.

#### 2 Bereitstellen der Connector-OVA-Datei

Sie können nach dem Download einer Konnektor-OVA-Datei diese unter Verwendung des VMware vSphere Client oder vSphere Web Client bereitstellen.

#### 3 Konfigurieren der Connector-Einstellungen

Sie müssen nach der Bereitstellung der Konnektor-OVA-Datei den Setup-Assistenten ausführen, um die Appliance zu aktivieren und die Administratorkennwörter zu konfigurieren.

#### 4 Anwenden einer öffentlichen Zertifizierungsstelle

Wenn Verzeichnisverwaltung installiert ist, wird ein standardmäßiges SSL-Zertifikat generiert. Sie können das Standardzertifikat für Testzwecke verwenden. Für Produktionsumgebungen müssen Sie jedoch gewerbliche SSL-Zertifikate generieren und installieren.

#### 5 Erstellen eines Arbeitsbereichs-Identitätsanbieters

Sie müssen einen Arbeitsbereichs-Identitätsanbieter für die Verwendung mit einem externen Konnektor erstellen.

#### 6 Konfigurieren der Zertifikatauthentifizierung und Konfigurieren der Regeln für Standardzugriffsrichtlinien

Sie müssen den externen Konnektor für die Verwendung mit Active Directory und der Domäne von vRealize Automation konfigurieren.

## Generieren eines Konnektor-Aktivierungstokens

Generieren Sie einen Aktivierungscode für den neuen Konnektor in der vRealize Automation-Konsole. Stellen Sie erst danach die virtuelle Konnektor-Appliance für die Verwendung für die Smartcard-Authentifizierung bereit. Der Aktivierungscode wird zur Einrichtung der Kommunikation zwischen Verzeichnisverwaltung und dem Konnektor verwendet.

Sie können einen einzelnen Konnektor oder einen Konnektor-Cluster konfigurieren. Wenn Sie einen Konnektor-Cluster verwenden möchten, wiederholen Sie diesen Vorgang für jeden benötigten Konnektor.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Konnektoren** aus.
- 2 Geben Sie im Textfeld **Konnektor-ID-Name** einen Namen für den neuen Konnektor ein.
- 3 Drücken Sie die **Eingabetaste**.  
Der Aktivierungscode für den Konnektor wird im Textfeld **Konnektor-Aktivierungscode** angezeigt.
- 4 Kopieren Sie den Aktivierungscode, der für die Konfiguration des Konnektors mit der OVA-Datei verwendet wird.

## Bereitstellen der Connector-OVA-Datei

Sie können nach dem Download einer Konnektor-OVA-Datei diese unter Verwendung des VMware vSphere Client oder vSphere Web Client bereitstellen.

Sie stellen die OVA-Datei unter Verwendung des vSphere Client oder vSphere Web Client bereit.

### Voraussetzungen

- Ermitteln Sie die DNS-Datensätze und den Hostnamen für Ihre Connector-OVA-Bereitstellung.
- Verwenden Sie für den vSphere Web Client Firefox oder Chrome. Verwenden Sie zum Bereitstellen der OVA-Datei nicht den Internet Explorer.
- Laden Sie die OVA-Datei herunter, die für die Konfiguration eines Konnektors aus [VMware vRealize Automation Tools und SDK](#) erforderlich ist.

### Vorgehensweise

- 1 Wählen Sie im vSphere Client oder im vSphere Web Client **Datei > OVF-Vorlage bereitstellen** aus.

- 2 Geben Sie auf den Seiten von „OVF-Vorlage bereitstellen“ die speziellen Daten für Ihre Connector-Bereitstellung ein.

Seite	Beschreibung
<b>Quelle</b>	Navigieren Sie zum Speicherort des OVA-Pakets oder geben Sie eine URL ein.
<b>Details der OVA-Vorlage</b>	Überprüfen Sie, ob Sie die richtige Version ausgewählt haben.
<b>Lizenz</b>	Lesen Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf <b>Akzeptieren</b> .
<b>Name und Speicherort</b>	Geben Sie den Namen der virtuellen Appliance ein. Der Name muss im Bestandsordner eindeutig sein und er darf bis zu 80 Zeichen lang sein. Bei Namen wird die Groß-/Kleinschreibung beachtet. Wählen Sie einen Speicherort für die virtuelle Appliance:
<b>Host/Cluster</b>	Wählen Sie den Host oder Cluster zum Ausführen der bereitgestellten Vorlage aus.
<b>Ressourcenpool</b>	Wählen Sie den Ressourcenpool aus.
<b>Speicher</b>	Wählen Sie den Speicherort aus, an dem die Dateien der virtuellen Maschine gespeichert werden sollen.
<b>Festplattenformat</b>	Wählen Sie das Festplattenformat für die Dateien aus. Wählen Sie für Produktionsumgebungen das Format <b>Thick Provision</b> aus. Verwenden Sie für Evaluierungen und Tests das Format <b>Thin Provision</b> aus.
<b>Netzwerkzuordnung</b>	Ordnen Sie die Netzwerke in Ihrer Umgebung den Netzwerken der OVF-Vorlage zu.
<b>Eigenschaften</b>	<p>a Wählen Sie im Feld <b>Einstellung der Zeitzone</b> die richtige Zeitzone aus.</p> <p>b Das Kontrollkästchen für das Programm zur Verbesserung der Kundenerfahrung ist standardmäßig aktiviert. VMware erfasst anonym Daten zu Ihrer Bereitstellung, damit VMware besser auf die Benutzeranforderungen reagieren kann. Wenn die Daten nicht erfasst werden sollen, deaktivieren Sie das Kontrollkästchen.</p> <p>c Geben Sie im Textfeld „Hostname“ den zu verwendenden Hostnamen ein. Wenn dieses Feld leer ist, wird zum Suchen des Hostnamens Reverse-DNS verwendet.</p> <p>d Um die statische IP-Adresse für Connector zu konfigurieren, geben Sie die Adresse für jedes der folgenden Felder ein: „Standard-Gateway“, „DNS“, „IP-Adresse“ und „Netzmaske“.</p> <p><b>Wichtig</b> Wenn eines dieser vier Felder oder das Feld „Hostname“ leer ist, wird DHCP verwendet.</p> <p>Um DHCP zu verwenden, lassen Sie die Adressfelder leer.</p>
<b>Bereit zum Abschließen</b>	Überprüfen Sie Ihre Auswahl und klicken Sie auf <b>Beenden</b> .

Je nach der Geschwindigkeit Ihres Netzwerks kann die Bereitstellung mehrere Minuten dauern. Im Dialogfeld mit der Fortschrittsanzeige können Sie den Stand der Bereitstellung verfolgen.

- 3 Ist die Bereitstellung abgeschlossen, wählen Sie die -Appliance aus, klicken Sie mit der rechten Maustaste und wählen Sie aus dem eingeblendeten Kontextmenü **Energie > Einschalten**.

Die -Appliance wird initialisiert. Sie können die Registerkarte **Konsole** öffnen, um die Details anzuzeigen. Wenn die Initialisierung der virtuellen Appliance abgeschlossen ist, werden auf dem Bildschirm „Konsole“ die -Version und die URLs zum Anmelden beim-Setup-Assistenten für das Abschließen des Setups angezeigt.

## Weiter

Mit dem Setup-Assistenten fügen Sie den Aktivierungscode und die Administrationskennwörter hinzu.

## Konfigurieren der Connector-Einstellungen

Sie müssen nach der Bereitstellung der Konnektor-OVA-Datei den Setup-Assistenten ausführen, um die Appliance zu aktivieren und die Administratorkennwörter zu konfigurieren.

### Voraussetzungen

- Sie haben einen Aktivierungscode für den Konnektor generiert.
- Stellen Sie sicher, dass die Konnektor-Appliance eingeschaltet ist und Sie über die Konnektor-URL verfügen.
- Stellen Sie eine Liste der Kennwörter für den Konnektor-Administrator, das Root-Konto und das sshuser-Konto zusammen.

### Vorgehensweise

- 1 Um den Setup-Assistenten auszuführen, geben Sie die Connector-URL ein, die auf der Registerkarte der Konsole angezeigt wird, nachdem die OVA-Datei bereitgestellt wurde.
- 2 Klicken Sie auf der Seite „Willkommen“ auf **Fortfahren**.
- 3 Erstellen Sie sichere Kennwörter für die folgenden Administratorkonten für die virtuelle Connector-Appliance.

Sichere Kennwörter bestehen aus mindestens acht Zeichen, enthalten Zeichen in Groß- und Kleinbuchstaben sowie mindestens eine Ziffer oder ein Sonderzeichen.

Option	Beschreibung
<b>Appliance-Administrator</b>	Erstellen Sie das Administratorkennwort für die Appliance. Der Benutzername lautet <b>admin</b> und kann nicht geändert werden. Sie verwenden dieses Konto und dieses Kennwort für die Anmeldung bei den Connector-Diensten, um Zertifikate, Appliance-Kennwörter und die Syslog-Konfiguration zu verwalten.  <b>Wichtig</b> Das Kennwort des Benutzers <b>admin</b> muss aus mindestens sechs Zeichen bestehen.
<b>Root-Konto</b>	Für die Installation der Connector-Appliance wird ein Standard-VMware-Root-Kennwort verwendet. Erstellen Sie ein neues Root-Kennwort.
<b>sshuser-Konto</b>	Erstellen Sie das Kennwort für den Remotezugriff auf die Connector-Appliance.

- 4 Klicken Sie auf **Fortfahren**.
- 5 Fügen Sie auf der Seite „Konnektor aktivieren“ den Aktivierungscode ein und klicken auf **Weiter**.

- 6 Wenn Sie ein selbstsigniertes Zertifikat im internen Konnektor von vRealize Automation verwenden, müssen Sie auch die **Zertifizierungsstellen-Stammzertifikat**-Informationen eingeben.

Sie können das Zertifizierungsstellen-Stammzertifikat über <https://:8443/cfg/ssl> abrufen. Wählen Sie die Registerkarte **SSL in einem Lastausgleichsdienst beenden** aus und klicken Sie anschließend auf den Link für `/horizon_workspace_rootca.pem`.

Der Aktivierungscode wird bestätigt und die Kommunikation zwischen dem Dienst und der Konnektor-Instanz wird hergestellt, um die Konnektor-Konfiguration abzuschließen.

## Weiter

Im Dienst richten Sie Ihre Umgebung gemäß Ihren Anforderungen ein. Wenn Sie beispielsweise einen zusätzlichen Konnektor hinzugefügt haben, um zwei Verzeichnisse mit integrierter Windows-Authentifizierung zu synchronisieren, erstellen Sie das Verzeichnis und verknüpfen es mit dem neuen Konnektor.

## Anwenden einer öffentlichen Zertifizierungsstelle

Wenn Verzeichnisverwaltung installiert ist, wird ein standardmäßiges SSL-Zertifikat generiert. Sie können das Standardzertifikat für Testzwecke verwenden. Für Produktionsumgebungen müssen Sie jedoch gewerbliche SSL-Zertifikate generieren und installieren.

---

**Hinweis** Wenn der Directories Management auf einen Lastausgleichsdienst verweist, wird das SSL-Zertifikat auf den Lastausgleichsdienst angewendet.

---

## Voraussetzungen

Generieren Sie eine Zertifikatssignieranforderung (CSR, Certificate Signing Request) und Sie erhalten ein gültiges, signiertes Zertifikat von einer Zertifizierungsstelle. Wenn Ihre Organisation von einer Zertifizierungsstelle signierte SSL-Zertifikate bereitstellt, können Sie diese verwenden. Das Zertifikat muss im PEM-Format vorliegen.

## Vorgehensweise

- 1 Melden Sie sich bei der Administratorseite für die Konnektor-Appliance als ein Admin-Benutzer unter dem folgenden Speicherort an: <https://myconnector.mycompany:8443/cfg>
- 2 In der Verwaltungskonsole klicken Sie auf **Appliance-Einstellungen**.  
Standardmäßig ist „VA-Konfiguration“ ausgewählt.
- 3 Klicken Sie auf **Manuelle Konfiguration**.
- 4 Im angezeigten Dialogfeld geben Sie das Serveradministratorkennwort von Directories Management ein.
- 5 Wählen Sie **Zertifikat installieren** aus.
- 6 Wählen Sie auf der Registerkarte „SSL auf einer Identity Manager-Appliance beenden“ den Eintrag **Benutzerdefiniertes Zertifikat** aus.

- 7 Geben Sie in das Textfeld **SSL-Zertifikatskette** die Host-, Zwischen- und Root-Zertifikate in dieser Reihenfolge ein.

Das SSL-Zertifikat funktioniert nur, wenn Sie die gesamte Zertifikatskette in der richtigen Reihenfolge eingeben. Kopieren Sie für jedes Zertifikat alle Angaben zwischen den Zeilen -----BEGIN CERTIFICATE----- und -----END CERTIFICATE----- inklusive dieser Zeilen.

Stellen Sie sicher, dass das Zertifikat den FQDN-Hostnamen enthält.

- 8 Fügen Sie den privaten Schlüssel in das Textfeld „Privater Schlüssel“ ein. Kopieren Sie alles zwischen -----BEGIN RSA PRIVATE KEY und -----END RSA PRIVATE KEY.
- 9 Klicken Sie auf **Speichern**.

## Beispiel: Beispiele für Zertifikate

### Zertifikatskette – Beispiel

-----ZERTIFIKATANFANG-----

jIQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+

...

...

...

W53+O05j5xsxzDJfWr1lqBiff/OkiYCPcyK1

-----ZERTIFIKATENDE-----

-----ZERTIFIKATANFANG-----

WdR9Vpg3WQT5+C3HU17bUOwvhp/rjIQvt90+

...

...

...

O05j5xsxzDJfWr1lqBiff/OkiYCPW53+cyK1

-----ZERTIFIKATENDE-----

-----ZERTIFIKATANFANG-----

dR9Vpg3WQTjIQvt9W5+C3HU17bUOwvhp/r0+

...

...

...

5j5xsxzDJfWr1lqW53+O0Biff/OkiYCPcyK1

-----ZERTIFIKATENDE-----

**Beispiel für einen privaten Schlüssel**

-----BEGIN RSA PRIVATE KEY-----

jIQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+

...

...

...

1lqBIFFW53+O05j5xsxzDJfWr/OklYCPcyK1

-----END RSA PRIVATE KEY-----

## Erstellen eines Arbeitsbereichs-Identitätsanbieter

Sie müssen einen Arbeitsbereichs-Identitätsanbieter für die Verwendung mit einem externen Konnektor erstellen.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Identitätsanbieter** aus.
- 2 Wählen Sie **Identitätsanbieter hinzufügen** aus.
- 3 Wählen Sie im angezeigten Menü **Arbeitsbereichs-IDP erstellen** aus.
- 4 Geben Sie im Feld **Name des Identitätsanbieters** einen Namen für den Identitätsanbieter ein.
- 5 Wählen Sie das Verzeichnis aus, das den Benutzern entspricht, die diesen Identitätsanbieter verwenden.

Mit dem ausgewählten Verzeichnis wird festgelegt, welche Konnektoren für die Auswahl mit diesem Identitätsanbieter angezeigt werden.

- 6 Wählen Sie den externen Konnektor oder die externen Konnektoren aus, den bzw. die Sie für die Smartcard-Authentifizierung konfiguriert haben.

**Hinweis** Wenn sich die Bereitstellung hinter einem Lastausgleichsdienst befindet, geben Sie die URL des Lastausgleichsdiensts ein.

- 7 Wählen Sie das Netzwerk für den Zugriff auf diesen Identitätsanbieter aus.
- 8 Klicken Sie auf **Hinzufügen**.

## Konfigurieren der Zertifikatauthentifizierung und Konfigurieren der Regeln für Standardzugriffsrichtlinien

Sie müssen den externen Konnektor für die Verwendung mit Active Directory und der Domäne von vRealize Automation konfigurieren.

## Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

## Vorgehensweise

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Konnektoren** aus.
- 2 Wählen Sie den gewünschten Konnektor in der Spalte **Worker** aus.  
Der ausgewählte Worker wird im Textfeld **Worker-Name** unter der Registerkarte **Detail** des Konnektors angezeigt. Informationen zum Konnektortyp werden im Textfeld **Konnektortyp** angezeigt.
- 3 Stellen Sie sicher, dass mit diesem Konnektor eine Verknüpfung zum gewünschten Active Directory hergestellt werden kann, indem dieses Verzeichnis im Textfeld **Zugehöriges Verzeichnis** angegeben wird.
- 4 Geben Sie den entsprechenden Domänennamen in das Textfeld **Zugehörige Domänen** ein.
- 5 Wählen Sie die Registerkarte **AuthAdapters** aus und aktivieren Sie „CertificateAuthAdapter“.
- 6 Konfigurieren Sie die Zertifikatauthentifizierung entsprechend der Bereitstellung.  
Siehe [Konfigurieren der Zertifikatauthentifizierung für die Verzeichnisverwaltung](#).
- 7 Wählen Sie **Administration > Verzeichnisverwaltung > Richtlinien** aus.
- 8 Klicken Sie auf **Standardrichtlinie bearbeiten**.
- 9 Fügen Sie das Zertifikat zu den Richtlinienregeln hinzu und bestimmen Sie es zur ersten Authentifizierungsmethode.  
Das Zertifikat muss die erste in der Richtlinienregel aufgeführte Authentifizierungsmethode sein, andernfalls schlägt die Zertifikatauthentifizierung fehl.

## Erstellen eines Links für Active Directory mit mehreren Domänen oder mit mehreren Gesamtstrukturen

Als Systemadministrator müssen Sie einen Link für Active Directory mit mehreren Domänen oder mit mehreren Gesamtstrukturen konfigurieren.

Der Vorgang für die Konfiguration eines Links für Active Directory mit mehreren Domänen oder mit mehreren Gesamtstrukturen ist grundsätzlich der gleiche. Bei einem Link mit mehreren Gesamtstrukturen ist eine bidirektionale Vertrauensstellung zwischen allen zutreffenden Domänen erforderlich.

## Voraussetzungen

- Installieren Sie eine verteilte vRealize Automation-Bereitstellung mit den entsprechenden Lastausgleichsdiensten. Siehe *Installieren von vRealize Automation 7.1*.
- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.
- Konfigurieren Sie die entsprechenden Domänen und Active Directory-Gesamtstrukturen für Ihre Bereitstellung.



## Vorgehensweise

- 1 Wählen Sie **Administration > Verwaltung der Verzeichnisse > Verzeichnisse** aus.
- 2 Klicken Sie auf **Verzeichnis hinzufügen**.
- 3 Geben Sie auf der Seite „Verzeichnis hinzufügen“ im Textfeld **Verzeichnisname** einen Namen für den Active Directory-Server an.
- 4 Wählen Sie **Active Directory (Integrierte Windows-Authentifizierung)** unter der Überschrift **Verzeichnisname** aus.
- 5 Konfigurieren Sie den Connector, der Benutzer aus dem Active Directory mit dem VMware Directories Management-Verzeichnis im Abschnitt „Verzeichnissynchronisierung und Authentifizierung“ synchronisiert.

Option	Beschreibung
<b>Synchronisierungs-Connector</b>	Wählen Sie den gewünschten Connector aus, der für Ihr System verwendet werden soll. Jede vRealize Automation-Appliance enthält einen Standard-Connector. Wenden Sie sich an Ihren Systemadministrator, falls Sie Hilfe bei der Auswahl des geeigneten Connectors benötigen.
<b>Authentifizierung</b>	Klicken Sie auf das entsprechende Optionsfeld, um anzugeben, ob der ausgewählte Connector auch Authentifizierung durchführt.
<b>Verzeichnissuchattribut</b>	Geben Sie das gewünschte Kontoattribut ein, das den Benutzernamen enthält.

Abhängig von der Bereitstellungsconfiguration steht Ihnen mindestens ein Connector für die Verwendung zur Verfügung.

- 6 Geben Sie die entsprechenden Anmeldedaten für den Beitritt zur Domäne in die Textfelder **Domänenname**, **Benutzername des Domänenadministrators** und **Kennwort des Domänenadministrators** ein.

Geben Sie beispielsweise Informationen ähnlich der folgenden ein: **Domänenname**:

hs.trcint.com, **Benutzername des Domänenadministrators**: devadmin, **Kennwort des Domänenadministrators**: xxxx.

- 7 Geben Sie im Abschnitt **Bind-Benutzerdetails** die entsprechenden Anmeldeinformationen für Active Directory (Integrierte Windows-Authentifizierung) ein, um die Verzeichnissynchronisierung zu erleichtern.

Option	Beschreibung
<b>Bind-Benutzer-UPN</b>	Geben Sie den User Principal Name (Benutzername des Prinzipals) des Benutzers ein, der die Domäne authentifizieren kann. Beispiel: Benutzername@example.com.
<b>Bind-DN-Kennwort</b>	Geben Sie das Bind-Benutzerkennwort ein.

- 8 Klicken Sie auf **Speichern und weiter**.

Die Seite „Domänen auswählen“ mit der Liste der Domänen wird angezeigt.


- 9 Klicken Sie auf die entsprechenden Kontrollkästchen, um die gewünschten Domänen für die Systembereitstellung auszuwählen.

10 Klicken Sie auf **Weiter**.

11 Stellen Sie sicher, dass die Attributnamen des Directories Management-Verzeichnisses den richtigen Active Directory-Attributen zugeordnet sind.

Wenn die Verzeichnisattributnamen nicht ordnungsgemäß zugeordnet wurden, wählen Sie das richtige Active Directory-Attribut aus dem Dropdown-Menü aus.

12 Klicken Sie auf **Weiter**.

13 Klicken Sie auf , um die Gruppen auszuwählen, die aus Active Directory mit dem Verzeichnis synchronisiert werden sollen.


Enthält eine aus Active Directory hinzugefügte Gruppe Mitglieder, die nicht in der Benutzerliste enthalten sind, werden sie hinzugefügt.


---

**Hinweis** Das Directories Management-Benutzerauthentifizierungssystem importiert beim Hinzufügen von Gruppen und Benutzern Daten aus Active Directory, und die Geschwindigkeit des Systems wird durch Active Directory-Funktionen eingeschränkt. Je nach Anzahl der hinzuzufügenden Gruppen und Benutzer können Importvorgänge daher eventuell viel Zeit in Anspruch nehmen. Beschränken Sie, um diesen eventuell auftretenden Verzögerungen oder Problemen entgegenzuwirken, die Anzahl der Gruppen und Benutzer auf jene, die für den Betrieb von vRealize Automation erforderlich sind. Falls sich Ihre Systemleistung verringert oder Fehler auftreten, schließen Sie alle nicht benötigten Anwendungen und stellen Sie sicher, dass Ihr System Active Directory die erforderliche Arbeitsspeicherzuteilung zugeteilt hat. Wenn das Problem weiterhin besteht, erhöhen Sie die Arbeitsspeicherzuteilung für Active Directory nach Bedarf. Bei Systemen mit einer großen Anzahl von Benutzern und Gruppen muss möglicherweise die Arbeitsspeicherzuteilung für Active Directory auf bis zu 24 GB erhöht werden.

---

14 Klicken Sie auf **Weiter**.

15 Klicken Sie auf , um weitere Benutzer hinzuzufügen. Geben Sie diese beispielsweise im Format **CN=Benutzername,CN=Benutzer,OU=MeineEinheit,DC=MeineFirma,DC=com** ein.

Klicken Sie zum Ausschließen von Benutzern auf , um einen Filter zum Ausschluss bestimmter Benutzertypen zu erstellen. Dazu wählen Sie das Benutzerattribut für den Filter, die Abfragerregel und den Wert aus.

16 Klicken Sie auf **Weiter**.

17 Überprüfen Sie die Seite, um sehen, wie viele Benutzer und Gruppen mit dem Verzeichnis synchronisiert werden.

Wenn Sie die Zusammenstellung der Benutzer und Gruppen ändern möchten, klicken Sie auf die Optionen zum Bearbeiten.

18 Um die Synchronisierung mit dem Verzeichnis zu starten, klicken Sie auf **An Workspace weitergeben**.

**Weiter**

## Konfigurieren von Gruppen und Benutzerrollen

Mandantenadministratoren erstellen Business-Gruppen und benutzerdefinierte Gruppen und erteilen Benutzern Zugriffsrechte auf die vRealize Automation-Konsole.

### Zuweisen von Rollen zu Directory-Benutzern oder -Gruppen Rollen zuweisen

Mandantenadministratoren erteilen Benutzern Zugriffsrechte, indem sie Benutzern oder Gruppen Rollen zuweisen.

#### Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

#### Vorgehensweise

- 1 Wählen Sie **Administration > Benutzer & Gruppen > Benutzer und Gruppen von Verzeichnissen** aus.
- 2 Geben Sie in das Feld **Suchen** einen Benutzer- oder Gruppennamen ein und drücken Sie die Eingabetaste.  
  
Verwenden Sie für den Namen kein At -Zeichen (@), keinen umgekehrten Schrägstrich (\) und keinen Schrägstrich (/). Die Suche können Sie optimieren, indem Sie den gesamten Benutzer- oder Gruppennamen im Format Benutzer@Domäne eingeben.
- 3 Klicken Sie auf den Namen des Benutzers bzw. der Gruppe, dem bzw. der Sie Rollen zuweisen möchten.
- 4 Wählen Sie mindestens eine Rolle aus der Liste „Diesem Benutzer Rollen hinzufügen“ aus.  
  
Auf der Liste „Durch ausgewählte Rollen erteilte Berechtigungen“ werden die spezifischen erteilten Berechtigungen angegeben.
- 5 (Optional) Klicken Sie auf **Weiter**, um weitere Informationen zu dem Benutzer oder zu der Gruppe anzuzeigen.
- 6 Klicken Sie auf **Aktualisieren**.

Benutzer, die aktuell an der vRealize Automation-Konsole angemeldet sind, müssen sich abmelden und wieder an der vRealize Automation-Konsole anmelden, bevor sie auf die Seiten navigieren können, auf die ihnen Zugriff gewährt wurde.

#### Weiter

Optional können Sie eigene benutzerdefinierte Gruppen anhand von Benutzern und Gruppen in Ihren Active Directory-Verbindungen erstellen. Siehe [Erstellen einer benutzerdefinierten Gruppe](#).

## Erstellen einer benutzerdefinierten Gruppe

Mandantenadministratoren können benutzerdefinierte Gruppen erstellen, indem sie andere benutzerdefinierte Gruppen, Identitätsquellengruppen und einzelne Identitätsquellenbenutzer zusammenfassen.

Sie können Ihrer benutzerdefinierten Gruppe Rollen zuweisen, aber dies ist nicht immer erforderlich. Beispielsweise können Sie die benutzerdefinierte Gruppe „Genehmiger für Maschinenspezifikationen“ erstellen, die für alle Vorabgenehmigungen für Maschinen verwendet werden soll. Darüber hinaus können Sie benutzerdefinierte Gruppen für die Zuordnung zu Ihren Business-Gruppen erstellen, damit Sie alle Gruppen zentral verwalten können. In diesen Fällen müssen Sie keine Rollen zuweisen.

### Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Benutzer & Gruppen > Benutzerdefinierte Gruppen** aus.
- 2 Klicken Sie auf das Symbol **Hinzufügen** (+).
- 3 Geben Sie in das Textfeld **Neuer Gruppenname** einen Gruppennamen ein.  
Für benutzerdefinierte Gruppennamen ist die Kombination aus einem Semikolon (;) gefolgt von einem Gleichheitszeichen (=) nicht zulässig.
- 4 (Optional) Geben Sie in das Textfeld **Neue Gruppenbeschreibung** eine Beschreibung ein.
- 5 Wählen Sie mindestens eine Rolle aus der Liste „Dieser Gruppe Rollen hinzufügen“ aus.  
Auf der Liste „Durch ausgewählte Rollen erteilte Berechtigungen“ werden die spezifischen erteilten Berechtigungen angegeben.
- 6 Klicken Sie auf **Weiter**.
- 7 Fügen Sie Benutzer und Gruppen hinzu, um Ihre benutzerdefinierte Gruppe zu erstellen.
  - a Geben Sie in das Feld **Suchen** einen Benutzer- oder Gruppennamen ein und drücken Sie die Eingabetaste.  
Verwenden Sie für den Namen kein At-Zeichen (@), keinen umgekehrten Schrägstrich (\) und keinen Schrägstrich (/). Die Suche können Sie optimieren, indem Sie den gesamten Benutzer- oder Gruppennamen im Format Benutzer@Domäne eingeben.
  - b Wählen Sie den Benutzer oder die Gruppe aus, der bzw. die Ihrer benutzerdefinierten Gruppe hinzugefügt werden soll.
- 8 Klicken Sie auf **Hinzufügen**.

Benutzer, die aktuell an der vRealize Automation-Konsole angemeldet sind, müssen sich abmelden und wieder an der vRealize Automation-Konsole anmelden, bevor sie auf die Seiten navigieren können, auf die ihnen Zugriff gewährt wurde.

## Erstellen einer Business-Gruppe

Mit Business-Gruppen wird ein Satz von Diensten und Ressourcen einer Gruppe von Benutzern zugeordnet, die oft einem Geschäftsbereich, einer Abteilung oder einer sonstigen Organisationseinheit entspricht. Eine Business-Gruppe wird erstellt, um Reservierungen zu konfigurieren und Benutzer dazu zu berechtigen, Servicekatalogelemente für die Mitglieder der Business-Gruppe bereitzustellen.

Um einer Business-Gruppen-Rolle mehrere Benutzer hinzuzufügen, können Sie mehrere einzelne Benutzer hinzufügen. Sie können aber auch mehrere Benutzer gleichzeitig hinzufügen, indem Sie eine Identitätsquellengruppe oder eine benutzerdefinierte Gruppe zu einer Rolle hinzufügen. Beispielsweise können Sie die benutzerdefinierte Gruppe „Vertriebs-Support-Team“ erstellen und diese Gruppe zur Supportrolle hinzufügen. Sie können auch vorhandene Identitätsquellenbenutzergruppen verwenden. Die Benutzer und Gruppen, die Sie auswählen, müssen in der Identitätsquelle gültig sein.

Um die vCloud Director-Integration zu unterstützen, müssen dieselben Mitglieder der vRealize Automation-Business-Gruppe auch Mitglieder der vCloud Director-Organisation sein.

Nachdem ein Mandantenadministrator die Business-Gruppe erstellt, hat der Business-Gruppenmanager die Berechtigung, die Manager-E-Mail-Adresse und die Mitglieder zu ändern. Der Mandantenadministrator kann alle Optionen ändern.

Bei diesem Verfahren wird davon ausgegangen, dass IaaS installiert und konfiguriert ist.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.
- Wenn Sie von Mitgliedern der Business-Gruppe erstellte Maschinen einer bestimmten Active Directory-Organisationseinheit hinzufügen möchten, konfigurieren Sie die Active Directory-Richtlinie. Siehe [Erstellen einer Active Directory-Richtlinie](#). Sie können die Richtlinie beim Erstellen der Business-Gruppe anwenden oder zu einem späteren Zeitpunkt hinzufügen.
- Wenn Sie ein Standardmaschinenpräfix angeben möchten, das Maschinennamen für von einem Mitglied der Business-Gruppe bereitgestellte Maschinen vorangestellt wird, fordern Sie bei einem Fabric-Administrator ein Maschinenpräfix an. Siehe [Konfigurieren von Maschinenpräfixen](#). Maschinenpräfixe sind nicht für XaaS-Anforderungen anwendbar.

### Vorgehensweise

- 1 Wählen Sie **Administration > Benutzer und Gruppen > Business-Gruppen** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Konfigurieren Sie die Details zur Business-Gruppe.

Option	Beschreibung
<b>Name</b>	Geben Sie den Namen für die Business-Gruppe ein.
<b>Beschreibung</b>	Geben Sie die Beschreibung ein.

Option	Beschreibung
<b>Manager E-Mails senden an</b>	Geben Sie einen oder mehrere Benutzer- oder Gruppennamen ein. Trennen Sie mehrere Einträge durch Kommas voneinander. Beispielsweise <b>JoeAdmin@mycompany.com,WeiMgr@mycompany.com.</b>
<b>Active Directory-Richtlinie</b>	Wählen Sie die Active Directory-Standardrichtlinie für die Business-Gruppe aus.

4 Fügen Sie benutzerdefinierte Eigenschaften hinzu.

5 Geben Sie einen Benutzernamen oder einen benutzerdefinierten Benutzergruppennamen ein und drücken Sie die Eingabetaste.

Sie können der Business-Gruppe eine oder mehrere Einzelpersonen oder benutzerdefinierte Benutzergruppen hinzufügen. Zu diesem Zeitpunkt müssen Sie keine Benutzer angeben. Sie können leere Business-Gruppen erstellen und diese später auffüllen.

Option	Beschreibung
<b>Gruppenmanagerrolle</b>	Kann für die Gruppe Berechtigungen erstellen und Genehmigungsrichtlinien zuweisen.
<b>Supportrolle</b>	Kann Katalogelemente im Namen von anderen Mitgliedern der Business-Gruppe anfordern und verwalten.
<b>Benutzerrolle</b>	Kann Dienstkatalogelemente anfordern, für die sie über eine Berechtigung verfügt.

6 Klicken Sie auf **Weiter**.

7 Konfigurieren Sie die Standard-Infrastrukturoptionen.

Option	Beschreibung
<b>Standardmaschinenpräfix</b>	Auswählen eines vorkonfigurierten Maschinenpräfixes für die Business-Gruppe. Dieses Präfix wird von Maschinen-Blueprints verwendet. Wenn der Blueprint so konfiguriert ist, dass das Standardpräfix verwendet wird, und Sie hier aber kein Standardpräfix angeben, wird für Sie ein Maschinenpräfix auf der Grundlage des Namens der Business-Gruppe erstellt. Es empfiehlt sich jedoch, ein Standardpräfix anzugeben. Sie können Blueprints mit bestimmten Präfixen auch weiter konfigurieren oder Servicekatalogbenutzern erlauben, einen angeforderten Blueprint zu überschreiben. XaaS-Blueprints verwenden keine Standard-Maschinenpräfixe. Wenn Sie hier ein Präfix konfigurieren und einen XaaS-Blueprint für diese Business-Gruppe berechtigen, hat dies keine Auswirkungen auf die Bereitstellung einer XaaS-Maschine.
<b>Active Directory-Container</b>	Eingabe eines Active Directory-Containers. Diese Option ist nur für die WIM-Bereitstellung anwendbar. Andere Bereitstellungsmethoden erfordern zusätzliche Konfiguration, um bereitgestellte Maschinen zu einem AD-Container hinzuzufügen.

8 Klicken Sie auf **Hinzufügen**.

Fabric-Administratoren können Ihrer Business-Gruppe durch Erstellen einer Reservierung Ressourcen zuteilen. Business-Gruppenmanager können Berechtigungen für Mitglieder der Business-Gruppe erstellen.

## Weiter

- Erstellen Sie eine auf dem Ort, an dem die Business-Gruppe Maschinen bereitstellt, basierende Reservierung für Ihre Business-Gruppe. Siehe [Auswählen eines Reservierungsszenarios](#).
- Wenn die Katalogelemente veröffentlicht und die Dienste vorhanden sind, können Sie eine Berechtigung für die Mitglieder der Business-Gruppe erstellen. Siehe [Erteilen der Berechtigung für Dienste, Katalogelemente und Aktionen](#).

## Fehlerbehebung bei fehlenden Daten einer Business-Gruppe

Business-Gruppen oder Daten von Business-Gruppen fehlen.

### Problem

Bei der Suche nach einer bekannten Business-Gruppe ist diese unter **Administration > Benutzer und Gruppen > Business-Gruppen** nicht vorhanden oder die Business-Gruppe interagiert mit Reservierungen oder Berechtigungen nicht erwartungsgemäß.

### Ursache

Informationen zu Business-Gruppen sind in zwei Datenbanken (CAFE und IaaS) vorhanden, und müssen in beiden jeweils identisch sein. Bei Standardvorgängen bleiben die Datenbanken synchronisiert. Wenn dieses Problem auftritt, müssen Sie möglicherweise eine Synchronisierung erzwingen.

Das Problem kann auftreten, wenn die Synchronisierung nach einem Upgrade nicht erwartungsgemäß ausgeführt wird. Es kann ebenso auftreten, wenn Sie die API zum Aktualisieren der IaaS-Datenbank mit einer neuen oder geänderten Business-Gruppe verwenden.

### Lösung

#### Voraussetzungen

Stellen Sie sicher, dass Sie Befehlszeilenbefehle ausführen können. Siehe *Programmierhandbuch*.

#### Vorgehensweise

- ◆ Geben Sie die Befehlszeichenfolge in der Befehlszeile vcac-cli ein.

Was der Befehl aktualisiert	Befehl	Verkürzte Version des Befehls
Synchronisieren der CAFE-Datenbank mit den IaaS-Werten.	<code>Vcac-Config.exe SynchronizeDatabases --DatabaseSyncSource IaaS -v</code>	<code>Vcac-Config.exe SynchronizeDatabases -dss IaaS -v</code>
Synchronisieren der IaaS-Datenbank mit den CAFE-Werten.	<code>Vcac-Config.exe SynchronizeDatabases --DatabaseSyncSource Cafe -v</code>	<code>Vcac-Config.exe SynchronizeDatabases -dss Cafe -v</code>

## Fehlerbehebung bei Leistungsbeeinträchtigungen bei der Anzeige von Gruppenmitgliedern

Mitglieder von Business-Gruppen oder benutzerdefinierten Gruppen werden beim Aufrufen von Gruppendetails nur langsam angezeigt.

### Problem

Beim Anzeigen von Benutzerinformationen in Umgebungen mit einer großen Anzahl von Benutzern werden die Benutzernamen in der Benutzeroberfläche nur langsam geladen.

### Ursache

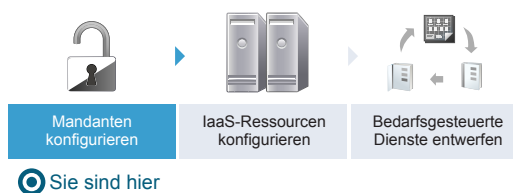
Die Zeitverzögerung beim Laden der Namen tritt in Umgebungen mit einer großen Active Directory-Umgebung auf.

### Lösung

- ◆ Verwenden Sie, soweit möglich, Active Directory-Gruppen oder benutzerdefinierte Gruppen, anstatt die Namen Hunderter einzelner Mitglieder hinzuzufügen, um so die Arbeitslast beim Abrufen zu verringern.

## Szenario: Konfigurieren des Standardmandanten für Rainpole

Als Systemadministrator möchten Sie Ihre vRealize Automation-Instanz als eine fortlaufende Entwicklungsumgebung konfigurieren. Erstellen Sie lokale Benutzerkonten und weisen Sie sich selbst zur Mandantenadministratorrolle zu. Unter Verwendung der Mandantenadministratorrechte beginnen Sie, vRealize Automation als eine Entwicklungsumgebung zum Erstellen und Testen von Blueprints zu konfigurieren.



### Vorgehensweise

#### 1 Szenario: Erstellen von lokalen Benutzerkonten für Rainpole

Mit Ihren standardmäßigen Systemadministratorrechten können Sie zwei lokale Benutzerkonten im Standardmandanten erstellen. Weisen Sie eines dieser Konten der Mandantenadministratorrolle zu, sodass Sie mit der Konfiguration des Standardmandanten beginnen können. Sie können das zweite Konto später als freigegebene Anmeldung verwenden, damit Ihre Architekten den Blueprint- und Katalogzugriff testen können.



## 2 Szenario: Verbinden des Active Directory Ihres Unternehmens mit vRealize Automation für Rainpole

Als Mandantenadministrator möchten Sie, dass vRealize Automation Anmeldungen beim Active Directory Ihres Unternehmens authentifiziert. Sie konfigurieren eine Verbindung zwischen vRealize Automation und Ihrer einzelnen Active Directory-Domäne über LDAP.

## 3 Szenario: Konfigurieren von Branding für den Standardmandanten für Rainpole

Mit Ihren Mandantenadministratorrechten passen Sie das Erscheinungsbild der vRealize Automation-Konsole an. Sie laden ein neues Logo hoch, ändern die Farben, aktualisieren die Kopf- und Fußzeileninformationen und konfigurieren das Branding des Anmeldebildschirms.

## 4 Szenario: Erstellen einer benutzerdefinierten Gruppe für Ihre Rainpole-Architekten

Mit Ihren Mandantenadministratorrechten erstellen Sie eine benutzerdefinierte Gruppe für Mitglieder Ihrer IT-Organisation, die umfangreichen Zugriff auf vRealize Automation benötigen. Beim Konfigurieren von vRealize Automation weisen Sie dieser benutzerdefinierten Gruppe Rollen zu.

## 5 Szenario: Zuweisen von IaaS-Administratorrechten zu Ihrer benutzerdefinierten Gruppe von Rainpole-Architekten

Mit Ihren standardmäßigen Systemadministratorrechten weisen Sie Ihre benutzerdefinierte Gruppe zur IaaS-Administratorrolle zu, damit die Gruppe die IaaS-Ressourcen konfigurieren kann.

# Szenario: Erstellen von lokalen Benutzerkonten für Rainpole

Mit Ihren standardmäßigen Systemadministratorrechten können Sie zwei lokale Benutzerkonten im Standardmandanten erstellen. Weisen Sie eines dieser Konten der Mandantenadministratorrolle zu, sodass Sie mit der Konfiguration des Standardmandanten beginnen können. Sie können das zweite Konto später als freigegebene Anmeldung verwenden, damit Ihre Architekten den Blueprint- und Katalogzugriff testen können.

### Vorgehensweise

- 1 Navigieren Sie zur vRealize Automation-Konsole: **<https://vra01svr01.rainpole.local/vcac>**.
- 2 Geben Sie den standardmäßigen Systemadministrator-Benutzernamen **administrator** und das Kennwort **VMware1!** ein.
- 3 Wählen Sie **Administration > Mandanten** aus.
- 4 Klicken Sie auf **vsphere.local**.
- 5 Wählen Sie die Registerkarte **Lokale Benutzer** aus.
- 6 Klicken Sie auf das Symbol **Neu (+)**.
- 7 Erstellen Sie ein lokales Benutzerkonto, das der Mandantenadministratorrolle zugewiesen wird.

Option	Eingabe
Vorname	Rainpole
Nachname	tenant admin
E-Mail	Geben Sie Ihre E-Mail-Adresse ein oder verwenden Sie den Platzhalter <b>rainpole_tenant_admin@rainpole.com</b> .

Option	Eingabe
Benutzername	Rainpole tenant admin
Kennwort	VMware1!

8 Klicken Sie auf **OK**.

9 Klicken Sie auf das Symbol **Neu** (+).

10 Erstellen Sie ein lokales Benutzerkonto, das Sie und Ihre Architekten später konfigurieren können, um Blueprints und den Katalogzugriff zu testen.

Option	Eingabe
Vorname	test
Nachname	user
E-Mail	Geben Sie eine E-Mail-Adresse ein oder verwenden Sie den Platzhalter <b>test_user@rainpole.com</b> .
Benutzername	test_user
Kennwort	VMware1!

11 Klicken Sie auf **OK**.

12 Klicken Sie auf die Registerkarte **Administratoren**.

13 Geben Sie **Rainpole** in das Suchfeld **Mandantenadministratoren** ein und drücken Sie die Eingabetaste. Wählen Sie Ihren Rainpole-Mandantenadministrator aus.

Die Mandantenadministratorrolle wird Ihrem Rainpole-Mandantenadministrator zugewiesen.

14 Klicken Sie auf **Beenden**.

15 Melden Sie sich von der Konsole ab.

Sie können den lokalen Rainpole-Mandantenadministrator für den Zugriff auf die Mandantenadministratoneinstellungen und zum Konfigurieren des Mandanten verwenden. Das Konto „test\_user“ kann als freigegebene Anmeldung für die Architekten und Katalogadministratoren verwendet werden. Sie können das Konto als Basisbenutzer konfigurieren und den Blueprint- und Katalogzugriff überprüfen sowie das Genehmigungsverhalten testen.

#### Weiter

Konfigurieren Sie vRealize Automation, um Anmeldungen an das vorhandene Active Directory Ihres Unternehmens zu authentifizieren.

## Szenario: Verbinden des Active Directory Ihres Unternehmens mit vRealize Automation für Rainpole

Als Mandantenadministrator möchten Sie, dass vRealize Automation Anmeldungen beim Active Directory Ihres Unternehmens authentifiziert. Sie konfigurieren eine Verbindung zwischen vRealize Automation und Ihrer einzelnen Active Directory-Domäne über LDAP.

## Vorgehensweise

- 1 Navigieren Sie zur vRealize Automation-Konsole: **https://vra01svr01.rainpole.local/vcac**.
- 2 Geben Sie den Benutzernamen **Rainpole-Mandantenadministrator** und das Kennwort **VMware1!** ein.
- 3 Wählen Sie **Administration > Verwaltung der Verzeichnisse > Verzeichnisse** aus.
- 4 Klicken Sie auf **Verzeichnis hinzufügen**.
- 5 Geben Sie die jeweiligen Active Directory-Kontoeinstellungen ein und akzeptieren Sie die Standardoptionen.

Option	Beispieleingabe
<b>Verzeichnisname</b>	Fügen Sie die IP-Adresse des Active Directory-Domänennamens hinzu.
<b>Synchronisierungs-Connector</b>	vra01svr01.rainpole.local
<b>Basis-DN</b>	Geben Sie den definierten Namen (DN, Distinguished Name) des Startpunkts für Verzeichnisserversuchen ein. Beispiel: <b>cn=users,dc=rainpole,dc=local</b> .
<b>Bind-DN</b>	Geben Sie den vollständigen definierten Namen (DN, Distinguished Name), einschließlich des allgemeinen Namens (Common Name, CN), eines Active Directory-Benutzerkontos mit Berechtigungen zum Suchen von Benutzern ein. Beispiel: <b>cn=config_admin_infra,cn=users,dc=rainpole,dc=local</b> .
<b>Bind-DN-Kennwort</b>	Geben Sie das Active Directory-Kennwort für das Konto ein, das nach Benutzern suchen kann.

- 6 Klicken Sie auf die Schaltfläche **Verbindung testen**, um die Verbindung zum konfigurierten Verzeichnis zu testen.
- 7 Klicken Sie auf **Speichern und weiter**.  
Die Seite „Domänen auswählen“ mit der Liste der Domänen wird angezeigt.
- 8 Übernehmen Sie die Einstellung für die Standarddomäne und klicken Sie auf **Weiter**.
- 9 Überprüfen Sie, ob die Attributnamen den richtigen Active Directory-Attributen zugeordnet sind, und klicken Sie auf **Weiter**.
- 10 Wählen Sie die Gruppen und Benutzer aus, die synchronisiert werden sollen.
  - a Klicken Sie auf das Symbol **Hinzufügen (+)**.
  - b Geben Sie die Benutzerdomäne ein und klicken Sie auf **Gruppen suchen**.  
Beispiel: **cn=users,dc=rainpole,dc=local**.
  - c Aktivieren Sie das Kontrollkästchen **Alle auswählen**.
  - d Klicken Sie auf **Auswählen**.
  - e Klicken Sie auf **Weiter**.
  - f Akzeptieren Sie die Standardeinstellungen auf der Seite „Benutzer auswählen“ und klicken Sie auf **Weiter**.

- 11 Überprüfen Sie auf der Seite, wie viele Benutzer und Gruppen mit dem Verzeichnis synchronisiert werden, und klicken Sie auf **Verzeichnis synchronisieren**.

Für die Verzeichnissynchronisierung wird einige Zeit benötigt. Der Prozess wird jedoch im Hintergrund ausgeführt und Sie können Ihre Arbeit fortsetzen.

Sie können allen Active Directory-Benutzern und -Gruppen, die Sie in vRealize Automation synchronisiert haben, Rechte zuweisen und Zugriff erteilen.

#### Weiter

Mit Ihren Mandantenadministratorrechten passen Sie das Erscheinungsbild der vRealize Automation-Konsole an.

## Szenario: Konfigurieren von Branding für den Standardmandanten für Rainpole

Mit Ihren Mandantenadministratorrechten passen Sie das Erscheinungsbild der vRealize Automation-Konsole an. Sie laden ein neues Logo hoch, ändern die Farben, aktualisieren die Kopf- und Fußzeileninformationen und konfigurieren das Branding des Anmeldebildschirms.

#### Vorgehensweise

- 1 Wählen Sie **Administration > Branding > Branding für Kopf- und Fußzeile** aus.
- 2 Deaktivieren Sie das Kontrollkästchen **Standardeinstellungen verwenden**.
- 3 Folgen Sie den Eingabeaufforderungen, um eine Kopfzeile zu erstellen.
- 4 Klicken Sie auf **Weiter**.
- 5 Folgen Sie den Eingabeaufforderungen, um eine Fußzeile zu erstellen.
- 6 Klicken Sie auf **Beenden**.

Die Konsole wird gemäß Ihren Änderungen aktualisiert.

- 7 Wählen Sie **Administration > Branding > Anmeldebildschirm-Branding** aus.
- 8 Folgen Sie den Eingabeaufforderungen, um das Branding des Anmeldebildschirms anzupassen.
- 9 Klicken Sie auf **Speichern**.

Die Konsole wird gemäß Ihren Änderungen aktualisiert.

Sie haben das Erscheinungsbild der Konsole für den Standardmandanten aktualisiert.

#### Weiter

Erstellen Sie eine benutzerdefinierte Gruppe für Mitglieder Ihrer IT-Organisation, die umfänglichen Zugriff auf vRealize Automation benötigen.

## Szenario: Erstellen einer benutzerdefinierten Gruppe für Ihre Rainpole-Architekten

Mit Ihren Mandantenadministratorrechten erstellen Sie eine benutzerdefinierte Gruppe für Mitglieder Ihrer IT-Organisation, die umfangreichen Zugriff auf vRealize Automation benötigen. Beim Konfigurieren von vRealize Automation weisen Sie dieser benutzerdefinierten Gruppe Rollen zu.

Wenn Sie diesen umfangreichen Zugriff für Benutzer hinzufügen oder deaktivieren möchten, können Sie die Mitgliedschaft der Gruppe ändern und müssen nicht die Einstellungen für jeden einzelnen Benutzer an verschiedenen Standorten bearbeiten.

### Vorgehensweise

- 1 Wählen Sie **Administration > Benutzer & Gruppen > Benutzerdefinierte Gruppen** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Geben Sie **Rainpole-Architekten** in das Textfeld **Name** ein.
- 4 Wählen Sie Rollen aus der Liste „Dieser Gruppe Rollen hinzufügen“ aus.

Auf dieser Seite können Sie keine IaaS-Administrator-, Fabric-Administrator-, Business-Gruppen-Manager- oder Business-Benutzer-Rollen zuweisen. Sie weisen die Rollen zu, die Sie bei der Konfiguration von vRealize Automation konfiguriert haben.

Option	Beschreibung
<b>Mandantenadministrator</b>	Verantwortlich für Benutzer- und Gruppenverwaltung, Mandanten-Branding sowie -Benachrichtigungen und Unternehmensrichtlinien wie Genehmigungen und Berechtigungen. Sie verfolgen die Ressourcennutzung aller Benutzer innerhalb des Mandanten nach und initiieren Rückforderungsanfragen für virtuelle Maschinen.
<b>Infrastruktur (IaaS)-Architekt</b>	Erstellen und Verwalten von Maschinen-Blueprints und Anwendungs-Blueprints.
<b>XaaS-Architekt</b>	Erstellen und Verwalten von XaaS-Blueprints für lizenzierte Advanced- und Enterprise-Benutzer.
<b>Softwarearchitekt</b>	Erstellen und verwalten Sie Softwarekomponenten und Anwendungs-Blueprints für lizenzierte Enterprise-Benutzer.

- 5 Klicken Sie auf **Weiter**.
- 6 Suchen Sie nach Benutzern des Active Directory Ihres Unternehmens und wählen Sie Benutzer zum Hinzufügen zu Ihrer benutzerdefinierten Gruppe aus.

Sie weisen sich und alle Benutzer, die einen umfangreichen Zugriff auf Ihre vRealize Automation-Entwicklungsumgebung benötigen, zu dieser Gruppe zu.

- 7 Klicken Sie auf **Beenden**.

Sie haben Ihrer benutzerdefinierten Gruppe Rechte erteilt, um den Standardmandanten zu verwalten, Blueprints zu erstellen und den Servicekatalog zu verwalten. Beim Konfigurieren von vRealize Automation fügen Sie Ihrer benutzerdefinierten Gruppe Berechtigungen und Rollen zu.

## Weiter

Weisen Sie Ihre benutzerdefinierte Gruppe zur IaaS-Administratorrolle zu.

## Szenario: Zuweisen von IaaS-Administratorrechten zu Ihrer benutzerdefinierten Gruppe von Rainpole-Architekten

Mit Ihren standardmäßigen Systemadministratorrechten weisen Sie Ihre benutzerdefinierte Gruppe zur IaaS-Administratorrolle zu, damit die Gruppe die IaaS-Ressourcen konfigurieren kann.

### Vorgehensweise

- 1 Melden Sie sich bei der vRealize Automation-Konsole ab.
- 2 Wählen Sie die Domäne **vsphere.local** aus und klicken Sie auf **Weiter**.
- 3 Geben Sie den standardmäßigen Systemadministrator-Benutzernamen **administrator** und das Kennwort **vmware** ein.
- 4 Wählen Sie **Administration > Mandanten** aus.
- 5 Klicken Sie auf den Namen des Standardmandanten **vsphere.local**.
- 6 Klicken Sie auf die Registerkarte **Administratoren**.
- 7 Geben Sie **Rainpole-Architekten** im Suchfeld **IaaS-Administratoren** ein und wählen Sie Ihre benutzerdefinierte Gruppe aus.
- 8 Klicken Sie auf **Beenden**.
- 9 Melden Sie sich von der Konsole ab.

Alle Mitglieder Ihrer benutzerdefinierten Gruppe können jetzt die Cloud-, virtuelle, Netzwerk- und Speicherinfrastruktur für alle Mandanten in Ihrer vRealize Automation-Instanz verwalten. Sie können Gruppenmitgliedschaften jederzeit aktualisieren, um diese Rechte zu erteilen oder zu widerrufen.

## Weiter

Mit den IaaS-Administratorrechten, die Sie Ihrer benutzerdefinierten Gruppe erteilt haben, können Sie Ihre IaaS-Ressourcen konfigurieren.

## Erstellen weiterer Mandanten

Als Systemadministrator können Sie weitere vRealize Automation-Mandanten erstellen, sodass Benutzer auf die entsprechenden Anwendungen und Ressourcen zugreifen können, die Sie zur Durchführung Ihrer Arbeitszuweisungen benötigen.

Bei einem Mandanten handelt es sich um eine Gruppe von Benutzern mit bestimmten Berechtigungen, die innerhalb einer Softwareinstanz arbeiten. In der Regel wird ein standardmäßiger vRealize Automation-Mandant bei der Systeminstallation und der Erstkonfiguration erstellt. Danach können Administratoren weitere Mandanten erstellen, sodass sich Benutzer anmelden und ihre Arbeitszuweisungen durchführen können. Administratoren können so viele Mandanten erstellen, wie für den Betrieb des Systems erforderlich sind. Beim Erstellen von Mandanten müssen Administratoren die Basiskonfigu-

ration durchführen und Elemente wie Name, Anmelde-URL, lokale Benutzer und Administratoren angeben. Nach der Konfiguration der Basisinformationen für den Mandanten muss sich der Mandantenadministrator anmelden und mithilfe der Verzeichnisverwaltungsfunktion auf der Verwaltungsregisterkarte der vRealize Automation-Konsole eine entsprechende Active Directory-Verbindung einrichten. Darüber hinaus können Mandantenadministratoren benutzerdefiniertes Branding auf Mandanten anwenden.

### Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Systemadministrator** an.

### Vorgehensweise

#### 1 Angeben von Mandanteninformationen

Der erste Schritt bei der Konfiguration eines Mandanten ist es, den neuen Mandanten zu benennen, ihn zu vRealize Automation hinzuzufügen und eine mandantenspezifische Zugriffs-URL zu erstellen.

#### 2 Konfigurieren von lokalen Benutzern

Der vRealize Automation-Systemadministrator muss die lokalen Benutzer für jeden anwendbaren Mandanten konfigurieren.

#### 3 Ernennen von Administratoren

Sie können über die für einen Mandanten konfigurierten Identitätsspeicher einen oder mehrere Mandantenadministratoren und IaaS-Administratoren bestimmen.

## Angeben von Mandanteninformationen

Der erste Schritt bei der Konfiguration eines Mandanten ist es, den neuen Mandanten zu benennen, ihn zu vRealize Automation hinzuzufügen und eine mandantenspezifische Zugriffs-URL zu erstellen.

### Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Systemadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Mandanten** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Geben Sie im Textfeld **Name** einen Namen ein.
- 4 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.

- 5 Geben Sie in das Textfeld **URL-Name** einen eindeutigen Bezeichner für den Mandanten ein.

Mithilfe dieses URL-Tokens wird ein mandantenspezifischer Bezeichner an die vRealize Automation-Konsolen-URL angefügt.

Geben Sie beispielsweise **meinMandant** ein, um die URL `https://vrealize-appliance-hostname.domain.name/vcac/org/meinMandant` zu erstellen.

---

**Hinweis** Für die Mandanten-URL dürfen in vRealize Automation 7.0 und 7.1 nur Kleinbuchstaben verwendet werden.

---

- 6 (Optional) Geben Sie in das Textfeld **E-Mail des Kontakts** eine E-Mail-Adresse ein.

- 7 Klicken Sie auf **Erstellen und Weiter**.

## Konfigurieren von lokalen Benutzern

Der vRealize Automation-Systemadministrator muss die lokalen Benutzer für jeden anwendbaren Mandanten konfigurieren.

Nachdem ein Administrator die allgemeinen Informationen für einen Mandanten erstellt, wird die Registerkarte „Lokale Benutzer“ aktiviert, und der Administrator kann Benutzer festlegen, die auf den Mandanten zugreifen können. Nach Abschluss der Mandantenkonfiguration können lokale Mandantenbenutzer sich bei ihren entsprechenden Mandanten anmelden, um Arbeitsaufträge abzuschließen.

---

**Hinweis** Nachdem Sie einen Benutzer hinzugefügt haben, können Sie seine Konfiguration nicht mehr ändern. Wenn Sie Änderungen an der Benutzerkonfiguration vornehmen müssen, müssen Sie den Benutzer löschen und neu erstellen.

---

### Vorgehensweise

- 1 Klicken Sie auf der Registerkarte „Lokale Benutzer“ auf **Hinzufügen**.
- 2 Geben Sie im Dialogfeld „Benutzerdetails“ den Vor- bzw. Nachnamen des Benutzers in die Felder **Vorname** und **Nachname** ein.
- 3 Geben Sie die E-Mail-Adresse des Benutzers in das Feld **E-Mail** ein.
- 4 Geben Sie die Benutzer-ID und das Kennwort des Benutzers in die Felder **Benutzername** und **Kennwort** ein.
- 5 Klicken Sie auf die Schaltfläche **Hinzufügen**.
- 6 Wiederholen Sie diese Schritte gegebenenfalls für alle lokalen Benutzer des Mandanten.

Die für den Mandanten angegebenen lokalen Benutzer werden erstellt.

## Ernennen von Administratoren

Sie können über die für einen Mandanten konfigurierten Identitätsspeicher einen oder mehrere Mandantenadministratoren und IaaS-Administratoren bestimmen.



Mandantenadministratoren sind für die Konfiguration von mandantenspezifischem Branding sowie für das Verwalten von Identitätsspeichern, Benutzern, Gruppen, Berechtigungen und freigegebenen Blueprints innerhalb des Kontexts ihres Mandanten zuständig. IaaS-Administratoren sind für die Konfiguration von Infrastrukturquellen-Endpoints in IaaS, die Bestimmung von Fabric-Administratoren und die Überwachung von IaaS-Protokollen zuständig.

### Voraussetzungen

- Bevor Sie IaaS-Administratoren bestimmen, müssen Sie IaaS installieren. Weitere Informationen zum Installieren von IaaS finden Sie unter *Installieren von vRealize Automation 7.1*.

### Vorgehensweise

- 1 Geben Sie in das Suchfeld **Mandantenadministratoren** den Namen eines Benutzers oder einer Gruppe ein und drücken Sie die Eingabetaste.

Um schneller Ergebnisse zu erhalten, geben Sie den gesamten Benutzer- oder Gruppennamen ein, wie beispielsweise myAdmins@mycompany.domain. Wiederholen Sie diesen Schritt, um zusätzliche Mandantenadministratoren zu ernennen.

- 2 Falls Sie IaaS installiert haben, geben Sie in das Suchfeld **IaaS-Administratoren** den Namen eines Benutzers oder einer Gruppe ein und drücken Sie die Eingabetaste.

Um schneller Ergebnisse zu erhalten, geben Sie den gesamten Benutzer- oder Gruppennamen ein, wie beispielsweise IaaSAdmins@mycompany.domain. Wiederholen Sie diesen Schritt, um zusätzliche Infrastrukturadministratoren zu ernennen.

- 3 Klicken Sie auf **Hinzufügen**.

## Löschen eines Mandanten

Ein Systemadministrator kann alle unerwünschten Mandanten aus vRealize Automation löschen.

Wenn Sie einen Mandanten löschen, wird dieser umgehend aus der vRealize Automation-Schnittstelle entfernt. Es kann jedoch mehrere Stunden dauern, bis der Mandant vollständig aus Ihrer Bereitstellung entfernt wurde. Wenn Sie einen Mandanten löschen und einen anderen Mandanten mit derselben URL erstellen möchten, warten Sie einige Stunden, bis der Löschvorgang vollständig abgeschlossen ist, bevor Sie den neuen Mandanten erstellen.

### Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Systemadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Mandanten** aus.
- 2 Wählen Sie den Mandanten aus, den Sie löschen möchten.

Klicken Sie nicht auf den eigentlichen Namen, um den Mandanten auszuwählen. Wenn Sie dies tun, wird der Mandant zur Bearbeitung geöffnet.

- 3 Klicken Sie auf **Löschen**.

Der Mandant wird aus Ihrer vRealize Automation-Bereitstellung gelöscht.

## (Optional) Konfigurieren des benutzerdefinierten Brandings

vRealize Automation ermöglicht Ihnen die Anwendung des benutzerdefinierten Brandings auf die Anmelde- und Anwendungsseiten von Mandanten.

Das benutzerdefinierte Branding kann Text- und Hintergrundfarben, Geschäftslogos, Unternehmensnamen, Datenschutzrichtlinien, Informationen zum Copyright und weitere relevante Informationen umfassen, die Sie auf Anmelde- oder Anwendungsseiten von Mandanten anzeigen möchten.

### Benutzerdefiniertes Branding für die Anmeldeseite des Mandanten

Verwenden Sie die Seite „Anmeldebildschirm-Branding“, um benutzerdefiniertes Branding auf den Anmeldeseiten des vRealize Automation-Mandanten anzuwenden.

Sie können benutzerdefiniertes vRealize Automation-Branding auf den Anmeldeseiten von Mandanten verwenden oder Sie können benutzerdefiniertes Branding über die Seite „Anmeldebildschirm-Branding“ konfigurieren. Beachten Sie, dass das benutzerdefinierte Branding für all Ihre Mandantenanwendungen in der gleichen Weise gilt.

Über diese Seite können Sie Branding auf allen Anmeldeseiten von Mandanten konfigurieren.

Auf der Seite „Anmeldebildschirm-Branding“ wird das derzeit bei der Mandantenanmeldung implementierte Branding im Bereich „Vorschau“ angezeigt.

---

**Hinweis** Nach dem Speichern des neuen Brandings auf den Anmeldeseiten von Mandanten kann es zu einer Verzögerung von bis zu fünf Minuten kommen, bevor das Branding auf allen Anmeldeseiten sichtbar ist.

---

#### Voraussetzungen

Um ein benutzerdefiniertes Logo oder ein anderes Bild mit Ihrem Branding zu verwenden, müssen die entsprechenden Dateien verfügbar sein.

#### Vorgehensweise

- 1 Melden Sie sich als System- oder Mandantenadministrator bei vRealize Automation an.
- 2 Klicken Sie auf die Registerkarte **Administration**.
- 3 Wählen Sie mithilfe der Kontrollkästchen unter der Überschrift „Effekte“ die gewünschten visuellen Effekte aus.  
Alle Effekte sind optional.
- 4 Wählen Sie **Branding > Anmeldebildschirm-Branding** aus.

- 5 Klicken Sie unter dem Feld „Logo“ auf **Hochladen**. Navigieren Sie anschließend zum entsprechenden Ordner und wählen Sie eine Logo-Bilddatei aus.
- 6 Klicken Sie, falls gewünscht, unter dem Feld „Bild (optional)“ auf **Hochladen**. Navigieren Sie anschließend zum entsprechenden Ordner und wählen Sie eine zusätzliche Logo-Bilddatei aus.
- 7 Geben Sie, falls gewünscht, die entsprechenden Hexadezimalcodes in die Felder **Hintergrundfarbe**, **Farbe des Mastertitels**, **Hintergrundfarbe der Anmeldeschaltfläche** und **Vordergrundfarbe der Anmeldeschaltfläche** ein.

Suchen Sie bei Bedarf im Internet nach einer Liste mit den Farbcodes im Hexadezimalformat.

- 8 Klicken Sie auf **Speichern**, um Ihre Einstellungen zu übernehmen.

Bei Mandantenbenutzern wird das benutzerdefinierte Branding auf deren Anmeldeseiten angezeigt.

## Benutzerdefiniertes Branding für Mandantenanwendungen

Verwenden Sie die Seite „Anwendungs-Branding“, um benutzerdefiniertes Branding auf vRealize Automation-Mandantenanwendungen anzuwenden.

Sie können benutzerdefiniertes vRealize Automation-Branding auf Ihren Benutzeranwendungen verwenden oder Sie können benutzerdefiniertes Branding über die Seite „Anwendungs-Branding“ konfigurieren. Über diese Seite können Sie das Branding in der Kopf- und Fußzeile von Anwendungsseiten konfigurieren. Beachten Sie, dass das benutzerdefinierte Branding für all Ihre Benutzeranwendungen in der gleichen Weise gilt.

Auf der Seite „Anwendungs-Branding“ wird das derzeit implementierte Branding in Kopf- und Fußzeile im unteren Bereich der Seite angezeigt.

### Voraussetzungen

Wenn Sie ein benutzerdefiniertes Logo mit Ihrem Branding verwenden möchten, muss die Logo-Bilddatei verfügbar sein.

### Vorgehensweise

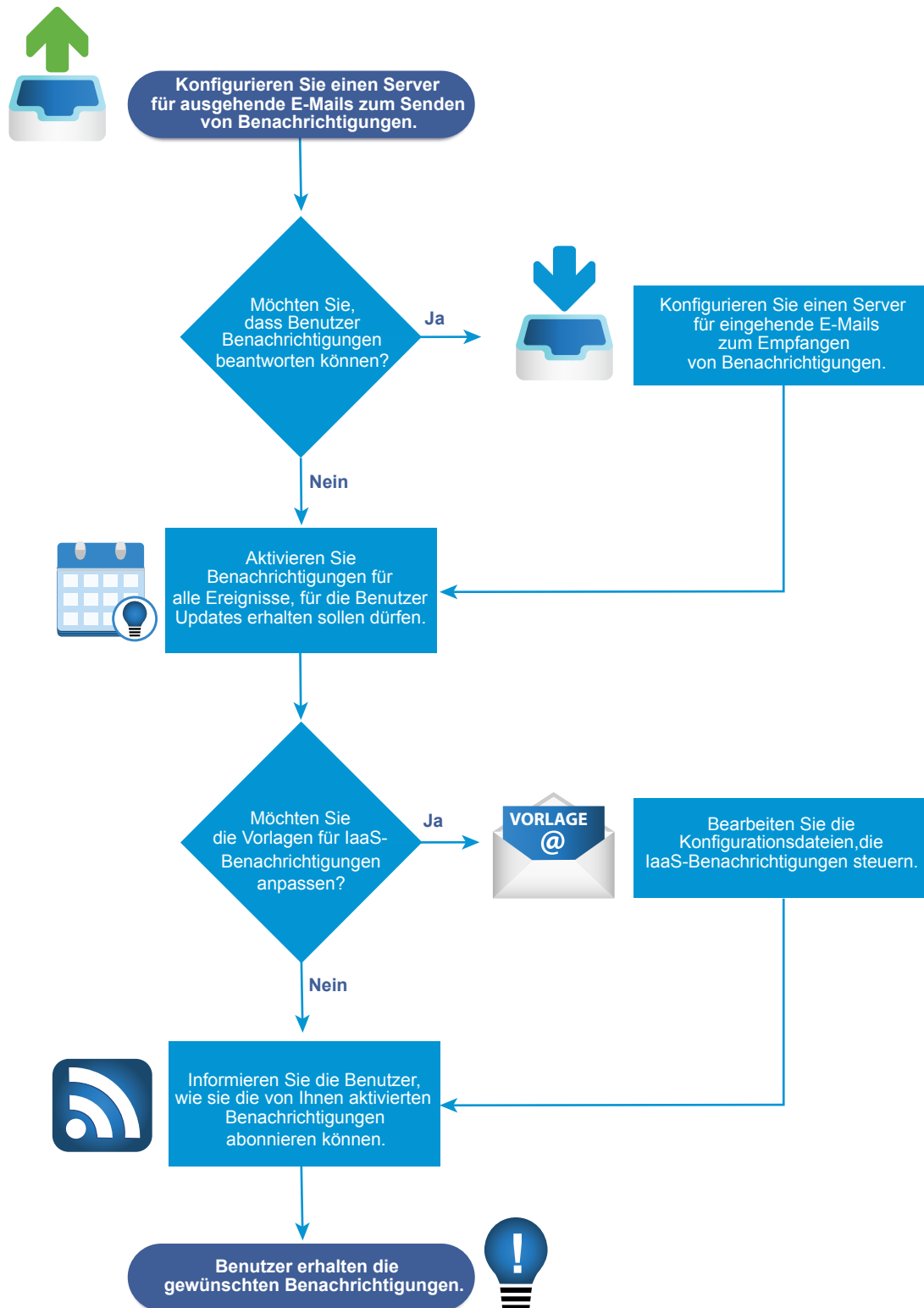
- 1 Melden Sie sich als System- oder Mandantenadministrator bei vRealize Automation an.
- 2 Klicken Sie auf die Registerkarte **Administration**.
- 3 Wählen Sie **Branding > Anwendungs-Branding** aus.
- 4 Klicken Sie auf die Registerkarte **Kopfzeile**, sofern diese noch nicht aktiv ist.
- 5 Wenn Sie das vRealize Automation-Standard-Branding verwenden möchten, aktivieren Sie das Kontrollkästchen **Standardeinstellungen verwenden**.

- 6 Nehmen Sie in den Feldern auf den Registerkarten **Kopfzeile** und **Fußzeile** die entsprechende Auswahl vor, um das benutzerdefinierte Branding zu implementieren.
  - a Klicken Sie im Feld **Kopfzeilenlogo** auf die Schaltfläche **Durchsuchen**. Navigieren Sie anschließend zum entsprechenden Ordner und wählen Sie eine Logo-Bilddatei aus.
  - b Geben Sie im Feld **Name des Unternehmens** den entsprechenden Unternehmensnamen ein.  
Der angegebene Name wird angezeigt, wenn ein Benutzer den Mauszeiger über das Logo bewegt.
  - c Geben Sie im Feld **Produktname** den entsprechenden Namen ein.  
Der hier eingegebene Name wird in der Kopfzeile der Anwendung neben dem Logo angezeigt.
  - d Geben Sie im Feld **Hintergrundfarbe im Hexadezimalformat** den entsprechenden Farbcode für die Hintergrundfarbe im Umkreis der Anwendung im Hexadezimalformat ein.  
Suchen Sie bei Bedarf im Internet nach einer Liste mit den Farbcodes im Hexadezimalformat.
  - e Geben Sie im Feld **Textfarbe im Hexadezimalformat** den entsprechenden Hexadezimalcode für die Textfarbe ein.  
Suchen Sie bei Bedarf im Internet nach einer Liste mit den Textfarbcodes im Hexadezimalformat.
  - f Klicken Sie auf **Weiter**, um die Registerkarte „Fußzeile“ zu aktivieren.
  - g Geben Sie im Feld **Copyright-Hinweis** die gewünschte Erklärung ein.
  - h Geben Sie im Feld **Link zu den Datenschutzrichtlinien** den Link zur Datenschutzerklärung Ihres Unternehmens ein.
  - i Geben Sie im Feld **Link zu Kontaktdaten** die gewünschten Kontaktinformationen des Unternehmens ein.
- 7 Klicken Sie auf **Aktualisieren**, um Ihre Konfiguration des Brandings zu implementieren.

Bei Mandantenbenutzern wird das benutzerdefinierte Branding auf deren Anwendungsseiten angezeigt.

## (Optional) Checkliste für die Konfiguration von Benachrichtigungen

Sie können vRealize Automation so konfigurieren, dass Benachrichtigungen an Benutzer gesendet werden, wenn bestimmte Ereignisse auftreten. Benutzer können wählen, welche Benachrichtigungen sie abonnieren möchten, aber sie können nur aus Ereignissen auswählen, die Sie als Benachrichtigungsauslöser aktiviert haben.



Die Checkliste für die Konfiguration von Benachrichtigungen bietet einen groben Überblick über die Abfolge der Schritte, die für das Konfigurieren von Benachrichtigungen erforderlich sind, und bietet Links zu Entscheidungspunkten oder detaillierten Anleitungen für jeden Schritt.

**Tabelle 2-9. Checkliste für die Konfiguration von Benachrichtigungen**

Aufgabe	Erforderliche Rolle	Details
<input type="checkbox"/> Konfigurieren Sie einen Postausgangsserver zum Senden von Benachrichtigungen.	<ul style="list-style-type: none"> <li>■ Systemadministratoren konfigurieren globale Standardserver.</li> <li>■ Mandantenadministratoren konfigurieren Server für ihre Mandanten.</li> </ul>	<p>Informationen zum ersten Konfigurieren eines Servers für einen Mandanten finden Sie unter <a href="#">Hinzufügen eines mandanten-spezifischen Postausgangsservers</a>. Informationen zur Vorgehensweise, wenn Sie einen globale Standardserver überschreiben müssen, finden Sie unter <a href="#">Überschreiben eines Standard-Ausgangs-E-Mail-Servers des Systems</a>. Informationen zum Konfigurieren globaler Standardserver für alle Mandanten finden Sie unter <a href="#">Erstellen eines globalen Postausgangsservers</a>.</p>
<input type="checkbox"/> (Optional) Konfigurieren Sie einen Posteingangsserver, sodass Benutzer Aufgaben ausführen können, indem sie auf Benachrichtigungen antworten.	<ul style="list-style-type: none"> <li>■ Systemadministratoren konfigurieren globale Standardserver.</li> <li>■ Mandantenadministratoren konfigurieren Server für ihre Mandanten.</li> </ul>	<p>Informationen zum ersten Konfigurieren eines Servers für einen Mandanten finden Sie unter <a href="#">Hinzufügen eines mandanten-spezifischen Posteingangsservers</a>. Informationen zur Vorgehensweise, wenn Sie einen globale Standardserver überschreiben müssen, finden Sie unter <a href="#">Überschreiben eines Standard-Eingangs-E-Mail-Servers des Systems</a>. Informationen zum Konfigurieren eines globalen Standardserver für alle Mandanten finden Sie unter <a href="#">Erstellen eines globalen Posteingangsservers</a>.</p>
<input type="checkbox"/> Wählen Sie die vRealize Automation-Ereignisse aus, bei denen Benutzerbenachrichtigungen ausgelöst werden sollen. Benutzer können nur Benachrichtigungen für Ereignisse abonnieren, die Sie als Benachrichtigungsauslöser aktiviert haben.	Mandantenadministrator	<p>Siehe <a href="#">Konfigurieren der Benachrichtigungen</a>.</p>

**Tabelle 2-9. Checkliste für die Konfiguration von Benachrichtigungen (Fortsetzung)**

Aufgabe	Erforderliche Rolle	Details
<input type="checkbox"/> (Optional) Konfigurieren Sie die Vorlagen für Benachrichtigungen, die an Maschinenbesitzer wegen Ereignissen im Zusammenhang mit ihren Maschinen gesendet werden, wie z. B. der Ablauf einer Lease.	Jeder Benutzer mit Zugriff auf das Verzeichnis \Vorlagen unter dem Installationsverzeichnis des vRealize Automation-Servers (meistens %SystemDrive%\Programme\x86\VMware\re\vmcac\Server) kann die Vorlagen für diese E-Mail-Benachrichtigungen konfigurieren.	Siehe <a href="#">Konfigurieren von Vorlagen für automatische IaaS-E-Mails</a> .
<input type="checkbox"/> Stellen Sie Ihren Benutzern Anweisungen darüber zur Verfügung, wie sie aktivierte Benachrichtigungen abonnieren können. Wenn sie möchten, können sie nur diejenigen Benachrichtigungen abonnieren, die für ihre Rollen relevant sind.	Alle Benutzer	Siehe <a href="#">Abonnieren von Benachrichtigungen</a> .

## Konfigurieren globaler E-Mail-Server für Benachrichtigungen

Mandantenadministratoren können E-Mail-Server im Rahmen der Konfiguration von Benachrichtigungen für ihre eigenen Mandanten hinzufügen. Als Systemadministrator können Sie globale Posteingangs- und Postausgangsserver einrichten, die allen Mandanten als Systemstandardeinstellungen angezeigt werden. Wenn Mandantenadministratoren diese Einstellungen nicht außer Kraft setzen, bevor sie Benachrichtigungen aktivieren, verwendet vRealize Automation die global konfigurierten E-Mail-Server.

### Erstellen eines globalen Posteingangsservers

Systemadministratoren erstellen einen globalen Posteingangsserver für eingehende E-Mail-Benachrichtigungen wie etwa Genehmigungsantworten. Sie können nur einen Posteingangsserver erstellen, der als Standardwert für alle Mandanten angezeigt wird. Wenn Mandantenadministratoren diese Einstellungen nicht außer Kraft setzen, bevor sie Benachrichtigungen aktivieren, verwendet vRealize Automation den global konfigurierten E-Mail-Server.

#### Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Systemadministrator** an.

#### Vorgehensweise

- 1 Wählen Sie **Administration > E-Mail-Server** aus.
- 2 Klicken Sie auf das Symbol **Hinzufügen (+)**.
- 3 Wählen Sie **E-Mail – Eingehend** aus.

- 4 Klicken Sie auf **OK**.
- 5 Geben Sie im Textfeld **Name** einen Namen ein.
- 6 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.
- 7 (Optional) Aktivieren Sie das Kontrollkästchen **SSL**, um als Sicherheitsoption SSL zu verwenden.
- 8 Wählen Sie ein Serverprotokoll aus.
- 9 Geben Sie den Namen des Servers im Textfeld **Servername** ein.
- 10 Geben Sie die Portnummer des Servers im Textfeld **Server-Port** ein.
- 11 Geben Sie den Ordernamen für E-Mails im Textfeld **Ordnername** ein.  
Diese Option ist nur erforderlich, wenn Sie IMAP-Serversteuerung wählen.
- 12 Geben Sie im Textfeld **Benutzername** einen Benutzernamen ein.
- 13 Geben Sie in das Textfeld **Kennwort** ein Kennwort ein.
- 14 Geben Sie die E-Mail-Adresse, an die vRealize Automation-Benutzer Antworten senden können, im Textfeld **E-Mail-Adresse** ein.
- 15 (Optional) Wählen Sie **Vom Server löschen** aus, um alle verarbeiteten E-Mails, die vom Benachrichtigungsdienst abgerufen werden, vom Server zu löschen.
- 16 Wählen Sie aus, ob vRealize Automation selbstsignierte Zertifikate vom E-Mail-Server annehmen kann.
- 17 Klicken Sie auf **Testverbindung**.
- 18 Klicken Sie auf **Hinzufügen**.

## Erstellen eines globalen Postausgangsservers

Systemadministratoren erstellen einen globalen Postausgangsserver für ausgehende E-Mail-Benachrichtigungen. Sie können nur einen Postausgangsserver erstellen, der als Standardwert für alle Mandanten angezeigt wird. Wenn Mandantenadministratoren diese Einstellungen nicht außer Kraft setzen, bevor sie Benachrichtigungen aktivieren, verwendet vRealize Automation den global konfigurierten E-Mail-Server.

### Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Systemadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > E-Mail-Server** aus.
- 2 Klicken Sie auf das Symbol **Hinzufügen** (+).
- 3 Wählen Sie **E-Mail – Ausgehend** aus.
- 4 Klicken Sie auf **OK**.
- 5 Geben Sie im Textfeld **Name** einen Namen ein.



- 6 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.
- 7 Geben Sie den Namen des Servers im Textfeld **Servername** ein.
- 8 Wählen Sie eine Verschlüsselungsmethode.
  - Klicken Sie auf **SSL verwenden**.
  - Klicken Sie auf **TLS verwenden**.
  - Klicken Sie für das Senden unverschlüsselter Kommunikation auf **Keine**.
- 9 Geben Sie die Portnummer des Servers im Textfeld **Server-Port** ein.
- 10 (Optional) Aktivieren Sie das Kontrollkästchen **Erforderlich**, wenn für den Server eine Authentifizierung erforderlich ist.
  - a Geben Sie im Textfeld **Benutzername** einen Benutzernamen ein.
  - b Geben Sie im Textfeld **Kennwort** ein Kennwort ein.
- 11 Geben Sie die E-Mail-Adresse, die als Absender der vRealize Automation-E-Mails angezeigt werden sollen, im Textfeld **Absenderadresse** ein.  
Diese E-Mail-Adresse entspricht dem von Ihnen angegebenen Benutzernamen und Kennwort.
- 12 Wählen Sie aus, ob vRealize Automation selbstsignierte Zertifikate vom E-Mail-Server annehmen kann.
- 13 Klicken Sie auf **Testverbindung**.
- 14 Klicken Sie auf **Hinzufügen**.

## Hinzufügen eines mandantenspezifischen Postausgangsservers

Mandantenadministratoren können einen Postausgangsserver hinzufügen, um Benachrichtigungen zum Durchführen von Arbeitselementen wie beispielsweise Genehmigungen zu senden.

Für jeden Mandanten ist nur ein Postausgangsserver zulässig. Für den Fall, dass Ihr Systemadministrator bereits einen globalen Postausgangsserver konfiguriert hat, finden Sie weitere Informationen unter [Überschreiben eines Standard-Ausgangs-E-Mail-Servers des Systems](#).

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.
- Wenn für den E-Mail-Server die Authentifizierung erforderlich ist, muss der angegebene Benutzer in einer Identitätsquelle und in der Business-Gruppe vorhanden sein.

### Vorgehensweise

- 1 Wählen Sie **Administration > Benachrichtigungen > E-Mail-Server** aus.
- 2 Klicken Sie auf das Symbol **Hinzufügen** (+).
- 3 Wählen Sie **E-Mail – Ausgehend** aus.

- 4 Klicken Sie auf **OK**.
- 5 Geben Sie im Textfeld **Name** einen Namen ein.
- 6 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.
- 7 Geben Sie den Namen des Servers im Textfeld **Servername** ein.
- 8 Wählen Sie eine Verschlüsselungsmethode.
  - Klicken Sie auf **SSL verwenden**.
  - Klicken Sie auf **TLS verwenden**.
  - Klicken Sie für das Senden unverschlüsselter Kommunikation auf **Keine**.
- 9 Geben Sie die Portnummer des Servers im Textfeld **Server-Port** ein.
- 10 (Optional) Aktivieren Sie das Kontrollkästchen **Erforderlich**, wenn für den Server eine Authentifizierung erforderlich ist.
  - a Geben Sie im Textfeld **Benutzername** einen Benutzernamen ein.
  - b Geben Sie im Textfeld **Kennwort** ein Kennwort ein.
- 11 Geben Sie die E-Mail-Adresse, die als Absender der vRealize Automation-E-Mails angezeigt werden sollen, im Textfeld **Absenderadresse** ein.

Diese E-Mail-Adresse entspricht dem von Ihnen angegebenen Benutzernamen und Kennwort.
- 12 Wählen Sie aus, ob vRealize Automation selbstsignierte Zertifikate vom E-Mail-Server annehmen kann.

Diese Option ist nur verfügbar, wenn Sie die Verschlüsselung aktiviert haben.

  - Klicken Sie zum Annehmen von selbstsignierten Zertifikaten auf **Ja**.
  - Klicken Sie zum Ablehnen von selbstsignierten Zertifikaten auf **Nein**.
- 13 Klicken Sie auf **Testverbindung**.
- 14 Klicken Sie auf **Hinzufügen**.

## Hinzufügen eines mandantenspezifischen Posteingangsservers

Mandantenadministratoren können einen Posteingangsserver hinzufügen, damit Benutzer Benachrichtigungen zum Durchführen von Arbeitselementen wie beispielsweise Genehmigungen beantworten können.

Für jeden Mandanten ist nur ein Posteingangsserver zulässig. Für den Fall, dass Ihr Systemadministrator bereits einen globalen Posteingangsserver konfiguriert hat, finden Sie weitere Informationen unter [Überschreiben eines Standard-Eingangs-E-Mail-Servers des Systems](#).

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

- Stellen Sie sicher, dass der angegebene Benutzer in einer Identitätsquelle und in der Business-Gruppe vorhanden ist.

### Vorgehensweise

- 1 Wählen Sie **Administration > Benachrichtigungen > E-Mail-Server** aus.
- 2 Klicken Sie auf das Symbol **Hinzufügen (+)**.
- 3 Wählen Sie **E-Mail – Eingehend** aus und klicken Sie auf **OK**.
- 4 Konfigurieren Sie die folgenden Optionen für den Posteingangsserver.

Option	Aktion
<b>Name</b>	Geben Sie einen Namen für den Posteingangsserver ein.
<b>Beschreibung</b>	Geben Sie eine Beschreibung für den Posteingangsserver ein.
<b>Sicherheit</b>	Aktivieren Sie das Kontrollkästchen <b>SSL verwenden</b> .
<b>Protokoll</b>	Wählen Sie ein Serverprotokoll aus.
<b>Servername</b>	Geben Sie den Servernamen ein.
<b>Server-Port</b>	Geben Sie die Server-Portnummer ein.

- 5 Geben Sie den Ordernamen für E-Mails im Textfeld **Ordnername** ein.  
Diese Option ist nur erforderlich, wenn Sie IMAP-Serversteuerung wählen.
- 6 Geben Sie im Textfeld **Benutzername** einen Benutzernamen ein.
- 7 Geben Sie in das Textfeld **Kennwort** ein Kennwort ein.
- 8 Geben Sie die E-Mail-Adresse, an die vRealize Automation-Benutzer Antworten senden können, im Textfeld **E-Mail-Adresse** ein.
- 9 (Optional) Wählen Sie **Vom Server löschen** aus, um alle verarbeiteten E-Mails, die vom Benachrichtigungsdienst abgerufen werden, vom Server zu löschen.
- 10 Wählen Sie aus, ob vRealize Automation selbstsignierte Zertifikate vom E-Mail-Server annehmen kann.  
Diese Option ist nur verfügbar, wenn Sie die Verschlüsselung aktiviert haben.
  - Klicken Sie zum Annehmen von selbstsignierten Zertifikaten auf **Ja**.
  - Klicken Sie zum Ablehnen von selbstsignierten Zertifikaten auf **Nein**.
- 11 Klicken Sie auf **Testverbindung**.
- 12 Klicken Sie auf **Hinzufügen**.

## Überschreiben eines Standard-Ausgangs-E-Mail-Servers des Systems

Wenn der Systemadministrator einen Standard-Ausgangs-E-Mail-Servers des Systems konfiguriert hat, kann der Mandantenadministrator diese globale Einstellung überschreiben.

## Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

## Vorgehensweise

- 1 Wählen Sie **Administration > Benachrichtigungen > E-Mail-Server** aus.
- 2 Wählen Sie den Ausgangs-E-Mail-Server aus.
- 3 Klicken Sie auf **Globale Einstellungen überschreiben**.
- 4 Geben Sie im Textfeld **Name** einen Namen ein.
- 5 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.
- 6 Geben Sie den Namen des Servers im Textfeld **Servername** ein.
- 7 Wählen Sie eine Verschlüsselungsmethode.
  - Klicken Sie auf **SSL verwenden**.
  - Klicken Sie auf **TLS verwenden**.
  - Klicken Sie für das Senden unverschlüsselter Kommunikation auf **Keine**.
- 8 Geben Sie die Portnummer des Servers im Textfeld **Server-Port** ein.
- 9 (Optional) Aktivieren Sie das Kontrollkästchen **Erforderlich**, wenn für den Server eine Authentifizierung erforderlich ist.
  - a Geben Sie im Textfeld **Benutzername** einen Benutzernamen ein.
  - b Geben Sie im Textfeld **Kennwort** ein Kennwort ein.
- 10 Geben Sie die E-Mail-Adresse, die als Absender der vRealize Automation-E-Mails angezeigt werden sollen, im Textfeld **Absenderadresse** ein.

Diese E-Mail-Adresse entspricht dem von Ihnen angegebenen Benutzernamen und Kennwort.
- 11 Wählen Sie aus, ob vRealize Automation selbstsignierte Zertifikate vom E-Mail-Server annehmen kann.

Diese Option ist nur verfügbar, wenn Sie die Verschlüsselung aktiviert haben.

  - Klicken Sie zum Annehmen von selbstsignierten Zertifikaten auf **Ja**.
  - Klicken Sie zum Ablehnen von selbstsignierten Zertifikaten auf **Nein**.
- 12 Klicken Sie auf **Testverbindung**.
- 13 Klicken Sie auf **Hinzufügen**.

## Überschreiben eines Standard-Eingangs-E-Mail-Servers des Systems

Wenn der Systemadministrator einen Standard-Eingangs-E-Mail-Server des Systems konfiguriert hat, können Mandantenadministratoren diese globale Einstellung überschreiben.

## Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

## Vorgehensweise

- 1 Wählen Sie **Administration > Benachrichtigungen > E-Mail-Server** aus.
- 2 Wählen Sie den Eingangs-E-Mail-Server in der Tabelle für die E-Mail-Server aus.
- 3 Klicken Sie auf **Globale Einstellungen überschreiben**.
- 4 Geben Sie die folgenden Optionen für den Eingangs-E-Mail-Server ein.

Option	Aktion
<b>Name</b>	Geben Sie den Namen des Eingangs-E-Mail-Servers ein.
<b>Beschreibung</b>	Geben Sie eine Beschreibung für den Posteingangsserver ein.
<b>Sicherheit</b>	Aktivieren Sie das Kontrollkästchen <b>SSL</b> , um als Sicherheitsoption SSL zu verwenden.
<b>Protokoll</b>	Wählen Sie ein Serverprotokoll aus.
<b>Servername</b>	Geben Sie den Servernamen ein.
<b>Server-Port</b>	Geben Sie die Server-Portnummer ein.

- 5 Geben Sie den Ordernamen für E-Mails im Textfeld **Ordnername** ein.  
Diese Option ist nur erforderlich, wenn Sie IMAP-Serversteuerung wählen.
- 6 Geben Sie im Textfeld **Benutzername** einen Benutzernamen ein.
- 7 Geben Sie in das Textfeld **Kennwort** ein Kennwort ein.
- 8 Geben Sie die E-Mail-Adresse, an die vRealize Automation-Benutzer Antworten senden können, im Textfeld **E-Mail-Adresse** ein.
- 9 (Optional) Wählen Sie **Vom Server löschen** aus, um alle verarbeiteten E-Mails, die vom Benachrichtigungsdienst abgerufen werden, vom Server zu löschen.
- 10 Wählen Sie aus, ob vRealize Automation selbstsignierte Zertifikate vom E-Mail-Server annehmen kann.  
Diese Option ist nur verfügbar, wenn Sie die Verschlüsselung aktiviert haben.
  - Klicken Sie zum Annehmen von selbstsignierten Zertifikaten auf **Ja**.
  - Klicken Sie zum Ablehnen von selbstsignierten Zertifikaten auf **Nein**.
- 11 Klicken Sie auf **Testverbindung**.
- 12 Klicken Sie auf **Hinzufügen**.

## Zurücksetzen von Systemstandard-E-Mail-Servern

Mandantenadministratoren, die Systemstandard-Server überschreiben, können die Einstellungen wieder auf die globalen Einstellungen zurücksetzen.

## Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

## Vorgehensweise

- 1 Wählen Sie **Administration > Benachrichtigungen > E-Mail-Server** aus.
- 2 Wählen Sie den zurückzusetzenden E-Mail-Server aus.
- 3 Klicken Sie auf **Zu globalen Einstellungen zurückkehren**.
- 4 Klicken Sie auf **Ja**.

## Konfigurieren der Benachrichtigungen

Jeder Benutzer bestimmt, ob er Benachrichtigungen empfangen möchte, aber Mandantenadministratoren bestimmen, durch welche Ereignisse Benachrichtigungen ausgelöst werden.

## Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.
- Stellen Sie sicher, dass ein Mandantenadministrator oder Systemadministrator einen Postausgangsserver konfiguriert hat. Siehe [Hinzufügen eines mandantenspezifischen Postausgangsservers](#).

## Vorgehensweise

- 1 Wählen Sie **Administration > Benachrichtigungen > Szenarien** aus.
- 2 Wählen Sie eine oder mehrere Benachrichtigungen aus.
- 3 Klicken Sie auf **Aktivieren**.

Benutzer, die in den Benutzervoreinstellungen Benachrichtigungen abonnieren, erhalten nun die Benachrichtigungen.

## Anpassen des Datums für E-Mail-Benachrichtigungen wegen des Ablaufs von Maschinen

Sie können angeben, wann vor Ablauf einer Maschine eine E-Mail-Benachrichtigung verschickt werden soll.

Sie können die Einstellung ändern, die die Anzahl der Tage vor dem Ablaufdatum der Maschine festlegt, wenn vRealize Automation eine Benachrichtigungs-E-Mail bezüglich des Ablaufs sendet. Die E-Mail benachrichtigt Benutzer über das Ablaufdatum einer Maschine. Standardmäßig liegt die Einstellung bei sieben Tagen vor dem Ablaufdatum der Maschine.

## Vorgehensweise

- 1 Melden Sie sich am vRealize Automation-Server mithilfe von Anmeldedaten mit Administratorzugriff an.
- 2 Navigieren Sie zur Datei `/etc/vcac/setenv-user` und öffnen Sie sie.

- 3 Fügen Sie folgende Zeile zur Datei hinzu, um die Anzahl der Tage vor dem Ablaufdatum der Maschine anzugeben, wobei 3 in diesem Beispiel drei Tage vor Ablauf der Maschine bedeutet.

```
VCAC_OPTS="$VCAC_OPTS -Dlease.enforcement.prearchive.notification.days=3"
```

- 4 Starten Sie die vCAC-Dienste auf der virtuellen Appliance neu, indem Sie folgenden Befehl ausführen:

```
service vcac-server restart
```

### Weiter

Wenn Sie in einer Lastausgleichsdienstumgebung mit hoher Verfügbarkeit arbeiten, wiederholen Sie diesen Vorgang für alle virtuellen Appliances in der HA-Umgebung.

## Konfigurieren von Vorlagen für automatische IaaS-E-Mails

Sie können festlegen, dass an Maschinenbesitzer Benachrichtigungs-E-Mails zu verschiedenen vRealize Automation-Ereignissen im Zusammenhang mit ihren Maschinen gesendet werden.

Zu den Ereignissen, durch die Benachrichtigungen ausgelöst werden, zählen beispielsweise der Ablauf oder der bevorstehende Ablauf von Archivierungszeiträumen und VM-Leases.

Informationen zum Konfigurieren und Aktivieren bzw. Deaktivieren von vRealize Automation-E-Mail-Benachrichtigungen finden Sie in den folgenden Knowledgebase-Artikeln:

- [Anpassen von E-Mail-Vorlagen in vRealize Automation \(2088805\)](#)
- [Beispiele für die Anpassung von E-Mail-Vorlagen in vRealize Automation \(2102019\)](#)

## Abonnieren von Benachrichtigungen

Wenn Ihre Administratoren Benachrichtigungen konfiguriert haben, können Sie Benachrichtigungen von vRealize Automation abonnieren. Benachrichtigungsereignisse können den erfolgreichen Abschluss einer Kataloganforderung oder einer erforderlichen Genehmigung beinhalten.

### Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole an.

### Vorgehensweise

- 1 Klicken Sie auf **Einstellungen**.
- 2 Wählen Sie das Kontrollkästchen **Aktiviert** für das E-Mail-Protokoll in der Tabelle „Benachrichtigungen“ aus.
- 3 Klicken Sie auf **Übernehmen**.
- 4 Klicken Sie auf **Schließen**.

## (Optional) Erstellen einer benutzerdefinierten RDP-Datei zur Unterstützung von RDP-Verbindungen für bereitgestellte Maschinen

Systemadministratoren erstellen eine benutzerdefinierte Remotedesktop-Protokolldatei, die von IaaS-Architekten in Blueprints zum Konfigurieren von RDP-Einstellungen verwendet wird. Nachdem Sie die RDP-Datei erstellen und den Architekten den vollständigen Pfadnamen für die Datei bereitstellen, damit diese sie in Blueprints einbinden können, erteilt ein Katalogadministrator den Benutzern die Berechtigung für die RDP-Aktion.

---

**Hinweis** Wenn Sie Internet Explorer verwenden und die „Verstärkte Sicherheitskonfiguration“ aktiviert ist, können Sie keine .rdp-Dateien herunterladen.

---

### Voraussetzungen

Melden Sie sich am IaaS Manager Service als Administrator an.

### Vorgehensweise

- 1 Setzen Sie das aktuelle Verzeichnis auf `<vRA_installation_dir>\Rdp`.
- 2 Kopieren Sie die Datei `Default.rdp` und benennen Sie diese im selben Verzeichnis in `Console.rdp` um.
- 3 Öffnen Sie die Datei `Console.rdp` in einem Editor.
- 4 Fügen Sie der Datei RDP-Einstellungen hinzu.  
Beispiel: **connect to console:i:1.**
- 5 Wenn Sie in einer verteilten Umgebung arbeiten, melden Sie sich bei der IaaS-Hostmaschine, auf der die Model Manager-Website-Komponente installiert ist, als Benutzer mit Administratorrechten an.
- 6 Kopieren Sie die Datei `Console.rdp` in das Verzeichnis `vRA_installation_dir\Website\Rdp`.

Ihre IaaS-Architekten können die benutzerdefinierten RDP-Eigenschaften zu Windows-Maschinen-Blueprints hinzufügen, woraufhin Katalogadministratoren Benutzern die Berechtigung für die Aktion „Verbindungsherstellung mithilfe von RDP“ erteilen können. Siehe [Hinzufügen der Unterstützung von RDP-Verbindungen zu Ihren Windows-Maschinen-Blueprints](#).

## (Optional) Szenario: Hinzufügen von Datacenter-Standorten für regionsenübergreifende Bereitstellungen

Sie möchten als Systemadministrator Standorte für Ihre Datacenter in Boston und London festlegen, damit Ihre Fabric-Administratoren für Computing-Ressourcen in jedem Datacenter die richtigen Standorte anwenden können. Wenn Ihre Blueprint-Architekten Blueprints erstellen, können sie die Standorte-Funktion aktivieren, damit die Benutzer Maschinen in Boston oder London bereitstellen können, wenn sie ihre Katalogelement-Anforderungsformulare ausfüllen.



Sie haben ein Datacenter in London und eines in Boston, und möchten nicht, dass Benutzer in Boston Maschinen Ihrer Londoner Infrastruktur bereitstellen und umgekehrt. Um sicherzustellen, dass Benutzer in Boston die Bereitstellung für Ihre Bostoner Infrastruktur vornehmen, und Benutzer in London die Bereitstellung für Ihre Londoner Infrastruktur vornehmen, sollten Sie den Benutzern erlauben, einen geeigneten Standort für die Bereitstellung auszuwählen, wenn sie Maschinen anfordern.



### Vorgehensweise

- 1 Melden Sie sich bei Ihrem IaaS-Webserver-Host mithilfe der Administratoranmeldedaten an.  
Dies ist der Computer, auf dem Sie die IaaS-Website-Komponente installiert haben.
- 2 Bearbeiten Sie die Datei `WebSite\XmlData\DataCenterLocations.xml` im Windows Server-Installationsverzeichnis (in der Regel `%SystemDrive%\Programme x86\VMware\vCAC\Server`).
- 3 Bearbeiten Sie den Abschnitt „CustomDataType“ der Datei, um für jeden Standort „Data Name“-Einträge zu erstellen.

```
<CustomDataType>
  <Data Name="London" Description="London datacenter" />
  <Data Name="Boston" Description="Boston datacenter" />
</CustomDataType>
```

- 4 Speichern und schließen Sie die Datei.
- 5 Starten Sie den Manager Service neu.
- 6 Wenn mehr als ein IaaS-Webserver-Host vorhanden ist, wiederholen Sie diesen Vorgang für jede redundante Instanz.

Ihr Fabric-Administrator kann für die in den einzelnen Datacentern vorhandenen Computing-Ressourcen den geeigneten Standort anwenden. Siehe [Szenario: Anwenden eines Standorts auf eine Computing-Ressource für regionsübergreifende Bereitstellungen](#).

## Konfigurieren von vRealize Orchestrator und Plug-ins

VMware vRealize™ Orchestrator™ ist eine Automatisierungs- und Verwaltungs-Engine, die vRealize Automation für die Unterstützung von XaaS und weiteren Erweiterungsmöglichkeiten erweitert.

Mit vRealize Orchestrator können Administratoren und Architekten mithilfe des Workflow-Designers komplexe Automatisierungsaufgabe entwickeln, und anschließend über vRealize Automation auf die Workflows zugreifen und diese ausführen.

vRealize Orchestrator kann mit vRealize Orchestrator-Plug-ins auf externe Technologien zugreifen und diese steuern.

## Konfigurationsrechte

System- und Mandantenadministratoren können vRealize Automation für die Verwendung eines externen vRealize Orchestrator-Servers konfigurieren.

Außerdem können Systemadministratoren festlegen, welche Workflow-Ordner den einzelnen Mandanten zur Verfügung stehen.

Mandantenadministratoren können die vRealize Orchestrator-Plug-ins als Endpoints konfigurieren.

Rolle	Mit vRealize Orchestrator verbundene Konfigurationsrechte
Systemadministratoren	<ul style="list-style-type: none"> <li>■ Konfigurieren des vRealize Orchestrator-Servers für alle Mandanten.</li> <li>■ Definieren des standardmäßigen vRealize Orchestrator-Workflow-Ordner für einen Mandanten.</li> </ul>
Mandantenadministratoren	<ul style="list-style-type: none"> <li>■ Konfigurieren des vRealize Orchestrator-Servers für ihren eigenen Mandanten.</li> <li>■ Hinzufügen von vRealize Orchestrator-Plug-ins als Endpoints.</li> </ul>

## Konfigurieren des standardmäßigen Workflow-Ordners für einen Mandanten

Systemadministratoren können Workflows in verschiedenen Ordnern gruppieren und anschließend pro Mandant Workflow-Kategorien definieren. Dadurch kann ein Systemadministrator Benutzern von verschiedenen Mandanten den Zugriff auf unterschiedliche Workflow-Ordner auf demselben vRealize Orchestrator-Server erteilen.

### Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Systemadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Zusätzliche Services > vRO-Standardordner** aus.
- 2 Klicken Sie auf den Namen des Mandanten, den Sie bearbeiten möchten.
- 3 Navigieren Sie in der vRealize Orchestrator-Workflow-Bibliothek und wählen Sie einen Ordner aus.
- 4 Klicken Sie auf **Hinzufügen**.

Sie haben den standardmäßigen vRealize Orchestrator-Workflow-Ordner für einen Mandanten definiert.

### Weiter

Wiederholen Sie diese Schritte für alle Mandanten, für die Sie einen Standard-Workflow-Ordner definieren möchten.

## Konfigurieren eines externen vRealize Orchestrator -Servers

Sie können vRealize Automation für die Verwendung eines externen vRealize Orchestrator-Servers einrichten.

Systemadministratoren können den vRealize Orchestrator-Standardserver global für alle Mandanten konfigurieren. Mandantenadministratoren können den vRealize Orchestrator-Server nur für ihre Mandanten konfigurieren.

Bei Verbindungen zu externen vRealize Orchestrator-Server-Instanzen muss das Benutzerkonto über Berechtigungen zum Anzeigen und Ausführen in vRealize Orchestrator verfügen.

- Single Sign On-Authentifizierung. Die Benutzerinformationen werden mit der XaaS-Anforderung an vRealize Orchestrator übergeben, und dem Benutzer werden Anzeige- und Ausführberechtigungen für den angeforderten Workflow gewährt.
- Standardauthentifizierung. Das angegebene Benutzerkonto muss Mitglied einer vRealize Orchestrator-Gruppe mit Anzeige- und Ausführberechtigungen oder Mitglied der „vcoadmin“-Gruppe sein.

### Voraussetzungen

- Installieren und konfigurieren Sie einen externen vRealize Orchestrator-Server. Sie können auch die vRealize Orchestrator-Appliance bereitstellen. Siehe *Installieren und Konfigurieren von VMware vCenter Orchestrator*.
- Melden Sie sich an der vRealize Automation-Konsole als **Systemadministrator** oder **Mandantenadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > vRO-Konfiguration > Serverkonfiguration** aus.
- 2 Klicken Sie auf **Externen Orchestrator-Server verwenden**.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 Geben Sie im Textfeld **Host** die IP-Adresse oder den DNS-Namen der Maschine ein, auf der der vRealize Orchestrator-Server ausgeführt wird.
- 5 Geben Sie im Textfeld **Port** die Portnummer für die Kommunikation mit dem externen vRealize Orchestrator-Server ein.

Der Standardport für vRealize Orchestrator ist 8281.

## 6 Wählen Sie den Authentifizierungstyp aus.

Option	Beschreibung
<b>Single Sign On</b>	<p>Stellt unter Verwendung von vCenter Single Sign On eine Verbindung zum vRealize Orchestrator-Server her.</p> <p>Diese Option kann nur dann angewendet werden, wenn Sie vRealize Orchestrator und vRealize Automation so konfiguriert haben, dass eine gemeinsame vCenter Single Sign-On-Instanz verwendet wird.</p>
<b>Einfach</b>	<p>Stellt mit dem Benutzernamen und dem Kennwort, die Sie in das Textfeld <b>Benutzername</b> bzw. <b>Kennwort</b> eingegeben haben, eine Verbindung zum vRealize Orchestrator-Server her.</p> <p>Das von Ihnen angegebene Benutzerkonto muss Mitglied der „vcoadmins“-Gruppe von vRealize Orchestrator oder Mitglied einer Gruppe mit Anzeige- und Ausführberechtigungen sein.</p>

## 7 Klicken Sie auf **Testverbindung**.

## 8 Klicken Sie auf **Aktualisieren**.

Sie haben die Verbindung zum externen vRealize Orchestrator-Server konfiguriert, woraufhin der Workflows-Ordner **vCAC** und die diesbezüglichen Dienstprogrammaktionen automatisch importiert werden. Der Workflows-Ordner **vCAC > ASD** enthält Workflows zum Konfigurieren von Endpoints und zum Erstellen von Ressourcenzuordnungen.

### Weiter

Konfigurieren Sie die vRealize Orchestrator-Plug-ins als Endpoints. Siehe [Konfigurieren von XaaS-Ressourcen](#).

## Anmelden bei der Konfigurationsschnittstelle von vRealize Orchestrator

Zum Bearbeiten der Konfiguration der vRealize Orchestrator-Standardinstanz, die in vRealize Automation integriert ist, müssen Sie den vRealize Orchestrator-Konfigurationsdienst starten und sich bei der Konfigurationsschnittstelle von vRealize Orchestrator anmelden.

Der vRealize Orchestrator-Konfigurationsdienst wird in der vRealize Automation-Appliance standardmäßig nicht gestartet. Sie müssen den vRealize Orchestrator-Konfigurationsdienst starten, um auf die vRealize Orchestrator-Konfigurationsschnittstelle zuzugreifen.

### Vorgehensweise

- 1 Starten Sie den vRealize Orchestrator-Konfigurationsdienst.
  - a Melden Sie sich an der Linux-Konsole der vRealize Automation-Appliance als Root-Benutzer an.
  - b Geben Sie **service vco-configurator start** ein und drücken Sie die Eingabetaste.
- 2 Navigieren Sie zur Managementkonsole der vRealize Automation-Appliance, indem Sie den vollqualifizierten Domännennamen verwenden (<https://vra-virtual-hostname.domain.name>).

**3 Klicken Sie auf vRealize Orchestrator Control Center.**

Sie werden zu <https://vra-virtual-hostname.domain.name:8283/vco-controlcenter> umgeleitet.

**4 Melden Sie sich beim vRealize Orchestrator Control Center an.**

Der Benutzername wird vom vRealize Automation-Appliance-Administrator konfiguriert.

**5 (Optional) Wenn Sie sich zum ersten Mal anmelden, ändern Sie das Standardkennwort und klicken Sie auf **Änderungen übernehmen**.**

Ihr neues Kennwort muss aus mindestens acht Zeichen bestehen und mindestens eine Zahl, ein Sonderzeichen und einen Großbuchstaben enthalten.

## Anmelden beim vRealize Orchestrator -Client

Zum Ausführen allgemeiner Verwaltungsaufgaben oder zum Bearbeiten und Erstellen von Workflows in der vRealize Orchestrator-Standardinstanz müssen Sie sich beim vRealize Orchestrator-Client anmelden.

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

### Vorgehensweise

**1 Navigieren Sie zur Managementkonsole der vRealize Automation-Appliance, indem Sie den vollqualifizierten Domännennamen verwenden (<https://vra-virtual-hostname.domain.name>).**

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

Die Clientdatei wird heruntergeladen.

**3 Klicken Sie auf den Download und befolgen Sie die Anweisungen.**

**4 Geben Sie auf der vRealize Orchestrator-Anmeldeseite die IP oder den Domännennamen der vRealize Automation-Appliance in das Textfeld **Hostname** ein und geben Sie **443** als Standardportnummer ein.**

Geben Sie beispielsweise Folgendes ein: `vrealize_automation_appliance_ip:443`.

**5 Melden Sie sich mit dem Benutzernamen und Kennwort für den vRealize Orchestrator-Client an.**

Die Anmeldedaten sind der Benutzername und das Kennwort des Standardmandantenadministrators.

## 6 Wählen Sie im Fenster **Zertifikatwarnung** eine Option zum Behandeln der Zertifikatwarnung aus.

Der vRealize Orchestrator-Client kommuniziert mit dem vRealize 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 vRealize Orchestrator-Server herstellen.

Option	Beschreibung
<b>Ignorieren</b>	Setzen Sie den Vorgang unter Verwendung des aktuellen SSL-Zertifikats fort. Die Warnmeldung wird erneut angezeigt, wenn Sie die Verbindung zum selben vRealize Orchestrator-Server erneut herstellen, oder wenn Sie versuchen, einen Workflow mit einem Orchestrator-Remoteserver zu synchronisieren.
<b>Abbrechen</b>	Schließen Sie das Fenster und beenden Sie den Anmeldevorgang.
<b>Dieses Zertifikat installieren und keine Sicherheitswarnungen für dieses mehr anzeigen.</b>	Wählen Sie dieses Kontrollkästchen und klicken Sie auf <b>Ignorieren</b> , 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 entwickeln oder Rechte für den Root-Zugriff auf dem System festlegen. Informationen dazu finden Sie unter *Verwendung des VMware vRealize Orchestrator-Clients* und *Entwickeln mit VMware vRealize Orchestrator*.

# Konfigurieren von Ressourcen

Sie können Ressourcen konfigurieren, wie z. B. Endpoints, Reservierungen und Netzwerkprofile, um Blueprint-Definitionen und Maschinenbereitstellungen durch vRealize Automation zu unterstützen.

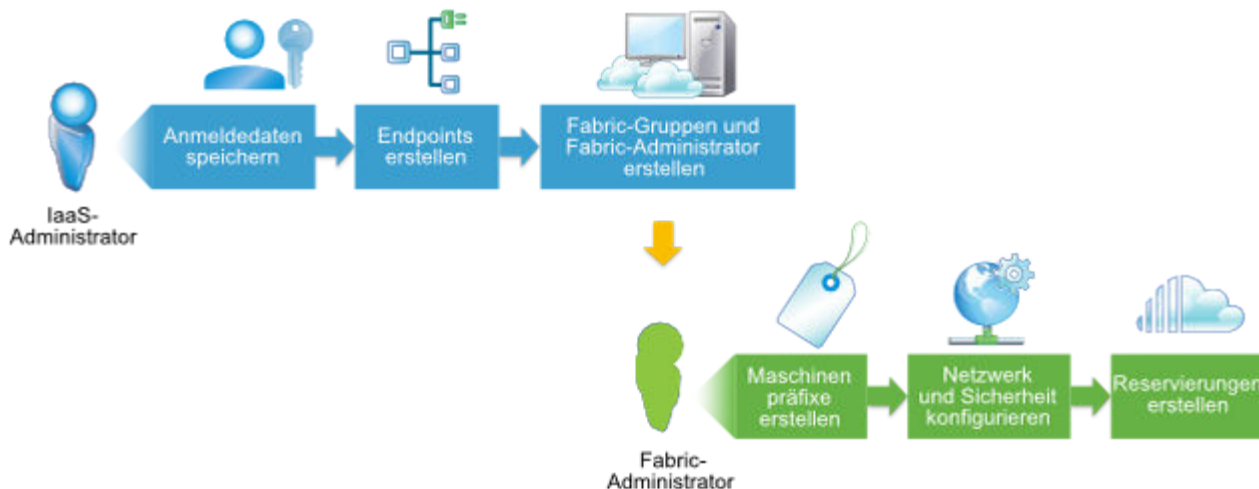
Dieses Kapitel behandelt die folgenden Themen:

- [Checkliste für die Konfiguration von IaaS-Ressourcen](#)
- [Konfigurieren von XaaS-Ressourcen](#)
- [Installieren zusätzlicher Plug-Ins auf dem vRealize Orchestrator-Standardserver](#)
- [Arbeiten mit Active Directory-Richtlinien](#)

## Checkliste für die Konfiguration von IaaS-Ressourcen

IaaS-Administratoren und Fabric-Administratoren konfigurieren IaaS-Ressourcen, um vorhandene Infrastrukturen in vRealize Automation zu integrieren und um vRealize Automation-Business-Gruppen Infrastrukturressourcen zuzuweisen.

Sie können die Checkliste für die Konfiguration von IaaS-Ressourcen verwenden, um eine allgemeine Übersicht über die Abfolge der Schritte zu erhalten, die für die Konfiguration von IaaS-Ressourcen erforderlich sind.



**Tabelle 3-1. Checkliste für die Konfiguration von IaaS-Ressourcen**

Aufgabe	vRealize Automation-Rolle	Details
<input type="checkbox"/> Speichern Sie Administratoranmeldedaten für Ihre Infrastruktur.	IaaS-Administrator	<a href="#">Speichern von Benutzeranmeldedaten.</a> Sie müssen keine Anmeldedaten angeben, wenn Sie eine der folgenden Plattformen integrieren: <ul style="list-style-type: none"> <li>■ Xen-Pool auf einem XenServer</li> <li>■ XenServer</li> <li>■ vSphere, und Ihr Systemadministrator hat für den Proxy-Agent die Verwendung integrierter Anmeldedaten konfiguriert</li> </ul>
<input type="checkbox"/> Erstellen Sie Endpoints für Ihre Infrastruktur, um Ressourcen mit vRealize Automation verwalten zu können.	IaaS-Administrator	<a href="#">Auswählen eines Endpoint-Szenarios.</a>
<input type="checkbox"/> Erstellen Sie eine Fabric-Gruppe, um Infrastrukturressourcen zu Gruppen zusammenzufassen und um mindestens einem Administrator die Verwaltung dieser Ressourcen als Ihr vRealize Automation-Fabric-Administrator zuzuweisen.	IaaS-Administrator	<a href="#">Erstellen einer Fabric-Gruppe.</a>
<input type="checkbox"/> Konfigurieren Sie Maschinenpräfixe, die für die Erstellung von Namen für durch vRealize Automation bereitgestellte Maschinen verwendet werden.	Fabric-Administrator	<a href="#">Konfigurieren von Maschinenpräfixen.</a>
<input type="checkbox"/> (Optional) Erstellen Sie Netzwerkprofile, um Netzwerkeinstellungen für bereitgestellte Maschinen zu konfigurieren.	Fabric-Administrator	<a href="#">Erstellen eines Netzwerkprofils.</a>
<input type="checkbox"/> Teilen Sie Business-Gruppen Infrastrukturressourcen zu, indem Sie Reservierungen und optional auch Reservierungs- und Speicherreservierungsprofile erstellen.	<ul style="list-style-type: none"> <li>■ IaaS-Administrator, wenn dieser auch als Fabric-Administrator konfiguriert wurde</li> <li>■ Fabric-Administrator</li> </ul>	<a href="#">Konfigurieren von Reservierungen und Reservierungsrichtlinien.</a>

## Speichern von Benutzeranmeldedaten

Sie müssen Anmeldedaten auf Administratorebene für Ihre Umgebung speichern, damit vRealize Automation mit den Endpoints kommunizieren kann. Da dieselben Anmeldedaten für mehrere Endpoints verwendet werden können, werden Anmeldedaten getrennt von Endpoints verwaltet und zugeordnet, wenn Endpoints erstellt oder bearbeitet werden.

### Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **IaaS-Administrator** an.

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Endpoints > Anmeldedaten** aus.



- 2 Klicken Sie auf **Neue Anmeldedaten**.
- 3 Geben Sie im Textfeld **Name** einen Namen ein.
- 4 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.
- 5 Geben Sie in das Textfeld **Benutzername** den Benutzernamen ein.

Plattform	Format und Details
vSphere	<b>Domäne\Benutzername</b> Geben Sie die Anmeldedaten mit der Berechtigung zum Ändern benutzerdefinierter Attribute ein.
vCloud Air	<b>Benutzername</b> wie in der Endpoint-Benutzerschnittstelle angegeben Geben Sie die Anmeldedaten für einen Organisationsadministrator mit Berechtigungen zur Verbindungsherstellung durch Verwendung von VMware Remote Console ein.
vCloud Director	<b>Benutzername</b> wie in der Endpoint-Benutzerschnittstelle angegeben Geben Sie die Anmeldedaten mit Berechtigungen zur Verbindungsherstellung durch Verwendung von VMware Remote Console ein. <ul style="list-style-type: none"> <li>■ Geben Sie zum Verwalten aller Organisationen mit einem einzelnen Endpoint die Anmeldedaten für einen Systemadministrator ein.</li> <li>■ Erstellen Sie zum Verwalten eines jeden virtuellen Datacenters einer Organisation (vDC) mit einem separaten Endpoint separate Anmeldedaten für Organisationsadministratoren für jedes vDC.</li> </ul> Erstellen Sie nicht einen einzelnen Endpoint auf Systemebene und einzelne Organisations-Endpoints für dieselbe vCloud Director-Instanz.
vRealize Orchestrator	<b>Benutzername@Domäne</b> Geben Sie Anmeldedaten für jede der vRealize Orchestrator-Instanzen mit Ausführberechtigungen auf allen Workflows ein, die Sie von vRealize Automation aufrufen möchten.
vCloud Networking and Security (nur vSphere)	<b>Domäne\Benutzername</b>
NSX (nur vSphere)	<b>Benutzername</b>
Amazon AWS	Geben Sie die Zugriffsschlüssel-ID ein. Informationen zum Abrufen der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels finden Sie in der Amazon AWS-Dokumentation.
Cisco UCS Manager	<b>Benutzername</b>
Dell iDRAC	<b>Benutzername</b>
HP iLO	<b>Benutzername</b>
Hyper-V (SCVMM)	<b>Domäne\Benutzername</b>
KVM (RHEV)	<b>Benutzername@Domäne</b>
NetApp ONTAP	<b>Benutzername</b>
Red Hat OpenStack	<b>Benutzername</b> Geben Sie die Anmeldedaten für einen einzelnen Benutzer ein, der ein Administrator in all Ihren Red Hat OpenStack-Mandanten ist, oder erstellen Sie einzelne Anmeldedaten für jeden Mandanten.

## 6 Geben Sie in die Textfelder **Kennwort** das Kennwort ein.

Plattform	Format
Amazon AWS	Geben Sie den geheimen Zugriffsschlüssel ein. Informationen zum Abrufen der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels finden Sie in der Amazon AWS-Dokumentation.
Alle anderen	Geben Sie das Kennwort für den eingegebenen Benutzernamen ein.

## 7 Klicken Sie auf das Symbol **Speichern** (✓).

### Weiter

Nun, da Ihre Anmeldedaten gespeichert sind, können Sie einen Endpoint erstellen. Siehe [Auswählen eines Endpoint-Szenarios](#).

## Auswählen eines Endpoint-Szenarios

Sie erstellen die Endpoints, mit denen vRealize Automation mit Ihrer Infrastruktur kommunizieren kann. Die Vorgehensweise zum Erstellen eines Endpoints hängt von Ihren Anforderungen an die Maschinenbereitstellung ab.

Wählen Sie ein Endpoint-Szenario basierend auf dem Typ des Ziel-Endpoints aus.

**Tabelle 3-2. Auswählen eines Endpoint-Szenarios**

Umgebung	Endpoint erstellen
vSphere	<a href="#">Erstellen eines vSphere-Endpoints</a>
vSphere mit NSX	<a href="#">Erstellen eines vSphere-Endpoints mit Netzwerk- und Sicherheitsintegration</a>
vSphere mit Net App FlexClone-Technologie für die Speicherung	<a href="#">Erstellen eines NetApp ONTAP-Endpoints</a>
vRealize Orchestrator	<a href="#">Erstellen eines vRealize Orchestrator-Endpoints</a>
Endpoint des externen IPAM-Anbieters	<a href="#">Erstellen eines Endpoints für externen IPAM-Anbieter</a>
vCloud Air-Abonnement oder OnDemand	<a href="#">Erstellen eines vCloud Air-Endpoints</a>
vCloud Director	<a href="#">Erstellen eines vCloud Director-Endpoints</a>
Hyper-V Eigenständig	<a href="#">Erstellen eines eigenständigen Endpoints für Hyper-V</a>
Hyper-V mit SCVMM (Microsoft Center Virtual Machine Manager)	<a href="#">Erstellen eines Hyper-V (SCVMM)-Endpoints</a>
KVM (RHEV)	<a href="#">Erstellen eines KVM (RHEV)-Endpoints</a>
Amazon Cloud-Dienstkonto	<ul style="list-style-type: none"> <li>■ <a href="#">Erstellen eines Amazon-Endpoints</a></li> <li>■ (Optional) <a href="#">Hinzufügen eines Amazon-Instanztyps</a></li> </ul>
OpenStack-Mandant	<a href="#">Erstellen eines OpenStack- oder PowerVC-Endpoints</a>
PowerVC	<a href="#">Erstellen eines OpenStack- oder PowerVC-Endpoints</a>
Xen-Pool auf einem XenServer	<a href="#">Erstellen eines Xen-Pool-Endpoints</a>

**Tabelle 3-2. Auswählen eines Endpoint-Szenarios (Fortsetzung)**

Umgebung	Endpoint erstellen
XenServer	<a href="#">Erstellen eines XenServer-Endpoints</a>
Liste von Endpoints importieren	<ul style="list-style-type: none"> <li>■ <a href="#">Vorbereiten einer Endpoint-CSV-Datei für den Import</a></li> <li>■ <a href="#">Importieren einer Liste von Endpoints</a></li> </ul>

## Erstellen eines vSphere -Endpoints

Sie können Endpoints erstellen, um vRealize Automation die Kommunikation mit der vSphere-Umgebung und die Erkennung von Computing-Ressourcen, die Datenerfassung und die Bereitstellung von Maschinen zu erlauben.

Wenn Ihre vSphere-Umgebung in NSX integriert ist, finden Sie weitere Informationen unter [Erstellen eines vSphere-Endpoints mit Netzwerk- und Sicherheitsintegration](#).

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **laaS-Administrator** an.
- Sie müssen einen vSphere-Proxy-Agent installieren, um Ihren vSphere-Endpoint zu verwalten, und Sie müssen genau den gleichen Namen für Ihren Endpoint und Agent verwenden. Informationen zum Installieren des Agents finden Sie unter *Installieren von vRealize Automation 7.1*.
- Wenn Ihr Systemadministrator für den Proxy-Agent nicht die Verwendung integrierter Anmeldedaten konfiguriert hat, müssen Sie Administratoranmeldedaten für Ihren Endpoint speichern. Siehe [Speichern von Benutzeranmeldedaten](#).

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Wählen Sie **Neu > Virtuell > vSphere** aus.
- 3 Geben Sie im Textfeld **Name** einen Namen ein.

Diese Angabe muss mit dem Endpoint-Namen übereinstimmen, der bei der Installation für den vSphere-Proxy-Agent angegeben wurde. Andernfalls schlägt die Datenerfassung fehl.

- 4 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.
- 5 Geben Sie in das Textfeld **Adresse** die URL für die vCenter Server-Instanz ein.

Die URL muss folgenden Typ aufweisen: **https://hostname/sdk** oder **https://IP\_address/sdk**.

Beispielsweise **https://vsphereA/sdk**.

- 6 Klicken Sie auf **Anmeldedaten** und wählen Sie die für diesen Endpoint gespeicherten Administratoranmeldedaten aus.

Wenn Ihr Systemadministrator für den vSphere-Proxy-Agent die Verwendung integrierter Anmeldedaten konfiguriert hat, können Sie die **Integrierten** Anmeldedaten auswählen.

- 7 Wählen Sie die Option **Manager für Netzwerk und Sicherheitsplattform angeben** nicht aus, es sei denn, Ihre Konfiguration unterstützt NSX.

Diese Einstellung ist für Implementierungen gedacht, die NSX verwenden, und erfordert zusätzliche Konfiguration.

- 8 (Optional) Klicken Sie im Abschnitt „Benutzerdefinierte Eigenschaften“ auf **Neu**, um Endpoint-Eigenschaften hinzuzufügen, die für den speziellen IPAM-Lösungsanbieter sinnvoll sind.

Jeder IPAM-Lösungsanbieter (z. B. Infoblox und Bluecat) verwendet eindeutige erweiterbare Attribute, die Sie mithilfe von benutzerdefinierten vRealize Automation-Eigenschaften emulieren können. Beispielsweise verwendet Infoblox erweiterbare Attribute, um primäre und sekundäre Endpoints zu unterscheiden.

- 9 Klicken Sie auf **OK**.

vRealize Automation erfasst Daten Ihres Endpoints und ermittelt Ihre Computing-Ressourcen.

---

**Wichtig** Benennen Sie vSphere-Datencenter nach der Datenerfassung nicht um, da andernfalls möglicherweise die Bereitstellung fehlschlägt.

---

#### Weiter

Fügen Sie die Computing-Ressourcen von Ihrem Endpoint zu einer Fabric-Gruppe hinzu. Siehe [Erstellen einer Fabric-Gruppe](#).

## Erstellen eines vSphere -Endpoints mit Netzwerk- und Sicherheitsintegration

Sie können Endpoints erstellen, damit vRealize Automation mit der vSphere-Umgebung und einer NSX-Instanz kommunizieren kann.

#### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **laaS-Administrator** an.
- Sie müssen einen vSphere-Proxy-Agent installieren, um Ihren vSphere-Endpoint zu verwalten, und Sie müssen genau den gleichen Namen für Ihren Endpoint und Agent verwenden. Informationen zum Installieren des Agents finden Sie unter *Installieren von vRealize Automation 7.1*.
- Speichern Sie Administratoranmeldedaten für Ihren vSphere-Endpoint und Ihren Networking and Security-Endpoint. Siehe [Speichern von Benutzeranmeldedaten](#). Wenn Ihr Systemadministrator für Ihren Proxy-Agent die Verwendung integrierter Anmeldedaten konfiguriert hat, müssen Sie nur die Anmeldedaten für NSX speichern.
- Konfigurieren Sie die Netzwerkeinstellungen. Siehe [Konfigurieren der Einstellungen für Netzwerk- und Sicherheitskomponenten](#).

#### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Wählen Sie **Neu > Virtuell > vSphere** aus.

- 3 Geben Sie im Textfeld **Name** einen Namen ein.

Diese Angabe muss mit dem Endpoint-Namen übereinstimmen, der bei der Installation für den vSphere-Proxy-Agent angegeben wurde. Andernfalls schlägt die Datenerfassung fehl.

- 4 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.

- 5 Geben Sie in das Textfeld **Adresse** die URL für die vCenter Server-Instanz ein.

Die URL muss folgenden Typ aufweisen: **https://hostname/sdk** oder **https://IP\_address/sdk**.

Beispielsweise **https://vsphereA/sdk**.

- 6 Klicken Sie auf **Anmeldedaten** und wählen Sie die für diesen Endpoint gespeicherten Administratoranmeldedaten aus.

Wenn Ihr Systemadministrator für den vSphere-Proxy-Agent die Verwendung integrierter Anmeldedaten konfiguriert hat, können Sie die **Integrierten** Anmeldedaten auswählen.

- 7 Konfigurieren Sie eine Netzwerklösungsplattform.

Dieser Schritt ist zum Aktivieren der NSX-Netzwerk- und Sicherheitsfunktionen erforderlich.

- a Wählen Sie **Manager für Netzwerk und Sicherheitsplattform angeben** aus.

- b Geben Sie in das Textfeld **Adresse** die URL für die NSX-Instanz ein.

Die URL muss folgenden Typ aufweisen: **https://hostname** oder **https://IP\_address**.

Beispiel: **https://nsx-manager**.

- c Klicken Sie auf **Anmeldedaten** und wählen Sie die für diesen Endpoint gespeicherten Administratoranmeldedaten aus.

- 8 (Optional) Fügen Sie benutzerdefinierte Eigenschaften hinzu.

- 9 Klicken Sie auf **OK**.

vRealize Automation erfasst Daten Ihres Endpoints und ermittelt Ihre Computing-Ressourcen.

---

**Wichtig** Benennen Sie vSphere-Datencenter nach der Datenerfassung nicht um, da andernfalls möglicherweise die Bereitstellung fehlschlägt.

---

## Weiter

Fügen Sie die Computing-Ressourcen von Ihrem Endpoint zu einer Fabric-Gruppe hinzu. Siehe [Erstellen einer Fabric-Gruppe](#).

## Erstellen eines vRealize Orchestrator -Endpoints

Sie können mehrere Endpoints für die Verbindungsherstellung mit unterschiedlichen vRealize Orchestrator-Servern konfigurieren, aber für jeden Endpoint müssen Sie die Priorität festlegen.

Beim Ausführen von vRealize Orchestrator-Workflows versucht vRealize Automation zuerst den vRealize Orchestrator Endpoint mit der höchsten Priorität. Wenn dieser Endpoint nicht erreichbar ist, folgt der Endpoint mit der nächsthöheren Priorität, bis ein vRealize Orchestrator-Server verfügbar ist, der den Workflow ausführen kann.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **laaS-Administrator** an.
- Konfigurieren Sie die Benutzeranmeldedaten. Siehe *Konfigurieren von vRealize Automation*.

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Wählen Sie **Neu > Orchestrierung > vCenter Orchestrator** aus.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 Geben Sie eine URL mit dem vollqualifizierten Namen oder der IP-Adresse des vRealize Orchestrator-Servers und die vRealize Orchestrator-Portnummer ein.

Das Transportprotokoll muss HTTPS sein. Wenn kein Port angegeben wurde, wird der Standardport 443 verwendet.

Um die in der vRealize Automation-Appliance eingebettete Standard-vRealize Orchestrator-Instanz zu verwenden, geben Sie **https://vrealize-automation-appliance-hostname:443/vco** ein.

- 5 Legen Sie die Priorität für die Endpoints fest.
  - a Klicken Sie auf **Neue Eigenschaft**.
  - b Geben Sie **VMware.VCenterOrchestrator.Priority** in das Textfeld **Name** ein.  
Bei Eigenschaftsnamen wird die Groß- und Kleinschreibung berücksichtigt.
  - c Geben Sie eine ganze Zahl größer oder gleich 1 in das Textfeld **Wert** ein.  
Je niedriger der Wert, desto höher die Priorität.
  - d Klicken Sie auf das Symbol **Speichern** (✔).
- 6 Klicken Sie auf **OK**.

### Konfigurieren von vRealize Orchestrator -Endpoints für das Netzwerk

Wenn Sie vRealize Automation-Workflows zum Aufrufen von vRealize Orchestrator-Workflows verwenden, müssen Sie die vRealize Orchestrator-Instanz oder den Server als Endpoint konfigurieren.

Informationen zum Hinzufügen eines vRealize Orchestrator-Endpoints finden Sie unter [Erstellen eines vRealize Orchestrator-Endpoints](#).

Sie können einen vRealize Orchestrator-Endpoint einem Maschinen-Blueprint zuordnen, um sicherzustellen, dass alle vRealize Orchestrator-Workflows für die mit diesem Blueprint bereitgestellten Maschinen unter Verwendung dieses Endpoints ausgeführt werden.

vRealize Automation enthält standardmäßig eine eingebettete vRealize Orchestrator-Instanz. Es wird empfohlen, dass Sie diese als vRealize Orchestrator-Endpoint für das Ausführen von vRealize Automation-Workflows in einer Testumgebung oder für das Erstellen eines Proof-of-Concepts verwenden.

Sie können auch ein Plug-In auf einem externen vRealize Orchestrator-Server installieren.

Es wird empfohlen, diesen vRealize Orchestrator-Endpoint zum Ausführen von vRealize Automation-Workflows in einer Produktionsumgebung zu verwenden.

Informationen zum Installieren des Plug-Ins finden Sie in der README-Datei, die im Lieferumfang der Installationsdatei für das Plug-In auf der VMware-Website für Produktdownloads unter

<http://vmware.com/web/vmware/downloads> über den Link vCloud Networking and Security oder NSX verfügbar ist.

## Erstellen eines Endpoints für externen IPAM-Anbieter

Wenn Sie einen IPAM-Endpoint-Typ in vRealize Orchestrator registriert und konfiguriert haben, können Sie einen Endpoint für diesen IPAM-Lösungsanbieter in vRealize Automation erstellen.

Wenn Sie ein vRealize Orchestrator-Paket zur Bereitstellung einer externen IPAM-Lösung importiert und den IPAM-Endpoint-Typ in vRealize Orchestrator registriert haben, können Sie diesen IPAM-Endpoint-Typ bei der Erstellung eines vRealize Automation-Endpoints auswählen.

---

**Hinweis** Dieses Beispiel basiert auf der Verwendung des Infoblox IPAM-Plug-Ins, das bei VMware Solution Exchange heruntergeladen werden kann. Sie können dieses Verfahren auch verwenden, wenn Sie Ihr eigenes IPAM-Anbieterpaket mithilfe des im Lieferumfang von VMware enthaltenen IPAM-Lösungs-SDKs erstellt haben. Das Verfahren zum Importieren und Konfigurieren eines eigenen von einem Drittanbieter bereitgestellten IPAM-Lösungspakets entspricht dem in den Voraussetzungen beschriebenen Verfahren.

---

Der erste IPAM-Endpoint für vRealize Automation wird erstellt, wenn Sie den Endpoint-Typ für das IPAM-Lösungs-Anbieter-Plug-In in vRealize Orchestrator registrieren.

### Voraussetzungen

- [Abrufen und Importieren des externen IPAM-Anbieterpakets in vRealize Orchestrator.](#)
- [Ausführen des Workflows zum Registrieren des Infoblox-IPAM-Endpoint-Typs in vRealize Orchestrator.](#)
- Melden Sie sich an der vRealize Automation-Konsole als **laaS-Administrator** an.
- Konfigurieren Sie die Benutzeranmeldedaten. Siehe *Konfigurieren von vRealize Automation*.

Erstellen Sie in diesem Beispiel einen Infoblox IPAM-Endpoint mithilfe eines Endpoint-Typs, den Sie in Ihrem importierten Infoblox VMware Plug-in for vCenter Orchestrator-Paket registriert haben.

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.

## 2 Wählen Sie **Neu > IPAM** aus.

Wählen Sie einen registrierten Endpoint-Typ für den externen IPAM-Anbieter wie beispielsweise Infoblox aus. Endpoints für externe IPAM-Anbieter sind nur verfügbar, wenn Sie ein vRealize Orchestrator-Paket eines Drittanbieters importiert haben und die Paketworkflows zum Registrieren des Endpoint-Typs ausführen.

Für den IPAM-Anbieter Infoblox werden nur primäre IPAM-Endpoint-Typen aufgeführt. Mithilfe benutzerdefinierter Eigenschaften können Sie sekundäre IPAM-Endpoint-Typen angeben.

Wählen Sie in diesem Beispiel einen registrierten Endpoint-Typ für den externen IPAM-Anbieter aus, wie beispielsweise **Infoblox NIOS**.

## 3 Geben Sie einen Namen und optional eine Beschreibung ein.

## 4 Geben Sie den Speicherort des registrierten IPAM-Endpoints in das Textfeld **Adresse** ein, indem Sie das anbieterspezifische URL-Format verwenden, wie beispielsweise `https://Hostname/Name`.

Beispielsweise können Sie mehrere IPAM-Endpoints wie etwa `https://nsx62-scale-infoblox` und `https://nsx62-scale-infoblox2` beim Registrieren des IPAM-Endpoint-Typs in vRealize Orchestrator erstellen. Geben Sie einen primären registrierten Endpoint-Typ ein. Um auch einen oder mehrere sekundäre IPAM-Endpoints anzugeben, können Sie mithilfe benutzerdefinierter Eigenschaften die erweiterbaren Attribute speziell für den IPAM-Lösungsanbieter emulieren.

## 5 Geben Sie den Benutzernamen und das Kennwort ein, die für den Zugriff auf das Konto des IPAM-Lösungsanbieters erforderlich sind.

Die Anmeldedaten für das Konto des IPAM-Lösungsanbieters sind erforderlich, um den Endpoint beim Arbeiten in vRealize Automation zu erstellen, konfigurieren und bearbeiten. vRealize Automation verwendet die Anmeldedaten des IPAM-Endpoints für die Kommunikation mit dem angegebenen Endpoint-Typ (z. B. Infoblox), um IP-Adressen zuzuteilen und sonstige Vorgänge durchzuführen. Dieses Verhalten ist mit der Art und Weise vergleichbar, wie vRealize Automation Anmeldedaten für vSphere-Endpoints verwendet.

## 6 (Optional) Klicken Sie im Abschnitt „Benutzerdefinierte Eigenschaften“ auf **Neu**, um Endpoint-Eigenschaften hinzuzufügen, die für den speziellen IPAM-Lösungsanbieter sinnvoll sind.

Jeder IPAM-Lösungsanbieter (z. B. Infoblox und Bluecat) verwendet eindeutige erweiterbare Attribute, die Sie mithilfe von benutzerdefinierten vRealize Automation-Eigenschaften emulieren können. Beispielsweise verwendet Infoblox erweiterbare Attribute, um primäre und sekundäre Endpoints zu unterscheiden.

## 7 Klicken Sie auf **OK**.

### Weiter

Fügen Sie die Computing-Ressourcen von Ihrem Endpoint zu einer Fabric-Gruppe hinzu. Siehe [Erstellen einer Fabric-Gruppe](#).

## Erstellen eines vCloud Air -Endpoints

Sie können für einen OnDemand- oder Abonnementdienst einen vCloud Air-Endpoint erstellen.



Informationen zur vCloud Air-Managementkonsole finden Sie in der vCloud Air-Dokumentation.

---

**Hinweis** Für vCloud Air-Endpoints und vCloud Director-Endpoints definierte Reservierungen wird die Verwendung von Netzwerkprofilen für die Bereitstellung von Maschinen nicht unterstützt.

---

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **laaS-Administrator** an.
- Stellen Sie sicher, dass Sie über die Berechtigung **Virtual Infrastructure-Administrator** für Ihr vCloud Air-Abonnementdienst- bzw. OnDemand-Konto verfügen.
- [Speichern von Benutzeranmeldedaten](#).

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Wählen Sie **Neu > Cloud > vCloud Air** aus.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 Übernehmen Sie die standardmäßige vCloud Air-Endpoint-Adresse im Textfeld **Adresse** oder geben Sie eine neue Adresse ein.

Die standardmäßige vCloud Air-Endpoint-Adresse lautet „https://vca.vmware.com“ gemäß der Angabe für die globale Eigenschaft Default URL for vCloud Air endpoint.

- 5 Klicken Sie auf **Anmeldedaten** und wählen Sie die für diesen Endpoint gespeicherten Administratoranmeldedaten aus.

Sie müssen sich als vCloud Air-Abonnementdienst- bzw. OnDemand-Kontoadministrator anmelden.

- 6 (Optional) Aktivieren Sie das Kontrollkästchen **Proxy-Server verwenden**, um zusätzliche Sicherheit zu konfigurieren und Verbindungen über einen Proxy-Server zu erzwingen.
  - a Geben in das Textfeld **Hostname** den Hostnamen Ihres Proxy-Servers ein.
  - b Geben Sie in das Textfeld **Port** die zu verwendende Portnummer für die Verbindung mit dem Proxy-Server ein.
  - c (Optional) Klicken Sie auf das Symbol **Durchsuchen** neben dem Textfeld **Anmeldedaten**.  
Wählen Sie Anmeldedaten aus oder erstellen Sie Anmeldedaten, die den Benutzernamen und das Kennwort für den Proxy-Server repräsentieren, falls dies für die Proxy-Konfiguration erforderlich ist.

- 7 (Optional) Fügen Sie benutzerdefinierte Eigenschaften hinzu.
- 8 Klicken Sie auf **OK**.

### Weiter

[Erstellen einer Fabric-Gruppe](#).

## Erstellen eines vCloud Director -Endpoints

Sie können einen vCloud Director-Endpoint für die Verwaltung aller vCloud Director-vDCs (virtuelle Datacenter) in Ihrer Umgebung erstellen, oder Sie erstellen separate Endpoints für die Verwaltung jeder vCloud Director-Organisation.

Informationen zu Organisations-vDCs finden Sie in der vCloud Director-Dokumentation.

Erstellen Sie keinen einzelnen Endpoint und keine separaten Organisations-Endpoints für dieselbe vCloud Director-Instanz.

vRealize Automation verwendet einen Proxy-Agent für die Verwaltung von vSphere-Ressourcen.

---

**Hinweis** Für vCloud Air-Endpoints und vCloud Director-Endpoints definierte Reservierungen wird die Verwendung von Netzwerkprofilen für die Bereitstellung von Maschinen nicht unterstützt.

---

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **laaS-Administrator** an.
- [Speichern von Benutzeranmeldedaten](#).

### Vorgehensweise

1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.

2 Wählen Sie **Neu > Cloud > vCloud Director** aus.

3 Geben Sie einen Namen und optional eine Beschreibung ein.

4 Geben Sie in das Textfeld **Adresse** die URL des vCloud Director-Servers ein.

Die URL muss vom Typ *FQDN* oder *IP\_address* sein.

Beispielsweise `https://mycompany.com`.

5 Klicken Sie auf **Anmeldedaten** und wählen Sie die für diesen Endpoint gespeicherten Administratoranmeldedaten aus.

- Melden Sie sich als Organisationsadministrator an, um eine Verbindung mit dem vCloud Director-Server herzustellen und die Organisation anzugeben, für die der Benutzer über die Administratorrolle verfügt. Mit diesen Anmeldedaten kann der Endpoint nur auf die zugeordneten Organisations-vDCs zugreifen. Sie können Endpoints für jede zusätzliche Organisation in der vCloud Director-Instanz hinzufügen, die in vRealize Automation integriert werden soll.
- Um den Zugriff auf alle Organisations-vDCs in der vCloud Director-Instanz zu erlauben, verwenden Sie Systemadministrator-Anmeldedaten für eine vCloud Director-Instanz und lassen Sie das Textfeld **Organisation** leer.

- 6 Als Organisationsadministrator können Sie den Namen einer vCloud Director-Organisation in das Textfeld **Organisation** eingeben.

Option	Beschreibung
<b>Alle Organisations-vCDs erkennen</b>	Wenn Sie vCloud Director in einer Private Cloud implementiert haben, können Sie das Textfeld <b>Organisation</b> leer lassen, um der Anwendung die Erkennung von allen verfügbaren Organisations-vDCs zu erlauben.
<b>Separate Endpoints für jedes Organisations-vCD</b>	Geben Sie in das Textfeld <b>Organisation</b> den Namen einer vCloud Director-Organisation ein.

Der Name der **Organisation** stimmt mit dem Namen Ihrer vCloud Director-Organisation überein, der möglicherweise auch als Name Ihres virtuellen Datencenters (vDC) angezeigt wird. Wenn Sie eine Virtual Private Cloud verwenden, ist dieser Name ein eindeutiger Bezeichner im Format M123456789-12345. In einer Dedicated Cloud ist dies der angegebene Name des Ziel-vDC.

Wenn Sie direkt eine Verbindung mit vCloud Director auf der Systemebene herstellen, indem Sie beispielsweise das Feld „Organisation“ leer lassen, benötigen Sie Anmeldedaten des Systemadministrators. Wenn Sie eine Organisation beim Endpoint eingeben, benötigen Sie einen Benutzer, der in dieser Organisation über Anmeldedaten des Organisationsadministrators verfügt.

- 7 (Optional) Aktivieren Sie das Kontrollkästchen **Proxy-Server verwenden**, um zusätzliche Sicherheit zu konfigurieren und Verbindungen über einen Proxy-Server zu erzwingen.
- Geben in das Textfeld **Hostname** den Hostnamen Ihres Proxy-Servers ein.
  - Geben Sie in das Textfeld **Port** die zu verwendende Portnummer für die Verbindung mit dem Proxy-Server sein.
  - (Optional) Klicken Sie auf das Symbol **Durchsuchen** neben dem Textfeld **Anmeldedaten**.  
Wählen Sie Anmeldedaten aus oder erstellen Sie Anmeldedaten, die den Benutzernamen und das Kennwort für den Proxy-Server repräsentieren, falls dies für die Proxy-Konfiguration erforderlich ist.
- 8 (Optional) Fügen Sie benutzerdefinierte Eigenschaften hinzu.
- 9 Klicken Sie auf **OK**.

Weiter

[Erstellen einer Fabric-Gruppe.](#)

## Erstellen eines Hyper-V (SCVMM)-Endpoints

IaaS-Administratoren können Endpoints erstellen, um vRealize Automation die Kommunikation mit Ihrer SCVMM-Umgebung und die Erkennung von Computing-Ressourcen, die Datenerfassung und die Bereitstellung von Maschinen zu erlauben.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **IaaS-Administrator** an.
- [Speichern von Benutzeranmeldedaten.](#)

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Wählen Sie **Neu > Virtuell > Hyper-V (SCVMM)** aus.
- 3 Geben Sie im Textfeld **Name** einen Namen ein.
- 4 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.
- 5 Geben Sie in das Textfeld **Adresse** die URL für den Endpoint ein.  
Die URL muss folgenden Typ aufweisen: *FQDN* oder *IP\_address*.  
Beispielsweise `mycompany-scvmm1.mycompany.local`.
- 6 Klicken Sie auf **Anmeldedaten** und wählen Sie die für diesen Endpoint gespeicherten Administratordaten aus.  
Falls Sie die Anmeldedaten noch nicht gespeichert haben, können Sie sie nun speichern.
- 7 (Optional) Fügen Sie benutzerdefinierte Eigenschaften hinzu.
- 8 Klicken Sie auf **OK**.

vRealize Automation erfasst Daten Ihres Endpoints und ermittelt Ihre Computing-Ressourcen.

### Weiter

Fügen Sie die Computing-Ressourcen von Ihrem Endpoint zu einer Fabric-Gruppe hinzu. Siehe [Erstellen einer Fabric-Gruppe](#).

## Erstellen eines eigenständigen Endpoints für Hyper-V

Sie können Endpoints erstellen, um vRealize Automation die Kommunikation mit der Hyper-V-Server-Umgebung und die Erkennung von Computing-Ressourcen, die Datenerfassung und die Bereitstellung von Maschinen zu erlauben.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **laaS-Administrator** an.
- Ein Systemadministrator muss einen Proxy-Agent mit entsprechenden gespeicherten Anmeldedaten für Ihren Endpoint erstellen. Siehe *Installieren von vRealize Automation 7.1*.

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Endpoints > Agents** aus.
- 2 Geben Sie in das Textfeld **Computing-Ressource** den vollqualifizierten DNS-Namen Ihres Hyper-V-Servers ein.
- 3 Wählen Sie aus dem Dropdown-Menü **Name des Proxy-Agents** den Proxy-Agent aus, den Ihr Systemadministrator für diesen Endpoint installiert hat.
- 4 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.

## 5 Klicken Sie auf **OK**.

vRealize Automation erfasst Daten Ihres Endpoints und ermittelt Ihre Computing-Ressourcen.

### Weiter

Fügen Sie die Computing-Ressourcen von Ihrem Endpoint zu einer Fabric-Gruppe hinzu. Siehe [Erstellen einer Fabric-Gruppe](#).

## Erstellen eines NetApp ONTAP -Endpoints

Sie können Endpoints erstellen, um vRealize Automation die Kommunikation mit Speichergeräten, die Net App FlexClone-Technologie verwenden, zu erlauben.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **laaS-Administrator** an.
- [Speichern von Benutzeranmeldedaten](#).

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Wählen Sie **Neu > Speicher > NetApp ONTAP** aus.
- 3 Geben Sie im Textfeld **Name** einen Namen ein.
- 4 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.
- 5 Geben Sie in das Textfeld **Adresse** die URL für den Endpoint ein.  
Die URL muss folgenden Typ aufweisen: **FQDN** oder **IP\_address**.  
Beispielsweise **netapp-1.mycompany.local**.
- 6 Klicken Sie auf **Anmeldedaten** und wählen Sie die für diesen Endpoint gespeicherten Administratoranmeldedaten aus.  
Falls Sie die Anmeldedaten noch nicht gespeichert haben, können Sie sie nun speichern.
- 7 (Optional) Fügen Sie benutzerdefinierte Eigenschaften hinzu.
- 8 Klicken Sie auf **OK**.

vRealize Automation erfasst Daten Ihres Endpoints und ermittelt Ihre Computing-Ressourcen.

### Weiter

Fügen Sie die Computing-Ressourcen von Ihrem Endpoint zu einer Fabric-Gruppe hinzu. Siehe [Erstellen einer Fabric-Gruppe](#).

## Erstellen eines KVM (RHEV) -Endpoints

Sie können Endpoints erstellen, um vRealize Automation die Kommunikation mit der KVM (RHEV)-Umgebung und die Erkennung von Computing-Ressourcen, die Datenerfassung und die Bereitstellung von Maschinen zu erlauben.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **laaS-Administrator** an.
- [Speichern von Benutzeranmeldedaten](#).

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Wählen Sie **Neu > Virtuell > KVM (RHEV)** aus.
- 3 Geben Sie im Textfeld **Name** einen Namen ein.
- 4 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.
- 5 Geben Sie in das Textfeld **Adresse** die URL für den Endpoint ein.

Die URL muss folgenden Typ aufweisen: **https://FQDN** oder **https://IP\_address**

Beispielsweise **https://mycompany-kvmrhev1.mycompany.local**.

- 6 Klicken Sie auf **Anmeldedaten** und wählen Sie die für diesen Endpoint gespeicherten Administratormeldedaten aus.

Falls Sie die Anmeldedaten noch nicht gespeichert haben, können Sie sie nun speichern.

- 7 (Optional) Fügen Sie benutzerdefinierte Eigenschaften hinzu.
- 8 Klicken Sie auf **OK**.

vRealize Automation erfasst Daten Ihres Endpoints und ermittelt Ihre Computing-Ressourcen.

### Weiter

Fügen Sie die Computing-Ressourcen von Ihrem Endpoint zu einer Fabric-Gruppe hinzu. Siehe [Erstellen einer Fabric-Gruppe](#).

## Erstellen eines Xen-Pool-Endpoints

Sie können Endpoints erstellen, um vRealize Automation die Kommunikation mit dem Xen-Pool-Master und die Erkennung von Computing-Ressourcen, die Datenerfassung und die Bereitstellung von Maschinen zu erlauben.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **laaS-Administrator** an.
- Ein Systemadministrator muss einen Proxy-Agent mit entsprechenden gespeicherten Anmeldedaten für Ihren Endpoint erstellen. Siehe *Installieren von vRealize Automation 7.1*.

**Vorgehensweise**

- 1 Wählen Sie **Infrastruktur > Endpoints > Agents** aus.
- 2 Geben Sie in das Textfeld **Computing-Ressource** den Namen Ihres Xen-Pool-Masters ein.

---

**Hinweis** Geben Sie nicht den Namen des Xen-Pools ein. Sie müssen den Namen des Pool-Masters eingeben.

---

Um doppelte Einträge in der vRealize Automation-Computing-Ressourcentabelle zu vermeiden, geben Sie eine Adresse an, die der konfigurierten Adresse des Xen-Pool-Masters entspricht. Wenn als Adresse des Xen-Pool-Masters beispielsweise der Hostname verwendet wird, geben Sie den Hostnamen ein und nicht den FQDN. Wenn der FQDN als Adresse des Xen-Pool-Masters verwendet wird, geben Sie den FQDN ein.

- 3 Wählen Sie aus dem Dropdown-Menü **Name des Proxy-Agents** den Proxy-Agent aus, den Ihr Systemadministrator für diesen Endpoint installiert hat.
- 4 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.
- 5 Klicken Sie auf **OK**.

vRealize Automation erfasst Daten Ihres Endpoints und ermittelt Ihre Computing-Ressourcen.

**Weiter**

Fügen Sie die Computing-Ressourcen von Ihrem Endpoint zu einer Fabric-Gruppe hinzu. Siehe [Erstellen einer Fabric-Gruppe](#).

**Erstellen eines XenServer-Endpoints**

Sie können Endpoints erstellen, um vRealize Automation die Kommunikation mit der XenServer-Umgebung und die Erkennung von Computing-Ressourcen, die Datenerfassung und die Bereitstellung von Maschinen zu erlauben.

**Voraussetzungen**

- Melden Sie sich an der vRealize Automation-Konsole als **laaS-Administrator** an.
- Ein Systemadministrator muss einen Proxy-Agent mit entsprechenden gespeicherten Anmeldedaten für Ihren Endpoint erstellen. Siehe *Installieren von vRealize Automation 7.1*.

**Vorgehensweise**

- 1 Wählen Sie **Infrastruktur > Endpoints > Agents** aus.
- 2 Geben Sie in das Textfeld **Computing-Ressource** den vollqualifizierten DNS-Namen Ihres XenServer-Servers ein.
- 3 Wählen Sie aus dem Dropdown-Menü **Name des Proxy-Agents** den Proxy-Agent aus, den Ihr Systemadministrator für diesen Endpoint installiert hat.
- 4 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.

## 5 Klicken Sie auf **OK**.

vRealize Automation erfasst Daten Ihres Endpoints und ermittelt Ihre Computing-Ressourcen.

### Weiter

Fügen Sie die Computing-Ressourcen von Ihrem Endpoint zu einer Fabric-Gruppe hinzu. Siehe [Erstellen einer Fabric-Gruppe](#).

## Erstellen eines Amazon-Endpoints

Sie können einen Endpoint erstellen, um eine Verbindung mit einer Amazon Web Services-Instanz herzustellen.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **IaaS-Administrator** an.
- [Speichern von Benutzeranmeldedaten](#).

### Vorgehensweise

1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.

2 Wählen Sie **Neu > Cloud > Amazon EC2** aus.

3 Geben Sie einen Namen und optional eine Beschreibung ein.

In der Regel verweist dieser Name auf das entsprechende Amazon Web Services-Konto für diesen Endpoint.

4 Klicken Sie auf **Anmeldedaten** und wählen Sie die für diesen Endpoint gespeicherten Administratoranmeldedaten aus.

Nur einem Endpoint kann eine Amazon-Zugriffsschlüssel-ID zugeordnet werden.

5 (Optional) Aktivieren Sie das Kontrollkästchen **Proxy-Server verwenden**, um zusätzliche Sicherheit zu konfigurieren und Verbindungen mit Amazon Web Services über einen Proxyserver zu erzwingen.

a Geben in das Textfeld **Hostname** den Hostnamen Ihres Proxy-Servers ein.

b Geben Sie in das Textfeld **Port** die zu verwendende Portnummer für die Verbindung mit dem Proxy-Server ein.

c (Optional) Klicken Sie auf das Symbol **Durchsuchen** neben dem Textfeld **Anmeldedaten**.

Wählen Sie Anmeldedaten aus oder erstellen Sie Anmeldedaten, die den Benutzernamen und das Kennwort für den Proxy-Server repräsentieren, falls dies für die Proxy-Konfiguration erforderlich ist.

6 (Optional) Fügen Sie benutzerdefinierte Eigenschaften hinzu.

7 Klicken Sie auf **OK**.

Nachdem der Endpoint erstellt wurde, beginnt vRealize Automation mit der Datenerfassung für die Amazon Web Services-Regionen.



## Weiter

vRealize Automation stellt mehrere Amazon Web Services-Instanztypen bereit, die Sie beim Erstellen von Blueprints verwenden können. Informationen zum Importieren eigener Instanztypen finden Sie unter [Hinzufügen eines Amazon-Instanztyps](#).

Fügen Sie die Computing-Ressourcen von Ihrem Endpoint zu einer Fabric-Gruppe hinzu. Siehe [Erstellen einer Fabric-Gruppe](#).

## Hinzufügen eines Amazon-Instanztyps

Mit vRealize Automation werden mehrere Instanztypen für die Verwendung mit Amazon-Blueprints zur Verfügung gestellt. Ein Administrator kann Instanztypen hinzufügen und entfernen.

Die von IaaS-Administratoren verwalteten Maschineninstanztypen stehen Blueprint-Architekten zur Verfügung, wenn sie einen Amazon-Blueprint erstellen oder bearbeiten. Amazon-Maschinen-Images und Instanztypen werden durch das Amazon Web Services-Produkt zur Verfügung gestellt.

## Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **IaaS-Administrator** an.

## Vorgehensweise

- 1 Klicken Sie auf **Infrastruktur > Administration > Instanztypen**.
- 2 Klicken Sie auf **Neuer Instanztyp**.
- 3 Fügen Sie einen neuen Instanztyp hinzu und geben Sie die folgenden Parameter an.

Informationen über die verfügbaren Amazon-Instanztypen und die Einstellungswerte, die Sie für diese Parameter angeben können, sind in der Amazon Web Services-Dokumentation in *EC2-Instance-Typen - Amazon Web Services (AWS)* unter „aws.amazon.com/ec2“ und *Instance Types* (Instanztypen) unter „docs.aws.amazon.com“ verfügbar.

- Name
- API-Name
- Name des Typs
- Name des E/A-Leistungsindikators
- CPUs
- Arbeitsspeicher (GB)
- Speicher (GB)
- Einheiten berechnen

- 4 Klicken Sie auf das Symbol **Speichern** (✔).

Wenn IaaS-Architekten Amazon Web Services-Blueprints erstellen, können sie Ihre benutzerdefinierten Instanztypen verwenden.

## Weiter

Fügen Sie die Computing-Ressourcen von Ihrem Endpoint zu einer Fabric-Gruppe hinzu. Siehe [Erstellen einer Fabric-Gruppe](#).

## Erstellen eines OpenStack- oder PowerVC-Endpoints

Sie erstellen einen Endpoint, damit vRealize Automation mit der OpenStack- oder PowerVC-Instanz kommunizieren kann.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **laaS-Administrator** an.
- [Speichern von Benutzeranmeldedaten](#).
- Stellen Sie sicher, dass die vRealize Automation-DEMs auf einem Computer installiert sind, der den Anforderungen von Openstack oder PowerVC entspricht. Siehe *Installieren von vRealize Automation 7.1*.
- Stellen Sie sicher, dass der verwendete Openstack-Typ aktuell unterstützt wird. Siehe *Übersicht über die Unterstützung von vRealize Automation*.

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Wählen Sie **Neu > Cloud > OpenStack** aus.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 Geben Sie in das Textfeld **Adresse** die URL für den Endpoint ein.

Option	Beschreibung
<b>PowerVC</b>	Die URL muss folgendes Format aufweisen: <b>https://FQDN/powervc/openstack/service</b> . Beispiel: <b>https://openstack.mycompany.com/powervc/openstack/admin</b> .
<b>OpenStack</b>	Die URL muss das Format <b>FQDN:5000</b> oder <b>IP_address:5000</b> aufweisen. Geben Sie das Suffix <b>/v2.0</b> nicht für die Endpoint-Adresse an. Beispiel: <b>https://openstack.mycompany.com:5000</b> .

- 5 Klicken Sie auf **Anmeldedaten** und wählen Sie die für diesen Endpoint gespeicherten Administratoranmeldedaten aus.

Die eingegebenen Anmeldedaten erfordern die Administratorrolle im OpenStack-Mandanten, der dem Endpoint zugeordnet ist.

- 6 Geben Sie in das Textfeld **OpenStack-Projekt** einen OpenStack-Mandantennamen ein.

Wenn Sie mehrere Endpoints mit unterschiedlichen OpenStack-Mandanten einrichten, erstellen Sie für jeden Mandanten Reservierungsrichtlinien. Dadurch wird sichergestellt, dass Maschinen für die entsprechenden Mandantenressourcen bereitgestellt werden.

- 7 (Optional) Fügen Sie benutzerdefinierte Eigenschaften hinzu.

8 Klicken Sie auf **OK**.

#### Weiter

Fügen Sie die Computing-Ressourcen von Ihrem Endpoint zu einer Fabric-Gruppe hinzu. Siehe [Erstellen einer Fabric-Gruppe](#).

## Importieren einer Liste von Endpoints

Das Importieren einer CSV-Datei mit Endpoints kann effizienter sein als das einzelne Hinzufügen von Endpoints mithilfe der vRealize Automation-Konsole.

#### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **laaS-Administrator** an.
- Speichern Sie die Anmeldedaten für Ihre Endpoints.
- Bereiten Sie eine Endpoint-CSV-Datei für den Import vor.

#### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Klicken Sie auf **Endpoints importieren**.
- 3 Klicken Sie auf **Durchsuchen**.
- 4 Suchen Sie nach der CSV-Datei, die Ihre Endpoints enthält.
- 5 Klicken Sie auf **Öffnen**.

Eine CSV-Datei wird geöffnet, die eine Liste von Endpoints im folgenden Format enthält:

```
InterfaceType,Address,Credentials,Name,Description
vCloud,https://abxpoint2vco,svc-admin,abxpoint2vco,abxpoint
```

- 6 Klicken Sie auf **Importieren**.

Ihre Endpoints können Sie über die vRealize Automation-Konsole bearbeiten und verwalten.

#### Vorbereiten einer Endpoint-CSV-Datei für den Import

Anstatt Endpoints einzeln unter Verwendung der vRealize Automation-Konsole hinzuzufügen, können Sie eine Liste von Endpoints importieren, indem Sie eine CSV-Datei hochladen.

Die CSV-Datei muss eine Kopfzeile mit den erwarteten Feldern enthalten. Bei den Feldern ist die Groß-/Kleinschreibung zu beachten, und sie müssen sich in einer bestimmten Reihenfolge befinden. Sie können mehrere Endpoints verschiedener Arten mit derselben CSV-Datei hochladen. Für vCloud Director werden Systemadministratorkonten anstatt Organisationsadministrator-Endpoints importiert.

**Tabelle 3-3. Felder der CSV-Datei und deren Reihenfolge für das Importieren von Endpoints**

Feld	Beschreibung
InterfaceType	(Erforderlich) Sie können mehrere Endpoint-Typen in einer einzelnen Datei hochladen. <ul style="list-style-type: none"> <li>■ vCloud Air</li> <li>■ vCloud Director</li> <li>■ vRealize Orchestrator</li> <li>■ vSphere</li> <li>■ Amazon EC2</li> <li>■ OpenStack</li> <li>■ NetAppOnTap</li> <li>■ SCVMM</li> <li>■ KVM</li> </ul>
Address	(Erforderlich für alle Schnittstellentypen außer Amazon) URL für den Endpoint. Informationen über das erforderliche Format für Ihren Plattfortmtypen finden Sie in der entsprechenden Vorgehensweise zum Erstellen eines Endpoints für Ihre Plattform.
Credentials	(Erforderlich) Name für die Benutzeranmeldedaten, als Sie sie in vRealize Automation gespeichert haben.
Name	(Erforderlich) Geben Sie einen Namen für den Endpoint ein. Für OpenStack wird die Adresse als der Standardname verwendet.
Description	(Optional) Geben Sie eine Beschreibung für den Endpoint ein.
OpenstackProject	(Nur für OpenStack erforderlich) Geben Sie den Projektnamen für den Endpoint ein.

## Fehlerbehebung – Verbundener vSphere -Endpoint kann nicht gefunden werden

Wenn die Datenerfassung bei einem vSphere-Endpoint fehlschlägt, geschieht dies häufig, weil Proxy-Name und Endpoint-Name nicht übereinstimmen.

### Problem

Die Datenerfassung bei einem vSphere-Endpoint schlägt fehl. Die Protokollmeldungen geben einen Fehler ähnlich dem folgenden zurück:

Diese Ausnahme wurde gefunden: Der verbundene vCenter-Endpoint kann nicht gefunden werden.

### Ursache

Der Endpoint-Name, den Sie in vRealize Automation konfigurieren, muss mit dem Endpoint-Namen übereinstimmen, der bei der Installation für den vSphere-Proxy-Agent angegeben wurde. Die Datenerfassung bei einem vSphere-Endpoint schlägt fehl, wenn der Endpoint-Name und der Name des Proxy-Agents nicht übereinstimmen. Bis ein Endpoint mit einem übereinstimmenden Namen konfiguriert ist, geben die Protokollmeldungen einen Fehler ähnlich dem folgenden zurück:

Diese Ausnahme wurde gefunden: Der verbundene Endpoint '*expected endpoint name*' kann nicht gefunden werden.

## Lösung

- 1 Wählen Sie **Infrastruktur > Überwachung > Protokoll** aus.
- 2 Suchen Sie nach einer Fehlermeldung „Verbundener Endpoint kann nicht gefunden werden“.

Beispiel:

Diese Ausnahme wurde gefunden: Der verbundene Endpoint '*expected endpoint name*' kann nicht gefunden werden.

- 3 Bearbeiten Sie Ihren vSphere-Endpoint, sodass sein Name mit dem erwarteten Endpoint-Namen übereinstimmt, der in der Protokollmeldung angezeigt wird.
  - a Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
  - b Klicken Sie zum Bearbeiten auf den Namen des Endpoints.
  - c Geben Sie im Textfeld **Name** den erwarteten Endpoint-Namen ein.
  - d Klicken Sie auf **OK**.

Der Proxy-Agent kann mit dem Endpoint kommunizieren und die Datenerfassung ist erfolgreich.

## Fehlerbehebung beim Suchen der vCloud Air -Verwaltungs-URL für ein virtuelles Datencenter einer Organisation

Zum Erstellen eines vCloud Air-Endpoints müssen Sie vRealize Automation mit der erforderlichen vCloud Air-Region und die Verwaltungs-URL bereitstellen.

### Lösung

Die vCloud Air-Verwaltungs-URL ist auch die URL des vCloud Director-Servers, der zum Verwalten eines bestimmten virtuellen Datencenters (Virtual Data Center, vDC) verwendet wird. Sie können mit den Regionsinformationen und der Verwaltungs-URL den vCloud Air-Endpoint konfigurieren.

Suchen Sie die Verwaltungs-URL für jedes Region-vDC aus der vCloud Air-Konsole.

### Vorgehensweise

- 1 Melden Sie sich bei der vCloud Air-Konsole als Benutzer mit Administratorrechten an.
- 2 Wählen Sie über das vCloud Air-Dashboard Ihr virtuelles Datencenter aus.
- 3 Klicken Sie auf den Link zum Anzeigen einer URL für das virtuelle Datencenter zur Verwendung in API-Befehlen.

Beispielsweise <https://mycompany.com:443/cloud/org/vCloudAutomation/>.

Die Verwaltungs-URL, die Sie für vRealize Automation bereitstellen müssen, ist der Host- und Portabschnitt der API-Befehls-URL, und die Region ist der Abschnitt der URL, die `cloud/org/` folgt. Im angegebenen Beispiel ist die Verwaltungs-URL `https://mycompany.com:443` und die Region `vCloudAutomation`.

## Erstellen einer Fabric-Gruppe

Sie können Infrastrukturressourcen zu Gruppen zusammenfassen und mindestens einem Fabric-Administrator die Verwaltung der Ressourcen in der Fabric-Gruppe zuweisen.

Fabric-Gruppen sind für virtuelle und Cloud-Endpoints erforderlich. Sie können die Rolle des Fabric-Administrators mehreren Benutzern zuweisen, indem Sie entweder mehrere Benutzer einzeln nacheinander hinzufügen oder aber eine Identitätsquellen-Gruppe oder benutzerdefinierte Gruppe als Fabric-Administrator wählen.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **laaS-Administrator** an.
- Erstellen Sie mindestens einen Endpoint.

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Fabric-Gruppen** aus.
- 2 Klicken Sie auf **Neue Fabric-Gruppe**.
- 3 Geben Sie im Textfeld **Name** einen Namen ein.
- 4 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.
- 5 Geben Sie in das Textfeld **Fabric-Administratoren** einen Benutzer- oder Gruppennamen ein und drücken Sie die Eingabetaste.

Wiederholen Sie diesen Schritt, um mehrere Benutzer oder Gruppen zu der Rolle hinzuzufügen.

- 6 Klicken Sie auf mindestens eine **Computing-Ressource**, die zu Ihrer Fabric-Gruppe hinzugefügt werden soll.

Während der Datenerfassung erkannt werden nur Ressourcen erkannt, die auf den Clustern vorhanden sind, welche Sie für Ihre Fabric-Gruppe auswählen. Beispielsweise werden nur diejenigen Vorlagen erkannt, die auf den ausgewählten Clustern vorhanden sind, und auch nur diese Vorlagen sind für das Klonen in den Reservierungen verfügbar, die Sie für Business-Gruppen erstellen.

- 7 Klicken Sie auf **OK**.

Fabric-Administratoren können nun Maschinenpräfixe konfigurieren. Siehe [Konfigurieren von Maschinenpräfixen](#).

Benutzer, die aktuell an der vRealize Automation-Konsole angemeldet sind, müssen sich abmelden und wieder an der vRealize Automation-Konsole anmelden, bevor sie auf die Seiten navigieren können, auf die ihnen Zugriff gewährt wurde.

## Konfigurieren von Maschinenpräfixen

Sie können Maschinenpräfixe erstellen, die für die Erstellung von Namen für Maschinen verwendet werden, die über vRealize Automation bereitgestellt werden. Ein Maschinenpräfix ist bei der Definition einer Maschinenkomponente auf der Design-Arbeitsfläche des Blueprints erforderlich.

Ein Präfix ist ein Basisname, auf den eine bestimmte Anzahl von Ziffern folgen muss. Wenn alle Ziffern verwendet werden, führt vRealize Automation ein Rollback auf die erste Zahl durch.

Maschinenpräfixe unterliegen folgenden Einschränkungen:

- Enthalten nur die ASCII-Buchstaben von A bis Z, wobei zwischen Groß- und Kleinschreibung unterschieden wird, die Ziffern von 0 bis 9 und Bindestriche (-).
- Beginnen nicht mit einem Bindestrich.
- Es dürfen keine anderen Symbole, Interpunktionszeichen oder Leerzeichen verwendet werden.
- Überschreiten nicht die Länge von 15 Zeichen, einschließlich der Zahlen, um dem Windows-Grenzwert von 15 Zeichen in Hostnamen zu entsprechen.

Längere Hostnamen werden bei der Bereitstellung der Maschine gekürzt und aktualisiert, wenn die nächste Datenerfassung ausgeführt wird. Bei WIM-Bereitstellungen werden die Namen jedoch nicht gekürzt, sondern die Bereitstellung schlägt fehl, wenn der angegebene Name mehr als 15 Zeichen umfasst.

- vRealize Automation unterstützt nicht mehrere virtuelle Maschinen mit demselben Namen in einer einzelnen Instanz. Wenn Sie eine Namenskonvention auswählen, bei der es zu einer Überschneidung von Maschinennamen kommt, stellt vRealize Automation die Maschine mit dem redundanten Namen nicht bereit. Wenn möglich überspringt vRealize Automation den Namen, der bereits verwendet wird, und generiert einen neuen Maschinennamen mit dem angegebenen Maschinenpräfix. Wenn kein eindeutiger Name generiert werden kann, schlägt die Bereitstellung fehl.

## Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.

## Vorgehensweise

- 1 Klicken Sie auf **Infrastruktur > Administration > Maschinenpräfixe**.
- 2 Klicken Sie auf **Neu**.
- 3 Geben Sie in das Textfeld **Name** das Maschinenpräfix ein.
- 4 Geben Sie in das Textfeld **Anzahl der Ziffern** die Anzahl der laufenden Ziffern ein.
- 5 Geben Sie in das Textfeld **Nächste Nummer** die laufende Startnummer ein.
- 6 Klicken Sie auf das Symbol **Speichern** (✓).

Mandantenadministratoren können Business-Gruppen erstellen, sodass Benutzer für das Anfordern von Maschinen auf vRealize Automation zugreifen können.

## Verwalten von Schlüsselpaaren

Schlüsselpaare werden für die Bereitstellung und Verbindung zu einer Cloudinstanz verwendet. Ein Schlüsselpaar wird zur Entschlüsselung von Windows-Kennwörtern oder zur Anmeldung bei einer Linux-Maschine verwendet.

Schlüsselpaare sind für die Bereitstellung mit Amazon AWS erforderlich. Für Red Hat OpenStack sind Schlüsselpaare optional.

Vorhandene Schlüsselpaare werden als Teil der Datenerfassung importiert, wenn Sie einen Cloud-Endpoint hinzufügen. Ein Fabric-Administrator kann auch unter Verwendung der vRealize Automation-Konsole Schlüsselpaare erstellen und verwalten. Wenn Sie ein Schlüsselpaar aus der vRealize Automation-Konsole löschen, wird es auch aus dem Cloud-Service-Konto gelöscht.

Zusätzlich zu der manuellen Verwaltung von Schlüsselpaaren können Sie vRealize Automation für das automatische Erstellen von Schlüsselpaaren per Maschine oder Business-Gruppe konfigurieren.

- Ein Fabric-Administrator kann die automatische Erstellung von Schlüsselpaaren auf einer Reservierungsebene konfigurieren.
- Wird das Schlüsselpaar auf der Blueprint-Ebene gesteuert, muss der Fabric-Administrator **Nicht angegeben** auf der Reservierung auswählen.
- Ein Mandantenadministrator oder Business-Gruppenmanager kann die automatische Erstellung von Schlüsselpaaren auf einer Blueprint-Ebene konfigurieren.
- Wenn die Schlüsselpaarerstellung auf Reservierungsebene und Blueprint-Ebene konfiguriert wird, überschreibt die Reservierungseinstellung die Blueprint-Einstellung.

## Erstellen eines Schlüsselpaars

Mithilfe von vRealize Automation können Sie Schlüsselpaare für die Verwendung mit Endpoints erstellen.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.
- Erstellen Sie einen Cloud-Endpoint und fügen Sie Ihre Cloud-Computing-Ressource zu einer Fabric-Gruppe hinzu. Siehe [Auswählen eines Endpoint-Szenarios](#) und [Erstellen einer Fabric-Gruppe](#).

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Schlüsselpaare** aus.
- 2 Klicken Sie auf **Neu**.
- 3 Geben Sie im Textfeld **Name** einen Namen ein.
- 4 Wählen Sie aus dem Dropdown-Menü **Computing-Ressource** eine Cloud-Region aus.
- 5 Klicken Sie auf das Symbol **Speichern** (👍).

Das Schlüsselpaar kann verwendet werden, wenn die Spalte „Geheimer Schlüssel“ den Wert \*\*\*\*\* aufweist.

## Hochladen des privaten Schlüssels für ein Schlüsselpaar



Sie können den privaten Schlüssel für ein Schlüsselpaar im PEM-Format hochladen.



### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.
- Sie müssen bereits über ein Schlüsselpaar verfügen. Siehe [Erstellen eines Schlüsselpaars](#).

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Schlüsselpaare** aus.
- 2 Suchen Sie das Schlüsselpaar, für das Sie einen privaten Schlüssel hochladen möchten.
- 3 Klicken Sie auf das Symbol **Bearbeiten** ().
- 4 Verwenden Sie zum Hochladen des Schlüssels eine der folgenden Methoden:
  - Suchen Sie nach einer PEM-codierten Datei und klicken Sie auf **Hochladen**.
  - Fügen Sie den Text des privaten Schlüssels ein, der mit -----PRIVATER RSA-SCHLÜSSEL ANFANG----- beginnt und auf -----PRIVATER RSA-SCHLÜSSEL ENDE----- endet.
- 5 Klicken Sie auf das Symbol **Speichern** (.


## Exportieren des privaten Schlüssels aus einem Schlüsselpaar

Den privaten Schlüssel können Sie aus einem Schlüsselpaar in eine PEM-codierte Datei exportieren.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.
- Ein Schlüsselpaar mit einem privaten Schlüssel muss vorhanden sein. Siehe [Hochladen des privaten Schlüssels für ein Schlüsselpaar](#).

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Schlüsselpaare** aus.
- 2 Suchen Sie nach dem Schlüsselpaar, aus dem der private Schlüssel exportiert werden soll.
- 3 Klicken Sie auf das Symbol **Exportieren** (.
- 4 Navigieren Sie zu dem Speicherort, in dem die Datei gespeichert werden soll, und klicken Sie auf **Speichern**.

## Erstellen eines Netzwerkprofils

Ein Netzwerkprofil enthält IP-Informationen, wie z. B. Gateway, Subnetz und Adressbereich.

vRealize Automation verwendet vSphere-DHCP oder einen bestimmten IPAM-Anbieter, um den bereitgestellten Maschinen IP-Adressen zuzuweisen.

Sie können ein Netzwerkprofil erstellen, um einen verfügbaren Netzwerktyp zu definieren, einschließlich externer Netzwerkprofile und Vorlagen für On-Demand-NAT- (Network Address Translation) und geroutete On-Demand-Netzwerkprofile, die logische NSX-Switches und entsprechende RoutingEinstellungen für einen neuen Netzwerkpfad erstellen. Netzwerkprofile werden beim Hinzufügen von Netzwerkkomponenten zu einem Blueprint benötigt.

Netzwerkprofile werden verwendet, um bei der Bereitstellung von Maschinen Netzwerkeinstellungen zu konfigurieren. Mit Netzwerkprofilen wird außerdem die Konfiguration von NSX Edge-Geräten festgelegt, die bei der Bereitstellung von Maschinen erstellt werden. Beim Erstellen von Reservierungen und Blueprints geben Sie ein Netzwerkprofil an. In einer Reservierung können Sie ein Netzwerkprofil einem Netzwerkpfad zuweisen und jeden dieser Pfade für eine Maschinenkomponente in einem Blueprint angeben.

Ein Blueprint-Ersteller gibt ein geeignetes Netzwerkprofil an, wenn er Netzwerkkomponenten im Blueprint definiert. Sie können ein vorhandenes Netzwerkprofil und ein On-Demand-NAT- oder geroutetes On-Demand-Netzwerkprofil verwenden, während Sie Netzwerkadapter und Lastausgleichsdienste für die Bereitstellung von Maschinen definieren.

Netzwerkprofile unterstützen darüber hinaus IPAM-Drittanbieter (IP Address Management), wie z. B. Infoblox. Wenn Sie ein Netzwerkprofil für IPAM konfigurieren, können die bereitgestellten Maschinen die IP-Adressdaten sowie zugehörige Informationen, wie z. B. DNS und Gateway, aus der konfigurierten IPAM-Lösung abrufen. Sie können ein externes IPAM-Paket für einen Drittanbieter (z. B. Infoblox) verwenden, um einen IPAM-Endpoint zur Verwendung mit einem externen Netzwerkprofil zu definieren.

Sie können die IP-Adressbereiche angeben, die von Netzwerkprofilen verwendet werden können. Jede IP-Adresse in den angegebenen Bereichen, die einer Maschine zugeteilt sind, werden wieder für die erneute Zuweisung freigegeben, wenn die Maschine gelöscht wird.

Sie können ein Netzwerkprofil erstellen, um einen statischen IP-Adressbereich zu definieren, der Maschinen zugewiesen werden kann. Netzwerkprofile können bestimmten Netzwerkpfaden in einer Reservierung zugewiesen werden. Bestimmten Typen von Maschinenkomponenten, wie z. B. vSphere, können Sie ein Netzwerkprofil zuweisen, wenn Sie Blueprints erstellen oder bearbeiten.

Bei der Bereitstellung von virtuellen Maschinen durch Klonen oder mithilfe der Kickstart/autoYaST-Bereitstellung kann der anfordernde Maschinenbesitzer statische IP-Adressen aus einem vordefinierten Bereich zuweisen.

Wenn Sie ein Netzwerkprofil in einer Reservierung und einem Blueprint angeben, hat der Blueprint-Wert Vorrang. Wenn Sie beispielsweise ein Netzwerkprofil im Blueprint mithilfe der benutzerdefinierten Eigenschaft `VirtualMachine.NetworkN.ProfileName` und in einer vom Blueprint verwendeten Reservierung angeben, hat das im Blueprint angegebene Netzwerkprofil Vorrang. Wenn die benutzerdefinierte Eigenschaft jedoch nicht im Blueprint verwendet wird und Sie ein Netzwerkprofil für eine Maschinen-NIC auswählen, verwendet vRealize Automation den Netzwerkreservierungspfad für die Maschinen-NIC, für die das Netzwerkprofil angegeben ist.

**Tabelle 3-4. Verfügbare Netzwerktypen für ein vRealize Automation -Netzwerkprofil**

Netzwerktyp	Beschreibung
Extern	<p>Vorhandene Netzwerke, die auf dem vSphere-Server konfiguriert sind. Dies ist die externe Komponente der NAT- und gerouteten Netzwerktypen. Ein externes Netzwerkprofil kann einen statischen IP-Adressbereich definieren, der im externen Netzwerk verfügbar ist.</p> <p>Sie können auch IP-Bereiche verwenden, die aus dem im Lieferumfang von VMware enthaltenen internen IPAM-Anbieter oder einer externen IPAM-Anbieterlösung (wie z. B. Infoblox IPAM) abgerufen werden, die Sie in vRealize Orchestrator importiert und registriert haben.</p> <p>Ein externes Netzwerkprofil mit einem statischen IP-Bereich ist die Voraussetzung für NAT- und geroutete Netzwerke.</p>
NAT	<p>Diese Netzwerke werden während der Bereitstellung erstellt. Hierbei handelt es sich um Netzwerke, die einen IP-Adressensatz für die externe Kommunikation und einen anderen IP-Adressensatz für die interne Kommunikation verwenden. Bei 1:1-NAT-Netzwerken wird jeder virtuellen Maschine eine externe IP-Adresse aus dem externen Netzwerkprofil und eine interne IP-Adresse aus dem NAT-Netzwerkprofil zugewiesen. Bei 1:n-NAT-Netzwerken verwenden alle Maschinen eine einzige IP-Adresse aus dem externen Netzwerkprofil für die externe Kommunikation.</p> <p>Ein NAT-Netzwerkprofil definiert lokale und externe Netzwerke, die eine Übersetzungstabelle für die wechselseitige Kommunikation verwenden.</p>
Weitergeleitet	<p>Diese Netzwerke werden während der Bereitstellung erstellt. Sie repräsentieren einen routingfähigen IP-Bereich, der auf Subnetze aufgeteilt ist, die mittels DLR (Distributed Logical Router) miteinander verknüpft sind. Jedem neuen gerouteten Netzwerk wird das nächste verfügbare Subnetz zugewiesen und es wird mit anderen gerouteten Netzwerken verbunden, die dasselbe Netzwerkprofil verwenden. Die virtuellen Maschinen, die mit gerouteten Netzwerken bereitgestellt werden, die dasselbe geroutete Netzwerkprofil aufweisen, können miteinander und mit dem externen Netzwerk kommunizieren.</p> <p>Ein geroutetes Netzwerkprofil definiert einen routingfähigen Bereich und verfügbare Subnetze.</p> <p>Weitere Informationen über Distributed Logical Router finden Sie im <i>NSX-Administratorhandbuch</i>.</p>

## Zuweisen eines statischen IP-Adressbereichs mithilfe von Netzwerkprofilen

Sie können mithilfe von Netzwerkprofilen virtuellen Maschinen, die durch Klonen bereitgestellt wurden, bzw. Cloud-Maschinen, die durch OpenStack bereitgestellt wurden, statische IP-Adressen aus einem vordefinierten Bereich zuweisen. Verwenden Sie dafür Linux kickstart oder autoYaST (für virtuelle Maschinen) bzw. kickstart (für Cloud-Maschinen).

vRealize Automation verwendet für die Zuweisung von IP-Adressen an bereitgestellte Maschinen standardmäßig Dynamic Host Configuration Protocol (DHCP).

Sie können Netzwerkprofile erstellen, um einen Bereich statischer IP-Adressen zu definieren, die Sie den Maschinen zuweisen können. Sie können bestimmten Netzwerkpfaden in einer Reservierung Netzwerkprofile zuweisen. Maschinen, die durch Klonen oder kickstart bzw. autoYaST bereitgestellt werden und mit einem Netzwerkpfad mit einem zugehörigen Netzwerkprofil verknüpft sind, werden mit einer zugewiesenen statischen IP-Adresse bereitgestellt. Für die Bereitstellung mit einer statischen IP-Adressenzuweisung müssen Sie eine Anpassungsspezifikation verwenden.

Sie können ein Netzwerkprofil einer vSphere-Maschinenkomponente in einem Blueprint zuweisen, indem Sie eine vorhandene, On-Demand-NAT- oder geroutete On-Demand-Netzwerkkomponente zur Design-Arbeitsfläche hinzufügen und ein Netzwerkprofil auswählen, mit dem die vSphere-Maschinenkomponente verbunden werden soll. Sie können Netzwerkprofilen auch Blueprints zuweisen, indem Sie die benutzerdefinierte Eigenschaft `VirtualMachine.NetworkN.ProfileName` verwenden, bei der *N* den Netzwerkbezeichner darstellt.

Optional können Sie den bereitgestellten internen VMware-IPAM- oder einen registrierten externen IPAM-Dienstanbieter verwenden, um IP-Adressen zu beziehen und zu konfigurieren. Informationen zu Anforderungen für externe IPAM-Anbieter finden Sie unter [Checkliste zum Vorbereiten der Unterstützung eines externen IPAM-Anbieters](#).

Wenn Sie einen externen IPAM-Endpoint in einem Netzwerkprofil auswählen, ruft vRealize Automation IP-Bereiche vom registrierten Endpoint-Typ für den externen IPAM-Anbieter ab, wie beispielsweise Infoblox. Anschließend werden IP-Werte von diesem Endpoint zugeordnet.

Wenn Sie ein Netzwerkprofil in einer Reservierung und einem Blueprint angeben, hat der Blueprint-Wert Vorrang. Wenn Sie beispielsweise ein Netzwerkprofil im Blueprint mithilfe der benutzerdefinierten Eigenschaft `VirtualMachine.NetworkN.ProfileName` und in einer vom Blueprint verwendeten Reservierung angeben, hat das im Blueprint angegebene Netzwerkprofil Vorrang. Wenn die benutzerdefinierte Eigenschaft jedoch nicht im Blueprint verwendet wird und Sie ein Netzwerkprofil für eine Maschinen-NIC auswählen, verwendet vRealize Automation den Netzwerkreservierungspfad für die Maschinen-NIC, für die das Netzwerkprofil angegeben ist.

Wenn Sie eine Maschine mit einer statischen IP-Adresse löschen, wird dessen IP-Adresse für die Verwendung für andere Maschinen verfügbar gemacht. Nicht verwendete Adressen sind möglicherweise nicht sofort verfügbar, nachdem die Maschinen, die diese verwendet haben, gelöscht wurden, da der Vorgang zur Rückforderung statischer IP-Adressen alle 30 Minuten ausgeführt wird. Wenn IP-Adressen im Netzwerkprofil nicht verfügbar sind, können Maschinen nicht mit statischer IP-Zuweisung auf dem zugeordneten Netzwerkpfad bereitgestellt werden.

## Grundlegendes zum CSV-Dateiformat für den Import von Netzwerkprofil-IP-Adressen

Mithilfe einer ordnungsgemäß formatierten CSV-Datei können Sie IP-Adressbereiche in ein vRealize Automation-Netzwerkprofil importieren.

Die Einträge in der CSV-Datei müssen folgendes Format aufweisen.

CSV-Feld	Beschreibung
<code>ip_address</code>	Eine IP-Adresse im IPv4-Format.
<code>machine_name</code>	Der Name einer verwalteten Maschine in vRealize Automation. Wenn dieses Feld leer ist, wird standardmäßig kein Name verwendet. Wenn dieses Feld leer ist, kann das Feld <code>status</code> nicht den Wert „Zugewiesen“ aufweisen.
<code>status</code>	Zugewiesen oder Nicht zugewiesen, Groß-/Kleinschreibung beachten. Wenn dieses Feld leer ist, lautet der Standardwert „Nicht zugewiesen“. Wenn der Status „Zugewiesen“ lautet, darf das Feld <code>machine_name</code> nicht leer sein.
<code>NIC_offset</code>	Eine nicht negative ganze Zahl.

Mit dem folgenden Beispieleintrag wird kein NIC-Versatz festgelegt:

```
100.10.100.1,mymachine01,Unallocated
```

### Importieren von IP-Adressen aus einer CSV-Datei in ein Netzwerkprofil

Sie können einem Netzwerkprofilbereich IP-Adressen hinzufügen, indem Sie eine ordnungsgemäß formatierte CSV-Datei importieren. Darüber hinaus können Sie die Adressen im Netzwerkprofilbereich ändern, indem Sie den Bereich in vRealize Automation bearbeiten oder eine geänderte oder andere CSV-Datei importieren.

Sie können die IP-Adressen in einem Netzwerkprofilbereich durch den Import aus einer CSV-Datei oder durch die manuelle Eingabe von Werten hinzufügen oder ändern. Sie können aber auch IP-Adressen von einem externen IPAM-Anbieter beziehen.

- Importieren Sie zunächst einen Bereich von IP-Adressen in ein vRealize Automation-Netzwerkprofil.
- Wenden Sie die importierten Werte an, um den ersten benannten Netzwerkbereich im Netzwerkprofil zu erstellen.
- Löschen Sie eine oder mehrere IP-Adressen aus dem Netzwerkbereich. vRealize Automation
- Importieren Sie eine geänderte oder andere CSV-Datei, um festzustellen, wie sich die Netzwerkbereichswerte ändern.

Für Netzwerkprofile, die einen externen IPAM-Endpoint-Typ verwenden, ist die Option **Aus CSV importieren** nicht vorhanden, da die IP-Adressen vom externen IPAM-Anbieter und nicht von vRealize Automation verwaltet werden.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.
- Erstellen Sie eine CSV-Datei, die IP-Adressen enthält, für den Import in einen Netzwerkbereich. Siehe [Erstellen eines externen Netzwerkprofils mithilfe eines externen IPAM-Anbieters](#) und [Grundlegendes zum CSV-Dateiformat für den Import von Netzwerkprofil-IP-Adressen](#).

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Netzwerkprofile** aus.
- 2 Klicken Sie auf **Neu** und wählen Sie aus dem Dropdown-Menü einen Netzwerkprofiltyp aus.  
Wählen Sie in diesem Beispiel *Extern* aus.
- 3 Geben Sie **Mein Netzwerkprofil mit CSV** in das Textfeld **Name** ein.
- 4 Geben Sie **Testen der Netzwerkbereich-IP-Adressen mit CSV** in das Textfeld **Beschreibung** ein.

Die Option zum Importieren aus einer CSV-Datei betrifft Einstellungen auf den Registerkarten **Netzwerkbereiche** und **IP-Adressen**. Befassen wir uns kurz mit den ersten beiden Registerkarten für die Eingabe von grundlegenden Informationen zum Netzwerkprofil.

- 5 Wählen Sie optional einen konfigurierten IPAM-Endpoint aus, falls ein solcher Endpoint verfügbar ist. Überspringen Sie andernfalls diesen Schritt.
- 6 Geben Sie einen entsprechenden Wert für die IP-Adresse in die Textfelder **Subnetzmaske** und **Gateway** ein.
- 7 Klicken Sie auf die Registerkarte **DNS**.
- 8 Geben Sie entsprechende Informationen wie beispielsweise das DNS-Suffix ein und klicken Sie auf die Registerkarte **Netzwerkbereiche**.

Die Option **Aus CSV importieren** ist verfügbar, wenn Sie auf die Registerkarte **Netzwerkbereiche** klicken.

- 9 Klicken Sie auf **Neu**, um einen neuen Netzwerkbereichsnamen und einen IP-Adressbereich manuell einzugeben, oder klicken Sie auf **Aus CSV importieren**, um die IP-Adressinformationen aus einer ordnungsgemäß formatierten CSV-Datei zu importieren.

- Klicken Sie auf **Hinzufügen**.

- a Geben Sie in das Textfeld **Netzwerkbereich** einen neuen Namen ein.
- b Geben Sie eine Beschreibung für den Netzwerkbereich ein.
- c Geben Sie in das Textfeld **IP-Startadresse** die IP-Startadresse des Bereichs ein.
- d Geben Sie in das Textfeld **IP-Endadresse** die IP-Endadresse des Bereichs ein.

- Klicken Sie auf **Aus CSV importieren**.

- a Navigieren Sie zu der CSV-Datei und wählen Sie sie aus, oder ziehen Sie die CSV-Datei in das Dialogfeld **Aus CSV importieren**.

Eine Zeile in der CSV-Datei hat das Format *ip\_address, machine\_name, status, NIC offset*.  
Beispiel:

```
100.10.100.1,mymachine01,Unallocated
```

CSV-Feld	Beschreibung
ip_address	Eine IP-Adresse im IPv4-Format.
machine_name	Der Name einer verwalteten Maschine in vRealize Automation. Wenn dieses Feld leer ist, wird standardmäßig kein Name verwendet. Wenn dieses Feld leer ist, kann das Feld status nicht den Wert „Zugewiesen“ aufweisen.
status	Zugewiesen oder Nicht zugewiesen, Groß-/Kleinschreibung beachten. Wenn dieses Feld leer ist, lautet der Standardwert „Nicht zugewiesen“. Wenn der Status „Zugewiesen“ lautet, darf das Feld machine_name nicht leer sein.
NIC_offset	Eine nicht negative ganze Zahl.

- b Klicken Sie auf **Übernehmen**.

**10 Klicken Sie auf OK.**

Der IP-Bereichsname wird in der Liste „Definierte Bereiche“ angezeigt. Die IP-Adressen in dem Bereich werden in der Liste „Definierte IP-Adressen“ angezeigt.

Die hochgeladenen IP-Adressen werden auf der Seite **IP-Adressen** angezeigt, wenn Sie auf **Übernehmen** klicken oder wenn Sie das Netzwerkprofil speichern und anschließend bearbeiten.

**11 Klicken Sie auf die Registerkarte IP-Adressen**, um die IP-Adressdaten für den angegebenen Adressbereich anzuzeigen.

Wenn Sie die IP-Adressinformationen aus einer CSV-Datei importiert haben, wird der Bereichsname als *Aus CSV importiert* generiert.

**12 (Optional) Wählen Sie aus dem Dropdown-Menü **Netzwerkbereich** IP-Adressinformationen aus**, um die Einträge für die IP-Adresse zu filtern.

Sie können Informationen zu allen definierten Netzwerkbereichen, zu den aus einer CSV-Datei importierten Netzwerkbereichen oder zu einem benannten Netzwerkbereich anzeigen. Die Details beinhalten die IP-Startadresse, den Maschinennamen, Datum und Uhrzeit der letzten Änderung sowie den IP-Status.

**Weiter**

Wenn Sie IP-Adressen erneut aus einer CSV-Datei importieren, werden die vorherigen IP-Adressen durch die Informationen aus der importierten CSV-Datei ersetzt.

**Erstellen eines externen Netzwerkprofils**

Sie können ein externes Netzwerkprofil erstellen, um Netzwerkeigenschaften und einen Bereich mit statischen IP-Adressen zu definieren, die bei Verwendung eines vorhandenen Netzwerks zur Bereitstellung von Maschinen eingesetzt werden sollen.

Sie können optional den im Lieferumfang enthaltenen internen IPAM-Anbieter oder das Paket eines externen IPAM-Drittanbieters (z. B. Infoblox) verwenden, das Sie in vRealize Orchestrator importiert, konfiguriert und registriert haben.

Sie können im Netzwerkprofil mindestens einen Netzwerkbereich mit statischen IP-Adressen für die Bereitstellung einer Maschine konfigurieren. Wenn Sie keinen Bereich angeben, können Sie ein Netzwerkprofil als Netzwerk-Reservierungsrichtlinie zur Auswahl eines Reservierungs-Netzwerkpfads für die Netzwerkkarte einer virtuellen Maschine (vNIC) verwenden.

Informationen zum Erstellen eines externen Netzwerkprofils und Verwenden des Endpoints eines externen IPAM-Anbieters finden Sie unter [Erstellen eines externen Netzwerkprofils mithilfe eines externen IPAM-Anbieters](#).

**Vorgehensweise****1 [Angaben von externen Netzwerkprofilinformationen](#)**

In einem externen Netzwerkprofil werden Netzwerkeigenschaften und Einstellungen für ein vorhandenes Netzwerk angegeben. Ein externes Netzwerkprofil ist für NAT- und geroutete Netzwerkprofile erforderlich.

## 2 Konfigurieren von IP-Bereichen für externe Netzwerkprofile

Sie können im Netzwerkprofil mindestens einen Netzwerkbereich mit statischen IP-Adressen für die Bereitstellung einer Maschine konfigurieren. Wenn Sie keinen Bereich angeben, können Sie ein Netzwerkprofil als Netzwerk-Reservierungsrichtlinie zur Auswahl eines Reservierungs-Netzwerkpfads für die Netzwerkkarte einer virtuellen Maschine (vNIC) verwenden.

### Angeben von externen Netzwerkprofilinformationen

In einem externen Netzwerkprofil werden Netzwerkeigenschaften und Einstellungen für ein vorhandenes Netzwerk angegeben. Ein externes Netzwerkprofil ist für NAT- und geroutete Netzwerkprofile erforderlich.

Informationen zum Erstellen eines externen Netzwerkprofils durch Abrufen von IPAM-Adressinformationen von einem registrierten IPAM-Endpoint eines Drittanbieters, wie z. B. Infoblox, finden Sie unter [Checkliste zum Vorbereiten der Unterstützung eines externen IPAM-Anbieters](#) und [Erstellen eines externen Netzwerkprofils mithilfe eines externen IPAM-Anbieters](#). Erstellen Sie anhand des folgenden Verfahrens ein Netzwerkprofil mithilfe des VMware-internen IPAM-Endpoints.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Netzwerkprofile** aus.
- 2 Klicken Sie auf **Neu** und wählen Sie **Vorhanden** oder **Extern** aus dem Dropdown-Menü aus.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 (Optional) Übernehmen Sie den vorgegebenen internen **VMware**-IPAM-Endpoint im Dropdown-Menü **IPAM-Endpoint**.
- 5 Geben Sie eine IP-Subnetzmaske in das Textfeld **Subnetzmaske** ein.  
Beispielsweise 255.255.0.0.
- 6 Geben Sie eine Adresse für ein Edge- oder geroutetes Gateway in das Textfeld **Gateway** ein.
- 7 Klicken Sie auf die Registerkarte **DNS**.
- 8 Geben Sie bei Bedarf DNS- und WINS-Werte ein.

Die DNS- und WINS-Felder sind bei Verwendung eines internen IPAM-Endpoints optional. Wenn Sie einen externen IPAM-Endpoint verwenden, werden die DNS- und WINS-Werte vom externen IPAM-Anbieter bereitgestellt.

- a (Optional) Geben Sie einen Wert für **Primärer DNS** ein.
- b (Optional) Geben Sie einen Wert für **Sekundärer DNS** ein.
- c (Optional) Geben Sie einen Wert für **DNS-Suffix** ein.

Das DNS-Suffix wird bei der Registrierung und Auflösung von DNS-Namen verwendet.

- d (Optional) Geben Sie einen Wert für **DNS-Suchsuffix** ein.



- e (Optional) Geben Sie einen Wert für **Bevorzugter WINS** ein.
- f (Optional) Geben Sie einen Wert für **Alternativer WINS** ein.

## Weiter

Sie können IP-Bereiche für statische IP-Adressen konfigurieren. Siehe [Konfigurieren von IP-Bereichen für externe Netzwerkprofile](#).

## Konfigurieren von IP-Bereichen für externe Netzwerkprofile

Sie können im Netzwerkprofil mindestens einen Netzwerkbereich mit statischen IP-Adressen für die Bereitstellung einer Maschine konfigurieren. Wenn Sie keinen Bereich angeben, können Sie ein Netzwerkprofil als Netzwerk-Reservierungsrichtlinie zur Auswahl eines Reservierungs-Netzwerkpfads für die Netzwerkkarte einer virtuellen Maschine (vNIC) verwenden.

Wenn für ein externes Netzwerkprofil keine IP-Bereiche definiert sind, können Sie damit angeben, welches Netzwerk für eine virtuelle Netzwerkkarte (vNIC) ausgewählt wird. Wenn Sie das vorhandene Netzwerkprofil in einem gerouteten oder NAT-Netzwerkprofil verwenden, muss dieses Profil mindestens einen statischen IP-Bereich aufweisen.

Sie können Werte für IP-Bereiche manuell anhand einer importierten CSV-Datei oder durch Verwendung von IP-Adressen definieren, die von einem externen IPAM-Anbieter bereitgestellt werden.

## Voraussetzungen

[Angaben von externen Netzwerkprofilinformationen](#).

## Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Netzwerkbereiche**.
- 2 Klicken Sie auf **Neu**, um einen neuen Netzwerkbereichsnamen und einen IP-Adressbereich manuell einzugeben, oder klicken Sie auf **Aus CSV importieren**, um die IP-Adressinformationen aus einer ordnungsgemäß formatierten CSV-Datei zu importieren.
  - Klicken Sie auf **Hinzufügen**.
    - a Geben Sie in das Textfeld **Netzwerkbereich** einen neuen Namen ein.
    - b Geben Sie eine Beschreibung für den Netzwerkbereich ein.
    - c Geben Sie in das Textfeld **IP-Startadresse** die IP-Startadresse des Bereichs ein.
    - d Geben Sie in das Textfeld **IP-Endadresse** die IP-Endadresse des Bereichs ein.
  - Klicken Sie auf **Aus CSV importieren**.
    - a Navigieren Sie zu der CSV-Datei und wählen Sie sie aus, oder ziehen Sie die CSV-Datei in das Dialogfeld **Aus CSV importieren**.  
Eine Zeile in der CSV-Datei hat das Format *ip\_address, machine\_name, status, NIC offset*.  
Beispiel:

```
100.10.100.1,mymachine01,Unallocated
```

CSV-Feld	Beschreibung
ip_address	Eine IP-Adresse im IPv4-Format.
machine_name	Der Name einer verwalteten Maschine in vRealize Automation. Wenn dieses Feld leer ist, wird standardmäßig kein Name verwendet. Wenn dieses Feld leer ist, kann das Feld status nicht den Wert „Zugeteilt“ aufweisen.
status	Zugeteilt oder Nicht zugeteilt, Groß-/Kleinschreibung beachten. Wenn dieses Feld leer ist, lautet der Standardwert „Nicht zugeteilt“. Wenn der Status „Zugeteilt“ lautet, darf das Feld machine_name nicht leer sein.
NIC_offset	Eine nicht negative ganze Zahl.

b Klicken Sie auf **Übernehmen**.

### 3 Klicken Sie auf **OK**.

Der IP-Bereichsname wird in der Liste „Definierte Bereiche“ angezeigt. Die IP-Adressen in dem Bereich werden in der Liste „Definierte IP-Adressen“ angezeigt.

Die hochgeladenen IP-Adressen werden auf der Seite **IP-Adressen** angezeigt, wenn Sie auf **Übernehmen** klicken oder wenn Sie das Netzwerkprofil speichern und anschließend bearbeiten.

### 4 Klicken Sie auf die Registerkarte **IP-Adressen**, um die IP-Adressdaten für den angegebenen Adressbereich anzuzeigen.

Wenn Sie die IP-Adressinformationen aus einer CSV-Datei importiert haben, wird der Bereichsname als *Aus CSV importiert* generiert.

### 5 (Optional) Wählen Sie aus dem Dropdown-Menü **Netzwerkbereich** IP-Adressinformationen aus, um die Einträge für die IP-Adresse zu filtern.

Sie können Informationen zu allen definierten Netzwerkbereichen, zu den aus einer CSV-Datei importierten Netzwerkbereichen oder zu einem benannten Netzwerkbereich anzeigen. Die Details beinhalten die IP-Startadresse, den Maschinennamen, Datum und Uhrzeit der letzten Änderung sowie den IP-Status.

### 6 (Optional) Wählen Sie aus dem Dropdown-Menü **IP-Status** einen Statustyp aus, um die Einträge für die IP-Adresse herauszufiltern, die dem ausgewählten IP-Status entsprechen. Mögliche Stauseinstellungen sind „Zugeteilt“, „Nicht zugeteilt“, „Gelöscht“ und „Abgelaufen“.

Für IP-Adressen mit dem Status „Abgelaufen“ oder „Gelöscht“ können Sie auf **Rückforderung** klicken, um diese IP-Adressbereiche für die Zuteilung verfügbar zu machen. Sie müssen das Profil speichern, damit die Rückforderung wirksam wird. Adressen werden nicht sofort zurückgewonnen, weshalb die Statusspalte nicht sofort von „Abgelaufen“ oder „Gelöscht“ in „Zugeteilt“ geändert wird.

### 7 Klicken Sie auf **OK**, um das Netzwerkprofil abzuschließen.

Sie können einem Netzwerkpfad in einer Reservierung ein Netzwerkprofil zuweisen, während ein Blueprint-Architekt das Netzwerkprofil in einem Blueprint angeben kann. Wenn Sie ein externes Netzwerkprofil erstellt haben, können Sie dieses beim Erstellen eines NAT- oder eines gerouteten Netzwerkprofils verwenden.

## Erstellen eines externen Netzwerkprofils mithilfe eines externen IPAM-Anbieters

Mithilfe eines vorhandenen Netzwerks können Sie ein externes Netzwerkprofil erstellen, um Netzwerkeigenschaften und einen Bereich statischer IP-Adressen zu definieren, die bei der Bereitstellung von Maschinen verwendet werden sollen. Sie können einen externen IPAM-Anbieter verwenden, den Sie in vRealize Orchestrator importiert, konfiguriert und registriert haben.

Sie können ein externes Netzwerkprofil erstellen, das den Endpoint eines registrierten IPAM-Lösungsanbieters verwendet, um Einstellungen für Gateways, Subnetzmasken und DHCP/WINS abzurufen.

Sie können im Netzwerkprofil mindestens einen Netzwerkbereich mit statischen IP-Adressen für die Bereitstellung einer Maschine konfigurieren. Wenn Sie keinen Bereich angeben, können Sie ein Netzwerkprofil als Netzwerk-Reservierungsrichtlinie zur Auswahl eines Reservierungs-Netzwerkpfads für die Netzwerkkarte einer virtuellen Maschine (vNIC) verwenden.

Informationen zum Erstellen eines externen Netzwerkprofils ohne einen IPAM-Anbieter oder mithilfe des im Lieferumfang enthaltenen Endpoints des internen IPAM-Anbieters finden Sie unter [Erstellen eines externen Netzwerkprofils](#).

### Vorgehensweise

#### 1 [Angabe von Informationen zum externen Netzwerkprofil für einen registrierten IPAM-Endpoint](#)

In einem externen Netzwerkprofil werden Netzwerkeigenschaften und Einstellungen für ein vorhandenes Netzwerk angegeben. Ein externes Netzwerkprofil ist für NAT- und geroutete Netzwerkprofile erforderlich. Wenn Sie einen IPAM-Endpoint in vRealize Orchestrator registriert und konfiguriert haben, können Sie festlegen, dass IP-Adressinformationen von einem IPAM-Anbieter bereitgestellt werden.

#### 2 [Konfigurieren von IP-Bereichen für ein externes Netzwerkprofil für einen registrierten IPAM-Endpoint](#)

Sie können im Netzwerkprofil mindestens einen Netzwerkbereich mit statischen IP-Adressen für die Bereitstellung einer Maschine konfigurieren. Wenn Sie keinen Bereich angeben, können Sie ein Netzwerkprofil als Netzwerk-Reservierungsrichtlinie zur Auswahl eines Reservierungs-Netzwerkpfads für die Netzwerkkarte einer virtuellen Maschine (vNIC) verwenden.

### Weiter

Sie können einem Netzwerkpfad in einer Reservierung ein Netzwerkprofil zuweisen, während ein Blueprint-Architekt das Netzwerkprofil in einem Blueprint angeben kann. Wenn Sie ein externes Netzwerkprofil erstellt haben, können Sie dieses beim Erstellen eines On-Demand-NAT- oder gerouteten On-Demand-Netzwerkprofils verwenden.

### Angeben von Informationen zum externen Netzwerkprofil für einen registrierten IPAM-Endpoint

In einem externen Netzwerkprofil werden Netzwerkeigenschaften und Einstellungen für ein vorhandenes Netzwerk angegeben. Ein externes Netzwerkprofil ist für NAT- und geroutete Netzwerkprofile erforderlich. Wenn Sie einen IPAM-Endpoint in vRealize Orchestrator registriert und konfiguriert haben, können Sie festlegen, dass IP-Adressinformationen von einem IPAM-Anbieter bereitgestellt werden.

## Voraussetzungen

- Vergewissern Sie sich, dass Sie ein externes IPAM-Anbieter-Plug-In in vRealize Orchestrator importiert und konfiguriert sowie den Endpoint-Typ des IPAM-Anbieters in vRealize Orchestrator registriert haben. In diesem Beispiel wird der externe IPAM-Lösungsanbieter Infoblox unterstützt. Siehe [Checkliste zum Vorbereiten der Unterstützung eines externen IPAM-Anbieters](#).
- [Erstellen eines Endpoints für externen IPAM-Anbieter](#).
- Konfigurieren Sie die vRealize Orchestrator Appliance mit dem registrierten IPAM-Endpoint-Workflow als eigenständige Orchestrator-Instanz im globalen Mandanten (administrator@vsphere.local).
- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.

## Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Netzwerkprofile** aus.
- 2 Klicken Sie auf **Neu** und wählen Sie **Vorhanden** oder **Extern** aus dem Dropdown-Menü aus.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 Wenn Sie einen externen IPAM-Dienstanbieter konfiguriert haben, können Sie den Namen des registrierten IPAM-Endpoints aus dem Dropdown-Menü **IPAM-Endpoint** auswählen.

Wenn Sie einen externen IPAM-Endpoint auswählen, den Sie in vRealize Orchestrator registriert haben, werden IP-Adressen vom angegebenen Endpoint des IPAM-Dienstanbieters bezogen. Die Subnetzmaske, das Gateway und die DNS/WINS-Optionen sind nicht verfügbar, da ihre Funktionen vom ausgewählten IPAM-Endpoint kontrolliert werden. Die Werte für die Subnetzmaske, das Gateway und die DNS/WINS-Optionen werden vom ausgewählten IPAM-Endpoint bereitgestellt.

## Weiter

Nun können Sie Netzwerkbereiche für IP-Adressen definieren, um die Netzwerkprofildefinition abzuschließen.

## Konfigurieren von IP-Bereichen für ein externes Netzwerkprofil für einen registrierten IPAM-Endpoint

Sie können im Netzwerkprofil mindestens einen Netzwerkbereich mit statischen IP-Adressen für die Bereitstellung einer Maschine konfigurieren. Wenn Sie keinen Bereich angeben, können Sie ein Netzwerkprofil als Netzwerk-Reservierungsrichtlinie zur Auswahl eines Reservierungs-Netzwerkpfads für die Netzwerkkarte einer virtuellen Maschine (vNIC) verwenden.

Sie können IP-Bereiche mithilfe der IP-Adressen definieren, die von einem externen IPAM-Anbieter zur Verfügung gestellt werden.

vRealize Automation speichert nur Bereichs-IDs des externen IPAM-Anbieters in der Datenbank, keine Bereichsdetails. Wenn Sie ein Netzwerkprofil auf dieser Seite oder in einem Blueprint bearbeiten, ruft vRealize Automation den IPAM-Dienst auf, um Bereichsdetails basierend auf den ausgewählten Bereichs-IDs abzurufen.

## Voraussetzungen

[Angaben von Informationen zum externen Netzwerkprofil für einen registrierten IPAM-Endpoint.](#)

## Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Netzwerkbereiche**, um einen neuen Netzwerkbereich zu erstellen, oder wählen Sie einen vorhandenen Netzwerkbereich aus.  
  
Details zum ausgewählten Bereich werden angezeigt, einschließlich Name, Beschreibung, IP-Startadresse und IP-Endadresse. Statusbezogene Informationen werden ebenfalls angezeigt.
- 2 Wählen Sie aus der Liste aller Adressbereiche, die für den Endpoint verfügbar sind, einen Adressbereich aus dem Dropdown-Menü **Adressbereich** aus.
- 3 Klicken Sie auf **Hinzufügen** und wählen Sie einen oder mehrere verfügbare Netzwerkbereiche für den angegebenen Adressbereich aus.
- 4 Klicken Sie auf **OK**.  
  
Der IP-Bereichsname wird in der Liste „Definierte Bereiche“ angezeigt. Die IP-Adressen in dem Bereich werden in der Liste „Definierte IP-Adressen“ angezeigt.  
  
Die hochgeladenen IP-Adressen werden auf der Seite **IP-Adressen** angezeigt, wenn Sie auf **Übernehmen** klicken oder wenn Sie das Netzwerkprofil speichern und anschließend bearbeiten.
- 5 Klicken Sie auf **OK**, um das Netzwerkprofil abzuschließen.

## Weiter

Sie können einem Netzwerkpfad in einer Reservierung ein Netzwerkprofil zuweisen, während ein Blueprint-Architekt das Netzwerkprofil in einem Blueprint angeben kann.

## Erstellen eines NAT-Netzwerkprofils

Sie können ein On-Demand-NAT-Netzwerkprofil erstellen, um ein NAT-Netzwerk zu definieren und diesem Bereiche statischer IP- und DHCP-Adressen zuzuweisen.

## Vorgehensweise

- 1 [Angaben von Informationen zum NAT-Netzwerkprofil](#)  
  
Im Netzwerkprofil werden die NAT-Netzwerkeigenschaften, das zugrunde liegende externe Netzwerkprofil, der NAT-Typ und sonstige Werte angegeben, die bei der Bereitstellung des Netzwerks verwendet werden.
- 2 [Konfigurieren von IP-Bereichen für NAT-Netzwerkprofile](#)  
  
Sie können einen oder mehrere statische-IP-Adressbereiche für die Bereitstellung eines Netzwerks konfigurieren.

## Angaben von Informationen zum NAT-Netzwerkprofil

Im Netzwerkprofil werden die NAT-Netzwerkeigenschaften, das zugrunde liegende externe Netzwerkprofil, der NAT-Typ und sonstige Werte angegeben, die bei der Bereitstellung des Netzwerks verwendet werden.

## Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.
- Erstellen Sie ein externes Netzwerkprofil. Siehe [Erstellen eines externen Netzwerkprofils](#) oder [Erstellen eines externen Netzwerkprofils mithilfe eines externen IPAM-Anbieters](#).

## Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Netzwerkprofile** aus.
- 2 Klicken Sie auf **Neu** und wählen Sie **NAT** aus dem Dropdown-Menü aus.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 Übernehmen Sie den standardmäßigen **IPAM-Endpoint** für den vorgegebenen internen **VMware-**IPAM-Anbieter oder wählen Sie einen anderen IPAM-Anbieter-Endpoint wie z. B. Infoblox aus, den Sie in vRealize Orchestrator importiert und registriert haben.

**Hinweis** Ein externer IPAM-Anbieter ist nicht für On-Demand-NAT- und geroutete On-Demand-Netzwerke verfügbar.

- 5 Wählen Sie aus dem Dropdown-Menü **Externes Netzwerkprofil** ein vorhandenes Netzwerkprofil aus.
- 6 Wählen Sie aus dem Dropdown-Menü **NAT-Typ** einen 1:1- oder 1:n-NAT-Typ (Network Address Translation, Netzwerkadressübersetzung) aus.

Option	Beschreibung
<b>Eins-zu-Eins</b>	Weisen Sie jedem Netzwerkadapter eine externe statische IP-Adresse zu. Jede Maschine kann auf das externe Netzwerk zugreifen, und es kann auf jede vom externen Netzwerk aus zugegriffen werden.
<b>Eins-zu-Viele</b>	Eine externe IP-Adresse wird von allen Maschinen auf dem Netzwerk gemeinsam genutzt. Eine interne Maschine kann entweder DHCP- oder statische IP-Adressen aufweisen. Jede Maschine kann auf das externe Netzwerk zugreifen, aber es kann vom externen Netzwerk aus auf keine Maschine zugegriffen werden. Durch Auswählen dieser Option wird das Kontrollkästchen <b>Aktiviert</b> in der DHCP-Gruppe aktiviert.

- 7 Geben Sie eine IP-Subnetzmaske in das Textfeld **Subnetzmaske** ein.  
Beispielsweise 255.255.0.0.
- 8 Geben Sie eine Adresse für ein Edge- oder geroutetes Gateway in das Textfeld **Gateway** ein.  
Verwenden Sie ein standardmäßiges IPv4-Adressformat. Beispielsweise 10.10.110.1.
- 9 (Optional) Aktivieren Sie in der DHCP-Gruppe das Kontrollkästchen **Aktiviert** und geben Sie Werte für **Beginn des IP-Bereichs** und **Ende des IP-Bereichs** ein.  
Sie können das Kontrollkästchen nur markieren, wenn Sie den NAT-Typ auf „Eins-zu-Viele“ festlegen.
- 10 (Optional) Legen Sie eine Leasedauer fest, um zu definieren, wie lange eine Maschine eine IP-Adresse verwenden kann.

11 Klicken Sie auf die Registerkarte **DNS**.

12 Geben Sie bei Bedarf DNS- und WINS-Werte ein.

Die DNS- und WINS-Felder sind bei Verwendung eines internen IPAM-Endpoints optional. Wenn Sie einen externen IPAM-Endpoint verwenden, werden die DNS- und WINS-Werte vom externen IPAM-Anbieter bereitgestellt.

- a (Optional) Geben Sie einen Wert für **Primärer DNS** ein.
- b (Optional) Geben Sie einen Wert für **Sekundärer DNS** ein.
- c (Optional) Geben Sie einen Wert für **DNS-Suffix** ein.

Das DNS-Suffix wird bei der Registrierung und Auflösung von DNS-Namen verwendet.

- d (Optional) Geben Sie einen Wert für **DNS-Suchsuffix** ein.
- e (Optional) Geben Sie einen Wert für **Bevorzugter WINS** ein.
- f (Optional) Geben Sie einen Wert für **Alternativer WINS** ein.

## Weiter

[Konfigurieren von IP-Bereichen für NAT-Netzwerkprofile.](#)

## Konfigurieren von IP-Bereichen für NAT-Netzwerkprofile

Sie können einen oder mehrere statische-IP-Adressbereiche für die Bereitstellung eines Netzwerks konfigurieren.

Die IP-Adressen des Start- und Endnetzwerkbereichs dürfen sich nicht mit den DHCP-Adressen überschneiden. Wenn Sie ein Profil speichern, das sich überschneidende Adressbereiche enthält, zeigt vRealize Automation einen Validierungsfehler an.

## Voraussetzungen

[Angaben von Informationen zum NAT-Netzwerkprofil.](#)

## Vorgehensweise

1 Klicken Sie auf die Registerkarte **Netzwerkbereiche**, um einen neuen Netzwerkbereich zu erstellen, oder wählen Sie einen vorhandenen Netzwerkbereich aus.

Details zum ausgewählten Bereich werden angezeigt, einschließlich Name, Beschreibung, IP-Startadresse und IP-Endadresse. Statusbezogene Informationen werden ebenfalls angezeigt.

2 Klicken Sie auf **Neu**, um einen neuen Netzwerkbereichsnamen und einen IP-Adressbereich manuell einzugeben, oder klicken Sie auf **Aus CSV importieren**, um die IP-Adressinformationen aus einer ordnungsgemäß formatierten CSV-Datei zu importieren.

### ■ Klicken Sie auf **Hinzufügen**.

- a Geben Sie in das Textfeld **Netzwerkbereich** einen neuen Namen ein.
- b Geben Sie eine Beschreibung für den Netzwerkbereich ein.
- c Geben Sie in das Textfeld **IP-Startadresse** die IP-Startadresse des Bereichs ein.

d Geben Sie in das Textfeld **IP-Endadresse** die IP-Endadresse des Bereichs ein.

■ Klicken Sie auf **Aus CSV importieren**.

- a Navigieren Sie zu der CSV-Datei und wählen Sie sie aus, oder ziehen Sie die CSV-Datei in das Dialogfeld **Aus CSV importieren**.

Eine Zeile in der CSV-Datei hat das Format *ip\_address, machine\_name, status, NIC offset*.  
Beispiel:

```
100.10.100.1,mymachine01,Unallocated
```

CSV-Feld	Beschreibung
ip_address	Eine IP-Adresse im IPv4-Format.
machine_name	Der Name einer verwalteten Maschine in vRealize Automation. Wenn dieses Feld leer ist, wird standardmäßig kein Name verwendet. Wenn dieses Feld leer ist, kann das Feld status nicht den Wert „Zugewiesen“ aufweisen.
status	Zugewiesen oder Nicht zugewiesen, Groß-/Kleinschreibung beachten. Wenn dieses Feld leer ist, lautet der Standardwert „Nicht zugewiesen“. Wenn der Status „Zugewiesen“ lautet, darf das Feld machine_name nicht leer sein.
NIC_offset	Eine nicht negative ganze Zahl.

- b Klicken Sie auf **Übernehmen**.

3 Klicken Sie auf **OK**.

Der IP-Bereichsname wird in der Liste „Definierte Bereiche“ angezeigt. Die IP-Adressen in dem Bereich werden in der Liste „Definierte IP-Adressen“ angezeigt.

Die hochgeladenen IP-Adressen werden auf der Seite **IP-Adressen** angezeigt, wenn Sie auf **Übernehmen** klicken oder wenn Sie das Netzwerkprofil speichern und anschließend bearbeiten.

- 4 Klicken Sie auf die Registerkarte **IP-Adressen**, um die IP-Adressen für den benannten Netzwerkbereich anzuzeigen.

- 5 (Optional) Wählen Sie aus dem Dropdown-Menü **Netzwerkbereich** IP-Adressinformationen aus, um die Einträge für die IP-Adresse zu filtern.

Sie können Informationen zu allen definierten Netzwerkbereichen, zu den aus einer CSV-Datei importierten Netzwerkbereichen oder zu einem benannten Netzwerkbereich anzeigen. Die Details beinhalten die IP-Startadresse, den Maschinennamen, Datum und Uhrzeit der letzten Änderung sowie den IP-Status.

- 6 (Optional) Wählen Sie aus dem Dropdown-Menü **IP-Status** einen Statustyp aus, um die Einträge für die IP-Adresse herauszufiltern, die dem ausgewählten IP-Status entsprechen. Mögliche Statusstellungen sind „Zugewiesen“, „Nicht zugewiesen“, „Gelöscht“ und „Abgelaufen“.

Für IP-Adressen mit dem Status „Abgelaufen“ oder „Gelöscht“ können Sie auf **Rückforderung** klicken, um diese IP-Adressbereiche für die Zuteilung verfügbar zu machen. Sie müssen das Profil speichern, damit die Rückforderung wirksam wird. Adressen werden nicht sofort zurückgewonnen, weshalb die Statusspalte nicht sofort von „Abgelaufen“ oder „Gelöscht“ in „Zugewiesen“ geändert wird.



7 Klicken Sie auf **OK**.

## Erstellen eines gerouteten Netzwerkprofils

Sie können ein geroutetes On-Demand-Netzwerkprofil erstellen, um einen routingfähigen IP-Bereich und verfügbare Subnetze für geroutete Netzwerke zu definieren.

### Vorgehensweise

#### 1 [Angaben von Informationen zum gerouteten Netzwerkprofil](#)

Die Informationen zum Netzwerkprofil identifizieren die gerouteten Netzwerkeigenschaften, das zugrunde liegende externe Netzwerkprofil und sonstige Werte, die bei der Bereitstellung des Netzwerks verwendet werden.

#### 2 [Konfigurieren von IP-Bereichen für geroutete Netzwerkprofile](#)

Sie können einen oder mehrere statische-IP-Adressbereiche für die Bereitstellung eines Netzwerks konfigurieren.

### Angaben von Informationen zum gerouteten Netzwerkprofil

Die Informationen zum Netzwerkprofil identifizieren die gerouteten Netzwerkeigenschaften, das zugrunde liegende externe Netzwerkprofil und sonstige Werte, die bei der Bereitstellung des Netzwerks verwendet werden.

Bei einem gerouteten Netzwerkprofil handelt es sich um einen routingfähigen IP-Bereich, der auf mehrere Netzwerke aufgeteilt ist. Jedes neue geroutete Netzwerk stellt das nächste verfügbare Subnetz aus dem routingfähigen IP-Bereich zur Verfügung. Ein geroutetes Netzwerk kann auf alle anderen gerouteten Netzwerke zugreifen, die dasselbe Netzwerkprofil verwenden.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.
- Erstellen Sie ein externes Netzwerkprofil. Siehe [Erstellen eines externen Netzwerkprofils](#) oder [Erstellen eines externen Netzwerkprofils mithilfe eines externen IPAM-Anbieters](#).
- Stellen Sie sicher, dass für den logischen NSX-Router im vSphere Client die Verwendung eines gerouteten Netzwerkprofils konfiguriert ist. Informationen dazu finden Sie im *NSX-Administratorhandbuch*.

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Netzwerkprofile** aus.
- 2 Klicken Sie auf **Neu** und wählen Sie **Weitergeleitet** aus dem Dropdown-Menü aus.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 Wählen Sie aus dem Dropdown-Menü **Externes Netzwerkprofil** ein vorhandenes Netzwerkprofil aus.

- 5 Übernehmen Sie den standardmäßigen **IPAM-Endpoint** für den vorgegebenen internen **VMware-**IPAM-Anbieter oder wählen Sie einen anderen IPAM-Anbieter-Endpoint wie z. B. Infoblox aus, den Sie in vRealize Orchestrator importiert und registriert haben.

---

**Hinweis** Ein externer IPAM-Anbieter ist nicht für On-Demand-NAT- und geroutete On-Demand-Netzwerke verfügbar.

---

- 6 Geben Sie die Subnetzmaske in das Textfeld **Subnetzmaske** ein, das dem externen Netzwerkprofil zugeordnet ist.  
Beispielsweise 255.255.0.0.
- 7 Geben Sie einen Wert in das Textfeld **Bereichssubnetzmaske** ein, um zu bestimmen, wie Bereiche von der Option **Bereiche generieren** auf der Seite **IP-Bereiche** generiert werden.  
Beispielsweise 255.255.255.0.
- 8 Geben Sie die erste verfügbare IP-Adresse in das Textfeld **Basis-IP** ein. Mithilfe der Einstellungen für die Basis-IP und die Bereichssubnetzmaske werden Bereiche generiert.  
Beispielsweise 120.120.0.1.
- 9 Klicken Sie auf die Registerkarte **DNS**.
- 10 Geben Sie bei Bedarf DNS- und WINS-Werte ein.

Die DNS- und WINS-Felder sind bei Verwendung eines internen IPAM-Endpoints optional. Wenn Sie einen externen IPAM-Endpoint verwenden, werden die DNS- und WINS-Werte vom externen IPAM-Anbieter bereitgestellt.

- a (Optional) Geben Sie einen Wert für **Primärer DNS** ein.
- b (Optional) Geben Sie einen Wert für **Sekundärer DNS** ein.
- c (Optional) Geben Sie einen Wert für **DNS-Suffix** ein.  
Das DNS-Suffix wird bei der Registrierung und Auflösung von DNS-Namen verwendet.
- d (Optional) Geben Sie einen Wert für **DNS-Suchsuffix** ein.
- e (Optional) Geben Sie einen Wert für **Bevorzugter WINS** ein.
- f (Optional) Geben Sie einen Wert für **Alternativer WINS** ein.

## Weiter

[Konfigurieren von IP-Bereichen für geroutete Netzwerkprofile.](#)

## Konfigurieren von IP-Bereichen für geroutete Netzwerkprofile

Sie können einen oder mehrere statische-IP-Adressbereiche für die Bereitstellung eines Netzwerks konfigurieren.

Während der Bereitstellung teilt jedes neue geroutete Netzwerk den nächsten verfügbaren Bereich zu und verwendet ihn als IP-Bereich.

## Voraussetzungen

[Angaben von Informationen zum gerouteten Netzwerkprofil.](#)

## Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Netzwerkbereiche**, um einen neuen Netzwerkbereich zu erstellen, oder wählen Sie einen vorhandenen Netzwerkbereich aus.

Details zum ausgewählten Bereich werden angezeigt, einschließlich Name, Beschreibung, IP-Startadresse und IP-Endadresse. Statusbezogene Informationen werden ebenfalls angezeigt.

- 2 Klicken Sie auf **Bereiche generieren**, um Netzwerkbereiche basierend auf der Subnetzmaske, der Bereichssubnetzmaske und der grundlegenden IP-Adressinformationen zu erzeugen, die Sie auf der Registerkarte „Allgemein“ eingegeben haben.

vRealize Automation generiert ausgehend von der Basis-IP-Adresse Bereiche basierend auf der Bereichssubnetzmaske.

vRealize Automation erzeugt beispielsweise Bereiche mit 255 IP-Bereichen, wenn die Subnetzmaske bei 255.255.0.0 und die Bereichssubnetzmaske bei 255.255.255.0 liegt und als Name Bereich1 bis Bereichn verwendet wird.

- 3 Klicken Sie auf **OK**.

## Konfigurieren von Reservierungen und Reservierungsrichtlinien

Eine vRealize Automation-Reservierung kann Richtlinien, Prioritäten und Kontingente definieren, welche die Maschinenplatzierung bei Bereitstellungsanforderungen bestimmen. Reservierungsrichtlinien schränken die Bereitstellung von Maschinen auf eine Teilmenge der verfügbaren Reservierungen ein. Mithilfe von Speicherreservierungsrichtlinien können Blueprint-Architekten Maschinenvolumen zu unterschiedlichen Datenspeichern zuweisen.

## Reservierungen

Sie können eine vRealize Automation-Reservierung erstellen, um Bereitstellungsressourcen in der Fabric-Gruppe einer bestimmten Business-Gruppe zuzuteilen.

Beispielsweise können Sie mithilfe von Reservierungen festlegen, dass ein Teil der Arbeitsspeicher-, CPU-, Netzwerk- und Speicherressourcen einer bestimmten Computing-Ressource zu einer bestimmten Business-Gruppe gehört, oder dass bestimmte Maschinen einer bestimmten Business-Gruppe zugeteilt werden sollen.

---

**Hinweis** Hinweis: Speicher und Arbeitsspeicher, der mittels einer Reservierung einer bereitgestellten Maschine zugewiesen ist, wird freigegeben, wenn die Maschine, der der Speicher oder Arbeitsspeicher zugewiesen ist, in vRealize Automation mithilfe der Aktion „Löschen“ gelöscht wird. Der Speicher und Arbeitsspeicher wird nicht freigegeben, wenn die Maschine auf dem vCenter Server gelöscht wird.

---

Reservierungen können für die folgenden Maschinentypen erstellt werden:

- vSphere

- vCloud Air
- vCloud Director
- Amazon
- Hyper-V
- KVM
- OpenStack
- SCVMM
- XenServer

### Auswählen eines Reservierungsszenarios

Sie können Reservierungen erstellen, um Business-Gruppen Ressourcen zuzuteilen. Die Vorgehensweise zum Erstellen einer Reservierung hängt von Ihrem Szenario ab.

Wählen Sie ein Reservierungsszenario basierend auf dem Typ des Ziel-Endpoints aus.

Jede Business-Gruppe benötigt mindestens eine Reservierung, damit ihre Mitglieder Maschinen dieses Typs bereitstellen können. Beispielsweise kann eine Business-Gruppe mit einer OpenStack-Reservierung, aber ohne Amazon-Reservierung, keine Maschine von Amazon anfordern. In diesem Beispiel muss der Business-Gruppe eine Reservierung speziell für Amazon-Ressourcen zugeteilt werden.

**Tabelle 3-5. Auswählen eines Reservierungsszenarios**

Szenario	Prozedur
Erstellen einer vSphere-Reservierung.	<a href="#">Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer</a>
Erstellen einer Reservierung, um für einen vCloud Air-Endpoint Ressourcen zuzuteilen.	<a href="#">Erstellen einer vCloud Air-Reservierung</a>
Erstellen einer Reservierung, um für einen vCloud Director-Endpoint Ressourcen zuzuteilen.	<a href="#">Erstellen einer vCloud Director-Reservierung</a>
Erstellen einer Reservierung, um Ressourcen auf einer Amazon-Ressource zuzuteilen (mit oder ohne Amazon Virtual Private Cloud).	<a href="#">Erstellen einer Amazon-Reservierung</a>
Erstellen einer Reservierung, um Ressourcen auf einer OpenStack-Ressource zuzuteilen.	<a href="#">Erstellen einer OpenStack-Reservierung</a>
Erstellen einer Reservierung, um Ressourcen für Hyper-V zuzuteilen.	<a href="#">Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer</a>
Erstellen einer Reservierung, um Ressourcen für KVM zuzuteilen.	<a href="#">Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer</a>
Erstellen einer Reservierung, um Ressourcen auf einer OpenStack-Ressource zuzuteilen.	<a href="#">Erstellen einer OpenStack-Reservierung</a>

**Tabelle 3-5. Auswählen eines Reservierungsszenarios (Fortsetzung)**

Szenario	Prozedur
Erstellen einer Reservierung, um Ressourcen für SCVMM zuzuteilen.	<a href="#">Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer</a>
Erstellen einer Reservierung, um Ressourcen für XenServer zuzuteilen.	<a href="#">Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer</a>

## Erstellen von Cloud-Kategorie-Reservierungen

Ein Kategorietyt einer Cloud-Reservierung bietet Zugriff auf die Bereitstellungsdienste eines Cloud-Dienstkontos für eine bestimmte vRealize Automation-Business-Gruppe. Zu den verfügbaren Cloud-Reservierungstypen zählen Amazon, OpenStack, vCloud Air und vCloud Director.

Bei einer Reservierung handelt es sich um einen Teil der Arbeitsspeicher-, CPU-, Netzwerk- und Speicherressourcen in einer Computing-Ressource, der einer bestimmten vRealize Automation-Business-Gruppe zugeteilt ist.

Eine Business-Gruppe kann mehrere Reservierungen auf einem Endpoint oder Reservierungen auf mehreren Endpoints aufweisen.

Das Zuteilungsmodell für eine Reservierung hängt vom Zuteilungsmodell im zugehörigen Datencenter ab. Verfügbare Zuteilungsmodelle sind „Zuteilungspool“, „Im Voraus bezahlen“ und „Reservierungspool“. Informationen zu Zuteilungsmodellen finden Sie in der vCloud Director- oder vCloud Air-Dokumentation.

Neben der Definition der Fabric-Ressourcen, die der Business-Gruppe zugeteilt sind, kann eine Reservierung auch Richtlinien, Prioritäten und Kontingente definieren, welche die Maschinenplatzierung bestimmen.

## Grundlegendes zur Auswahllogik für Cloud-Reservierungen

Wenn das Mitglied einer Business-Gruppe eine Bereitstellungsanforderung für eine Cloud-Maschine erstellt, wählt vRealize Automation eine Maschine von einer der für diese Business-Gruppe verfügbaren Reservierungen aus. Cloud-Reservierungen umfassen Amazon, OpenStack, vCloud Air und vCloud Director.

Die für eine Maschine bereitgestellte Reservierung muss die folgenden Kriterien erfüllen:

- Die Reservierung muss denselben Plattfortmtyp wie der Blueprint aufweisen, von dem die Maschine angefordert wurde.
- Die Reservierung muss aktiviert sein.
- Die Reservierung muss über eine verbleibende Kapazität in ihrem Maschinenkontingent oder über ein unbegrenztes Kontingent verfügen.

Das zugeteilte Maschinenkontingent umfasst nur Maschinen, die eingeschaltet sind. Wenn eine Reservierung beispielsweise über ein Kontingent von 50 verfügt und 40 Maschinen bereitgestellt wurden, von denen jedoch nur 20 eingeschaltet sind, beträgt das zugeteilte Kontingent der Reservierung 40 Prozent und nicht 80 Prozent.

- Bei der Reservierung müssen die Sicherheitsgruppen in der Maschinenanforderung angegeben sein.

- Die Reservierung muss einer Region zugeordnet sein, bei der das Maschinen-Image im Blueprint angegeben ist.
- Die Reservierung muss über genügend nicht zugeteilte Arbeitsspeicher- und Speicherressourcen für die Bereitstellung der Maschine verfügen.

Bei einer Vorausbezahlungs-Reservierung können Ressourcen unbegrenzt sein.

- Bei Anforderungen für Amazon-Maschinen wird ein Verfügbarkeitsbereich angegeben und auch, ob der Maschine ein Subnetz am Speicherort einer virtuellen privaten Cloud (VPC) oder Nicht-VPC bereitgestellt werden soll. Die Reservierung muss dem Netzwerktyp (VPC oder Nicht-VPC) entsprechen.
- Wenn bei der Anforderung für vCloud Air oder vCloud Director ein Zuteilungsmodell angegeben wird, muss das virtuelle Datencenter, das der Reservierung zugewiesen ist, dasselbe Zuteilungsmodell aufweisen.
- Für vCloud Director oder vCloud Air muss die angegebene Organisation aktiviert sein.
- Alle Blueprint-Vorlagen müssen in Reservierungen verfügbar sein. Wenn die Reservierungsrichtlinie mehr als einer Ressource zugeordnet wird, sollten die Vorlagen öffentlich sein.
- Wenn der Cloud-Anbieter die Netzwerkauswahl unterstützt und der Blueprint bestimmte Netzwerkeinstellungen aufweist, muss die Reservierung dieselben Netzwerke aufweisen.

Wenn der Blueprint oder die Reservierung ein Netzwerkprofil für statische IP-Adressenzuweisung angibt, muss eine IP-Adresse verfügbar sein, die der neuen Maschine zugewiesen werden kann.

- Wenn bei der Anforderung ein Zuteilungsmodell angegeben wird, muss das Zuteilungsmodell der Reservierung mit dem Zuteilungsmodell in der Anforderung übereinstimmen.
- Wenn der Blueprint eine Reservierungsrichtlinie angibt, muss die Reservierung dieser Reservierungsrichtlinie angehören.

Reservierungsrichtlinien stellen eine Möglichkeit dar, wie garantiert werden kann, dass die ausgewählte Reservierung alle zusätzlichen Anforderungen für die Bereitstellung von Maschinen von einem bestimmten Blueprint erfüllt. Wenn ein Blueprint beispielsweise ein bestimmtes Maschinen-Image verwendet, können Sie Reservierungsrichtlinien dazu verwenden, die Bereitstellung auf Reservierungen zu beschränken, die den Regionen mit dem erforderlichen Image zugewiesen sind.

Wenn keine Reservierung mit all diesen Auswahlkriterien verfügbar ist, schlägt die Bereitstellung fehl.

Wenn mehrere Reservierungen all diesen Kriterien entsprechen, wird die Reservierung, von der eine angeforderte Maschine bereitgestellt wird, durch die folgende Logik festgelegt:

- Eine Reservierung mit einem niedrigeren Prioritätswert wird vor einer Reservierung mit einem höheren Prioritätswert ausgewählt.
- Wenn mehrere Reservierungen dieselbe Priorität aufweisen, wird diejenige Reservierung ausgewählt, deren zugeteiltes Maschinenkontingent den geringsten Prozentsatz aufweist.

- Wenn mehrere Reservierungen dieselbe Priorität und dieselbe Kontingentauslastung aufweisen, werden Maschinen im Round-Robin-Verfahren (Rundlauf-Verfahren) auf Reservierungen verteilt.

---

**Hinweis** Die Round-Robin-Auswahl von Netzwerkprofilen wird nicht unterstützt, die Round-Robin-Auswahl von Netzwerken (soweit vorhanden) dagegen schon; diese können im Zusammenhang mit unterschiedlichen Netzwerkprofilen stehen.

---

Wenn in einer Reservierung mehrere Speicherpfade mit genügend Kapazität zur Bereitstellung der Maschinen-Volumes verfügbar sind, werden Speicherpfade nach der folgenden Logik ausgewählt.

- Ein Speicherpfad mit einem niedrigeren Prioritätswert wird vor einem Speicherpfad mit einem höheren Prioritätswert ausgewählt.
- Wenn der Blueprint oder die Anforderung eine Speicherreservierungsrichtlinie angibt, muss der Speicherpfad dieser Speicherreservierungsrichtlinie angehören.

Wenn die benutzerdefinierte Eigenschaft `VirtualMachine.DiskN.StorageReservationPolicyMode` auf „Nicht genau“ festgelegt ist und in der Speicherreservierungsrichtlinie kein Speicherpfad mit genügend Kapazität verfügbar ist, wird die Bereitstellung mit einem Speicherpfad außerhalb der angegebenen Speicherreservierungsrichtlinie fortgesetzt. Der Standardwert von `VirtualMachine.DiskN.StorageReservationPolicyMode` lautet „Genau“.

- Wenn mehrere Speicherpfade dieselbe Priorität aufweisen, werden Maschinen im Round-Robin-Verfahren (Rundlauf-Verfahren) auf Speicherpfade verteilt.

## Verwenden von Amazon-Sicherheitsgruppen

Geben Sie beim Erstellen einer Amazon-Reservierung mindestens eine Sicherheitsgruppe an. Jede verfügbare Region erfordert mindestens eine angegebene Sicherheitsgruppe.

Eine Sicherheitsgruppe dient als Firewall, um den Zugriff auf die Maschine zu kontrollieren. Jede Region enthält zumindest die Standardsicherheitsgruppe. Mithilfe der Amazon Web Services Management Console können Administratoren zusätzliche Sicherheitsgruppen erstellen, Ports für Microsoft Remote Desktop Protocol oder SSH konfigurieren und ein virtuelles privates Netzwerk für ein Amazon VPN einrichten.

Bei der Erstellung einer Amazon-Reservierung oder Konfiguration einer Maschinenkomponente im Blueprint können Sie aus einer Liste Sicherheitsgruppen auswählen, die für die Region des angegebenen Amazon-Kontos verfügbar sind. Sicherheitsgruppen werden während der Datenerfassung importiert.

Weitere Informationen zur Erstellung und Verwendung von Sicherheitsgruppen in Amazon Web Services finden Sie in der Dokumentation zu Amazon.

## Erstellen einer Amazon-Reservierung

Sie müssen Maschinen durch Erstellen einer Reservierung Ressourcen zuteilen, bevor Mitglieder einer Business-Gruppe die Maschinenbereitstellung anfordern können.

Sie können Amazon-Reservierungen für Amazon Virtual Private Cloud oder Amazon-Nicht-VPC verwenden. Benutzer von Amazon Web Services können eine Amazon Virtual Private Cloud erstellen, um eine virtuelle Netzwerktopologie gemäß Ihren Spezifikationen zu entwerfen. Wenn Sie Amazon VPC verwenden möchten, müssen Sie einer vRealize Automation-Reservierung eine Amazon VPC-Instanz zuweisen. Siehe .

---

**Hinweis** Nach dem Erstellen einer Reservierung können Sie die Zuordnungen der Business-Gruppen oder Computing-Ressourcen nicht mehr ändern.

---

Informationen zum Erstellen einer Amazon VPC-Instanz mithilfe der AWS Management Console finden Sie in der Dokumentation zu Amazon Web Services.

### Vorgehensweise

#### 1 Angeben von Informationen zu Amazon-Reservierungen

Jede Reservierung wird für eine bestimmte Business-Gruppe konfiguriert, um ihr die Berechtigung für das Anfordern von Maschinen auf einer angegebenen Computing-Ressource zu erteilen.

#### 2 Angeben von Ressourcen- und Netzwerkeinstellungen für Amazon-Reservierungen

Geben Sie Ressourcen- und Netzwerkeinstellungen für die Bereitstellung von Maschinen über die vRealize Automation-Reservierung ein.

#### 3 Angeben benutzerdefinierter Eigenschaften und Warnungen für Amazon-Reservierungen

Sie können einer vRealize Automation-Reservierung benutzerdefinierte Eigenschaften zuordnen. Darüber hinaus können Sie Warnungen konfigurieren, um bei niedrigen Reservierungsressourcen E-Mail-Benachrichtigungen zu senden.

### Angeben von Informationen zu Amazon-Reservierungen

Jede Reservierung wird für eine bestimmte Business-Gruppe konfiguriert, um ihr die Berechtigung für das Anfordern von Maschinen auf einer angegebenen Computing-Ressource zu erteilen.

---

**Hinweis** Nach dem Erstellen einer Reservierung können Sie die Zuordnungen der Business-Gruppen oder Computing-Ressourcen nicht mehr ändern.

---

Sie können die Anzeige von Reservierungen beim Hinzufügen, Bearbeiten oder Löschen steuern, indem Sie auf der Seite „Reservierungen“ die Option **Nach Kategorie filtern** verwenden. Beachten Sie, dass Test-Agent-Reservierungen beim Filtern nach Kategorie nicht in der Reservierungsliste angezeigt werden.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.
- Stellen Sie sicher, dass der Mandantenadministrator mindestens eine Business-Gruppe erstellt hat.
- Stellen Sie sicher, dass eine Computing-Ressource vorhanden ist.
- Konfigurieren Sie die Netzwerkeinstellungen.
- (Optional) Konfigurieren Sie die Informationen zum Netzwerkprofil.



- Stellen Sie sicher, dass Sie Zugriff auf das gewünschte Amazon-Netzwerk haben. Wenn Sie beispielsweise VPC verwenden möchten, stellen Sie sicher, dass Sie Zugriff auf ein Amazon Virtual Private Cloud (VPC)-Netzwerk haben.
- Stellen Sie sicher, dass erforderliche Schlüsselpaare vorhanden sind. Siehe [Verwalten von Schlüsselpaaren](#).

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Reservierungen** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)** und wählen Sie den zu erstellenden Reservierungstyp aus.  
Wählen Sie **Amazon** aus.
- 3 (Optional) Wählen Sie aus dem Dropdown-Menü **Aus vorhandener Reservierung kopieren** eine vorhandene Reservierung aus.  
  
Die Daten zu der ausgewählten Reservierung wird angezeigt. Sie können für Ihre neue Reservierung bei Bedarf Änderungen vornehmen.
- 4 Geben Sie im Textfeld **Name** einen Namen ein.
- 5 Wählen Sie aus dem Dropdown-Menü **Mandant** einen Mandanten aus.
- 6 Wählen Sie aus dem Dropdown-Menü **Business-Gruppe** eine Business-Gruppe aus.  
  
Nur Benutzer in dieser Business-Gruppe können Maschinen mit dieser Reservierung bereitstellen.
- 7 (Optional) Wählen Sie aus dem Dropdown-Menü **Reservierungsrichtlinie** eine Reservierungsrichtlinie aus.  
  
Diese Option setzt voraus, dass mindestens eine Reservierungsrichtlinie vorhanden ist. Sie können die Reservierung später bearbeiten, um eine Reservierungsrichtlinie anzugeben.  
  
Sie verwenden eine Reservierungsrichtlinie zur Einschränkung der Bereitstellung auf bestimmte Reservierungen.
- 8 Geben Sie im Textfeld **Priorität** eine Zahl ein, um die Priorität für die Reservierung festzulegen.  
  
Die Priorität wird verwendet, wenn eine Business-Gruppe über mehr als eine Reservierung verfügt. Einer Reservierung der Priorität 1 wird bei einer Bereitstellung der Vorzug gegenüber einer Reservierung der Priorität 2 gegeben.
- 9 (Optional) Deaktivieren Sie das Kontrollkästchen **Diese Reservierung aktivieren**, wenn Sie nicht möchten, dass diese Reservierung aktiv ist.

Verlassen Sie diese Seite nicht. Ihre Reservierung ist noch nicht abgeschlossen.

### Angeben von Ressourcen- und Netzwerkeinstellungen für Amazon-Reservierungen

Geben Sie Ressourcen- und Netzwerkeinstellungen für die Bereitstellung von Maschinen über die vRealize Automation-Reservierung ein.

Weitere Informationen zu Lastausgleichsdiensten finden Sie unter *Konfigurieren von vRealize Automation*.

## Voraussetzungen

### Angeben von Informationen zu Amazon-Reservierungen.

## Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Ressourcen**.
- 2 Wählen Sie aus dem Dropdown-Menü **Computing-Ressource** eine Computing-Ressource aus, auf der Maschinen bereitgestellt werden sollen.

Die verfügbaren Amazon-Regionen werden aufgelistet.

- 3 (Optional) Geben Sie im Textfeld **Maschinenkontingent** eine Zahl ein, um die maximale Anzahl von Maschinen festzulegen, die in dieser Reservierung bereitgestellt werden können.

Nur eingeschaltete Maschinen werden beim Kontingent berücksichtigt. Lassen Sie das Feld leer, wenn die Reservierung unbegrenzt sein soll.

- 4 Wählen Sie aus dem Dropdown-Menü **Schlüsselpaar** eine Methode aus, wie Schlüsselpaare Computing-Instanzen zugewiesen werden sollen.

Option	Beschreibung
<b>Nicht angegeben</b>	Das Verhalten von Schlüsselpaaren wird auf der Blueprint-Ebene anstatt auf der Reservierungsebene gesteuert.
<b>Automatisch generiert pro Business-Gruppe</b>	Jede in einer Business-Gruppe bereitgestellte Maschine verfügt über dasselbe Schlüsselpaar. Dies trifft auch für Maschinen zu, die in anderen Reservierungen bereitgestellt wurden, sofern die Maschine dieselbe Computing-Ressource und Business-Gruppe aufweist. Da auf diese Weise generierte Schlüsselpaare mit einer Business-Gruppe verknüpft sind, werden die Schlüsselpaare beim Löschen der Business-Gruppe ebenfalls gelöscht.
<b>Automatisch generiert pro Maschine</b>	Jede Maschine weist ein eindeutiges Schlüsselpaar auf. Dies stellt die sicherste Methode dar, da keine Schlüsselpaare von Maschinen gemeinsam genutzt werden.
<b>Bestimmtes Schlüsselpaar</b>	Jede in dieser Reservierung bereitgestellte Maschine verfügt über dasselbe Schlüsselpaar. Suchen Sie nach einem Schlüsselpaar, das für diese Reservierung verwendet werden soll.

- 5 Wenn Sie im Dropdown-Menü **Schlüsselpaar** die Option **Bestimmtes Schlüsselpaar** ausgewählt haben, wählen Sie aus dem Dropdown-Menü **Bestimmtes Schlüsselpaar** einen Schlüsselpaarwert aus.
- 6 Wenn Sie für Amazon Virtual Private Cloud konfiguriert sind, aktivieren Sie das Kontrollkästchen **Einem Subnetz in einem VPC zuweisen**. Lassen Sie dieses Kontrollkästchen andernfalls deaktiviert.  
  
Wenn Sie **Einem Subnetz in einem VPC zuweisen** aktivieren, werden die folgenden Speicherorte oder Subnetze, Sicherheitsgruppen und Lastausgleichsdienste in einem Popup-Menü anstatt auf dieser Seite angezeigt.

- 7 Wählen Sie in der Liste **Speicherorte** oder **Subnetze** einen oder mehrere verfügbare Speicherorte (Nicht-VPC-Speicherorte) oder Subnetze (VPC) aus.

Wählen Sie alle verfügbaren Speicherorte oder Subnetze aus, die für die Bereitstellung verfügbar sein sollen.

- 8 Wählen Sie aus der Liste **Sicherheitsgruppen** mindestens eine Sicherheitsgruppe aus, die einer Maschine während der Bereitstellung zugewiesen werden kann.

Wählen Sie alle Sicherheitsgruppen aus, die bei der Bereitstellung einer Maschine zugewiesen werden können.

- 9 Wählen Sie aus der Liste **Lastausgleichsdienste** mindestens einen verfügbaren Lastausgleichsdienst aus.

Wenn Sie das elastische Lastausgleichsmodul verwenden, wählen Sie einen oder mehrere verfügbare Lastausgleichsdienste für die ausgewählten Speicherorte oder Subnetze aus.

Sie können die Reservierung nun durch Klicken auf **Speichern** speichern. Sie können noch benutzerdefinierte Eigenschaften hinzufügen, um Reservierungsspezifikationen besser zu steuern. Zudem können Sie E-Mail-Warnungen konfigurieren, damit Sie Benachrichtigungen erhalten, wenn die dieser Reservierung zugeteilten Ressourcen einen niedrigen Stand erreichen.

### Angeben benutzerdefinierter Eigenschaften und Warnungen für Amazon-Reservierungen

Sie können einer vRealize Automation-Reservierung benutzerdefinierte Eigenschaften zuordnen. Darüber hinaus können Sie Warnungen konfigurieren, um bei niedrigen Reservierungsressourcen E-Mail-Benachrichtigungen zu senden.

Benutzerdefinierte Eigenschaften und E-Mail-Warnungen sind optionale Konfigurationen für die Reservierung. Wenn Sie weder benutzerdefinierte Eigenschaften verknüpfen noch Warnungen festlegen möchten, klicken Sie auf **Speichern**, um die Erstellung der Reservierung zu beenden.

Sie können beliebig viele benutzerdefinierte Eigenschaften hinzufügen.

Falls konfiguriert, werden Warnungen täglich generiert und nicht erst bei Erreichen des angegebenen Schwellenwerts.

---

**Wichtig** Benachrichtigungen werden nur dann gesendet, wenn E-Mail-Warnungen konfiguriert und Benachrichtigungen aktiviert wurden.

---

### Voraussetzungen

[Angeben von Ressourcen- und Netzwerkeinstellungen für Amazon-Reservierungen.](#)

### Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Eigenschaften**.
- 2 Klicken Sie auf **Neu**.
- 3 Geben Sie einen gültigen Namen für die benutzerdefinierte Eigenschaft ein.
- 4 Geben Sie gegebenenfalls einen Eigenschaftswert ein.

- 5 Klicken Sie auf **Speichern**.
- 6 (Optional) Fügen Sie zusätzliche benutzerdefinierte Eigenschaften hinzu.
- 7 Klicken Sie auf die Registerkarte **Warnungen**.
- 8 Aktivieren Sie das Kontrollkästchen **Kapazitätswarnungen**, um das Senden von Warnungen zu konfigurieren.
- 9 Verwenden Sie den Schieberegler, um für verfügbare Ressourcenzuteilungen Schwellenwerte festzulegen.
- 10 Geben Sie im Textfeld **Empfänger** mindestens eine E-Mail-Adresse eines Benutzers oder einen Gruppennamen ein, um festzulegen, wer Warnbenachrichtigungen erhalten soll.  
Drücken Sie die Eingabetaste, um mehrere Einträge zu trennen.
- 11 Wählen Sie **Warnungen an Gruppenmanager senden** aus, um Gruppenmanager in den Erhalt der E-Mail-Warnungen einzubeziehen.
- 12 Legen Sie eine Erinnerungshäufigkeit (in Tagen) fest.
- 13 Klicken Sie auf **Speichern**.

Die Reservierung wird gespeichert und in der Liste „Reservierungen“ angezeigt.

#### Weiter

Sie können optionale Reservierungsrichtlinien konfigurieren oder mit der Vorbereitung auf die Bereitstellung beginnen.

Zur Erstellung von Blueprints autorisierte Benutzer können diese nun erstellen.

#### Erstellen einer OpenStack-Reservierung

Sie müssen Maschinen durch Erstellen einer Reservierung Ressourcen zuteilen, bevor Mitglieder einer Business-Gruppe die Maschinenbereitstellung anfordern können.

Erstellen Sie eine OpenStack-Reservierung.

#### Vorgehensweise

- 1 [Angaben von Informationen zu OpenStack-Reservierungen](#)  
Jede Reservierung wird für eine bestimmte Business-Gruppe konfiguriert, um ihr die Berechtigung für das Anfordern von Maschinen auf einer angegebenen Computing-Ressource zu erteilen.
- 2 [Angaben von Ressourcen- und Netzwerkeinstellungen für OpenStack-Reservierungen](#)  
Geben Sie Ressourcen- und Netzwerkeinstellungen an, die für Maschinen verfügbar sind, die über diese vRealize Automation-Reservierung bereitgestellt werden.
- 3 [Angaben benutzerdefinierter Eigenschaften und Warnungen für OpenStack-Reservierungen](#)  
Sie können einer vRealize Automation-Reservierung benutzerdefinierte Eigenschaften zuordnen. Darüber hinaus können Sie Warnungen konfigurieren, um bei niedrigen Reservierungsressourcen E-Mail-Benachrichtigungen zu senden.

## Angeben von Informationen zu OpenStack-Reservierungen

Jede Reservierung wird für eine bestimmte Business-Gruppe konfiguriert, um ihr die Berechtigung für das Anfordern von Maschinen auf einer angegebenen Computing-Ressource zu erteilen.

---

**Hinweis** Nach dem Erstellen einer Reservierung können Sie die Zuordnungen der Business-Gruppen oder Computing-Ressourcen nicht mehr ändern.

---

Sie können die Anzeige von Reservierungen beim Hinzufügen, Bearbeiten oder Löschen steuern, indem Sie auf der Seite „Reservierungen“ die Option **Nach Kategorie filtern** verwenden. Beachten Sie, dass Test-Agent-Reservierungen beim Filtern nach Kategorie nicht in der Reservierungsliste angezeigt werden.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.
- Stellen Sie sicher, dass der Mandantenadministrator mindestens eine Business-Gruppe erstellt hat.
- Stellen Sie sicher, dass eine Computing-Ressource vorhanden ist.
- Stellen Sie sicher, dass optionale Sicherheitsgruppen oder Pool-IP-Adressen konfiguriert sind.
- Stellen Sie sicher, dass erforderliche Schlüsselpaare vorhanden sind. Siehe [Verwalten von Schlüsselpaaren](#).
- Stellen Sie sicher, dass eine Computing-Ressource vorhanden ist.
- Konfigurieren Sie die Netzwerkeinstellungen.

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Reservierungen** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)** und wählen Sie den zu erstellenden Reservierungstyp aus.  
Wählen Sie **OpenStack** aus.
- 3 (Optional) Wählen Sie aus dem Dropdown-Menü **Aus vorhandener Reservierung kopieren** eine vorhandene Reservierung aus.  
Die Daten zu der ausgewählten Reservierung wird angezeigt. Sie können für Ihre neue Reservierung bei Bedarf Änderungen vornehmen.
- 4 Geben Sie im Textfeld **Name** einen Namen ein.
- 5 Wählen Sie aus dem Dropdown-Menü **Mandant** einen Mandanten aus.
- 6 Wählen Sie aus dem Dropdown-Menü **Business-Gruppe** eine Business-Gruppe aus.  
Nur Benutzer in dieser Business-Gruppe können Maschinen mit dieser Reservierung bereitstellen.

- 7 (Optional) Wählen Sie aus dem Dropdown-Menü **Reservierungsrichtlinie** eine Reservierungsrichtlinie aus.

Diese Option setzt voraus, dass mindestens eine Reservierungsrichtlinie vorhanden ist. Sie können die Reservierung später bearbeiten, um eine Reservierungsrichtlinie anzugeben.

Sie verwenden eine Reservierungsrichtlinie zur Einschränkung der Bereitstellung auf bestimmte Reservierungen.

- 8 Geben Sie im Textfeld **Priorität** eine Zahl ein, um die Priorität für die Reservierung festzulegen.

Die Priorität wird verwendet, wenn eine Business-Gruppe über mehr als eine Reservierung verfügt. Einer Reservierung der Priorität 1 wird bei einer Bereitstellung der Vorzug gegenüber einer Reservierung der Priorität 2 gegeben.

- 9 (Optional) Deaktivieren Sie das Kontrollkästchen **Diese Reservierung aktivieren**, wenn Sie nicht möchten, dass diese Reservierung aktiv ist.

Verlassen Sie diese Seite nicht. Ihre Reservierung ist noch nicht abgeschlossen.

### Angeben von Ressourcen- und Netzwerkeinstellungen für OpenStack-Reservierungen

Geben Sie Ressourcen- und Netzwerkeinstellungen an, die für Maschinen verfügbar sind, die über diese vRealize Automation-Reservierung bereitgestellt werden.

#### Voraussetzungen

[Angeben von Informationen zu OpenStack-Reservierungen.](#)

#### Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Ressourcen**.
- 2 Wählen Sie aus dem Dropdown-Menü **Computing-Ressource** eine Computing-Ressource aus, auf der Maschinen bereitgestellt werden sollen.

Nur Vorlagen, die sich auf dem ausgewählten Cluster befinden, sind für das Klonen mit dieser Reservierung verfügbar.

Während der Bereitstellung werden die Maschinen auf einem Host platziert, der mit dem lokalen Speicher verbunden ist. Wenn die Reservierung lokalen Speicher verwendet, werden alle Maschinen, die mithilfe der Reservierung bereitgestellt werden, auf dem Host erstellt, der diesen lokalen Speicher enthält. Wenn Sie allerdings die benutzerdefinierte Eigenschaft `VirtualMachine.Admin.ForceHost` verwenden, mit der die Bereitstellung einer Maschine auf einem anderen Host erzwungen wird, schlägt die Bereitstellung fehl. Die Bereitstellung schlägt auch fehl, wenn sich die Vorlage, über die die Maschine geklont wird, auf lokalem Speicher befindet, aber einer Maschine in einem anderen Cluster hinzugefügt ist. In diesem Fall schlägt die Bereitstellung fehl, da kein Zugriff auf die Vorlage möglich ist.

- 3 (Optional) Geben Sie im Textfeld **Maschinenkontingent** eine Zahl ein, um die maximale Anzahl von Maschinen festzulegen, die in dieser Reservierung bereitgestellt werden können.

Nur eingeschaltete Maschinen werden beim Kontingent berücksichtigt. Lassen Sie das Feld leer, wenn die Reservierung unbegrenzt sein soll.

- 4 Wählen Sie aus dem Dropdown-Menü **Schlüsselpaar** eine Methode aus, wie Schlüsselpaare Computing-Instanzen zugewiesen werden sollen.

Option	Beschreibung
<b>Nicht angegeben</b>	Das Verhalten von Schlüsselpaaren wird auf der Blueprint-Ebene anstatt auf der Reservierungsebene gesteuert.
<b>Automatisch generiert pro Business-Gruppe</b>	Jede in einer Business-Gruppe bereitgestellte Maschine verfügt über dasselbe Schlüsselpaar. Dies trifft auch für Maschinen zu, die in anderen Reservierungen bereitgestellt wurden, sofern die Maschine dieselbe Computing-Ressource und Business-Gruppe aufweist. Da auf diese Weise generierte Schlüsselpaare mit einer Business-Gruppe verknüpft sind, werden die Schlüsselpaare beim Löschen der Business-Gruppe ebenfalls gelöscht.
<b>Automatisch generiert pro Maschine</b>	Jede Maschine weist ein eindeutiges Schlüsselpaar auf. Dies stellt die sicherste Methode dar, da keine Schlüsselpaare von Maschinen gemeinsam genutzt werden.
<b>Bestimmtes Schlüsselpaar</b>	Jede in dieser Reservierung bereitgestellte Maschine verfügt über dasselbe Schlüsselpaar. Suchen Sie nach einem Schlüsselpaar, das für diese Reservierung verwendet werden soll.

- 5 Wenn Sie im Dropdown-Menü **Schlüsselpaar** die Option **Bestimmtes Schlüsselpaar** ausgewählt haben, wählen Sie aus dem Dropdown-Menü **Bestimmtes Schlüsselpaar** einen Schlüsselpaarwert aus.
- 6 Wählen Sie aus der Liste **Sicherheitsgruppen** mindestens eine Sicherheitsgruppe aus, die einer Maschine während der Bereitstellung zugewiesen werden kann.
- 7 Klicken Sie auf die Registerkarte **Netzwerk**.

## 8 Konfigurieren Sie mit dieser Reservierung einen Netzwerkpfad für bereitgestellte Maschinen.

- a (Optional) Wenn die Option verfügbar ist, wählen Sie einen Speicher-Endpoint aus dem Drop-down-Menü **Endpoint** aus.

Die FlexClone-Option wird in der Endpoint-Spalte angezeigt, wenn ein NetApp ONTAP-Endpoint vorhanden ist und wenn der Host virtuell ist. Wenn ein NetApp ONTAP-Endpoint vorhanden ist, wird auf der Reservierungsseite der dem Speicherpfad zugewiesene Endpoint angezeigt. Wenn Sie einen Endpoint für einen Speicherpfad hinzufügen, aktualisieren oder löschen, wird die Änderung in allen zutreffenden Reservierungen angezeigt.

Wenn Sie einen Endpoint für einen Speicherpfad hinzufügen, aktualisieren oder löschen, wird die Änderung auf der Reservierungsseite angezeigt.

- b Wählen Sie aus der Liste **Netzwerkpfade** die Netzwerkpfade für durch diese Reservierung bereitgestellte Maschinen aus.
- c (Optional) Wählen Sie aus dem Dropdown-Menü **Netzwerkprofil** ein aufgelistetes Netzwerkprofil aus.

Diese Option setzt voraus, dass mindestens ein Netzwerkprofil vorhanden ist.

Sie können in einer Reservierung mehr als einen Netzwerkpfad auswählen, aber bei der Bereitstellung einer Maschine wird nur ein Netzwerk verwendet.

Sie können die Reservierung nun durch Klicken auf **Speichern** speichern. Sie können noch benutzerdefinierte Eigenschaften hinzufügen, um Reservierungsspezifikationen besser zu steuern. Zudem können Sie E-Mail-Warnungen konfigurieren, damit Sie Benachrichtigungen erhalten, wenn die dieser Reservierung zugeteilten Ressourcen einen niedrigen Stand erreichen.

### Angeben benutzerdefinierter Eigenschaften und Warnungen für OpenStack-Reservierungen

Sie können einer vRealize Automation-Reservierung benutzerdefinierte Eigenschaften zuordnen. Darüber hinaus können Sie Warnungen konfigurieren, um bei niedrigen Reservierungsressourcen E-Mail-Benachrichtigungen zu senden.

Benutzerdefinierte Eigenschaften und E-Mail-Warnungen sind optionale Konfigurationen für die Reservierung. Wenn Sie weder benutzerdefinierte Eigenschaften verknüpfen noch Warnungen festlegen möchten, klicken Sie auf **Speichern**, um die Erstellung der Reservierung zu beenden.

Sie können beliebig viele benutzerdefinierte Eigenschaften hinzufügen.

---

**Wichtig** Benachrichtigungen werden nur dann gesendet, wenn E-Mail-Warnungen konfiguriert und Benachrichtigungen aktiviert wurden.

---

Falls konfiguriert, werden Warnungen täglich generiert und nicht erst bei Erreichen des angegebenen Schwellenwerts.

### Voraussetzungen

[Angeben von Ressourcen- und Netzwerkeinstellungen für OpenStack-Reservierungen.](#)



### Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Eigenschaften**.
- 2 Klicken Sie auf **Neu**.
- 3 Geben Sie einen gültigen Namen für die benutzerdefinierte Eigenschaft ein.
- 4 Geben Sie gegebenenfalls einen Eigenschaftswert ein.
- 5 Klicken Sie auf **Speichern**.
- 6 (Optional) Fügen Sie zusätzliche benutzerdefinierte Eigenschaften hinzu.
- 7 Klicken Sie auf die Registerkarte **Warnungen**.
- 8 Aktivieren Sie das Kontrollkästchen **Kapazitätswarnungen**, um das Senden von Warnungen zu konfigurieren.
- 9 Verwenden Sie den Schieberegler, um für verfügbare Ressourcenzuteilungen Schwellenwerte festzulegen.
- 10 Geben Sie im Textfeld **Empfänger** mindestens eine E-Mail-Adresse eines Benutzers oder einen Gruppennamen ein, um festzulegen, wer Warnbenachrichtigungen erhalten soll.  
  
Drücken Sie die Eingabetaste, um mehrere Einträge zu trennen.
- 11 Wählen Sie **Warnungen an Gruppenmanager senden** aus, um Gruppenmanager in den Erhalt der E-Mail-Warnungen einzubeziehen.
- 12 Legen Sie eine Erinnerungshäufigkeit (in Tagen) fest.
- 13 Klicken Sie auf **Speichern**.

Die Reservierung wird gespeichert und in der Liste „Reservierungen“ angezeigt.

### Weiter

Sie können optionale Reservierungsrichtlinien konfigurieren oder mit der Vorbereitung auf die Bereitstellung beginnen.

Zur Erstellung von Blueprints autorisierte Benutzer können diese nun erstellen.

### Erstellen einer vCloud Air -Reservierung

Sie müssen Maschinen durch Erstellen einer vRealize Automation-Reservierung Ressourcen zuteilen, bevor Mitglieder einer Business-Gruppe die Maschinenbereitstellung anfordern können.

Jede Business-Gruppe benötigt mindestens eine Reservierung, damit ihre Mitglieder Maschinen dieses Typs bereitstellen können.

### Vorgehensweise

- 1 [Angaben von Reservierungsinformationen für vCloud Air](#)

Sie können für jedes vCloud Air-Maschinenabonnement bzw. für jede OnDemand-Ressource eine Reservierung erstellen. Jede Reservierung wird für eine bestimmte Business-Gruppe konfiguriert, um ihr die Berechtigung für das Anfordern von Maschinen zu erteilen.

## 2 Angeben von Ressourcen- und Netzwerkeinstellungen für eine vCloud Air-Reservierung

Geben Sie Ressourcen- und Netzwerkeinstellungen an, die für vCloud Air-Maschinen verfügbar sind, die über diese vRealize Automation-Reservierung bereitgestellt werden.

## 3 Angeben benutzerdefinierter Eigenschaften und Warnungen für eine vCloud Air-Reservierung

Sie können einer vRealize Automation-Reservierung benutzerdefinierte Eigenschaften zuordnen. Darüber hinaus können Sie Warnungen konfigurieren, um bei niedrigen Reservierungsressourcen E-Mail-Benachrichtigungen zu senden.

### Weiter

Sie können optionale Reservierungsrichtlinien konfigurieren oder mit der Vorbereitung auf die Bereitstellung beginnen.

Zur Erstellung von Blueprints autorisierte Benutzer können diese nun erstellen.

### Angeben von Reservierungsinformationen für vCloud Air

Sie können für jedes vCloud Air-Maschinenabonnement bzw. für jede OnDemand-Ressource eine Reservierung erstellen. Jede Reservierung wird für eine bestimmte Business-Gruppe konfiguriert, um ihr die Berechtigung für das Anfordern von Maschinen zu erteilen.

Sie können die Anzeige von Reservierungen beim Hinzufügen, Bearbeiten oder Löschen steuern, indem Sie auf der Seite „Reservierungen“ die Option **Nach Kategorie filtern** verwenden. Beachten Sie, dass Test-Agent-Reservierungen beim Filtern nach Kategorie nicht in der Reservierungsliste angezeigt werden.

---

**Hinweis** Nach dem Erstellen einer Reservierung können Sie die Zuordnungen der Business-Gruppen oder Computing-Ressourcen nicht mehr ändern.

---

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.
- Stellen Sie sicher, dass der Mandantenadministrator mindestens eine Business-Gruppe erstellt hat.
- Stellen Sie sicher, dass eine Computing-Ressource vorhanden ist.
- Konfigurieren Sie die Netzwerkeinstellungen.
- (Optional) Konfigurieren Sie die Informationen zum Netzwerkprofil.

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Reservierungen** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)** und wählen Sie den zu erstellenden Reservierungstyp aus.  
Die verfügbaren Typen von Cloud-Reservierungen sind Amazon, OpenStack, vCloud Air und vCloud Director.  
Wählen Sie **vCloud Air** aus.

- 3 (Optional) Wählen Sie aus dem Dropdown-Menü **Aus vorhandener Reservierung kopieren** eine vorhandene Reservierung aus.

Die Daten zu der ausgewählten Reservierung wird angezeigt. Sie können für Ihre neue Reservierung bei Bedarf Änderungen vornehmen.

- 4 Geben Sie im Textfeld **Name** einen Namen ein.

- 5 Wählen Sie aus dem Dropdown-Menü **Mandant** einen Mandanten aus.

- 6 Wählen Sie aus dem Dropdown-Menü **Business-Gruppe** eine Business-Gruppe aus.

Nur Benutzer in dieser Business-Gruppe können Maschinen mit dieser Reservierung bereitstellen.

- 7 (Optional) Wählen Sie aus dem Dropdown-Menü **Reservierungsrichtlinie** eine Reservierungsrichtlinie aus.

Diese Option setzt voraus, dass mindestens eine Reservierungsrichtlinie vorhanden ist. Sie können die Reservierung später bearbeiten, um eine Reservierungsrichtlinie anzugeben.

Sie verwenden eine Reservierungsrichtlinie zur Einschränkung der Bereitstellung auf bestimmte Reservierungen.

- 8 Geben Sie im Textfeld **Priorität** eine Zahl ein, um die Priorität für die Reservierung festzulegen.

Die Priorität wird verwendet, wenn eine Business-Gruppe über mehr als eine Reservierung verfügt. Einer Reservierung der Priorität 1 wird bei einer Bereitstellung der Vorzug gegenüber einer Reservierung der Priorität 2 gegeben.

- 9 (Optional) Deaktivieren Sie das Kontrollkästchen **Diese Reservierung aktivieren**, wenn Sie nicht möchten, dass diese Reservierung aktiv ist.

Verlassen Sie diese Seite nicht. Ihre Reservierung ist noch nicht abgeschlossen.

### Angeben von Ressourcen- und Netzwerkeinstellungen für eine vCloud Air -Reservierung

Geben Sie Ressourcen- und Netzwerkeinstellungen an, die für vCloud Air-Maschinen verfügbar sind, die über diese vRealize Automation-Reservierung bereitgestellt werden.

Die verfügbaren Ressourcenzuteilungsmodelle für über eine vCloud Director-Reservierung bereitgestellte Maschinen sind „Zuteilungspool“, „Im Voraus bezahlen“ und „Reservierungspool“. Für „Im Voraus bezahlen“ müssen Sie keine Speicher- oder Arbeitsspeicherwerte angeben, allerdings müssen Sie für den Speicherpfad eine Priorität festlegen. Ausführliche Informationen zu diesen Zuteilungsmodellen finden Sie in der vCloud Air-Dokumentation.

Sie können ein Standardspeicherprofil oder ein Speicherprofil auf Festplattenebene angeben. Datenspeicher auf mehreren Ebenen ist auf vCloud Air-Endpoints verfügbar.

Für Integrationen mit Storage Distributed Resource Scheduler-Speicher (SDRS-Speicher) können Sie einen Speicher-Cluster auswählen, sodass SDRS automatisch Speicherplatzierung und Lastausgleich für von dieser Reservierung bereitgestellte Maschinen verarbeiten kann. Der SDRS-Automatisierungsmodus muss auf „Automatisch“ festgelegt werden. Andernfalls wählen Sie innerhalb des Clusters einen Datenspeicher für das Verhalten von eigenständigen Datenspeichern aus. SDRS wird für FlexClone-Speichergeräte nicht unterstützt.

---

**Hinweis** Für vCloud Air-Endpoints und vCloud Director-Endpoints definierte Reservierungen wird die Verwendung von Netzwerkprofilen für die Bereitstellung von Maschinen nicht unterstützt.

---

## Voraussetzungen

### Angeben von Reservierungsinformationen für vCloud Director.

#### Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Ressourcen**.
- 2 Wählen Sie aus dem Dropdown-Menü **Computing-Ressource** eine Computing-Ressource aus, auf der Maschinen bereitgestellt werden sollen.  
  
Nur Vorlagen, die sich auf dem ausgewählten Cluster befinden, sind für das Klonen mit dieser Reservierung verfügbar.
- 3 Wählen Sie ein Zuweisungsmodell aus.
- 4 (Optional) Geben Sie im Textfeld **Maschinenkontingent** eine Zahl ein, um die maximale Anzahl von Maschinen festzulegen, die in dieser Reservierung bereitgestellt werden können.  
  
Nur eingeschaltete Maschinen werden beim Kontingent berücksichtigt. Lassen Sie das Feld leer, wenn die Reservierung unbegrenzt sein soll.
- 5 Geben Sie die Menge des Arbeitsspeichers in GB an, die dieser Reservierung aus der Speichertabelle zugewiesen werden soll.  
  
Der gesamte Arbeitsspeicherwert für die Reservierung wird Ihrer Auswahl der Computing-Ressource entnommen.
- 6 Wählen Sie mindestens einen aufgelisteten Speicherpfad aus.  
  
Die verfügbaren Speicherpfad-Optionen werden Ihrer Auswahl der Computing-Ressource entnommen.
  - a Geben Sie im Textfeld **Diese Reservierung wurde vorgenommen** einen Wert ein, um festzulegen, wie viel Speicher dieser Reservierung zugewiesen werden soll.
  - b Geben Sie im Textfeld **Priorität** einen Wert ein, um den Prioritätswert für den Speicherpfad im Verhältnis zu anderen Speicherpfaden anzugeben, die sich auf diese Reservierung beziehen.  
  
Die Priorität wird für mehrere Speicherpfade verwendet. Ein Speicherpfad der Priorität 0 wird vor einem Pfad der Priorität 1 verwendet.

- c Klicken Sie auf die Option **Deaktivieren**, wenn Sie nicht möchten, dass der Speicherpfad für die Verwendung durch diese Reservierung aktiviert wird.
- d Wiederholen Sie diesen Schritt zur Konfiguration von Clustern und Datenspeichern, sofern dies notwendig ist.

7 Klicken Sie auf die Registerkarte **Netzwerk**.

8 Konfigurieren Sie mit dieser Reservierung einen Netzwerkpfad für bereitgestellte Maschinen.

- a (Optional) Wenn die Option verfügbar ist, wählen Sie einen Speicher-Endpoint aus dem Drop-down-Menü **Endpoint** aus.

Die FlexClone-Option wird in der Endpoint-Spalte angezeigt, wenn ein NetApp ONTAP-Endpoint vorhanden ist und wenn der Host virtuell ist. Wenn ein NetApp ONTAP-Endpoint vorhanden ist, wird auf der Reservierungsseite der dem Speicherpfad zugewiesene Endpoint angezeigt. Wenn Sie einen Endpoint für einen Speicherpfad hinzufügen, aktualisieren oder löschen, wird die Änderung in allen zutreffenden Reservierungen angezeigt.

Wenn Sie einen Endpoint für einen Speicherpfad hinzufügen, aktualisieren oder löschen, wird die Änderung auf der Reservierungsseite angezeigt.

- b Wählen Sie aus der Liste **Netzwerkpfade** die Netzwerkpfade für durch diese Reservierung bereitgestellte Maschinen aus.
- c (Optional) Wählen Sie aus dem Dropdown-Menü **Netzwerkprofil** ein aufgelistetes Netzwerkprofil aus.

Diese Option setzt voraus, dass mindestens ein Netzwerkprofil vorhanden ist.

Sie können in einer Reservierung mehr als einen Netzwerkpfad auswählen, aber bei der Bereitstellung einer Maschine wird nur ein Netzwerk verwendet.

Sie können die Reservierung nun durch Klicken auf **Speichern** speichern. Sie können noch benutzerdefinierte Eigenschaften hinzufügen, um Reservierungsspezifikationen besser zu steuern. Zudem können Sie E-Mail-Warnungen konfigurieren, damit Sie Benachrichtigungen erhalten, wenn die dieser Reservierung zugeteilten Ressourcen einen niedrigen Stand erreichen.

### Angeben benutzerdefinierter Eigenschaften und Warnungen für eine vCloud Air - Reservierung

Sie können einer vRealize Automation-Reservierung benutzerdefinierte Eigenschaften zuordnen. Darüber hinaus können Sie Warnungen konfigurieren, um bei niedrigen Reservierungsressourcen E-Mail-Benachrichtigungen zu senden.

Benutzerdefinierte Eigenschaften und E-Mail-Warnungen sind optionale Konfigurationen für die Reservierung. Wenn Sie weder benutzerdefinierte Eigenschaften verknüpfen noch Warnungen festlegen möchten, klicken Sie auf **Speichern**, um die Erstellung der Reservierung zu beenden.

Sie können beliebig viele benutzerdefinierte Eigenschaften hinzufügen.

Falls konfiguriert, werden Warnungen täglich generiert und nicht erst bei Erreichen des angegebenen Schwellenwerts.

---

**Wichtig** Benachrichtigungen werden nur dann gesendet, wenn E-Mail-Warnungen konfiguriert und Benachrichtigungen aktiviert wurden.

---

Für Vorausbezahlungs-Reservierungen, die ohne angegebene Grenzwerte erstellt wurden, sind Warnungen nicht verfügbar.

## Voraussetzungen

### [Angaben von Ressourcen- und Netzwerkeinstellungen für eine vCloud Air-Reservierung](#)

## Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Eigenschaften**.
- 2 Klicken Sie auf **Neu**.
- 3 Geben Sie einen gültigen Namen für die benutzerdefinierte Eigenschaft ein.
- 4 Geben Sie gegebenenfalls einen Eigenschaftswert ein.
- 5 (Optional) Aktivieren Sie das Kontrollkästchen **Verschlüsselt**, um den Eigenschaftswert zu verschlüsseln.
- 6 (Optional) Aktivieren Sie das Kontrollkästchen **Eingabeaufforderung**, damit Benutzer einen Wert eingeben müssen.  
  
Diese Option kann bei der Bereitstellung nicht außer Kraft gesetzt werden.
- 7 Klicken Sie auf **Speichern**.
- 8 (Optional) Fügen Sie zusätzliche benutzerdefinierte Eigenschaften hinzu.
- 9 Klicken Sie auf die Registerkarte **Warnungen**.
- 10 Aktivieren Sie das Kontrollkästchen **Kapazitätswarnungen**, um das Senden von Warnungen zu konfigurieren.
- 11 Verwenden Sie den Schieberegler, um für verfügbare Ressourcenzuteilungen Schwellenwerte festzulegen.
- 12 Geben Sie im Textfeld **Empfänger** mindestens eine E-Mail-Adresse eines Benutzers oder einen Gruppennamen ein, um festzulegen, wer Warnbenachrichtigungen erhalten soll.  
  
Drücken Sie die Eingabetaste, um mehrere Einträge zu trennen.
- 13 Wählen Sie **Warnungen an Gruppenmanager senden** aus, um Gruppenmanager in den Erhalt der E-Mail-Warnungen einzubeziehen.
- 14 Legen Sie eine Erinnerungshäufigkeit (in Tagen) fest.
- 15 Klicken Sie auf **Speichern**.

Die Reservierung wird gespeichert und in der Liste „Reservierungen“ angezeigt.

## Erstellen einer vCloud Director -Reservierung

Sie müssen Maschinen durch Erstellen einer vRealize Automation-Reservierung Ressourcen zuteilen, bevor Mitglieder einer Business-Gruppe die Maschinenbereitstellung anfordern können.

Jede Business-Gruppe benötigt mindestens eine Reservierung, damit ihre Mitglieder Maschinen dieses Typs bereitstellen können.

### Vorgehensweise

#### 1 Angeben von Reservierungsinformationen für vCloud Director

Sie können für jedes Organisations-vDC (virtuelles Datencenter) von vCloud Director eine Reservierung erstellen. Jede Reservierung wird für eine bestimmte Business-Gruppe konfiguriert, um ihr die Berechtigung für das Anfordern von Maschinen auf einer angegebenen Computing-Ressource zu erteilen.

#### 2 Angeben von Ressourcen- und Netzwerkeinstellungen für eine vCloud Director-Reservierung

Geben Sie Ressourcen- und Netzwerkeinstellungen an, die für vCloud Director-Maschinen verfügbar sind, die über diese vRealize Automation-Reservierung bereitgestellt werden.

#### 3 Angeben benutzerdefinierter Eigenschaften und Warnungen für vCloud Director-Reservierungen

Sie können einer vRealize Automation-Reservierung benutzerdefinierte Eigenschaften zuordnen. Darüber hinaus können Sie Warnungen konfigurieren, um bei niedrigen Reservierungsressourcen E-Mail-Benachrichtigungen zu senden.

### Weiter

Sie können optionale Reservierungsrichtlinien konfigurieren oder mit der Vorbereitung auf die Bereitstellung beginnen.

Zur Erstellung von Blueprints autorisierte Benutzer können diese nun erstellen.

### Angeben von Reservierungsinformationen für vCloud Director

Sie können für jedes Organisations-vDC (virtuelles Datencenter) von vCloud Director eine Reservierung erstellen. Jede Reservierung wird für eine bestimmte Business-Gruppe konfiguriert, um ihr die Berechtigung für das Anfordern von Maschinen auf einer angegebenen Computing-Ressource zu erteilen.

Sie können die Anzeige von Reservierungen beim Hinzufügen, Bearbeiten oder Löschen steuern, indem Sie auf der Seite „Reservierungen“ die Option **Nach Kategorie filtern** verwenden. Beachten Sie, dass Test-Agent-Reservierungen beim Filtern nach Kategorie nicht in der Reservierungsliste angezeigt werden.

---

**Hinweis** Nach dem Erstellen einer Reservierung können Sie die Zuordnungen der Business-Gruppen oder Computing-Ressourcen nicht mehr ändern.

---

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.
- Stellen Sie sicher, dass der Mandantenadministrator mindestens eine Business-Gruppe erstellt hat.

- Stellen Sie sicher, dass eine Computing-Ressource vorhanden ist.
- Konfigurieren Sie die Netzwerkeinstellungen.
- (Optional) Konfigurieren Sie die Informationen zum Netzwerkprofil.

#### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Reservierungen** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)** und wählen Sie den zu erstellenden Reservierungstyp aus.  
Die verfügbaren Typen von Cloud-Reservierungen sind Amazon, OpenStack, vCloud Air und vCloud Director.  
Wählen Sie **vCloud Director** aus.
- 3 (Optional) Wählen Sie aus dem Dropdown-Menü **Aus vorhandener Reservierung kopieren** eine vorhandene Reservierung aus.  
Die Daten zu der ausgewählten Reservierung wird angezeigt. Sie können für Ihre neue Reservierung bei Bedarf Änderungen vornehmen.
- 4 Geben Sie im Textfeld **Name** einen Namen ein.
- 5 Wählen Sie aus dem Dropdown-Menü **Mandant** einen Mandanten aus.
- 6 Wählen Sie aus dem Dropdown-Menü **Business-Gruppe** eine Business-Gruppe aus.  
Nur Benutzer in dieser Business-Gruppe können Maschinen mit dieser Reservierung bereitstellen.
- 7 (Optional) Wählen Sie aus dem Dropdown-Menü **Reservierungsrichtlinie** eine Reservierungsrichtlinie aus.  
Diese Option setzt voraus, dass mindestens eine Reservierungsrichtlinie vorhanden ist. Sie können die Reservierung später bearbeiten, um eine Reservierungsrichtlinie anzugeben.  
Sie verwenden eine Reservierungsrichtlinie zur Einschränkung der Bereitstellung auf bestimmte Reservierungen.
- 8 Geben Sie im Textfeld **Priorität** eine Zahl ein, um die Priorität für die Reservierung festzulegen.  
Die Priorität wird verwendet, wenn eine Business-Gruppe über mehr als eine Reservierung verfügt. Einer Reservierung der Priorität 1 wird bei einer Bereitstellung der Vorzug gegenüber einer Reservierung der Priorität 2 gegeben.
- 9 (Optional) Deaktivieren Sie das Kontrollkästchen **Diese Reservierung aktivieren**, wenn Sie nicht möchten, dass diese Reservierung aktiv ist.

Verlassen Sie diese Seite nicht. Ihre Reservierung ist noch nicht abgeschlossen.

#### Angeben von Ressourcen- und Netzwerkeinstellungen für eine vCloud Director - Reservierung

Geben Sie Ressourcen- und Netzwerkeinstellungen an, die für vCloud Director-Maschinen verfügbar sind, die über diese vRealize Automation-Reservierung bereitgestellt werden.



Die verfügbaren Ressourcenzuteilungsmodelle für über eine vCloud Director-Reservierung bereitgestellte Maschinen sind „Zuteilungspool“, „Im Voraus bezahlen“ und „Reservierungspool“. Für „Im Voraus bezahlen“ müssen Sie keine Speicher- oder Arbeitsspeicherwerte angeben, allerdings müssen Sie für den Speicherpfad eine Priorität festlegen. Ausführliche Informationen zu diesen Zuteilungsmodellen finden Sie in der vCloud Director-Dokumentation.

Sie können ein Standardspeicherprofil oder ein Speicherprofil auf Festplattenebene angeben. Datenspeicher auf mehreren Ebenen ist für vCloud Director 5.6 und höhere Endpoints verfügbar. Datenspeicher auf mehreren Ebenen wird nicht für vCloud Director 5.5-Endpoints unterstützt.

Für Integrationen mit Storage Distributed Resource Scheduler-Speicher (SDRS-Speicher) können Sie einen Speicher-Cluster auswählen, sodass SDRS automatisch Speicherplatzierung und Lastausgleich für von dieser Reservierung bereitgestellte Maschinen verarbeiten kann. Der SDRS-Automatisierungsmodus muss auf „Automatisch“ festgelegt werden. Andernfalls wählen Sie innerhalb des Clusters einen Datenspeicher für das Verhalten von eigenständigen Datenspeichern aus. SDRS wird für FlexClone-Speichergeräte nicht unterstützt.

---

**Hinweis** Für vCloud Air-Endpoints und vCloud Director-Endpoints definierte Reservierungen wird die Verwendung von Netzwerkprofilen für die Bereitstellung von Maschinen nicht unterstützt.

---

## Voraussetzungen

Angeben von Reservierungsinformationen für vCloud Director.

### Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Ressourcen**.
- 2 Wählen Sie aus dem Dropdown-Menü **Computing-Ressource** eine Computing-Ressource aus, auf der Maschinen bereitgestellt werden sollen.  
  
Nur Vorlagen, die sich auf dem ausgewählten Cluster befinden, sind für das Klonen mit dieser Reservierung verfügbar.
- 3 Wählen Sie ein Zuweisungsmodell aus.
- 4 (Optional) Geben Sie im Textfeld **Maschinenkontingent** eine Zahl ein, um die maximale Anzahl von Maschinen festzulegen, die in dieser Reservierung bereitgestellt werden können.  
  
Nur eingeschaltete Maschinen werden beim Kontingent berücksichtigt. Lassen Sie das Feld leer, wenn die Reservierung unbegrenzt sein soll.
- 5 Geben Sie die Menge des Arbeitsspeichers in GB an, die dieser Reservierung aus der Speichertabelle zugewiesen werden soll.  
  
Der gesamte Arbeitsspeicherwert für die Reservierung wird Ihrer Auswahl der Computing-Ressource entnommen.

## 6 Wählen Sie mindestens einen aufgelisteten Speicherpfad aus.

Die verfügbaren Speicherpfad-Optionen werden Ihrer Auswahl der Computing-Ressource entnommen.

- a Geben Sie im Textfeld **Diese Reservierung wurde vorgenommen** einen Wert ein, um festzulegen, wie viel Speicher dieser Reservierung zugewiesen werden soll.
- b Geben Sie im Textfeld **Priorität** einen Wert ein, um den Prioritätswert für den Speicherpfad im Verhältnis zu anderen Speicherpfaden anzugeben, die sich auf diese Reservierung beziehen.

Die Priorität wird für mehrere Speicherpfade verwendet. Ein Speicherpfad der Priorität 0 wird vor einem Pfad der Priorität 1 verwendet.

- c Klicken Sie auf die Option **Deaktivieren**, wenn Sie nicht möchten, dass der Speicherpfad für die Verwendung durch diese Reservierung aktiviert wird.
- d Wiederholen Sie diesen Schritt zur Konfiguration von Clustern und Datenspeichern, sofern dies notwendig ist.

## 7 Klicken Sie auf die Registerkarte **Netzwerk**.

## 8 Konfigurieren Sie mit dieser Reservierung einen Netzwerkpfad für bereitgestellte Maschinen.

- a (Optional) Wenn die Option verfügbar ist, wählen Sie einen Speicher-Endpoint aus dem Dropdown-Menü **Endpoint** aus.

Die FlexClone-Option wird in der Endpoint-Spalte angezeigt, wenn ein NetApp ONTAP-Endpoint vorhanden ist und wenn der Host virtuell ist. Wenn ein NetApp ONTAP-Endpoint vorhanden ist, wird auf der Reservierungsseite der dem Speicherpfad zugewiesene Endpoint angezeigt. Wenn Sie einen Endpoint für einen Speicherpfad hinzufügen, aktualisieren oder löschen, wird die Änderung in allen zutreffenden Reservierungen angezeigt.

Wenn Sie einen Endpoint für einen Speicherpfad hinzufügen, aktualisieren oder löschen, wird die Änderung auf der Reservierungsseite angezeigt.

- b Wählen Sie aus der Liste **Netzwerkpfade** die Netzwerkpfade für durch diese Reservierung bereitgestellte Maschinen aus.
- c (Optional) Wählen Sie aus dem Dropdown-Menü **Netzwerkprofil** ein aufgelistetes Netzwerkprofil aus.

Diese Option setzt voraus, dass mindestens ein Netzwerkprofil vorhanden ist.

Sie können in einer Reservierung mehr als einen Netzwerkpfad auswählen, aber bei der Bereitstellung einer Maschine wird nur ein Netzwerk verwendet.

Sie können die Reservierung nun durch Klicken auf **Speichern** speichern. Sie können noch benutzerdefinierte Eigenschaften hinzufügen, um Reservierungsspezifikationen besser zu steuern. Zudem können Sie E-Mail-Warnungen konfigurieren, damit Sie Benachrichtigungen erhalten, wenn die dieser Reservierung zugeteilten Ressourcen einen niedrigen Stand erreichen.

## Angeben benutzerdefinierter Eigenschaften und Warnungen für vCloud Director - Reservierungen

Sie können einer vRealize Automation-Reservierung benutzerdefinierte Eigenschaften zuordnen. Darüber hinaus können Sie Warnungen konfigurieren, um bei niedrigen Reservierungsressourcen E-Mail-Benachrichtigungen zu senden.

Benutzerdefinierte Eigenschaften und E-Mail-Warnungen sind optionale Konfigurationen für die Reservierung. Wenn Sie weder benutzerdefinierte Eigenschaften verknüpfen noch Warnungen festlegen möchten, klicken Sie auf **Speichern**, um die Erstellung der Reservierung zu beenden.

Sie können beliebig viele benutzerdefinierte Eigenschaften hinzufügen.

Falls konfiguriert, werden Warnungen täglich generiert und nicht erst bei Erreichen des angegebenen Schwellenwerts.

---

**Wichtig** Benachrichtigungen werden nur dann gesendet, wenn E-Mail-Warnungen konfiguriert und Benachrichtigungen aktiviert wurden.

---

Für Vorausbezahlungs-Reservierungen, die ohne angegebene Grenzwerte erstellt wurden, sind Warnungen nicht verfügbar.

### Voraussetzungen

[Angaben von Ressourcen- und Netzwerkeinstellungen für eine vCloud Director-Reservierung.](#)

### Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Eigenschaften**.
- 2 Klicken Sie auf **Neu**.
- 3 Geben Sie einen gültigen Namen für die benutzerdefinierte Eigenschaft ein.
- 4 Geben Sie gegebenenfalls einen Eigenschaftswert ein.
- 5 (Optional) Aktivieren Sie das Kontrollkästchen **Verschlüsselt**, um den Eigenschaftswert zu verschlüsseln.
- 6 (Optional) Aktivieren Sie das Kontrollkästchen **Eingabeaufforderung**, damit Benutzer einen Wert eingeben müssen.  
Diese Option kann bei der Bereitstellung nicht außer Kraft gesetzt werden.
- 7 Klicken Sie auf **Speichern**.
- 8 (Optional) Fügen Sie zusätzliche benutzerdefinierte Eigenschaften hinzu.
- 9 Klicken Sie auf die Registerkarte **Warnungen**.
- 10 Aktivieren Sie das Kontrollkästchen **Kapazitätswarnungen**, um das Senden von Warnungen zu konfigurieren.
- 11 Verwenden Sie den Schieberegler, um für verfügbare Ressourcenzuteilungen Schwellenwerte festzulegen.

- 12 Geben Sie im Textfeld **Empfänger** mindestens eine E-Mail-Adresse eines Benutzers oder einen Gruppennamen ein, um festzulegen, wer Warnbenachrichtigungen erhalten soll.

Drücken Sie die Eingabetaste, um mehrere Einträge zu trennen.

- 13 Wählen Sie **Warnungen an Gruppenmanager senden** aus, um Gruppenmanager in den Erhalt der E-Mail-Warnungen einzubeziehen.

- 14 Legen Sie eine Erinnerungshäufigkeit (in Tagen) fest.

- 15 Klicken Sie auf **Speichern**.

Die Reservierung wird gespeichert und in der Liste „Reservierungen“ angezeigt.

### Szenario: Erstellen einer Amazon-Reservierung für eine Proof-of-Concept-Umgebung

Da Sie einen SSH-Tunnel verwendet haben, um eine temporäre Netzwerk-zu-Amazon-VPC-Verbindung für Ihre Machbarkeitsnachweis-Umgebung einzurichten, müssen Sie benutzerdefinierte Eigenschaften zu Ihren Amazon-Reservierungen hinzufügen, um sicherzustellen, dass der Software-Bootstrap-Agent und der Gast-Agent Kommunikationen über den Tunnel leiten.

Die Netzwerk-zu-Amazon-VPC-Verbindung ist nur erforderlich, wenn Sie den Gast-Agent zum Anpassen der bereitgestellten Maschinen verwenden möchten, oder wenn Sie Software-Komponenten in Ihre Blueprints einschließen möchten. Für eine Produktionsumgebung würden Sie diese Verbindung offiziell über Amazon Web Services konfigurieren; da Sie jedoch in einer Machbarkeitsnachweis-Umgebung arbeiten, haben Sie stattdessen einen temporären SSH-Tunnel konfiguriert.

Nutzen Sie Ihre Fabric-Administratorrechte, um eine Reservierung zu erstellen, mit der Sie Ihre Amazon Web Services-Ressourcen zuweisen. Daneben schließen Sie mehrere benutzerdefinierte Eigenschaften ein, um den SSH-Tunnel zu unterstützen. Daneben konfigurieren Sie die Reservierung in der gleichen Region und VPC wie die Tunnelmaschine.

#### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.
- Konfigurieren Sie einen SSH-Tunnel, um eine Netzwerk-zu-Amazon-VPC-Verbindung herzustellen. Notieren Sie sich das Subnetz, die Sicherheitsgruppe und die private IP-Adresse Ihrer Amazon AWS-Tunnelmaschine. Siehe [Szenario: Konfigurieren der VPC-Konnektivität zwischen Netzwerk und Amazon für eine Proof-of-Concept-Umgebung](#).
- Erstellen Sie eine Business-Gruppe für Mitglieder Ihrer IT-Organisation, die Blueprints in Ihrer Machbarkeitsnachweis-Umgebung bearbeiten müssen. Siehe [Erstellen einer Business-Gruppe](#).
- Stellen Sie sicher, dass der Mandantenadministrator mindestens eine Business-Gruppe erstellt hat.

#### Vorgehensweise

- 1 [Szenario: Angeben von Amazon AWS-Reservierungsinformationen für eine Machbarkeitsnachweis-Umgebung](#)

Sie möchten Ressourcen für Ihr Team aus Blueprint-Architekten reservieren, damit diese die Funktionalität in Ihrer Machbarkeitsnachweis-Umgebung testen können. Daher konfigurieren Sie diese Reservierung, um Ihrer Business-Gruppe für Architekten Ressourcen zuzuteilen.

## 2 Szenario: Angeben von Amazon AWS-Netzwerkeinstellungen für eine Proof-of-Concept-Umgebung

Sie konfigurieren die Reservierung so, dass die gleichen Einstellungen für Region und Netzwerk wie für die Tunnelmaschine verwendet werden. Außerdem beschränken Sie die Anzahl der Maschinen, die für diese Reservierung eingeschaltet werden können, um die Ressourcenauslastung zu verwalten.

## 3 Szenario: Angeben von benutzerdefinierten Eigenschaften zur Ausführung von Agent-Kommunikationen über Ihren Tunnel

Beim Konfigurieren der Netzwerk-zu-Amazon-VPC-Konnektivität haben Sie die Portweiterleitung konfiguriert, um Ihrer Amazon AWS-Tunnelmaschine den Zugriff auf vRealize Automation-Ressourcen zu gestatten. Sie müssen der Reservierung benutzerdefinierte Eigenschaften hinzufügen, um die Agents für den Zugriff auf diese Ports zu konfigurieren.

### Szenario: Angeben von Amazon AWS -Reservierungsinformationen für eine Machbarkeitsnachweis-Umgebung

Sie möchten Ressourcen für Ihr Team aus Blueprint-Architekten reservieren, damit diese die Funktionalität in Ihrer Machbarkeitsnachweis-Umgebung testen können. Daher konfigurieren Sie diese Reservierung, um Ihrer Business-Gruppe für Architekten Ressourcen zuzuteilen.

---

**Hinweis** Nach dem Erstellen einer Reservierung können Sie die Zuordnungen der Business-Gruppen oder Computing-Ressourcen nicht mehr ändern.

---

#### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Reservierungen** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)** und wählen Sie den zu erstellenden Reservierungstyp aus.  
Wählen Sie **Amazon** aus.
- 3 Geben Sie **Amazon Tunnel PoC** in das Textfeld **Name** ein.
- 4 Wählen Sie die Business-Gruppe, die Sie für Ihre Blueprint-Architekten erstellt haben, im Dropdown-Menü **Business-Gruppe** aus.
- 5 Geben Sie **1** in das Textfeld **Priorität** ein, um diese Reservierung als höchste Priorität festzulegen.

Sie haben die Business-Gruppe und die Priorität für die Reservierung konfiguriert; Sie müssen jedoch noch Ressourcen zuteilen und die benutzerdefinierten Eigenschaften für den SSH-Tunnel konfigurieren.

### Szenario: Angeben von Amazon AWS -Netzwerkeinstellungen für eine Proof-of-Concept-Umgebung

Sie konfigurieren die Reservierung so, dass die gleichen Einstellungen für Region und Netzwerk wie für die Tunnelmaschine verwendet werden. Außerdem beschränken Sie die Anzahl der Maschinen, die für diese Reservierung eingeschaltet werden können, um die Ressourcenauslastung zu verwalten.

#### Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Ressourcen**.

- 2 Wählen Sie aus dem Dropdown-Menü **Computing-Ressource** eine Computing-Ressource aus, auf der Maschinen bereitgestellt werden sollen.

Wählen Sie die Amazon AWS-Region aus, in der sich Ihre Tunnelmaschine befindet.

- 3 (Optional) Geben Sie im Textfeld **Maschinenkontingent** eine Zahl ein, um die maximale Anzahl von Maschinen festzulegen, die in dieser Reservierung bereitgestellt werden können.

Nur eingeschaltete Maschinen werden beim Kontingent berücksichtigt. Lassen Sie das Feld leer, wenn die Reservierung unbegrenzt sein soll.

- 4 Wählen Sie im Dropdown-Menü **Schlüsselpaar** die Option **Schlüsselpaar angeben** aus.

Da es sich hierbei um eine Proof-of-Concept-Umgebung handelt, wählen Sie die Freigabe eines einzelnen Schlüsselpaars für alle mithilfe dieser Reservierung freigegebenen Maschinen.

- 5 Wählen Sie das Schlüsselpaar, dass Sie mit den Architektenbenutzern gemeinsam verwenden möchten, im Dropdown-Menü **Schlüsselpaar** aus.

- 6 Aktivieren Sie das Kontrollkästchen **Einem Subnetz in einem VPC zuweisen**.

- 7 Wählen Sie das gleiche Subnetz und die gleichen Sicherheitsgruppen aus, die auch von der Tunnelmaschine verwendet werden.

Sie haben die Reservierung so konfiguriert, dass die gleichen Regions- und Netzwerkeinstellungen verwendet werden wie für die Tunnelmaschine. Sie müssen jedoch weiterhin benutzerdefinierte Eigenschaften hinzufügen, um sicherzustellen, dass die Kommunikation des Bootstrap-Agent und des Gast-Agent von Software über den Tunnel durchgeführt werden.

### Szenario: Angeben von benutzerdefinierten Eigenschaften zur Ausführung von Agent-Kommunikationen über Ihren Tunnel

Beim Konfigurieren der Netzwerk-zu-Amazon-VPC-Konnektivität haben Sie die Portweiterleitung konfiguriert, um Ihrer Amazon AWS-Tunnelmaschine den Zugriff auf vRealize Automation-Ressourcen zu gestatten. Sie müssen der Reservierung benutzerdefinierte Eigenschaften hinzufügen, um die Agents für den Zugriff auf diese Ports zu konfigurieren.

#### Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Eigenschaften**.
- 2 Klicken Sie auf **Neu**.
- 3 Konfigurieren Sie die benutzerdefinierten Tunneleigenschaften.

Verwenden Sie die private IP-Adresse Ihrer Amazon AWSTunnelmaschine sowie Port 1443, den Sie beim Aufrufen des SSH-Tunnels für *vRealize\_automation\_appliance\_fqdn* zugewiesen haben.

Option	Wert
<code>software.ebs.url</code>	<code>https://Private_IP:1443/event-broker-service/api</code>
<code>software.agent.service.url</code>	<code>https://Private_IP:1443/software-service/api</code>
<code>agent.download.url</code>	<code>https://Private_IP:1443/software-service/resources/nobel-agent.jar</code>

#### 4 Klicken Sie auf **Speichern**.

Sie haben eine Reservierung erstellt, um Amazon AWS-Ressourcen der Business-Gruppe Ihrer Architekten zuzuteilen. Sie haben die Reservierung für die Unterstützung des Gast-Agent und des Software-Bootstrap-Agent konfiguriert. Die Architekten können Blueprints erstellen, die den Gast-Agent nutzen, um bereitgestellte Maschinen anzupassen oder Software-Komponenten hinzuzufügen.

#### **Erstellen virtueller Kategoriereservierungen**

Eine virtuelle Reservierung eines Kategorietyps bietet Zugriff auf die Bereitstellungsdienste einer Bereitstellung virtueller Maschinen für eine bestimmte vRealize Automation-Business-Gruppe. Verfügbare virtuelle Reservierungstypen umfassen vSphere, Hyper-V, KVM, SCVMM und XenServer.

Bei einer Reservierung handelt es sich um einen Teil der Arbeitsspeicher-, CPU-, Netzwerk- und Speicherressourcen in einer Computing-Ressource, der einer bestimmten vRealize Automation-Business-Gruppe zugeteilt ist.

Eine Business-Gruppe kann mehrere Reservierungen auf einem Endpoint oder Reservierungen auf mehreren Endpoints aufweisen.

Zum Bereitstellen virtueller Maschinen muss eine Business-Gruppe über mindestens eine Reservierung auf einer virtuellen Computing-Ressource verfügen. Jede Reservierung ist ausschließlich für eine Business-Gruppe, aber eine Business-Gruppe kann über mehrere Reservierungen auf einer einzelnen Computing-Ressource oder mehrere Reservierungen auf Computing-Ressourcen unterschiedlichen Typs verfügen.

Neben der Definition der Fabric-Ressourcen, die der Business-Gruppe zugeteilt sind, kann eine Reservierung auch Richtlinien, Prioritäten und Kontingente definieren, welche die Maschinenplatzierung bestimmen.

#### **Grundlegendes zur Auswahllogik für Reservierungen**

Wenn das Mitglied einer Business-Gruppe eine Bereitstellungsanforderung für eine virtuelle Maschine erstellt, wählt vRealize Automation eine Maschine von einer der für diese Business-Gruppe verfügbaren Reservierungen aus.

Die für eine Maschine bereitgestellte Reservierung muss die folgenden Kriterien erfüllen:

- Die Reservierung muss denselben Plattfortmtyp wie der Blueprint aufweisen, von dem die Maschine angefordert wurde.  
Ein generischer virtueller Blueprint kann in jedem Typ virtueller Reservierungen bereitgestellt werden.
- Die Reservierung muss aktiviert sein.
- Der Zugriff auf die Computing-Ressource muss möglich sein, und sie darf sich nicht im Wartungsmodus befinden.
- Die Reservierung muss über eine verbleibende Kapazität in ihrem Maschinenkontingent oder über ein unbegrenztes Kontingent verfügen.

Das zugeteilte Maschinenkontingent umfasst nur Maschinen, die eingeschaltet sind. Wenn eine Reservierung beispielsweise über ein Kontingent von 50 verfügt und 40 Maschinen bereitgestellt wurden, von denen jedoch nur 20 eingeschaltet sind, beträgt das zugeteilte Kontingent der Reservierung 40 Prozent und nicht 80 Prozent.

- Die Reservierung muss über genügend nicht zugeteilte Arbeitsspeicher- und Speicherressourcen für die Bereitstellung der Maschine verfügen.

Wenn das Maschinenkontingent, der Arbeitsspeicher oder der Speicher einer virtuellen Reservierung vollständig zugeteilt ist, können von ihr keine weiteren virtuellen Maschinen bereitgestellt werden. Ressourcen sind möglicherweise über die physische Kapazität einer Virtualisierungs-Computing-Ressource hinaus reserviert (überbelegt). Wenn jedoch die physische Kapazität einer Computing-Ressource zu 100 % zugeteilt ist, können in Reservierungen mit dieser Computing-Ressource so lange keine weiteren Maschinen mehr bereitgestellt werden, bis die Ressourcen zurückgefordert wurden.

- Wenn der Blueprint bestimmte Netzwerkeinstellungen aufweist, muss die Reservierung dieselben Netzwerke aufweisen.

Wenn der Blueprint oder die Reservierung ein Netzwerkprofil für statische IP-Adressenzuweisung angibt, muss eine IP-Adresse verfügbar sein, die der neuen Maschine zugewiesen werden kann.

- Wenn der Blueprint oder die Anforderung einen Speicherort angibt, muss die Computing-Ressource diesem Speicherort zugeordnet sein.

Wenn die benutzerdefinierte Eigenschaft *VRM.Datacenter.Policy* den Wert **Exact** aufweist und keine Reservierung für eine diesem Speicherort zugeordnete Computing-Ressource vorhanden ist, die allen anderen Kriterien entspricht, schlägt die Bereitstellung fehl.

Wenn *VRM.Datacenter.Policy* den Wert **NotExact** aufweist und keine Reservierung für eine diesem Speicherort zugeordnete Computing-Ressource vorhanden ist, die allen anderen Kriterien entspricht, kann die Bereitstellung in einer anderen Reservierung unabhängig vom Speicherort fortgesetzt werden. Diese Option ist der Standard.

- Wenn der Blueprint oder die Anforderung die benutzerdefinierte Eigenschaft *VirtualMachine.Host.TpmEnabled* angibt, muss auf der Computing-Ressource für diese Reservierung vertrauenswürdige Hardware installiert werden.
- Wenn der Blueprint eine Reservierungsrichtlinie angibt, muss die Reservierung dieser Reservierungsrichtlinie angehören.

Reservierungsrichtlinien stellen eine Möglichkeit dar, wie garantiert werden kann, dass die ausgewählte Reservierung alle zusätzlichen Anforderungen für die Bereitstellung von Maschinen von einem bestimmten Blueprint erfüllt. Sie können Reservierungsrichtlinien beispielsweise dazu verwenden, die Bereitstellung auf Computing-Ressourcen mit einer bestimmten Vorlage zum Klonen zu beschränken.

Wenn keine Reservierung mit all diesen Auswahlkriterien verfügbar ist, schlägt die Bereitstellung fehl.

Wenn mehrere Reservierungen all diesen Kriterien entsprechen, wird die Reservierung, von der eine angeforderte Maschine bereitgestellt wird, durch die folgende Logik festgelegt:

- Eine Reservierung mit einem niedrigeren Prioritätswert wird vor einer Reservierung mit einem höheren Prioritätswert ausgewählt.



- Wenn mehrere Reservierungen dieselbe Priorität aufweisen, wird diejenige Reservierung ausgewählt, deren zugeteiltes Maschinenkontingent den geringsten Prozentsatz aufweist.
- Wenn mehrere Reservierungen dieselbe Priorität und dieselbe Kontingentauslastung aufweisen, werden Maschinen im Round-Robin-Verfahren (Rundlauf-Verfahren) auf Reservierungen verteilt.

---

**Hinweis** Die Round-Robin-Auswahl von Netzwerkprofilen wird nicht unterstützt, die Round-Robin-Auswahl von Netzwerken (soweit vorhanden) dagegen schon; diese können im Zusammenhang mit unterschiedlichen Netzwerkprofilen stehen.

---

Wenn in einer Reservierung mehrere Speicherpfade mit genügend Kapazität zur Bereitstellung der Maschinen-Volumes verfügbar sind, werden Speicherpfade nach der folgenden Logik ausgewählt:

- Wenn der Blueprint oder die Anforderung eine Speicherreservierungsrichtlinie angibt, muss der Speicherpfad dieser Speicherreservierungsrichtlinie angehören.

Wenn die benutzerdefinierte Eigenschaft *VirtualMachine.DiskN.StorageReservationPolicyMode* den Wert **NotExact** aufweist und in der Speicherreservierungsrichtlinie kein Speicherpfad mit genügend Kapazität vorhanden ist, kann die Bereitstellung mit einem Speicherpfad außerhalb der angegebenen Speicherreservierungsrichtlinie fortgesetzt werden. Der Standardwert von *VirtualMachine.DiskN.StorageReservationPolicyMode* lautet **Exact**.

- Ein Speicherpfad mit einem niedrigeren Prioritätswert wird vor einem Speicherpfad mit einem höheren Prioritätswert ausgewählt.
- Wenn mehrere Speicherpfade dieselbe Priorität aufweisen, werden Maschinen im Round-Robin-Verfahren (Rundlauf-Verfahren) auf Speicherpfade verteilt.

### Erstellen einer vSphere -Reservierung für die NSX -Netzwerk- und Sicherheitsvirtualisierung

Sie können eine vSphere-Reservierung erstellen, um externe Netzwerke und geroutete Gateways zu Netzwerkprofilen für Netzwerke zuzuweisen, die Transportzone anzugeben sowie Sicherheitsgruppen zu Maschinenkomponenten zuzuweisen.

Wenn Sie VMware NSX konfiguriert und das NSX-Plug-In für vRealize Automation installiert haben, können Sie beim Erstellen oder Bearbeiten eines Blueprints Einstellungen für NSX-Transportzonen, Reservierungsrichtlinien für die Edge und das geroutete Gateway sowie Anwendungsisolierungen angeben. Diese Einstellungen sind auf der Registerkarte **NSX-Einstellungen** auf den Seiten **Neuer Blueprint** und **Blueprint-Eigenschaften** verfügbar.

Die Netzwerk- und Sicherheitskomponenteneinstellungen, die Sie zur Blueprint-Design-Arbeitsfläche hinzufügen, werden von der NSX-Konfiguration abgeleitet. Das NSX-Plug-In muss dafür installiert sein und die Datenerfassung für den NSX-Bestand für vSphere-Cluster muss ausgeführt werden. Netzwerk- und Sicherheitskomponenten sind für NSX spezifisch und ausschließlich für die Verwendung mit vSphere-Maschinenkomponenten verfügbar. Informationen über das Konfigurieren von NSX finden Sie im *NSXAdministratorhandbuch*.

Wenn vRealize Automation Maschinen mit NAT- oder gerouteten Netzwerken bereitstellt, wird ein geroutetes Gateway als Netzwerkrouter bereitgestellt. Das Edge- oder geroutete Gateway ist eine Verwaltungsmaschine, die Computing-Ressourcen verbraucht. Darüber hinaus verwaltet es die Netzwerkkommunikation für die bereitgestellten Maschinenkomponenten. Die für die Bereitstellung des Edge- oder gerouteten

Gateways verwendete Reservierung bestimmt das externe Netzwerk, das für NAT- und geroutete Netzwerkprofile verwendet wird. Sie bestimmt außerdem das Edge- oder geroutete Reservierungsgateway, das zum Konfigurieren von gerouteten Netzwerken verwendet wird. Das geroutete Reservierungsgateway verknüpft geroutete Netzwerke mit Einträgen in der Routing-Tabelle.

Sie können eine Reservierungsrichtlinie für das Edge- oder geroutete Gateway angeben, um die Reservierungen festzulegen, die bei der Bereitstellung der Maschinen mithilfe des Edge- oder gerouteten Gateways verwendet werden sollen. Standardmäßig verwendet vRealize Automation für das geroutete Gateway und die Maschinenkomponenten dieselben Reservierungen.

Sie wählen eine oder mehrere Sicherheitsgruppen in der Reservierung aus, um die Basissicherheitsrichtlinie für alle Komponentenmaschinen zu erzwingen, die mit dieser Reservierung in vRealize Automation bereitgestellt werden. Jede bereitgestellte Maschine wird zu diesen angegebenen Sicherheitsgruppen hinzugefügt.

Für die erfolgreiche Bereitstellung muss die Transportzone der Reservierung mit der Transportzone eines Maschinen-Blueprints übereinstimmen, wenn dieser Blueprint Maschinennetzwerke definiert. Entsprechend erfordert die Bereitstellung des gerouteten Gateways einer Maschine, dass die in der Reservierung definierte Transportzone mit der für den Blueprint definierten Transportzone übereinstimmt.

Wenn Sie bei der Konfiguration von gerouteten Netzwerken ein Edge- oder ein geroutetes Gateway und ein Netzwerkprofil in einer Reservierung auswählen, wählen Sie den Netzwerkpfad aus, der zum Verknüpfen gerouteter Netzwerke verwendet werden soll, und weisen Sie ihm das externe Netzwerkprofil zu, das zur Konfiguration des gerouteten Netzwerkprofils verwendet wurde. Die Liste von Netzwerkprofilen, die einem Netzwerkpfad zugewiesen werden können, wird gefiltert, sodass das Subnetz des Netzwerkpfads, basierend auf der Subnetzmaske, mit der primären IP-Adresse übereinstimmt, die für die Netzwerkschnittstelle ausgewählt wurde.

Wenn Sie in vRealize Automation-Reservierungen ein Edge- oder ein geroutetes Gateway verwenden möchten, konfigurieren Sie das geroutete Gateway extern in der NSX-Umgebung und führen Sie anschließend die Erfassung von Bestandslistendaten aus. Für NSX müssen Sie über eine funktionierende NSX-Edge-Instanz verfügen, bevor Sie das Standardgateway für statische Routen oder dynamische Routingdetails für ein Edge-Services-Gateway oder einen verteilten Router konfigurieren können. Informationen dazu finden Sie im *NSX-Administratorhandbuch*.

### **Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer**

Sie müssen Maschinen durch Erstellen einer Reservierung Ressourcen zuteilen, bevor Mitglieder einer Business-Gruppe die Maschinenbereitstellung anfordern können.

Jede Business-Gruppe benötigt mindestens eine Reservierung, damit ihre Mitglieder Maschinen dieses Typs bereitstellen können. Beispielsweise kann eine Business-Gruppe mit einer vSphere-Reservierung, aber ohne KVM (RHEV)-Reservierung, keine KVM (RHEV)-VM anfordern. In diesem Beispiel muss der Business-Gruppe eine Reservierung speziell für KVM (RHEV)-Ressourcen zugeteilt werden.

## Vorgehensweise

### 1 Angeben von Informationen zu virtuellen Reservierungen

Jede Reservierung wird für eine bestimmte Business-Gruppe konfiguriert, um den Benutzern die Berechtigung für das Anfordern von Maschinen auf einer angegebenen Computing-Ressource zu erteilen.

### 2 Angeben von Ressourcen- und Netzwerkeinstellungen für eine virtuelle Reservierung

Geben Sie Ressourcen- und Netzwerkeinstellungen für die Bereitstellung von Maschinen über die vRealize Automation-Reservierung ein.

### 3 Angeben benutzerdefinierter Eigenschaften und Warnungen für virtuelle Reservierungen

Sie können einer vRealize Automation-Reservierung benutzerdefinierte Eigenschaften zuordnen. Darüber hinaus können Sie Warnungen konfigurieren, um bei niedrigen Reservierungsressourcen E-Mail-Benachrichtigungen zu senden.

## Angeben von Informationen zu virtuellen Reservierungen

Jede Reservierung wird für eine bestimmte Business-Gruppe konfiguriert, um den Benutzern die Berechtigung für das Anfordern von Maschinen auf einer angegebenen Computing-Ressource zu erteilen.

Sie können die Anzeige von Reservierungen beim Hinzufügen, Bearbeiten oder Löschen steuern, indem Sie auf der Seite „Reservierungen“ die Option **Nach Kategorie filtern** verwenden. Beachten Sie, dass Test-Agent-Reservierungen beim Filtern nach Kategorie nicht in der Reservierungsliste angezeigt werden.

---

**Hinweis** Nach dem Erstellen einer Reservierung können Sie die Zuordnungen der Business-Gruppen oder Computing-Ressourcen nicht mehr ändern.

---

## Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.
- Stellen Sie sicher, dass der Mandantenadministrator mindestens eine Business-Gruppe erstellt hat.
- Stellen Sie sicher, dass eine Computing-Ressource vorhanden ist.
- Konfigurieren Sie die Netzwerkeinstellungen.
- (Optional) Konfigurieren Sie die Informationen zum Netzwerkprofil.

## Vorgehensweise

1 Wählen Sie **Infrastruktur > Reservierungen > Reservierungen** aus.

2 Klicken Sie auf das Symbol **Neu (+)** und wählen Sie den zu erstellenden Reservierungstyp aus.

Die verfügbaren Typen von virtuellen Reservierungen sind Hyper-V, KVM, SCVMM, vSphere und XenServer.

Wählen Sie beispielsweise **vSphere** aus.

- 3 (Optional) Wählen Sie aus dem Dropdown-Menü **Aus vorhandener Reservierung kopieren** eine vorhandene Reservierung aus.

Die Daten zu der ausgewählten Reservierung wird angezeigt. Sie können für Ihre neue Reservierung bei Bedarf Änderungen vornehmen.

- 4 Geben Sie im Textfeld **Name** einen Namen ein.

- 5 Wählen Sie aus dem Dropdown-Menü **Mandant** einen Mandanten aus.

- 6 Wählen Sie aus dem Dropdown-Menü **Business-Gruppe** eine Business-Gruppe aus.

Nur Benutzer in dieser Business-Gruppe können Maschinen mit dieser Reservierung bereitstellen.

- 7 (Optional) Wählen Sie aus dem Dropdown-Menü **Reservierungsrichtlinie** eine Reservierungsrichtlinie aus.

Diese Option setzt voraus, dass mindestens eine Reservierungsrichtlinie vorhanden ist. Sie können die Reservierung später bearbeiten, um eine Reservierungsrichtlinie anzugeben.

Sie verwenden eine Reservierungsrichtlinie zur Einschränkung der Bereitstellung auf bestimmte Reservierungen.

- 8 Geben Sie im Textfeld **Priorität** eine Zahl ein, um die Priorität für die Reservierung festzulegen.

Die Priorität wird verwendet, wenn eine Business-Gruppe über mehr als eine Reservierung verfügt. Einer Reservierung der Priorität 1 wird bei einer Bereitstellung der Vorzug gegenüber einer Reservierung der Priorität 2 gegeben.

- 9 (Optional) Deaktivieren Sie das Kontrollkästchen **Diese Reservierung aktivieren**, wenn Sie nicht möchten, dass diese Reservierung aktiv ist.

Verlassen Sie diese Seite nicht. Ihre Reservierung ist noch nicht abgeschlossen.

### Angeben von Ressourcen- und Netzwerkeinstellungen für eine virtuelle Reservierung

Geben Sie Ressourcen- und Netzwerkeinstellungen für die Bereitstellung von Maschinen über die vRealize Automation-Reservierung ein.

Sie können in Ihrer Reservierung einen FlexClone-Datenspeicher auswählen, wenn Sie über eine vSphere-Umgebung und Speichergeräte mit Net App FlexClone-Technologie verfügen. SDRS wird für FlexClone-Speichergeräte nicht unterstützt.

### Voraussetzungen

[Angeben von Informationen zu virtuellen Reservierungen.](#)

### Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Ressourcen**.

- 2 Wählen Sie aus dem Dropdown-Menü **Computing-Ressource** eine Computing-Ressource aus, auf der Maschinen bereitgestellt werden sollen.

Nur Vorlagen, die sich auf dem ausgewählten Cluster befinden, sind für das Klonen mit dieser Reservierung verfügbar.

Während der Bereitstellung werden die Maschinen auf einem Host platziert, der mit dem lokalen Speicher verbunden ist. Wenn die Reservierung lokalen Speicher verwendet, werden alle Maschinen, die mithilfe der Reservierung bereitgestellt werden, auf dem Host erstellt, der diesen lokalen Speicher enthält. Wenn Sie allerdings die benutzerdefinierte Eigenschaft `VirtualMachine.Admin.ForceHost` verwenden, mit der die Bereitstellung einer Maschine auf einem anderen Host erzwungen wird, schlägt die Bereitstellung fehl. Die Bereitstellung schlägt auch fehl, wenn sich die Vorlage, über die die Maschine geklont wird, auf lokalem Speicher befindet, aber einer Maschine in einem anderen Cluster hinzugefügt ist. In diesem Fall schlägt die Bereitstellung fehl, da kein Zugriff auf die Vorlage möglich ist.

- 3 (Optional) Geben Sie im Textfeld **Maschinenkontingent** eine Zahl ein, um die maximale Anzahl von Maschinen festzulegen, die in dieser Reservierung bereitgestellt werden können.

Nur eingeschaltete Maschinen werden beim Kontingent berücksichtigt. Lassen Sie das Feld leer, wenn die Reservierung unbegrenzt sein soll.

- 4 Geben Sie die Menge des Arbeitsspeichers in GB an, die dieser Reservierung aus der Speichertabelle zugewiesen werden soll.

Der gesamte Arbeitsspeicherwert für die Reservierung wird Ihrer Auswahl der Computing-Ressource entnommen.

- 5 Wählen Sie mindestens einen aufgelisteten Speicherpfad aus.

Die verfügbaren Speicherpfad-Optionen werden Ihrer Auswahl der Computing-Ressource entnommen.

Für Integrationen mit Storage Distributed Resource Scheduler-Speicher (SDRS-Speicher) können Sie einen Speicher-Cluster auswählen, sodass SDRS automatisch Speicherplatzierung und Lastausgleich für von dieser Reservierung bereitgestellte Maschinen verarbeiten kann. Der SDRS-Automatisierungsmodus muss auf „Automatisch“ festgelegt werden. Andernfalls wählen Sie innerhalb des Clusters einen Datenspeicher für das Verhalten von eigenständigen Datenspeichern aus. SDRS wird für FlexClone-Speichergeräte nicht unterstützt.

- 6 Wählen Sie soweit dies für die Computing-Ressource verfügbar ist im Dropdown-Menü **Ressourcenpool** einen Ressourcenpool aus.

- 7 Klicken Sie auf die Registerkarte **Netzwerk**.

## 8 Konfigurieren Sie mit dieser Reservierung einen Netzwerkpfad für bereitgestellte Maschinen.

- a (Optional) Wenn die Option verfügbar ist, wählen Sie einen Speicher-Endpoint aus dem Dropdown-Menü **Endpoint** aus.

Die FlexClone-Option wird in der Endpoint-Spalte angezeigt, wenn ein NetApp ONTAP-Endpoint vorhanden ist und wenn der Host virtuell ist. Wenn ein NetApp ONTAP-Endpoint vorhanden ist, wird auf der Reservierungsseite der dem Speicherpfad zugewiesene Endpoint angezeigt. Wenn Sie einen Endpoint für einen Speicherpfad hinzufügen, aktualisieren oder löschen, wird die Änderung in allen zutreffenden Reservierungen angezeigt.

Wenn Sie einen Endpoint für einen Speicherpfad hinzufügen, aktualisieren oder löschen, wird die Änderung auf der Reservierungsseite angezeigt.

- b Wählen Sie aus der Liste **Netzwerkpfade** die Netzwerkpfade für durch diese Reservierung bereitgestellte Maschinen aus.
- c (Optional) Wählen Sie aus dem Dropdown-Menü **Netzwerkprofil** ein aufgelistetes Netzwerkprofil aus.

Diese Option setzt voraus, dass mindestens ein Netzwerkprofil vorhanden ist.

Sie können in einer Reservierung mehr als einen Netzwerkpfad auswählen, aber bei der Bereitstellung einer Maschine wird nur ein Netzwerk verwendet.

Sie können die Reservierung nun durch Klicken auf **Speichern** speichern. Sie können noch benutzerdefinierte Eigenschaften hinzufügen, um Reservierungsspezifikationen besser zu steuern. Zudem können Sie E-Mail-Warnungen konfigurieren, damit Sie Benachrichtigungen erhalten, wenn die dieser Reservierung zugeteilten Ressourcen einen niedrigen Stand erreichen.

### Angeben benutzerdefinierter Eigenschaften und Warnungen für virtuelle Reservierungen

Sie können einer vRealize Automation-Reservierung benutzerdefinierte Eigenschaften zuordnen. Darüber hinaus können Sie Warnungen konfigurieren, um bei niedrigen Reservierungsressourcen E-Mail-Benachrichtigungen zu senden.

Benutzerdefinierte Eigenschaften und E-Mail-Warnungen sind optionale Konfigurationen für die Reservierung. Wenn Sie weder benutzerdefinierte Eigenschaften verknüpfen noch Warnungen festlegen möchten, klicken Sie auf **Speichern**, um die Erstellung der Reservierung zu beenden.

Sie können beliebig viele benutzerdefinierte Eigenschaften hinzufügen.

---

**Wichtig** Benachrichtigungen werden nur dann gesendet, wenn E-Mail-Warnungen konfiguriert und Benachrichtigungen aktiviert wurden.

---

Falls konfiguriert, werden Warnungen täglich generiert und nicht erst bei Erreichen des angegebenen Schwellenwerts.

### Voraussetzungen

[Angaben von Ressourcen- und Netzwerkeinstellungen für eine virtuelle Reservierung.](#)

## Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Eigenschaften**.
- 2 Klicken Sie auf **Neu**.
- 3 Geben Sie einen gültigen Namen für die benutzerdefinierte Eigenschaft ein.
- 4 Geben Sie gegebenenfalls einen Eigenschaftswert ein.
- 5 (Optional) Aktivieren Sie das Kontrollkästchen **Verschlüsselt**, um den Eigenschaftswert zu verschlüsseln.
- 6 (Optional) Aktivieren Sie das Kontrollkästchen **Eingabeaufforderung**, damit Benutzer einen Wert eingeben müssen.  
Diese Option kann bei der Bereitstellung nicht außer Kraft gesetzt werden.
- 7 (Optional) Fügen Sie zusätzliche benutzerdefinierte Eigenschaften hinzu.
- 8 Klicken Sie auf die Registerkarte **Warnungen**.
- 9 Aktivieren Sie das Kontrollkästchen **Kapazitätswarnungen**, um das Senden von Warnungen zu konfigurieren.
- 10 Verwenden Sie den Schieberegler, um für verfügbare Ressourcenzuteilungen Schwellenwerte festzulegen.
- 11 Geben Sie im Textfeld **Empfänger** mindestens eine E-Mail-Adresse eines Benutzers oder einen Gruppennamen ein, um festzulegen, wer Warnbenachrichtigungen erhalten soll.  
Drücken Sie die Eingabetaste, um mehrere Einträge zu trennen.
- 12 Wählen Sie **Warnungen an Gruppenmanager senden** aus, um Gruppenmanager in den Erhalt der E-Mail-Warnungen einzubeziehen.
- 13 Legen Sie eine Erinnerungshäufigkeit (in Tagen) fest.
- 14 Klicken Sie auf **Speichern**.

Die Reservierung wird gespeichert und in der Liste „Reservierungen“ angezeigt.

## Weiter

Sie können optionale Reservierungsrichtlinien konfigurieren oder mit der Vorbereitung auf die Bereitstellung beginnen.

Zur Erstellung von Blueprints autorisierte Benutzer können diese nun erstellen.

## Bearbeiten einer Reservierung zum Zuweisen eines Netzwerkprofils

Sie können ein Netzwerkprofil zu einer Reservierung zuweisen, um beispielsweise die Zuweisung von statischen IP-Adressen für Maschinen zu aktivieren, die im Rahmen dieser Reservierung bereitgestellt werden.

Sie können ein Netzwerkprofil auch einem Blueprint zuweisen, indem Sie die benutzerdefinierte Eigenschaft `VirtualMachine.NetworkN.ProfileName` auf der Registerkarte **Eigenschaften** auf der Seite **Neuer Blueprint** bzw. **Blueprint-Eigenschaften** verwenden.

Wenn Sie ein Netzwerkprofil in einer Reservierung und einem Blueprint angeben, hat der Blueprint-Wert Vorrang. Wenn Sie beispielsweise ein Netzwerkprofil im Blueprint mithilfe der benutzerdefinierten Eigenschaft `VirtualMachine.NetworkN.ProfileName` und in einer vom Blueprint verwendeten Reservierung angeben, hat das im Blueprint angegebene Netzwerkprofil Vorrang. Wenn die benutzerdefinierte Eigenschaft jedoch nicht im Blueprint verwendet wird und Sie ein Netzwerkprofil für eine Maschinen-NIC auswählen, verwendet vRealize Automation den Netzwerkreservierungspfad für die Maschinen-NIC, für die das Netzwerkprofil angegeben ist.

---

**Hinweis** Diese Informationen gelten für Amazon Web Services nicht.

---

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.
- Erstellen Sie ein Netzwerkprofil. Siehe [Erstellen eines Netzwerkprofils](#).

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Reservierungen** aus.
- 2 Zeigen Sie auf eine Reservierung und klicken Sie auf **Bearbeiten**.
- 3 Klicken Sie auf die Registerkarte **Netzwerk**.
- 4 Weisen Sie ein Netzwerkprofil einem Netzwerkpfad zu.
  - a Wählen Sie einen Netzwerkpfad aus, für den die statischen IP-Adressen aktiviert werden sollen.  
Die Optionen für die Netzwerkpfade werden den Einstellungen auf der Registerkarte **Ressourcen** entnommen.
  - b Ordnen Sie dem Pfad ein verfügbares Netzwerkprofil zu, indem Sie aus dem Dropdown-Menü **Netzwerkprofil** ein Profil auswählen.
  - c (Optional) Wiederholen Sie diesen Schritt, um Netzwerkprofile zusätzlichen Netzwerkpfaden in dieser Reservierung zuzuweisen.
- 5 Klicken Sie auf **OK**.

## Reservierungsrichtlinien

Sie können eine Reservierungsrichtlinie verwenden, um die Verarbeitung von Reservierungsanforderungen zu steuern. Wenn Sie Maschinen über den Blueprint bereitstellen, ist die Bereitstellung auf die in Ihrer Reservierungsrichtlinie angegebenen Ressourcen eingeschränkt.

Reservierungsrichtlinien stellen ein optionales Mittel dar, um die Verarbeitung von Reservierungsanforderungen zu steuern. Sie können eine Reservierungsrichtlinie zu einem Blueprint hinzufügen, um die Maschinen einzuschränken, die von diesem Blueprint für eine Teilmenge der verfügbaren Reservierungen bereitgestellt werden.



Sie können eine Reservierungsrichtlinie zur Gruppierung ähnlicher Ressourcen verwenden, um verschiedene Service-Ebenen zu definieren oder einen konkreten Ressourcentyp für einen bestimmten Zweck zur Verfügung zu stellen. Wenn ein Benutzer eine Maschine anfordert, kann sie in einer Reservierung des entsprechenden Typs bereitgestellt werden, der über ausreichende Kapazität für die Maschine verfügt. Folgende Szenarien veranschaulichen die Verwendungsmöglichkeiten von Reservierungsrichtlinien:

- Sicherstellung, dass bereitgestellte Maschinen in Reservierungen mit bestimmten Geräten platziert werden, die NetApp FlexClone unterstützen.
- Einschränkung der Bereitstellung von Cloud-Maschinen auf eine spezifische Region, die ein Maschinen-Image aufweist, das für einen bestimmten Blueprint erforderlich ist.
- Als zusätzliches Mittel zur Verwendung eines Vorausbezahlungs-Zuteilungsmodells für Maschinentypen, die diese Funktionalität unterstützen.

Sie können einer Reservierungsrichtlinie mehrere Reservierungen hinzufügen, aber eine Reservierung kann nur einer Richtlinie angehören. Sie können eine einzelne Reservierungsrichtlinie mehreren Blueprints hinzufügen. Ein Blueprint kann nur eine Reservierungsrichtlinie aufweisen.

---

**Hinweis** Für vCloud Air-Endpoints und vCloud Director-Endpoints definierte Reservierungen wird die Verwendung von Netzwerkprofilen für die Bereitstellung von Maschinen nicht unterstützt.

---

**Hinweis** Wenn auf Ihrer Plattform SDRS aktiviert ist, kann SDRS den Speicher-Lastausgleich für einzelne Festplatten der virtuellen Maschine oder für den gesamten Speicher der virtuellen Maschine vornehmen. Falls Sie mit SDRS Datastore Clusters arbeiten, können bei Verwendung von Reservierungsrichtlinien und Speicherreservierungsrichtlinien Konflikte auftreten. Wenn zum Beispiel ein eigenständiger Datenspeicher oder ein Datenspeicher in einem SDRS-Cluster in einer der Reservierungen einer Richtlinie oder Speicherrichtlinie ausgewählt wird, kann der Speicher ihrer virtuellen Maschine stillgelegt werden, anstatt von SDRS gesteuert zu werden. Wenn Sie die erneute Bereitstellung für eine Maschine mit Speicherplatzierung in einem SDRS-Cluster anfordern, wird die Maschine gelöscht, wenn die SDRS-Automatisierungsstufe deaktiviert wird.

---

## Konfigurieren einer Reservierungsrichtlinie

Sie können Reservierungsrichtlinien zur Gruppierung ähnlicher Ressourcen erstellen, um verschiedene Service-Level zu definieren oder einen konkreten Ressourcentyp für einen bestimmten Zweck zur Verfügung zu stellen. Nachdem Sie die Reservierungsrichtlinie erstellt haben, müssen Sie sie mit Reservierungen auffüllen, bevor Mandantenadministratoren und Business-Gruppenmanager die Richtlinie tatsächlich in einem Blueprint verwenden können.

Eine Reservierungsrichtlinie kann verschiedene Reservierungstypen enthalten, aber bei der Auswahl einer Reservierung für eine bestimmte Anforderung werden nur die Reservierungen berücksichtigt, die mit dem Blueprint-Typ übereinstimmen.

## Vorgehensweise

### 1 Erstellen einer Reservierungsrichtlinie

Mithilfe von Reservierungsrichtlinien können Sie ähnliche Reservierungen gruppieren.

## 2 Zuweisen einer Reservierungsrichtlinie zu einer Reservierung

Sie können einer Reservierung eine Reservierungsrichtlinie zuweisen, wenn Sie die Reservierung erstellen. Darüber hinaus können Sie eine vorhandene Reservierung bearbeiten, um ihr eine Reservierungsrichtlinie zuzuweisen, oder die Zuweisung der Reservierungsrichtlinie ändern.

### Erstellen einer Reservierungsrichtlinie

Mithilfe von Reservierungsrichtlinien können Sie ähnliche Reservierungen gruppieren.

Erstellen Sie zunächst die Reservierungsrichtlinie und fügen Sie anschließend die Richtlinie zu Reservierungen hinzu, damit ein Blueprint-Ersteller die Reservierungsrichtlinie in einem Blueprint verwenden kann.

Die Richtlinie wird als leerer Container erstellt.

Sie können die Anzeige von Reservierungsrichtlinien beim Hinzufügen, Bearbeiten oder Löschen steuern, indem Sie auf der Seite „Reservierungsrichtlinien“ die Option **Nach Typ filtern** verwenden.

### Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Reservierungsrichtlinien** aus.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Geben Sie im Textfeld **Name** einen Namen ein.
- 4 Wählen Sie aus dem Dropdown-Menü **Typ** die Option **Reservierungsrichtlinie** aus.
- 5 Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.
- 6 Klicken Sie auf **Aktualisieren**, um die Richtlinie zu speichern.

### Zuweisen einer Reservierungsrichtlinie zu einer Reservierung

Sie können einer Reservierung eine Reservierungsrichtlinie zuweisen, wenn Sie die Reservierung erstellen. Darüber hinaus können Sie eine vorhandene Reservierung bearbeiten, um ihr eine Reservierungsrichtlinie zuzuweisen, oder die Zuweisung der Reservierungsrichtlinie ändern.

### Voraussetzungen

[Erstellen einer Reservierungsrichtlinie](#).

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Reservierungen > Reservierungen** aus.
- 2 Zeigen Sie auf eine Reservierung und klicken Sie auf **Bearbeiten**.
- 3 Wählen Sie aus dem Dropdown-Menü **Reservierungsrichtlinie** eine Reservierungsrichtlinie aus.
- 4 Klicken Sie auf **Speichern**.

## Speicherreservierungsrichtlinien

Sie können Speicherreservierungsrichtlinien erstellen, damit Blueprint-Architekten die Volumes einer virtuellen Maschine verschiedenen Datenspeichern für die vSphere-, KVM (RHEV)- und SCVMM-Plattformtypen oder verschiedenen Speicherprofilen für andere Ressourcen wie beispielsweise vCloud Air- oder vCloud Director-Ressourcen zuweisen können.

Durch das Zuweisen der Volumes einer virtuellen Maschine zu verschiedenen Datenspeichern oder zu einem anderen Speicherprofil können Blueprint-Architekten Speicherplatz effektiver steuern und verwenden. Beispielsweise können sie das Betriebssystemvolume für einen langsameren, kostengünstigen Datenspeicher oder ein Speicherprofil bereitstellen, und das Datenbankvolume für einen schnelleren Datenspeicher oder ein Speicherprofil.

Manche Maschinen-Endpoints unterstützen nur ein einziges Speicherprofil, andere wiederum unterstützen eine mehrstufige Speicherung. Die mehrstufige Datenspeicherung ist für vCloud Director-5.6-Endpoints und höhere Endpoints sowie für vCloud Air-Endpoints verfügbar. Die mehrstufige Datenspeicherung wird für vCloud Director-5.5-Endpoints nicht unterstützt.

Wenn Sie einen Blueprint erstellen, können Sie einen einzelnen Datenspeicher oder eine Speicherreservierungsrichtlinie zuweisen, die mehrere Datenspeicher für ein Volume darstellt. Wenn sie einen einzelnen Datenspeicher oder ein Speicherprofil einem Volume zuweisen, verwendet vRealize Automation diesen Datenspeicher oder dieses Speicherprofil, wenn möglich, zur Bereitstellungszeit. Wenn sie eine Speicherreservierungsrichtlinie einem Volume zuweisen, verwendet vRealize Automation eine seiner Datenspeicher oder Speicherprofile, wenn sie mit anderen Ressourcen funktionieren, wie z. B. vCloud Air oder vCloud Director, zur Bereitstellungszeit.

Eine Speicherreservierungsrichtlinie ist im Prinzip ein Tag, das von einem Fabric-Administrator auf mindestens einen Datenspeicher oder auf mindestens ein Speicherprofil angewendet wird, um Datenspeicher oder Speicherprofile zu gruppieren, die ähnliche Eigenschaften wie z. B. Geschwindigkeit oder Preis aufweisen. Ein Datenspeicher oder ein Speicherprofil kann jeweils nur einer Speicherreservierungsrichtlinie zugewiesen werden, aber eine Speicherreservierungsrichtlinie kann über viele verschiedene Datenspeicher oder Speicherprofile verfügen.

Sie können eine Speicherreservierungsrichtlinie erstellen und sie mindestens einem Datenspeicher oder Speicherprofil zuweisen. Ein Blueprint-Ersteller kann dann die Speicherreservierungsrichtlinie einem Volume in einem virtuellen Blueprint zuweisen. Wenn ein Benutzer eine Maschine anfordert, die den Blueprint verwendet, verwendet vRealize Automation die im Blueprint angegebene Speicherreservierungsrichtlinie zum Auswählen eines Datenspeichers oder Speicherprofils für das Volume der Maschine.

**Hinweis** Wenn auf Ihrer Plattform SDRS aktiviert ist, kann SDRS den Speicher-Lastausgleich für einzelne Festplatten der virtuellen Maschine oder für den gesamten Speicher der virtuellen Maschine vornehmen. Falls Sie mit SDRS Datastore Clusters arbeiten, können bei Verwendung von Reservierungsrichtlinien und Speicherreservierungsrichtlinien Konflikte auftreten. Wenn zum Beispiel ein eigenständiger Datenspeicher oder ein Datenspeicher in einem SDRS-Cluster in einer der Reservierungen einer Richtlinie oder Speicherrichtlinie ausgewählt wird, kann der Speicher ihrer virtuellen Maschine stillgelegt werden, anstatt von SDRS gesteuert zu werden. Wenn Sie die erneute Bereitstellung für eine Maschine mit Speicherplatzierung in einem SDRS-Cluster anfordern, wird die Maschine gelöscht, wenn die SDRS-Automatisierungsstufe deaktiviert wird.

## Konfigurieren einer Speicherreservierungsrichtlinie

Sie können Speicherreservierungsrichtlinien erstellen, um Datenspeicher zu gruppieren, die ähnliche Merkmale aufweisen, wie beispielsweise Geschwindigkeit oder Preis. Nachdem Sie die Speicherreservierungsrichtlinie erstellt haben, müssen Sie sie mit Datenspeichern auffüllen, bevor die Richtlinie in einem Blueprint verwendet werden kann.

### Vorgehensweise

#### 1 Erstellen einer Speicherreservierungsrichtlinie

Mithilfe einer Speicherreservierungsrichtlinie können Sie Datenspeicher gruppieren, die ähnliche Merkmale aufweisen, wie beispielsweise Geschwindigkeit oder Preis.

#### 2 Zuweisen einer Speicherreservierungsrichtlinie zu einem Datenspeicher

Sie können einer Computing-Ressource eine Speicherreservierungsrichtlinie zuordnen. Nachdem die Speicherreservierungsrichtlinie erstellt wurde, füllen Sie sie mit Datenspeichern auf. Ein Datenspeicher kann nur zu einer einzigen Speicherreservierungsrichtlinie gehören. Fügen Sie mehrere Datenspeicher hinzu, um eine Gruppe von Datenspeichern für die Verwendung mit einem Blueprint zu erstellen.

## Erstellen einer Speicherreservierungsrichtlinie

Mithilfe einer Speicherreservierungsrichtlinie können Sie Datenspeicher gruppieren, die ähnliche Merkmale aufweisen, wie beispielsweise Geschwindigkeit oder Preis.

Die Richtlinie wird als leerer Container erstellt.

Sie können die Anzeige von Reservierungsrichtlinien beim Hinzufügen, Bearbeiten oder Löschen steuern, indem Sie auf der Seite „Reservierungsrichtlinien“ die Option **Nach Typ filtern** verwenden.

### Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.

**Vorgehensweise**

- 1 Wählen Sie **Infrastruktur > Reservierungen > Reservierungsrichtlinien** aus.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Geben Sie im Textfeld **Name** einen Namen ein.
- 4 Wählen Sie aus dem Dropdown-Menü **Typ** die Option **Speicherreservierungsrichtlinie** aus.
- 5 Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.
- 6 Klicken Sie auf **Aktualisieren**, um die Richtlinie zu speichern.



**Zuweisen einer Speicherreservierungsrichtlinie zu einem Datenspeicher**

Sie können einer Computing-Ressource eine Speicherreservierungsrichtlinie zuordnen. Nachdem die Speicherreservierungsrichtlinie erstellt wurde, füllen Sie sie mit Datenspeichern auf. Ein Datenspeicher kann nur zu einer einzigen Speicherreservierungsrichtlinie gehören. Fügen Sie mehrere Datenspeicher hinzu, um eine Gruppe von Datenspeichern für die Verwendung mit einem Blueprint zu erstellen.

**Voraussetzungen**

[Erstellen einer Speicherreservierungsrichtlinie](#).

**Vorgehensweise**

- 1 Wählen Sie **Infrastruktur > Computing-Ressourcen > Computing-Ressourcen** aus.
- 2 Zeigen Sie auf eine Computing-Ressource und klicken Sie auf **Bearbeiten**.
- 3 Klicken Sie auf die Registerkarte **Konfiguration**.
- 4 Suchen Sie in der Speichertabelle nach dem Datenspeicher, der Ihrer Speicherreservierungsrichtlinie hinzugefügt werden soll.
- 5 Klicken Sie auf das Symbol **Bearbeiten** () neben dem gewünschten **Speicherpfad**-Objekt.
- 6 Wählen Sie aus dem Dropdown-Menü **Speicherreservierungsrichtlinie** eine Speicherreservierungsrichtlinie aus.  
  
Nach Bereitstellung einer Maschine können Sie deren Speicherreservierungsrichtlinie nicht ändern, wenn dies zu einer Änderung des Speicherprofils auf einer Festplatte führen würde.
- 7 Klicken Sie auf das Symbol **Speichern** ()
- 8 Klicken Sie auf **OK**.
- 9 (Optional) Weisen Sie Ihrer Speicherreservierungsrichtlinie zusätzliche Datenspeicher zu.

**Szenario: Konfigurieren von IaaS-Ressourcen für Rainpole**

Unter Verwendung einer Kombination aus Ihren IaaS-Administratorrechten und Mandantenadministratorrechten, erstellen Sie ein Präfix zum Voranstellen an Ihre vSphere-Maschinen, die in vRealize Automation erstellt wurden, organisieren Ihre vSphere-Ressourcen in einer Fabric-Gruppe und weisen Ressourcen zur benutzerdefinierten Gruppe der vRealize Automation-Architekten zu.



## Vorgehensweise

### 1 Szenario: Erstellen einer Fabric-Komponente für Rainpole

Mit Ihren Rechten als IaaS-Administrator erstellen Sie eine Fabric-Gruppe, die die Computing-Ressourcen enthält, die beim Erstellen des vSphere-Endpoints erkannt wurden. Weisen Sie Ihre benutzerdefinierte Gruppe von vRealize Automation-Architekten und Entwicklern zur Fabric-Administratorrolle für diese Gruppe zu.

### 2 Szenario: Konfigurieren von Maschinenpräfixen für Rainpole

Mit Ihren Fabric-Administratorrechten erstellen Sie einen Präfix, den Sie so konfigurieren können, dass er den von Ihren vRealize Automation-Architekten und Entwicklern während der Entwicklung und dem Testen bereitgestellten Maschinen vorangestellt wird.

### 3 Szenario: Einrichten einer Business-Gruppe für Ihre Rainpole-Architekten zum Testen von Katalogelementen

Mit Ihren Mandantenadministratorrechten erstellen Sie eine Business-Gruppe für das IT-Team, das für das Entwerfen und Testen Ihrer vRealize Automation-Blueprints verantwortlich ist.

### 4 Szenario: Erstellen einer Reservierung zum Zuweisen von Ressourcen zu Ihren Rainpole-Architekten

Mit Ihren Fabric-Administratorrechten erstellen Sie eine Reservierung für Ihre Rainpole-Business-Gruppe, um dieser vSphere-Ressourcen zuzuweisen.

## Szenario: Erstellen einer Fabric-Komponente für Rainpole

Mit Ihren Rechten als IaaS-Administrator erstellen Sie eine Fabric-Gruppe, die die Computing-Ressourcen enthält, die beim Erstellen des vSphere-Endpoints erkannt wurden. Weisen Sie Ihre benutzerdefinierte Gruppe von vRealize Automation-Architekten und Entwicklern zur Fabric-Administratorrolle für diese Gruppe zu.

Sie müssen keinen vSphere-Endpoint erstellen, weil dieser schon beim Anfordern des Katalogelements für anfänglichen Inhalt erstellt wurde.

## Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Fabric-Gruppen** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Geben Sie **Rainpole-Fabric** in das Textfeld „Name“ ein.
- 4 Geben Sie **Rainpole-Administratoren** im Suchfeld **Fabric-Architekten** ein und wählen Sie Ihre benutzerdefinierte Gruppe aus.

- 5 Wählen Sie die Computing-Ressource aus Ihrer vSphere-Umgebung aus, um sie in Ihre Fabric-Gruppe einzubinden.
- 6 Klicken Sie auf **OK**.
- 7 Aktualisieren Sie Ihren Browser, um die neuen Menüoptionen anzuzeigen, die Ihnen als Fabric-Administrator zur Verfügung stehen.

#### Weiter

Mit Ihren Fabric-Administratorrechten erstellen Sie einen Maschinen-Präfix für Ihre Rainpole-Architekten, damit alle Maschinen, die sie während der Entwicklungs- und Testphase bereitstellen, leicht erkannt werden.

### Szenario: Konfigurieren von Maschinenpräfixen für Rainpole

Mit Ihren Fabric-Administratorrechten erstellen Sie einen Präfix, den Sie so konfigurieren können, dass er den von Ihren vRealize Automation-Architekten und Entwicklern während der Entwicklung und dem Testen bereitgestellten Maschinen vorangestellt wird.

#### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Administration > Maschinenpräfixe** aus.
- 2 Klicken Sie auf **Neu**.
- 3 Geben Sie **Rainpole** in das Textfeld **Maschinenpräfix** ein.
- 4 Geben Sie **3** in das Textfeld **Anzahl der Ziffern** ein.
- 5 Geben Sie **1** in das Textfeld **Nächste Nummer** ein.
- 6 Klicken Sie auf das Symbol **Speichern** (✓).

#### Weiter

Mit Ihren Mandantenadministratorrechten erstellen Sie eine Business-Gruppe für das IT-Team, das für das Entwerfen und Testen Ihrer vRealize Automation-Blueprints verantwortlich ist.

### Szenario: Einrichten einer Business-Gruppe für Ihre Rainpole-Architekten zum Testen von Katalogelementen

Mit Ihren Mandantenadministratorrechten erstellen Sie eine Business-Gruppe für das IT-Team, das für das Entwerfen und Testen Ihrer vRealize Automation-Blueprints verantwortlich ist.

#### Vorgehensweise

- 1 Wählen Sie **Administration > Benutzer und Gruppen > Business-Gruppen** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Geben Sie **Rainpole-Business-Gruppe** in das Textfeld **Name** ein.

- 4 Geben Sie mindestens eine E-Mail-Adresse in das Textfeld **Manager-E-Mails senden an** ein.

Geben Sie beispielsweise Ihre eigene E-Mail-Adresse oder die E-Mail-Adresse Ihres IT-Managers ein.

- 5 Fügen Sie eine benutzerdefinierte Eigenschaft hinzu, die Ihren Architekten bei der Fehlerbehebung im Zusammenhang mit ihren Blueprints helfen kann.
- a Klicken Sie auf das Symbol **Neu (+)**.
  - b Geben Sie **\_debug\_deployment** in das Textfeld **Name** ein.
  - c Geben Sie **true** in das Textfeld **Wert** ein.
  - d Wählen Sie **Eingabeaufforderung** aus, damit Ihre Architekten diese Funktion beim Anfordern eines Katalogelements aktivieren bzw. deaktivieren können.

Wenn eine Komponente eines Katalogelements nicht bereitgestellt werden kann, führt vRealize Automation ein Rollback aller Ressourcen für das gesamte Katalogelement durch. Sie verwenden diese benutzerdefinierte Eigenschaft, um dieses Verhalten außer Kraft zu setzen, damit Ihre Architekten die Stellen ausfindig machen können, an denen ihre Blueprints fehlschlagen. Anstelle der Blueprints fügen Sie der Business-Gruppe diese Eigenschaft hinzu, um sicherzustellen, dass Architekten dieses Verhalten immer außer Kraft setzen können. Diese Auswahlmöglichkeit wird den Benutzern jedoch niemals zufällig zur Verfügung gestellt.

- 6 Klicken Sie auf **Weiter**.
- 7 Geben Sie **Rainpole-Architekten** in das Suchfeld **Gruppenmanager** ein und wählen Sie Ihre benutzerdefinierte Gruppe aus.
- 8 Geben Sie **test\_user** in das Suchfeld **Benutzerrolle** ein und wählen Sie den lokalen Benutzer aus, den Sie als freigegebene Anmeldung zum Testen von Blueprints eingerichtet haben.
- 9 Klicken Sie auf **Weiter**.
- 10 Wählen Sie im Dropdown-Menü den Eintrag **Rainpole** als Standardmaschinenpräfix aus.
- 11 Klicken Sie auf **Beenden**.

### Weiter

Mit Ihren Fabric-Administratorrechten weisen Sie IaaS-Ressourcen zur Rainpole-Business-Gruppe hinzu, indem Sie eine Reservierung erstellen.

## Szenario: Erstellen einer Reservierung zum Zuweisen von Ressourcen zu Ihren Rainpole-Architekten

Mit Ihren Fabric-Administratorrechten erstellen Sie eine Reservierung für Ihre Rainpole-Business-Gruppe, um dieser vSphere-Ressourcen zuzuweisen.

---

**Hinweis** Nach dem Erstellen einer Reservierung können Sie die Business-Gruppe oder Computing-Ressource nicht mehr ändern.

---



**Vorgehensweise**

- 1 Wählen Sie **Infrastruktur > Reservierungen > Reservierungen** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Wählen Sie im Dropdown-Menü den Eintrag **vSphere** aus.
- 4 Geben Sie die Reservierungsinformationen ein.

Option	Eingabe
Name	Rainpole-Reservierung
Mandant	vsphere.local
Business-Gruppe	Rainpole-Business-Gruppe
Priorität	1

- 5 Wählen Sie die Registerkarte **Ressourcen** aus.
- 6 Geben Sie die Ressourceninformationen aus Ihrer Entwicklungsumgebung ein.

Option	Eingabe
Computing-Ressourcen	Wählen Sie im Dropdown-Menü ein Netzwerk aus.
Maschinenkontingent	Geben Sie die maximale Anzahl an eingeschalteten Maschinen für diese Reservierung ein.
Arbeitsspeicher	Geben Sie die maximale Anzahl an Arbeitsspeicher (MB) an, den diese Reservierung nutzen kann.
Speicher	Wählen Sie mindestens einen Speicherpfad sowie Reservierungsspeicher (GB) für diese Reservierung aus. Priorisieren Sie die Speicherpfade (wobei 1 die höchste Priorität darstellt).

- 7 Wählen Sie die Registerkarte **Netzwerk** aus.
- 8 Wählen Sie mindestens einen vSphere-Netzwerkpfad aus.
- 9 Klicken Sie auf **OK**.

Ihre vSphere-Infrastruktur wird jetzt von vRealize Automation verwaltet und Ihrem Team wurden vSphere-Ressourcen zugewiesen.

**Weiter**

Mit Ihren Rechten als IaaS-Architekt erstellen Sie einen Maschinen-Blueprint, um vSphere CentOS-Maschinen zu klonen.

## Szenario: Anwenden eines Standorts auf eine Computing-Ressource für regionsübergreifende Bereitstellungen

Als Fabric-Administrator sollten Sie Ihre Computing-Ressourcen als zu Ihrem Bostoner oder Londoner Datacenter gehörend bezeichnen, um regionsübergreifende Bereitstellungen zu ermöglichen. Wenn Ihre Blueprint-Architekten für deren Blueprints die Standorte-Funktion aktivieren, können die Benutzer auswählen, ob Maschinen in Ihrem Bostoner oder in Ihrem Londoner Datacenter bereitgestellt werden sollen.



Sie haben ein Datacenter in London und eines in Boston, und möchten nicht, dass Benutzer in Boston Maschinen Ihrer Londoner Infrastruktur bereitstellen und umgekehrt. Um sicherzustellen, dass Benutzer in Boston die Bereitstellung für Ihre Bostoner Infrastruktur vornehmen, und Benutzer in London die Bereitstellung für Ihre Londoner Infrastruktur vornehmen, sollten Sie den Benutzern erlauben, einen geeigneten Standort für die Bereitstellung auszuwählen, wenn sie Maschinen anfordern.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Fabric-Administrator** an.
- Als Systemadministrator definieren Sie die Datacenter-Standorte. Siehe [Szenario: Hinzufügen von Datacenter-Standorten für regionsübergreifende Bereitstellungen](#).

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Computing-Ressourcen > Computing-Ressourcen** aus.
- 2 Zeigen Sie auf die Computing-Ressource in Ihrem Bostoner Datacenter und klicken Sie auf **Bearbeiten**.
- 3 Wählen Sie Boston aus dem Dropdown-Menü **Standorte** aus.
- 4 Klicken Sie auf **OK**.
- 5 Wiederholen Sie diese Vorgehensweise so oft wie erforderlich, um Ihre Computing-Ressourcen Ihren Standorten in Boston und London zuzuordnen.

IaaS-Architekten können die Standorte-Funktion aktivieren, damit die Benutzer Maschinen in Boston oder London bereitstellen können, wenn sie ihre Katalogelement-Anforderungsformulare ausfüllen. Siehe [Szenario: Benutzern das Auswählen von Datacenter-Standorten für regionsübergreifende Bereitstellungen ermöglichen](#).

## Checkliste für die Implementierung einer vRealize Automation - Bereitstellung mithilfe eines externen IPAM-Anbieters.

Sie können IP-Adressen und -Bereiche zur Verwendung in einem externen und vorhandenen vRealize Automation-Netzwerkprofil bei einem unterstützten externen IPAM-Lösungsanbieter, wie z. B. Infoblox, erhalten. Die IP-Adressbereiche im Netzwerkprofil werden in einer verknüpften Reservierung verwendet, die Sie in einem Blueprint festlegen. Wenn ein berechtigter Benutzer mithilfe des Blueprint-Katalogelements die Bereitstellung einer Maschine anfordert, wird eine IP-Adresse aus dem IPAM-spezifischen IP-Adressbereich von Infoblox abgerufen. Nach Bereitstellung der Maschine können Sie die verwendete IP-Adresse ermitteln, indem Sie auf der Seite „Details“ des zugehörigen vRealize Automation-Elements eine Abfrage durchführen.

**Tabelle 3-6. Vorbereitungen für die Bereitstellung einer vRealize Automation -Bereitstellung mithilfe der IPAM-Checkliste von Infoblox.**

Aufgabe	Speicherort	Details
<input type="checkbox"/> Plug-In oder Paket des externen IPAM-Lösungsanbieters abrufen, importieren und konfigurieren.	Rufen Sie das vRealize Orchestrator-Plug-In ab und importieren Sie es, führen Sie die vRealize Orchestrator-Konfigurationsworkflows aus und registrieren Sie den Endpoint-Typ des IPAM-Anbieters in vRealize Orchestrator.  Wenn VMware Solution Exchange ( <a href="https://solution-exchange.vmware.com/store/category_groups/cloud-management">https://solution-exchange.vmware.com/store/category_groups/cloud-management</a> ) das benötigte IPAM-Anbieterpaket nicht enthält, können Sie mithilfe des SDKs des IPAM-Lösungsanbieters und der zugehörigen Dokumentation Ihr eigenes Paket erstellen.	Siehe <a href="#">Checkliste zum Vorbereiten der Unterstützung eines externen IPAM-Anbieters</a> .
<input type="checkbox"/> Endpoint für externen IPAM-Lösungsanbieter erstellen.	Erstellen Sie einen neuen IPAM-Endpoint in vRealize Automation.	Siehe <a href="#">Erstellen eines Endpoints für externen IPAM-Anbieter</a> .
<input type="checkbox"/> Endpoint-Einstellungen für externen IPAM-Lösungsanbieter in einem externen Netzwerkprofil angeben.	Erstellen Sie ein externes Netzwerkprofil und geben Sie den definierten IPAM-Endpoint in vRealize Automation an.	Siehe <a href="#">Erstellen eines externen Netzwerkprofils mithilfe eines externen IPAM-Anbieters</a> .
<input type="checkbox"/> Eine Reservierung definieren, um das externe Netzwerkprofil für einen vorhandenen Netzwerkpfad zu verwenden.	Erstellen Sie eine Reservierung, die das Netzwerkprofil in vRealize Automation aufruft.	Siehe <a href="#">Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer</a> .
<input type="checkbox"/> Einen Blueprint definieren, der das externe Netzwerkprofil verwendet.	Erstellen Sie einen Blueprint, der die Reservierung in vRealize Automation verwendet.	
<input type="checkbox"/> Berechtigungen für den Blueprint erteilen und zum Katalog hinzufügen.	Erteilen Sie Berechtigungen für den Blueprint und fügen Sie ihn zum Katalog in vRealize Automation hinzu.	

**Tabelle 3-6. Vorbereitungen für die Bereitstellung einer vRealize Automation -Bereitstellung mithilfe der IPAM-Checkliste von Infoblox. (Fortsetzung)**

Aufgabe	Speicherort	Details
<input type="checkbox"/> Bereitstellung einer Maschine mithilfe des Blueprint-Katalogelements anfordern.	Verwenden Sie das Blueprint-Katalogelement, um die Bereitstellung einer Maschine in vRealize Automation anzufordern.	
<input type="checkbox"/> Auf der Seite „Meine Elemente“ die IP-Adresse abfragen, auf der sich die Bereitstellung befindet.	Geben Sie die für die Bereitstellung in vRealize Automation verwendete IP-Netzwerkadresse an.	

## Konfigurieren von XaaS -Ressourcen

Durch das Konfigurieren von XaaS-Endpoints können Sie vRealize Automation mit Ihrer Umgebung verbinden. Wenn Sie vRealize Orchestrator-Plug-ins als Endpoints konfigurieren, müssen Sie zum Konfigurieren der Plug-ins die vRealize Automation-Benutzeroberfläche anstelle der vRealize Orchestrator-Konfigurationsschnittstelle verwenden.

Um mit vRealize Orchestrator-Funktionen und den vRealize Orchestrator-Plug-ins VMware und Drittanbietertechnologien für vRealize Automation verfügbar zu machen, können Sie die vRealize Orchestrator-Plug-ins konfigurieren, indem Sie sie als Endpoints hinzufügen. Auf diese Weise werden Verbindungen zu verschiedenen Hosts und Servern, wie zum Beispiel vCenter Server-Instanzen, einem Microsoft Active Directory-Host usw. erstellt.

Wenn Sie ein vRealize Orchestrator-Plug-in über die Benutzeroberfläche von vRealize Automation als Endpoint hinzufügen, führen Sie auf dem vRealize Orchestrator-Standardserver einen Konfigurations-Workflow aus. Die Konfigurations-Workflows befinden sich im Workflows-Ordner **vRealize Automation > XaaS > Endpoint-Konfiguration**.

**Wichtig** Das Konfigurieren eines einzelnen Plug-ins in vRealize Orchestrator und in der vRealize Automation-Konsole wird nicht unterstützt und führt zu Fehlern.

## Konfigurieren des Active Directory-Plug-Ins als Endpoint

Sie fügen einen Endpoint hinzu und konfigurieren das Active Directory-Plug-in, um eine Verbindung mit einer laufenden Active Directory-Instanz herzustellen und Benutzer und Benutzergruppen, Active Directory-Computer, Organisationseinheiten usw. zu konfigurieren.

Nach Hinzufügen eines Active Directory-Endpoints kann dieser jederzeit aktualisiert werden.

### Voraussetzungen

- Stellen Sie sicher, dass Sie Zugriff auf eine Microsoft Active Directory-Instanz haben. Weitere Informationen finden Sie in der Dokumentation zu Microsoft Active Directory.
- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

## Vorgehensweise

- 1 Wählen Sie **Administration > vRO-Konfiguration > Endpoints** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Wählen Sie im Dropdown-Menü **Plug-In** die Option **Active Directory** aus.
- 4 Klicken Sie auf **Weiter**.
- 5 Geben Sie einen Namen und optional eine Beschreibung ein.
- 6 Klicken Sie auf **Weiter**.
- 7 Konfigurieren Sie die Serverdetails für Active Directory.

- a Geben Sie im Textfeld **IP/URL des Active Directory-Hosts** die IP-Adresse oder den DNS-Namen des Hosts ein, auf dem Active Directory ausgeführt wird.
- b Geben Sie im Textfeld **Port** den Suchport Ihres Active Directory-Servers ein.

vRealize Orchestrator unterstützt die hierarchisch aufgebaute 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. Zusätzlich zu den Ports 389 und 3268 können Sie Port 636 für LDAPS verwenden.

- c Geben Sie im Textfeld **Stamm** das Stammelement des Active Directory-Dienstes ein.

Lautet Ihr Domänenname beispielsweise *mycompany.com*, dann lautet Ihr Active Directory-Stammverzeichnis **dc=mycompany,dc=com**.

Dieser Knoten wird zum Durchsuchen Ihres Dienstverzeichnisses nach Eingabe der entsprechenden Anmeldedaten verwendet. Im Falle großer Dienstverzeichnisse wird durch Angabe eines Knotens im Baum die Suche eingeeengt und die Leistung verbessert. Zum Beispiel können Sie **ou=employees,dc=mycompany,dc=com** angeben, anstatt das gesamte Verzeichnis zu durchsuchen. Dieses Stammelement zeigt alle Benutzer der Mitarbeiter-Gruppe an.

- d (Optional) Um die verschlüsselte Zertifizierung für die Verbindung zwischen vRealize Orchestrator und Active Directory zu aktivieren, wählen Sie aus dem Dropdown-Menü **SSL verwenden** die Option **Ja** aus.

Das SSL-Zertifikat wird, selbst wenn das Zertifikat selbstsigniert ist, automatisch und ohne Bestätigungsaufforderung importiert.

- e (Optional) Geben Sie im Textfeld **Standarddomäne** die Domäne ein.

Lautet Ihr Domänenname beispielsweise *mycompany.com*, geben Sie **@mycompany.com** ein.

## 8 Konfigurieren Sie die Einstellungen für gemeinsame Sitzungen.

Die Anmeldedaten werden von vRealize Orchestrator zur Ausführung aller Active Directory-Workflows und -Aktionen verwendet.

- a Geben Sie im Textfeld **Benutzername für die gemeinsame Sitzung** den Benutzernamen für die gemeinsame Sitzung ein.
- a Geben Sie im Textfeld **Kennwort für die gemeinsame Sitzung** das Kennwort für die gemeinsame Sitzung ein.

## 9 Klicken Sie auf **Beenden**.

Sie haben eine Active Directory-Instanz als Endpoint hinzugefügt. XaaS-Architekten können mit XaaS Workflows des Active Directory-Plug-ins als Katalogelemente und Ressourcenaktionen veröffentlichen.

### Weiter

- Um vRealize Automation-Blueprints zur Verwaltung der Active Directory-Benutzer in Ihrer Umgebung zu verwenden, erstellen Sie einen XaaS-Blueprint basierend auf Active Directory. Ein Beispiel finden Sie unter [Erstellen eines XaaS-Blueprints und einer Aktion zum Erstellen und Ändern eines Benutzers](#).
- Um vRealize Automation zum Erstellen von Active Directory-Datensätzen beim Bereitstellen einer Maschine zu verwenden, können Sie verschiedene Active Directory-Richtlinien erstellen und diese auf verschiedene Business-Gruppen und Blueprints anwenden. Siehe [Erstellen und Anwenden von Active Directory-Richtlinien](#).

## Konfigurieren des HTTP-REST-Plug-Ins als Endpoint

Sie können einen Endpoint hinzufügen und das HTTP-REST-Plug-in zur Verbindung mit einem REST-Host konfigurieren.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.
- Stellen Sie sicher, dass Sie Zugriff auf einen REST-Host haben.

### Vorgehensweise

- 1 Wählen Sie **Administration > vRO-Konfiguration > Endpoints** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Wählen Sie aus dem Dropdown-Menü **Plug-in** die Option **HTTP-REST** aus.
- 4 Klicken Sie auf **Weiter**.
- 5 Geben Sie einen Namen und optional eine Beschreibung ein.
- 6 Klicken Sie auf **Weiter**.

**7** Geben Sie Informationen zum REST-Host an.

- a Geben Sie im Textfeld **Name** den Namen des Hosts ein.
- b Geben Sie im Textfeld **URL** die Adresse des Hosts ein.

---

**Hinweis** Wenn Sie die Kerberos-Zugriffsauthentifizierung verwenden, müssen Sie die Hostadresse im FQDN-Format eingeben.

---

- c (Optional) Geben Sie im Textfeld **Zeitüberschreitung bei der Verbindung (Sekunden)** ein, nach wie vielen Sekunden die Zeitbegrenzung der Verbindung überschritten wird.

Die Standardeinstellung beträgt 30 Sekunden.

- d (Optional) Geben Sie im Textfeld **Zeitüberschreitung beim Vorgang (Sekunden)** ein, nach wie vielen Sekunden die Zeitbegrenzung eines Vorgangs überschritten wird.

Die Standardeinstellung beträgt 60 Sekunden.

**8** (Optional) Konfigurieren Sie die Proxy-Einstellungen.

- a Wählen Sie im Dropdown-Menü **Proxy verwenden** die Option **Ja** aus, um einen Proxy zu verwenden.
- b Geben Sie im Textfeld **Proxy-Adresse** die IP-Adresse des Proxy-Servers ein.
- c Geben Sie im Textfeld **Proxy-Port** die Portnummer für die Kommunikation mit dem Proxy-Server ein.

**9** Klicken Sie auf **Weiter**.**10** Wählen Sie den Authentifizierungstyp aus.

Option	Aktion
<b>Keine</b>	Es ist keine Authentifizierung erforderlich.
<b>OAuth 1.0</b>	<p>Verwendet das Protokoll OAuth 1.0. Sie müssen die erforderlichen Authentifizierungsparameter unter OAuth 1.0 angeben.</p> <ul style="list-style-type: none"> <li>a Geben Sie im Textfeld <b>Consumer-Schlüssel</b> den Schlüssel ein, der den Consumer als Dienstanbieter identifiziert.</li> <li>b Geben Sie im Textfeld <b>Consumer-Geheimnis</b> das Geheimnis zum Nachweis der Nutzungsberechtigung für den Consumer-Schlüssel ein.</li> <li>c (Optional) Geben Sie im Textfeld <b>Zugriffstoken</b> den Zugriffstoken ein, den der Consumer für den Zugriff auf die geschützten Ressourcen verwendet.</li> <li>d (Optional) Geben Sie im Textfeld <b>Zugriffstoken-Geheimnis</b> das Geheimnis ein, das dem Consumer als Nachweis der Nutzungsberechtigung für einen Token dient.</li> </ul>
<b>OAuth 2.0</b>	<p>Verwendet das Protokoll OAuth 2.0.</p> <p>Geben Sie im Textfeld <b>Token</b> das Authentifizierungstoken ein.</p>

Option	Aktion
<b>Einfach</b>	<p>Bietet eine Standardauthentifizierung für den Zugriff. Die Kommunikation mit dem Host erfolgt im Modus „Gemeinsame Sitzung“.</p> <ol style="list-style-type: none"> <li>Geben Sie im Textfeld <b>Authentifizierungs-Benutzername</b> den Benutzernamen für die gemeinsame Sitzung ein.</li> <li>Geben Sie im Textfeld <b>Authentifizierungskennwort</b> das Kennwort für die gemeinsame Sitzung ein.</li> </ol>
<b>Digest</b>	<p>Bietet eine Digest-Zugriffsauthentifizierung mit Verschlüsselung. Die Kommunikation mit dem Host erfolgt im Modus „Gemeinsame Sitzung“.</p> <ol style="list-style-type: none"> <li>Geben Sie im Textfeld <b>Authentifizierungs-Benutzername</b> den Benutzernamen für die gemeinsame Sitzung ein.</li> <li>Geben Sie im Textfeld <b>Authentifizierungskennwort</b> das Kennwort für die gemeinsame Sitzung ein.</li> </ol>
<b>NTLM</b>	<p>Bietet NT LAN Manager-Zugriffsauthentifizierung (NTLM) im Rahmen des Windows Security Support Provider (SSP). Die Kommunikation mit dem Host erfolgt im Modus „Gemeinsame Sitzung“.</p> <ol style="list-style-type: none"> <li>Geben Sie die Anmeldedaten für die gemeinsame Sitzung an. <ul style="list-style-type: none"> <li>Geben Sie im Textfeld <b>Authentifizierungs-Benutzername</b> den Benutzernamen für die gemeinsame Sitzung ein.</li> <li>Geben Sie im Textfeld <b>Authentifizierungskennwort</b> das Kennwort für die gemeinsame Sitzung ein.</li> </ul> </li> <li>Konfigurieren der NTLM-Angaben <ul style="list-style-type: none"> <li>(Optional) Geben Sie im Textfeld <b>Workstation für die NTLM-Authentifizierung</b> den Workstation-Namen ein.</li> <li>Geben Sie im Textfeld <b>Domäne für die NTLM-Authentifizierung</b> den Domänennamen ein.</li> </ul> </li> </ol>
<b>Kerberos</b>	<p>Bietet Kerberos-Zugriffsauthentifizierung. Die Kommunikation mit dem Host erfolgt im Modus „Gemeinsame Sitzung“.</p> <ol style="list-style-type: none"> <li>Geben Sie im Textfeld <b>Authentifizierungs-Benutzername</b> den Benutzernamen für die gemeinsame Sitzung ein.</li> <li>Geben Sie im Textfeld <b>Authentifizierungskennwort</b> das Kennwort für die gemeinsame Sitzung ein.</li> </ol>

## 11 Klicken Sie auf **Beenden**.

Sie haben den Endpoint konfiguriert und einen REST-Host hinzugefügt. XaaS-Architekten können mit XaaS Workflows des HTTP-REST-Plug-ins als Katalogelemente und Ressourcenaktionen veröffentlichen.

## Konfigurieren des PowerShell-Plug-ins als Endpoint

Sie können einen Endpoint hinzufügen und das PowerShell-Plug-in zur Verbindung mit einem laufenden PowerShell-Host konfigurieren, um auf diese Weise PowerShell-Skripts und PowerShell-cmdlets aus vRealize Orchestrator-Aktionen und -Workflows aufrufen und mit den Ergebnissen arbeiten zu können.

### Voraussetzungen

- Stellen Sie sicher, dass Sie Zugriff auf einen Windows PowerShell-Host haben. Weitere Informationen zu Microsoft Windows PowerShell finden Sie in der Dokumentation zu Windows PowerShell.
- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.



**Vorgehensweise**

- 1 Wählen Sie **Administration > vRO-Konfiguration > Endpoints** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Wählen Sie aus dem Dropdown-Menü **Plug-in** die Option **PowerShell** aus.
- 4 Klicken Sie auf **Weiter**.
- 5 Geben Sie einen Namen und optional eine Beschreibung ein.
- 6 Klicken Sie auf **Weiter**.
- 7 Geben Sie die Details zum PowerShell-Host an.
  - a Geben Sie im Textfeld **Name** den Namen des Hosts ein.
  - b Geben Sie im Textfeld **Host/IP** die IP-Adresse oder den FQDN des Hosts ein.
- 8 Wählen Sie den PowerShell-Hosttyp aus, mit dem das Plug-in eine Verbindung herstellen soll.

Option	Aktion
WinRM	<ol style="list-style-type: none"> <li>a Geben Sie im Textfeld <b>Port</b> unter den Details zum PowerShell-Host die Portnummer für die Kommunikation mit dem Host ein.</li> <li>b Wählen Sie aus dem Dropdown-Menü <b>Transportprotokoll</b> ein Transportprotokoll aus.</li> </ol> <p><b>Hinweis</b> Wenn Sie das HTTPS-Transportprotokoll verwenden, wird das Zertifikat des Remote-Powershell-Hosts in den vRealize Orchestrator-Keystore importiert.</p> <ol style="list-style-type: none"> <li>c Wählen Sie den Authentifizierungstyp aus dem Dropdown-Menü <b>Authentifizierung</b> aus.</li> </ol> <p><b>Hinweis</b> Um die Kerberos-Authentifizierung zu verwenden, aktivieren Sie diese im WinRM-Dienst. Informationen zum Konfigurieren der Kerberos-Authentifizierung finden Sie unter <i>Verwenden des PowerShell-Plug-ins</i>.</p>
SSH	Keine.

- 9 Geben Sie in den Feldern **Benutzername** und **Kennwort** die Anmeldedaten für die Kommunikation mit dem PowerShell-Host in einer gemeinsamen Sitzung ein.
- 10 Klicken Sie auf **Beenden**.

Sie haben einen Windows PowerShell-Host als Endpoint hinzugefügt. XaaS-Architekten können mit XaaS Workflows des PowerShell-Plug-ins als Katalogelemente und Ressourcenaktionen veröffentlichen.

**Konfigurieren des SOAP-Plug-Ins als Endpoint**

Sie können einen Endpoint hinzufügen und das SOAP-Plug-in so konfigurieren, dass ein SOAP-Dienst als Bestandslistenobjekt definiert wird und SOAP-Vorgänge an den definierten Objekten vorgenommen werden.

## Voraussetzungen

- Stellen Sie sicher, dass Sie Zugriff auf einen SOAP-Host haben. Das Plug-in unterstützt die SOAP-Versionen 1.1 und 1.2 sowie WSDL 1.1 und 2.0.
- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

## Vorgehensweise

- 1 Wählen Sie **Administration > vRO-Konfiguration > Endpoints** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Wählen Sie aus dem Dropdown-Menü **Plug-in** die Option **SOAP** aus.
- 4 Klicken Sie auf **Weiter**.
- 5 Geben Sie einen Namen und optional eine Beschreibung ein.
- 6 Klicken Sie auf **Weiter**.
- 7 Geben Sie die Details für den SOAP-Host an.
  - a Geben Sie im Textfeld **Name** den Namen des Hosts ein.
  - b Wählen Sie über das Dropdown-Menü **WSDL-Inhalte bereitstellen** aus, ob WSDL-Inhalte als Text bereitgestellt werden sollen.

Option	Aktion
<b>Ja</b>	Geben Sie im Textfeld <b>WSDL-Inhalte</b> den WSDL-Text ein.
<b>Nein</b>	Geben Sie im Textfeld <b>WSDL-URL</b> den richtigen Pfad ein.

- c (Optional) Geben Sie im Textfeld **Zeitüberschreitung bei der Verbindung (in Sekunden)** ein, nach wie vielen Sekunden die Zeitbegrenzung der Verbindung überschritten wird.  
Die Standardeinstellung beträgt 30 Sekunden.
  - d (Optional) Geben Sie im Textfeld **Zeitüberschreitung bei der Anforderung (in Sekunden)** ein, nach wie vielen Sekunden die Zeitbegrenzung eines Vorgangs überschritten wird.  
Die Standardeinstellung beträgt 60 Sekunden.
- 8 (Optional) Geben Sie die Proxy-Einstellungen an.
  - a Wählen Sie im Dropdown-Menü **Proxy** die Option **Ja** aus, um einen Proxy zu verwenden.
  - b Geben Sie im Textfeld **Adresse** die IP-Adresse des Proxy-Servers ein.
  - c Geben Sie im Textfeld **Port** die Portnummer für die Kommunikation mit dem Proxy-Server ein.
- 9 Klicken Sie auf **Weiter**.

## 10 Wählen Sie den Authentifizierungstyp aus.

Option	Aktion
<b>Keine</b>	Es ist keine Authentifizierung erforderlich.
<b>Einfach</b>	<p>Bietet eine Standardauthentifizierung für den Zugriff. Die Kommunikation mit dem Host erfolgt im Modus „Gemeinsame Sitzung“.</p> <ol style="list-style-type: none"> <li>Geben Sie im Textfeld <b>Benutzername</b> den Benutzernamen für die gemeinsame Sitzung ein.</li> <li>Geben Sie im Textfeld <b>Kennwort</b> das Kennwort für die gemeinsame Sitzung ein.</li> </ol>
<b>Digest</b>	<p>Bietet eine Digest-Zugriffsauthentifizierung mit Verschlüsselung. Die Kommunikation mit dem Host erfolgt im Modus „Gemeinsame Sitzung“.</p> <ol style="list-style-type: none"> <li>Geben Sie im Textfeld <b>Benutzername</b> den Benutzernamen für die gemeinsame Sitzung ein.</li> <li>Geben Sie im Textfeld <b>Kennwort</b> das Kennwort für die gemeinsame Sitzung ein.</li> </ol>
<b>NTLM</b>	<p>Bietet NT LAN Manager-Zugriffsauthentifizierung (NTLM) im Rahmen des Windows Security Support Provider (SSP). Die Kommunikation mit dem Host erfolgt im Modus „Gemeinsame Sitzung“.</p> <ol style="list-style-type: none"> <li>Geben Sie die Anmeldedaten an. <ul style="list-style-type: none"> <li>Geben Sie im Textfeld <b>Benutzername</b> den Benutzernamen für die gemeinsame Sitzung ein.</li> <li>Geben Sie im Textfeld <b>Kennwort</b> das Kennwort für die gemeinsame Sitzung ein.</li> </ul> </li> <li>Geben Sie die NTLM-Einstellungen an. <ul style="list-style-type: none"> <li>Geben Sie im Textfeld <b>NTLM-Domäne</b> den Domänennamen ein.</li> <li>(Optional) Geben Sie im Textfeld <b>NTLM-Workstation</b> den Workstation-Namen ein.</li> </ul> </li> </ol>
<b>Negotiate</b>	<p>Bietet Kerberos-Zugriffsauthentifizierung. Die Kommunikation mit dem Host erfolgt im Modus „Gemeinsame Sitzung“.</p> <ol style="list-style-type: none"> <li>Geben Sie die Anmeldedaten an. <ol style="list-style-type: none"> <li>Geben Sie im Textfeld <b>Benutzername</b> den Benutzernamen für die gemeinsame Sitzung ein.</li> <li>Geben Sie im Textfeld <b>Kennwort</b> das Kennwort für die gemeinsame Sitzung ein.</li> </ol> </li> <li>Geben Sie im Textfeld <b>SPN des Kerberos-Diensts</b> den SPN des Kerberos-Diensts ein.</li> </ol>

## 11 Klicken Sie auf **Beenden**.

Sie haben einen SOAP-Dienst hinzugefügt. XaaS-Architekten können mit XaaS Workflows des SOAP-Plug-ins als Katalogelemente und Ressourcenaktionen veröffentlichen.

## Konfigurieren des vCenter Server -Plug-ins als Endpoint

Sie können einen Endpoint hinzufügen und das vCenter Server-Plug-in zur Verbindung mit einer laufenden vCenter Server-Instanz konfigurieren, um XaaS-Blueprints zur Verwaltung von vSphere-Bestandslistenobjekten zu erstellen.

## Voraussetzungen

- Installieren und konfigurieren Sie vCenter Server. Siehe *Installations- und Einrichtungshandbuch für vSphere*.
- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

## Vorgehensweise

- 1 Wählen Sie **Administration > vRO-Konfiguration > Endpoints** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Wählen Sie aus dem Dropdown-Menü **Plug-in** die Option **vCenter Server** aus.
- 4 Klicken Sie auf **Weiter**.
- 5 Geben Sie einen Namen und optional eine Beschreibung ein.
- 6 Klicken Sie auf **Weiter**.
- 7 Geben Sie Informationen zur vCenter Server-Instanz an.
  - a Geben Sie im Textfeld **IP oder Hostname der hinzuzufügenden vCenter Server-Instanz** die IP-Adresse oder den DNS-Namen der Maschine ein.

Dabei handelt es sich um die IP-Adresse oder den DNS-Namen der Maschine, auf der die vCenter Server-Instanz, die Sie hinzufügen möchten, installiert ist.
  - b Geben Sie im Textfeld **Port der vCenter Server-Instanz** den Port für die Kommunikation mit der vCenter Server-Instanz ein.

Der Standardport lautet 443.
  - c Geben Sie im Textfeld **Speicherort des SDK, das zur Verbindung mit der vCenter Server-Instanz verwendet werden soll** den Speicherort des SDK, das zur Verbindung mit Ihrer vCenter Server-Instanz verwendet werden soll, ein.

Beispiel: `/sdk`.
- 8 Klicken Sie auf **Weiter**.
- 9 Legen Sie die Verbindungsparameter fest.
  - a Geben Sie im Textfeld **HTTP-Port der vCenter Server-Instanz – VC-Plug-in-Version 5.5.2 oder früher** den HTTP-Port der vCenter Server-Instanz ein.
  - b Geben Sie in den Textfeldern **Benutzername des Benutzers, den Orchestrator zur Verbindung mit der vCenter Server-Instanz verwenden wird** und **Kennwort des Benutzers, den Orchestrator zur Verbindung mit der vCenter Server-Instanz verwenden wird** die Anmeldedaten ein, die vRealize Orchestrator zum Herstellen einer Verbindung mit der vCenter Server-Instanz verwenden soll.

Der ausgewählte Benutzer muss ein gültiger Benutzer mit Berechtigungen zur Verwaltung von vCenter Server-Erweiterungen und einer Reihe von benutzerdefinierten Berechtigungen sein.
- 10 Klicken Sie auf **Beenden**.

Sie haben eine vCenter Server-Instanz als Endpoint hinzugefügt. XaaS-Architekten können mit XaaS Workflows des vCenter Server-Plug-ins als Katalogelemente und Ressourcenaktionen veröffentlichen.

## Installieren zusätzlicher Plug-Ins auf dem vRealize Orchestrator -Standardserver

Auf dem vRealize Orchestrator-Standardserver können Sie mithilfe der vRealize Orchestrator-Konfigurationsschnittstelle zusätzliche Pakete und Plug-Ins installieren.

Auf dem vRealize Orchestrator-Standardserver können Sie zusätzliche Plug-Ins installieren und die Workflows mit XaaS verwenden.

Darüber hinaus können Sie zusätzliche Pakete auf dem vRealize Orchestrator-Standardserver für die Konfiguration als vRealize Automation-Endpoint-Typen für den externen IPAM-Anbieter importieren. Beispielsweise finden Sie Informationen zum Abrufen, Importieren und Konfigurieren des IPAM-Pakets Infoblox unter [Checkliste zum Vorbereiten der Unterstützung eines externen IPAM-Anbieters](#).

Paketdateien (.package) und Plug-In-Installationsdateien (.vmoapp oder .dar) sind über den VMware Solution Exchange unter [https://solutionexchange.vmware.com/store/category\\_groups/cloud-management](https://solutionexchange.vmware.com/store/category_groups/cloud-management) verfügbar. Informationen zu Plug-In-Dateien finden Sie in der Dokumentation zu vRealize Orchestrator-Plug-Ins unter [https://www.vmware.com/support/pubs/vco\\_plugins\\_pubs.html](https://www.vmware.com/support/pubs/vco_plugins_pubs.html).

Weitere Informationen zum Installieren neuer Plug-Ins finden Sie unter *Installieren und Konfigurieren von VMware vCenter Orchestrator*.

## Arbeiten mit Active Directory-Richtlinien

Anhand von Active Directory-Richtlinien werden die Eigenschaften eines Maschinendatensatzes (z. B. „domain“) sowie die Organisationseinheit, in der der Datensatz erstellt wird, mithilfe eines vRealize Automation-Blueprints definiert.

Wenn Sie eine Richtlinie auf eine Business-Gruppe anwenden, werden alle Maschinenanforderungen von den Mitgliedern der Business-Gruppe der angegebenen Organisationseinheit hinzugefügt. Sie können unterschiedliche Richtlinien für verschiedene Organisationseinheiten erstellen und dann die unterschiedlichen Richtlinien auf verschiedene Business-Gruppen anwenden.

Active Directory-Richtlinien sind eine tech preview-Funktion in vRealize Automation 7.1 und sollten in einer Produktionsumgebung nicht verwendet werden.

## Verwenden von benutzerdefinierten Eigenschaften zum Überschreiben einer Active Directory-Richtlinie

Mithilfe der angegebenen benutzerdefinierten Active Directory-Eigenschaften können Sie die Active Directory-Richtlinie, die Domäne, die Organisationseinheit und andere Werte in einem bestimmten Blueprint überschreiben, wenn dieser bereitgestellt wird.

Die Liste der angegebenen benutzerdefinierten Active Directory-Eigenschaften ist in der *Referenz für benutzerdefinierte Eigenschaften* enthalten. Das Präfix der benutzerdefinierten Eigenschaft ist `ext.policy.activedirectory`.

Zusätzlich zu den angegebenen Eigenschaften können Sie eigene benutzerdefinierte Eigenschaften erstellen. Ihren benutzerdefinierten Eigenschaften muss das Präfix `ext.policy.activedirectory` vorangestellt werden. Beispiel: `ext.policy.activedirectory.domain.extension` oder `ext.policy.activedirectory.yourproperty`. Die Eigenschaften werden an die benutzerdefinierten Active Directory-Workflows von vRealize Orchestrator übergeben.

Weitere Informationen zu benutzerdefinierten Eigenschaften finden Sie unter *Referenz für benutzerdefinierte Eigenschaften*. Je nachdem, welche Werte Sie überschreiben, müssen Sie möglicherweise eine Eigenschaftsdefinition erstellen. Sie können beispielsweise eine Eigenschaftsdefinition erstellen, die die verfügbaren Active Directory-Richtlinien von vRealize Automation abrufen. Alternativ können Sie eine Definition erstellen, die es dem anfordernden Benutzer gestattet, unter zwei oder mehr alternativen Organisationseinheiten zu wählen. Siehe *Referenz für benutzerdefinierte Eigenschaften*.

## Erstellen und Anwenden von Active Directory-Richtlinien

Sie erstellen eine oder mehrere Active Directory-Richtlinien, damit Sie verschiedenen Business-Gruppen unterschiedliche Richtlinien zuweisen können. Die unterschiedlichen Richtlinien können Sie verwenden, um Maschinendatensätze basierend auf der Mitgliedschaft in Business-Gruppen verschiedenen Organisationseinheiten zuzuweisen.

Die zugewiesene Richtlinie kann bei Bedarf überschrieben werden.

Active Directory-Richtlinien sind eine tech preview-Funktion in vRealize Automation 7.1 und sollten in einer Produktionsumgebung nicht verwendet werden.

### Vorgehensweise

#### 1 Erstellen einer Active Directory-Richtlinie

Eine Active Directory-Richtlinie wird erstellt, um festzulegen, wo Datensätze in einer Active Directory-Instanz hinzugefügt werden, wenn Benutzer Maschinen bereitstellen. Sie können eine Richtlinie einer Business-Gruppe zuweisen, sodass sich aus allen von den Mitgliedern der Business-Gruppe bereitgestellten Maschinen ein in der angegebenen Organisationseinheit erstellter Datensatz ergibt.

#### 2 Szenario: Hinzufügen einer benutzerdefinierten Eigenschaft zu Blueprints, um eine Active Directory-Richtlinie zu überschreiben

Als Blueprint-Architekt für die Business-Gruppe der Entwicklungsabteilung verfügen Sie über einen Blueprint, der eine Anwendungsmaschine und eine Datenbankmaschine umfasst. Sie möchten den Datensatz einer Datenbankmaschine zu einer Organisationseinheit hinzufügen, die sich von der angewendeten Active Directory-Richtlinie unterscheidet.

## Erstellen einer Active Directory-Richtlinie

Eine Active Directory-Richtlinie wird erstellt, um festzulegen, wo Datensätze in einer Active Directory-Instanz hinzugefügt werden, wenn Benutzer Maschinen bereitstellen. Sie können eine Richtlinie einer Business-Gruppe zuweisen, sodass sich aus allen von den Mitgliedern der Business-Gruppe bereitgestellten Maschinen ein in der angegebenen Organisationseinheit erstellter Datensatz ergibt.

Sie erstellen unterschiedliche Active Directory-Richtlinien, wenn von verschiedenen Business-Gruppen bereitgestellte Maschinen sich in unterschiedlichen Domänen befinden oder zu verschiedenen Active Directory-Instanzen hinzugefügt werden sollen.

### Voraussetzungen

- Stellen Sie sicher, dass Sie einen Active Directory-Endpoint erstellt haben. Siehe [Konfigurieren des Active Directory-Plug-Ins als Endpoint](#).
- Überprüfen Sie bei Verwendung eines externen vRealize Orchestrator-Servers, dass dieser ordnungsgemäß eingerichtet wurde. Siehe [Konfigurieren eines externen vRealize Orchestrator-Servers](#).
- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > AD-Richtlinien** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Konfigurieren Sie die Details der Active Directory-Richtlinie.

Option	Beschreibung
<b>ID</b>	Geben Sie den dauerhaften Wert ein. Der Wert darf keine Leerzeichen oder Sonderzeichen enthalten. Der Wert kann zu einem späteren Zeitpunkt nicht mehr geändert werden. Sie können die Richtlinie lediglich mit einer neuen ID neu erstellen.
<b>Beschreibung</b>	Die Beschreibung der Richtlinie.
<b>Active Directory-Endpoint</b>	Wählen Sie den Active Directory-Endpoint aus, für den diese Richtlinie erstellt wird.
<b>Domäne</b>	Geben Sie die Root-Domäne ein. Format: <i>meinunternehmen.com</i> .
<b>Organisationseinheit</b>	Geben Sie den definierten Namen der Organisationseinheit für diese Richtlinie ein. Die Hierarchie muss in Form einer kommagetrennten Liste eingegeben werden. Beispiel: ou=development,dc=corp,dc=domain,dc=com.

- 4 Klicken Sie auf **OK**.

Der Active Directory-Endpoint für vRealize Orchestrator wird der Liste hinzugefügt. Sie können die Richtlinie in Business-Gruppen anwenden oder die Richtlinie in Blueprints oder Business-Gruppen verwenden.

### Weiter

- Erstellen Sie weitere Richtlinien, um mehrere Richtlinienoptionen anzugeben.

- Um Datensätze beim Bereitstellen eines Blueprints basierend auf der Mitgliedschaft in Business-Gruppen zu Active Directory hinzuzufügen, fügen Sie die entsprechende Active Directory-Richtlinie einer Business-Gruppe hinzu. Siehe [Erstellen einer Business-Gruppe](#). Sie können die Richtlinie beim Erstellen der Business-Gruppe anwenden oder zu einem späteren Zeitpunkt hinzufügen.
- Um die Active Directory-Richtlinie für die Business-Gruppe für einen bestimmten Blueprint zu überschreiben, fügen Sie dem Blueprint benutzerdefinierte Active Directory-Eigenschaften hinzu. Siehe [Szenario: Hinzufügen einer benutzerdefinierten Eigenschaft zu Blueprints, um eine Active Directory-Richtlinie zu überschreiben](#).

## Szenario: Hinzufügen einer benutzerdefinierten Eigenschaft zu Blueprints, um eine Active Directory-Richtlinie zu überschreiben

Als Blueprint-Architekt für die Business-Gruppe der Entwicklungsabteilung verfügen Sie über einen Blueprint, der eine Anwendungsmaschine und eine Datenbankmaschine umfasst. Sie möchten den Datensatz einer Datenbankmaschine zu einer Organisationseinheit hinzufügen, die sich von der angewendeten Active Directory-Richtlinie unterscheidet.

Auf die Business-Gruppe der Entwicklungsabteilung wurde eine Richtlinie angewendet. Die Richtlinie fügt Maschinendatensätze zu „ou=development,dc=corp,dc=domain,dc=com“ hinzu. Alle Datenbankmaschinen sollen zu „ou=databases,dc=corp,dc=domain,dc=com“ hinzugefügt werden. In einem Blueprint, der einen Datenbankserver enthält, überschreiben Sie die Active Directory-Organisationseinheit, um den Datensatz der Datenbankmaschine zu „ou=databases,dc=corp,dc=domain,dc=com“ hinzuzufügen.

Bei diesem Szenario wird von folgenden Annahmen ausgegangen:

- Ihr Active Directory enthält Organisationseinheiten für die Entwicklungsabteilung und für Datenbanken.
- Sie haben einen Test-Blueprint, der in einem Dienst enthalten ist, und der Dienst verfügt über eine Berechtigung.

Zusätzlich zu diesem einfachen Beispiel, in dem gezeigt wird, wie Sie die Richtlinie überschreiben können, können Sie in Verbindung mit der Active Directory-Richtlinie benutzerdefinierte Eigenschaften verwenden, um beim Bereitstellen von Blueprints weitere Änderungen an Active Directory vorzunehmen. Siehe [Arbeiten mit Active Directory-Richtlinien](#).

### Voraussetzungen

- Stellen Sie sicher, dass Sie über mindestens eine Active Directory-Richtlinie verfügen. Siehe [Erstellen einer Active Directory-Richtlinie](#). Sie erstellen beispielsweise eine Entwicklungsrichtlinie, die Datensätze zu „ou=development,dc=corp,dc=domain,dc=com“ hinzufügt.
- Stellen Sie sicher, dass Sie über eine Business-Gruppe verfügen, auf die Sie eine Active Directory-Richtlinie angewendet haben. Siehe [Erstellen einer Business-Gruppe](#). Beispielsweise verwendet die Business-Gruppe für die Entwicklungsabteilung die Entwicklungsrichtlinie.

### Vorgehensweise

- 1 Wählen Sie im Test-Blueprint die Datenbankmaschine auf der Arbeitsfläche aus.



- 2 Klicken Sie auf die Registerkarte **Eigenschaften**.
- 3 Klicken Sie auf die Registerkarte **Benutzerdefinierte Eigenschaften**.
- 4 Klicken Sie auf das Symbol **Neu** (+).
- 5 Fügen Sie die benutzerdefinierte Eigenschaft zum Ändern der Standardorganisationseinheit hinzu.
  - a Geben Sie im Textfeld **Name** Folgendes ein: **ext.policy.activedirectory.orgunit**.
  - b Geben Sie im Textfeld **Wert** Folgendes ein: **ou=databases,dc=corp,dc=domain,dc=com**.
  - c Deaktivieren Sie **Überschreibbar**.
  - d Klicken Sie auf **OK**.
- 6 Klicken Sie auf **Fertig stellen**.

Der Test-Blueprint enthält die benutzerdefinierte Eigenschaft. Die benutzerdefinierte Eigenschaft wird den Benutzern im Anforderungsformular jedoch nicht angezeigt.

#### Weiter

Fordern Sie den Test-Blueprint an. Überprüfen Sie, ob der Datensatz für die Datenbankmaschine der Organisationseinheit der Datenbank und der Datensatz für die Anwendungsmaschine der Organisationseinheit der Entwicklungsabteilung hinzugefügt wurde. Wenn Sie mit den Ergebnissen zufrieden sind, können Sie die benutzerdefinierte Eigenschaft Ihren Produktions-Blueprints hinzufügen.

# Bereitstellen von bedarfsgesteuerten Diensten für Benutzer

## 4

Sie stellen Benutzern bedarfsgesteuerte Dienste bereit, indem Sie Katalogelemente und Aktionen erstellen, und anschließend sorgfältig steuern, wer diese Dienste anfordern kann, indem Sie Berechtigungen und Genehmigungen verwenden.

Dieses Kapitel behandelt die folgenden Themen:

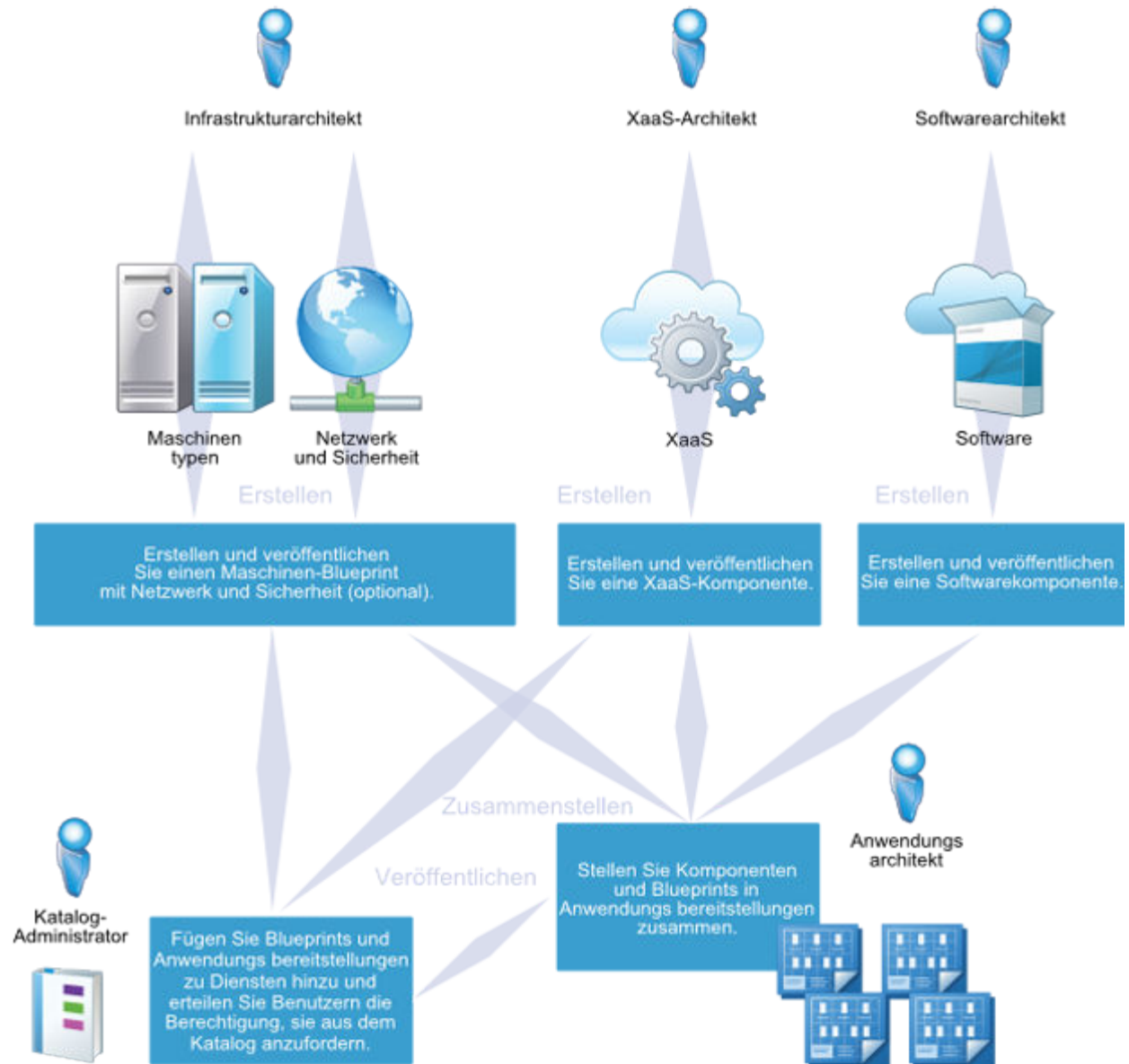
- [Entwerfen von Blueprints](#)
- [Exportieren und Importieren von Blueprints](#)
- [Erstellen Ihrer Design-Bibliothek](#)
- [Erstellen zusammengesetzter Blueprints](#)
- [Verwalten des Servicekatalogs](#)

## Entwerfen von Blueprints

Blueprint-Architekten erstellen Software-Komponenten, Maschinen-Blueprints und benutzerdefinierte XaaS-Blueprints und stellen diese Komponenten zu den Blueprints zusammen, welche die Elemente definieren, die von den Benutzern aus dem Katalog angefordert werden.

Sie können Blueprints für eine einzelne Maschine oder aber einen einzelnen benutzerdefinierten XaaS-Blueprint erstellen und veröffentlichen. Darüber hinaus können Sie Maschinenkomponenten und XaaS-Blueprints mit anderen Bausteinen zusammenfassen, um ausgefeilte Katalogelement-Blueprints zu entwerfen, die mehrere Maschinen, Netzwerk- und Sicherheitskomponenten, Software mit vollständiger Lebenszyklusunterstützung sowie benutzerdefinierte XaaS-Funktionalität enthalten.

In Abhängigkeit vom zu definierenden Katalogelement kann der Prozess einfach darin bestehen, dass ein einzelner Infrastrukturarchitekt eine Maschinenkomponente als Blueprint veröffentlicht, oder aber es können mehrere Infrastrukturarchitekten beteiligt sein, die viele verschiedene Komponententypen erstellen, um einen umfassenden Anwendungs-Stack für die Benutzer zu entwerfen.



## Software -Komponenten

Sie können Softwarekomponenten erstellen und veröffentlichen, um Software während des Maschinenbereitstellungsprozesses zu installieren und den Softwarelebenszyklus zu unterstützen. Beispielsweise können Sie einen Blueprint erstellen, mit dem Entwickler eine Maschine mit bereits installierter und konfigurierter Bereitstellungsumgebung anfordern können. Softwarekomponenten sind keine separaten Katalogelemente, und Sie müssen sie mit einer Maschinenkomponente kombinieren, um einen Katalogelement-Blueprint zu erstellen.

## Maschinen-Blueprints

Sie können einfache Blueprints erstellen und veröffentlichen, um einzelne Maschinen bereitzustellen. Sie können aber auch Multi-Maschinen-Blueprints erstellen, die mehrere unterschiedliche Typen von Maschinenkomponenten enthalten. Darüber hinaus können Sie Netzwerk- und Sicherheitskomponenten zu Maschinen-Blueprints hinzufügen, wie beispielsweise Sicherheitsgruppen oder Netzwerkprofile.

## XaaS -Blueprints

Sie können Ihre vRealize Orchestrator-Workflows als XaaS-Blueprints veröffentlichen. Beispielsweise können Sie eine benutzerdefinierte Ressource für Active Directory-Benutzer erstellen und einen XaaS-Blueprint entwerfen, damit Manager neue Benutzer in ihrer Active Directory-Gruppe bereitstellen können. XaaS-Komponenten werden außerhalb der Registerkarte „Design“ erstellt und verwaltet. Sie können veröffentlichte XaaS-Blueprints zum Erstellen von Anwendungs-Blueprints wiederverwenden, jedoch nur in Kombination mit mindestens einer Maschinenkomponente.

## Anwendungs-Blueprints mit Multi-Maschinen-, XaaS - und Software -Komponenten.

Sie können einem Maschinen-Blueprint eine beliebige Anzahl von Maschinenkomponenten, Software-Komponenten und XaaS-Blueprints hinzufügen, um Ihren Benutzern ausgefeilte Funktionen bereitzustellen. Beispielsweise können Sie einen Blueprint erstellen, mit dem Manager ein Setup für neue Mitarbeiter bereitstellen können. Sie können mehrere Maschinenkomponenten, Softwarekomponenten und einen XaaS-Blueprint für die Bereitstellung neuer Active Directory-Benutzer kombinieren. Der QE-Manager kann Ihr Katalogelement für neue Mitarbeiter anfordern, und der neue Qualitätsingenieur wird in Active Directory bereitgestellt und erhält zwei funktionierende virtuelle Maschinen (eine Windows- und eine Linux-VM), die jeweils mit der gesamten erforderlichen Software zum Ausführen von Testläufen in diesen Umgebungen ausgestattet sind.

## Exportieren und Importieren von Blueprints

Mithilfe der vRealize Automation-REST-API oder dem vRealize CloudClient können Sie Inhalte programmgesteuert aus einer vRealize Automation-Umgebung exportieren und in eine andere Umgebung importieren.

Beispielsweise können Sie Ihre Blueprints in einer Entwicklungsumgebung erstellen und testen und anschließend in Ihre Produktionsumgebung importieren. Sie können aber auch eine Eigenschaftsdefinition aus einem Community-Forum in Ihre aktive vRealize Automation-Mandanteninstanz importieren.

Die folgenden vRealize Automation-Inhalte können Sie programmgesteuert importieren und exportieren:

- Anwendungs-Blueprints und alle zugehörigen Komponenten
- IaaS-Maschinen-Blueprints
- Software-Komponenten
- XaaS-Blueprints

## ■ Eigenschaftsgruppen

Informationen zu Eigenschaftsgruppen sind mandantenspezifisch und werden nur mit dem Blueprint importiert, wenn die Eigenschaftsgruppe bereits in der vRealize Automation-Zielinstanz vorhanden ist.

Wenn Sie einen Blueprint aus einer vRealize Automation-Mandanteninstanz in eine andere Mandanteninstanz exportieren, werden die Informationen zu Eigenschaftsgruppen für diesen Blueprint für den importierten Blueprint nur erkannt, wenn die Eigenschaftsgruppe bereits in der Zielmandanteninstanz vorhanden ist. Wenn Sie beispielsweise einen Blueprint importieren, der die Eigenschaftsgruppe `mica1` enthält, ist die Eigenschaftsgruppe `mica1` nur im importierten Blueprint vorhanden, wenn die Eigenschaftsgruppe `mica1` bereits in der vRealize Automation-Instanz vorhanden ist, in die Sie den Blueprint importieren. Um den Verlust von Informationen zu Eigenschaftsgruppen beim Exportieren eines Blueprints aus einer vRealize Automation-Instanz in eine andere zu vermeiden, erstellen Sie mithilfe von vRealize CloudClient eine Exportpaket-ZIP-Datei, die die Eigenschaftsgruppe enthält. Importieren Sie dann diese Paket-ZIP-Datei in den Zielmandanten, bevor Sie den Blueprint importieren. Weitere Informationen zur Verwendung von vRealize CloudClient zum Auflisten, Verpacken, Exportieren und Importieren von Eigenschaftsgruppen sowie anderen vRealize Automation-Elementen finden Sie im VMware Developer Center unter <https://developercenter.vmware.com/tool/cloudclient>.

**Tabelle 4-1. Auswählen Ihres Import- und Exporttools**

Tool	Weitere Informationen
vRealize CloudClient	Weitere Informationen finden Sie auf der VMware Developer-Website unter <a href="https://developercenter.vmware.com/tool/cloudclient">https://developercenter.vmware.com/tool/cloudclient</a> .
vRealize Automation-REST-API	Weitere Informationen finden Sie im <i>Programmierhandbuch</i> im vRealize Automation Informationscenter unter <a href="https://www.vmware.com/support/pubs/vcac-pubs.html">https://www.vmware.com/support/pubs/vcac-pubs.html</a> .

**Hinweis** Wenn Sie Blueprints programmgesteuert über vRealize Automation-Bereitstellungen hinweg exportieren und importieren, z. B. von einer Test- zu einer Produktionsumgebung oder von einer Organisation zu einer anderen, ist es wichtig zu erkennen, dass geklonte Vorlagendaten in dem Paket enthalten sind. Wenn Sie das Blueprint-Paket importieren, werden Standardeinstellungen basierend auf den Informationen im Paket aufgefüllt. Wenn Sie z. B. einen Blueprint, der mithilfe eines geklonten Workflows erstellt wurde, exportieren und anschließend importieren und die Vorlage, von der die geklonten Daten abgeleitet wurden, an keinem Endpoint innerhalb derjenigen vRealize Automation-Bereitstellung vorhanden ist, in welche Sie den Blueprint importieren, sind einige importierte Blueprint-Einstellungen bei dieser Bereitstellung nicht anwendbar.

## Szenario: Importieren der vSphere -Beispielanwendung „Dukes Bank“ und Konfigurieren für Ihre Umgebung

Als IT-Experte, der vRealize Automation bewertet oder sich damit vertraut macht, möchten Sie eine stabile Beispielanwendung in Ihre vRealize Automation-Instanz importieren, sodass Sie schnell die verfügbare Funktionalität erkunden und festlegen können, wie Sie möglicherweise vRealize Automation-Blueprints erstellen, die für die Anforderungen Ihrer Organisation geeignet sind.

## Voraussetzungen

- Bereiten Sie eine CentOS 6.x-Linux-Referenzmaschine vor, konvertieren Sie sie in eine Vorlage und erstellen Sie eine Anpassungsspezifikation. Siehe [Szenario: Vorbereiten auf den Import des vSphere-Beispielanwendungs-Blueprints „Dukes Bank“](#).
- Erstellen Sie ein externes Netzwerkprofil zum Bereitstellen eines Gateways und eines Bereichs von IP-Adressen. Siehe [Erstellen eines externen Netzwerkprofils mithilfe eines externen IPAM-Anbieters](#).
- Ordnen Sie Ihr externes Netzwerkprofil zu Ihrer vSphere-Reservierung zu. Siehe [Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer](#). Die Beispielanwendung kann ohne ein externes Netzwerkprofil nicht erfolgreich bereitgestellt werden.
- Stellen Sie sicher, dass Sie sowohl über die Rechte als **Infrastrukturarchitekt** als auch über die Rechte als **Softwarearchitekt** verfügen. Beide Rollen sind für den Import der Dukes Bank-Beispielanwendung sowie für die Interaktion mit den Dukes Bank-Blueprints und Softwarekomponenten erforderlich.

## Vorgehensweise

### 1 [Szenario: Importieren der vSphere-Beispielanwendung „Dukes Bank“](#)

Sie laden die vSphere-Anwendung „Dukes Bank“ von Ihrer vRealize Automation-Appliance herunter. Sie importieren die Beispielanwendung in Ihren vRealize Automation-Mandanten, um ein funktionierendes Beispiel eines vRealize Automation-Blueprints mit mehreren Ebenen anzuzeigen.

### 2 [Szenario: Konfigurieren der vSphere-Beispielkomponenten der Anwendung „Dukes Bank“ für Ihre Umgebung](#)

Mit Ihren Rechten als Infrastrukturarchitekt konfigurieren Sie die Maschinenkomponenten von Dukes Bank für die Verwendung der Anpassungsspezifikation, der Vorlage und der Maschinenpräfixe, die Sie für Ihre Umgebung erstellt haben.

Sie haben die vSphere-Beispielanwendung „Dukes Bank“ für Ihre Umgebung zur Verwendung als Ausgangspunkt für die Entwicklung Ihrer eigenen Blueprints konfiguriert, als Tool zum Bewerten von vRealize Automation oder als Schulungsressource, die Ihnen dabei hilft, die vRealize Automation-Funktionalität und -Komponenten zu verstehen.

## Szenario: Importieren der vSphere -Beispielanwendung „Dukes Bank“

Sie laden die vSphere-Anwendung „Dukes Bank“ von Ihrer vRealize Automation-Appliance herunter. Sie importieren die Beispielanwendung in Ihren vRealize Automation-Mandanten, um ein funktionierendes Beispiel eines vRealize Automation-Blueprints mit mehreren Ebenen anzuzeigen.

## Vorgehensweise

- 1 Melden Sie sich bei der vRealize Automation-Appliance als Root mit SSH an.

- 2 Laden Sie die vSphere-Beispielanwendung „Dukes Bank“ von Ihrer vRealize Automation-Appliance in das Verzeichnis /tmp herunter.

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn:5480/blueprints/DukesBankAppForvSphere.zip
```

Entzippen Sie das Paket nicht.

- 3 Laden Sie Cloud Client-Version 4.x von <http://developercenter.vmware.com/tool/cloudclient> in das Verzeichnis /tmp herunter.
- 4 Dekomprimieren Sie das Paket cloudclient-4x-dist.zip.
- 5 Führen Sie Cloud Client unter dem /bin-Verzeichnis aus.

```
$>./bin/cloudclient.sh
```

- 6 Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung.
- 7 Verwenden Sie Cloud Client, um sich bei der vRealize Automation-Appliance als Benutzer mit den Rechten als **Softwarearchitekt** und als **Infrastrukturarchitekt** anzumelden.

```
CloudClient>vra login userpass --server https://vRealize_VA_Hostname_fqdn --user <user@domain.com> --tenant <TenantName>
```

- 8 Geben Sie bei Aufforderung Ihr Anmeldekennwort ein.
- 9 Vergewissern Sie sich, dass der Inhalt von DukesBankAppForvSphere.zip verfügbar ist.

```
vra content import --path /<Pfad>/DukesBankAppForvSphere.zip --dry-run true --resolution overwrite
```

Indem Sie als Lösung „Überschreiben“ anstelle von *Überspringen* konfigurieren, gestatten Sie vRealize Automation Konflikte zu beheben, sofern möglich.

- 10 Importieren Sie die Beispielanwendung „Dukes Bank“.

```
vra content import --path /<Pfad>/DukesBankAppForvSphere.zip --dry-run false --resolution overwrite
```

Wenn Sie sich bei der vRealize Automation-Konsole als Benutzer mit den Rechten als **Softwarearchitekt** und als **Infrastrukturarchitekt** anmelden, werden Blueprints und Komponenten von Dukes Bank auf der Registerkarte **Design > Blueprints** und der Registerkarte **Design > Softwarekomponenten** angezeigt.

## Szenario: Konfigurieren der vSphere -Beispielkomponenten der Anwendung „Dukes Bank“ für Ihre Umgebung

Mit Ihren Rechten als Infrastrukturarchitekt konfigurieren Sie die Maschinenkomponenten von Dukes Bank für die Verwendung der Anpassungsspezifikation, der Vorlage und der Maschinenpräfixe, die Sie für Ihre Umgebung erstellt haben.

Dieses Szenario konfiguriert die Maschinenkomponenten zum Klonen von Maschinen von der Vorlage, die Sie im vSphere Web Client erstellt haben. Wenn Sie speichereffiziente Kopien einer virtuellen Maschine basierend auf einem Snapshot erstellen möchten, unterstützt dieselbe Anwendung auch verknüpfte Klone. Verknüpfte Klone verwenden eine Kette von Delta-Festplatten, um Unterschiede zu einer übergeordneten Maschine nachzuverfolgen, werden schnell bereitgestellt, reduzieren Speicherkosten und sind ideal geeignet, wenn die Leistung nicht am wichtigsten ist.

### Vorgehensweise

- 1 Melden Sie sich an der vRealize Automation-Konsole als **Infrastrukturarchitekt** an.

Sie können die Dukes Bank-Beispielanwendung so konfigurieren, dass sie in Ihrer Umgebung nur mit der Rolle **Infrastrukturarchitekt** funktioniert, wenn Sie jedoch die Komponenten der Beispielsoftware anzeigen oder bearbeiten möchten, müssen Sie auch über die Rolle **Softwarearchitekt** verfügen.

- 2 Wählen Sie **Design > Blueprints** aus.
- 3 Wählen Sie den **DukesBankApplication**-Blueprint aus und klicken Sie auf das Symbol **Bearbeiten**.
- 4 Bearbeiten Sie den „appserver-node“, sodass vRealize Automation diese Maschinenkomponente in Ihrer Umgebung bereitstellen kann.

Sie konfigurieren den Blueprint zum Bereitstellen mehrerer Instanzen dieser Maschinenkomponente, sodass Sie die Funktionalität des Lastausgleichsdienstknotens überprüfen können.

- a Klicken Sie auf die Komponente **appserver-node** auf der Design-Arbeitsfläche.  
Konfigurationsdetails werden im unteren Bereich angezeigt.
- b Wählen Sie das Maschinenpräfix aus dem Dropdown-Menü **Maschinenpräfix** aus.
- c Konfigurieren Sie Ihren Blueprint für die Bereitstellung von mindestens zwei und maximal zehn Instanzen dieses Knotens, indem Sie mindestens zwei und höchstens zehn Instanzen auswählen.

Im Anforderungsformular können Benutzer mindestens zwei und bis zu zehn appserver-Knoten bereitstellen. Wenn Benutzer über die Berechtigung für die Aktionen zur vertikalen oder horizontalen Skalierung verfügen, können sie ihre Bereitstellung skalieren, um geänderten Anforderungen gerecht zu werden.

- d Klicken Sie auf die Registerkarte **Build-Informationen**.
- e Wählen Sie **CloneWorkflow** aus dem Dropdown-Menü **Bereitstellungsworkflow** aus.
- f Wählen Sie **dukes\_bank\_template** aus dem Dialogfeld **Klonen von** aus.
- g Geben Sie **Customspecs\_sample** in das Textfeld **Anpassungsspezifikation** ein.  
Bei diesem Feld ist die Groß-/Kleinschreibung zu beachten.
- h Klicken Sie auf die Registerkarte **Maschinenressourcen**.
- i Stellen Sie sicher, dass die Speichereinstellungen auf mindestens 2048 MB festgelegt sind.



- 5 Bearbeiten Sie den Lastausgleichsdienst-Knoten, sodass vRealize Automation diese Maschinenkomponente in Ihrer Umgebung bereitstellen kann.
  - a Klicken Sie auf die **Lastausgleichsdienst-Knoten**-Komponente in der Design-Arbeitsfläche.
  - b Wählen Sie das Maschinenpräfix aus dem Dropdown-Menü **Maschinenpräfix** aus.
  - c Klicken Sie auf die Registerkarte **Build-Informationen**.
  - d Wählen Sie **CloneWorkflow** aus dem Dropdown-Menü **Bereitstellungsworkflow** aus.
  - e Wählen Sie **dukes\_bank\_template** aus dem Dialogfeld **Klonen von** aus.
  - f Geben Sie **Customspecs\_sample** in das Textfeld **Anpassungsspezifikation** ein.  
Bei diesem Feld ist die Groß-/Kleinschreibung zu beachten.
  - g Klicken Sie auf die Registerkarte **Maschinenressourcen**.
  - h Stellen Sie sicher, dass die Speichereinstellungen auf mindestens 2048 MB festgelegt sind.
- 6 Wiederholen Sie diesen Vorgang für die Maschinenkomponente **database-node**.
- 7 Klicken Sie auf **Speichern und beenden**.  
Ihre Änderungen werden gespeichert, und Sie werden zur Registerkarte **Blueprints** zurückgeleitet.
- 8 Wählen Sie den **DukesBankApplication**-Blueprint aus und klicken Sie auf **Veröffentlichen**.

Sie haben den Dukes Bank-Beispielanwendungs-Blueprint für Ihre Umgebung konfiguriert und den fertiggestellten Blueprint veröffentlicht.

#### Weiter

Veröffentliche Blueprints werden erst dann Benutzern im Katalog angezeigt, wenn Sie einen Katalogdienst konfigurieren, den Blueprint zu einem Dienst hinzufügen und Benutzern die Berechtigung erteilen, Ihren Blueprint anzufordern. Siehe [Checkliste für die Konfiguration des Servicekatalogs](#).

Nachdem Sie Ihren Dukes Bank-Blueprint zum Anzeigen im Katalog konfiguriert haben, können Sie die Bereitstellung der Beispielanwendung anfordern. Siehe [Szenario: Testen der Beispielanwendung „Dukes Bank“](#).

## Szenario: Testen der Beispielanwendung „Dukes Bank“

Sie fordern das Dukes Bank-Katalogelement an und melden sich bei der Beispielanwendung an, um Ihre Arbeit zu überprüfen und vRealize Automation-Blueprint-Funktionalität anzuzeigen.

#### Voraussetzungen

- Importieren Sie die Beispielanwendung „Dukes Bank“ und konfigurieren Sie die Blueprint-Komponenten für Ihre Umgebung. Siehe [Szenario: Importieren der vSphere-Beispielanwendung „Dukes Bank“ und Konfigurieren für Ihre Umgebung](#).

- Konfigurieren Sie den Servicekatalog und stellen Sie Ihren veröffentlichten Dukes Bank-Blueprint bereit, damit Benutzer ihn anfordern können. Siehe [Checkliste für die Konfiguration des Servicekatalogs](#).
- Stellen Sie sicher, dass von Ihnen bereitgestellte virtuelle Maschinen das YUM-Repository erreichen.

### Vorgehensweise

- 1 Melden Sie sich bei der vRealize Automation-Konsole als Benutzer mit Berechtigung für das Katalogelement „Dukes Bank“ an.
- 2 Klicken Sie auf die Registerkarte **Katalog**.
- 3 Suchen Sie das Beispielanwendungs-Katalogelement „Dukes Bank“ und klicken Sie auf **Anfordern**.
- 4 Geben Sie die erforderlichen Anforderungsdetails für jede mit einem Sternchen gekennzeichnete Komponente ein.
  - a Navigieren Sie zur Komponente „JBossAppServer“, um die erforderlichen Anforderungsdetails einzugeben.
  - b Geben Sie im Textfeld **app\_content\_server\_ip** den vollqualifizierten Domännennamen Ihrer vRealize Automation-Appliance ein.
  - c Navigieren Sie zu den Dukes\_Bank\_App-Softwarekomponenten, um die erforderlichen Anforderungsdetails einzugeben.
  - d Geben Sie in den **app\_content\_server\_ip**-Textfeldern den vollqualifizierten Domännennamen Ihrer vRealize Automation-Appliance ein.
- 5 Klicken Sie auf **Übernehmen**.
 

In Abhängigkeit von Ihrem Netzwerk und Ihrer vCenter Server-Instanz kann die vollständige Bereitstellung der Beispielanwendung „Dukes Bank“ etwa 15 bis 20 Minuten dauern. Auf der Registerkarte **Anforderungen** können Sie den Status überwachen, und nach der Bereitstellung der Anwendung können Sie auf der Registerkarte **Elemente** die Katalogelementdetails anzeigen.
- 6 Suchen Sie nach der Bereitstellung der Anwendung die IP-Adresse des Lastausgleichsservers, damit Sie auf die Beispielanwendung „Dukes Bank“ zugreifen können.
  - a Wählen Sie **Elemente > Bereitstellungen** aus.
  - b Erweitern Sie die Bereitstellung Ihrer Beispielanwendung „Dukes Bank“ und wählen Sie den Apache-Lastausgleichsserver aus.
  - c Klicken Sie auf **Details anzeigen**.
  - d Wählen Sie die Registerkarte **Netzwerk** aus.
  - e Notieren Sie sich die IP-Adresse.

**7** Melden Sie sich bei der Beispielanwendung „Dukes Bank“ an.

- a Navigieren Sie zu Ihrem Lastausgleichsdienstserver unter `http://IP_Apache_Load_Balancer:8081/bank/main.faces`.

Wenn Sie direkt auf die Anwendungsserver zugreifen möchten, können Sie zu `http://IP_AppServer:8080/bank/main.faces` navigieren.

- b Geben Sie **200** im Textfeld **Benutzername** ein.
- c Geben Sie **foobar** im Textfeld **Kennwort** ein.

Sie verfügen über eine funktionierende Beispielanwendung „Dukes Bank“ als Ausgangspunkt für die Entwicklung Ihrer eigenen Blueprints, als Tool zum Bewerten von vRealize Automation oder als Schulungsressource, die Ihnen dabei hilft, die vRealize Automation-Funktionalität und -Komponenten zu verstehen.

## Erstellen Ihrer Design-Bibliothek

Sie können eine Bibliothek mit wiederverwendbaren Blueprint-Komponenten erstellen, die Ihre Architekten zu Anwendungs-Blueprints zusammenfügen können, um Ihren Benutzern ausgefeilte On-Demand-Dienste bereitzustellen.

Erstellen Sie anhand kleinster Blueprint-Designkomponenten (einzelne Maschinen-Blueprints, Software-Komponenten und XaaS-Blueprints) eine Bibliothek, kombinieren Sie diese Grundbausteine auf neue und andere Weise und schaffen Sie aufwendige Katalogelemente, die Ihren Benutzern einen höheren Funktionsumfang bieten.

Tabelle 4-2. Erstellen Ihrer Design-Bibliothek

Katalogelement	Rolle	Komponenten	Beschreibung	Details
Maschinen	Infrastrukturarchitekt	Erstellen Sie Maschinen-Blueprints auf der Registerkarte <b>Blueprints</b> .	<p>Sie können Maschinen-Blueprints erstellen, um Ihren Benutzern virtuelle private und öffentliche bzw. Hybrid-Cloud-Maschinen schnell bereitzustellen.</p> <p>Veröffentlichte Maschinen-Blueprints sind für Katalog-Administratoren zur Aufnahme in den Katalog als eigenständige Blueprints verfügbar. Sie können jedoch auch Maschinen-Blueprints mit anderen Komponenten kombinieren, um ausgefeiltere Katalogelemente zu erstellen, die mehrere Maschinen-Blueprints, Software- oder XaaS-Blueprints enthalten.</p>	<a href="#">Konfigurieren eines Maschinen-Blueprints</a>
NSX-Netzwerk und Sicherheit auf Maschinen	Infrastrukturarchitekt	Fügen Sie NSX-Netzwerk- und Sicherheitskomponenten zu vSphere-Maschinen-Blueprints auf der Registerkarte <b>Blueprints</b> hinzu.	<p>Sie können Netzwerk- und Sicherheitskomponenten, wie z. B. Netzwerkprofile und Sicherheitsgruppen, so konfigurieren, dass virtuelle Maschinen über physische und virtuelle Netzwerke sicher und effizient miteinander kommunizieren können.</p> <p>Sie müssen Netzwerk- und Sicherheitskomponenten mit mindestens einer vSphere-Maschine kombinieren, bevor Katalog-Administratoren sie in den Katalog aufnehmen können. Sie können nur NSX-Netzwerk- und Sicherheitskomponenten auf vSphere-Maschinen-Blueprints anwenden.</p>	<a href="#">Entwerfen von Maschinen-Blueprints mit NSX-Netzwerk und -Sicherheit</a>
Software auf Maschinen	Softwarearchitekt	Erstellen und veröffentlichen Sie Software-Komponenten auf der Registerkarte <b>Software</b> . Kombinieren Sie diese anschließend mit Maschinen-Blueprints auf der Registerkarte <b>Blueprints</b> .	<p>Fügen Sie zu Ihren Maschinen-Blueprints Software-Komponenten hinzu, um komplexe Anwendungen in Cloud-Umgebungen zu standardisieren, bereitzustellen, zu konfigurieren, zu aktualisieren und zu skalieren. Diese Anwendungen können von einfachen Webanwendungen bis hin zu ausgefeilten benutzerdefinierten Anwendungen und Anwendungspaketen reichen.</p> <p>Software-Komponenten können im Katalog nicht alleine angezeigt werden. Sie müssen Ihre Software-Komponenten erstellen und veröffentlichen und anschließend einen Anwendungs-Blueprint zusammenfügen, der mindestens eine Maschine enthält.</p>	<a href="#">Erstellen einer Software-Komponente</a>

**Tabelle 4-2. Erstellen Ihrer Design-Bibliothek (Fortsetzung)**

Katalogelement	Rolle	Komponenten	Beschreibung	Details
Benutzerdefinierte IT-Dienste	XaaS-Architekten	Erstellen und veröffentlichen Sie XaaS-Blueprints auf der Registerkarte <b>XaaS</b> .	Sie können XaaS-Katalogelemente erstellen, die über die vRealize Automation-Funktionalität von Maschinen, Netzwerken, Sicherheit und Bereitstellung von Softwares hinausgehen. Wenn Sie vorhandene vRealize Orchestrator-Workflows und Plug-Ins bzw. benutzerdefinierte, in vRealize Orchestrator entwickelte Skripts verwenden, können Sie die Bereitstellung aller IT-Dienste automatisieren.  Veröffentlichte XaaS-Blueprints sind für Katalog-Administratoren zur Aufnahme in den Katalog als eigenständige Blueprints verfügbar. Sie können jedoch auch Maschinen mit anderen Komponenten auf der Registerkarte <b>Blueprints</b> kombinieren, um ausgefeiltere Katalogelemente zu erstellen.	<a href="#">Erstellen von XaaS-Blueprints und -Ressourcenaktionen</a>
Zusammenfügen von veröffentlichten Blueprint-Bauteilen in neuen Katalogelementen	<ul style="list-style-type: none"> <li>■ Anwendungsarchitekt</li> <li>■ Infrastrukturarchitekt</li> <li>■ Softwarearchitekt</li> </ul>	Kombinieren Sie auf der Registerkarte <b>Blueprints</b> zusätzliche Maschinen-Blueprints, XaaS-Blueprints und Software-Komponenten mit mindestens einer Maschinenkomponente oder Maschinen-Blueprint.	Sie können veröffentlichte Komponenten und Blueprints wiederverwenden und in neuer Art und Weise kombinieren, um IT-Dienst-Pakete zu erstellen, über die Ihren Benutzern ausgefeilte Funktionen bereitgestellt werden.	<a href="#">Erstellen zusammengesetzter Blueprints</a>

## Entwerfen von Maschinen-Blueprints

Maschinen-Blueprints sind die vollständige Spezifikation für eine Maschine und bestimmen die Attribute einer Maschine, die Art und Weise der Bereitstellung sowie die Richtlinien- und Verwaltungseinstellungen. In Abhängigkeit von der Komplexität des Katalogelements, das Sie erstellen, können Sie eine oder mehrere Maschinenkomponenten im Blueprint mit anderen Komponenten in der Design-Arbeitsfläche kombinieren. Auf diese Weise können Sie ausgefeiltere Katalogelemente erstellen, die Netzwerk- und Sicherheitskomponenten, Software-Komponenten, XaaS-Komponenten und sonstige Blueprint-Komponenten enthalten.

## Platzsparende Speicher für die virtuelle Bereitstellung

Die speichereffiziente Speichertechnologie behebt die Ineffizienz traditioneller Speichermethoden, indem nur der Speicher verwendet wird, der tatsächlich für die Vorgänge einer Maschine erforderlich ist. Dies ist normalerweise nur ein Bruchteil des Speichers, der Maschinen tatsächlich zugewiesen ist.

vRealize Automation unterstützt zwei Methoden der Bereitstellung mit speichereffizienter Technologie: Thin Provisioning und FlexClone-Bereitstellung.

Bei Verwendung des Standardspeichers wird der einer bereitgestellten Maschine zugewiesene Speicher vollständig dieser Maschine zugesichert, selbst wenn sie ausgeschaltet ist. Dies kann eine beträchtliche Verschwendung von Speicherressourcen bedeuten, da wenige virtuelle Maschinen den gesamten ihnen zugewiesenen Speicher tatsächlich verwenden, genau so, wie wenige physische Maschinen mit einer vollständigen Festplattenkapazität von 100 % betrieben werden. Wenn eine speichereffiziente Speichertechnologie verwendet wird, werden der zugewiesene Speicher und der verwendete Speicher einzeln verfolgt, und nur der verwendete Speicher wird der bereitgestellten Maschine vollständig zugesichert.

### Thin Provisioning

Thin Provisioning wird für alle virtuellen Bereitstellungsmethoden unterstützt. Je nach Virtualisierungsplattform, Speichertyp und Standardspeicherkonfiguration wird Thin Provisioning bei der Maschinenbereitstellung möglicherweise immer verwendet. Beispielsweise wird für vSphere ESX-Server-Integrationen unter Verwendung des NFS-Speichers Thin Provisioning immer verwendet. Jedoch wird für vSphere ESX-Server-Integrationen, die einen lokalen oder iSCSI-Speicher verwenden, Thin Provisioning nur für die Bereitstellung von Maschinen verwendet, wenn die benutzerdefinierte Eigenschaft `VirtualMachine.Admin.ThinProvision` im Blueprint angegeben ist. Weitere Informationen über Thin Provisioning finden Sie in der von der Virtualisierungsplattform bereitgestellten Dokumentation.

### Net App FlexClone -Bereitstellung

Sie können einen Blueprint für die Net App FlexClone-Bereitstellung erstellen, wenn Sie in einer vSphere-Umgebung arbeiten, die einen NFS-Speicher (Network File System) und FlexClone-Technologie verwendet.

Sie können nur den NFS-Speicher verwenden, da sonst die Maschinenbereitstellung fehlschlägt. Sie können einen FlexClone-Speicherpfad für andere Typen der Maschinenbereitstellung angeben, aber der FlexClone-Speicherpfad verhält sich wie der Standardspeicher.

Das Folgende ist ein allgemeiner Überblick über die Abfolge der Schritte, die für die Bereitstellung von Maschinen erforderlich sind, die die FlexClone-Technologie verwenden:

- 1 Ein IaaS-Administrator erstellt einen NetApp ONTAP-Endpoint. Siehe [Erstellen eines NetApp ONTAP-Endpoints](#).
- 2 Ein IaaS-Administrator führt eine Datenerfassung auf dem Endpoint aus, damit der Endpoint auf der Computing-Ressource und den Reservierungsseiten angezeigt werden kann.

Die FlexClone-Option wird auf einer Reservierungsseite in der Endpoint-Spalte angezeigt, wenn ein NetApp ONTAP-Endpoint vorhanden und der Host virtuell ist. Wenn ein NetApp ONTAP-Endpoint vorhanden ist, wird auf der Reservierungsseite der dem Speicherpfad zugewiesene Endpoint angezeigt.

- 3 Ein Fabric-Administrator erstellt eine vSphere-Reservierung, aktiviert den FlexClone-Speicher und gibt einen NFS-Speicherpfad an, der FlexClone-Technologie verwendet.
- 4 Ein Infrastrukturarchitekt oder ein anderer autorisierter Benutzer erstellt einen Blueprint für die FlexClone-Bereitstellung.

## Konfigurieren eines Maschinen-Blueprints

Konfigurieren und veröffentlichen Sie eine Maschinenkomponente als eigenständigen Blueprint, den andere Architekten als Komponente in Anwendungs-Blueprints wiederverwenden und Katalog-Administratoren in Katalogdienste einbeziehen können.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Infrastrukturarchitekt** an.
- Schließen Sie die externen Vorbereitungen für die Bereitstellung ab, wie beispielsweise das Erstellen von Vorlagen, WinPEs und ISOs, oder erfassen Sie die Informationen zu externen Vorbereitungen von Ihren Administratoren.
- Konfigurieren Sie Ihren Mandanten. [Kapitel 2 Konfigurieren der Mandanteneinstellungen](#).
- Konfigurieren Sie Ihre IaaS-Ressourcen. [Checkliste für die Konfiguration von IaaS-Ressourcen](#).
- Siehe *Konfigurieren von vRealize Automation*.

### Vorgehensweise

- 1 Wählen Sie **Design > Blueprints** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Folgen Sie den Anweisungen im Dialogfeld **Neuer Blueprint** zum Konfigurieren allgemeiner Einstellungen.
- 4 Klicken Sie auf **OK**.
- 5 Klicken Sie im Bereich „Kategorien“ auf **Maschinentypen**, um eine Liste der verfügbaren Maschinentypen anzuzeigen.
- 6 Ziehen Sie den Maschinentyp, den Sie bereitstellen möchten, auf die Design-Arbeitsfläche.
- 7 Folgen Sie den Anweisungen auf den verschiedenen Registerkarten zum Konfigurieren der Details zur Maschinenbereitstellung.
- 8 Klicken Sie auf **Beenden**.
- 9 Wählen Sie Ihren Blueprint aus und klicken Sie auf **Veröffentlichen**.

Sie haben eine Maschinenkomponente als eigenständigen Blueprint konfiguriert und veröffentlicht. Katalog-Administratoren können diesen Maschinen-Blueprint in Katalogdienste einbeziehen und Benutzern die Berechtigung zum Anfordern dieses Blueprints erteilen. Andere Architekten können diesen Maschinen-Blueprint wiederverwenden, um ausgefeiltere Anwendungs-Blueprints zu erstellen, die Softwarekomponenten, XaaS-Blueprints oder zusätzliche Maschinen-Blueprints enthalten.

## Weiter

Sie können einen Maschinen-Blueprint mit Softwarekomponenten, XaaS-Blueprints oder zusätzlichen Maschinen-Blueprints kombinieren, um ausgefeiltere Anwendungs-Blueprints zu erstellen. Siehe [Erstellen zusammengesetzter Blueprints](#).

## Einstellungen für Maschinen-Blueprints

Machen Sie sich mit den Einstellungen und Optionen vertraut, die Sie beim Erstellen von Maschinen-Blueprints konfigurieren können.

### Neue Blueprint- und Blueprint-Eigenschaften-Einstellungen

Machen Sie sich mit den Einstellungen und Optionen vertraut, die Sie im Dialogfeld „Neuer Blueprint“ konfigurieren können. Nach dem Erstellen des Blueprints können Sie diese Eigenschaften im Dialogfeld „Blueprint-Eigenschaften“ bearbeiten.

### Registerkarte Allgemein

Wenden Sie Einstellungen auf den gesamten Blueprint an, einschließlich aller Komponenten, die Sie jetzt oder später hinzufügen möchten.

**Tabelle 4-3. Einstellungen auf der Registerkarte Allgemein**

Einstellung	Beschreibung
<b>Name</b>	Geben Sie einen Namen für Ihren Blueprint ein.
<b>Bezeichner</b>	Das Feld „Bezeichner“ wird automatisch basierend auf dem von Ihnen eingegebenen Namen aufgefüllt. Sie können dieses Feld jetzt bearbeiten, aber nach der Speicherung des Blueprints kann es nicht mehr geändert werden. Bezeichner sind innerhalb Ihres Mandanten permanent und eindeutig, weshalb Sie damit programmgesteuert mit Blueprints interagieren und Eigenschaftsbindungen erstellen können.
<b>Beschreibung</b>	Eine Zusammenfassung Ihres Blueprints für andere Architekten. Diese Beschreibung wird Benutzern auch im Anforderungsformular angezeigt.
<b>Archivierung (Tage)</b>	Sie können einen Archivierungszeitraum für die vorübergehende Speicherung von Bereitstellungen angeben, anstatt Bereitstellungen unmittelbar nach Ablauf der Lease zu löschen. Geben Sie 0 (Standardwert) an, um die Bereitstellung bei Ablauf der Lease zu löschen. Der Archivierungszeitraum beginnt am Tag des Ablaufs der Lease. Wenn der Archivierungszeitraum endet, wird die Bereitstellung gelöscht.
<b>Leasetage: Mindestwert und Maximalwert</b>	Geben Sie einen Mindestwert und einen Maximalwert ein, damit Benutzer eine Leasedauer in diesem Bereich auswählen können. Wenn die Lease endet, wird die Bereitstellung entweder gelöscht oder archiviert.



## Registerkarte NSX-Einstellungen

Wenn Sie VMware NSX konfiguriert und das NSX-Plug-In für vRealize Automation installiert haben, können Sie beim Erstellen oder Bearbeiten eines Blueprints Einstellungen für NSX-Transportzonen, Reservierungsrichtlinien für die Edge und das geroutete Gateway sowie Anwendungsisolierungen angeben. Diese Einstellungen sind auf der Registerkarte **NSX-Einstellungen** auf den Seiten **Neuer Blueprint** und **Blueprint-Eigenschaften** verfügbar.

Informationen zu NSX-Einstellungen finden Sie unter [Neue Blueprint- und Blueprint-Eigenschaften-Einstellungen mit NSX](#).

## Registerkarte Eigenschaften

Benutzerdefinierte Eigenschaften, die Sie auf der Blueprint-Ebene hinzufügen, gelten für den gesamten Blueprint, einschließlich aller Komponenten. Sie können jedoch durch benutzerdefinierte Eigenschaften außer Kraft gesetzt werden, die zu einem späteren Zeitpunkt in der Rangfolge zugewiesen werden. Weitere Informationen zur Rangfolge für benutzerdefinierte Eigenschaften finden Sie unter *Referenz für benutzerdefinierte Eigenschaften*.

**Tabelle 4-4. Einstellungen auf der Registerkarte Eigenschaften**

Registerkarte	Einstellung	Beschreibung
<b>Eigenschaftsgruppen</b>		Eigenschaftsgruppen sind wiederverwendbare Gruppen von Eigenschaften, mit denen das Hinzufügen benutzerdefinierter Eigenschaften zu Blueprints vereinfacht werden soll. Ihre Mandantenadministratoren und Fabric-Administratoren können Eigenschaften, die häufig gemeinsam verwendet werden, gruppieren, damit die Eigenschaftsgruppe einem Blueprint hinzugefügt werden kann, anstatt benutzerdefinierte Eigenschaften einzeln einzufügen.
	<b>Nach oben verschieben/Nach unten verschieben</b>	Kontrollieren Sie die Rangfolge aller Eigenschaftsgruppen zueinander durch die Priorisierung der Gruppen. Die erste Gruppe in der Liste hat die höchste Priorität, und deren benutzerdefinierte Eigenschaften haben absoluten Vorrang. Sie können die Elemente auch per Drag & Drop neu anordnen.
	<b>Eigenschaften anzeigen</b>	Zeigen Sie die benutzerdefinierten Eigenschaften in der ausgewählten Eigenschaftsgruppe an.
	<b>Zusammengeführte Eigenschaften anzeigen</b>	Wenn eine benutzerdefinierte Eigenschaft in mehreren Eigenschaftsgruppen vorhanden ist, hat der Wert in der Eigenschaftsgruppe mit der höchsten Priorität den Vorrang. Sie können diese zusammengeführten Eigenschaften anzeigen, um die Priorisierung von Eigenschaftsgruppen zu unterstützen.
<b>Benutzerdefinierte Eigenschaften</b>		Anstelle von Eigenschaftsgruppen können Sie auch einzelne benutzerdefinierte Eigenschaften hinzufügen.
	<b>Name</b>	Eine Aufstellung der Namen und Verhaltensweisen benutzerdefinierter Eigenschaften finden Sie unter <i>Referenz für benutzerdefinierte Eigenschaften</i> .

**Tabelle 4-4. Einstellungen auf der Registerkarte *Eigenschaften* (Fortsetzung)**

Registerkarte	Einstellung	Beschreibung
	<b>Wert</b>	Geben Sie den Wert für die benutzerdefinierte Eigenschaft ein.
	<b>Verschlüsselt</b>	Sie können den Eigenschaftswert verschlüsseln. Beispielsweise für den Fall, dass es sich bei dem Wert um ein Kennwort handelt.
	<b>Überschreibbar</b>	Sie können festlegen, dass der Eigenschaftswert von der nächsten Person, die die Eigenschaft verwendet, oder der nachfolgenden Person überschrieben werden darf. In der Regel handelt es sich bei dieser Person um einen anderen Architekten. Wenn Sie jedoch „In Anforderung anzeigen“ auswählen, können Ihre Unternehmensbenutzer Eigenschaftswerte anzeigen oder bearbeiten, wenn sie Katalogelemente anfordern.
	<b>In Anforderung anzeigen</b>	Wenn Sie Ihren Endbenutzern den Namen und den Wert der Eigenschaft anzeigen möchten, können Sie festlegen, dass beim Anfordern einer Maschinenbereitstellung die Eigenschaft im Anforderungsformular angezeigt wird. Sie müssen „Überschreibbar“ auch auswählen, wenn die Benutzer einen Wert eingeben können sollen.

## vSphere -Maschinenkomponenteneinstellungen

Machen Sie sich mit den Einstellungen und Optionen vertraut, die Sie für eine vSphere-Maschinenkomponente in der vRealize Automation-Blueprint-Design-Arbeitsfläche konfigurieren können. vSphere ist der einzige Maschinenkomponententyp, der NSX-Netzwerk- und Sicherheitskomponenteneinstellungen in der Design-Arbeitsfläche verwenden kann.

### Registerkarte **Allgemein**

Konfigurieren Sie die allgemeinen Einstellungen für eine vSphere-Maschinenkomponente.

**Tabelle 4-5. Einstellungen auf der Registerkarte *Allgemein***

Einstellung	Beschreibung
<b>ID</b>	Geben Sie einen Namen für Ihre Maschinenkomponente ein oder übernehmen Sie den Standardwert.
<b>Beschreibung</b>	Eine Zusammenfassung Ihrer Maschinenkomponente für andere Architekten.

**Tabelle 4-5. Einstellungen auf der Registerkarte Allgemein (Fortsetzung)**

Einstellung	Beschreibung
<b>Speicherort auf Anforderung anzeigen</b>	<p>In einer Cloud-Umgebung wie vCloud Air wird Benutzern auf diese Weise ermöglicht, eine Region für ihre bereitgestellten Maschinen auszuwählen.</p> <p>Für eine virtuelle Umgebung wie beispielsweise vSphere können Sie die Standorte-Funktion so konfigurieren, dass den Benutzern die Auswahl eines bestimmten Datacenter-Standorts, an dem eine angeforderte Maschine bereitgestellt werden soll, erlaubt wird. Für die vollständige Konfiguration dieser Option fügt ein Systemadministrator Informationen zum Datacenter-Standort zu einer Standortdatei hinzu und ein Fabric-Administrator bearbeitet eine Computing-Ressource, um sie einem Standort zuzuordnen.</p>
<b>Reservierungsrichtlinie</b>	<p>Anwenden einer Reservierungsrichtlinie auf einen Blueprint, um die von diesem Blueprint bereitgestellten Maschinen auf eine Teilmenge der verfügbaren Reservierungen einzuschränken. Fabric-Administratoren erstellen Reservierungsrichtlinien, um eine optionale und hilfreiche Methode zur Kontrolle der Verarbeitung von Reservierungsanforderungen bereitzustellen. Beispielsweise, um Ressourcen in Gruppen für unterschiedliche Service-Level zu erfassen oder um einen bestimmten Ressourcentyp für einen bestimmten Verwendungszweck zur Verfügung zu stellen. Wenn Ihr Fabric-Administrator keine Reservierungsrichtlinien konfiguriert hat, werden in diesem Dropdown-Menü keine verfügbaren Optionen angezeigt.</p>
<b>Maschinenpräfix</b>	<p>Maschinenpräfixe werden von Fabric-Administratoren erstellt und zum Erstellen der Namen von bereitgestellten Maschinen verwendet. Wenn Sie <b>Gruppenstandardwert verwenden</b> auswählen, werden über Ihren Blueprint bereitgestellte Maschinen gemäß dem Maschinenpräfix benannt, das als Standardwert für die Business-Gruppe des Benutzers konfiguriert ist. Falls kein Maschinenpräfix konfiguriert wurde, wird für Sie eines auf der Grundlage der Business-Gruppe generiert.</p> <p>Wenn Ihr Fabric-Administrator andere Maschinenpräfixe zu Ihrer Auswahl konfiguriert, können Sie ein Präfix auf alle Maschinen anwenden, die über Ihren Blueprint bereitgestellt werden, und zwar unabhängig vom Anforderer.</p>
<b>Instanzen: Mindestwert und Maximalwert</b>	<p>Konfigurieren Sie die minimale oder maximale Anzahl an Instanzen, die Benutzer für eine Bereitstellung oder für eine vertikale oder horizontale Skalierungsaktion anfordern können. Wenn Benutzern keine Auswahlmöglichkeit eingeräumt werden soll, wird durch Eingabe desselben Werts in den Feldern <b>Minimalwert</b> und <b>Maximalwert</b> die genaue Anzahl der bereitzustellenden Instanzen festgelegt und die Skalierungsaktionen für diese Maschinenkomponente werden deaktiviert.</p> <p>XaaS-Komponenten sind nicht skalierbar und werden bei einem Skalierungsvorgang nicht aktualisiert. Wenn Sie XaaS-Komponenten in Ihrem Blueprint verwenden, könnten Sie eine Ressourcenaktion erstellen, die Benutzer nach einem Skalierungsvorgang ausführen können, um Ihre XaaS-Komponenten zu skalieren oder aktualisieren. Alternativ könnten Sie die Skalierung deaktivieren, indem Sie genau die Anzahl von Instanzen konfigurieren, die Sie für jede Maschinenkomponente zulassen möchten.</p>

## Registerkarte Build-Informationen

Konfigurieren Sie Einstellungen für Build-Informationen für eine vSphere-Maschinenkomponente.

**Tabelle 4-6. Registerkarte Build-Informationen**

Einstellung	Beschreibung
<b>Blueprint-Typ</b>	Wählen Sie zu Statistik- und Lizenzierungszwecken aus, ob über diesen Blueprint bereitgestellte Maschinen als „Desktop“ oder „Server“ klassifiziert werden.
<b>Aktion</b>	<p>Die im Dropdown-Menü „Aktion“ angezeigten Optionen hängen vom ausgewählten Maschinentyp ab.</p> <p>Die folgenden Aktionen sind verfügbar:</p> <ul style="list-style-type: none"> <li>■ Erstellen <p>Erstellt die Spezifikation der Maschinenkomponente ohne die Verwendung einer Klon-Option.</p> </li> <li>■ Klonen <p>Erstellt Kopien einer virtuellen Maschine anhand einer Vorlage und eines Anpassungsobjekts.</p> </li> <li>■ LinkedClone <p>Stellen Sie eine speichereffiziente Kopie einer virtuellen Maschine bereit, einen so genannten verknüpften Klon. Verknüpfte Klone basieren auf einem Snapshot einer VM und verwenden eine Kette von Delta-Datenträgern zum Nachverfolgen von Unterschieden von einer übergeordneten Maschine.</p> </li> <li>■ NetAppFlexClone <p>Wenn Ihre Fabric-Administratoren für ihre Reservierungen die Verwendung von NetApp FlexClone-Speicher konfiguriert haben, können Sie mithilfe dieser Technologie platzsparende Kopien von Maschinen klonen.</p> </li> </ul>

Tabelle 4-6. Registerkarte **Build-Informationen** (Fortsetzung)

Einstellung	Beschreibung
<b>Bereitstellungsworkflow</b>	<p data-bbox="810 264 1406 354">Die im Dropdown-Menü „Bereitstellungsworkflow“ angezeigten Optionen hängen vom ausgewählten Maschinentyp und der ausgewählten Aktion ab.</p> <ul style="list-style-type: none"> <li data-bbox="810 367 1038 394">■ <b>BasicVmWorkflow</b> <p data-bbox="847 415 1358 443">Stellt eine Maschine ohne Gastbetriebssystem bereit.</p> </li> <li data-bbox="810 453 1161 480">■ <b>ExternalProvisioningWorkflow</b> <p data-bbox="847 501 1406 558">Erstellt eine Maschine durch Starten über eine VM-Instanz oder ein Cloud-basiertes Image.</p> </li> <li data-bbox="810 569 1098 596">■ <b>LinuxKickstartWorkflow</b> <p data-bbox="847 617 1406 768">Stellen Sie eine Maschine durch Starten von einem ISO-Image bereit. Verwenden Sie dabei eine Kickstart- oder AutoYaST-Konfigurationsdatei und ein Linux-Distributions-Image zum Installieren des Betriebssystems auf der Maschine.</p> </li> <li data-bbox="810 779 1201 806">■ <b>VirtualSccmProvisioningWorkflow</b> <p data-bbox="847 827 1406 978">Stellen Sie eine Maschine bereit und geben Sie die Steuerung an eine SCCM-Aufgabensequenz zum Starten von einem ISO-Image weiter, stellen Sie ein Windows-Betriebssystem bereit und installieren Sie den vRealize Automation-Gast-Agent.</p> </li> <li data-bbox="810 989 1054 1016">■ <b>WIMImageWorkflow</b> <p data-bbox="847 1037 1406 1188">Stellen Sie eine Maschine durch Starten in eine WinPE-Umgebung bereit und durch Installieren eines Betriebssystems unter Verwendung eines WIM-Images (Windows Imaging Format) einer vorhandenen Windows-Referenzmaschine.</p> <p data-bbox="810 1199 1406 1419">Wenn Sie in einem Blueprint einen WIM-Bereitstellungsworkflow verwenden, geben Sie einen Speicherwert an, der die Größe jeder Festplatte berücksichtigt, die auf der Maschine verwendet werden soll. Verwenden Sie den Gesamtwert aller Festplatten als Mindestspeicherwert für die Maschinenkomponente. Geben Sie zudem für jede Festplatte eine Größe an, die für das Betriebssystem ausreicht.</p> </li> </ul>
<b>Klonen von</b>	<p data-bbox="810 1440 1406 1497">Wählen Sie für Klonen oder NetApp FlexClone eine zu klonende Maschinenvorlage aus.</p> <p data-bbox="810 1507 1406 1629">Wählen Sie für verknüpfte Klone eine Maschine aus der Liste der Maschinen aus. Es werden Ihnen nur Maschinen mit verfügbaren klonbaren Snapshots angezeigt, die Sie als Mandantenadministrator oder Business-Gruppenmanager verwalten.</p> <p data-bbox="810 1640 1406 1730">Sie können nur von Vorlagen klonen, die auf Maschinen vorhanden sind, die Sie als Business-Gruppenmanager oder Mandantenadministrator verwalten.</p>

**Tabelle 4-6. Registerkarte Build-Informationen (Fortsetzung)**

Einstellung	Beschreibung
Von Snapshot klonen	<p>Wählen Sie für verknüpfte Klone einen vorhandenen zu klonenden Snapshot aus, basierend auf der ausgewählten Maschinenvorlage. In der Liste werden nur Maschinen angezeigt, für die bereits ein Snapshot vorhanden ist und die Sie als Mandantenadministrator oder Business-Gruppenmanager verwalten.</p> <p>Wenn Sie <b>Aktuellen Snapshot verwenden</b> auswählen, wird der Klon mit den Merkmalen des aktuellsten Zustands der virtuellen Maschine definiert. Wenn Sie stattdessen basierend auf einem tatsächlichen Snapshot klonen möchten, klicken Sie auf die Dropdown-Menüoption und wählen Sie den betreffenden Snapshot aus der Liste aus.</p> <p>Diese Option ist für die Aktion „Verknüpfter Klon“ verfügbar.</p>
Anpassungsspezifikation	<p>Angabe einer verfügbaren Anpassungsspezifikation aus. Eine Anpassungsspezifikation ist nur dann erforderlich, wenn Sie mit statischen IP-Adressen klonen.</p> <p>Sie können eine Anpassung von Windows-Maschinen nicht ohne Anpassungsspezifikation durchführen. Bei Linux-Klonmaschinen können Sie eine Anpassungsspezifikation und/oder ein externes Skript zum Durchführen von Anpassungen verwenden.</p>

**Registerkarte Maschinenressourcen**

Geben Sie die Einstellungen für CPU, Arbeitsspeicher und Speicher für die vSphere-Maschinenkomponente an.

**Tabelle 4-7. Registerkarte Maschinenressourcen**

Einstellung	Beschreibung
<b>CPUs: Mindestwert und Maximalwert</b>	Geben Sie eine Mindest- und eine Maximalanzahl an CPUs ein, die durch diese Maschinenkomponente bereitgestellt werden können.
<b>Arbeitsspeicher (MB): Mindestwert und Maximalwert</b>	Geben Sie eine Mindest- und eine Maximalmenge für Arbeitsspeicher ein, die von dieser Maschinenkomponente bereitgestellte Maschinen verbrauchen können.
<b>Speicher (GB): Mindestwert und Maximalwert</b>	<p>Geben Sie eine Mindest- und eine Maximalmenge für Speicher ein, die von dieser Maschinenkomponente bereitgestellte Maschinen verbrauchen können. Bei vSphere, KVM (RHEV), SCVMM, vCloud Air und vCloud Director wird der Mindestspeicher in Abhängigkeit dessen festgelegt, was Sie auf der Registerkarte „Speicher“ eingeben.</p> <p>Wenn Sie in einem Blueprint einen WIM-Bereitstellungsworkflow verwenden, geben Sie einen Speicherwert an, der die Größe jeder Festplatte berücksichtigt, die auf der Maschine verwendet werden soll. Verwenden Sie den Gesamtwert aller Festplatten als Mindestspeicherwert für die Maschinenkomponente. Geben Sie zudem für jede Festplatte eine Größe an, die für das Betriebssystem ausreicht.</p>

## Registerkarte Speicher

Für die Kontrolle von Speicherplatz können Sie Speichervolume-Eigenschaften zu der Maschinenkomponente hinzufügen, einschließlich einer oder mehrerer Speicherreservierungsrichtlinien.

**Tabelle 4-8. Einstellungen auf der Registerkarte Speicher**

Einstellung	Beschreibung
<b>ID</b>	Geben Sie eine ID oder einen Namen für das Speichervolume ein.
<b>Kapazität (GB)</b>	Geben Sie die Speicherkapazität für das Speichervolume ein.
<b>Laufwerkbuchstabe / Bereitstellungspfad</b>	Geben Sie einen Laufwerkbuchstaben oder einen Bereitstellungspfad für das Speichervolume ein.
<b>Bezeichnung</b>	Geben Sie eine Bezeichnung für den Laufwerkbuchstaben und den Bereitstellungspfad für das Speichervolume ein.
<b>Speicherreservierungsrichtlinie</b>	Geben Sie die vorhandene Speicherreservierungsrichtlinie ein, die mit diesem Speichervolume verwendet werden soll.
<b>Benutzerdefinierte Eigenschaften</b>	Geben Sie alle benutzerdefinierten Eigenschaften ein, die mit diesem Speichervolume verwendet werden sollen.
<b>Maximale Anzahl von Volumes</b>	Geben Sie die maximale Anzahl an zulässigen Speichervolumes ein, die bei der Bereitstellung über die Maschinenkomponente verwendet werden können. Geben Sie „0“ ein, damit Andere keine Speichervolumes hinzufügen können. Der Standardwert ist 60.
<b>Anzeigen und Ändern von Speicherreservierungsrichtlinien durch Benutzer zulassen</b>	Aktivieren Sie das Kontrollkästchen, um Benutzern bei der Bereitstellung das Entfernen einer zugeordneten Reservierungsrichtlinie oder die Angabe einer anderen Reservierungsrichtlinie zu ermöglichen.

## Registerkarte **Netzwerk**

Sie können Netzwerkeinstellungen für eine vSphere-Maschinenkomponente konfigurieren, basierend auf Einstellungen für NSX-Netzwerke und Lastausgleichsdienste, die außerhalb von vRealize Automation konfiguriert werden. Sie können Einstellungen von einer oder mehreren vorhandenen und bedarfsgesteuerten NSX-Netzwerkkomponenten auf der Design-Arbeitsfläche des Blueprints verwenden.

Informationen zum Hinzufügen und Konfigurieren von NSX-Netzwerk- und Sicherheitskomponenten vor der Verwendung von Einstellungen für die Registerkarte „Netzwerk“ auf einer vSphere-Maschinenkomponente finden Sie unter [Konfigurieren der Einstellungen für Netzwerk- und Sicherheitskomponenten](#).

Informationen zum Angeben von NSX-Einstellungen auf Blueprint-Ebene, die für vSphere-Maschinenkomponenten gelten, finden Sie unter [Neue Blueprint- und Blueprint-Eigenschaften-Einstellungen mit NSX](#).

**Tabelle 4-9. Einstellungen auf der Registerkarte **Netzwerk****

Einstellung	Beschreibung
<b>Netzwerk</b>	Wählen Sie aus dem Dropdown-Menü eine Netzwerkkomponente aus. Es werden nur Netzwerkkomponenten aufgelistet, die auf der Design-Arbeitsfläche des Blueprints vorhanden sind.
<b>Zuweisungstyp</b>	Akzeptieren Sie die der Netzwerkkomponente entnommene Standardzuweisung oder wählen Sie aus dem Dropdown-Menü einen Zuweisungstyp aus. Die Optionswerte <b>DHCP</b> und <b>Statisch</b> werden den Einstellungen in der Netzwerkkomponente entnommen.
<b>Adresse</b>	Geben Sie die IP-Adresse für das Netzwerk an. Die Option ist nur für den statischen IP-Adresstyp verfügbar.
<b>Lastenausgleich</b>	Geben Sie den für den Lastausgleich zu verwendenden Dienst ein.
<b>Benutzerdefinierte Eigenschaften</b>	Zeigt benutzerdefinierte Eigenschaften an, die für die ausgewählte Netzwerkkomponente bzw. das Netzwerkprofil konfiguriert werden.
<b>Maximale Anzahl von Netzwerkkadaptern</b>	Geben Sie die maximale Anzahl von Netzwerkkadaptern oder Netzwerkkarten an, die für diese Maschinenkomponente zugelassen werden soll. Der Standardwert ist „unlimited“. Setzen Sie diese Option auf 0, um das Hinzufügen von Netzwerkkarten für die Maschinenkomponenten zu deaktivieren.

## Registerkarte **Sicherheit**

Sie können Sicherheitseinstellungen für eine vSphere-Maschinenkomponente konfigurieren, basierend auf NSX-Einstellungen, die außerhalb von vRealize Automation konfiguriert werden. Optional können Sie Einstellungen von vorhandenen und bedarfsgesteuerten NSX-Sicherheitskomponenten auf der Design-Arbeitsfläche des Blueprints verwenden.

Die Sicherheitseinstellungen von vorhandenen und bedarfsgesteuerten Sicherheitsgruppen und Sicherheits-Tag-Komponenten auf der Design-Arbeitsfläche des Blueprints sind automatisch verfügbar.



Informationen zum Hinzufügen und Konfigurieren von NSX-Netzwerk- und Sicherheitskomponenten vor der Verwendung von Einstellungen für die Registerkarte „Sicherheit“ auf einer vSphere-Maschinenkomponente finden Sie unter [Konfigurieren der Einstellungen für Netzwerk- und Sicherheitskomponenten](#).

Informationen zum Angeben von NSX-Informationen auf Blueprint-Ebene, die für vSphere-Maschinenkomponenten gelten, finden Sie unter [Neue Blueprint- und Blueprint-Eigenschaften-Einstellungen mit NSX](#).

**Tabelle 4-10. Einstellungen auf der Registerkarte Sicherheit**

Einstellung	Beschreibung
<b>Name</b>	<p>Zeigt den Namen einer NSX-Sicherheitsgruppe bzw. eines Sicherheits-Tags an. Die Namen werden den Sicherheitskomponenten auf der Design-Arbeitsfläche des Blueprints entnommen.</p> <p>Aktivieren Sie das Kontrollkästchen neben einer aufgelisteten Sicherheitsgruppe bzw. einem Sicherheits-Tag, um die Bereitstellung über diese Maschinenkomponente durchzuführen.</p>
<b>Typ</b>	Gibt an, ob es sich bei dem Sicherheitselement um eine bedarfsgesteuerte Sicherheitsgruppe, eine vorhandene Sicherheitsgruppe oder ein Sicherheits-Tag handelt.
<b>Beschreibung</b>	Zeigt die für die Sicherheitsgruppe bzw. den Sicherheits-Tag definierte Beschreibung an.
<b>Endpoint</b>	Zeigt den durch die NSX-Sicherheitsgruppe bzw. den Sicherheits-Tag verwendeten Endpoint an.

## Registerkarte **Eigenschaften**

Geben Sie optional benutzerdefinierte Eigenschafts- und Eigenschaftsgruppeninformationen für die vSphere-Maschinenkomponente an.

Mithilfe der Registerkarte **Eigenschaften** können Sie benutzerdefinierte Eigenschaften einzeln oder in Gruppen zu der Maschinenkomponente hinzufügen. Mithilfe der Registerkarte **Eigenschaften** können Sie beim Erstellen oder Bearbeiten eines Blueprints auch benutzerdefinierte Eigenschaften und Eigenschaftsgruppen zum gesamten Blueprint hinzufügen. Verwenden Sie dazu die Seite **Neuer Blueprint** bzw. **Blueprint-Eigenschaften**.

Mithilfe der Registerkarte **Benutzerdefinierte Eigenschaften** können Sie Optionen für vorhandene benutzerdefinierte Eigenschaften hinzufügen und konfigurieren. Benutzerdefinierte Einstellungen sind in vRealize Automation enthalten, und Sie können auch Eigenschaftsdefinitionen erstellen.

**Tabelle 4-11. Einstellungen auf der Registerkarte **Eigenschaften** > **Benutzerdefinierte Eigenschaften****

Einstellung	Beschreibung
<b>Name</b>	Geben Sie den Namen einer benutzerdefinierten Eigenschaft ein oder wählen Sie aus dem Dropdown-Menü eine verfügbare benutzerdefinierte Eigenschaft aus. Geben Sie beispielsweise für die benutzerdefinierte Eigenschaft den Namen <code>Machine.SSH</code> ein, um anzugeben, ob mithilfe dieses Blueprints bereitgestellte Maschinen SSH-Verbindungen zulassen. Eigenschaften werden nur dann im Dropdown-Menü angezeigt, wenn Ihr Mandantenadministrator oder Fabric-Administrator Eigenschaftsdefinitionen erstellt hat.
<b>Wert</b>	Geben Sie einen Wert ein bzw. bearbeiten Sie einen Wert, der mit der benutzerdefinierten Eigenschaft verknüpft werden soll. Legen Sie beispielsweise den Wert auf <code>true</code> fest, um berechtigten Benutzern zu ermöglichen, sich via SSH mit Maschinen zu verbinden, die mithilfe Ihres Blueprints bereitgestellten Maschinen zu verbinden wurden.
<b>Verschlüsselt</b>	Sie können den Eigenschaftswert verschlüsseln. Beispielsweise für den Fall, dass es sich bei dem Wert um ein Kennwort handelt.
<b>Überschreibbar</b>	Sie können festlegen, dass der Eigenschaftswert von der nächsten Person, die die Eigenschaft verwendet, oder der nachfolgenden Person überschrieben werden darf. In der Regel handelt es sich bei dieser Person um einen anderen Architekten. Wenn Sie jedoch „In Anforderung anzeigen“ auswählen, können Ihre Unternehmensbenutzer Eigenschaftswerte anzeigen oder bearbeiten, wenn sie Katalogelemente anfordern.
<b>In Anforderung anzeigen</b>	Wenn Sie Ihren Endbenutzern den Namen und den Wert der Eigenschaft anzeigen möchten, können Sie festlegen, dass beim Anfordern einer Maschinenbereitstellung die Eigenschaft im Anforderungsformular angezeigt wird. Sie müssen „Überschreibbar“ auch auswählen, wenn die Benutzer einen Wert eingeben können sollen.

Mithilfe der Registerkarte **Eigenschaftsgruppen** können Sie Eigenschaften für vorhandene benutzerdefinierte Eigenschaftsgruppen hinzufügen und konfigurieren. Sie können eigene Eigenschaftsgruppen erstellen oder Eigenschaftsgruppen verwenden, die für Sie erstellt wurden.

**Tabelle 4-12. Einstellungen auf der Registerkarte **Eigenschaften** > **Eigenschaftsgruppen****

Einstellung	Beschreibung
<b>Name</b>	Wählen Sie aus dem Dropdown-Menü eine verfügbare Sicherheitsgruppe aus.
<b>Nach oben und Nach unten</b>	Steuern Sie die Rangfolge der aufgelisteten Eigenschaftsgruppen in absteigender Reihenfolge. Die zuerst aufgelistete Eigenschaftsgruppe hat Vorrang vor der als nächstes aufgelisteten Eigenschaftsgruppe etc.

**Tabelle 4-12. Einstellungen auf der Registerkarte *Eigenschaften* > *Eigenschaftsgruppen* (Fortsetzung)**

Einstellung	Beschreibung
<b>Eigenschaften anzeigen</b>	Zeigen Sie die benutzerdefinierten Eigenschaften in der ausgewählten Eigenschaftsgruppe an.
<b>Zusammengeführte Eigenschaften anzeigen</b>	Zeigen Sie alle benutzerdefinierten Eigenschaften in den aufgelisteten Eigenschaftsgruppen in der Reihenfolge an, in der sie in der Liste der Eigenschaftsgruppen angezeigt werden. Wenn dieselbe Eigenschaft in mehr als einer Eigenschaftsgruppe angezeigt wird, wird der Eigenschaftsname nur einmal in der Liste angezeigt, je nach dem, wann sie in der Liste zum ersten Mal auftritt.

### vCloud Air -Maschinenkomponenteneinstellungen

Machen Sie sich mit den Einstellungen und Optionen vertraut, die Sie für eine vCloud Air-Maschinenkomponente in der vRealize Automation-Blueprint-Design-Arbeitsfläche konfigurieren können.

### Registerkarte **Allgemein**

Konfigurieren Sie die allgemeinen Einstellungen für eine vCloud Air-Maschinenkomponente.

**Tabelle 4-13. Einstellungen auf der Registerkarte *Allgemein***

Einstellung	Beschreibung
<b>ID</b>	Geben Sie einen Namen für Ihre Maschinenkomponente ein oder übernehmen Sie den Standardwert.
<b>Beschreibung</b>	Eine Zusammenfassung Ihrer Maschinenkomponente für andere Architekten.
<b>Speicherort auf Anforderung anzeigen</b>	In einer Cloud-Umgebung wie vCloud Air wird Benutzern auf diese Weise ermöglicht, eine Region für ihre bereitgestellten Maschinen auszuwählen. Für eine virtuelle Umgebung wie beispielsweise vSphere können Sie die Standorte-Funktion so konfigurieren, dass den Benutzern die Auswahl eines bestimmten Datacenter-Standorts, an dem eine angeforderte Maschine bereitgestellt werden soll, erlaubt wird. Für die vollständige Konfiguration dieser Option fügt ein Systemadministrator Informationen zum Datacenter-Standort zu einer Standortdatei hinzu und ein Fabric-Administrator bearbeitet eine Computing-Ressource, um sie einem Standort zuzuordnen.
<b>Reservierungsrichtlinie</b>	Anwenden einer Reservierungsrichtlinie auf einen Blueprint, um die von diesem Blueprint bereitgestellten Maschinen auf eine Teilmenge der verfügbaren Reservierungen einzuschränken. Fabric-Administratoren erstellen Reservierungsrichtlinien, um eine optionale und hilfreiche Methode zur Kontrolle der Verarbeitung von Reservierungsanforderungen bereitzustellen. Beispielsweise, um Ressourcen in Gruppen für unterschiedliche Service-Level zu erfassen oder um einen bestimmten Ressourcentyp für einen bestimmten Verwendungszweck zur Verfügung zu stellen. Wenn Ihr Fabric-Administrator keine Reservierungsrichtlinien konfiguriert hat, werden in diesem Dropdown-Menü keine verfügbaren Optionen angezeigt.

**Tabelle 4-13. Einstellungen auf der Registerkarte Allgemein (Fortsetzung)**

Einstellung	Beschreibung
<b>Maschinenpräfix</b>	<p>Maschinenpräfixe werden von Fabric-Administratoren erstellt und zum Erstellen der Namen von bereitgestellten Maschinen verwendet. Wenn Sie <b>Gruppenstandardwert verwenden</b> auswählen, werden über Ihren Blueprint bereitgestellte Maschinen gemäß dem Maschinenpräfix benannt, das als Standardwert für die Business-Gruppe des Benutzers konfiguriert ist. Falls kein Maschinenpräfix konfiguriert wurde, wird für Sie eines auf der Grundlage der Business-Gruppe generiert.</p> <p>Wenn Ihr Fabric-Administrator andere Maschinenpräfixe zu Ihrer Auswahl konfiguriert, können Sie ein Präfix auf alle Maschinen anwenden, die über Ihren Blueprint bereitgestellt werden, und zwar unabhängig vom Anforderer.</p>
<b>Instanzen: Mindestwert und Maximalwert</b>	<p>Konfigurieren Sie die minimale oder maximale Anzahl an Instanzen, die Benutzer für eine Bereitstellung oder für eine vertikale oder horizontale Skalierungsaktion anfordern können. Wenn Benutzern keine Auswahlmöglichkeit eingeräumt werden soll, wird durch Eingabe desselben Werts in den Feldern <b>Minimalwert</b> und <b>Maximalwert</b> die genaue Anzahl der bereitzustellenden Instanzen festgelegt und die Skalierungsaktionen für diese Maschinenkomponente werden deaktiviert.</p> <p>XaaS-Komponenten sind nicht skalierbar und werden bei einem Skalierungsvorgang nicht aktualisiert. Wenn Sie XaaS-Komponenten in Ihrem Blueprint verwenden, könnten Sie eine Ressourcenaktion erstellen, die Benutzer nach einem Skalierungsvorgang ausführen können, um Ihre XaaS-Komponenten zu skalieren oder aktualisieren. Alternativ könnten Sie die Skalierung deaktivieren, indem Sie genau die Anzahl von Instanzen konfigurieren, die Sie für jede Maschinenkomponente zulassen möchten.</p>

## Registerkarte Build-Informationen

Konfigurieren Sie Einstellungen für Build-Informationen für eine vCloud Air-Maschinenkomponente.

**Tabelle 4-14. Registerkarte Build-Informationen**

Einstellung	Beschreibung
<b>Blueprint-Typ</b>	Wählen Sie zu Statistik- und Lizenzierungszwecken aus, ob über diesen Blueprint bereitgestellte Maschinen als „Desktop“ oder „Server“ klassifiziert werden.
<b>Aktion</b>	<p>Die im Dropdown-Menü „Aktion“ angezeigten Optionen hängen vom ausgewählten Maschinentyp ab.</p> <p>Die folgenden Aktionen sind verfügbar:</p> <ul style="list-style-type: none"> <li>■ Klonen</li> </ul> <p>Erstellt Kopien einer virtuellen Maschine anhand einer Vorlage und eines Anpassungsobjekts.</p>

**Tabelle 4-14. Registerkarte Build-Informationen (Fortsetzung)**

Einstellung	Beschreibung
<b>Bereitstellungsworkflow</b>	<p>Die im Dropdown-Menü „Bereitstellungsworkflow“ angezeigten Optionen hängen vom ausgewählten Maschinentyp und der ausgewählten Aktion ab.</p> <p>Die folgenden Aktionen sind verfügbar:</p> <ul style="list-style-type: none"> <li>■ CloneWorkflow</li> </ul> <p>Erstellt Kopien einer virtuellen Maschine entweder mit „Klonen“, „Verknüpfter Klon“ oder „NetApp FlexClone“.</p>
<b>Klonen von</b>	<p>Wählen Sie für Klonen oder NetApp FlexClone eine zu klonende Maschinenvorlage aus.</p> <p>Wählen Sie für verknüpfte Klone eine Maschine aus der Liste der Maschinen aus. Es werden Ihnen nur Maschinen mit verfügbaren klonbaren Snapshots angezeigt, die Sie als Mandantenadministrator oder Business-Gruppenmanager verwalten.</p> <p>Sie können nur von Vorlagen klonen, die auf Maschinen vorhanden sind, die Sie als Business-Gruppenmanager oder Mandantenadministrator verwalten.</p>

## Registerkarte Maschinenressourcen

Geben Sie die Einstellungen für CPU, Arbeitsspeicher und Speicher für die vCloud Air-Maschinenkomponente an.

**Tabelle 4-15. Registerkarte Maschinenressourcen**

Einstellung	Beschreibung
<b>CPUs: Mindestwert und Maximalwert</b>	Geben Sie eine Mindest- und eine Maximalanzahl an CPUs ein, die durch diese Maschinenkomponente bereitgestellt werden können.
<b>Arbeitsspeicher (MB): Mindestwert und Maximalwert</b>	Geben Sie eine Mindest- und eine Maximalmenge für Arbeitsspeicher ein, die von dieser Maschinenkomponente bereitgestellte Maschinen verbrauchen können.
<b>Speicher (GB): Mindestwert und Maximalwert</b>	Geben Sie eine Mindest- und eine Maximalmenge für Speicher ein, die von dieser Maschinenkomponente bereitgestellte Maschinen verbrauchen können. Bei vSphere, KVM (RHEV), SCVMM, vCloud Air und vCloud Director wird der Mindestspeicher in Abhängigkeit dessen festgelegt, was Sie auf der Registerkarte „Speicher“ eingeben.

## Registerkarte Speicher

Für die Kontrolle von Speicherplatz können Sie Speichervolume-Eigenschaften zu der Maschinenkomponente hinzufügen, einschließlich einer oder mehrerer Speicherreservierungsrichtlinien.

**Tabelle 4-16. Einstellungen auf der Registerkarte Speicher**

Einstellung	Beschreibung
<b>ID</b>	Geben Sie eine ID oder einen Namen für das Speichervolume ein.
<b>Kapazität (GB)</b>	Geben Sie die Speicherkapazität für das Speichervolume ein.
<b>Laufwerkbuchstabe / Bereitstellungspfad</b>	Geben Sie einen Laufwerkbuchstaben oder einen Bereitstellungspfad für das Speichervolume ein.
<b>Bezeichnung</b>	Geben Sie eine Bezeichnung für den Laufwerkbuchstaben und den Bereitstellungspfad für das Speichervolume ein.
<b>Speicherreservierungsrichtlinie</b>	Geben Sie die vorhandene Speicherreservierungsrichtlinie ein, die mit diesem Speichervolume verwendet werden soll.
<b>Benutzerdefinierte Eigenschaften</b>	Geben Sie alle benutzerdefinierten Eigenschaften ein, die mit diesem Speichervolume verwendet werden sollen.
<b>Maximale Anzahl von Volumes</b>	Geben Sie die maximale Anzahl an zulässigen Speichervolumes ein, die bei der Bereitstellung über die Maschinenkomponente verwendet werden können. Geben Sie „0“ ein, damit Andere keine Speichervolumes hinzufügen können. Der Standardwert ist 60.
<b>Anzeigen und Ändern von Speicherreservierungsrichtlinien durch Benutzer zulassen</b>	Aktivieren Sie das Kontrollkästchen, um Benutzern bei der Bereitstellung das Entfernen einer zugeordneten Reservierungsrichtlinie oder die Angabe einer anderen Reservierungsrichtlinie zu ermöglichen.

## Registerkarte **Eigenschaften**

Geben Sie optional benutzerdefinierte Eigenschafts- und Eigenschaftsgruppeninformationen für die vCloud Air-Maschinenkomponente an.

Mithilfe der Registerkarte **Eigenschaften** können Sie benutzerdefinierte Eigenschaften einzeln oder in Gruppen zu der Maschinenkomponente hinzufügen. Mithilfe der Registerkarte **Eigenschaften** können Sie beim Erstellen oder Bearbeiten eines Blueprints auch benutzerdefinierte Eigenschaften und Eigenschaftsgruppen zum gesamten Blueprint hinzufügen. Verwenden Sie dazu die Seite **Neuer Blueprint** bzw. **Blueprint-Eigenschaften**.

Mithilfe der Registerkarte **Benutzerdefinierte Eigenschaften** können Sie Optionen für vorhandene benutzerdefinierte Eigenschaften hinzufügen und konfigurieren. Benutzerdefinierte Einstellungen sind in vRealize Automation enthalten, und Sie können auch Eigenschaftsdefinitionen erstellen.

**Tabelle 4-17. Einstellungen auf der Registerkarte *Eigenschaften* > *Benutzerdefinierte Eigenschaften***

Einstellung	Beschreibung
<b>Name</b>	Geben Sie den Namen einer benutzerdefinierten Eigenschaft ein oder wählen Sie aus dem Dropdown-Menü eine verfügbare benutzerdefinierte Eigenschaft aus. Geben Sie beispielsweise für die benutzerdefinierte Eigenschaft den Namen <code>Machine.SSH</code> ein, um anzugeben, ob mithilfe dieses Blueprints bereitgestellte Maschinen SSH-Verbindungen zulassen. Eigenschaften werden nur dann im Dropdown-Menü angezeigt, wenn Ihr Mandantenadministrator oder Fabric-Administrator Eigenschaftsdefinitionen erstellt hat.
<b>Wert</b>	Geben Sie einen Wert ein bzw. bearbeiten Sie einen Wert, der mit der benutzerdefinierten Eigenschaft verknüpft werden soll. Legen Sie beispielsweise den Wert auf <code>true</code> fest, um berechtigten Benutzern zu ermöglichen, sich via SSH mit Maschinen zu verbinden, die mithilfe Ihres Blueprints bereitgestellten Maschinen zu verbinden wurden.
<b>Verschlüsselt</b>	Sie können den Eigenschaftswert verschlüsseln. Beispielsweise für den Fall, dass es sich bei dem Wert um ein Kennwort handelt.
<b>Überschreibbar</b>	Sie können festlegen, dass der Eigenschaftswert von der nächsten Person, die die Eigenschaft verwendet, oder der nachfolgenden Person überschrieben werden darf. In der Regel handelt es sich bei dieser Person um einen anderen Architekten. Wenn Sie jedoch „In Anforderung anzeigen“ auswählen, können Ihre Unternehmensbenutzer Eigenschaftswerte anzeigen oder bearbeiten, wenn sie Katalogelemente anfordern.
<b>In Anforderung anzeigen</b>	Wenn Sie Ihren Endbenutzern den Namen und den Wert der Eigenschaft anzeigen möchten, können Sie festlegen, dass beim Anfordern einer Maschinenbereitstellung die Eigenschaft im Anforderungsformular angezeigt wird. Sie müssen „Überschreibbar“ auch auswählen, wenn die Benutzer einen Wert eingeben können sollen.

Mithilfe der Registerkarte **Eigenschaftsgruppen** können Sie Eigenschaften für vorhandene benutzerdefinierte Eigenschaftsgruppen hinzufügen und konfigurieren. Sie können eigene Eigenschaftsgruppen erstellen oder Eigenschaftsgruppen verwenden, die für Sie erstellt wurden.

**Tabelle 4-18. Einstellungen auf der Registerkarte *Eigenschaften* > *Eigenschaftsgruppen***

Einstellung	Beschreibung
<b>Name</b>	Wählen Sie aus dem Dropdown-Menü eine verfügbare Sicherheitsgruppe aus.
<b>Nach oben und Nach unten</b>	Steuern Sie die Rangfolge der aufgelisteten Eigenschaftsgruppen in absteigender Reihenfolge. Die zuerst aufgelistete Eigenschaftsgruppe hat Vorrang vor der als nächstes aufgelisteten Eigenschaftsgruppe etc.

**Tabelle 4-18. Einstellungen auf der Registerkarte *Eigenschaften* > *Eigenschaftsgruppen* (Fortsetzung)**

Einstellung	Beschreibung
<b>Eigenschaften anzeigen</b>	Zeigen Sie die benutzerdefinierten Eigenschaften in der ausgewählten Eigenschaftsgruppe an.
<b>Zusammengeführte Eigenschaften anzeigen</b>	Zeigen Sie alle benutzerdefinierten Eigenschaften in den aufgelisteten Eigenschaftsgruppen in der Reihenfolge an, in der sie in der Liste der Eigenschaftsgruppen angezeigt werden. Wenn dieselbe Eigenschaft in mehr als einer Eigenschaftsgruppe angezeigt wird, wird der Eigenschaftsname nur einmal in der Liste angezeigt, je nach dem, wann sie in der Liste zum ersten Mal auftritt.

### Einstellungen für Amazon-Maschinenkomponenten

Machen Sie sich mit den Einstellungen und Optionen vertraut, die Sie auf der Design-Arbeitsfläche des vRealize Automation-Blueprints für eine Amazon-Maschinenkomponente konfigurieren können.

### Registerkarte **Allgemein**

Konfigurieren Sie allgemeine Einstellungen für eine Amazon-Maschinenkomponente.

**Tabelle 4-19. Einstellungen auf der Registerkarte *Allgemein***

Einstellung	Beschreibung
<b>ID</b>	Geben Sie einen Namen für Ihre Maschinenkomponente ein oder übernehmen Sie den Standardwert.
<b>Beschreibung</b>	Eine Zusammenfassung Ihrer Maschinenkomponente für andere Architekten.
<b>Speicherort auf Anforderung anzeigen</b>	In einer Cloud-Umgebung wie vCloud Air wird Benutzern auf diese Weise ermöglicht, eine Region für ihre bereitgestellten Maschinen auszuwählen. Für eine virtuelle Umgebung wie beispielsweise vSphere können Sie die Standorte-Funktion so konfigurieren, dass den Benutzern die Auswahl eines bestimmten Datacenter-Standorts, an dem eine angeforderte Maschine bereitgestellt werden soll, erlaubt wird. Für die vollständige Konfiguration dieser Option fügt ein Systemadministrator Informationen zum Datacenter-Standort zu einer Standortdatei hinzu und ein Fabric-Administrator bearbeitet eine Computing-Ressource, um sie einem Standort zuzuordnen.
<b>Reservierungsrichtlinie</b>	Anwenden einer Reservierungsrichtlinie auf einen Blueprint, um die von diesem Blueprint bereitgestellten Maschinen auf eine Teilmenge der verfügbaren Reservierungen einzuschränken. Fabric-Administratoren erstellen Reservierungsrichtlinien, um eine optionale und hilfreiche Methode zur Kontrolle der Verarbeitung von Reservierungsanforderungen bereitzustellen. Beispielsweise, um Ressourcen in Gruppen für unterschiedliche Service-Level zu erfassen oder um einen bestimmten Ressourcentyp für einen bestimmten Verwendungszweck zur Verfügung zu stellen. Wenn Ihr Fabric-Administrator keine Reservierungsrichtlinien konfiguriert hat, werden in diesem Dropdown-Menü keine verfügbaren Optionen angezeigt.



**Tabelle 4-19. Einstellungen auf der Registerkarte Allgemein (Fortsetzung)**

Einstellung	Beschreibung
<b>Maschinenpräfix</b>	<p>Maschinenpräfixe werden von Fabric-Administratoren erstellt und zum Erstellen der Namen von bereitgestellten Maschinen verwendet. Wenn Sie <b>Gruppenstandardwert verwenden</b> auswählen, werden über Ihren Blueprint bereitgestellte Maschinen gemäß dem Maschinenpräfix benannt, das als Standardwert für die Business-Gruppe des Benutzers konfiguriert ist. Falls kein Maschinenpräfix konfiguriert wurde, wird für Sie eines auf der Grundlage der Business-Gruppe generiert.</p> <p>Wenn Ihr Fabric-Administrator andere Maschinenpräfixe zu Ihrer Auswahl konfiguriert, können Sie ein Präfix auf alle Maschinen anwenden, die über Ihren Blueprint bereitgestellt werden, und zwar unabhängig vom Anforderer.</p>
<b>Instanzen: Mindestwert und Maximalwert</b>	<p>Konfigurieren Sie die minimale oder maximale Anzahl an Instanzen, die Benutzer für eine Bereitstellung oder für eine vertikale oder horizontale Skalierungsaktion anfordern können. Wenn Benutzern keine Auswahlmöglichkeit eingeräumt werden soll, wird durch Eingabe desselben Werts in den Feldern <b>Minimalwert</b> und <b>Maximalwert</b> die genaue Anzahl der bereitzustellenden Instanzen festgelegt und die Skalierungsaktionen für diese Maschinenkomponente werden deaktiviert.</p> <p>XaaS-Komponenten sind nicht skalierbar und werden bei einem Skalierungsvorgang nicht aktualisiert. Wenn Sie XaaS-Komponenten in Ihrem Blueprint verwenden, könnten Sie eine Ressourcenaktion erstellen, die Benutzer nach einem Skalierungsvorgang ausführen können, um Ihre XaaS-Komponenten zu skalieren oder aktualisieren. Alternativ könnten Sie die Skalierung deaktivieren, indem Sie genau die Anzahl von Instanzen konfigurieren, die Sie für jede Maschinenkomponente zulassen möchten.</p>

## Registerkarte Build-Informationen

Konfigurieren Sie Einstellungen für Build-Informationen für eine Amazon-Maschinenkomponente.

**Tabelle 4-20. Registerkarte „Build-Informationen“**

Einstellung	Beschreibung
<b>Blueprint-Typ</b>	Wählen Sie zu Statistik- und Lizenzierungszwecken aus, ob über diesen Blueprint bereitgestellte Maschinen als „Desktop“ oder „Server“ klassifiziert werden.
<b>Bereitstellungsworkflow</b>	<p>Der einzige, für eine Amazon-Maschinenkomponente verfügbare Bereitstellungsworkflow ist CloudProvisioningWorkflow.</p> <p>Erstellt eine Maschine durch Starten über eine VM-Instanz oder ein Cloud-basiertes Image.</p>
<b>Amazon-Maschinen-Image</b>	Wählen Sie ein verfügbares Amazon-Maschinen-Image aus. Ein Amazon-Maschinen-Image ist eine Vorlage, die eine Softwarekonfiguration einschließlich eines Betriebssystems enthält. Maschinen-Images werden über Amazon Web Services-Konten verwaltet.

**Tabelle 4-20. Registerkarte „Build-Informationen“ (Fortsetzung)**

Einstellung	Beschreibung
<b>Schlüsselpaar</b>	<p>Schlüsselpaare sind für die Bereitstellung mit Amazon Web Services erforderlich.</p> <p>Schlüsselpaare werden für die Bereitstellung und Verbindung zu einer Cloudinstanz verwendet. Sie werden auch zur Entschlüsselung von Windows-Kennwörtern und zur Anmeldung bei einer Linux-Maschine verwendet.</p> <p>Die folgenden Optionen sind für Schlüsselpaare verfügbar:</p> <ul style="list-style-type: none"> <li>■ Nicht angegeben <p>Das Verhalten von Schlüsselpaaren wird auf der Blueprint-Ebene anstatt auf der Reservierungsebene gesteuert.</p> </li> <li>■ Automatisch generiert pro Business-Gruppe <p>Gibt an, dass jede bereitgestellte Maschine in einer Business-Gruppe über dasselbe Schlüsselpaar verfügt. Dies trifft auch für Maschinen zu, die in anderen Reservierungen bereitgestellt wurden, sofern die Maschine dieselbe Computing-Ressource und Business-Gruppe aufweist. Da die Schlüsselpaare mit einer Business-Gruppe verknüpft sind, werden die Schlüsselpaare beim Löschen der Business-Gruppe ebenfalls gelöscht.</p> </li> <li>■ Automatisch generiert pro Maschine <p>Gibt an, dass jede Maschine ein eindeutiges Schlüsselpaar aufweist. Die Option „Automatisch generiert pro Maschine“ stellt die sicherste Methode dar, da keine Schlüsselpaare von Maschinen gemeinsam genutzt werden.</p> </li> </ul>
<b>Amazon-Netzwerkoptionen auf der Maschine aktivieren</b>	<p>Wählen Sie aus, ob Benutzer eine Maschine am Speicherort einer Virtual Private Cloud (VPC) oder Nicht-VPC bereitstellen dürfen, wenn Sie die Maschinenanforderung übermitteln.</p>
<b>Instanztypen</b>	<p>Wählen Sie einen oder mehrere Instanztypen aus. Eine Amazon-Instanz ist ein virtueller Server, der Anwendungen in Amazon Web Services ausführen kann. Instanzen werden aus einem Amazon-Maschinen-Image erstellt und indem ein geeigneter Instanztyp ausgewählt wird. vRealize Automation verwaltet die Instanztypen der Maschinen-Images, die für die Bereitstellung verfügbar sind.</p> <p>Informationen zur Verwendung von Amazon-Instanztypen in vRealize Automation finden Sie unter <a href="#">Grundlegendes zu Amazon-Instanztypen</a> und <a href="#">Hinzufügen eines Amazon-Instanztyps</a>.</p>

### Registerkarte Maschinenressourcen

Geben Sie Einstellungen für CPU, Arbeitsspeicher, Speicher und EBS-Datenträger für Ihre Amazon-Maschinenkomponente an.

**Tabelle 4-21. Registerkarte Maschinenressourcen**

Einstellung	Beschreibung
<b>CPUs: Mindestwert</b> und <b>Maximalwert</b>	Geben Sie eine Mindest- und eine Maximalanzahl an CPUs ein, die durch diese Maschinenkomponente bereitgestellt werden können.
<b>Arbeitsspeicher (MB): Mindestwert</b> und <b>Maximalwert</b>	Geben Sie eine Mindest- und eine Maximalmenge für Arbeitsspeicher ein, die von dieser Maschinenkomponente bereitgestellte Maschinen verbrauchen können.
<b>Speicher (GB): Mindestwert</b> und <b>Maximalwert</b>	Geben Sie eine Mindest- und eine Maximalmenge für Speicher ein, die von dieser Maschinenkomponente bereitgestellte Maschinen verbrauchen können. Bei vSphere, KVM (RHEV), SCVMM, vCloud Air und vCloud Director wird der Mindestspeicher in Abhängigkeit dessen festgelegt, was Sie auf der Registerkarte „Speicher“ eingeben.
<b>EBS-Speicher (GB): Mindestwert</b> und <b>Maximalwert</b>	Geben Sie eine Mindest- und Maximalmenge für Speichervolumen von Amazon Elastic Block Store (EBS) ein, die von dieser Maschinenkomponente bereitgestellte Maschinenressourcen verbrauchen können.  Beim Löschen einer Bereitstellung, die eine Amazon-Maschinenkomponente enthält, werden alle EBS-Volumes, die der Maschine während ihres Lebenszyklus hinzugefügt wurden, getrennt und nicht gelöscht. vRealize Automation bietet keine Option zum Löschen von EBS-Volumes.

## Registerkarte **Eigenschaften**

Geben Sie optional Informationen zu benutzerdefinierten Eigenschaften und Eigenschaftsgruppen für Ihre Amazon-Maschinenkomponente an.

Mithilfe der Registerkarte **Eigenschaften** können Sie benutzerdefinierte Eigenschaften einzeln oder in Gruppen zu der Maschinenkomponente hinzufügen. Mithilfe der Registerkarte **Eigenschaften** können Sie beim Erstellen oder Bearbeiten eines Blueprints auch benutzerdefinierte Eigenschaften und Eigenschaftsgruppen zum gesamten Blueprint hinzufügen. Verwenden Sie dazu die Seite **Neuer Blueprint** bzw. **Blueprint-Eigenschaften**.

Mithilfe der Registerkarte **Benutzerdefinierte Eigenschaften** können Sie Optionen für vorhandene benutzerdefinierte Eigenschaften hinzufügen und konfigurieren. Benutzerdefinierte Einstellungen sind in vRealize Automation enthalten, und Sie können auch Eigenschaftsdefinitionen erstellen.

**Tabelle 4-22. Einstellungen auf der Registerkarte *Eigenschaften* > *Benutzerdefinierte Eigenschaften***

Einstellung	Beschreibung
<b>Name</b>	Geben Sie den Namen einer benutzerdefinierten Eigenschaft ein oder wählen Sie aus dem Dropdown-Menü eine verfügbare benutzerdefinierte Eigenschaft aus. Geben Sie beispielsweise für die benutzerdefinierte Eigenschaft den Namen <code>Machine.SSH</code> ein, um anzugeben, ob mithilfe dieses Blueprints bereitgestellte Maschinen SSH-Verbindungen zulassen. Eigenschaften werden nur dann im Dropdown-Menü angezeigt, wenn Ihr Mandantenadministrator oder Fabric-Administrator Eigenschaftsdefinitionen erstellt hat.
<b>Wert</b>	Geben Sie einen Wert ein bzw. bearbeiten Sie einen Wert, der mit der benutzerdefinierten Eigenschaft verknüpft werden soll. Legen Sie beispielsweise den Wert auf <code>true</code> fest, um berechtigten Benutzern zu ermöglichen, sich via SSH mit Maschinen zu verbinden, die mithilfe Ihres Blueprints bereitgestellten Maschinen zu verbinden wurden.
<b>Verschlüsselt</b>	Sie können den Eigenschaftswert verschlüsseln. Beispielsweise für den Fall, dass es sich bei dem Wert um ein Kennwort handelt.
<b>Überschreibbar</b>	Sie können festlegen, dass der Eigenschaftswert von der nächsten Person, die die Eigenschaft verwendet, oder der nachfolgenden Person überschrieben werden darf. In der Regel handelt es sich bei dieser Person um einen anderen Architekten. Wenn Sie jedoch „In Anforderung anzeigen“ auswählen, können Ihre Unternehmensbenutzer Eigenschaftswerte anzeigen oder bearbeiten, wenn sie Katalogelemente anfordern.
<b>In Anforderung anzeigen</b>	Wenn Sie Ihren Endbenutzern den Namen und den Wert der Eigenschaft anzeigen möchten, können Sie festlegen, dass beim Anfordern einer Maschinenbereitstellung die Eigenschaft im Anforderungsformular angezeigt wird. Sie müssen „Überschreibbar“ auch auswählen, wenn die Benutzer einen Wert eingeben können sollen.

Mithilfe der Registerkarte **Eigenschaftsgruppen** können Sie Eigenschaften für vorhandene benutzerdefinierte Eigenschaftsgruppen hinzufügen und konfigurieren. Sie können eigene Eigenschaftsgruppen erstellen oder Eigenschaftsgruppen verwenden, die für Sie erstellt wurden.

**Tabelle 4-23. Einstellungen auf der Registerkarte *Eigenschaften* > *Eigenschaftsgruppen***

Einstellung	Beschreibung
<b>Name</b>	Wählen Sie aus dem Dropdown-Menü eine verfügbare Sicherheitsgruppe aus.
<b>Nach oben und Nach unten</b>	Steuern Sie die Rangfolge der aufgelisteten Eigenschaftsgruppen in absteigender Reihenfolge. Die zuerst aufgelistete Eigenschaftsgruppe hat Vorrang vor der als nächstes aufgelisteten Eigenschaftsgruppe etc.

**Tabelle 4-23. Einstellungen auf der Registerkarte *Eigenschaften* > *Eigenschaftsgruppen* (Fortsetzung)**

Einstellung	Beschreibung
<b>Eigenschaften anzeigen</b>	Zeigen Sie die benutzerdefinierten Eigenschaften in der ausgewählten Eigenschaftsgruppe an.
<b>Zusammengeführte Eigenschaften anzeigen</b>	Zeigen Sie alle benutzerdefinierten Eigenschaften in den aufgelisteten Eigenschaftsgruppen in der Reihenfolge an, in der sie in der Liste der Eigenschaftsgruppen angezeigt werden. Wenn dieselbe Eigenschaft in mehr als einer Eigenschaftsgruppe angezeigt wird, wird der Eigenschaftsname nur einmal in der Liste angezeigt, je nach dem, wann sie in der Liste zum ersten Mal auftritt.

## Einstellungen für OpenStack-Maschinenkomponenten

Machen Sie sich mit den Einstellungen und Optionen vertraut, die Sie für eine OpenStack-Maschinenkomponente in der vRealize Automation-Blueprint-Design-Arbeitsfläche konfigurieren können.

### Registerkarte **Allgemein**

Konfigurieren Sie die allgemeinen Einstellungen für eine OpenStack-Maschinenkomponente.

**Tabelle 4-24. Einstellungen auf der Registerkarte *Allgemein***

Einstellung	Beschreibung
<b>ID</b>	Geben Sie einen Namen für Ihre Maschinenkomponente ein oder übernehmen Sie den Standardwert.
<b>Beschreibung</b>	Eine Zusammenfassung Ihrer Maschinenkomponente für andere Architekten.
<b>Speicherort auf Anforderung anzeigen</b>	In einer Cloud-Umgebung wie vCloud Air wird Benutzern auf diese Weise ermöglicht, eine Region für ihre bereitgestellten Maschinen auszuwählen. Für eine virtuelle Umgebung wie beispielsweise vSphere können Sie die Standorte-Funktion so konfigurieren, dass den Benutzern die Auswahl eines bestimmten Datacenter-Standorts, an dem eine angeforderte Maschine bereitgestellt werden soll, erlaubt wird. Für die vollständige Konfiguration dieser Option fügt ein Systemadministrator Informationen zum Datacenter-Standort zu einer Standortdatei hinzu und ein Fabric-Administrator bearbeitet eine Computing-Ressource, um sie einem Standort zuzuordnen.
<b>Reservierungsrichtlinie</b>	Anwenden einer Reservierungsrichtlinie auf einen Blueprint, um die von diesem Blueprint bereitgestellten Maschinen auf eine Teilmenge der verfügbaren Reservierungen einzuschränken. Fabric-Administratoren erstellen Reservierungsrichtlinien, um eine optionale und hilfreiche Methode zur Kontrolle der Verarbeitung von Reservierungsanforderungen bereitzustellen. Beispielsweise, um Ressourcen in Gruppen für unterschiedliche Service-Level zu erfassen oder um einen bestimmten Ressourcentyp für einen bestimmten Verwendungszweck zur Verfügung zu stellen. Wenn Ihr Fabric-Administrator keine Reservierungsrichtlinien konfiguriert hat, werden in diesem Dropdown-Menü keine verfügbaren Optionen angezeigt.

**Tabelle 4-24. Einstellungen auf der Registerkarte Allgemein (Fortsetzung)**

Einstellung	Beschreibung
<b>Maschinenpräfix</b>	<p>Maschinenpräfixe werden von Fabric-Administratoren erstellt und zum Erstellen der Namen von bereitgestellten Maschinen verwendet. Wenn Sie <b>Gruppenstandardwert verwenden</b> auswählen, werden über Ihren Blueprint bereitgestellte Maschinen gemäß dem Maschinenpräfix benannt, das als Standardwert für die Business-Gruppe des Benutzers konfiguriert ist. Falls kein Maschinenpräfix konfiguriert wurde, wird für Sie eines auf der Grundlage der Business-Gruppe generiert.</p> <p>Wenn Ihr Fabric-Administrator andere Maschinenpräfixe zu Ihrer Auswahl konfiguriert, können Sie ein Präfix auf alle Maschinen anwenden, die über Ihren Blueprint bereitgestellt werden, und zwar unabhängig vom Anforderer.</p>
<b>Instanzen: Mindestwert und Maximalwert</b>	<p>Konfigurieren Sie die minimale oder maximale Anzahl an Instanzen, die Benutzer für eine Bereitstellung oder für eine vertikale oder horizontale Skalierungsaktion anfordern können. Wenn Benutzern keine Auswahlmöglichkeit eingeräumt werden soll, wird durch Eingabe desselben Werts in den Feldern <b>Minimalwert</b> und <b>Maximalwert</b> die genaue Anzahl der bereitzustellenden Instanzen festgelegt und die Skalierungsaktionen für diese Maschinenkomponente werden deaktiviert.</p> <p>XaaS-Komponenten sind nicht skalierbar und werden bei einem Skalierungsvorgang nicht aktualisiert. Wenn Sie XaaS-Komponenten in Ihrem Blueprint verwenden, könnten Sie eine Ressourcenaktion erstellen, die Benutzer nach einem Skalierungsvorgang ausführen können, um Ihre XaaS-Komponenten zu skalieren oder aktualisieren. Alternativ könnten Sie die Skalierung deaktivieren, indem Sie genau die Anzahl von Instanzen konfigurieren, die Sie für jede Maschinenkomponente zulassen möchten.</p>

## Registerkarte Build-Informationen

Konfigurieren Sie Einstellungen für Build-Informationen für eine OpenStack-Maschinenkomponente.

**Tabelle 4-25. Registerkarte Build-Informationen**

Einstellung	Beschreibung
<b>Blueprint-Typ</b>	Wählen Sie zu Statistik- und Lizenzierungszwecken aus, ob über diesen Blueprint bereitgestellte Maschinen als „Desktop“ oder „Server“ klassifiziert werden.
<b>Bereitstellungsworkflow</b>	<p>Die folgenden Bereitstellungsworkflows sind für eine Open-Stack-Maschinenkomponente verfügbar:</p> <ul style="list-style-type: none"> <li>■ <b>CloudLinuxKickstartWorkflow</b> <p>Stellen Sie eine Maschine durch Starten von einem ISO-Image bereit. Verwenden Sie dabei eine Kickstart- oder AutoYaST-Konfigurationsdatei und ein Linux-Distributions-Image zum Installieren des Betriebssystems auf der Maschine.</p> </li> <li>■ <b>CloudProvisioningWorkflow</b> <p>Erstellt eine Maschine durch Starten über eine VM-Instanz oder ein Cloud-basiertes Image.</p> </li> <li>■ <b>CloudWIMImageWorkflow</b> <p>Stellen Sie eine Maschine durch Starten in eine WinPE-Umgebung bereit und durch Installieren eines Betriebssystems unter Verwendung eines WIM-Images (Windows Imaging Format) einer vorhandenen Windows-Referenzmaschine.</p> <p>Wenn Sie in einem Blueprint einen WIM-Bereitstellungsworkflow verwenden, geben Sie einen Speicherwert an, der die Größe jeder Festplatte berücksichtigt, die auf der Maschine verwendet werden soll. Verwenden Sie den Gesamtwert aller Festplatten als Mindestspeicherwert für die Maschinenkomponente. Geben Sie zudem für jede Festplatte eine Größe an, die für das Betriebssystem ausreicht.</p> </li> </ul>
<b>OpenStack-Image</b>	Wählen Sie ein verfügbares OpenStack-Maschinen-Image aus. Ein OpenStack-Maschinen-Image ist eine Vorlage, die eine Softwarekonfiguration einschließlich eines Betriebssystems enthält. Maschinen-Images werden über OpenStack-Konten verwaltet.

**Tabelle 4-25. Registerkarte Build-Informationen (Fortsetzung)**

Einstellung	Beschreibung
<b>Schlüsselpaar</b>	<p>Schlüsselpaare sind für die Bereitstellung mit OpenStack optional.</p> <p>Schlüsselpaare werden für die Bereitstellung und Verbindung zu einer Cloudinstanz verwendet. Sie werden auch zur Entschlüsselung von Windows-Kennwörtern und zur Anmeldung bei einer Linux-Maschine verwendet.</p> <p>Die folgenden Optionen sind für Schlüsselpaare verfügbar:</p> <ul style="list-style-type: none"> <li>■ Nicht angegeben <p>Das Verhalten von Schlüsselpaaren wird auf der Blueprint-Ebene anstatt auf der Reservierungsebene gesteuert.</p> </li> <li>■ Automatisch generiert pro Business-Gruppe <p>Gibt an, dass jede bereitgestellte Maschine in einer Business-Gruppe über dasselbe Schlüsselpaar verfügt. Dies trifft auch für Maschinen zu, die in anderen Reservierungen bereitgestellt wurden, sofern die Maschine dieselbe Computing-Ressource und Business-Gruppe aufweist. Da die Schlüsselpaare mit einer Business-Gruppe verknüpft sind, werden die Schlüsselpaare beim Löschen der Business-Gruppe ebenfalls gelöscht.</p> </li> <li>■ Automatisch generiert pro Maschine <p>Gibt an, dass jede Maschine ein eindeutiges Schlüsselpaar aufweist. Die Option „Automatisch generiert pro Maschine“ stellt die sicherste Methode dar, da keine Schlüsselpaare von Maschinen gemeinsam genutzt werden.</p> </li> </ul>
<b>Typen</b>	<p>Wählen Sie eine oder mehrere OpenStack-Typen aus. Ein OpenStack-Typ ist eine virtuelle Hardwarevorlage, die die Spezifikationen der Maschinenressourcen für in OpenStack bereitgestellte Instanzen definiert. Typen werden durch den OpenStack-Anbieter verwaltet und während der Datenerfassung importiert.</p>

**Registerkarte Maschinenressourcen**

Geben Sie die Einstellungen für CPU, Arbeitsspeicher und Speicher für die OpenStack-Maschinenkomponente an.



**Tabelle 4-26. Registerkarte Maschinenressourcen**

Einstellung	Beschreibung
<b>CPUs: Mindestwert und Maximalwert</b>	Geben Sie eine Mindest- und eine Maximalanzahl an CPUs ein, die durch diese Maschinenkomponente bereitgestellt werden können.
<b>Arbeitsspeicher (MB): Mindestwert und Maximalwert</b>	Geben Sie eine Mindest- und eine Maximalmenge für Arbeitsspeicher ein, die von dieser Maschinenkomponente bereitgestellte Maschinen verbrauchen können.
<b>Speicher (GB): Mindestwert und Maximalwert</b>	<p>Geben Sie eine Mindest- und eine Maximalmenge für Speicher ein, die von dieser Maschinenkomponente bereitgestellte Maschinen verbrauchen können. Bei vSphere, KVM (RHEV), SCVMM, vCloud Air und vCloud Director wird der Mindestspeicher in Abhängigkeit dessen festgelegt, was Sie auf der Registerkarte „Speicher“ eingeben.</p> <p>Wenn Sie in einem Blueprint einen WIM-Bereitstellungsworkflow verwenden, geben Sie einen Speicherwert an, der die Größe jeder Festplatte berücksichtigt, die auf der Maschine verwendet werden soll. Verwenden Sie den Gesamtwert aller Festplatten als Mindestspeicherwert für die Maschinenkomponente. Geben Sie zudem für jede Festplatte eine Größe an, die für das Betriebssystem ausreicht.</p>

### Registerkarte **Eigenschaften**

Geben Sie optional benutzerdefinierte Eigenschafts- und Eigenschaftsgruppeninformationen für die OpenStack-Maschinenkomponente an.

Mithilfe der Registerkarte **Eigenschaften** können Sie benutzerdefinierte Eigenschaften einzeln oder in Gruppen zu der Maschinenkomponente hinzufügen. Mithilfe der Registerkarte **Eigenschaften** können Sie beim Erstellen oder Bearbeiten eines Blueprints auch benutzerdefinierte Eigenschaften und Eigenschaftsgruppen zum gesamten Blueprint hinzufügen. Verwenden Sie dazu die Seite **Neuer Blueprint** bzw. **Blueprint-Eigenschaften**.

Mithilfe der Registerkarte **Benutzerdefinierte Eigenschaften** können Sie Optionen für vorhandene benutzerdefinierte Eigenschaften hinzufügen und konfigurieren. Benutzerdefinierte Einstellungen sind in vRealize Automation enthalten, und Sie können auch Eigenschaftsdefinitionen erstellen.

**Tabelle 4-27. Einstellungen auf der Registerkarte *Eigenschaften* > *Benutzerdefinierte Eigenschaften***

Einstellung	Beschreibung
<b>Name</b>	Geben Sie den Namen einer benutzerdefinierten Eigenschaft ein oder wählen Sie aus dem Dropdown-Menü eine verfügbare benutzerdefinierte Eigenschaft aus. Geben Sie beispielsweise für die benutzerdefinierte Eigenschaft den Namen <code>Machine.SSH</code> ein, um anzugeben, ob mithilfe dieses Blueprints bereitgestellte Maschinen SSH-Verbindungen zulassen. Eigenschaften werden nur dann im Dropdown-Menü angezeigt, wenn Ihr Mandantenadministrator oder Fabric-Administrator Eigenschaftsdefinitionen erstellt hat.
<b>Wert</b>	Geben Sie einen Wert ein bzw. bearbeiten Sie einen Wert, der mit der benutzerdefinierten Eigenschaft verknüpft werden soll. Legen Sie beispielsweise den Wert auf <code>true</code> fest, um berechtigten Benutzern zu ermöglichen, sich via SSH mit Maschinen zu verbinden, die mithilfe Ihres Blueprints bereitgestellten Maschinen zu verbinden wurden.
<b>Verschlüsselt</b>	Sie können den Eigenschaftswert verschlüsseln. Beispielsweise für den Fall, dass es sich bei dem Wert um ein Kennwort handelt.
<b>Überschreibbar</b>	Sie können festlegen, dass der Eigenschaftswert von der nächsten Person, die die Eigenschaft verwendet, oder der nachfolgenden Person überschrieben werden darf. In der Regel handelt es sich bei dieser Person um einen anderen Architekten. Wenn Sie jedoch „In Anforderung anzeigen“ auswählen, können Ihre Unternehmensbenutzer Eigenschaftswerte anzeigen oder bearbeiten, wenn sie Katalogelemente anfordern.
<b>In Anforderung anzeigen</b>	Wenn Sie Ihren Endbenutzern den Namen und den Wert der Eigenschaft anzeigen möchten, können Sie festlegen, dass beim Anfordern einer Maschinenbereitstellung die Eigenschaft im Anforderungsformular angezeigt wird. Sie müssen „Überschreibbar“ auch auswählen, wenn die Benutzer einen Wert eingeben können sollen.

Mithilfe der Registerkarte **Eigenschaftsgruppen** können Sie Eigenschaften für vorhandene benutzerdefinierte Eigenschaftsgruppen hinzufügen und konfigurieren. Sie können eigene Eigenschaftsgruppen erstellen oder Eigenschaftsgruppen verwenden, die für Sie erstellt wurden.

**Tabelle 4-28. Einstellungen auf der Registerkarte *Eigenschaften* > *Eigenschaftsgruppen***

Einstellung	Beschreibung
<b>Name</b>	Wählen Sie aus dem Dropdown-Menü eine verfügbare Sicherheitsgruppe aus.
<b>Nach oben und Nach unten</b>	Steuern Sie die Rangfolge der aufgelisteten Eigenschaftsgruppen in absteigender Reihenfolge. Die zuerst aufgelistete Eigenschaftsgruppe hat Vorrang vor der als nächstes aufgelisteten Eigenschaftsgruppe etc.

**Tabelle 4-28. Einstellungen auf der Registerkarte **Eigenschaften > Eigenschaftsgruppen** (Fortsetzung)**

Einstellung	Beschreibung
<b>Eigenschaften anzeigen</b>	Zeigen Sie die benutzerdefinierten Eigenschaften in der ausgewählten Eigenschaftsgruppe an.
<b>Zusammengeführte Eigenschaften anzeigen</b>	Zeigen Sie alle benutzerdefinierten Eigenschaften in den aufgelisteten Eigenschaftsgruppen in der Reihenfolge an, in der sie in der Liste der Eigenschaftsgruppen angezeigt werden. Wenn dieselbe Eigenschaft in mehr als einer Eigenschaftsgruppe angezeigt wird, wird der Eigenschaftsname nur einmal in der Liste angezeigt, je nach dem, wann sie in der Liste zum ersten Mal auftritt.

### Fehlerbehebung bei Blueprints für Klone und verknüpfte Klone

Beim Erstellen eines Klon- bzw. verknüpften Klon-Blueprints fehlen Maschinen oder Vorlagen. Wenn Sie mit Ihrem freigegebenen Klon-Blueprint Maschinen anfordern, schlägt die Bereitstellung von Maschinen fehl.

#### Problem

Beim Arbeiten mit Klon- bzw. verknüpften Klon-Blueprints tritt möglicherweise eines der folgenden Probleme auf:

- Beim Erstellen eines verknüpften Klon-Blueprints werden in der Liste keinerlei Maschinen zum Klonen angezeigt oder die zu klonende Maschine wird nicht angezeigt.
- Beim Erstellen eines Klon-Blueprints werden in der Vorlagenliste keinerlei Vorlagen zum Klonen angezeigt oder die zu klonende Vorlage wird nicht angezeigt.
- Beim Anfordern von Maschinen mit Ihrem freigegebenen Klon-Blueprint schlägt die Bereitstellung fehl.
- Aufgrund des Zeitpunkts der Datenerfassung wird den Benutzern eine Vorlage, die entfernt wurde, noch angezeigt, wenn sie verknüpfte Klon-Blueprints erstellen oder bearbeiten.

#### Ursache

Für Probleme mit allgemeinen und verknüpften Klon-Blueprints gibt es mehrere mögliche Ursachen.

**Tabelle 4-29. Ursachen für Probleme mit allgemeinen und verknüpften Klon-Blueprints**

Problem	Ursache	Lösung
Fehlende Maschinen	Sie können verknüpfte Klon-Blueprints nur mit Maschinen erstellen, die Sie als Mandantenadministrator oder Business-Gruppenmanager verwalten.	<p>Ein Benutzer in Ihrer Mandanten- oder Business-Gruppe muss eine vSphere-Maschine anfordern. Wenn Sie über die entsprechenden Rollen verfügen, können Sie dies selbst durchführen.</p> <p>In diesem Dialogfeld werden auch nicht verwaltete Maschinen angezeigt.</p> <p>Verwaltete Maschinen wurden möglicherweise importiert. Es ist nicht erforderlich, dass Maschinen über vRealize Automation bereitgestellt werden, um in diesem Dialogfeld angezeigt zu werden.</p>
Fehlende Vorlagen	Die Datenerfassung ist an einem bestimmten Endpoint fehlgeschlagen oder es sind keine Endpoints für die Plattform der Komponente verfügbar.	<ul style="list-style-type: none"> <li>■ Wenn sich Ihre Endpoints im Cluster befinden und mehrere Computing-Ressourcen enthalten, stellen Sie sicher, dass Ihr IaaS-Administrator den Cluster mit den Vorlagen zu Ihrer Fabric-Gruppe hinzugefügt hat.</li> <li>■ Stellen Sie bei neuen Vorlagen sicher, dass die IT-Abteilung die Vorlagen auf demselben Cluster platziert hat, der in Ihrer Fabric-Gruppe enthalten ist.</li> </ul>
Bereitstellungsfehler bei einem freigegebenen Blueprint	Bei Blueprints ist keine Validierung verfügbar, um sicherzustellen, dass die ausgewählte Vorlage in der Reservierung vorhanden ist, die für die Bereitstellung einer Maschine mit Ihrem freigegebenen Klon-Blueprint verwendet wird.	Sie sollten die Verwendung von Berechtigungen in Betracht ziehen, um den Blueprint auf Benutzer einzuschränken, die auf der Computing-Ressource mit der Vorlage über Reservierungen verfügen.
Bereitstellungsfehler mit einem Gast-Agent	Die virtuelle Maschine wird möglicherweise sofort neu gestartet, nachdem die Anpassung des Gastbetriebssystems abgeschlossen wurde, jedoch die Arbeitselemente des Gast-Agent noch nicht abgeschlossen wurden. Dies führt dazu, dass die Bereitstellung fehlschlägt. Zum Erhöhen der Zeitverzögerung können Sie die benutzerdefinierte Eigenschaft <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> verwenden.	Stellen Sie sicher, dass Sie die benutzerdefinierte Eigenschaft <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> hinzugefügt haben. Für diesen Wert ist das Format HH:MM:SS erforderlich. Wenn dieser Wert nicht festgelegt wird, wird der Standardwert von einer Minute (00:01:00) verwendet.

**Tabelle 4-29. Ursachen für Probleme mit allgemeinen und verknüpften Klon-Blueprints (Fortsetzung)**

Problem	Ursache	Lösung
Bereitstellung mit einem verknüpften Klon schlägt bei Verwendung von SDRS fehl	Wenn Sie die Bereitstellung mit einem verknüpften Klon (Linked Clone) und SDRS verwenden, muss sich die neue Maschine auf demselben Cluster befinden. Ein Bereitstellungsfehler tritt auf, wenn sich die Festplatten der Quellmaschine auf einem bestimmten Cluster befinden und Sie die Bereitstellung einer Maschine auf einem anderen Cluster anfordern.	Wenn Sie die Bereitstellung mit einem verknüpften Klon und SDRS verwenden, müssen Sie Maschinen im selben Cluster wie die Quelle des verknüpften Klon bereitstellen. Die Bereitstellung in einem anderen Cluster ist nicht zulässig.
Die Bereitstellung von Klon- oder verknüpften Klon-Blueprints schlägt fehl, da die Vorlage, auf der der Klon basiert, nicht gefunden werden konnte	Es ist nicht möglich, Maschinen über einen Blueprint bereitzustellen, der von einer nicht mehr vorhandenen Vorlage geklont wurde. vRealize Automation führt die Datenerfassung regelmäßig aus. Der Standard ist alle 24 Stunden. Wenn eine Vorlage entfernt wurde, wird die Änderung bis zur nächsten Datenerfassung nicht angezeigt. Aus diesem Grund ist es möglich, einen Blueprint zu erstellen, der auf einer nicht vorhandenen Vorlage basiert.	Definieren Sie den Blueprint neu, indem Sie eine vorhandene Vorlage verwenden und anschließend die Bereitstellung anfordern. Als Vorsichtsmaßnahme und soweit anwendbar, können Sie die Datenerfassung ausführen, bevor Sie den Klon- oder verknüpften Klon-Blueprint definieren.

## Hinzufügen von Netzwerk- und Sicherheitseigenschaften zu einer Maschinenkomponente

Nicht-vSphere-Maschinenkomponenten verfügen nicht über die Registerkarten „Netzwerk“ und „Sicherheit“. Mithilfe von benutzerdefinierten Eigenschaften können Sie Netzwerk- und Sicherheitsoptionen zu Nicht-vSphere-Maschinenkomponenten auf der Design-Arbeitsfläche des Blueprints hinzufügen.

Die **Netzwerk- und Sicherheitskomponenten** sind ausschließlich für die Verwendung mit vSphere-Maschinenkomponenten verfügbar.

Für Maschinenkomponenten, die nicht über eine Registerkarte **Netzwerk** oder **Sicherheit** verfügen, können Sie benutzerdefinierte Eigenschaften für Netzwerk und Sicherheit wie z. B. `VirtualMachine.Network0.Name` zu deren Registerkarte **Eigenschaften** in der Blueprint-Arbeitsfläche hinzufügen. Die Eigenschaften des NSX-Lastausgleichsdiensts betreffen nur vSphere-Maschinen.

Benutzerdefinierte Eigenschaften können einzeln oder im Rahmen einer vorhandenen Eigenschaftsgruppe definiert werden, indem Sie die Registerkarte **Eigenschaften** beim Konfigurieren einer Maschinenkomponente in der Design-Arbeitsfläche verwenden. Die von Ihnen für eine Maschinenkomponente definierten benutzerdefinierten Eigenschaften betreffen Maschinen dieses Typs, die über den Blueprint bereitgestellt werden.

Informationen zu den verfügbaren benutzerdefinierten Eigenschaften finden Sie unter *Referenz für benutzerdefinierte Eigenschaften*.

## Szenario: Erstellen eines vSphere CentOS-Blueprints zum Klonen in Rainpole

Mit Ihren Rechten als IaaS-Architekt erstellen und veröffentlichen Sie einen Basis-Blueprint, um vSphere CentOS-Maschinen zu klonen.



Nach der Veröffentlichung Ihres Blueprints kann dieser von anderen Architekten als Komponente in neuen Blueprints wiederverwendet werden. Niemand kann Ihren Blueprint im Katalog sehen oder anfordern, es sei denn, Sie stellen ihn mit Ihren Mandantenadministratorrechten zur Verfügung.

## Vorgehensweise

### 1 Szenario: Erstellen eines Blueprints für Ihre Rainpole-Maschinenkomponente

Mit Ihren Rechten als IaaS-Architekt erstellen Sie einen Blueprint und konfigurieren den Namen und die Beschreibung für Ihren CentOS-Maschinen-Blueprint von vSphere. Ein eindeutiger Bezeichner wird auf den Blueprint angewendet, sodass Sie mit Blueprints programmatisch interagieren können oder bei Bedarf Eigenschaftsbindungen erstellen können. Wenn Sie möchten, dass Benutzer über eine gewisse Flexibilität hinsichtlich ihrer Blueprint-Leases verfügen, können Sie den Blueprint so konfigurieren, dass Benutzer ihre Leasedauer für bis zu einem Monat auswählen können.

### 2 Szenario: Konfigurieren von allgemeinen Details für Ihre Rainpole-Maschinenkomponente

Mit Ihren Rechten als IaaS-Architekt ziehen Sie eine vSphere-Maschinenkomponente auf die Design-Arbeitsfläche und konfigurieren die allgemeinen Details für Maschinen, die unter Verwendung Ihres Blueprints bereitgestellt wurden.

### 3 Szenario: Angeben von Build-Informationen für Ihre Rainpole-Maschinenkomponente

Mit Ihren Rechten als IaaS-Architekt konfigurieren Sie Ihren Blueprint zum Klonen von Maschinen aus der CentOS-Vorlage, die Sie in vSphere erstellt haben.

### 4 Szenario: Konfigurieren von Maschinenressourcen für Rainpole-Maschinen

Mit den Berechtigungen eines IaaS-Architekts statten Sie Benutzer mit minimalen und maximalen Parametern für den Arbeitsspeicher sowie mit der Anzahl an zulässigen CPUs aus. Damit werden nicht unnötig viele Ressourcen in Anspruch genommen und es wird den Anforderungen Ihrer Benutzer entsprochen.

## Szenario: Erstellen eines Blueprints für Ihre Rainpole-Maschinenkomponente

Mit Ihren Rechten als IaaS-Architekt erstellen Sie einen Blueprint und konfigurieren den Namen und die Beschreibung für Ihren CentOS-Maschinen-Blueprint von vSphere. Ein eindeutiger Bezeichner wird auf den Blueprint angewendet, sodass Sie mit Blueprints programmatisch interagieren können oder bei Bedarf Eigenschaftsbindungen erstellen können. Wenn Sie möchten, dass Benutzer über eine gewisse Flexibilität hinsichtlich ihrer Blueprint-Leases verfügen, können Sie den Blueprint so konfigurieren, dass Benutzer ihre Leasedauer für bis zu einem Monat auswählen können.

**Vorgehensweise**

- 1 Wählen Sie **Design > Blueprints** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Geben Sie **CentOS auf vSphere** in das Textfeld **Name** ein.
- 4 Überprüfen Sie den generierten eindeutigen Bezeichner.

Sie können dieses Feld jetzt bearbeiten, aber nach der Speicherung des Blueprints kann es nicht mehr geändert werden. Bezeichner sind innerhalb Ihres Mandanten permanent und eindeutig, weshalb Sie damit programmgesteuert mit Blueprints interagieren und Eigenschaftsbindungen erstellen können.

Das Feld „Bezeichner“ wird automatisch basierend auf dem von Ihnen eingegebenen Namen aufgefüllt.

- 5 Geben Sie **Goldstandard CentOS-Maschinenkonfiguration** in das Textfeld **Beschreibung** ein.
- 6 Konfigurieren Sie einen Lease-Bereich, aus dem Benutzer auswählen können, indem Sie **1** in das Textfeld **Minimum** und **30** in das Textfeld **Maximum** eingeben.
- 7 Klicken Sie auf **OK**.

**Weiter**

Sie ziehen eine vSphere-Maschinenkomponente in die Arbeitsfläche und konfigurieren sie für das Klonen der CentOS-Vorlage, die Sie in vSphere erstellt haben.

**Szenario: Konfigurieren von allgemeinen Details für Ihre Rainpole-Maschinenkomponente**

Mit Ihren Rechten als IaaS-Architekt ziehen Sie eine vSphere-Maschinenkomponente auf die Design-Arbeitsfläche und konfigurieren die allgemeinen Details für Maschinen, die unter Verwendung Ihres Blueprints bereitgestellt wurden.

Nur IaaS-Architekten können Maschinenkomponenten konfigurieren. Anwendungs- und Software-Architekten sind nur berechtigt, Maschinenkomponenten zu verwenden, indem sie die von Ihnen erstellten Maschinen-Blueprints wiederverwenden.

**Vorgehensweise**

- 1 Klicken Sie auf die Kategorie **Maschinentypen** im linken Navigationsfenster.  
Maschinenkomponententypen werden im unteren Fensterbereich angezeigt.
- 2 Ziehen Sie eine vSphere-Maschinenkomponente und legen Sie sie auf der Arbeitsfläche ab.
- 3 Geben Sie **Goldstandard CentOS-Maschine** in das Textfeld **Beschreibung** ein.
- 4 Wählen Sie **Gruppenstandardwert verwenden** aus dem Dropdown-Menü **Maschinenpräfix** aus.

Wenn Sie diese Blueprints in andere Umgebungen importieren möchten, können Sie bei Auswahl des Gruppenstandardwerts des angegebenen Rainpole-Präfix Ihren Blueprint nicht mehr zum Arbeiten mit einem möglicherweise nicht mehr verfügbaren Maschinen-Präfix konfigurieren.

**Weiter**

Sie konfigurieren die Maschinenkomponente zum Klonen von Maschinen aus der von Ihnen erstellten CentOS-Vorlage.

**Szenario: Angeben von Build-Informationen für Ihre Rainpole-Maschinenkomponente**

Mit Ihren Rechten als IaaS-Architekt konfigurieren Sie Ihren Blueprint zum Klonen von Maschinen aus der CentOS-Vorlage, die Sie in vSphere erstellt haben.

Sie konfigurieren Ihre Maschinenkomponenten für die Durchführung der Klonaktion und wählen die Vorlage aus, die Sie als Objekt für den Klon erstellt haben. Sie geben die Anpassungsspezifikation an, die Sie erstellt haben, um mögliche Konflikte zu vermeiden, die aus der Bereitstellung mehrerer virtueller Maschinen mit identischen Einstellungen entstehen können.

**Vorgehensweise**

- 1 Klicken Sie auf die Registerkarte **Build-Informationen**.
- 2 Wählen Sie aus dem Dropdown-Menü **Blueprint-Typ** aus, ob über diesen Blueprint bereitgestellte Maschinen als „Desktop“ oder „Server“ klassifiziert werden.  
Diese Informationen dienen nur zu Statistik- und Lizenzierungszwecken.
- 3 Wählen Sie aus dem Dropdown-Menü **Aktion** den Eintrag **Klonen** aus.
- 4 Wählen Sie **CloneWorkflow** aus dem Dropdown-Menü **Bereitstellungsworkflow** aus.
- 5 Klicken Sie auf das Symbol **Durchsuchen** neben dem Textfeld **Klonen von**.
- 6 Wählen Sie **Rainpole\_centos\_63\_x86** aus, um Maschinen aus der in vSphere erstellen Vorlage zu klonen.
- 7 Klicken Sie auf **OK**.
- 8 Geben Sie **Linux** in das Textfeld **Anpassungsspezifikation** ein, um die in vSphere erstellte Anpassungsspezifikation zu verwenden.

---

**Hinweis** Bei diesem Wert ist die Groß-/Kleinschreibung zu beachten.

---

**Weiter**

Sie konfigurieren CPU-, Arbeitsspeicher- und Speichereinstellungen für Maschinen, die Sie mit Ihrem Blueprint bereitgestellt haben.

**Szenario: Konfigurieren von Maschinenressourcen für Rainpole-Maschinen**

Mit den Berechtigungen eines IaaS-Architekten stellen Sie Benutzer mit minimalen und maximalen Parametern für den Arbeitsspeicher sowie mit der Anzahl an zulässigen CPUs aus. Damit werden nicht unnötig viele Ressourcen in Anspruch genommen und es wird den Anforderungen Ihrer Benutzer entsprochen.



Softwarearchitekten und Anwendungsarchitekten dürfen keine Maschinenkomponenten konfigurieren. Sie können allerdings Blueprints wiederverwenden, in denen Maschinenkomponenten enthalten sind. Wenn Sie die Bearbeitung einer Maschinenkomponente abgeschlossen haben, veröffentlichen Sie Ihren Blueprint, sodass andere Anwendungen Ihren Maschinen-Blueprint wiederverwenden können, um ihre eigenen Katalogelemente zu entwerfen. Der veröffentlichte Blueprint steht auch Katalogadministratoren und Mandantenadministratoren zum Hinzufügen zum Servicekatalog zur Verfügung.

### Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Maschinenressourcen**.
- 2 Geben Sie CPU-Einstellungen für bereitgestellte Maschinen an.
  - a Geben Sie **1** in das Textfeld **Minimalwert** ein.
  - b Geben Sie **4** in das Textfeld **Maximalwert** ein.
- 3 Geben Sie Arbeitsspeichereinstellungen für bereitgestellte Maschinen an.
  - a Geben Sie **1024** in das Textfeld **Minimalwert** ein.  
Dieses Feld wird automatisch basierend auf dem Speicher Ihrer Vorlage aufgefüllt.
  - b Geben Sie **4096** in das Textfeld **Maximalwert** ein.
- 4 Geben Sie Speichereinstellungen für bereitgestellte Maschinen an.  
Einige Speicherinformationen werden basierend auf der Konfiguration Ihrer Vorlage aufgefüllt, Sie können jedoch keinen zusätzlichen Speicher hinzufügen.
  - a Klicken Sie auf das Symbol **Neu** (+).
  - b Geben Sie im Textfeld **Kapazität (GB)** den Wert **10** ein.
  - c Klicken Sie auf **OK**.
- 5 Klicken Sie auf **Beenden**.
- 6 Wählen Sie die Zeile aus, die CentOS unter vSphere enthält, und klicken Sie auf **Veröffentlichen**.

Sie haben einen katalogbereiten Blueprint erstellt, um den Benutzern geklonte vSphere-CentOS-Maschinen zur Verfügung zu stellen und um in anderen Blueprints als Standard für CentOS-Maschinen verwendet zu werden.

### Weiter

Erstellen Sie mit Ihren Mandantenadministratorrechten einen Katalogdienst für Architekten, um deren Blueprints zu validieren. Veröffentlichen Sie Ihr Maschinen-Blueprint „CentOS unter vSphere“ als ein Katalogelement und fordern Sie es zwecks Validierung Ihrer Arbeit an.

## Szenario: Ändern Ihrer Rainpole-Maschine in eine Basis für das Übermitteln von Softwarekomponenten

Mit Ihren Rechten als IaaS-Architekt erstellen Sie einen Blueprint, der Softwarekomponenten unterstützt, indem ein Snapshot Ihrer bereitgestellten Maschine als die Referenzmaschine verwendet wird, von der geklont wird. Da Sie Softwarekomponenten unterstützen möchten, installieren Sie den Gast-Agent und den Bootstrap-Agent auf Ihrer bereitgestellten Maschine, bevor Sie den Snapshot aufnehmen.



### Vorgehensweise

#### 1 [Szenario: Installieren des Gast-Agents und des Software-Bootstrap-Agents auf der Rainpole-Maschine](#)

Melden Sie sich unter Verwendung Ihrer Berechtigungen für Business-Gruppenmanager bei der Rainpole001-Maschine an, die Sie als Testbenutzer bereitgestellt haben. Sie installieren den Gast-Agent und den Software -Bootstrap-Agent auf der Maschine, um die Bereitstellung von Software vorzubereiten. Wenn Sie damit fertig sind, erstellen Sie einen Snapshot der Maschine, der als Basis für das Klonen von Maschinen verwendet wird für die Verwendung mit Software-Komponenten.

#### 2 [Szenario: Erstellen eines verknüpften Klon-Blueprints basierend auf Ihrem Rainpole-Snapshot](#)

Mit Ihren Rechten als IaaS-Architekt möchten Sie Softwarearchitekten speicherplatzeffiziente Kopien der von Ihnen vorbereiteten CentOS-Maschine bereitstellen.

### Szenario: Installieren des Gast-Agents und des Software -Bootstrap-Agents auf der Rainpole-Maschine

Melden Sie sich unter Verwendung Ihrer Berechtigungen für Business-Gruppenmanager bei der Rainpole001-Maschine an, die Sie als Testbenutzer bereitgestellt haben. Sie installieren den Gast-Agent und den Software -Bootstrap-Agent auf der Maschine, um die Bereitstellung von Software vorzubereiten. Wenn Sie damit fertig sind, erstellen Sie einen Snapshot der Maschine, der als Basis für das Klonen von Maschinen verwendet wird für die Verwendung mit Software-Komponenten.

### Vorgehensweise

- 1 Wählen Sie **Elemente > Maschinen** aus.
- 2 Klicken Sie auf das Element „CentOS in vSphere“, um die Elementdetails anzuzeigen.
- 3 Klicken Sie im Menü „Aktionen“ auf der rechten Seite auf **Mit Remote-Konsole verbinden**.
- 4 Melden Sie sich an der Maschine als Root-Benutzer an.

- 5 Laden Sie das Installationsskript aus der vRealize Automation-Appliance herunter.

```
wget https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

Wenn in Ihrer Umgebung selbst signierte Zertifikate verwendet werden, müssen Sie möglicherweise die wget-Option `--no-check-certificate` verwenden. Beispiel:

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

- 6 Sorgen Sie dafür, dass das Skript `prepare_vra_template.sh` ausgeführt werden kann.

```
chmod +x prepare_vra_template.sh
```

- 7 Führen Sie das Installationsprogramm-Skript `prepare_vra_template.sh` aus.

```
./prepare_vra_template.sh
```

Sie können den Hilfebefehl `./prepare_vra_template.sh --help` ausführen, um Informationen zu nicht interaktiven Optionen und erwarteten Werten zu erhalten.

- 8 Folgen Sie den Eingabeaufforderungen, um die Installation abzuschließen.

Wenn die Installation erfolgreich abgeschlossen wurde, wird eine Bestätigungsmeldung angezeigt. Werden in der Konsole eine Fehlermeldung und Protokolle angezeigt, beheben Sie die Fehler und führen Sie das Installationsprogramm-Skript erneut aus.

- 9 Wechseln Sie wieder zur vRealize Automation-Konsole und erstellen Sie den Snapshot.

- a Klicken Sie im Menü „Aktionen“ auf der rechten Seite auf **Snapshot erstellen** und befolgen Sie die Anweisungen.
- b Klicken Sie auf die Registerkarte **Snapshots**, um den Prozess zu überwachen.

Sie haben den Software-Bootstrap-Agent und den Gast-Agent installiert. Damit kann der Snapshot als die Klonbasis in Blueprints verwendet werden, die Softwarekomponenten enthalten.

### Szenario: Erstellen eines verknüpften Klon-Blueprints basierend auf Ihrem Rainpole-Snapshot

Mit Ihren Rechten als IaaS-Architekt möchten Sie Softwarearchitekten speicherplatzeffiziente Kopien der von Ihnen vorbereiteten CentOS-Maschine bereitstellen.

Als Ausgangspunkt kopieren Sie den vorhandenen Blueprint „CentOS auf vSphere“ und bearbeiten die Kopie, um verknüpfte Klonkopien des vorbereiteten Snapshots zu erstellen. Verknüpfte Klone verwenden eine Kette von Delta-Festplatten, um Unterschiede zu einer übergeordneten Maschine zu verfolgen. Sie werden schnell bereitgestellt, reduzieren Speicherkosten und eignen sich ideal zur Verwendung, wenn die Leistung keine hohe Priorität hat.

#### Vorgehensweise

- 1 Wählen Sie **Design > Blueprints** aus.

- 2 Wählen Sie die Zeile mit „CentOS auf vSphere“ aus und klicken Sie auf **Kopieren**.  
Sie haben eine unabhängige Kopie des Maschinen-Blueprints „CentOS auf vSphere“ erstellt.
- 3 Geben Sie **CentOS für Softwaretests** in das Textfeld **Name** ein.
- 4 Geben Sie **Speicherplatzeffizientes vSphere CentOS für Softwaretests** in das Textfeld **Beschreibung** ein.
- 5 Klicken Sie auf **OK**.
- 6 Wählen Sie die Maschinenkomponente auf der Arbeitsfläche aus, um die Details zu bearbeiten.
- 7 Klicken Sie auf die Registerkarte **Build-Informationen**.
- 8 Wählen Sie **Verknüpfter Klon** im Dropdown-Menü **Aktion** aus.
- 9 Klicken Sie auf das Symbol **Durchsuchen** neben dem Textfeld **Klonen von**.
- 10 Wählen Sie die bereitgestellte Maschine **Rainpole001** aus, auf der Sie die Software-Bootstrap- und Gast-Agents installiert haben.
- 11 Wählen Sie Ihren Snapshot aus dem Dropdown-Menü **Von Snapshot klonen** aus.
- 12 Klicken Sie auf **Beenden**.
- 13 Wählen Sie die Zeile mit „CentOS für Softwaretests“ aus und klicken Sie auf **Veröffentlichen**.

Sie haben einen verknüpften Klon-Blueprint erstellt, den Sie und Ihre Architekten zur Bereitstellung von Software auf CentOS-Maschinen verwenden können.

#### Weiter

Verwenden Sie Ihre Rechte als Softwarearchitekt, um eine Softwarekomponente zum Installieren von MySQL zu erstellen.

## Hinzufügen der Unterstützung von RDP-Verbindungen zu Ihren Windows-Maschinen-Blueprints

Wenn Ihre Katalogadministratoren in der Lage sein sollen, den Benutzern die Berechtigung für die Aktion „Verbindungsherstellung mithilfe von RDP“ für Ihre Windows-Blueprints zu erteilen, müssen Sie die benutzerdefinierten RDP-Eigenschaften zu Ihrem Maschinen-Blueprint hinzufügen und auf die von Ihrem Systemadministrator vorbereitete benutzerdefinierte RDP-Datei verweisen.

---

**Hinweis** Wenn Ihr Fabric-Administrator eine Eigenschaftsgruppe erstellt, die die erforderlichen benutzerdefinierten Eigenschaften enthält, und Sie diese in Ihren Blueprint einbeziehen, müssen Sie die benutzerdefinierten Eigenschaften nicht einzeln zum Blueprint hinzufügen.

---

#### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** oder **Business-Gruppenmanager** an.

- Rufen Sie den Namen der benutzerdefinierten RDP-Datei ab, die Ihr Systemadministrator für Sie erstellt hat. Siehe [Erstellen einer benutzerdefinierten RDP-Datei zur Unterstützung von RDP-Verbindungen für bereitgestellte Maschinen](#).
- Erstellen Sie mindestens einen Windows-Maschinen-Blueprint.

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Blueprints** aus.
- 2 Zeigen Sie auf den zu aktualisierenden Blueprint und klicken Sie auf **Bearbeiten**.
- 3 Wählen Sie die Maschinenkomponente auf der Arbeitsfläche aus, um die Details zu bearbeiten.
- 4 Klicken Sie auf die Registerkarte **Eigenschaften**.
- 5 Klicken Sie auf die Registerkarte **Benutzerdefinierte Eigenschaften**.
- 6 Konfigurieren Sie die RDP-Einstellungen.
  - a Klicken Sie auf **Neue Eigenschaft**.
  - b Geben Sie im Textfeld **Name** die Namen der benutzerdefinierten RDP-Eigenschaften sowie im Textfeld **Wert** die entsprechenden Werte ein.

Option	Beschreibung und Wert
(Erforderlich)RDP.File.Name	Gibt eine RDP-Datei an, aus der Einstellungen bezogen werden sollen, wie beispielsweise My_RDP_Settings.rdp. Diese Datei muss im Unterverzeichnis Website\Rdp des Installationsverzeichnisses von vRealize Automation gespeichert sein.
(Erforderlich) VirtualMachine.Rdp.SettingN	Konfiguriert bestimmte RDP-Einstellungen. N ist eine eindeutige Zahl zur Unterscheidung der RDP-Einstellungen. Um beispielsweise die Authentifizierungsebene so festzulegen, dass keine Authentifizierung erforderlich ist, definieren Sie die benutzerdefinierte Eigenschaft VirtualMachine.Rdp.Setting1 und legen Sie deren Wert auf „authentication level:i:3“ fest. Verwenden Sie diese Eigenschaft, um einen RDP-Link zum Angeben von Einstellungen zu öffnen.  Eine Liste der verfügbaren Einstellungen und die zugehörige korrekte Syntax finden Sie in der Microsoft Windows RDP-Dokumentation.
VirtualMachine.Admin.NameCompletion	Gibt den Domänennamen an, der in den vollqualifizierten Domänennamen der Maschine einbezogen werden soll, den die RDP- oder SSH-Dateien für die Benutzeroberflächenoptionen <b>Verbindungsherstellung mithilfe von RDP</b> oder <b>Verbindungsherstellung mithilfe von SSH</b> generieren. Legen Sie beispielsweise „myCompany.com“ als Wert fest, um den vollqualifizierten Domänennamen my-machine-name.myCompany.com in der RDP- oder SSH-Datei zu generieren.

- c Klicken Sie auf **Speichern**.

- 7 Wählen Sie die Zeile aus, in der Ihr Blueprint vorhanden ist, und klicken Sie auf **Veröffentlichen**.

Ihre Katalogadministratoren können Benutzern die Berechtigung für die Aktion „Verbindungsherstellung mithilfe von RDP“ für über Ihren Blueprint bereitgestellte Maschinen erteilen. Wenn Benutzer nicht über die Berechtigung für diese Aktion verfügen, können sie keine Verbindung mithilfe von RDP herstellen.

## Szenario: Hinzufügen der Active Directory-Bereinigung zu Ihrem CentOS-Blueprint

Als IaaS-Architekt möchten Sie vRealize Automation so konfigurieren, dass Ihre Active Directory-Umgebung immer dann bereinigt wird, wenn bereitgestellte Maschinen aus Ihren Hypervisoren entfernt werden. Deshalb bearbeiten Sie den vorhandenen vSphere CentOS-Blueprint, um das Active Directory-Bereinigungs-Plug-In zu konfigurieren.

Mit dem Active Directory-Bereinigungs-Plug-In können Sie festlegen, dass die folgenden Active Directory-Kontoaktionen ausgeführt werden, wenn eine Maschine aus einem Hypervisor gelöscht wird:

- AD-Konto löschen
- AD-Konto deaktivieren
- AD-Konto umbenennen
- AD-Konto in eine andere AD-Organisationseinheit (Organizational Unit, OU) verschieben

### Voraussetzungen

---

**Hinweis** Diese Informationen gelten für Amazon Web Services nicht.

---

- Melden Sie sich an der vRealize Automation-Konsole als **Infrastrukturarchitekt** an.
- Erfassen Sie die folgenden Informationen zu Ihrer Active Directory-Umgebung:
  - Ein Benutzername und ein Kennwort für ein Active Directory-Konto mit den erforderlichen Rechten zum Löschen, Deaktivieren, Umbenennen oder Verschieben von AD-Konten. Der Benutzername muss im Format Domäne\Benutzername angegeben werden.
  - (Optional) Der Name der OU, zu der gelöschte Maschinen verschoben werden sollen.
  - (Optional) Das Präfix zum Anhängen an gelöschte Maschinen.
- Erstellen Sie einen Maschinen-Blueprint. Siehe [Szenario: Erstellen eines vSphere CentOS-Blueprints zum Klonen in Rainpole](#).

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Blueprints** aus.
- 2 Zeigen Sie auf Ihren **CentOS in vSphere**-Blueprint und klicken Sie auf **Bearbeiten**.
- 3 Wählen Sie die Maschinenkomponente in der Arbeitsfläche aus, um die Registerkarte „Details“ anzuzeigen.
- 4 Klicken Sie auf die Registerkarte **Eigenschaften**.
- 5 Klicken Sie auf die Registerkarte **Benutzerdefinierte Eigenschaften**, um das Active Directory-Bereinigungs-Plug-In zu konfigurieren.
  - a Klicken Sie auf **Neue Eigenschaft**.
  - b Geben Sie `Plugin.AdMachineCleanup.Execute` im Textfeld **Name** ein.

- c Geben Sie **true** im Textfeld **Wert** ein.
  - d Klicken Sie auf das Symbol **Speichern** (✓).
- 6 Konfigurieren Sie das Active Directory-Bereinigungs-Plug-In durch Hinzufügen benutzerdefinierter Eigenschaften.

Option	Beschreibung und Wert
<code>Plugin.AdMachineCleanup.UserName</code>	Geben Sie im Textfeld <b>Wert</b> den Benutzernamen des Active Directory-Kontos ein. Dieser Benutzer benötigt ausreichende Rechte zum Löschen, Deaktivieren, Verschieben und Umbenennen von Active Directory-Konten. Der Benutzername muss im Format Domäne\Benutzername angegeben werden.
<code>Plugin.AdMachineCleanup.Password</code>	Geben Sie im Textfeld <b>Wert</b> das Kennwort für den Benutzernamen des Active Directory-Kontos ein.
<code>Plugin.AdMachineCleanup.Delete</code>	Legen Sie diese Eigenschaft auf „True“ fest, um die Konten gelöschter Maschinen zu entfernen, anstatt sie zu deaktivieren.
<code>Plugin.AdMachineCleanup.MoveToOu</code>	Verschiebt das Konto von gelöschten Maschinen in eine neue Active Directory-Organisationseinheit. Der Wert ist die Organisationseinheit, in die Sie das Konto verschieben. Für diesen Wert ist das Format <code>ou=OU, dc=dc</code> erforderlich, wie beispielsweise „ou=trash,cn=computers,dc=lab,dc=local“.
<code>Plugin.AdMachineCleanup.Rename-Prefix</code>	Benennt die Konten von gelöschten Maschinen durch Hinzufügen eines Präfixes um. Dieser Wert ist die voranzustellende Präfixzeichenfolge, wie beispielsweise „destroyed_“.

- 7 Klicken Sie auf **OK**.

Wenn über Ihren Blueprint bereitgestellte Maschinen aus Ihrem Hypervisor gelöscht werden, wird Ihre Active Directory-Umgebung aktualisiert.

## Szenario: Anforderern das Angeben des Hostnamens der Maschine erlauben

Als Blueprint-Architekt möchten Sie Ihren Benutzern beim Anfordern Ihrer Blueprints die Auswahl eigener Maschinennamen erlauben. Deshalb bearbeiten Sie den vorhandenen CentOS-vSphere-Blueprint, um die benutzerdefinierte Eigenschaft „Hostname“ hinzuzufügen und so zu konfigurieren, dass die Benutzer bei ihren Anforderungen zur Eingabe eines Werts aufgefordert werden.

**Hinweis** Wenn Ihr Fabric-Administrator eine Eigenschaftsgruppe erstellt, die die erforderlichen benutzerdefinierten Eigenschaften enthält, und Sie diese in Ihren Blueprint einbeziehen, müssen Sie die benutzerdefinierten Eigenschaften nicht einzeln zum Blueprint hinzufügen.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Infrastrukturarchitekt** an.
- Erstellen Sie einen Maschinen-Blueprint. Siehe [Szenario: Erstellen eines vSphere CentOS-Blueprints zum Klonen in Rainpole](#).

### Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Blueprints** aus.

- 2 Zeigen Sie auf Ihren **CentOS in vSphere**-Blueprint und klicken Sie auf **Bearbeiten**.
- 3 Wählen Sie die Maschinenkomponente in der Arbeitsfläche aus, um die Registerkarte „Details“ anzuzeigen.
- 4 Klicken Sie auf die Registerkarte **Eigenschaften**.
- 5 Klicken Sie auf **Neue Eigenschaft**.
- 6 Geben Sie **Hostname** im Textfeld **Name** ein.
- 7 Lassen Sie das Textfeld **Wert** leer.
- 8 Konfigurieren Sie vRealize Automation so, dass Benutzer bei Anforderungen zur Eingabe eines Werts für den Hostnamen aufgefordert werden.
  - a Wählen Sie **Überschreibbar** aus.
  - b Wählen Sie **In Anforderung anzeigen** aus.

Hostnamen müssen eindeutig sein, weshalb Benutzer jeweils immer nur eine Maschine über diesen Blueprint anfordern können.
- 9 Klicken Sie auf das Symbol **Speichern** (✓).
- 10 Klicken Sie auf **OK**.

Benutzer, die eine Maschine über Ihren Blueprint anfordern, müssen einen Hostnamen für ihre Maschine angeben. vRealize Automation überprüft, ob der angegebene Hostname eindeutig ist.

## Szenario: Benutzern das Auswählen von Datacenter-Standorten für regionsübergreifende Bereitstellungen ermöglichen

Als Blueprint-Architekt möchten Sie Benutzern gestatten, zu wählen, ob Maschinen in Ihrer Infrastruktur in Boston oder London bereitgestellt werden. Daher bearbeiten Sie Ihren vorhandenen vSphere CentOS-Blueprint, um die Standortfunktion zu aktivieren.



Sie haben ein Datacenter in London und eines in Boston, und möchten nicht, dass Benutzer in Boston Maschinen Ihrer Londoner Infrastruktur bereitstellen und umgekehrt. Um sicherzustellen, dass Benutzer in Boston die Bereitstellung für Ihre Bostoner Infrastruktur vornehmen, und Benutzer in London die Bereitstellung für Ihre Londoner Infrastruktur vornehmen, sollten Sie den Benutzern erlauben, einen geeigneten Standort für die Bereitstellung auszuwählen, wenn sie Maschinen anfordern.



## Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Infrastrukturarchitekt** an.
- Als Systemadministrator definieren Sie die Datacenter-Standorte. Siehe [Szenario: Hinzufügen von Datacenter-Standorten für regionenübergreifende Bereitstellungen](#).
- Als Fabric-Administrator wenden Sie die entsprechenden Standorte auf Ihre Computing-Ressourcen an. Siehe [Szenario: Anwenden eines Standorts auf eine Computing-Ressource für regionenübergreifende Bereitstellungen](#).
- Erstellen Sie einen Maschinen-Blueprint. Siehe [Szenario: Erstellen eines vSphere CentOS-Blueprints zum Klonen in Rainpole](#).

## Vorgehensweise

- 1 Wählen Sie **Infrastruktur > Blueprints** aus.
- 2 Zeigen Sie auf Ihren **CentOS in vSphere**-Blueprint und klicken Sie auf **Bearbeiten**.
- 3 Wählen Sie die Maschinenkomponente auf der Arbeitsfläche aus, um die Registerkarte **Allgemein** zu öffnen.
- 4 Aktivieren Sie das Kontrollkästchen **Speicherort auf Anforderung anzeigen**.
- 5 Klicken Sie auf **Beenden**.
- 6 Zeigen Sie auf den Blueprint **CentOS auf vSphere** und klicken Sie auf **Veröffentlichen**.

Benutzer in Business-Gruppen werden jetzt zur Auswahl eines Datacenter-Standorts aufgefordert, wenn sie die Bereitstellung einer Maschine aus dem Blueprint anfordern.

## Entwerfen von Maschinen-Blueprints mit NSX -Netzwerk und -Sicherheit

Wenn Sie über eine in vRealize Automation integrierte NSX-Instanz verfügen, können Sie Ihre vSphere-Blueprints für das Zurückgreifen auf NSX für die Netzwerk- und Sicherheitsvirtualisierung konfigurieren.

Wenn Sie die vRealize Automation-Integration mit NSX konfiguriert haben, können Sie Komponenten für Netzwerk, Sicherheit und Lastausgleichsdienst auf der Design-Arbeitsfläche verwenden, um Ihren Blueprint für die Maschinenbereitstellung zu konfigurieren. Sie können auch die folgenden NSX-Netzwerk- und Sicherheitseinstellungen zum gesamten Blueprint hinzufügen, wenn Sie einen neuen Blueprint erstellen oder einen vorhandenen Blueprint bearbeiten.

- Transportzone – Enthält die Netzwerke, die für die bereitgestellte Maschine verwendet werden.
- Reservierungsrichtlinie für Edge- und geroutete Gateways – Verwaltet die Netzwerkkommunikation für die bereitgestellte Maschine.
- Anwendungsisolierung – Lässt nur internen Datenverkehr zwischen Maschinen in der Maschinenbereitstellung zu.

NSX-Einstellungen betreffen nur Typen der vSphere-Maschinenkomponenten.

## Neue Blueprint- und Blueprint-Eigenschaften-Einstellungen mit NSX

Sie können Eigenschaften angeben, die für den gesamten Blueprint gelten. Nach dem Erstellen des Blueprints können Sie diese Eigenschaften im Dialogfeld „Blueprint-Eigenschaften“ bearbeiten.

### Registerkarte Allgemein

Wenden Sie Einstellungen auf den gesamten Blueprint an, einschließlich aller Komponenten, die Sie jetzt oder später hinzufügen möchten.

**Tabelle 4-30. Einstellungen auf der Registerkarte Allgemein**

Einstellung	Beschreibung
<b>Name</b>	Geben Sie einen Namen für Ihren Blueprint ein.
<b>Bezeichner</b>	Das Feld „Bezeichner“ wird automatisch basierend auf dem von Ihnen eingegebenen Namen aufgefüllt. Sie können dieses Feld jetzt bearbeiten, aber nach der Speicherung des Blueprints kann es nicht mehr geändert werden. Bezeichner sind innerhalb Ihres Mandanten permanent und eindeutig, weshalb Sie damit programmgesteuert mit Blueprints interagieren und Eigenschaftsbindungen erstellen können.
<b>Beschreibung</b>	Eine Zusammenfassung Ihres Blueprints für andere Architekten. Diese Beschreibung wird Benutzern auch im Anforderungsformular angezeigt.
<b>Archivierung (Tage)</b>	Sie können einen Archivierungszeitraum für die vorübergehende Speicherung von Bereitstellungen angeben, anstatt Bereitstellungen unmittelbar nach Ablauf der Lease zu löschen. Geben Sie 0 (Standardwert) an, um die Bereitstellung bei Ablauf der Lease zu löschen. Der Archivierungszeitraum beginnt am Tag des Ablaufs der Lease. Wenn der Archivierungszeitraum endet, wird die Bereitstellung gelöscht.
<b>Leasetage: Mindestwert und Maximalwert</b>	Geben Sie einen Mindestwert und einen Maximalwert ein, damit Benutzer eine Leasedauer in diesem Bereich auswählen können. Wenn die Lease endet, wird die Bereitstellung entweder gelöscht oder archiviert.

### Registerkarte NSX-Einstellungen

Wenn Sie VMware NSX konfiguriert und das NSX-Plug-In für vRealize Automation installiert haben, können Sie beim Erstellen oder Bearbeiten eines Blueprints Einstellungen für NSX-Transportzonen, Reservierungsrichtlinien für die Edge und das geroutete Gateway sowie Anwendungsisolierungen angeben. Diese Einstellungen sind auf der Registerkarte **NSX-Einstellungen** auf den Seiten **Neuer Blueprint** und **Blueprint-Eigenschaften** verfügbar.

Informationen über das Konfigurieren von NSX finden Sie im *NSXAdministratorhandbuch*.

**Tabelle 4-31. Einstellungen auf der Registerkarte NSX-Einstellungen**

Einstellung	Beschreibung
<b>Transportzone</b>	<p>Wählen Sie eine vorhandene NSX-Transportzone für das Netzwerk bzw. die Netzwerke aus, die von der bereitgestellten Maschine verwendet werden soll.</p> <p>Eine Transportzone definiert, über welche Cluster sich die Netzwerke erstrecken können. Wenn in einer Reservierung und in einem Blueprint eine Transportzone angegeben ist, müssen die Transportzonenwerte bei der Bereitstellung von Maschinen übereinstimmen.</p> <p>Eine Transportzone ist nur für diejenigen Blueprints erforderlich, die über ein bedarfsgesteuertes Netzwerk verfügen. Bei Sicherheitsgruppen, Sicherheits-Tags und Lastausgleichsdiensten ist die Transportzone optional. Wenn Sie keine Transportzone angeben, wird der Endpoint durch den Standort der Sicherheitsgruppe, des Sicherheits-Tags oder des Netzwerks bestimmt, mit dem bzw. der der Lastausgleichsdienst eine Verbindung herstellt.</p>
<b>Reservierungsrichtlinie für die Edge und das geroutete Gateway</b>	<p>Wählen Sie eine NSX-Reservierungsrichtlinie für die Edge oder das geroutete Gateway aus. Diese Reservierungsrichtlinie gilt für geroutete Gateways und alle Edges, die einen Teil der Bereitstellung darstellen. Pro Bereitstellung ist nur eine Edge vorhanden.</p> <p>Bei gerouteten Netzwerken sind keine Edges vorhanden, doch können Sie eine Reservierungsrichtlinie verwenden, um eine Reservierung mit den für die Bereitstellung von gerouteten Netzwerken zu verwendenden gerouteten Gateways auszuwählen.</p> <p>Wenn vRealize Automation eine Maschine mit NAT- oder gerouteten Netzwerken bereitstellt, wird ein geroutetes Gateway als Netzwerkrouter bereitgestellt. Die Edge oder das geroutete Gateway ist eine Verwaltungsmaschine, die Computing-Ressourcen wie andere virtuelle Maschinen verbraucht, aber die Netzwerkkommunikation aller Maschinen in dieser Bereitstellung verwaltet. Die für die Bereitstellung der Edge oder des gerouteten Gateways verwendete Reservierung bestimmt das externe Netzwerk, das für NAT und die virtuellen IP-Adressen des Lastausgleichsdiensts verwendet wird. Es hat sich bewährt, für Verwaltungsmaschinen wie NSX-Edges separate Verwaltungscluster zu verwenden.</p>
<b>Anwendungsisolierung</b>	<p>Aktivieren Sie das Kontrollkästchen <b>Anwendungsisolierung</b>, um die in NSX konfigurierte Anwendungsisolierungs-Sicherheitsrichtlinie zu verwenden. Die Anwendungsisolierungsrichtlinie wird auf alle vSphere-Maschinenkomponenten im Blueprint angewendet. Optional können Sie NSX-Sicherheitsgruppen und -Tags hinzufügen, sodass vRealize Orchestrator die isolierte Netzwerkkonfiguration öffnen kann und zusätzliche Pfade in die und aus der Anwendungsisolierung zugelassen werden.</p>

## Registerkarte **Eigenschaften**

Benutzerdefinierte Eigenschaften, die Sie auf der Blueprint-Ebene hinzufügen, gelten für den gesamten Blueprint, einschließlich aller Komponenten. Sie können jedoch durch benutzerdefinierte Eigenschaften außer Kraft gesetzt werden, die zu einem späteren Zeitpunkt in der Rangfolge zugewiesen werden. Weitere Informationen zur Rangfolge für benutzerdefinierte Eigenschaften finden Sie unter *Referenz für benutzerdefinierte Eigenschaften*.

**Tabelle 4-32. Einstellungen auf der Registerkarte **Eigenschaften****

Registerkarte	Einstellung	Beschreibung
<b>Eigenschaftsgruppen</b>		Eigenschaftsgruppen sind wiederverwendbare Gruppen von Eigenschaften, mit denen das Hinzufügen benutzerdefinierter Eigenschaften zu Blueprints vereinfacht werden soll. Ihre Mandantenadministratoren und Fabric-Administratoren können Eigenschaften, die häufig gemeinsam verwendet werden, gruppieren, damit die Eigenschaftsgruppe einem Blueprint hinzugefügt werden kann, anstatt benutzerdefinierte Eigenschaften einzeln einzufügen.
	<b>Nach oben verschieben/Nach unten verschieben</b>	Kontrollieren Sie die Rangfolge aller Eigenschaftsgruppen zueinander durch die Priorisierung der Gruppen. Die erste Gruppe in der Liste hat die höchste Priorität, und deren benutzerdefinierte Eigenschaften haben absoluten Vorrang. Sie können die Elemente auch per Drag & Drop neu anordnen.
	<b>Eigenschaften anzeigen</b>	Zeigen Sie die benutzerdefinierten Eigenschaften in der ausgewählten Eigenschaftsgruppe an.
	<b>Zusammengeführte Eigenschaften anzeigen</b>	Wenn eine benutzerdefinierte Eigenschaft in mehreren Eigenschaftsgruppen vorhanden ist, hat der Wert in der Eigenschaftsgruppe mit der höchsten Priorität den Vorrang. Sie können diese zusammengeführten Eigenschaften anzeigen, um die Priorisierung von Eigenschaftsgruppen zu unterstützen.
<b>Benutzerdefinierte Eigenschaften</b>		Anstelle von Eigenschaftsgruppen können Sie auch einzelne benutzerdefinierte Eigenschaften hinzufügen.
	<b>Name</b>	Eine Aufstellung der Namen und Verhaltensweisen benutzerdefinierter Eigenschaften finden Sie unter <i>Referenz für benutzerdefinierte Eigenschaften</i> .
	<b>Wert</b>	Geben Sie den Wert für die benutzerdefinierte Eigenschaft ein.
	<b>Verschlüsselt</b>	Sie können den Eigenschaftswert verschlüsseln. Beispielsweise für den Fall, dass es sich bei dem Wert um ein Kennwort handelt.

**Tabelle 4-32. Einstellungen auf der Registerkarte *Eigenschaften* (Fortsetzung)**

Registerkarte	Einstellung	Beschreibung
	Überschreibbar	Sie können festlegen, dass der Eigenschaftswert von der nächsten Person, die die Eigenschaft verwendet, oder der nachfolgenden Person überschrieben werden darf. In der Regel handelt es sich bei dieser Person um einen anderen Architekten. Wenn Sie jedoch „In Anforderung anzeigen“ auswählen, können Ihre Unternehmensbenutzer Eigenschaftswerte anzeigen oder bearbeiten, wenn sie Katalogelemente anfordern.
	In Anforderung anzeigen	Wenn Sie Ihren Endbenutzern den Namen und den Wert der Eigenschaft anzeigen möchten, können Sie festlegen, dass beim Anfordern einer Maschinenbereitstellung die Eigenschaft im Anforderungsformular angezeigt wird. Sie müssen „Überschreibbar“ auch auswählen, wenn die Benutzer einen Wert eingeben können sollen.

### Anwenden einer NSX -Transportzone auf einen Blueprint

Ein NSX-Administrator kann Transportzonen erstellen, um die Cluster-Verwendung von Netzwerken zu kontrollieren.

Wenn der Blueprint ein On-Demand-Netzwerk enthält, müssen Sie die NSX-Transportzone angeben, die die von der bereitgestellten Maschine verwendeten Netzwerke enthält. In der Reservierung muss dieselbe Transportzone angegeben werden.

### Anwenden einer Reservierungsrichtlinie für NSX oder geroutete Gateways auf einen Blueprint

Sie können eine Reservierungsrichtlinie angeben, um die Netzwerkkommunikation für vom Blueprint bereitgestellte Maschinen zu verwalten. Beim Anfordern der Maschinenbereitstellung werden mithilfe der Reservierungsrichtlinie die Reservierungen gruppiert, die für die Bereitstellung in Betracht kommen. Die Reservierungsrichtlinie für geroutete Gateways wird auch als Edge-Reservierungsrichtlinie bezeichnet.

Jede Reservierung enthält Netzwerkinformationen. Wenn die Maschinen bereitgestellt werden, wird ein Edge Gateway oder geroutetes Gateway als Netzwerkrouter zugeteilt, um die Netzwerkkommunikation für die bereitgestellten Maschinen in der Bereitstellung zu verwalten. Eigenschaften auf Blueprint-Ebene können Sie mithilfe der Seite „Blueprint-Eigenschaften“ hinzufügen oder bearbeiten.

Eine Reservierungsrichtlinie für geroutete Gateways ist optional. Sie bestimmt, welche Reservierung bzw. Reservierungen verwendet werden kann bzw. können, um den NSX Edge für On-Demand-Netzwerk- und On-Demand-Lastausgleichskomponenten, die im Blueprint angegeben sind, bereitzustellen.

Die Auswahl von Reservierungen kontrollieren Sie mithilfe von Reservierungsrichtlinien. Sie wählen eine Reservierungsrichtlinie in der VM-Definition des Blueprints aus und weisen dann diese Richtlinie den Reservierungen zu, die Ihre virtuellen Maschinen verwenden sollen.

Reservierungen können nicht für mehrere Business-Gruppen gemeinsam verwendet werden.

vRealize Automation stellt ein geroutetes Gateway, beispielsweise ein Edge-Services-Gateway (ESG), für NAT-Netzwerke und für Lastausgleichsdienste bereit. Für geroutete Netzwerke nutzt vRealize Automation vorhandene verteilte Router.

Mit einem NAT-Netzwerkprofil und einem Lastausgleichsdienst kann vRealize Automation ein NSX Edge-Services-Gateway bereitstellen. Ein geroutetes Netzwerkprofil verwendet einen NSX Distributed Logical Router (DLR). Der DLR muss zunächst in NSX erstellt werden, damit er von vRealize Automation verwendet werden kann. vRealize Automation kann keine DLRs erstellen. Nach der Datenerfassung kann vRealize Automation den DLR für die Bereitstellung von virtuellen Maschinen verwenden.

Die für die Bereitstellung des Edge Gateway oder gerouteten Gateways verwendete Reservierung bestimmt das für NAT- und geroutete Netzwerkprofile verwendete externe Netzwerk sowie die virtuellen IP-Adressen für den Lastausgleichsdienst.

Wenn Sie den Blueprint für eine Maschinenbereitstellung verwenden, versucht vRealize Automation, nur die Reservierungen im Zusammenhang mit der angegebenen Reservierungsrichtlinie zum Bereitstellen des Edge Gateway oder gerouteten Gateways zu verwenden.

### Anwenden einer NSX -Anwendungsisolierungs-Sicherheitsrichtlinie auf einen Blueprint

Eine NSX-Anwendungsisolierungsrichtlinie dient als Firewall, um den gesamten ein- und ausgehenden Datenverkehr zu und von den bereitgestellten Maschinen in der Bereitstellung zu blockieren. Wenn Sie eine definierte NSX-Anwendungsisolierungsrichtlinie angeben, können die von dem Blueprint bereitgestellten Maschinen zwar miteinander kommunizieren, aber keine Verbindung außerhalb der Firewall herstellen.

Sie können die Anwendungsisolierung auf der Blueprint-Ebene anwenden, indem Sie das Dialogfeld **Neuer Blueprint** oder **Blueprint-Eigenschaften** verwenden.

Wenn eine NSX-Anwendungsisolierungsrichtlinie verwendet wird, ist nur interner Datenverkehr zwischen den durch den Blueprint bereitgestellten Maschinen zulässig. Wenn Sie die Bereitstellung anfordern, wird eine Sicherheitsgruppe für die bereitzustellenden Maschinen erstellt. Eine Anwendungsisolierungsrichtlinie wird in NSX erstellt und auf die Sicherheitsgruppe angewendet. Firewallregeln werden in der Sicherheitsrichtlinie definiert, um nur internen Datenverkehr zwischen den Komponenten in der Bereitstellung zuzulassen. Informationen hierzu finden Sie unter [Erstellen eines vSphere-Endpoints mit Netzwerk- und Sicherheitsintegration](#).

---

**Hinweis** Bei der Bereitstellung mit einem Blueprint, der sowohl einen NSX Edge-Lastausgleichsdienst als auch eine NSX-Anwendungsisolierungsrichtlinie verwendet, wird der dynamisch bereitgestellte Lastausgleichsdienst nicht zur Sicherheitsgruppe hinzugefügt. Dadurch wird verhindert, dass der Lastausgleichsdienst mit den Maschinen kommuniziert, für die er Verbindungen abwickeln soll. Edges sind von der NSX Distributed Firewall ausgeschlossen, weshalb sie nicht zu Sicherheitsgruppen hinzugefügt werden können. Für die ordnungsgemäße Funktion des Lastausgleichsdiensts sollten Sie eine andere Sicherheitsgruppe oder Sicherheitsrichtlinie verwenden, welche die Übertragung des erforderlichen Datenverkehrs an die Komponenten-VMs wegen des Lastausgleichs erlaubt.

---

Die Anwendungsisolierungsrichtlinie weist eine niedrigere Priorität als andere Sicherheitsrichtlinien in NSX auf. Wenn beispielsweise die zur Verfügung gestellte Bereitstellung eine Webkomponenten-Maschine und eine Anwendungskomponenten-Maschine enthält und die Webkomponenten-Maschine einen Webdienst hostet, muss der Dienst eingehenden Datenverkehr auf den Ports 80 und 443 zulassen. In diesem Fall müssen die Benutzer eine Websicherheitsrichtlinie in NSX erstellen, deren Firewallregeln so definiert sind, dass eingehender Datenverkehr auf diesen Ports zulässig ist. In vRealize Automation müssen die Benutzer die Websicherheitsrichtlinie auf die Webkomponente der Maschinenbereitstellung anwenden.

Wenn die Webkomponenten-Maschine Zugriff auf die Anwendungskomponenten-Maschine mithilfe eines Lastausgleichsdiensts auf den Ports 8080 und 8443 benötigt, sollte die Websicherheitsrichtlinie zusätzlich zu den vorhandenen Firewallregeln, die eingehenden Datenverkehr auf den Ports 80 und 443 erlauben, auch Firewallregeln enthalten, um ausgehenden Datenverkehr auf diesen Ports zu erlauben.

Informationen zu Sicherheitsfunktionen, die auf eine Maschinenkomponente in einem Blueprint angewendet werden können, finden Sie unter [Verwenden von Sicherheitskomponenten auf der Blueprint-Arbeitsfläche](#).

## Konfigurieren der Einstellungen für Netzwerk- und Sicherheitskomponenten

vRealize Automation unterstützt virtualisierte Netzwerke basierend auf den Plattformen vCloud Networking and Security und NSX.

Mithilfe der Netzwerk- und Sicherheitsvirtualisierung können virtuelle Maschinen über physische und virtuelle Netzwerke sicher und effizient miteinander kommunizieren.

Zur Integration von Netzwerk und Sicherheit mit vRealize Automation muss ein IaaS-Administrator die NSX-Plug-Ins in vRealize Orchestrator installieren und vRealize Orchestrator- und vSphere-Endpoints erstellen.

Informationen zur externen Vorbereitung finden Sie unter *Konfigurieren von vRealize Automation*.

Sie können Netzwerkprofile erstellen, mit denen Netzwerkeinstellungen in Reservierungen und in der Blueprint-Arbeitsfläche angegeben werden. Externe Netzwerkprofile definieren vorhandene physische Netzwerke. NAT und geroutete Profile sind Vorlagen, mit denen logische NSX-Switches und entsprechende Routingeneinstellungen für einen neuen Netzwerkpfad und zur Konfiguration von Netzwerkschnittstellen für die Verbindung mit dem Netzwerkpfad erstellt werden, wenn Sie virtuelle Maschinen bereitstellen und NSX Edge-Geräte konfigurieren.

Die Netzwerk- und Sicherheitskomponenteneinstellungen, die Sie zur Blueprint-Design-Arbeitsfläche hinzufügen, werden von der NSX-Konfiguration abgeleitet. Das NSX-Plug-In muss dafür installiert sein und die Datenerfassung für den NSX-Bestand für vSphere-Cluster muss ausgeführt werden. Netzwerk- und Sicherheitskomponenten sind für NSX spezifisch und ausschließlich für die Verwendung mit vSphere-Maschinenkomponenten verfügbar. Informationen über das Konfigurieren von NSX finden Sie im *NSXAdministratorhandbuch*.

Für Maschinenkomponenten, die nicht über eine Registerkarte **Netzwerk** oder **Sicherheit** verfügen, können Sie benutzerdefinierte Eigenschaften für Netzwerk und Sicherheit wie z. B. `VirtualMachine.Network0.Name` zu deren Registerkarte **Eigenschaften** in der Blueprint-Arbeitsfläche hinzufügen. Die Eigenschaften des NSX-Lastausgleichsdiensts betreffen nur vSphere-Maschinen.

Wenn Sie ein Netzwerkprofil in einer Reservierung und einem Blueprint angeben, hat der Blueprint-Wert Vorrang. Wenn Sie beispielsweise ein Netzwerkprofil im Blueprint mithilfe der benutzerdefinierten Eigenschaft `VirtualMachine.NetworkN.ProfileName` und in einer vom Blueprint verwendeten Reservierung angeben, hat das im Blueprint angegebene Netzwerkprofil Vorrang. Wenn die benutzerdefinierte Eigenschaft jedoch nicht im Blueprint verwendet wird und Sie ein Netzwerkprofil für eine Maschinen-NIC auswählen, verwendet vRealize Automation den Netzwerkreservierungspfad für die Maschinen-NIC, für die das Netzwerkprofil angegeben ist.

In Abhängigkeit von der Computing-Ressource können Sie eine Transportzone auswählen, die einen vSphere-Endpoint identifiziert. Eine Transportzone gibt die Hosts und Cluster an, die in dieser Zone erstellten logischen Switches zugeordnet werden können. Eine Transportzone kann sich über mehrere vSphere-Cluster erstrecken. Der für die Bereitstellung verwendete Blueprint und die verwendeten Reservierungen müssen dieselbe Transportzonen-Einstellung aufweisen. Transportzonen werden in den NSX-Umgebungen definiert. Informationen dazu finden Sie im *NSX-Administratorhandbuch*.

### Verwenden von Sicherheitskomponenten auf der Blueprint-Arbeitsfläche

Sie können NSX-Sicherheitskomponenten zur Arbeitsfläche hinzufügen, damit die konfigurierten Einstellungen für mindestens eine vSphere-Maschinenkomponente im Blueprint verfügbar wird.

Sicherheitsgruppen, -Tags und -Richtlinien werden außerhalb von vRealize Automation in der NSX-Anwendung konfiguriert.

Die Netzwerk- und Sicherheitskomponenteneinstellungen, die Sie zur Blueprint-Design-Arbeitsfläche hinzufügen, werden von der NSX-Konfiguration abgeleitet. Das NSX-Plug-In muss dafür installiert sein und die Datenerfassung für den NSX-Bestand für vSphere-Cluster muss ausgeführt werden. Netzwerk- und Sicherheitskomponenten sind für NSX spezifisch und ausschließlich für die Verwendung mit vSphere-Maschinenkomponenten verfügbar. Informationen über das Konfigurieren von NSX finden Sie im *NSXAdministratorhandbuch*.

Sie können Sicherheitssteuerelemente zu Blueprints hinzufügen, indem Sie Sicherheitsgruppen, Sicherheits-Tags und Sicherheitsrichtlinien für die vSphere-Computing-Ressource in NSX konfigurieren. Nach dem Ausführen der Datenerfassung sind die Sicherheitskonfigurationen, unter denen ausgewählt werden kann, in vRealize Automation verfügbar.

### Sicherheitsgruppe

Eine Sicherheitsgruppe ist eine Sammlung von Assets oder Gruppierungsobjekten aus der vSphere-Bestandsliste, die einer Gruppe von Sicherheitsrichtlinien zugeordnet werden, beispielsweise Distributed Firewall-Regeln und Sicherheitsdienstintegrationen von Drittanbietern wie etwa Virenschutz und Erkennung von Eindringversuchen. Mit der Gruppierungsfunktion können Sie benutzerdefinierte Container erstellen, denen Sie zum Schutz durch die Distributed Firewall Ressourcen wie virtuelle Maschinen und Netzwerkdapter hinzufügen können. Nach dem Definieren einer Gruppe können Sie diese zum Schutz als Quelle oder Ziel zu einer Firewallregel hinzufügen.



Zusätzlich zu den in der Reservierung angegebenen Sicherheitsgruppen können Sie Sicherheitsgruppen zu einem Blueprint hinzufügen.

Sicherheitsgruppen werden in der Quellressource verwaltet. Informationen zum Verwalten von Sicherheitsgruppen für verschiedene Ressourcentypen finden Sie in der Dokumentation des Anbieters.

Sie können eine vorhandene NSX-Sicherheitsgruppe oder eine Sicherheitsgruppe nach Bedarf zur Blueprint-Arbeitsfläche hinzufügen.

### **Sicherheits-Tag**

Ein Sicherheits-Tag ist ein Bezeichnerobjekt oder Kategorisierungseintrag, das bzw. den Sie als Gruppierungsmechanismus verwenden können. Sie definieren die Kriterien, die ein Objekt erfüllen muss, damit es zu der von Ihnen erstellten Sicherheitsgruppe hinzugefügt werden kann. Dadurch können Sie Maschinen einbeziehen, indem Sie ein Filterkriterium mit einer Anzahl von unterstützten Parametern zur Entsprechung der Suchkriterien definieren. Sie können z. B. alle Maschinen mit einem bestimmten Sicherheits-Tag zu einer Sicherheitsgruppe hinzufügen.

Sie können ein Sicherheits-Tag zur Blueprint-Arbeitsfläche hinzufügen.

### **Sicherheitsrichtlinie**

Eine Sicherheitsrichtlinie ist ein Satz von Endpoint-, Firewall- und Netzwerk-Introspektionsdiensten, die auf eine Sicherheitsgruppe angewendet werden können. Mithilfe einer Sicherheitsgruppe bei Bedarf in einem Blueprint können Sie Sicherheitsrichtlinien zu einer virtuellen vSphere-Maschine hinzufügen. Eine Sicherheitsrichtlinie kann nicht direkt zu einer Reservierung hinzugefügt werden. Nach der Datenerfassung sind alle Sicherheitsrichtlinien, die in NSX für eine Computing-Ressource definiert wurden, in einem Blueprint als Auswahloptionen verfügbar.

### **Anwendungsisolierung**

Wenn die Anwendungsisolierung aktiviert ist, wird eine separate Sicherheitsrichtlinie erstellt. Bei der Anwendungsisolierung wird eine logische Firewall zum Blockieren jeglichen eingehenden und ausgehenden Datenverkehrs zu den Anwendungen im Blueprint verwendet. Komponentenmaschinen, die über einen Blueprint bereitgestellt werden, der eine Anwendungsisolierungsrichtlinie enthält, können miteinander kommunizieren, aber keine Verbindung außerhalb der Firewall herstellen, außer dem Blueprint werden andere Sicherheitsgruppen mit Sicherheitsrichtlinien, die den Zugriff erlauben, hinzugefügt.

### **Hinzufügen einer vorhandenen Sicherheitsgruppenkomponente**

Sie können eine vorhandene Sicherheitsgruppenkomponente zur Design-Arbeitsfläche hinzufügen, um die Zuordnung ihrer Einstellungen zu einer oder mehreren Maschinenkomponenten oder zu anderen verfügbaren Komponententypen im Blueprint vorzubereiten.

Sie können eine vorhandene Sicherheitsgruppenkomponente verwenden, um eine NSX-Sicherheitsgruppe zur Design-Arbeitsfläche hinzuzufügen und deren Einstellungen für die Verwendung mit vSphere-Maschinenkomponenten und Software- oder XaaS-Komponenten, die zu vSphere gehören, zu konfigurieren.

Sie können mehrere Netzwerk- und Sicherheitskomponenten zur Blueprint-Design-Arbeitsfläche hinzufügen.

## Voraussetzungen

- Erstellen und konfigurieren Sie eine Sicherheitsgruppe in NSX. Weitere Informationen hierzu finden Sie unter *Konfigurieren von vRealize Automation* und im *NSX-Administratorhandbuch*.
- Stellen Sie sicher, dass das NSX-Plug-In für vRealize Automation installiert ist und dass die NSX-Bestandsliste erfolgreich für Ihren Cluster ausgeführt wurde.

Um NSX-Konfigurationen in vRealize Automation zu verwenden, müssen Sie das NSX-Plug-In installieren und die Datenerfassung ausführen.

- Melden Sie sich an der vRealize Automation-Konsole als **Infrastrukturarchitekt** an.
- Öffnen Sie mithilfe der Registerkarte **Design** einen neuen oder vorhandenen Blueprint in der Design-Arbeitsfläche.

## Vorgehensweise

- 1 Klicken Sie im Abschnitt „Kategorien“ auf **Netzwerk und Sicherheit**, um die Liste der verfügbaren Netzwerk- und Sicherheitskomponenten anzuzeigen.
- 2 Ziehen Sie eine **Vorhandene Sicherheitsgruppe**-Komponente auf die Design-Arbeitsfläche.
- 3 Wählen Sie aus dem Dropdown-Menü **Sicherheitsgruppe** eine vorhandene Sicherheitsgruppe aus.
- 4 Klicken Sie auf **OK**.
- 5 Klicken Sie auf **Fertig stellen**, um den Blueprint als Entwurf zu speichern, oder setzen Sie die Konfiguration des Blueprints fort.

Sie können weitere Sicherheitseinstellungen konfigurieren, indem Sie zusätzliche Sicherheitskomponenten hinzufügen und indem Sie Einstellungen auf der Registerkarte **Sicherheit** einer vSphere-Maschinenkomponente in der Blueprint-Arbeitsfläche auswählen.

## Hinzufügen einer bedarfsgesteuerten Sicherheitsgruppenkomponente

Sie können eine bedarfsgesteuerte Sicherheitsgruppenkomponente zur Design-Arbeitsfläche hinzufügen, um die Zuordnung ihrer Einstellungen zu einer oder mehreren vSphere-Maschinenkomponenten oder zu anderen verfügbaren Komponententypen im Blueprint vorzubereiten.

## Voraussetzungen

- Erstellen und konfigurieren Sie eine Sicherheitsrichtlinie in NSX. Informationen dazu finden Sie im *NSX-Administratorhandbuch*.
- Stellen Sie sicher, dass das NSX-Plug-In für vRealize Automation installiert ist und dass die NSX-Bestandsliste erfolgreich für Ihren Cluster ausgeführt wurde.

Um NSX-Konfigurationen in vRealize Automation zu verwenden, müssen Sie das NSX-Plug-In installieren und die Datenerfassung ausführen.

- Melden Sie sich an der vRealize Automation-Konsole als **Infrastrukturarchitekt** an.
- Öffnen Sie mithilfe der Registerkarte **Design** einen neuen oder vorhandenen Blueprint in der Design-Arbeitsfläche.

## Vorgehensweise

- 1 Klicken Sie im Abschnitt „Kategorien“ auf **Netzwerk und Sicherheit**, um die Liste der verfügbaren Netzwerk- und Sicherheitskomponenten anzuzeigen.
- 2 Ziehen Sie eine **Sicherheitsgruppe nach Bedarf**-Komponente auf die Design-Arbeitsfläche.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 Fügen Sie eine oder mehrere Sicherheitsrichtlinien hinzu, indem Sie im Bereich **Sicherheitsrichtlinien** auf das Symbol „Hinzufügen“ klicken und verfügbare Sicherheitsrichtlinien auswählen.
- 5 Klicken Sie auf **OK**.
- 6 Klicken Sie auf **Fertig stellen**, um den Blueprint als Entwurf zu speichern, oder setzen Sie die Konfiguration des Blueprints fort.

Sie können weitere Sicherheitseinstellungen konfigurieren, indem Sie zusätzliche Sicherheitskomponenten hinzufügen und indem Sie Einstellungen auf der Registerkarte **Sicherheit** einer vSphere-Maschinenkomponente in der Blueprint-Arbeitsfläche auswählen.

## Hinzufügen einer vorhandenen Sicherheits-Tag-Komponente

Sie können eine Sicherheits-Tag-Komponente zur Blueprint-Design-Arbeitsfläche hinzufügen, um die Zuordnung ihrer Einstellungen zu einer oder mehreren Maschinenkomponenten im Blueprint vorzubereiten.

Sie können eine Sicherheits-Tag-Komponente verwenden, um ein NSX-Sicherheits-Tag zur Design-Arbeitsfläche hinzuzufügen und deren Einstellungen für die Verwendung mit vSphere-Maschinenkomponenten und Software-Komponenten, die zu vSphere gehören, zu konfigurieren.

Sie können mehrere Netzwerk- und Sicherheitskomponenten zur Blueprint-Design-Arbeitsfläche hinzufügen.

## Voraussetzungen

- Erstellen und konfigurieren Sie Sicherheits-Tags in NSX. Weitere Informationen hierzu finden Sie unter *Konfigurieren von vRealize Automation* und im *NSX-Administratorhandbuch*.
- Stellen Sie sicher, dass das NSX-Plug-In für vRealize Automation installiert ist und dass die NSX-Bestandsliste erfolgreich für Ihren Cluster ausgeführt wurde.

Um NSX-Konfigurationen in vRealize Automation zu verwenden, müssen Sie das NSX-Plug-In installieren und die Datenerfassung ausführen.

- Stellen Sie sicher, dass das NSX-Plug-In für vRealize Automation installiert ist und dass die NSX-Bestandsliste erfolgreich für Ihren Cluster ausgeführt wurde.

Um NSX-Konfigurationen in vRealize Automation zu verwenden, müssen Sie das NSX-Plug-In installieren und die Datenerfassung ausführen.

- Melden Sie sich an der vRealize Automation-Konsole als **Infrastrukturarchitekt** an.
- Öffnen Sie mithilfe der Registerkarte **Design** einen neuen oder vorhandenen Blueprint in der Design-Arbeitsfläche.

## Vorgehensweise

- 1 Klicken Sie im Abschnitt „Kategorien“ auf **Netzwerk und Sicherheit**, um die Liste der verfügbaren Netzwerk- und Sicherheitskomponenten anzuzeigen.
- 2 Ziehen Sie eine **Vorhandenes Sicherheits-Tag**-Komponente auf die Design-Arbeitsfläche.
- 3 Klicken Sie auf das Textfeld **Sicherheits-Tag** und wählen Sie ein vorhandenes Sicherheits-Tag aus.
- 4 Klicken Sie auf **OK**.
- 5 Klicken Sie auf **Fertig stellen**, um den Blueprint als Entwurf zu speichern, oder setzen Sie die Konfiguration des Blueprints fort.

Sie können weitere Sicherheitseinstellungen konfigurieren, indem Sie zusätzliche Sicherheitskomponenten hinzufügen und indem Sie Einstellungen auf der Registerkarte **Sicherheit** einer vSphere-Maschinenkomponente in der Blueprint-Arbeitsfläche auswählen.

## Verwenden von Netzwerkkomponenten auf der Blueprint-Arbeitsfläche

Sie können mindestens eine NSX-Netzwerkkomponente zur Design-Arbeitsfläche hinzufügen und deren Einstellungen für vSphere-Maschinenkomponenten in dem Blueprint konfigurieren.

Sie können Netzwerkkomponenten zur Arbeitsfläche hinzufügen, um deren konfigurierte Einstellungen ein oder mehreren Maschinenkomponenten im Blueprint zur Verfügung zu stellen.

Die Netzwerk- und Sicherheitskomponenteneinstellungen, die Sie zur Blueprint-Design-Arbeitsfläche hinzufügen, werden von der NSX-Konfiguration abgeleitet. Das NSX-Plug-In muss dafür installiert sein und die Datenerfassung für den NSX-Bestand für vSphere-Cluster muss ausgeführt werden. Netzwerk- und Sicherheitskomponenten sind für NSX spezifisch und ausschließlich für die Verwendung mit vSphere-Maschinenkomponenten verfügbar. Informationen über das Konfigurieren von NSX finden Sie im *NSX Administratorhandbuch*.

## Hinzufügen einer vorhandenen Netzwerkkomponente

Sie können eine vorhandene NSX-Netzwerkkomponente zur Design-Arbeitsfläche hinzufügen, um die Zuordnung ihrer Einstellungen zu einer oder mehreren vSphere-Maschinenkomponenten im Blueprint vorzubereiten.

Sie können eine vorhandene Netzwerkkomponente verwenden, um ein NSX-Netzwerk zur Design-Arbeitsfläche hinzuzufügen und deren Einstellungen für die Verwendung mit vSphere-Maschinenkomponenten und Software- oder XaaS-Komponenten, die zu vSphere gehören, zu konfigurieren.

Wenn Sie eine vorhandene Netzwerkkomponente oder eine On-Demand-Netzwerkkomponente einer Maschinenkomponente zuordnen, werden die NIC-Informationen mit der Maschinenkomponente gespeichert. Die angegebenen Netzwerkprofilinformationen werden mit der Netzwerkkomponente gespeichert.

Sie können mehrere Netzwerk- und Sicherheitskomponenten zur Blueprint-Design-Arbeitsfläche hinzufügen.

Für Maschinenkomponenten, die nicht über eine Registerkarte **Netzwerk** oder **Sicherheit** verfügen, können Sie benutzerdefinierte Eigenschaften für Netzwerk und Sicherheit wie z. B. `VirtualMachine.Network0.Name` zu deren Registerkarte **Eigenschaften** in der Blueprint-Arbeitsfläche hinzufügen. Die Eigenschaften des NSX-Lastausgleichsdiensts betreffen nur vSphere-Maschinen.

### Voraussetzungen

- Erstellen und konfigurieren Sie Netzwerkeinstellungen für NSX. Weitere Informationen hierzu finden Sie unter *Konfigurieren von vRealize Automation* und im *NSX-Administratorhandbuch*.
- Stellen Sie sicher, dass das NSX-Plug-In für vRealize Automation installiert ist und dass die NSX-Bestandsliste erfolgreich für Ihren Cluster ausgeführt wurde.

Um NSX-Konfigurationen in vRealize Automation zu verwenden, müssen Sie das NSX-Plug-In installieren und die Datenerfassung ausführen.

- Erstellen Sie ein Netzwerkprofil.
- Melden Sie sich an der vRealize Automation-Konsole als **Infrastrukturarchitekt** an.
- Öffnen Sie mithilfe der Registerkarte **Design** einen neuen oder vorhandenen Blueprint in der Design-Arbeitsfläche.

### Vorgehensweise

- 1 Klicken Sie im Abschnitt „Kategorien“ auf **Netzwerk und Sicherheit**, um die Liste der verfügbaren Netzwerk- und Sicherheitskomponenten anzuzeigen.
- 2 Ziehen Sie eine **Vorhandenes Netzwerk**-Komponente auf die Design-Arbeitsfläche.
- 3 Klicken Sie auf das Textfeld **Vorhandenes Netzwerk** und wählen Sie ein vorhandenes Netzwerkprofil aus.

Die Werte für die Beschreibung, die Subnetzmasken und das Gateway werden basierend auf dem ausgewählten Netzwerkprofil aufgefüllt.

- 4 (Optional) Klicken Sie auf die Registerkarte **DNS/WINS**.
- 5 (Optional) Geben Sie die DNS- und WINS-Einstellungen für das Netzwerkprofil an oder akzeptieren Sie die bereitgestellten Einstellungen.
  - Primärer DNS
  - Sekundärer DNS
  - DNS-Suffix
  - Bevorzugter WINS
  - Alternativer WINS

Sie können die DNS- oder WINS-Einstellungen für ein bestehendes Netzwerk nicht ändern.

## 6 (Optional) Klicken Sie auf die Registerkarte **IP-Bereiche**.

Der im Netzwerkprofil angegebene IP-Bereich bzw. die im Netzwerkprofil angegebenen IP-Bereiche werden angezeigt. Sie können die Sortierreihenfolge oder die Spaltenanzeige ändern. Bei NAT-Netzwerken können Sie auch IP-Bereichswerte ändern.

## 7 Klicken Sie auf **Fertig stellen**, um den Blueprint als Entwurf zu speichern, oder setzen Sie die Konfiguration des Blueprints fort.

### Weiter

Sie können weitere Netzwerkeinstellungen konfigurieren, indem Sie zusätzliche Netzwerkkomponenten hinzufügen und indem Sie Einstellungen auf der Registerkarte **Netzwerk** einer vSphere-Maschinenkomponente auf der Blueprint-Arbeitsfläche auswählen.

### Hinzufügen einer bedarfsgesteuerten NAT- oder bedarfsgesteuerten gerouteten Netzwerkkomponente

Sie können eine bedarfsgesteuerte NSX-NAT- oder eine bedarfsgesteuerte geroutete NSX-Netzwerkkomponente zur Design-Arbeitsfläche hinzufügen, um die Zuordnung ihrer Einstellungen zu einer oder mehreren vSphere-Maschinenkomponenten im Blueprint vorzubereiten.

Wenn Sie eine vorhandene Netzwerkkomponente oder eine On-Demand-Netzwerkkomponente einer Maschinenkomponente zuordnen, werden die NIC-Informationen mit der Maschinenkomponente gespeichert. Die angegebenen Netzwerkprofilinformationen werden mit der Netzwerkkomponente gespeichert.

Sie können mehrere Netzwerk- und Sicherheitskomponenten zur Blueprint-Design-Arbeitsfläche hinzufügen.

Für Maschinenkomponenten, die nicht über eine Registerkarte **Netzwerk** oder **Sicherheit** verfügen, können Sie benutzerdefinierte Eigenschaften für Netzwerk und Sicherheit wie z. B. `VirtualMachine.Network0.Name` zu deren Registerkarte **Eigenschaften** in der Blueprint-Arbeitsfläche hinzufügen. Die Eigenschaften des NSX-Lastausgleichsdiensts betreffen nur vSphere-Maschinen.

### Voraussetzungen

- Erstellen und konfigurieren Sie Netzwerkeinstellungen für NSX. Weitere Informationen hierzu finden Sie unter *Konfigurieren von vRealize Automation* und im *NSX-Administratorhandbuch*.
- Stellen Sie sicher, dass das NSX-Plug-In für vRealize Automation installiert ist und dass die NSX-Bestandsliste erfolgreich für Ihren Cluster ausgeführt wurde.

Um NSX-Konfigurationen in vRealize Automation zu verwenden, müssen Sie das NSX-Plug-In installieren und die Datenerfassung ausführen.

- Erstellen Sie ein Netzwerkprofil.

Wenn Sie z. B. eine bedarfsgesteuerte NAT-Netzwerkkomponente hinzufügen, erstellen Sie ein Netzwerkprofil für NAT.

- Melden Sie sich an der vRealize Automation-Konsole als **Infrastrukturarchitekt** an.
- Öffnen Sie mithilfe der Registerkarte **Design** einen neuen oder vorhandenen Blueprint in der Design-Arbeitsfläche.

## Vorgehensweise

- 1 Klicken Sie im Abschnitt „Kategorien“ auf **Netzwerk und Sicherheit**, um die Liste der verfügbaren Netzwerk- und Sicherheitskomponenten anzuzeigen.
- 2 Ziehen Sie, je nachdem, ob Sie eine bedarfsgesteuerte NAT- oder eine geroutete Komponente konfigurieren möchten, eine der bedarfsgesteuerten Netzwerkkomponenten auf die Design-Arbeitsfläche.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 Wählen Sie aus dem Dropdown-Menü **Netzwerkprofil** ein entsprechendes Netzwerkprofil aus.

Wenn Sie z. B. eine Komponente **Bedarfsgesteuertes NAT-Netzwerk** hinzufügen, wählen Sie ein NAT-Netzwerkprofil aus.

Die folgenden Netzwerkeinstellungen werden basierend auf Ihrem ausgewählten Netzwerkprofil aufgefüllt. Änderungen an diesen Werten müssen im Netzwerkprofil vorgenommen werden:

- Name des externen Netzwerkprofils
- NAT-Typ (Bedarfsgesteuertes NAT-Netzwerk)
- Subnetzmaske
- Bereichssubnetzmaske (Bedarfsgesteuertes geroutetes Netzwerk)
- Bereichssubnetzmaske (Bedarfsgesteuertes geroutetes Netzwerk)
- Basis-IP-Adresse (Bedarfsgesteuertes geroutetes Netzwerk)

- 5 (Optional) Klicken Sie auf die Registerkarte **DNS/WINS**.
- 6 (Optional) Geben Sie die DNS- und WINS-Einstellungen für das Netzwerkprofil an oder akzeptieren Sie die bereitgestellten Einstellungen.
  - Primärer DNS
  - Sekundärer DNS
  - DNS-Suffix
  - Bevorzugter WINS
  - Alternativer WINS

Sie können die DNS- oder WINS-Einstellungen für ein bestehendes Netzwerk nicht ändern.

- 7 (Optional) Klicken Sie bei einer bedarfsgesteuerten NAT-Netzwerkkomponente auf die Registerkarte **DHCP**, um die Werte für den IP-Adressbereich und die Leasedauer anzugeben.

Sie können die Werte der IP-Startadressen und IP-Endadressen für den DHCP-Bereich bearbeiten. Wenn die virtuelle Maschine mit DHCP bereitgestellt wird, weist der Netzwerkadapter der Maschine eine IP-Adresse zu, die sich innerhalb dieses Bereichs befindet. Standardmäßig handelt es sich dabei um einen statischen Netzwerkadapter. Die Werte für die IP-Adressen dürfen nicht denjenigen entsprechen, die in den zugeordneten Subnetzen als Netzwerk- bzw. Broadcastadressen verwendet wurden. Statische IP-Bereiche dürfen sich nicht überschneiden.

DHCP ist nur für bedarfsgesteuerte 1:1-NAT-Netzwerkkomponenten verfügbar.

- 8 (Optional) Geben Sie im Textfeld **Beginn des IP-Bereichs** den Wert für eine IP-Startadresse ein.
- 9 (Optional) Geben Sie im Textfeld **Ende des IP-Bereichs** den Wert für eine IP-Endadresse ein.
- 10 Geben Sie im Textfeld **Leasedauer (Sekunden)** eine DHCP-Leasedauer in Sekunden ein oder lassen Sie das Feld leer, wenn die Leasedauer unbegrenzt sein soll.
- 11 (Optional) Klicken Sie auf die Registerkarte **IP-Bereiche**.

Der im Netzwerkprofil angegebene IP-Bereich bzw. die im Netzwerkprofil angegebenen IP-Bereiche werden angezeigt. Sie können die Sortierreihenfolge oder die Spaltenanzeige ändern. Bei NAT-Netzwerken können Sie auch IP-Bereichswerte ändern.

- 12 Klicken Sie auf **Fertig stellen**, um den Blueprint als Entwurf zu speichern, oder setzen Sie die Konfiguration des Blueprints fort.

### Weiter

Sie können weitere Netzwerkeinstellungen konfigurieren, indem Sie zusätzliche Netzwerkkomponenten hinzufügen und indem Sie Einstellungen auf der Registerkarte **Netzwerk** einer vSphere-Maschinenkomponente auf der Blueprint-Arbeitsfläche auswählen.

### Verwenden von Lastausgleichsdienst-Komponenten auf der Blueprint-Arbeitsfläche

Sie können mindestens eine bedarfsgesteuerte NSX-Lastausgleichsdienst-Komponente zur Design-Arbeitsfläche hinzufügen, um die Einstellungen für vSphere-Maschinenkomponenten in dem Blueprint zu konfigurieren.

Die Netzwerk- und Sicherheitskomponenteneinstellungen, die Sie zur Blueprint-Design-Arbeitsfläche hinzufügen, werden von der NSX-Konfiguration abgeleitet. Das NSX-Plug-In muss dafür installiert sein und die Datenerfassung für den NSX-Bestand für vSphere-Cluster muss ausgeführt werden. Netzwerk- und Sicherheitskomponenten sind für NSX spezifisch und ausschließlich für die Verwendung mit vSphere-Maschinenkomponenten verfügbar. Informationen über das Konfigurieren von NSX finden Sie im *NSX Administratorhandbuch*.

Die folgenden Regeln gelten für Lastausgleichsdienst-Pools und VIP-Netzwerkeinstellungen im Blueprint:

- Wenn das Pool-Netzwerkprofil NAT ist, kann das VIP-Netzwerkprofil das gleiche NAT-Netzwerkprofil im gleichen NAT-Netzwerkprofil sein.
- Ist das Poolnetzwerkprofil geroutet, kann das VIP-Netzwerkprofil nur dasselbe geroutete Netzwerk sein.
- Ist das Poolnetzwerkprofil extern, kann das VIP-Netzwerkprofil nur dasselbe externe Netzwerkprofil sein.

Zudem wird eine NSX Edge-Ressource erstellt, und Lastausgleichsdienst-Details wie VIP, Lastausgleichsebene und konfigurierte Dienste werden als Eigenschaften der Edge-Ressource erfasst.



## Hinzufügen einer Komponente für den Lastausgleichsdienst nach Bedarf

Sie können eine Komponente für den Lastausgleichsdienst nach Bedarf verwenden, um einen NSX-Lastausgleichsdienst zur Design-Arbeitsfläche hinzuzufügen und deren Einstellungen für die Verwendung mit vSphere-Maschinenkomponenten und Software- oder XaaS-Komponenten, die zu vSphere gehören, zu konfigurieren.

Durch die Einstellungen für den Lastausgleichsdienst wird die Verarbeitung von Aufgaben auf in einem Netzwerk bereitgestellte Maschinen verteilt.

Weitere Informationen über die Erstellung von NSX-Anwendungsprofilen zur Definition des Verhaltens eines bestimmten Netzwerkverkehrstyps finden Sie im *Administratorhandbuch für NSX*.

### Voraussetzungen

- Erstellen und konfigurieren Sie Einstellungen für den Lastausgleichsdienst für NSX. Weitere Informationen hierzu finden Sie unter *Konfigurieren von vRealize Automation* und im *NSX-Administratorhandbuch*.
- Stellen Sie sicher, dass das NSX-Plug-In für vRealize Automation installiert ist und dass die NSX-Bestandsliste erfolgreich für Ihren Cluster ausgeführt wurde.

Um NSX-Konfigurationen in vRealize Automation zu verwenden, müssen Sie das NSX-Plug-In installieren und die Datenerfassung ausführen.

- Erstellen Sie ein Netzwerkprofil.
- Melden Sie sich an der vRealize Automation-Konsole als **Infrastrukturarchitekt** an.
- Öffnen Sie mithilfe der Registerkarte **Design** einen neuen oder vorhandenen Blueprint in der Design-Arbeitsfläche.
- Stellen Sie sicher, dass auf der Design-Arbeitsfläche des Blueprints mindestens eine vSphere-Maschinenkomponente vorhanden ist.

### Vorgehensweise

- 1 Klicken Sie im Abschnitt „Kategorien“ auf **Netzwerk und Sicherheit**, um die Liste der verfügbaren Netzwerk- und Sicherheitskomponenten anzuzeigen.
- 2 Ziehen Sie eine **Lastenausgleich bei Bedarf**-Komponente auf die Design-Arbeitsfläche.
- 3 Geben Sie im Textfeld **Name** einen Namen ein.
- 4 Wählen Sie aus dem Dropdown-Menü **Maschine** einen Maschinennamen aus.  
Die Liste enthält nur vSphere-Maschinenkomponenten in dem aktiven Blueprint.
- 5 Wählen Sie aus dem Dropdown-Menü **NIC** eine Netzwerkkarte (NIC) aus.  
Die Liste enthält Netzwerkkarten, die für die ausgewählte vSphere-Maschinenkomponente definiert sind.
- 6 Wählen Sie aus dem Dropdown-Menü **VIP-Netzwerk** ein VIP-Netzwerk aus.

- 7 (Optional) Geben Sie über **IP-Adresse** die VIP-Adresse für die Netzwerkkarte ein.

Die Standardeinstellung ist die statische IP-Adresse, die mit dem VIP-Netzwerk verknüpft ist. Sie können eine andere IP-Adresse oder einen anderen IP-Adressbereich angeben. Standardmäßig wird VIP die nächste verfügbare IP-Adresse über das Netzwerkprofil zugeteilt. Um eine IP-Adresse angeben zu können, muss VIP in einem NAT-Netzwerk erstellt werden.

- 8 Aktivieren Sie das Kontrollkästchen neben den Diensten, für die Sie den Lastausgleich verwenden möchten.

Zu den Dienstoptionen zählen HTTP, HTTPS und TCP.

- 9 (Optional) Akzeptieren oder bearbeiten Sie die Einstellungen des Ports und der Systemstatusprüfung für jeden ausgewählten Dienst.

- 10 Geben Sie in das Textfeld **URL für HTTP-Dienst** die Adresse für den ausgewählten Dienst ein.

Für jeden Lastausgleichsdienst ist nur eine einzige URL für die HTTP-Dienststeuerung verfügbar.

Die eingegebene URL wird für Integritätsprüfungen des Diensts verwendet.

Geben Sie die Adress-URL ein, an die der HTTP-Verkehr umgeleitet werden soll. Sie können Verkehr beispielsweise von `http://myweb.com` zu `https://myweb.com` umleiten. Der eingegebene Wert muss dem Wert entsprechen, der in der Einstellung **URL für HTTP-Umleitung** in der NSX-Anwendung angegeben ist.

- 11 Klicken Sie auf **Fertig stellen**, um den Blueprint als Entwurf zu speichern, oder setzen Sie die Konfiguration des Blueprints fort.

Die konfigurierten Einstellungen sind auf der Registerkarte **Netzwerk** in der zugehörigen vSphere-Maschinenkomponente verfügbar.

## Zuordnen von Netzwerk- und Sicherheitskomponenten

Sie können Netzwerk- und Sicherheitskomponenten auf die Design-Arbeitsfläche ziehen, um deren Einstellungen für die Konfiguration von Maschinenkomponenten im Blueprint verfügbar zu machen. Nachdem Sie Netzwerk- und Sicherheitseinstellungen für die Maschine definiert haben, können Sie optional Einstellungen über eine Lastausgleichsdienst-Komponente zuordnen.

Nachdem Sie eine NSX-Netzwerk- oder -Sicherheitskomponente auf der Arbeitsfläche hinzugefügt und die verfügbaren Einstellungen definiert haben, können Sie die Registerkarten „Netzwerk“ und „Sicherheit“ einer vSphere-Maschinenkomponente in der Arbeitsfläche öffnen und die entsprechenden Einstellungen konfigurieren.

Die Netzwerk- und Sicherheitskomponenteneinstellungen, die Sie zur Blueprint-Design-Arbeitsfläche hinzufügen, werden von der NSX-Konfiguration abgeleitet. Das NSX-Plug-In muss dafür installiert sein und die Datenerfassung für den NSX-Bestand für vSphere-Cluster muss ausgeführt werden. Netzwerk- und Sicherheitskomponenten sind für NSX spezifisch und ausschließlich für die Verwendung mit vSphere-Maschinenkomponenten verfügbar. Informationen über das Konfigurieren von NSX finden Sie im *NSX Administratorhandbuch*.

Beispielsweise können Sie eine „Bei Bedarf NAT“-Netzwerkkomponente auf die Design-Arbeitsfläche des Blueprints ziehen, um diese für eine vSphere-Maschinenkomponente verfügbar zu machen, die ebenfalls in der Arbeitsfläche vorhanden ist.

## Entwerfen von Software -Komponenten

Als Softwarearchitekt erstellen Sie wiederverwendbare Softwarekomponenten, standardisieren Konfigurationseigenschaften und verwenden Aktionsskripts, um anzugeben, wie genau Komponenten bei Bereitstellungsskalierungsvorgängen installiert, konfiguriert, deinstalliert oder aktualisiert werden. Diese Aktionsskripts können Sie jederzeit umschreiben und live veröffentlichen, um die Änderungen an bereitgestellte Softwarekomponenten zu übergeben.

Sie können allgemeine und wiederverwendbare Aktionsskripts erstellen, indem Sie Namenswertpaare, so genannte Softwareeigenschaften, definieren und als Parameter an Ihre Aktionsskripts übergeben. Wenn Ihre Softwareeigenschaften Werte aufweisen, die unbekannt sind oder in Zukunft definiert werden müssen, können Sie andere Blueprint-Architekten oder Endbenutzer auffordern oder ihnen erlauben, die Werte einzugeben. Wenn Sie einen Wert aus einer anderen Komponente in einem Blueprint benötigen, beispielsweise die IP-Adresse einer Maschine, können Sie die Softwareeigenschaft an die IP-Adresseeigenschaft dieser Maschine binden. Durch die Verwendung von Softwareeigenschaften zum Parametrisieren Ihrer Aktionsskripts werden sie als allgemein und wiederverwendbar definiert. Sie können dann Softwarekomponenten in unterschiedlichen Umgebungen bereitstellen, ohne Ihre Skripts ändern zu müssen.

**Tabelle 4-33. Lebenszyklusaktionen**

Lebenszyklusaktionen	Beschreibung
Installieren	Installiert Ihre Software. Beispielsweise können Sie Tomcat-Server-Installationsbits herunterladen und einen Tomcat-Dienst installieren. Skripts, die Sie für die Installationslebenszyklus-Aktion erstellen, werden bei der erstmaligen Bereitstellung von Software ausgeführt, entweder während der Erstinstallationsanforderung oder im Rahmen einer horizontalen Skalierung.
Konfigurieren	Konfiguriert Ihre Software. Für das Tomcat-Beispiel können Sie JAVA_OPTS und CATALINA_OPTS festlegen. Konfigurationsskripts werden nach Abschluss der Installationsaktion ausgeführt.
Start	Startet Ihre Software. Beispielsweise können Sie den Tomcat-Dienst mithilfe des Startbefehls auf dem Tomcat-Server starten. Startskripts werden nach Abschluss der Konfigurationsaktion ausgeführt.
Aktualisieren	Wenn Sie für Ihre Softwarekomponente die Unterstützung skalierbarer Blueprints konfigurieren, werden alle Aktualisierungen durchgeführt, die nach einer vertikalen oder horizontalen Skalierung erforderlich sind. Beispielsweise können Sie die Clustergröße für eine skalierte Bereitstellung ändern und die Clusterknoten mithilfe eines Lastausgleichsdiensts verwalten. Konfigurieren Sie Ihre Aktualisierungsskripts für die mehrmalige Ausführung (idempotent) und für die horizontale und vertikale Skalierung. Wenn ein Skalierungsvorgang durchgeführt wird, werden Aktualisierungsskripts auf allen abhängigen Softwarekomponenten ausgeführt.
Deinstallieren	Deinstalliert Ihre Software. Beispielsweise können Sie bestimmte Aktionen für die Anwendung ausführen, bevor eine Bereitstellung gelöscht wird. Deinstallationsskripts werden ausgeführt, wenn Softwarekomponenten gelöscht werden.

Für eine Reihe von Middleware-Diensten und Anwendungen können Sie vordefinierte Software-Komponenten von VMware Solution Exchange herunterladen. Mithilfe von vRealize CloudClient oder der vRealize Automation-REST-API können Sie programmgesteuert vordefinierte Software-Komponenten in Ihre vRealize Automation-Instanz importieren.

- Informationen zum Besuchen von VMware Solution Exchange finden Sie unter [https://solutionexchange.vmware.com/store/category\\_groups/cloud-management](https://solutionexchange.vmware.com/store/category_groups/cloud-management).
- Informationen zur vRealize Automation-REST-API finden Sie im *Programmierhandbuch* und in der *Referenz für vRealize Automation-API*.
- Weitere Informationen zu vRealize CloudClient finden Sie unter <https://developercenter.vmware.com/tool/cloudclient>.

## Eigenschaftstypen und Einstellungsoptionen

Sie können allgemeine und wiederverwendbare Aktionsskripts erstellen, indem Sie Namenswertpaare, so genannte Softwareeigenschaften, definieren und als Parameter an Ihre Aktionsskripts übergeben. Sie können Softwareeigenschaften erstellen, die Zeichenfolgen-, Array-, Inhalts-, Ganzzahl- oder boolesche Werte erwarten. Sie haben die Möglichkeit, den Wert selbst einzugeben, jemanden zur Eingabe des Werts aufzufordern oder den Wert aus einer anderen Blueprint-Komponente durch Erstellen einer Bindung abzurufen.

### Eigenschaftsoptionen

Sie können den Wert jeder Zeichenfolgen-Eigenschaft berechnen, indem Sie das Kontrollkästchen „Computing“ aktivieren, und Sie können jede Eigenschaft als verschlüsselt, überschreibbar oder erforderlich festlegen, indem Sie beim Konfigurieren der Software-Eigenschaften die entsprechenden Kontrollkästchen aktivieren. Kombinieren Sie diese Optionen mit Ihren Werten, um verschiedene Zwecke zu erreichen. Angenommen, Sie möchten Blueprint-Architekten auffordern, einen Wert für ein Kennwort einzugeben und diesen Wert zu verschlüsseln, wenn sie Ihre Softwarekomponente in einem Blueprint verwenden. Erstellen Sie die Kennworteigenschaft, aber lassen Sie das Textfeld für den Wert leer. Wählen Sie „Überschreibbar“, „Erforderlich“ und „Verschlüsselt“ aus. Wenn das erwartete Kennwort zu Ihrem Endbenutzer gehört, kann der Blueprint-Architekt **In Anforderung anzeigen** auswählen, damit die Benutzer beim Ausfüllen des Anforderungsformulars das Kennwort eingeben müssen.

Option	Beschreibung
<b>Verschlüsselt</b>	Markieren Sie Eigenschaften als verschlüsselt, um den Wert zu maskieren und als Sternchen in vRealize Automation anzuzeigen. Wenn Sie eine Eigenschaft von verschlüsselt zu unverschlüsselt ändern, setzt vRealize Automation den Eigenschaftswert zurück. Sie müssen aus Sicherheitsgründen einen neuen Wert für die Eigenschaft festlegen.
<b>Überschreibbar</b>	Lassen Sie zu, dass Architekten den Wert dieser Eigenschaft bearbeiten können, wenn sie einen Anwendungs-Blueprint zusammenstellen. Wenn Sie einen Wert eingeben, wird er als Standardwert angezeigt.

Option	Beschreibung
<b>Erforderlich</b>	Architekten müssen einen Wert für diese Eigenschaft eingeben oder den von Ihnen eingegebenen Standardwert akzeptieren.
<b>Computing</b>	Werte für Computing-Eigenschaften werden von den Lebenszyklusskripts INSTALL, CONFIGURE, START oder UPDATE zugewiesen. Der zugewiesene Wert wird an die nachfolgend verfügbaren Lebenszyklusphasen und an Komponenten übertragen, die an diese Eigenschaften in einem Blueprint gebunden sind. Wenn Sie „Computing“ für eine Eigenschaft auswählen, die keine Zeichenfolgen-Eigenschaft ist, wird der Eigenschaftstyp in „Zeichenfolge“ geändert.

Wenn Sie die Option für die Computing-Eigenschaft wählen, lassen Sie den Wert für Ihre benutzerdefinierte Eigenschaft leer. Designen Sie Ihre Skripts für die Computing-Werte.

**Tabelle 4-34. Skriptbeispiele für die Computing-Eigenschaftsoption**

Beispiel für die Zeichenfolgen-Eigenschaft	Skriptsyntax	Beispiel für die Nutzung
my_unique_id = ""	Bash - \$my_unique_id	export my_unique_id="0123456789"
	Windows CMD - %my_unique_id%	set my_unique_id=0123456789
	Windows PowerShell - \$my_unique_id	\$my_unique_id = "0123456789"

## Zeichenfolgen-Eigenschaft

Zeichenfolgen-Eigenschaften erwarten Zeichenfolgenwerte. Sie haben die Möglichkeit, die Zeichenfolge selbst einzugeben, jemanden zur Eingabe des Werts aufzufordern oder den Wert aus einer anderen Blueprint-Komponente durch Erstellen einer Bindung zu einer anderen Zeichenfolgen-Eigenschaft abzurufen. Zeichenfolgenwerte können beliebige ASCII-Zeichen enthalten. Verwenden Sie für eine Eigenschaftsbindung die Registerkarte **Eigenschaften** auf der Design-Arbeitsfläche, um die entsprechende Eigenschaft für die Bindung auszuwählen. Der Eigenschaftswert wird dann als Raw-Zeichenfolgendaten an die Aktionsskripte übergeben. Stellen Sie beim Binden einer Blueprint-Zeichenfolgen-Eigenschaft sicher, dass die Blueprint-Komponente, mit der Sie eine Bindung herstellen, nicht clusterfähig ist. Wenn es sich um eine Clusterkomponente handelt, wird der Zeichenfolgenwert zu einem Array und es wird nicht der erwartete Wert abgerufen.

Beispiel für die Zeichenfolgen-Eigenschaft	Skript-Syntax	Beispiel für die Nutzung
admin_email = "admin@email987.com"	Bash - \$admin_email	echo \$admin_email
	Windows CMD - %admin_email%	echo %admin_email%
	Windows PowerShell - \$admin_email	write-output \$admin_email

## Array-Eigenschaft

Array-Eigenschaften erwarten ein Array von Zeichenfolgen-, Ganzzahl-, Dezimal- oder booleschen Werten im Format `["Wert1", "Wert2", "Wert3"...]`. Sie haben die Möglichkeit, die Werte selbst einzugeben, jemanden zur Eingabe der Werte aufzufordern oder die Werte aus einer anderen Blueprint-Komponente durch Erstellen einer Eigenschaftsbindung abzurufen. Wenn Sie Werte für eine Array-Eigenschaft definieren, müssen Sie das Array in eckigen Klammern einschließen. Der Wert in den Array-Elementen für ein Array von Zeichenfolgen kann beliebige ASCII-Zeichen enthalten. Um einen umgekehrten Schrägstrich ordnungsgemäß in einem Wert der Array-Eigenschaft zu codieren, fügen Sie einen zusätzlichen umgekehrten Schrägstrich hinzu. Beispiel: `["c:\\test1\\test2"]`. Verwenden Sie für eine gebundene Eigenschaft die Registerkarte **Eigenschaften** auf der Blueprint-Arbeitsfläche, um die entsprechende Eigenschaft für die Bindung auszuwählen. Wenn Sie eine Bindung zu einem Array herstellen, müssen Sie Ihre Softwarekomponenten so konfigurieren, dass sie kein Werte-Array in einer bestimmten Reihenfolge erwarten.

Beispiel: Nehmen Sie eine virtuelle Maschine des Lastausgleichsdiensts, die die Last für einen Cluster von virtuellen Maschinen des Anwendungsservers ausgleicht. In einem solchen Fall ist eine Array-Eigenschaft für den Lastausgleichsdienst definiert und für das Array der IP-Adressen der virtuellen Maschinen des Anwendungsservers konfiguriert.

Die Konfigurationsskripte des Lastausgleichsdiensts verwenden die Array-Eigenschaft, um das entsprechende Lastausgleichsschema auf den Betriebssystemen Red Hat, Windows und Ubuntu zu konfigurieren.

Beispiel für die Array-Eigenschaft	Skript-Syntax	Beispiel für die Nutzung
operating_systems = ["Red Hat", "Windows", "Ubuntu"]	Bash - \${operating_systems[@]} für das gesamte Array der Zeichenfolgen  \${operating_systems[N]} für das individuelle Array-Element	for (( i = 0 ; i < \${#operating_systems[@]} ; i++ )) ; do echo \${operating_systems[i]} done
	Windows CMD - %operating_systems_N% wo N die Position des Elements im Array darstellt	for /F "delims== tokens=2" %%A in ('set operating_systems_') do ( echo %%A )

Beispiel für die Array-Eigenschaft	Skript-Syntax	Beispiel für die Nutzung
	Windows PowerShell - \$operating_systems für das gesamte Array der Zeichenfolgen \$operating_systems[N] für das individuelle Array-Element	<pre>foreach (\$os in \$operating_systems){     write-output \$os }</pre>

## Inhalts-Eigenschaft

Der aktuelle Eigenschaftswert ist eine URL zu einer Datei, um Inhalte herunterzuladen. Der Software-Agent lädt den Inhalt von der URL auf die virtuelle Maschine herunter und übergibt dem Skript den Speicherort der lokalen Datei in der virtuellen Maschine.

Inhalts-Eigenschaften müssen als gültige URL mit dem HTTP- bzw. HTTPS-Protokoll definiert sein. Beispielsweise wird für die JBOSS Application Server Software-Komponente in der Beispielanwendung „Duke's Bank“ eine Inhaltseigenschaft „cheetah\_tgz\_url“ angegeben. Die Artefakte werden in der Software-Appliance gehostet, und die URL zeigt auf den Speicherort in der Appliance. Der Software-Agent lädt die Artefakte vom angegebenen Speicherort auf die bereitgestellte virtuelle Maschine herunter.

Informationen zu `software.http.proxy`-Einstellungen, die Sie zusammen mit Inhaltseigenschaften verwenden können, finden Sie unter *Referenz für benutzerdefinierte Eigenschaften*.

Beispiel für die Zeichenfolgen-Eigenschaft	Skript-Syntax	Beispiel für die Nutzung
<code>cheetah_tgz_url = "http://app_content_server_ip:port/artifacts/software/jboss/cheetah-2.4.4.tar.gz"</code>	Bash - \$cheetah_tgz_url	<code>tar -zxvf \$cheetah_tgz_url</code>
	Windows CMD - %cheetah_tgz_url%	<code>start /wait c:\unzip.exe %cheetah_tgz_url%</code>
	Windows PowerShell - \$cheetah_tgz_url	<code>&amp; c:\unzip.exe \$cheetah_tgz_url</code>

## Boolesche Eigenschaft

Verwenden Sie den booleschen Eigenschaftstyp, um eine Wahl zwischen „Wahr“ und „Falsch“ im Drop-down-Menü „Wert“ anzubieten.

## Ganzzahleigenschaft

Verwenden Sie den Ganzzahl-Eigenschaftstyp für Nullwerte und positive oder negative ganzzahlige Werte.

## Dezimaleigenschaft

Verwenden Sie den Dezimal-Eigenschaftstyp für Werte, die nicht-periodische Dezimalstellen darstellen.

## Wann Ihre Softwarekomponente Informationen einer anderen Komponente benötigt

Bei verschiedenen Bereitstellungsszenarien ist für eine Komponente der Eigenschaftswert einer anderen Komponente erforderlich, damit sie selbst angepasst werden kann. Zu diesem Zweck können Sie mit vRealize Automation Eigenschaftsbindungen erstellen. Sie können Ihre Softwareaktionsskripts für Eigenschaftsbindungen erstellen, aber die eigentlichen Bindungen werden vom Softwarearchitekten konfiguriert, der den Blueprint zusammenstellt.

Neben der Festlegung eines hartcodierten Werts für eine Eigenschaft kann ein Softwarearchitekt, IaaS-Architekt oder Anwendungsarchitekt Softwarekomponenteneigenschaften an andere Eigenschaften im Blueprint binden, zum Beispiel an eine IP-Adresse oder einen Installationsspeicherort. Beim Binden einer Software-Eigenschaft an eine andere Eigenschaft können Sie ein Skript basierend auf dem Wert einer anderen Komponenteneigenschaft oder VM-Eigenschaft anpassen. Beispielsweise kann eine WAR-Komponente den Installationsspeicherort des Apache Tomcat-Servers benötigen. In Ihren Skripten können Sie die WAR-Komponente so konfigurieren, dass diese den `server_home`-Eigenschaftswert in Ihrem Skript auf den `install_path`-Eigenschaftswert des Apache Tomcat-Servers festlegt. Solange der Architekt, der den Blueprint zusammenstellt, die `server_home`-Eigenschaft an die `install_path`-Eigenschaft des Apache Tomcat-Servers bindet, ist der `server_home`-Eigenschaftswert korrekt festgelegt.

Ihre Aktionsskripts können nur Eigenschaften verwenden, die Sie in diesen Skripten definieren. Darüber hinaus können Sie nur Eigenschaftsbindungen mit Zeichenfolgen- und Array-Werten erstellen. Blueprint-Eigenschafts-Arrays werden nicht in einer bestimmten Reihenfolge zurückgegeben, weshalb die Bindung an clusterfähige oder skalierbare Komponenten möglicherweise nicht die erwarteten Ergebnisse liefert. Angenommen, Ihre Softwarekomponente benötigt alle Maschinen-IDs eines Maschinenclusters und Sie erlauben Ihren Benutzern, einen Cluster zwischen 1 und 10 anzufordern und für die Bereitstellung einen Wert zwischen einer Maschine und 10 Maschinen zu skalieren. Wenn Sie die Softwareeigenschaft als Zeichenfolgentyp konfigurieren, erhalten Sie eine einzelne, zufällig aus dem Cluster ausgewählte Maschinen-ID. Wenn Sie die Softwareeigenschaft als Array-Typ konfigurieren, erhalten Sie ein Array mit allen Maschinen-IDs im Cluster, jedoch nicht in einer bestimmten Reihenfolge. Wenn Ihre Benutzer die Bereitstellung skalieren, könnte die Reihenfolge der Werte für jeden Vorgang variieren. Um sicherzustellen, dass keine Werte für Clusterkomponenten verloren gehen, können Sie den Array-Typ für alle Softwareeigenschaften verwenden. Sie müssen jedoch Ihre Softwarekomponenten so konfigurieren, dass sie kein Werte-Array in einer bestimmten Reihenfolge erwarten.

Beispiele für das Binden eines Zeichenfolgen-Eigenschaftswerts an verschiedene Typen von Eigenschaften finden Sie in der Tabelle „Beispiele für Zeichenfolgen-Eigenschafts-Bindungen“.

**Tabelle 4-35. Beispiele für Zeichenfolgen-Eigenschafts-Bindungen**

Beispiel eines Eigenschaftstyps	Zu bindender Eigenschaftstyp	Ergebnis der Bindung (A wird an B gebunden)
Zeichenfolge (Eigenschaft A)	Zeichenfolge (Eigenschaft B="Hi")	A="Hi"
Zeichenfolge (Eigenschaft A)	Inhalt (Eigenschaft B="http://my.com/content")	A="http://my.com/content"



**Tabelle 4-35. Beispiele für Zeichenfolgen-Eigenschafts-Bindungen (Fortsetzung)**

Beispiel eines Eigenschaftstyps	Zu bindender Eigenschaftstyp	Ergebnis der Bindung (A wird an B gebunden)
Zeichenfolge (Eigenschaft A)	Array (Eigenschaft B=["1", "2"])	A=["1", "2"]
Zeichenfolge (Eigenschaft A)	Computing (Eigenschaft B="Hello")	A="Hello"

Beispiele für das Binden eines Array-Eigenschaftswerts an verschiedene Typen von Eigenschaften finden Sie in der Tabelle „Beispiele für Array-Eigenschafts-Bindungen“.

**Tabelle 4-36. Beispiele für Array-Eigenschafts-Bindungen**

Beispiel eines Eigenschaftstyps	Zu bindender Eigenschaftstyp	Ergebnis der Bindung (A wird an B gebunden)
Array (Eigenschaft A)	Zeichenfolge (Eigenschaft B="Hi")	A="Hi"
Array (Eigenschaft A)	Inhalt (Eigenschaft B="http://my.com/content")	A="http://my.com/content"
Array (Eigenschaft A)	Computing (Eigenschaft B="Hello")	A="Hello"

## Übergeben von Eigenschaftswerten zwischen Lebenszyklusphasen

Mithilfe der Aktionsskripte können Sie Eigenschaftswerte ändern und zwischen Lebenszyklusphasen übergeben.

Sie können den Wert für eine berechnete Eigenschaft ändern und ihn an die nächste Lebenszyklusphase eines Aktionsskripts übergeben. Wenn z. B. der Wert für „progress\_status“ in Komponente A als „bereitgestellt“ definiert ist, können Sie in den Lebenszyklusphasen INSTALLATION und KONFIGURATION den Wert in den entsprechenden Aktionsskripten in „progress\_status=installed“ ändern. Wenn Komponente B an Komponente A gebunden wird, entsprechen die Eigenschaftswerte für „progress\_status“ in den Lebenszyklusphasen des Aktionsskripts denen von Komponente A.

Definieren Sie in der Softwarekomponente, dass Komponente B von Komponente A abhängt. Durch diese Abhängigkeit wird die Übergabe der korrekten Eigenschaftswerte zwischen Komponenten unabhängig davon festgelegt, ob sie sich im selben Knoten oder in verschiedenen Knoten befinden.

Sie können z. B. einen Eigenschaftswert in einem Aktionsskript aktualisieren, indem Sie die unterstützten Skripte verwenden.

- Bash: progress\_status="completed"
- Windows CMD: set progress\_status=completed
- Windows PowerShell: \$progress\_status="completed"

**Hinweis** Die Array- und Inhaltseigenschaft unterstützt nicht die Übergabe von geänderten Eigenschaftswerten zwischen Aktionsskripten von Lebenszyklusphasen.

## Best Practices für die Komponentenentwicklung

Um sich mit Best Practices für die Definition von Eigenschaften und Aktionsskripten vertraut zu machen, können Sie Software-Komponenten und Anwendungs-Blueprints von VMware Solution Exchange herunterladen und importieren.

Halten Sie sich bei der Entwicklung von Software-Komponenten an diese Best Practices.

- Damit ein Skript unterbrechungsfrei ausgeführt werden kann, muss der Rückgabewert auf null (0) gesetzt werden. Mit dieser Einstellung kann der Agent alle Eigenschaften erfassen und sie auf den Software-Server übertragen.
- Für einige Installationsprogramme kann Zugriff auf die TTY-Konsole erforderlich sein. Leiten Sie die Eingabe aus `/dev/console` um. Beispiel: Die Software-Komponente RabbitMQ verwendet den Befehl `./rabbitmq_rhel.py --setup-rabbitmq < /dev/console` im Installationsskript.
- Wenn eine Komponente mehrere Lebenszyklusphasen verwendet, kann der Eigenschaftswert in der Lebenszyklusphase INSTALLATION geändert werden. Der neue Wert wird in die nächste Lebenszyklusphase übernommen. Aktionsskripte können den Wert einer Eigenschaft während der Bereitstellung berechnen, um ihn anderen abhängigen Skripten zur Verfügung zu stellen. Beispiel: In der Beispielanwendung „Clustered Dukes Bank“ berechnet der JBossAppServer-Dienst die Eigenschaft JVM\_ROUTE während der Installationslebenszyklusphase. Diese Eigenschaft wird vom JBossAppServer-Dienst zur Konfiguration des Lebenszyklus verwendet. Der Apache-Lastausgleichsdienst bindet sodann seine Eigenschaft JVM\_ROUTE an die Eigenschaft `all(appserver:JbossAppServer:JVM_ROUTE)`, um den berechneten Endwert von node0 und node1 zu erhalten. Wenn eine Komponente einen Eigenschaftswert aus einer anderen Komponente benötigt, um eine Anwendungsbereitstellung erfolgreich abzuschließen, müssen Sie explizite Abhängigkeiten im Blueprint für die Anwendung angeben.

---

**Hinweis** Sie können den Inhaltseigenschaftswert für eine Komponente, die mehrere Lebenszyklusphasen verwendet, nicht ändern.

---

## Erstellen einer Software -Komponente

Konfigurieren und veröffentlichen Sie eine Software-Komponente, die andere Software-, IaaS- und Anwendungsarchitekten zum Zusammenfügen von Anwendungs-Blueprints verwenden können.

### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **Softwarearchitekt** an.

### Vorgehensweise

- 1 Wählen Sie **Design > Softwarekomponenten** aus.
- 2 Klicken Sie auf das Symbol **Hinzufügen** (+).

### 3 Geben Sie einen Namen und optional eine Beschreibung ein.

Unter Verwendung des Namens, den Sie für die Software-Komponente angegeben haben, erstellt vRealize Automation eine ID für die Software-Komponente, die innerhalb Ihres Mandanten einzigartig ist. Sie können dieses Feld jetzt bearbeiten, aber nach der Speicherung des Blueprints kann es nicht mehr geändert werden. Da IDs permanent und einzigartig innerhalb Ihres Mandanten sind, können Sie sie zum programmatischen Interagieren mit Blueprints und zum Erstellen von Eigenschaftsbindingen verwenden.

### 4 (Optional) Wenn Sie steuern möchten, wie Ihre Software-Komponente in Blueprints eingebunden werden soll, wählen Sie aus dem Dropdown-Menü **Container** einen Containertyp aus.

Option	Beschreibung
<b>Maschinen</b>	Ihre Software-Komponente muss direkt auf einer Maschine abgelegt werden.
<b>Eine Ihrer veröffentlichten Software-Komponenten</b>	Wenn Sie eine Software-Komponente speziell zur Installation auf einer anderen von Ihnen erstellten Software-Komponente entwerfen, wählen Sie diese Software-Komponente aus der Liste aus. Wenn Sie beispielsweise eine EAR-Komponente speziell zur Installation auf einer zuvor erstellten JBOSS-Komponente entwerfen, wählen Sie Ihre JBOSS-Komponente aus der Liste aus.
<b>Software-Komponenten</b>	Wenn Sie eine Software-Komponente entwerfen, die nicht direkt auf einer Maschine installiert werden soll, sondern auf mehreren verschiedenen Software-Komponenten installiert werden kann, wählen Sie die Option „Software-Komponenten“ aus. Wenn Sie beispielsweise eine WAR-Komponente entwerfen, die auf Ihrer Tomcat-Server-Software-Komponente und auf Ihrer Tcserver-Software-Komponente installiert werden soll, wählen Sie den Containertyp „Software-Komponenten“ aus.

### 5 Klicken Sie auf **Weiter**.

### 6 Definieren Sie Eigenschaften, die Sie in Ihren Aktionsskripts zu verwenden beabsichtigen.

- a Klicken Sie auf das Symbol **Hinzufügen (+)**.
- b Geben Sie einen Namen für die Eigenschaft ein.
- c Geben Sie eine Beschreibung für die Eigenschaft ein.

Diese Beschreibung wird Architekten angezeigt, die Ihre Software-Komponente in Blueprints verwenden.

- d Wählen Sie den erwarteten Typ für den Wert Ihrer Eigenschaft aus.
- e Definieren Sie den Wert für Ihre Eigenschaft.

Option	Beschreibung
Von Ihnen jetzt angegebenen Wert verwenden	<ul style="list-style-type: none"> <li>■ Geben Sie einen Wert ein.</li> <li>■ Deaktivieren Sie <b>Überschreibbar</b>.</li> <li>■ Wählen Sie <b>Erforderlich</b> aus.</li> </ul>
Architekten zur Angabe eines Wert auffordern	<ul style="list-style-type: none"> <li>■ Geben Sie einen Wert als Standardwert ein.</li> <li>■ Wählen Sie <b>Überschreibbar</b> aus.</li> <li>■ Wählen Sie <b>Erforderlich</b> aus.</li> </ul>
Architekten, falls von diesen erwünscht, die Angabe eines Wert erlauben	<ul style="list-style-type: none"> <li>■ Geben Sie einen Wert als Standardwert ein.</li> <li>■ Wählen Sie <b>Überschreibbar</b> aus.</li> <li>■ Deaktivieren Sie <b>Erforderlich</b>.</li> </ul>

Architekten können Ihre Software-Eigenschaften so konfigurieren, dass diese Benutzern im Anforderungsformular angezeigt werden. Über die Option „In Anforderung anzeigen“ können Architekten von den Benutzern verlangen oder diese dazu auffordern, Werte für Eigenschaften einzugeben, die Sie als überschreibbar markieren.

- 7 Folgen Sie den Anweisungen, um ein Skript für mindestens eine der Software-Lebenszyklusaktionen bereitzustellen.

**Tabelle 4-37. Lebenszyklusaktionen**

Lebenszyklusaktionen	Beschreibung
Installieren	Installiert Ihre Software. Beispielsweise können Sie Tomcat-Server-Installationsbits herunterladen und einen Tomcat-Dienst installieren. Skripts, die Sie für die Installationslebenszyklus-Aktion erstellen, werden bei der erstmaligen Bereitstellung von Software ausgeführt, entweder während der Erstinstallationsanforderung oder im Rahmen einer horizontalen Skalierung.
Konfigurieren	Konfiguriert Ihre Software. Für das Tomcat-Beispiel können Sie JAVA_OPTS und CATALINA_OPTS festlegen. Konfigurationsskripts werden nach Abschluss der Installationsaktion ausgeführt.
Start	Startet Ihre Software. Beispielsweise können Sie den Tomcat-Dienst mithilfe des Startbefehls auf dem Tomcat-Server starten. Startskripts werden nach Abschluss der Konfigurationsaktion ausgeführt.
Aktualisieren	Wenn Sie für Ihre Softwarekomponente die Unterstützung skalierbarer Blueprints konfigurieren, werden alle Aktualisierungen durchgeführt, die nach einer vertikalen oder horizontalen Skalierung erforderlich sind. Beispielsweise können Sie die Clustergröße für eine skalierte Bereitstellung ändern und die Clusterknoten mithilfe eines Lastausgleichsdiensts verwalten. Konfigurieren Sie Ihre Aktualisierungsskripts für die mehrmalige Ausführung (idempotent) und für die horizontale und vertikale Skalierung. Wenn ein Skalierungsvorgang durchgeführt wird, werden Aktualisierungsskripts auf allen abhängigen Softwarekomponenten ausgeführt.
Deinstallieren	Deinstalliert Ihre Software. Beispielsweise können Sie bestimmte Aktionen für die Anwendung ausführen, bevor eine Bereitstellung gelöscht wird. Deinstallationsskripts werden ausgeführt, wenn Softwarekomponenten gelöscht werden.

Beziehen Sie Beendigungs- und Statuscodes in Ihre Aktionsskripts ein. Jeder unterstützte Skripttyp hat jeweils spezifische Anforderungen in Bezug auf Exit- und Status-Codes.

Skripttyp	Erfolgsstatus	Fehlerstatus	Nicht unterstützte Befehle
Bash	<ul style="list-style-type: none"> <li>■ return 0</li> <li>■ exit 0</li> </ul>	<ul style="list-style-type: none"> <li>■ return non-zero</li> <li>■ exit non-zero</li> </ul>	Keine
Windows CMD	exit /b 0	exit /b non-zero	Keine exit 0- oder exit non-zero-Codes verwenden.
PowerShell	exit 0	exit non-zero;	Keine warning-, verbose-, debug- oder host-Aufrufe verwenden.

- 8 Wählen Sie für jedes Skript, das einen Neustart der Maschine erfordert, das Kontrollkästchen **Neu starten** aus.

Nach der Ausführung des Skripts wird die Maschine vor dem Start des nächsten Lebenszyklusskripts neu gestartet.

- 9 Klicken Sie auf **Beenden**.

- 10 Wählen Sie Ihre Software-Komponente aus und klicken Sie auf **Veröffentlichen**.

Sie haben eine Software-Komponente konfiguriert und veröffentlicht. Andere Software-, IaaS- und Anwendungsarchitekten können diese Software-Komponente verwenden, um Software zu Anwendungs-Blueprints hinzuzufügen.

#### Weiter

Fügen Sie Ihre veröffentlichte Software-Komponente einem Anwendungs-Blueprint hinzu. Siehe [Erstellen zusammengesetzter Blueprints](#).

## Szenario: Erstellen einer MySQL- Software komponente für Rainpole

Mit Ihren Rechten als Softwarearchitekt erstellen Sie eine MySQL-Softwarekomponente, um MySQL auf vSphere CentOS-Maschinen zu installieren. Beim Entwerfen der MySQL-Softwarekomponente für eine virtuelle CentOS-Maschine konfigurieren Sie die Installations-, Konfigurations- und Startparameter sowie die Skripts für Linux-Betriebssysteme.

#### Vorgehensweise

- 1 Wählen Sie **Design > Softwarekomponenten** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Geben Sie **MySQL für virtuelle Linux-Maschinen** in das Textfeld **Name** ein.
- 4 Stellen Sie sicher, dass der Bezeichner dem angegebenen Namen entsprechend aufgefüllt wird.  
Beispiel: Software.MySQLforLinuxVirtualMachines

- 5 Geben Sie **MySQL-Installation und -Konfiguration** in das Textfeld **Beschreibung** ein.

- 6 Wählen Sie **Maschine** aus dem Dropdown-Menü **Container** aus.

Da MySQL nur direkt auf einer Maschine installiert werden soll, wird vermieden, dass Architekten Ihre MySQL Software-Komponente auf anderen Software-Komponenten ablegen.

- 7 Klicken Sie auf **Weiter**.

- 8 Klicken Sie auf **Neu**, um daraufhin jede der folgenden Eigenschaften für das Installationsskript hinzuzufügen und zu konfigurieren.

Klicken Sie auf **OK**, um die einzelnen Eigenschaften zu speichern.

Architekten können Ihre Software-Eigenschaften so konfigurieren, dass diese Benutzern im Anforderungsformular angezeigt werden. Über die Option „In Anforderung anzeigen“ können Architekten von den Benutzern verlangen oder diese dazu auffordern, Werte für Eigenschaften einzugeben, die Sie als überschreibbar markieren.

Name	Beschreibung	Typ	Wert	Ver-schlüs-selt	Über-schreiben-zulassen	Erfor-derlich	Compu-ting
db_root_username	Root-Benutzername der Datenbank	String	root	Nein	Ja	Ja	Nein
JAVA_HOME	Das Verzeichnis, in dem JRE 1.8 oder höher installiert ist	String	/opt/vmware-jre	Nein	Ja	Ja	Nein
global_ftp_proxy	URL des FTP-Proxys, sofern vorhanden. Nicht erforderlich.	String		Nein	Ja	Nein	Nein
db_port	MySQL-Datenbankport	String		Nein	Ja	Ja	Nein
db_root_password	Root-Benutzerkennwort der Datenbank	String	Kennwort	Ja	Ja	Ja	Nein
global_http_proxy	URL des HTTP-Proxys, sofern vorhanden. Nicht erforderlich.	String		Nein	Ja	Nein	Nein
global_https_proxy	URL des HTTPS-Proxys, sofern vorhanden. Nicht erforderlich.	String		Nein	Ja	Nein	Nein
max_allowed_packet_size	Maximal zulässige Paketgröße für den Server	Integer	1024	Nein	Ja	Nein	Nein

- 9 Klicken Sie auf **Weiter**.
- 10 Konfigurieren Sie die Aktion „Installieren“.
- Wählen Sie **Bash** aus dem Dropdown-Menü **Skripttyp** aus.
  - Klicken Sie auf **Zum Bearbeiten hier klicken**.

## c Fügen Sie das folgende Skript ein.

```
#!/bin/bash

#Setting proxies
export ftp_proxy=${ftp_proxy:-$global_ftp_proxy}
echo "Setting ftp_proxy to $ftp_proxy"

export http_proxy=${http_proxy:-$global_http_proxy}
echo "Setting http_proxy to $http_proxy"

export https_proxy=${https_proxy:-$global_https_proxy}
echo "Setting https_proxy to $https_proxy"

#
# Determine operating system and version
#
export OS=
export OS_VERSION=

if [ -f /etc/redhat-release ]; then
    # For CentOS the result will be 'CentOS'
    # For RHEL the result will be 'Red'
    OS=$(cat /etc/redhat-release | awk '{print $1}')

    if [ -n $OS ] && [ $OS = 'CentOS' ]; then
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $3}')
    else
        # RHEL
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $7}')
    fi

elif [ -f /etc/SuSE-release ]; then
    OS=SuSE

    MAJOR_VERSION=$(cat /etc/SuSE-release | grep VERSION | awk '{print $3}')
    PATCHLEVEL=$(cat /etc/SuSE-release | grep PATCHLEVEL | awk '{print $3}')

    OS_VERSION="$MAJOR_VERSION.$PATCHLEVEL"

elif [ -f /usr/bin/lsb_release ]; then
    # For Ubuntu the result is 'Ubuntu'
    OS=$(lsb_release -a 2> /dev/null | grep Distributor | awk '{print $3}')
    OS_VERSION=$(lsb_release -a 2> /dev/null | grep Release | awk '{print $2}')

fi

echo "Using operating system '$OS' and version '$OS_VERSION'"

if [ "x${global_http_proxy}" == "x" ] || [ "x${global_https_proxy}" == "x" ] ||
[ "x${global_ftp_proxy}" == "x" ]; then
    echo ""
    echo "#####"
    echo "# One or more PROXY(s) not set. Network downloads may fail #"
    echo "#####"
```

```

    echo ""
fi

export PATH=$PATH:$JAVA_HOME/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
set -e

# Tested on CentOS
if [ -x /usr/sbin/selinuxenabled ] && /usr/sbin/selinuxenabled; then
    # SELinux can be disabled by setting "/usr/sbin/setenforce Permissive"
    echo 'SELinux is enabled on this VM template. This service requires SELinux to be disabled to install successfully'
    exit 1
fi

if [ "x$OS" != "x" ] && [ "$OS" = 'Ubuntu' ]; then
    # Fix the linux-firmware package
    export DEBIAN_FRONTEND=noninteractive
    apt-get install -y linux-firmware < /dev/console > /dev/console
    # Install MySQL package
    apt-get install -y mysql-server
else
    yum --nogpgcheck --noplugins -y install -x MySQL-server-community mysql-server
fi

# Set Install Path to the default install path (For monitoring)
Install_Path=/usr
echo Install_Path is set to $Install_Path, please modify this script if the install path is not correct.

```

d Klicken Sie auf **OK**.

## 11 Konfigurieren Sie die Aktion „Konfigurieren“.

- a Wählen Sie **Bash** aus dem Dropdown-Menü **Skripttyp** aus.
- b Klicken Sie auf **Zum Bearbeiten hier klicken**.



## c Fügen Sie das folgende Skript ein.

```
#!/bin/bash

#Setting proxies
export ftp_proxy=${ftp_proxy:-$global_ftp_proxy}
echo "Setting ftp_proxy to $ftp_proxy"

export http_proxy=${http_proxy:-$global_http_proxy}
echo "Setting http_proxy to $http_proxy"

export https_proxy=${https_proxy:-$global_https_proxy}
echo "Setting https_proxy to $https_proxy"

#
# Determine operating system and version
#
export OS=
export OS_VERSION=

if [ -f /etc/redhat-release ]; then
    # For CentOS the result will be 'CentOS'
    # For RHEL the result will be 'Red'
    OS=$(cat /etc/redhat-release | awk '{print $1}')

    if [ -n $OS ] && [ $OS = 'CentOS' ]; then
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $3}')
    else
        # RHEL
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $7}')
    fi

elif [ -f /etc/SuSE-release ]; then
    OS=SuSE

    MAJOR_VERSION=$(cat /etc/SuSE-release | grep VERSION | awk '{print $3}')
    PATCHLEVEL=$(cat /etc/SuSE-release | grep PATCHLEVEL | awk '{print $3}')

    OS_VERSION="$MAJOR_VERSION.$PATCHLEVEL"

elif [ -f /usr/bin/lsb_release ]; then
    # For Ubuntu the result is 'Ubuntu'
    OS=$(lsb_release -a 2> /dev/null | grep Distributor | awk '{print $3}')
    OS_VERSION=$(lsb_release -a 2> /dev/null | grep Release | awk '{print $2}')

fi

echo "Using operating system '$OS' and version '$OS_VERSION'"

if [ "x${global_http_proxy}" == "x" ] || [ "x${global_https_proxy}" == "x" ] ||
[ "x${global_ftp_proxy}" == "x" ]; then
    echo ""
    echo "#####"
    echo "# One or more PROXY(s) not set. Network downloads may fail #"
    echo "#####"
```

```

        echo ""
    fi

    export PATH=$PATH:$JAVA_HOME/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
    set -e

    # Locate the my.cnf file
    my_cnf_file=
    if [ -f /etc/my.cnf ]; then
        my_cnf_file=/etc/my.cnf
    elif [ -f /etc/mysql/my.cnf ]; then
        my_cnf_file=/etc/mysql/my.cnf
    fi

    if [ "x$my_cnf_file" = "x" ]; then
        echo "Neither /etc/my.cnf nor /etc/mysql/my.cnf can be found, stopping configuration"
        exit 1
    fi

    # update mysql configuration to handle big packets
    sed -ie "s/\[mysqld\]/\[mysqld\]\n\
max_allowed_packet=$max_allowed_packet/g" $my_cnf_file
    # update listening port
    sed -ie "s/\[mysqld\]/\[mysqld\]\n\
port=$db_port/g" $my_cnf_file

    sed -i "s/port.*=[0-9]*/port=$db_port/g" $my_cnf_file

    if [ "x$OS" != "x" ] && [ "$OS" = 'Ubuntu' ]; then
        # Make sure that MySQL is started
        service mysql restart
    else
        # set up auto-start on booting
        chkconfig mysqld on
        # restart mysqld service
        service mysqld start
    fi

    # this will assign a password for mysql admin user 'root'
    mysqladmin -u $db_root_username password $db_root_password

```

d Klicken Sie auf **OK**.

## 12 Konfigurieren Sie die Aktion „Start“.

- a Wählen Sie **Bash** aus dem Dropdown-Menü **Skripttyp** aus.
- b Klicken Sie auf **Zum Bearbeiten hier klicken**.

- c Fügen Sie das folgende Skript ein.

```
#!/bin/sh

echo "The maximum allowed packet size is: "
```

- d Setzen Sie den Cursor zwischen den Doppelpunkt und das Anführungszeichen.
- e Wählen Sie **max\_allowed\_packet\_size** aus dem Dropdown-Menü **Einzufügende Eigenschaft auswählen** aus.

Die Eigenschaft ist jetzt im Skript enthalten.

```
#!/bin/sh

echo "The maximum allowed packet size is: $max_allowed_packet_size"
```

- f Klicken Sie auf **OK**.

**13** Klicken Sie auf **Weiter**.

**14** Klicken Sie auf **Fertig stellen**.

**15** Wählen Sie die Zeile aus, die „MySQL für virtuelle Linux-Maschinen“ enthält, und klicken Sie auf **Veröffentlichen**.

Ihre MySQL-Softwarekomponente steht anderen Architekten auf der Blueprint-Design-Seite zur Verfügung. Softwarekomponenten können aber erst verfügbar gemacht werden, wenn Sie sie mit einer Maschine kombinieren.

## Weiter

Mit Ihren Rechten als Softwarearchitekt, Anwendungsarchitekt oder IaaS-Architekt kombinieren Sie Ihre MySQL-Komponente mit dem Blueprint für die CentOS für Software-Maschine.

## Software -Komponenteneinstellungen

Konfigurieren Sie allgemeine Einstellungen, erstellen Sie Eigenschaften und schreiben Sie benutzerdefinierte Aktionsskripts zum Installieren, Konfigurieren, Aktualisieren oder Deinstallieren der Software-Komponente auf bereitgestellten Maschinen.

Als Software-Architekt klicken Sie auf **Design > Softwarekomponenten** und anschließend auf das Symbol **Hinzufügen** zum Erstellen einer neuen Software-Komponente.

## Neue allgemeine Software -Einstellungen

Wenden Sie allgemeine Einstellungen auf die Software-Komponente an.

**Tabelle 4-38. Neue allgemeine Software -Einstellungen**

Einstellung	Beschreibung
<b>Name</b>	Geben Sie einen Namen für die Software-Komponente ein.
<b>ID</b>	Unter Verwendung des Namens, den Sie für die Software-Komponente angegeben haben, erstellt vRealize Automation eine ID für die Software-Komponente, die innerhalb Ihres Mandanten einzigartig ist. Sie können dieses Feld jetzt bearbeiten, aber nach der Speicherung des Blueprints kann es nicht mehr geändert werden. Da IDs permanent und einzigartig innerhalb Ihres Mandanten sind, können Sie sie zum programmatischen Interagieren mit Blueprints und zum Erstellen von Eigenschaftsbindungen verwenden.
<b>Beschreibung</b>	Fassen Sie die Software-Komponente zugunsten anderer Architekten zusammen.
<b>Container</b>	<p>Auf der Design-Arbeitsfläche können Blueprint-Architekten Ihre Softwarekomponente nur in dem von Ihnen ausgewählten Container-Typ platzieren.</p> <ul style="list-style-type: none"> <li>■ Wählen Sie <b>Maschinen</b> aus, damit Architekten Ihre Softwarekomponente direkt auf einer Maschinenkomponente in der Design-Arbeitsfläche platzieren müssen.</li> <li>■ Wählen Sie <b>Softwarekomponenten</b> aus, wenn Sie eine Softwarekomponente entwerfen, die nie direkt auf einer Maschinenkomponente platziert werden sollte, aber in einer von mehreren verschiedenen Softwarekomponenten verschachtelt werden kann.</li> <li>■ Wählen Sie eine bestimmte veröffentlichte Softwarekomponente aus, wenn Sie eine Softwarekomponente speziell zum Verschachteln in einer anderen von Ihnen erstellten Softwarekomponente entwerfen.</li> </ul>

## Neue Software -Eigenschaften

Software-Komponenteneigenschaften werden verwendet, um Skripts so zu parametrisieren, dass sie definierte Eigenschaften als Umgebungsvariablen an Skripts übergeben können, die in einer Maschine ausgeführt werden. Vor dem Ausführen der Skripts kommuniziert der Software-Agent in der bereitgestellten Maschine mit vRealize Automation, um die Eigenschaften aufzulösen. Der Agent erstellt dann aus diesen Eigenschaften die skriptspezifischen Variablen und übergibt sie an die Skripts.

**Tabelle 4-39. Neue Software -Eigenschaften**

Einstellung	Beschreibung
<b>Name</b>	Geben Sie einen Namen für die Software-Eigenschaft ein. Bei den Eigenschaftsnamen wird die Groß- und Kleinschreibung berücksichtigt. Die Namen können nur alphabetische bzw. numerische Zeichen, Bindestriche (-) oder Unterstriche (_) enthalten.
<b>Beschreibung</b>	Fassen Sie zugunsten anderer Benutzer die Eigenschaft und alle Anforderungen für den Wert zusammen.

Tabelle 4-39. Neue Software -Eigenschaften (Fortsetzung)

Einstellung	Beschreibung
Typ	Software unterstützt Zeichenfolgen-, Array-, Inhalts-, Ganzzahl- und boolesche Typen. Eine ausführliche Erklärung der unterstützten Eigenschaftstypen finden Sie unter <a href="#">Eigenschaftstypen und Einstellungsoptionen</a> . Informationen zu Eigenschaftsbindungen finden Sie unter <a href="#">Wann Ihre Softwarekomponente Informationen einer anderen Komponente benötigt</a> und <a href="#">Erstellen von Eigenschaftsbindungen zwischen Blueprint-Komponenten</a> .
Wert	<ul style="list-style-type: none"> <li>■ So verwenden Sie den von Ihnen angegebenen Wert: <ul style="list-style-type: none"> <li>■ Geben Sie einen <b>Wert</b> ein.</li> <li>■ Wählen Sie <b>Erforderlich</b> aus.</li> <li>■ Deaktivieren Sie <b>Überschreibbar</b>.</li> </ul> </li> <li>■ So fordern Sie Architekten zur Angabe eines Werts auf: <ul style="list-style-type: none"> <li>■ (Optional) Geben Sie einen <b>Wert</b> ein, um einen Standardwert festzulegen.</li> <li>■ Wählen Sie <b>Überschreibbar</b> aus.</li> <li>■ Wählen Sie <b>Erforderlich</b> aus.</li> </ul> </li> <li>■ So erlauben Sie Architekten, einen Wert anzugeben oder den Wert leer zu lassen: <ul style="list-style-type: none"> <li>■ (Optional) Geben Sie einen <b>Wert</b> ein, um einen Standardwert festzulegen.</li> <li>■ Wählen Sie <b>Überschreibbar</b> aus.</li> <li>■ Deaktivieren Sie <b>Erforderlich</b>.</li> </ul> </li> </ul>
Verschlüsselt	<p>Markieren Sie Eigenschaften als verschlüsselt, um den Wert zu maskieren und als Sternchen in vRealize Automation anzuzeigen. Wenn Sie eine Eigenschaft von verschlüsselt zu unverschlüsselt ändern, setzt vRealize Automation den Eigenschaftswert zurück. Sie müssen aus Sicherheitsgründen einen neuen Wert für die Eigenschaft festlegen.</p> <p><b>Wichtig</b> Wenn geschützte Eigenschaften im Skript mit dem Befehl <code>echo</code> oder mit anderen ähnlichen Befehlen ausgegeben werden, werden diese Werte in Protokolldateien in Klartext angezeigt. Die Werte in den Protokolldateien werden nicht verborgen.</p>
Überschreibbar	Lassen Sie zu, dass Architekten den Wert dieser Eigenschaft bearbeiten können, wenn sie einen Anwendungs-Blueprint zusammenstellen. Wenn Sie einen Wert eingeben, wird er als Standardwert angezeigt.

**Tabelle 4-39. Neue Software -Eigenschaften (Fortsetzung)**

Einstellung	Beschreibung
Erforderlich	Architekten müssen einen Wert für diese Eigenschaft eingeben oder den von Ihnen eingegebenen Standardwert akzeptieren.
Computing	Werte für Computing-Eigenschaften werden von den Lebenszyklusskripts INSTALL, CONFIGURE, START oder UPDATE zugewiesen. Der zugewiesene Wert wird an die nachfolgend verfügbaren Lebenszyklusphasen und an Komponenten übertragen, die an diese Eigenschaften in einem Blueprint gebunden sind. Wenn Sie „Computing“ für eine Eigenschaft auswählen, die keine Zeichenfolgen-Eigenschaft ist, wird der Eigenschaftstyp in „Zeichenfolge“ geändert.

### Neue Software -Aktionen

Sie erstellen Bash-, Windows CMD- oder PowerShell-Aktionsskripts, um anzugeben, wie genau Komponenten bei Bereitstellungsskalierungsvorgängen installiert, konfiguriert, deinstalliert oder aktualisiert werden.

**Tabelle 4-40. Lebenszyklusaktionen**

Lebenszyklusaktionen	Beschreibung
Installieren	Installiert Ihre Software. Beispielsweise können Sie Tomcat-Server-Installationsbits herunterladen und einen Tomcat-Dienst installieren. Skripts, die Sie für die Installationslebenszyklus-Aktion erstellen, werden bei der erstmaligen Bereitstellung von Software ausgeführt, entweder während der Erstinstallationsanforderung oder im Rahmen einer horizontalen Skalierung.
Konfigurieren	Konfiguriert Ihre Software. Für das Tomcat-Beispiel können Sie JAVA_OPTS und CATALINA_OPTS festlegen. Konfigurationsskripts werden nach Abschluss der Installationsaktion ausgeführt.
Start	Startet Ihre Software. Beispielsweise können Sie den Tomcat-Dienst mithilfe des Startbefehls auf dem Tomcat-Server starten. Startskripts werden nach Abschluss der Konfigurationsaktion ausgeführt.
Aktualisieren	Wenn Sie für Ihre Softwarekomponente die Unterstützung skalierbarer Blueprints konfigurieren, werden alle Aktualisierungen durchgeführt, die nach einer vertikalen oder horizontalen Skalierung erforderlich sind. Beispielsweise können Sie die Clustergröße für eine skalierte Bereitstellung ändern und die Clusterknoten mithilfe eines Lastausgleichsdiensts verwalten. Konfigurieren Sie Ihre Aktualisierungsskripts für die mehrmalige Ausführung (idempotent) und für die horizontale und vertikale Skalierung. Wenn ein Skalierungsvorgang durchgeführt wird, werden Aktualisierungsskripts auf allen abhängigen Softwarekomponenten ausgeführt.
Deinstallieren	Deinstalliert Ihre Software. Beispielsweise können Sie bestimmte Aktionen für die Anwendung ausführen, bevor eine Bereitstellung gelöscht wird. Deinstallationsskripts werden ausgeführt, wenn Softwarekomponenten gelöscht werden.

Wählen Sie für jedes Skript, das einen Neustart der Maschine erfordert, das Kontrollkästchen **Neu starten** aus. Nach der Ausführung des Skripts wird die Maschine vor dem Start des nächsten Lebenszyklusskripts neu gestartet. Stellen Sie sicher, dass keine Prozesse zu Benutzereingaben auffordern, wenn das Aktionsskript ausgeführt wird. Unterbrechungen halten das Skript an, sodass es im Leerlauf verbleibt, bis

es schließlich fehlschlägt. Darüber hinaus müssen Ihre Skripts entsprechende Beendigungs- und Rückgabecodes für die Anwendungsbereitstellung enthalten. Wenn ein Skript keine Beendigungs- und Rückgabecodes aufweist, wird der zuletzt im Skript ausgeführte Befehl zum Beendigungsstatus. Beendigungs- und Rückgabecodes variieren für die unterstützten Skripttypen „Bash“, „Windows CMD“ und „PowerShell“.

Skripttyp	Erfolgsstatus	Fehlerstatus	Nicht unterstützte Befehle
Bash	<ul style="list-style-type: none"> <li>■ return 0</li> <li>■ exit 0</li> </ul>	<ul style="list-style-type: none"> <li>■ return non-zero</li> <li>■ exit non-zero</li> </ul>	Keine
Windows CMD	exit /b 0	exit /b non-zero	Keine exit 0- oder exit non-zero-Codes verwenden.
PowerShell	exit 0	exit non-zero;	Keine warning-, verbose-, debug- oder host-Aufrufe verwenden.

## Erstellen von XaaS -Blueprints und -Ressourcenaktionen

Die XaaS-Blueprints können als Katalogelemente veröffentlicht oder auf der Design-Arbeitsfläche des Blueprints verwendet werden. Die Ressourcenaktionen sind Aktionen, die für bereitgestellte Elemente ausgeführt werden.

XaaS verwendet vRealize Orchestrator zur Ausführung von Workflows, die Elemente bereitstellen oder Aktionen ausführen. Beispielsweise können Sie die Workflows zum Erstellen von virtuellen vSphere-Maschinen, Active Directory-Benutzern in Gruppen oder PowerShell-Skripts konfigurieren. Wenn Sie einen benutzerdefinierten vRealize Orchestrator-Workflow erstellen, können Sie diesen Workflow als Element im Servicekatalog bereitstellen, damit die berechtigten Benutzer den Workflow ausführen können.

## Verwenden von XaaS -Blueprints auf der Design-Arbeitsfläche des Blueprints

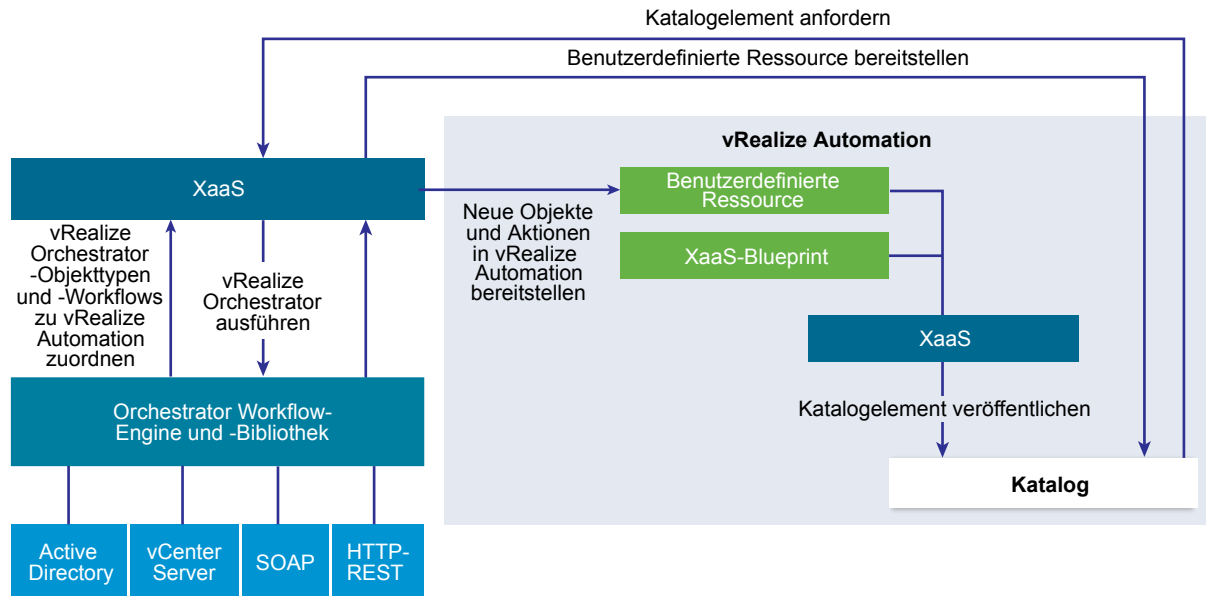
Wenn Sie einen XaaS-Blueprint auf der Design-Arbeitsfläche als Blueprint-Maschinenkomponente verwenden, wird der XaaS-Blueprint aus den vertikalen und horizontalen Skalierungsaktionen ausgeschlossen, die in der Umgebung ausgeführt werden können. Alle Änderungen, die Sie an der XaaS-Komponente in einer Bereitstellung vornehmen, werden von den Skalierungsaktionen nicht erkannt. Wenn Sie die XaaS-Komponente mit den Skalierungsänderungen abgleichen möchten, die Sie an der Bereitstellung vorgenommen haben, müssen Sie diese Aktionen mithilfe von XaaS-Ressourcenaktionen separat auf der XaaS-Komponente ausführen.

## vRealize Orchestrator -Integration in vRealize Automation

vRealize Orchestrator ist die in vRealize Automation integrierte Workflow-Engine.

Der vRealize Orchestrator-Server, der mit vRealize Automation verteilt wird, ist vorkonfiguriert. Wenn daher der Systemadministrator die vRealize Automation-Appliance bereitstellt, wird der vRealize Orchestrator-Server bereits ausgeführt.

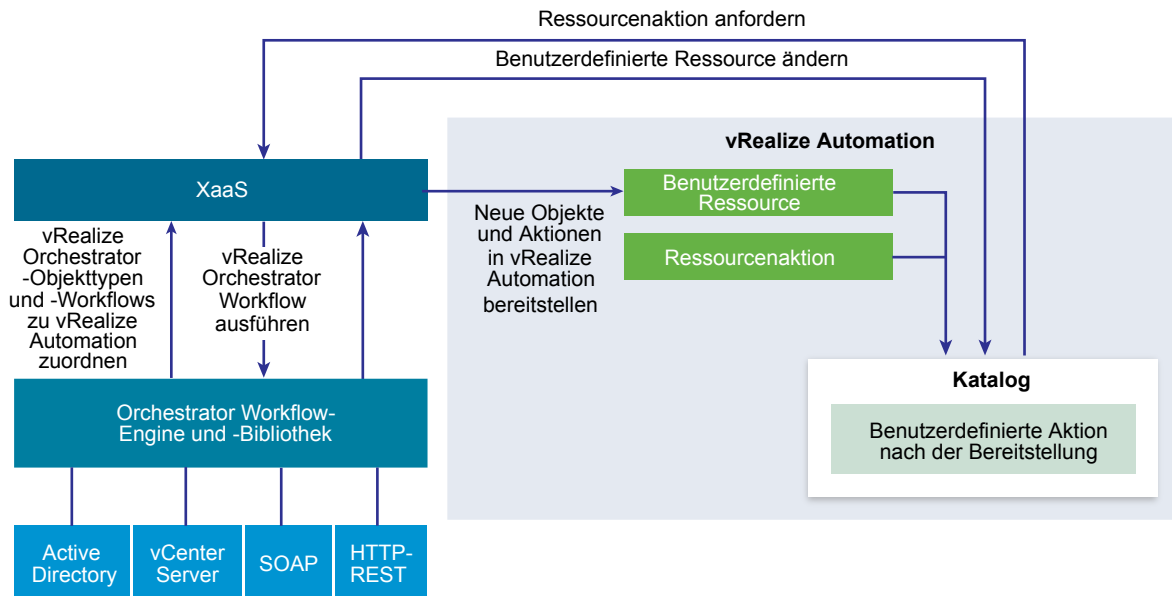
**Abbildung 4-1. Erstellen und Anfordern von Katalogelementen in XaaS zur Bereitstellung einer benutzerdefinierten Ressource**



XaaS-Architekten fügen benutzerdefinierte Ressourcen für die unterstützten Endpoints und bereitgestellten Workflows hinzu und erstellen dann XaaS-Blueprints und Aktionen auf Grundlage dieser Ressourcen. Mandantenadministratoren und Business-Gruppenmanager können die XaaS-Blueprints und Aktionen zum Servicekatalog hinzufügen. Der XaaS-Blueprint kann auch im Blueprint-Designer verwendet werden.

Wenn der Servicekatalogbenutzer ein Element anfordert, führt vRealize Automation einen vRealize Orchestrator-Workflow aus, um die benutzerdefinierte Ressource bereitzustellen.

**Abbildung 4-2. Erstellen und Anfordern von Aktionen für benutzerdefinierte Ressourcen zum Ändern einer benutzerdefinierten Ressource**





XaaS-Architekten können auch vRealize Orchestrator-Workflows als Ressourcenaktionen hinzufügen, um die vRealize Automation-Möglichkeiten zu erweitern. Nachdem die Servicekatalogbenutzer eine benutzerdefinierte Ressource bereitgestellt haben, können sie die Aktion nach der Bereitstellung ausführen. So können die Verbraucher einen vRealize Orchestrator-Workflow ausführen und die bereitgestellte benutzerdefinierte Ressource ändern.

Wenn ein Servicekatalogbenutzer einen XaaS-Blueprint oder eine Ressourcenaktion als Katalogelement anfordert, führt der XaaS-Dienst den entsprechenden vRealize Orchestrator-Workflow aus und übergibt die folgenden Daten als globale Parameter an den Workflow:

**Tabelle 4-41. Globale XaaS -Parameter**

Parameter	Beschreibung
__asd_tenantRef	Der Mandant des Benutzers, der den Workflow anfordert.
__asd_subtenantRef	Die Business-Gruppe des Benutzers, der den Workflow anfordert.
__asd_catalogRequestId	Die Anforderungs-ID aus dem Katalog für diese Workflow-Ausführung.
__asd_requestedFor	Der Zielbenutzer der Anforderung. Wenn die Aufforderung für einen Benutzer erfolgt, dann ist dies der Benutzer, für den der Workflow angefordert wird; andernfalls handelt es sich um den Benutzer, der den Workflow anfordert.
__asd_requestedBy	Der Benutzer, der den Workflow anfordert.

Wenn ein XaaS-Blueprint oder eine Ressourcenaktion einen vRealize Orchestrator-Workflow verwendet, der ein Benutzerinteraktions-Schemaelement enthält, und ein Verbraucher den Dienst anfordert, dann hält der Workflow die Ausführung an und wartet, bis der Benutzer die erforderlichen Daten bereitstellt. Um eine wartende Benutzerinteraktion zu beantworten, navigiert der Benutzer zu **Posteingang > Manuelle Benutzeraktion**.

Die Standard-vRealize Orchestrator-Serverbestandsliste wird für alle Mandanten freigegeben und kann nicht auf Mandantenbasis verwendet werden. Wenn beispielsweise ein Dienstarchitekt einen Dienst-Blueprint erstellt, um eine Cluster-Computing-Ressource zu erstellen, müssen die Verbraucher von verschiedenen Mandanten die Bestandslistenelemente aller vCenter Server-Instanzen durchsuchen, auch wenn sie zu einem anderen Mandanten gehören.

Systemadministratoren können vRealize Orchestrator installieren oder die VMware vRealize™ Orchestrator Appliance™ getrennt bereitstellen, um eine externe vRealize Orchestrator-Instanz einzurichten, und vRealize Automation für die Arbeit mit dieser externen vRealize Orchestrator-Instanz konfigurieren.

Systemadministratoren können auch vRealize Orchestrator-Workflow-Kategorien nach Mandant konfigurieren und definieren, welche Workflows für jeden Mandanten verfügbar sind.

Zudem können Mandantenadministratoren ebenfalls eine externe vRealize Orchestrator-Instanz konfigurieren, jedoch nur für ihre eigenen Mandanten.

Informationen zum Konfigurieren einer externen vRealize Orchestrator-Instanz und vRealize Orchestrator-Workflow-Kategorien finden Sie unter *Konfigurieren von vCenter Orchestrator und Plug-Ins*.

## Liste der vRealize Orchestrator -Plug-Ins

Mit Plug-Ins können Sie vRealize Orchestrator verwenden, um auf externe Technologien und Anwendungen zuzugreifen und diese zu steuern. Indem Sie eine externe Technologie in einem vRealize Orchestrator-Plug-In verfügbar machen, können Sie Objekte und Funktionen in Workflows einbinden, die auf die Objekte und Funktionen der externen Technologie zugreifen.

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

Mit dem Standardsatz der vRealize Orchestrator-Plug-Ins können Sie externe Technologien wie die vCenter Server-API und E-Mail-Funktionen in Workflows einbinden. Darüber hinaus können Sie mit der offenen Plug-In-Architektur von vRealize Orchestrator Plug-Ins für den Zugriff auf andere Anwendungen entwickeln.

**Tabelle 4-42. Standardmäßig in vRealize Orchestrator enthaltene Plug-Ins**

Plug-In	Zweck
vCenter Server	Ermöglicht den Zugriff auf die vCenter Server-API, sodass Sie alle vCenter Server-Objekte und -Funktionen in die Verwaltungsprozesse einbinden können, die mittels vRealize Orchestrator automatisiert werden.
Konfiguration	Stellt Workflows für die Konfiguration der vRealize Orchestrator-Authentifizierung, der Datenbankverbindung, der SSL-Zertifikate usw. zur Verfügung.
vCO Library	Stellt Workflows zur Verfügung, die als grundlegende Bausteine für die Anpassung und Automatisierung von Clientprozessen dienen. Die Workflow-Bibliothek umfasst Vorlagen für die Lebenszyklusverwaltung, die Bereitstellung, die Notfallwiederherstellung, Hotbackup und andere Standardprozesse. Sie können die Vorlagen kopieren und bearbeiten, um sie an ihre Anforderungen anzupassen.
SQL	Stellt die JDBC-API (Java Database Connectivity) zur Verfügung, Hierbei handelt es sich um den Branchenstandard für die datenbankunabhängige Konnektivität zwischen der Java-Programmiersprache und einem breiten Spektrum von Datenbanken. Die Datenbanken umfassen SQL-Datenbanken sowie weitere tabellarische Datenquellen wie beispielsweise Tabellen oder Flatfiles. Die JDBC-API bietet eine Call-Level-API für den SQL-basierten Datenbankzugriff aus Workflows.
SSH	Stellt eine Implementierung des SSH-2-Protokolls (Secure Shell v2) zur Verfügung. Erlaubt Remotebefehl- und Dateiübertragungssitzungen mit auf Kennwörtern und öffentlichen Schlüsseln basierender Authentifizierung in Workflows. Unterstützt die interaktive Authentifizierung über die Tastatur. Optional kann das SSH-Plug-In das Browsen im Remotedateisystem direkt im vRealize Orchestrator-Clientbestand unterstützen.
XML	Ein vollständiger DOM-XML-Parser (Document Object Model), der in Workflows implementiert werden kann. Alternativ können Sie die Implementierung von ECMAScript for XML (E4X) in der JavaScript-API von vRealize Orchestrator verwenden.

**Tabelle 4-42. Standardmäßig in vRealize Orchestrator enthaltene Plug-Ins (Fortsetzung)**

Plug-In	Zweck
Mail	Verwendet SMTP (Simple Mail Transfer Protocol) zum Senden von E-Mails aus Workflows.
Net	Umschließt die Jakarta Apache Commons Net Library. Stellt Implementierungen von Telnet, FTP, POP3 und IMAP zur Verfügung. Der POP3- und IMAP-Teil dient zum Lesen von E-Mails. In Kombination mit dem Mail-Plug-In stellt das Net-Plug-In umfassende Funktionen zum Senden und Empfangen von E-Mails in Workflows zur Verfügung.
Enumeration	Stellt gängige Enumerationstypen zur Verfügung, die von anderen Plug-Ins in Workflows verwendet werden können.
Workflow-Dokumentation	Stellt Workflows zur Verfügung, mit denen Sie Informationen über einen Workflow oder eine Workflow-Kategorie im PDF-Format generieren können.
HTTP-REST	Ermöglicht Ihnen die Verwaltung der REST-Webdienste durch Bereitstellung einer Interaktion zwischen vCenter Orchestrator und REST-Hosts.
SOAP	Ermöglicht Ihnen die Verwaltung der SOAP-Webdienste durch Bereitstellung einer Interaktion zwischen vCenter Orchestrator und SOAP-Hosts.
AMQP	Ermöglicht Ihnen die Interaktion mit auch als Broker bezeichneten AMQP-Servern (Advanced Message Queuing Protocol).
SNMP	Ermöglicht vCenter Orchestrator die Herstellung einer Verbindung und den Abruf von Informationen von SNMP-fähigen Systemen und Geräten.
Active Directory	Ermöglicht die Interaktion zwischen vCenter Orchestrator und Microsoft Active Directory.
vCO WebOperator	Eine Webansicht, in der Sie auf die Workflows in der vRealize Orchestrator-Bibliothek zugreifen und mit diesen über ein Netzwerk mithilfe eines Webbrowsers interagieren können.
Dynamic Types	Hiermit können Sie dynamische Typen erstellen und Objekte dieser dynamischen Typen verwenden.
PowerShell	Ermöglicht Ihnen die Verwaltung von PowerShell-Hosts und die Ausführung von benutzerdefinierten PowerShell-Vorgängen.
Multi-Node	Enthält Workflows für die hierarchische Orchestrierung, die Verwaltung von Orchestrator-Instanzen und die horizontale Skalierung von Orchestrator-Aktivitäten.
vRealize Automation (nur in der in vRealize Automation eingebetteten Instanz)	Ermöglicht Ihnen die Erstellung und Ausführung von Workflows für die Interaktion zwischen vRealize Orchestrator und vRealize Automation.

Weitere Informationen über die von VMware entwickelten und verteilten vRealize Orchestrator-Plug-Ins finden Sie auf der Startseite für die Dokumentation zu VMware vRealize™ Orchestrator™.

## Erstellen von benutzerdefinierten Ressourcen

Eine benutzerdefinierte Ressource wird einem vRealize Orchestrator-Objektyp als XaaS-Ressource zugeordnet, sodass Sie Blueprints und Ressourcenaktionen erstellen können.

Beispielsweise können Sie eine benutzerdefinierte Ressource basierend auf „VC:virtual machine“ erstellen, sodass Sie Blueprints zur Bereitstellung von virtuellen vCenter Server-Maschinen erstellen und Ressourcenaktionen zur Ausführung für die Maschinen hinzufügen können.

### Hinzufügen einer benutzerdefinierten Ressource

Sie erstellen eine benutzerdefinierte Ressource zum Definieren des XaaS-Elements für die Bereitstellung.

Durch Erstellen einer benutzerdefinierten Ressource ordnen Sie einen Objekttyp, der durch die API eines vRealize Orchestrator-Plug-Ins verfügbar gemacht wird, als Ressource zu. Sie erstellen eine benutzerdefinierte Ressource, um die Ausgabeparameter eines XaaS-Blueprints für die Bereitstellung und einen Eingabeparameter einer Ressourcenaktion zu definieren.

Beim Erstellen einer benutzerdefinierten Ressource können Sie auf der Seite „Detailformular“ die Felder des schreibgeschützten Formulars für die Ressource angeben, in dem Informationen in der Detailansicht eines bereitgestellten Elements angezeigt werden. Siehe [Entwerfen eines benutzerdefinierten Ressourcenformulars](#).

### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.

### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Benutzerdefinierte Ressourcen** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Geben Sie den vRealize Orchestrator-Objekttyp im Textfeld **Orchestrator-Typ** ein und drücken Sie die Eingabetaste.  
 Geben Sie beispielsweise **v** ein, um alle Typen anzuzeigen, die den Buchstaben „v“ enthalten. Um alle Typen anzuzeigen, geben Sie ein Leerzeichen ein und klicken Sie auf **Suchen**.
- 4 Geben Sie einen Namen und optional eine Beschreibung ein.
- 5 Geben Sie eine Version ein.  
 Die Version unterstützt nur GanzzahlenInteger. Das unterstützte Format erstreckt sich auch auf major.minor.micro-revision.
- 6 Klicken Sie auf **Weiter**.

## 7 Bearbeiten Sie das Formular der benutzerdefinierten Ressource.

Sie können das benutzerdefinierte Ressourcenformular bearbeiten, indem Sie Elemente löschen, bearbeiten und neu anordnen. Darüber hinaus können Sie ein neues Formular und Formularseiten hinzufügen und die Elemente auf die Seite „Neues Formular“ und „Formular“ ziehen.

Option	Beschreibung
<b>Formular hinzufügen</b>	Klicken Sie neben dem Formularnamen auf das Symbol <b>Neues Formular</b> (+), geben Sie die erforderlichen Informationen ein und klicken Sie auf <b>Übernehmen</b> .
<b>Formularseite hinzufügen</b>	Klicken Sie neben dem Formularnamen auf das Symbol <b>Neue Seite</b> (+), geben Sie die erforderlichen Informationen ein und klicken Sie auf <b>Übernehmen</b> .
<b>Element zur Formularseite hinzufügen</b>	Ziehen Sie ein Element aus dem Bereich „Neue Felder“ auf der linken Seite in den Bereich auf der rechten Seite. Anschließend können Sie die erforderlichen Informationen eingeben und auf <b>Übernehmen</b> klicken. Die verfügbaren Elemente gelten speziell für den vRealize Orchestrator-Objekttyp.
<b>Element bearbeiten</b>	Klicken Sie neben dem zu bearbeitenden Element auf das Symbol <b>Bearbeiten</b> (✎), nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf <b>Übernehmen</b> .
<b>Element löschen</b>	Klicken Sie neben dem zu löschenden Element auf das Symbol <b>Löschen</b> (✖) und klicken Sie im Bestätigungsdiaologfeld auf <b>OK</b> .
<b>Formular löschen</b>	Klicken Sie neben dem Formularnamen auf das Symbol <b>Löschen</b> (✖) und klicken Sie im Bestätigungsdiaologfeld auf <b>OK</b> .

## 8 Klicken Sie auf **Beenden**.

Sie haben eine benutzerdefinierte Ressource erstellt, die auf der Seite „Benutzerdefinierte Ressourcen“ aufgeführt wird.

### Weiter

Erstellen Sie einen XaaS-Blueprint. Siehe [Erstellen Sie einen XaaS-Blueprint](#).

## Erstellen von XaaS -Blueprints und -Ressourcenaktionen

Die XaaS-Blueprints können berechtigten Benutzern als Katalogelemente zur Verfügung gestellt werden oder sie können mithilfe der Design-Arbeitsfläche in zusammengesetzten Blueprints zusammengestellt werden. Die Ressourcenaktionen werden für die bereitgestellten Elemente ausgeführt, um die Elemente nach der Bereitstellung zu verwalten.

Beispielsweise können Sie einen XaaS-Blueprint verwenden, um Active Directory-Benutzer in einer Gruppe zu erstellen. Anschließend können Sie mithilfe einer Ressourcenaktion die Anforderung ändern, dass der Benutzer das Kennwort ändern muss.

### Erstellen eines XaaS -Blueprints als Katalogelement

Ein XaaS-Blueprint ist ein Bereitstellungs-Blueprint. Zu den verfügbaren Bereitstellungsworkflows gehören unter anderem das Erstellen von virtuellen Maschinen, das Hinzufügen von Benutzern zu Active Directory oder das Erstellen von Snapshots einer virtuellen Maschine.

## Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.
- Erstellen Sie eine benutzerdefinierte Ressource für den Zielressourcentyp. Siehe [Hinzufügen einer benutzerdefinierten Ressource](#).

## Vorgehensweise

### 1 Erstellen Sie einen XaaS-Blueprint

Bei einem XaaS-Blueprint handelt es sich um eine vollständige Spezifikation für die Bereitstellung. Der Blueprint kann die Eingabeparameter, die Sendeformulare und schreibgeschützten Formulare, die Aktionsabfolge und die Bereitstellung enthalten.

### 2 Veröffentlichen eines XaaS-Blueprints als Katalogelement

Nachdem Sie einen XaaS-Blueprint erstellt haben, befindet sich dieser im Entwurfsstatus und kann als Katalogelement veröffentlicht werden.

### 3 Hinzufügen eines XaaS-Blueprints zu einem Anwendungs-Blueprint

Sie fügen einen XaaS-Blueprint zu einem Anwendungs-Blueprint in ähnlicher Weise hinzu, wie Sie andere Blueprints auf der Design-Arbeitsfläche hinzufügen.

## Erstellen Sie einen XaaS -Blueprint

Bei einem XaaS-Blueprint handelt es sich um eine vollständige Spezifikation für die Bereitstellung. Der Blueprint kann die Eingabeparameter, die Sendeformulare und schreibgeschützten Formulare, die Aktionsabfolge und die Bereitstellung enthalten.

Sie können Dienst-Blueprints erstellen, um zuvor erstellte benutzerdefinierte Ressourcen bereitzustellen. Wenn diese Katalogelemente durch Verbraucher angefordert werden, werden die bereitgestellten Elemente auf der Registerkarte **Elemente** gespeichert und Sie können für bereitgestellte Ressourcen dieses Typs die Vorgänge nach erfolgter Bereitstellung definieren.

Wenn Sie beim Erstellen eines Dienst-Blueprints für die Bereitstellung keinen Ausgabeparameter festlegen, erfolgt, wenn der Verbraucher dieses Katalogelement anfordert, zwar eine Bereitstellung durch den Blueprint, doch werden die bereitgestellten Elemente nicht auf der Registerkarte **Elemente** hinzugefügt. Sie können bei bereitgestellten Ressourcen dieses Typs keine Vorgänge nach der Bereitstellung durchführen.

Sie können auch über keine Ausgabeparameter verfügende und keine Bereitstellung auslösende Dienst-Blueprints für Anforderungen erstellen. Beispielsweise können Sie einen Dienst-Blueprint für das Senden von Benachrichtigungen erstellen.

Durch das Erstellen eines Dienst-Blueprints veröffentlichen Sie einen vRealize Orchestrator-Workflow als Katalogelement. Während dieses Vorgangs können Sie die generierten Standardformulare bearbeiten. Siehe [Entwerfen eines XaaS-Blueprint-Formulars](#).

## Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.

- Erstellen Sie für die Bereitstellung von Elementen eine benutzerdefinierte Ressource, die dem Ausgabeparameter des Dienst-Blueprints entspricht. Siehe [Hinzufügen einer benutzerdefinierten Ressource](#).

## Vorgehensweise

- 1 Wählen Sie **Design > XaaS > XaaS-Blueprints** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Navigieren Sie in der vRealize Orchestrator-Workflow-Bibliothek und wählen Sie einen Workflow aus.  
Der Name und die Beschreibung des ausgewählten Workflows sowie die in vRealize Orchestrator definierten Ein- und Ausgabeparameter werden angezeigt.

- 4 Klicken Sie auf **Weiter**.

- 5 Geben Sie einen Namen und optional eine Beschreibung ein.

Die Textfelder **Name** und **Beschreibung** werden mit dem Namen und der Beschreibung des Workflows gemäß der Definition in vRealize Orchestrator aufgefüllt.

- 6 (Optional) Wenn Sie die Verbraucher nicht zur Eingabe einer Beschreibung und einer Begründung für die Anforderung dieser Ressourcenaktion auffordern möchten, aktivieren Sie das Kontrollkästchen **Informationsseite zur Kataloganforderung ausblenden**.

- 7 Geben Sie eine Version ein.





Die Version unterstützt nur GanzzahlenInteger. Das unterstützte Format erstreckt sich auch auf major.minor.micro-revision.

- 8 Klicken Sie auf **Weiter**.

- 9 (Optional) Bearbeiten Sie das Formular des Dienst-Blueprints auf der Seite „Blueprint-Formular“.

Das Dienst-Blueprint-Formular wird standardmäßig der vRealize Orchestrator-Workflow-Präsentation zugeordnet. Sie können das Blueprint-Formular bearbeiten, indem Sie Elemente im Formular löschen, bearbeiten und neu anordnen. Darüber hinaus können Sie ein neues Formular und Formularseiten hinzufügen und die Elemente auf die Seite „Neues Formular“ und „Formular“ ziehen.

Option	Aktion
<b>Formular hinzufügen</b>	Klicken Sie neben dem Formularnamen auf das Symbol <b>Neues Formular</b> (+), geben Sie die erforderlichen Informationen ein und klicken Sie auf <b>Übernehmen</b> .
<b>Formular bearbeiten</b>	Klicken Sie neben dem Formularnamen auf das Symbol <b>Bearbeiten</b> (✎), nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf <b>Übernehmen</b> .
<b>Workflow-Präsentation neu generieren</b>	Klicken Sie neben dem Formularnamen auf das Symbol <b>Neu erstellen</b> (↺) und klicken Sie auf <b>OK</b> .
<b>Formular löschen</b>	Klicken Sie neben dem Formularnamen auf das Symbol <b>Löschen</b> (✖) und klicken Sie im Bestätigungsdiaologfeld auf <b>OK</b> .
<b>Formularseite hinzufügen</b>	Klicken Sie neben dem Formularnamen auf das Symbol <b>Neue Seite</b> (+), geben Sie die erforderlichen Informationen ein und klicken Sie auf <b>Übernehmen</b> .

Option	Aktion
<b>Formularseite bearbeiten</b>	Klicken Sie neben dem Namen der Formularseite auf das Symbol <b>Bearbeiten</b> (  ) , nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf <b>Übernehmen</b> .
<b>Formularseite löschen</b>	Klicken Sie neben dem Formularnamen auf das Symbol <b>Löschen</b> (  ) und klicken Sie im Bestätigungsdialogfeld auf <b>OK</b> .
<b>Element zur Formularseite hinzufügen</b>	Ziehen Sie ein Element aus dem Bereich „Neue Felder“ auf der linken Seite in den Bereich auf der rechten Seite. Anschließend können Sie die erforderlichen Informationen eingeben und auf <b>Übernehmen</b> klicken.
<b>Element bearbeiten</b>	Klicken Sie neben dem zu bearbeitenden Element auf das Symbol <b>Bearbeiten</b> (  ) , nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf <b>Übernehmen</b> .
<b>Element löschen</b>	Klicken Sie neben dem zu löschenden Element auf das Symbol <b>Löschen</b> (  ) und klicken Sie im Bestätigungsdialogfeld auf <b>OK</b> .

10 Klicken Sie auf **Weiter**.

11 Wählen Sie aus dem Dropdown-Menü einen Ausgabeparameter aus.

Option	Beschreibung
<b>Eine zuvor erstellte benutzerdefinierte Ressource</b>	Wenn dieses Katalogelement durch Verbraucher angefordert wird, werden die bereitgestellten Elemente auf der Registerkarte <b>Elemente</b> gespeichert.
<b>Keine Bereitstellung</b>	Der Dienst-Blueprint fügt der Registerkarte <b>Elemente</b> keine neuen Elemente hinzu.

12 Klicken Sie auf **Beenden**.

Sie haben einen Dienst-Blueprint erstellt und dieser wird auf der Seite mit den XaaS-Blueprints angezeigt.

## Weiter

Veröffentlichen Sie den Blueprint als Katalogelement. Siehe [Veröffentlichen eines XaaS-Blueprints als Katalogelement](#).

## Veröffentlichen eines XaaS -Blueprints als Katalogelement

Nachdem Sie einen XaaS-Blueprint erstellt haben, befindet sich dieser im Entwurfsstatus und kann als Katalogelement veröffentlicht werden.

## Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.

## Vorgehensweise

- 1 Wählen Sie **Design > XaaS > XaaS-Blueprints** aus.
- 2 Wählen Sie die Zeile des zu veröffentlichenden XaaS-Blueprints aus und klicken Sie auf die Schaltfläche **Veröffentlichen**.



Der Status des XaaS-Blueprints ändert sich zu „Veröffentlicht“. Durch Auswahl von **Administration > Katalogmanagement > Katalogelemente** können Sie sehen, dass der Blueprint als Katalogelement veröffentlicht wurde.

#### Weiter

- Um den XaaS-Blueprint im Servicekatalog verfügbar zu machen, müssen Sie das Element einem Dienst hinzufügen. Siehe [Erstellen eines Diensts](#).
- Wenn Sie den XaaS-Blueprint im Blueprint einer Anwendung verwenden, fügen Sie ihn in der Design-Arbeitsfläche hinzu. Siehe [Hinzufügen eines XaaS-Blueprints zu einem Anwendungs-Blueprint](#).
- Sie können eine Ressourcenaktion erstellen, die auf bereitgestellten Elementen ausgeführt wird. Siehe [Erstellen einer Ressourcenaktion](#).

#### Hinzufügen eines XaaS -Blueprints zu einem Anwendungs-Blueprint

Sie fügen einen XaaS-Blueprint zu einem Anwendungs-Blueprint in ähnlicher Weise hinzu, wie Sie andere Blueprints auf der Design-Arbeitsfläche hinzufügen.

Verwenden Sie diese Methode, um einen XaaS-Blueprint zu einem Anwendungs-Blueprint hinzuzufügen, der andere Blueprints enthält. Wenn Sie Ihren Benutzern nur den XaaS-Blueprint bereitstellen möchten, können Sie ihn zu einem Dienst hinzufügen und den Benutzern die Berechtigung dafür erteilen, ohne ihn zu einem Anwendungs-Blueprint hinzuzufügen.

Wenn Sie eine vertikale oder horizontale Skalierungsaktion auf einem bereitgestellten Anwendungs-Blueprint ausführen, wird der XaaS-Blueprint nicht skaliert.

#### Voraussetzungen

- Erstellen und veröffentlichen Sie einen XaaS-Blueprint. Siehe [Erstellen eines XaaS-Blueprints als Katalogelement](#).
- Lesen Sie nach, wie Sie die XaaS-Blueprint-Formulare anpassen. Siehe [Entwerfen von Formularen für XaaS-Blueprints und Aktionen](#).
- Melden Sie sich an der vRealize Automation-Konsole als **Infrastrukturarchitekt** an.

#### Vorgehensweise

- 1 Wählen Sie **Design > Blueprints** aus.
- 2 Wählen Sie den Namen des Blueprints aus, zu dem Sie den XaaS-Blueprint hinzufügen möchten.  
Die Design-Arbeitsfläche wird angezeigt. Sie enthält die aktuellen Anwendungskomponenten-Blueprints und andere Komponenten.
- 3 Klicken Sie in der Liste „Kategorien“ auf **XaaS**.
- 4 Ziehen Sie Ihren Blueprint auf die Arbeitsfläche.
- 5 Konfigurieren Sie die Standardwerte für die allgemeinen Parameter und Infrastrukturoptionen.  
Diese Standardwerte werden im Servicekatalogformular angezeigt, wenn ein Benutzer das Element anfordert.

## 6 Klicken Sie auf **Fertig stellen**.

Der XaaS-Blueprint ist nun Teil des Anwendungs-Blueprints.

### Weiter

Vergewissern Sie sich, dass der Anwendungs-Blueprint zu einem Dienst hinzugefügt wird und den Benutzern die Berechtigung dafür erteilt wird. Siehe [Verwalten des Servicekatalogs](#).

## Erstellen einer XaaS -Ressourcenaktion als Katalogelement

Sie erstellen eine Ressourcenaktion, um bereitgestellte Elemente mithilfe von vRealize Orchestrator-Workflows verwalten zu können.

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.
- Überprüfen Sie, ob eine benutzerdefinierte Ressource vorhanden ist, die die Aktion unterstützt. Siehe [Hinzufügen einer benutzerdefinierten Ressource](#).
- Wenn Sie Aktionen zur Ausführung an Elementen erstellen, die nicht als XaaS-Katalogelemente bereitgestellt sind, müssen Sie überprüfen, ob die Zielressourcen zugeordnet wurden. Siehe [Zuordnen anderer Ressourcen zur Verwendung mit XaaS-Ressourcenaktionen](#).

### Vorgehensweise

#### 1 Erstellen einer Ressourcenaktion

Eine Ressourcenaktion ist ein XaaS-Workflow, den Servicekatalogbenutzer auf bereitgestellten Katalogelementen ausführen können. Als XaaS-Architekt können Sie Ressourcenaktionen erstellen, um die Vorgänge zu definieren, die Verbraucher für die bereitgestellten Elemente ausführen können.

#### 2 Veröffentlichen einer Ressourcenaktion

Die neu erstellte Ressourcenaktion befindet sich im Entwurfzustand, und Sie müssen die Ressourcenaktion veröffentlichen.

#### 3 Zuweisen eines Symbols zu einer Ressourcenaktion

Nachdem Sie eine Ressourcenaktion erstellt und veröffentlicht haben, können Sie sie bearbeiten und der Aktion ein Symbol zuweisen.

## Erstellen einer Ressourcenaktion

Eine Ressourcenaktion ist ein XaaS-Workflow, den Servicekatalogbenutzer auf bereitgestellten Katalogelementen ausführen können. Als XaaS-Architekt können Sie Ressourcenaktionen erstellen, um die Vorgänge zu definieren, die Verbraucher für die bereitgestellten Elemente ausführen können.

Durch das Erstellen einer Ressourcenaktion ordnen Sie einen vRealize Orchestrator-Workflow als Vorgang nach erfolgter Bereitstellung zu. Während dieses Vorgangs können Sie die standardmäßigen übermittelten und schreibgeschützten Formulare bearbeiten. Siehe [Entwerfen eines Ressourcenaktionsformulars](#).

## Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.
- Erstellen Sie eine benutzerdefinierte Ressource, die dem Eingabeparameter der Ressourcenaktion entspricht.

## Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Navigieren Sie in der vRealize Orchestrator-Workflow-Bibliothek und wählen Sie einen Workflow aus.  
Der Name und die Beschreibung des ausgewählten Workflows sowie die in vRealize Orchestrator definierten Ein- und Ausgabeparameter werden angezeigt.
- 4 Klicken Sie auf **Weiter**.
- 5 Wählen Sie aus dem Dropdown-Menü **Ressourcentyp** die zuvor erstellte benutzerdefinierte Ressource aus.
- 6 Wählen Sie aus dem Dropdown-Menü **Eingabeparameter** den Eingabeparameter für die Ressourcenaktion aus.
- 7 Klicken Sie auf **Weiter**.
- 8 Geben Sie einen Namen und optional eine Beschreibung ein.  
Die Textfelder **Name** und **Beschreibung** werden mit dem Namen und der Beschreibung des Workflows gemäß der Definition in vRealize Orchestrator aufgefüllt.
- 9 (Optional) Wenn Sie die Verbraucher nicht zur Eingabe einer Beschreibung und einer Begründung für die Anforderung dieser Ressourcenaktion auffordern möchten, aktivieren Sie das Kontrollkästchen **Informationsseite zur Kataloganforderung ausblenden**.
- 10 Geben Sie eine Version ein.  
Die Version unterstützt nur GanzzahlenInteger. Das unterstützte Format erstreckt sich auch auf major.minor.micro-revision.

## 11 (Optional) Wählen Sie den Aktionstyp aus.

Option	Beschreibung
<b>Löschung</b>	Der Eingabeparameter des Ressourcenaktionsworkflows wird gelöscht und das Element wird auf der Registerkarte <b>Elemente</b> entfernt. Beispielsweise dient die Ressourcenaktion zum Löschen einer bereitgestellten Maschine.
<b>Bereitstellung</b>	Bei der Ressourcenaktion geht es um die Bereitstellung. Beispielsweise dient die Ressourcenaktion zum Kopieren eines Katalogelements.  Wählen Sie aus dem Dropdown-Menü einen Ausgabeparameter aus. Sie können eine zuvor erstellte benutzerdefinierte Ressource auswählen. Wenn die Verbraucher dann diese Ressourcenaktion anfordern, werden die bereitgestellten Elemente auf der Registerkarte <b>Elemente</b> hinzugefügt. Wenn nur die Option <b>Keine Bereitstellung</b> verfügbar ist, dient entweder die Ressourcenaktion nicht für die Bereitstellung oder Sie haben keine geeignete benutzerdefinierte Ressource für den Ausgabeparameter erstellt und können deshalb den Vorgang nicht fortsetzen.



In Abhängigkeit vom Aktionsworkflow können Sie eine Option, beide Optionen oder keine Option auswählen.

## 12 Wählen Sie die Bedingungen aus, unter denen die Ressourcenaktion für Benutzer verfügbar ist, und klicken Sie auf **Weiter**.

## 13 (Optional) Bearbeiten Sie auf der Registerkarte **Formular** das Formular der Ressourcenaktion.

Das Formular der Ressourcenaktion ordnet die vRealize Orchestrator-Workflow-Präsentation zu. Sie können das Formular ändern, indem Sie Elemente löschen, bearbeiten und neu anordnen. Darüber hinaus können Sie ein neues Formular und Formularseiten hinzufügen und die erforderlichen Elemente auf die Seite „Neues Formular“ und „Formular“ ziehen.

Option	Aktion
<b>Formular hinzufügen</b>	Klicken Sie neben dem Formularnamen auf das Symbol <b>Neues Formular</b> (+), geben Sie die erforderlichen Informationen ein und klicken Sie auf <b>Übernehmen</b> .
<b>Formular bearbeiten</b>	Klicken Sie neben dem Formularnamen auf das Symbol <b>Bearbeiten</b> (✎), nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf <b>Übernehmen</b> .
<b>Workflow-Präsentation neu generieren</b>	Klicken Sie neben dem Formularnamen auf das Symbol <b>Neu erstellen</b> (↺) und klicken Sie auf <b>OK</b> .
<b>Formular löschen</b>	Klicken Sie neben dem Formularnamen auf das Symbol <b>Löschen</b> (✖) und klicken Sie im Bestätigungsdialogfeld auf <b>OK</b> .
<b>Formularseite hinzufügen</b>	Klicken Sie neben dem Formularnamen auf das Symbol <b>Neue Seite</b> (+), geben Sie die erforderlichen Informationen ein und klicken Sie auf <b>Übernehmen</b> .
<b>Formularseite bearbeiten</b>	Klicken Sie neben dem Namen der Formularseite auf das Symbol <b>Bearbeiten</b> (✎), nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf <b>Übernehmen</b> .
<b>Formularseite löschen</b>	Klicken Sie neben dem Formularnamen auf das Symbol <b>Löschen</b> (✖) und klicken Sie im Bestätigungsdialogfeld auf <b>OK</b> .
<b>Element zur Formularseite hinzufügen</b>	Ziehen Sie ein Element aus dem Bereich „Neue Felder“ auf der linken Seite in den Bereich auf der rechten Seite. Anschließend können Sie die erforderlichen Informationen eingeben und auf <b>Übernehmen</b> klicken.

Option	Aktion
<b>Element bearbeiten</b>	Klicken Sie neben dem zu bearbeitenden Element auf das Symbol <b>Bearbeiten</b> (  ) , nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf <b>Übernehmen</b> .
<b>Element löschen</b>	Klicken Sie neben dem zu löschenden Element auf das Symbol <b>Löschen</b> (  ) und klicken Sie im Bestätigungsdialogfeld auf <b>OK</b> .

#### 14 Klicken Sie auf **Beenden**.

Sie haben eine Ressourcenaktion erstellt, und die Ressourcenaktion wird auf der Seite „Ressourcenaktionen“ aufgeführt.

#### Weiter

Veröffentlichen Sie die Ressourcenaktion. Siehe [Veröffentlichen einer Ressourcenaktion](#).

#### Veröffentlichen einer Ressourcenaktion

Die neu erstellte Ressourcenaktion befindet sich im Entwurfzustand, und Sie müssen die Ressourcenaktion veröffentlichen.

#### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.

#### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Wählen Sie die Zeile der zu veröffentlichenden Ressourcenaktion aus und klicken Sie auf die Schaltfläche **Veröffentlichen**.

Der Status der Ressourcenaktion ändert sich zu „Veröffentlicht“.

#### Weiter

Weisen Sie der Ressourcenaktion ein Symbol zu. Siehe [Zuweisen eines Symbols zu einer Ressourcenaktion](#). Mandantenadministratoren und Business-Gruppenmanager können dann die Aktion beim Erstellen einer Berechtigung verwenden.

#### Zuweisen eines Symbols zu einer Ressourcenaktion

Nachdem Sie eine Ressourcenaktion erstellt und veröffentlicht haben, können Sie sie bearbeiten und der Aktion ein Symbol zuweisen.

#### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.

#### Vorgehensweise

- 1 Wählen Sie **Administration > Katalogmanagement > Aktionen** aus.
- 2 Wählen Sie die Ressourcenaktion aus, die Sie erstellt haben.

- 3 Klicken Sie auf **Konfigurieren**.
- 4 Klicken Sie auf **Durchsuchen** und wählen Sie das gewünschte Symbol aus.
- 5 Klicken Sie auf **Öffnen**.
- 6 Klicken Sie auf **Aktualisieren**.

Sie haben der Ressourcenaktion ein Symbol zugewiesen. Business-Gruppenmanager und Mandantenadministratoren können die Ressourcenaktion in einer Berechtigung verwenden.

## Zuordnen anderer Ressourcen zur Verwendung mit XaaS - Ressourcenaktionen

Sie ordnen Elemente zu, die nicht mithilfe von XaaS bereitgestellt wurden, sodass Sie Ressourcenaktionen für diese Elemente ausführen können.

### Skriptaktionen und Workflows für Ressourcenzuordnungen

Sie können die angegebenen Ressourcenzuordnungen für virtuelle vSphere-, vCloud Director- oder vCloud Air-Maschinen verwenden oder Sie können benutzerdefinierte Skriptaktionen oder Workflows für vRealize Orchestrator erstellen, um zusätzliche Katalogressourcentypen von vRealize Automation zu Bestandslistentypen von vRealize Orchestrator zuzuordnen.

### Ressourcenzuordnungen bereitgestellt mit vRealize Automation

vRealize Automation enthält Ressourcenzuordnungen für virtuelle IaaS vSphere-Maschinen, IaaS vCloud Director und Bereitstellungen.

vRealize Automation enthält Skriptaktionen für Ressourcenzuordnungen von vRealize Orchestrator für jede der bereitgestellten XaaS-Ressourcenzuordnungen. Skriptaktionen für die angegebenen Ressourcenzuordnungen sind im Paket `com.vmware.vcac.asd.mappings` des eingebetteten vRealize Orchestrator-Servers zu finden.

Wenn Sie eine Ressourcenaktion erstellen, die auf einem bereitgestellten zusammengesetzten Blueprint ausgeführt wird, der einem vRealize Orchestrator-Workflow mit `vCACAFE:CatalogResource` als einen Eingabeparameter verwendet, wird die Bereitstellungszuordnung als der Eingaberessourcentyp angewendet. Die Bereitstellungszuordnung wird nur angewendet, wenn der ausgewählte Workflow `vCACAFE:CatalogResource` als einen Eingabeparameter enthält. Wenn Sie beispielsweise eine Aktion erstellen, um eine Ressourcenaktion im Namen eines Benutzers anzufordern, ist „Bereitstellung“ der Ressourcentyp auf der Registerkarte „Eingaberessource“, da dieser Workflow `vCACAFE:CatalogResource` verwendet.

Die IaaS vCD VM- und IaaS VC VirtualMachine-Ressourcenzuordnungen werden von einer Aktion verwendet, um die virtuellen Maschinen, die mit der IaaS-Ressource übereinstimmen, der virtuellen vRealize Orchestrator vSphere- oder vCloud Director-Maschine zuzuordnen.

## Entwicklung von Ressourcenzuordnungen

Je nach Ihrer Version von vRealize Orchestrator können Sie entweder einen Workflow oder eine Skriptaktion für vRealize Orchestrator erstellen, um Ressourcen zwischen vRealize Orchestrator und vRealize Automation zuzuordnen.

Sie entwickeln eine Ressourcenzuordnung, indem Sie einen Eingabeparameter vom Typ **Properties**, verwenden, der ein Schlüssel-Wert-Paar, das die bereitgestellte Ressource definiert, und einen Ausgabeparameter eines vRealize Orchestrator-Bestandstyps, der vom entsprechenden Plug-In für vRealize Orchestrator erwartet wird, enthält. Die für die Zuordnung verfügbaren Eigenschaften richten sich nach dem Typ der Ressource. Beispielsweise ist die Eigenschaft **EXTERNAL\_REFERENCE\_ID** ein üblicher Schlüsselparameter, mit dem einzelne Maschinen definiert werden. Sie können diese Eigenschaft verwenden, um eine Katalogressource abzufragen. Wenn Sie eine Zuordnung für eine Ressource erstellen, die keine **EXTERNAL\_REFERENCE\_ID** verwendet, können Sie eine der anderen Eigenschaften verwenden, die für die einzelnen Maschinen übergeben werden. Zum Beispiel **Name**, **Beschreibung** usw.

Weitere Informationen zur Entwicklung von Workflows und Skriptaktionen finden Sie unter *Entwickeln mit VMware vCenter Orchestrator*.

## Erstellen einer Ressourcenzuordnung

vRealize Automation stellt Ressourcenzuordnungen für vSphere-, vCloud Director- und vCloud Air-Maschinen bereit. Sie können weitere Ressourcenzuordnungen für andere Katalogressourcentypen erstellen.

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.
- Stellen Sie sicher, dass das Zuordnungs-Skript oder Zuordnungs-Workflow in vRealize Orchestrator ist. Siehe [Skriptaktionen und Workflows für Ressourcenzuordnungen](#).

### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenzuordnungen** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 Geben Sie eine Version ein.

Die Version unterstützt nur GanzzahlenInteger. Das unterstützte Format erstreckt sich auch auf major.minor.micro-revision.

- 5 Geben Sie im Textfeld **Katalogressourcentyp** den Typ der Katalogressource ein und drücken Sie die Eingabetaste.

Der Katalogressourcentyp wird in der Detailansicht des bereitgestellten Elements angezeigt.

- 6 Geben Sie den vRealize Orchestrator-Objekttyp im Textfeld **Orchestrator-Typ** ein und drücken Sie die Eingabetaste.

Dies ist der Ausgabeparameter des Ressourcenzuordnungsworkflows.

- 7 (Optional) Fügen Sie Zielkriterien hinzu, um die Verfügbarkeit der durch diese Ressourcenzuordnung erstellten Ressourcenaktionen einzuschränken.

Ressourcenaktion unterliegen außerdem auf Genehmigungen und Berechtigungen basierenden Einschränkungen.

- a Wählen Sie **Verfügbar nach Bedingungen** aus.
- b Wählen Sie den Bedingungstyp aus.

Option	Beschreibung
<b>Alle folgenden Optionen</b>	Wenn alle der definierten Klauseln erfüllt werden, stehen dem Benutzer die durch diese Ressourcenzuordnung erstellten Ressourcenaktionen zur Verfügung.
<b>Eine der folgenden Optionen</b>	Wenn eine der definierten Klauseln erfüllt wird, stehen dem Benutzer die durch diese Ressourcenzuordnung erstellten Ressourcenaktionen zur Verfügung.
<b>Nicht die folgende</b>	Wenn die von Ihnen definierte Klausel vorhanden ist, stehen die durch diese Ressourcenzuordnung erstellten Ressourcenaktionen nicht zur Verfügung.

- c Folgen Sie den Anweisungen, um Ihre Klausel zu erstellen und die Bedingung abzuschließen.
- 8 Wählen Sie in der vRealize Orchestrator-Bibliothek Ihre Skriptaktion bzw. Ihren Workflow für die Ressourcenzuordnung aus.
- 9 Klicken Sie auf **OK**.

## Entwerfen von Formularen für XaaS -Blueprints und Aktionen

XaaS umfasst einen Formulardesigner, den Sie zum Entwerfen von Sende- und Detailformularen für Blueprints und Ressourcenaktionen verwenden können. Basierend auf der Präsentation der Workflows generiert der Designer für Formulare dynamisch Standardformulare sowie Felder, mit denen Sie die Standardformulare ändern können.

Sie können interaktive Formulare erstellen, die die Benutzer zum Senden von Katalogelementen und Ressourcenaktionen ausfüllen können. Darüber hinaus können Sie schreibgeschützte Formulare erstellen, die definieren, welche Informationen dem Benutzer in der Detailansicht für ein Katalogelement oder eine bereitgestellte Ressource angezeigt werden.

Beim Erstellen von benutzerdefinierten XaaS-Ressourcen, XaaS-Blueprints und Ressourcenaktionen werden Formulare für häufige Anwendungsfälle erstellt.



**Tabelle 4-43. XaaS -Objekttypen und zugehörige Formulare**

Objekttyp	Standardformular	Zusätzliche Formulare
Benutzerdefinierte Ressource	Ressourcendetailformular auf Basis der Attribute des Bestandslistentyps des vRealize Orchestrator-Plug-Ins (schreibgeschützt).	■ Keine
XaaS-Blueprint	Anforderungssendeformular auf Basis der Präsentation des ausgewählten Workflows.	■ Katalogelementdetails (schreibgeschützt) ■ Details der gesendeten Anforderung (schreibgeschützt)
Ressourcenaktion	Aktionssendeformular auf Basis der Präsentation des ausgewählten Workflows.	■ Details der gesendeten Aktion (schreibgeschützt)

Sie können Standardformulare ändern und neue Formulare entwerfen. Sie können Felder durch Ziehen hinzufügen oder im Formular neu anordnen. Sie können Einschränkungen für die Werte von bestimmten Feldern festlegen, Standardwerte angeben oder Anweisungen für die Endbenutzer bereitstellen, die das Formular ausfüllen.

Aufgrund der unterschiedlichen Zwecke sind die Vorgänge, die Sie beim Entwerfen von schreibgeschützten Formularen ausführen können, verglichen mit den Vorgängen beim Entwerfen von Sendeformularen eingeschränkt.

### Felder im Formulardesigner

Die Workflow-Präsentation und Funktionalität können Sie durch Hinzufügen neuer vordefinierter Felder zu den generierten Standardformularen mit Ressourcenaktionen und XaaS-Blueprints erweitern.

Wenn ein Eingabeparameter im vRealize Orchestrator-Workflow definiert ist, wird er in vRealize Automation im generierten Standardformular angezeigt. Wenn Sie die generierten Standardfelder nicht im Formular verwenden möchten, können Sie sie löschen und per Drag & Drop neue Felder aus der Palette einfügen. Generierte Standardfelder können Sie ersetzen, ohne die Workflow-Zuordnungen zu deaktivieren, wenn Sie dieselbe ID wie für das Feld, das Sie ersetzen, verwenden.

Sie können außer den Feldern, die basierend auf Workflow-Eingaben von vRealize Orchestrator generiert wurden, auch neue Felder hinzufügen, um die Workflow-Präsentation und die Funktionalität in den folgenden Fällen zu erweitern:

#### ■ Hinzufügen von Optionen zu den vorhandenen Feldern

Beispielsweise können Sie ein neues Dropdown-Menü erstellen und **dd** benennen. Sie können auch vordefinierte Optionen für „Gold“, „Silver“, „Bronze“ und „Benutzerdefiniert“ erstellen. Wenn ein vordefiniertes Feld wie beispielsweise „CPU“ vorhanden ist, können Sie diesem Feld die folgenden Optionen hinzufügen:

- Wenn dd „Gold“ entspricht, dann hat die CPU 2000 MHz
- Wenn dd „Silver“ entspricht, dann hat die CPU 1000 MHz
- Wenn dd „Bronze“ entspricht, dann hat die CPU 500 MHz
- Wenn dd „Benutzerdefiniert“ entspricht, dann ist das Feld „CPU“ bearbeitbar und der Verbraucher kann einen benutzerdefinierten Wert angeben

- Hinzufügen externer Wertdefinitionen zu Feldern

Sie können einem Feld eine externe Wertdefinition hinzufügen, damit Sie vRealize Orchestrator-Skriptaktionen ausführen und in den von Ihnen entworfenen Formularen zusätzliche Informationen angeben können. Beispielsweise können Sie einen Workflow erstellen, um die Firewall-Einstellungen einer virtuellen Maschine zu ändern. Auf der Seite für Ressourcenaktionsanforderungen möchten Sie dem Benutzer das Ändern der Einstellungen für geöffnete Ports ermöglichen, aber gleichzeitig die Optionen auf geöffnete Ports beschränken. Sie können einem dualen Listenfeld eine externe Wertdefinition hinzufügen und eine benutzerdefinierte vRealize Orchestrator-Skriptaktion auswählen, mit der geöffnete Ports abgefragt werden. Wenn das Anforderungsformular geladen wird, werden die Skriptaktionen ausgeführt und die geöffneten Ports werden dem Benutzer als Optionen angezeigt.

- Hinzufügen neuer Felder, die im vRealize Orchestrator-Workflow als globale Parameter behandelt werden

Beispielsweise ermöglicht der Workflow die Integration in ein Drittanbietersystem und der Workflow-Entwickler hat Eingabeparameter für allgemeine Anwendungsfälle definiert, aber auch eine Methode für die Übergabe benutzerdefinierter Felder bereitgestellt. Beispielsweise werden in einem Skripterstellungsfeld alle globalen Parameter, die mit **my3rdparty** beginnen, verarbeitet. Wenn dann der XaaS-Architekt bestimmte Werte zur Eingabe durch die Verbraucher übergeben möchte, kann der XaaS-Architekt das neue Feld **my3rdparty\_CPU** hinzufügen.

**Tabelle 4-44. Neue Felder im Ressourcenaktions- oder XaaS -Blueprint-Formular**

Feld	Beschreibung
Textfeld	Einzeiliges Textfeld
Textbereich	Mehrzeiliges Textfeld
Link	Feld zur Eingabe einer URL durch Verbraucher
E-Mail	Feld zur Eingabe einer E-Mail-Adresse durch Verbraucher
Kennwortfeld	Feld zur Eingabe eines Kennworts durch Verbraucher
Ganzzahlfeld	Textfeld zur Eingabe einer ganzen Zahl durch Verbraucher Sie können dieses Feld als Schieberegler mit einem Minimal- und Maximalwert sowie einem Inkrement definieren.
Dezimalfeld	Textfeld zur Eingabe einer Dezimalzahl durch Verbraucher Sie können dieses Feld als Schieberegler mit einem Minimal- und Maximalwert sowie einem Inkrement definieren.
Datum und Uhrzeit	Textfelder zur Angabe eines Datums (durch Auswahl eines Datums in einem Kalendermenü) sowie zur Auswahl der Uhrzeit (mithilfe der Aufwärts- und Abwärtspfeile) durch Verbraucher
Duale Liste	Eine Listenerstellungsfunktion, bei der Verbraucher einen vordefinierten Wertesatz zwischen zwei Listen verschieben, wobei die erste Liste alle nicht ausgewählten Optionen und die zweite Liste die vom Benutzer ausgewählten Optionen enthält.
Kontrollkästchen	Kontrollkästchen
Ja/Nein	Dropdown-Menü für die Auswahl von <b>Ja</b> oder <b>Nein</b>
Dropdown	Dropdown-Menü

**Tabelle 4-44. Neue Felder im Ressourcenaktions- oder XaaS -Blueprint-Formular (Fortsetzung)**

Feld	Beschreibung
Liste	Liste
Kontrollkästchen-Liste	Kontrollkästchen-Liste
Radio Buttons	Gruppe von Optionsfeldern
Suchen	Suchtextfeld, das die Abfrage automatisch vervollständigt und für das Verbraucher ein Objekt auswählen
Baumstruktur	Eine Baumstruktur, mit deren Hilfe Verbraucher verfügbare Objekte suchen und auswählen
Zuordnung	Eine Zuordnungstabelle, mit deren Hilfe Verbraucher Schlüssel/-Wert-Paare für Eigenschaften definieren

Sie können auch das Formularfeld **Abschnittstitel** verwenden, um Formularseiten in Abschnitte mit separaten Überschriften zu unterteilen, und das Formularfeld **Text**, um schreibgeschützten informativen Text hinzuzufügen.

### Optionen und Werte im Formulardesigner

Beim Bearbeiten von Elementen des Blueprint- oder Ressourcenaktionsformulars können Sie verschiedene Optionen und Werte auf die Elemente anwenden.

#### Optionen

Die Optionen, die Sie auf ein Element anwenden können, sind abhängig vom Elementtyp, den Sie bearbeiten oder zum Formular hinzufügen. Einige Optionswerte werden möglicherweise im vRealize Orchestrator-Workflow konfiguriert. Diese Werte werden nicht auf der Registerkarte „Optionen“ angezeigt, da sie häufig von Bedingungen abhängig sind, die beim Ausführen des Workflows bewertet werden. Alle Optionen, die Sie für das Blueprint-Formular konfigurieren, setzen alle im vRealize Orchestrator-Workflow angegebenen Optionen außer Kraft.

Für jede Option, die Sie auf ein Element anwenden, können Sie eines der folgenden Attribute zum Definieren der Option auswählen:

<b>Nicht eingestellt</b>	Ruft die Eigenschaft aus der vRealize Orchestrator-Workflow-Präsentation ab.
<b>Konstante</b>	Legt das Element, das Sie bearbeiten, auf „Erforderlich“ oder „Optional“ fest.
<b>Feld</b>	Bindet das Element an ein anderes Element im Formular. Beispielsweise können Sie das Element nur dann als erforderlich festlegen, wenn ein anderes Element, wie beispielsweise ein Kontrollkästchen, ausgewählt ist.

<b>Bedingt</b>	Wendet eine Bedingung an. Mithilfe von Bedingungen können Sie verschiedene Klauseln und Ausdrücke erstellen und auf den Status oder die Optionen des Elements anwenden.
<b>Extern</b>	Wählen Sie eine vRealize Orchestrator-Skriptaktion aus, um den Wert zu definieren.

**Tabelle 4-45. Optionen im Formulardesigner**

Option	Beschreibung
Erforderlich	Gibt an, ob das Element erforderlich ist.
Nur Lesen	Gibt an, ob das Feld schreibgeschützt ist.
Wert	Ermöglicht die Festlegung eines Werts für das Element.
Sichtbar	Gibt an, ob das Element für den Verbraucher sichtbar ist.
Mindestlänge	Ermöglicht die Festlegung einer Mindestanzahl von Zeichen für das Zeichenfolgeingabeelement.
Maximallänge	Ermöglicht die Festlegung einer maximal zulässigen Anzahl von Zeichen für das Zeichenfolgeingabeelement.
Minimalwert	Ermöglicht die Festlegung eines Minimalwerts für das Zahleneingabeelement.
Maximalwert	Ermöglicht die Festlegung eines Maximalwerts für das Zahleneingabeelement.
Inkrement	Ermöglicht die Festlegung eines Inkrements für ein Element wie beispielsweise ein Feld vom Typ <b>Dezimal</b> oder <b>Integer</b> . Wenn beispielsweise ein Feld vom Typ <b>Integer</b> als <b>Schieberegler</b> dargestellt werden soll, können Sie den Wert dieses Schritts verwenden.
Mindestanzahl	Ermöglicht die Festlegung einer Mindestanzahl für ein Element. Wenn Sie beispielsweise eine <b>Kontrollkästchen-Liste</b> hinzufügen oder bearbeiten, können Sie die Mindestanzahl von Kontrollkästchen festlegen, die der Verbraucher auswählen muss, um den Vorgang fortsetzen zu können.
Höchstanzahl	Ermöglicht die Festlegung einer Höchstanzahl für ein Element. Wenn Sie beispielsweise eine <b>Kontrollkästchen-Liste</b> hinzufügen oder bearbeiten, können Sie die Höchstanzahl von Kontrollkästchen festlegen, die der Verbraucher auswählen muss, um den Vorgang fortsetzen zu können.

## Werte

Für manche Felder können Sie Werte auf einige Elemente anwenden und definieren, was dem Verbraucher angezeigt wird. Die verfügbaren Optionen sind abhängig vom Elementtyp, den Sie bearbeiten oder zum Formular hinzufügen.

**Tabelle 4-46. Werte im Formulardesigner**

Wert	Beschreibung
Nicht eingestellt	Ruft den Wert des Elements ab, das Sie in der vRealize Orchestrator-Workflow-Präsentation bearbeiten.
Vordefinierte Werte	Wählen Sie in der vRealize Orchestrator-Bestandsliste Werte aus einer Liste mit verwandten Objekten aus.

**Tabelle 4-46. Werte im Formulardesigner (Fortsetzung)**

Wert	Beschreibung
Wert	Definiert statische benutzerdefinierte Werte mit Bezeichnungen.
Externe Werte	Wählen Sie eine vRealize Orchestrator-Skriptaktion aus, um für den Wert Informationen zu definieren, die nicht direkt vom Workflow verfügbar gemacht werden.

### Externe Wertdefinitionen im Formulardesigner

Beim Bearbeiten bestimmter Elemente im Formulardesigner können Sie externe Wertdefinitionen zuweisen, die mithilfe von benutzerdefinierten vRealize Orchestrator-Skriptaktionen Informationen bereitstellen, die nicht direkt vom Workflow verfügbar gemacht werden.

Beispielsweise können Sie eine Ressourcenaktion veröffentlichen, um Software auf einer bereitgestellten Maschine zu installieren. Anstatt dem Verbraucher eine statische Liste mit der gesamten herunterladbaren Software bereitzustellen, können Sie diese Liste dynamisch auffüllen mit relevanter Software für das Betriebssystem der Maschine, mit Software, die der Benutzer noch nicht auf der Maschine installiert hat oder mit Software, die auf der Maschine veraltet ist und aktualisiert werden muss.

Um benutzerdefinierten dynamischen Inhalt für Ihre Verbraucher bereitzustellen, erstellen Sie eine vRealize Orchestrator-Skriptaktion, mit der die Informationen abgerufen werden, die Ihren Verbrauchern angezeigt werden sollen. Sie weisen Ihre Skriptaktion einem Feld im Formulardesigner als externe Wertdefinition zu. Wenn das Ressourcen- oder Dienst-Blueprint-Formular Ihren Verbrauchern präsentiert wird, ruft die Skriptaktion Ihre benutzerdefinierten Informationen ab und zeigt sie Ihrem Verbraucher an.

Mithilfe externer Wertdefinitionen können Sie Standardwerte oder schreibgeschützte Werte bereitstellen, boolesche Ausdrücke erstellen, Einschränkungen definieren oder Verbrauchern auswählbare Optionen in Listen, Kontrollkästchen usw. bereitstellen.

### Arbeiten mit dem Formulardesigner

Beim Erstellen von XaaS-Blueprints, benutzerdefinierten Ressourcenaktionen und benutzerdefinierten Ressourcen können Sie die Formulare der Blueprints, Aktionen und Ressourcen mithilfe des Formulardesigners bearbeiten. Sie können die Darstellung ändern und definieren, was die Verbraucher des Elements oder der Aktion sehen, wenn sie das Katalogelement anfordern oder die Vorgänge nach erfolgter Bereitstellung ausführen.

Standardmäßig wird jedes Formular von XaaS-Blueprints, Ressourcenaktionen und benutzerdefinierten Ressourcen basierend auf der Workflow-Präsentation in vRealize Orchestrator generiert.

Die Schritte in der vRealize Orchestrator-Präsentation werden als Formularseiten und die vRealize Orchestrator-Präsentationsgruppen als getrennte Abschnitte dargestellt. Die Eingabetypen des ausgewählten Workflows werden im Formular als verschiedene Felder angezeigt. Der vRealize Orchestrator-Typ string wird beispielsweise durch ein Textfeld dargestellt. Ein komplexer Typ wie z. B. VC:VirtualMachine wird durch ein Suchfeld oder eine Baumstruktur dargestellt, sodass der Verbraucher einen alphanumerischen Wert eingeben kann, um nach einer virtuellen Maschine zu suchen oder eine virtuelle Maschine auszuwählen.

#### Create cluster - Blueprint bearbeiten

Sie können die Darstellungsweise eines Objekts im Formulardesigner bearbeiten. Sie können beispielsweise die Standarddarstellung VC:VirtualMachine bearbeiten und eine Baumstruktur anstelle eines Suchfelds verwenden. Sie können auch neue Felder wie z. B. Kontrollkästchen, Dropdown-Menüs etc. hinzufügen sowie verschiedene Optionen anwenden. Wenn der Verbraucher den Workflow ausführt und die neu hinzugefügten Felder nicht gültig sind oder den vRealize Orchestrator-Workflow-Eingaben nicht ordnungsgemäß zugeordnet wurden, überspringt vRealize Orchestrator die nicht gültigen oder nicht zugeordneten Felder.

## Entwerfen eines benutzerdefinierten Ressourcenformulars

Alle Felder im Ressourcendetailformular werden dem Verbraucher auf der Seite „Elementdetails“ schreibgeschützt angezeigt, wenn er Ihre benutzerdefinierte Ressource bereitstellt. Sie können einfache Bearbeitungsvorgänge für das Formular ausführen, wie beispielsweise das Löschen, Ändern oder Neuordnen von Feldern. Sie können aber auch neue extern definierte Felder hinzufügen, die vRealize Orchestrator-Skriptaktionen verwenden, um den Verbrauchern zusätzliche schreibgeschützte Informationen verfügbar zu machen.

### ■ [Bearbeiten eines benutzerdefinierten Ressourcenelements](#)

Auf der Seite mit dem benutzerdefinierten Ressourcendetailformular können Sie bestimmte Merkmale eines Elements bearbeiten. Jedes Standardfeld auf dieser Seite stellt eine Eigenschaft der benutzerdefinierten Ressource dar. Den Eigenschaftstyp oder die Standardwerte können Sie nicht ändern, jedoch den Namen, die Größe und die Beschreibung.

### ■ [Hinzufügen einer neuen Formularseite mit benutzerdefinierten Ressourcen](#)

Sie können eine neue Seite hinzufügen, um das Formular in mehreren Registerkarten neu anzuordnen.

### ■ [Einfügen eines Abschnittstitels in ein benutzerdefiniertes Ressourcenformular](#)

Sie können einen Abschnittstitel einfügen, um das Formular in Abschnitte aufzuteilen.

### ■ [Einfügen eines Textelements in einem benutzerdefinierten Ressourcenformular](#)

Sie können ein Textfeld einfügen, um dem Formular beschreibenden Text hinzuzufügen.

### ■ [Einfügen eines extern definierten Felds in ein benutzerdefiniertes Ressourcenformular](#)

Sie können ein neues Feld einfügen und diesem eine Definition des externen Werts zuweisen, um dynamisch schreibgeschützte Informationen bereitzustellen, die Verbrauchern auf der Seite mit den Elementdetails angezeigt werden, wenn sie eine benutzerdefinierte Ressource bereitstellen.

## Bearbeiten eines benutzerdefinierten Ressourcenelements

Auf der Seite mit dem benutzerdefinierten Ressourcendetailformular können Sie bestimmte Merkmale eines Elements bearbeiten. Jedes Standardfeld auf dieser Seite stellt eine Eigenschaft der benutzerdefinierten Ressource dar. Den Eigenschaftstyp oder die Standardwerte können Sie nicht ändern, jedoch den Namen, die Größe und die Beschreibung.

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **XaaS-Architekt** an.

- [Hinzufügen einer benutzerdefinierten Ressource.](#)

#### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Benutzerdefinierte Ressourcen** aus.
- 2 Klicken Sie auf die benutzerdefinierte Ressource, um sie zu bearbeiten.
- 3 Klicken Sie auf die Registerkarte **Detailformular**.
- 4 Zeigen Sie auf das Element, das Sie bearbeiten möchten, und klicken Sie auf das Symbol **Bearbeiten**.
- 5 Geben Sie in das Textfeld **Bezeichnung** einen neuen Namen für das Feld ein, um die Bezeichnung zu ändern.
- 6 Geben Sie in das Textfeld **Beschreibung** eine Beschreibung ein.
- 7 Wählen Sie aus dem Dropdown-Menü **Größe** eine Option aus, um die Größe des Elements zu ändern.
- 8 Wählen Sie aus dem Dropdown-Menü **Beschriftungsgröße** eine Option aus, um die Beschriftungsgröße zu ändern.
- 9 Klicken Sie auf **Übernehmen**.
- 10 Klicken Sie auf **Beenden**.

#### Hinzufügen einer neuen Formularseite mit benutzerdefinierten Ressourcen

Sie können eine neue Seite hinzufügen, um das Formular in mehreren Registerkarten neu anzuordnen.

#### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Hinzufügen einer benutzerdefinierten Ressource.](#)

#### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Benutzerdefinierte Ressourcen** aus.
- 2 Klicken Sie auf die benutzerdefinierte Ressource, um sie zu bearbeiten.
- 3 Klicken Sie auf die Registerkarte **Detailformular**.
- 4 Klicken Sie neben dem Namen der Formularseite auf das Symbol **Neue Seite (+)**.
- 5 Wählen Sie den nicht verwendeten Bildschirmtyp aus und klicken Sie auf **Übernehmen**.

Wenn Sie bereits eine Ressourcendetailansicht oder eine Ressourcenlistenansicht haben, können Sie keine zwei Ansichten desselben Typs erstellen.

- 6 Klicken Sie auf **Übernehmen**.
- 7 Konfigurieren Sie das Formular.



## 8 Klicken Sie auf **Beenden**.

Sie können einige Elemente auf der ursprünglichen Formularseite löschen und auf der neuen Formularseite einfügen. Alternativ können Sie auch neue Felder hinzufügen, die externe Wertdefinitionen verwenden, um Verbrauchern Informationen bereitzustellen, die vom vRealize Orchestrator-Workflow nicht direkt verfügbar gemacht werden.

### Einfügen eines Abschnittstitels in ein benutzerdefiniertes Ressourcenformular

Sie können einen Abschnittstitel einfügen, um das Formular in Abschnitte aufzuteilen.

#### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Hinzufügen einer benutzerdefinierten Ressource](#).

#### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Benutzerdefinierte Ressourcen** aus.
- 2 Klicken Sie auf die benutzerdefinierte Ressource, um sie zu bearbeiten.
- 3 Klicken Sie auf die Registerkarte **Detailformular**.
- 4 Ziehen Sie das **Abschnittstitel**-Element aus dem Bereich „Formular“ in den Bereich „Formularseite“.
- 5 Geben Sie einen Namen für den Abschnitt ein.
- 6 Klicken Sie außerhalb des Elements, um die Änderungen zu speichern.
- 7 Klicken Sie auf **Beenden**.

### Einfügen eines Textelements in einem benutzerdefinierten Ressourcenformular

Sie können ein Textfeld einfügen, um dem Formular beschreibenden Text hinzuzufügen.

#### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Hinzufügen einer benutzerdefinierten Ressource](#).

#### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Benutzerdefinierte Ressourcen** aus.
- 2 Klicken Sie auf die benutzerdefinierte Ressource, um sie zu bearbeiten.
- 3 Klicken Sie auf die Registerkarte **Detailformular**.
- 4 Ziehen Sie das **Text**-Element aus dem Bereich „Formular“ in den Bereich „Formularseite“.
- 5 Geben Sie den Text ein, den Sie hinzufügen möchten.
- 6 Klicken Sie außerhalb des Elements, um die Änderungen zu speichern.

## 7 Klicken Sie auf **Beenden**.

### Einfügen eines extern definierten Felds in ein benutzerdefiniertes Ressourcenformular

Sie können ein neues Feld einfügen und diesem eine Definition des externen Werts zuweisen, um dynamisch schreibgeschützte Informationen bereitzustellen, die Verbrauchern auf der Seite mit den Elementdetails angezeigt werden, wenn sie eine benutzerdefinierte Ressource bereitstellen.

#### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Hinzufügen einer benutzerdefinierten Ressource](#).
- Entwickeln oder importieren Sie eine vRealize Orchestrator-Skriptaktion zum Abrufen der Informationen, die Sie Verbrauchern bereitstellen möchten.

#### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Benutzerdefinierte Ressourcen** aus.
- 2 Klicken Sie auf die benutzerdefinierte Ressource, um sie zu bearbeiten.
- 3 Klicken Sie auf die Registerkarte **Detailformular**.
- 4 Ziehen Sie ein Element aus dem Bereich „Neue Felder“ und fügen Sie es im Bereich „Formularseite“ ein.
- 5 Geben Sie eine ID für das Element in das Textfeld **ID** ein.
- 6 Geben Sie in das Textfeld **Bezeichnung** eine Bezeichnung ein.  
Bezeichnungen sind für Verbraucher in den Formularen sichtbar.
- 7 (Optional) Wählen Sie aus dem Dropdown-Menü **Typ** einen Typ für das Feld aus.
- 8 Geben Sie den Ergebnistyp Ihrer vRealize Orchestrator-Skriptaktion in das Suchfeld **Entitätstyp** ein und drücken Sie die Eingabetaste.  
  
Wenn Sie beispielsweise eine Skriptaktion zum Anzeigen des aktuellen Benutzers verwenden möchten und das Skript gibt einen vRealize Orchestrator-Ergebnistyp von `LdapUser` zurück, geben Sie **LdapUser** in das Suchfeld **Entitätstyp** ein und drücken Sie die Eingabetaste.
- 9 Klicken Sie auf **Externen Wert hinzufügen**.
- 10 Wählen Sie Ihre benutzerdefinierte vRealize Orchestrator-Skriptaktion aus.
- 11 Klicken Sie auf **Übernehmen**.
- 12 Klicken Sie noch einmal auf **Senden**.
- 13 Klicken Sie auf **Beenden**.

Wenn das Formular den Verbrauchern angezeigt wird, ruft die Skriptaktion die benutzerdefinierten Informationen ab und zeigt sie den Verbrauchern an.

## Entwerfen eines XaaS -Blueprint-Formulars

Wenn Sie einen XaaS-Blueprint erstellen, können Sie das Formular mit dem Blueprint bearbeiten, indem Sie dem Formular neue Felder hinzufügen, die vorhandenen Felder bearbeiten oder Felder löschen und neu anordnen. Darüber hinaus können Sie neue Formulare und Formularseiten erstellen und per Drag & Drop neue Felder einfügen.

- **Hinzufügen eines neuen XaaS-Blueprint-Formulars**

Beim Bearbeiten des generierten Standardformulars eines Workflows, den Sie als XaaS-Blueprint veröffentlichen möchten, können Sie ein neues XaaS-Blueprint-Formular hinzufügen.

- **Bearbeiten eines XaaS-Blueprint-Elements**

Auf der Seite „Blueprint-Formular“ eines XaaS-Blueprints können Sie einige der Merkmale eines Elements bearbeiten. Sie können den Elementtyp und dessen Standardwerte ändern und verschiedene Optionen und Werte anwenden.

- **Hinzufügen eines neuen Elements**

Beim Bearbeiten des generierten Standardformulars eines XaaS-Blueprints können Sie dem Formular ein vordefiniertes neues Element hinzufügen. Wenn Sie beispielsweise ein standardmäßig generiertes Feld nicht verwenden möchten, können Sie es löschen und durch ein neues ersetzen.

- **Einfügen eines Abschnittstitels in ein XaaS-Blueprint-Formular**

Sie können einen Abschnittstitel einfügen, um das Formular in Abschnitte aufzuteilen.

- **Hinzufügen eines Textelements zu einem XaaS-Blueprint-Formular**

Sie können ein Textfeld einfügen, um dem Formular beschreibenden Text hinzuzufügen.

## Hinzufügen eines neuen XaaS -Blueprint-Formulars

Beim Bearbeiten des generierten Standardformulars eines Workflows, den Sie als XaaS-Blueprint veröffentlichen möchten, können Sie ein neues XaaS-Blueprint-Formular hinzufügen.

Durch das Hinzufügen eines neuen XaaS-Blueprint-Formulars definieren Sie das Erscheinungsbild der Seiten „Details zu Katalogelementen“ und „Übermittelte Anforderungsdetails“. Wenn Sie kein Formular für Details zu Katalogelementen und übermittelte Aktionsdetails hinzufügen, sieht der Verbraucher, was im Anforderungsformular definiert ist.

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **XaaS-Architekt** an.
- **Erstellen Sie einen XaaS-Blueprint.**

### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > XaaS-Blueprints** aus.
- 2 Klicken Sie auf den XaaS-Blueprint, den Sie bearbeiten möchten.
- 3 Klicken Sie auf die Registerkarte **Blueprint-Formular**.
- 4 Klicken Sie auf das Symbol **Neues Formular** (+).

- 5 Geben Sie einen Namen und optional eine Beschreibung ein.
- 6 Wählen Sie im Menü **Bildschirmtyp** den Bildschirmtyp aus.

Option	Beschreibung
<b>Details zu Katalogelementen</b>	Die Seite „Details zu Katalogelementen“ wird Verbrauchern angezeigt, wenn sie auf ein Katalogelement klicken.
<b>Anforderungsformular</b>	Das standardmäßige XaaS-Blueprint-Formular. Die Verbraucher sehen das Anforderungsformular, wenn sie das Katalogelement anfordern.
<b>Übermittelte Anforderungsdetails</b>	Eine Anforderungsdetailsseite, die Verbrauchern angezeigt wird, wenn sie das Element anfordern und die Anforderungsdetails auf der Registerkarte <b>Anforderung</b> anzeigen möchten.

- 7 Klicken Sie auf **Übernehmen**.

### Weiter

Fügen Sie die gewünschten Felder hinzu, indem Sie sie aus dem Bereich „Neue Felder“ in den Bereich „Formularseite“ ziehen.


### Bearbeiten eines XaaS -Blueprint-Elements

Auf der Seite „Blueprint-Formular“ eines XaaS-Blueprints können Sie einige der Merkmale eines Elements bearbeiten. Sie können den Elementtyp und dessen Standardwerte ändern und verschiedene Optionen und Werte anwenden.

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Erstellen Sie einen XaaS-Blueprint](#).

### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > XaaS-Blueprints** aus.
- 2 Klicken Sie auf den XaaS-Blueprint, den Sie bearbeiten möchten.
- 3 Klicken Sie auf die Registerkarte **Blueprint-Formular**.
- 4 Suchen Sie das Element, das Sie bearbeiten möchten.
- 5 Klicken Sie auf das Symbol **Bearbeiten** ().
- 6 Geben Sie in das Textfeld **Bezeichnung** einen neuen Namen für das Feld ein, um die den Verbrauchern angezeigte Bezeichnung zu ändern.
- 7 Geben Sie in das Textfeld **Beschreibung** eine Beschreibung ein.
- 8 Wählen Sie aus dem Dropdown-Menü **Typ** eine Option aus, um den Anzeigetyp des Elements zu ändern.

Die verfügbaren Optionen hängen vom bearbeiteten Elementtyp ab.

- 9 Wählen Sie aus dem Dropdown-Menü **Größe** eine Option aus, um die Größe des Elements zu ändern.
- 10 Wählen Sie aus dem Dropdown-Menü **Beschriftungsgröße** eine Option aus, um die Beschriftungsgröße zu ändern.
- 11 Bearbeiten Sie den Standardwert des Elements.

Option	Beschreibung
<b>Nicht eingestellt</b>	Ruft den Wert des Elements ab, das Sie in der vRealize Orchestrator-Workflow-Präsentation bearbeiten.
<b>Konstante</b>	Legt den Standardwert des Elements, das Sie bearbeiten, auf einen von Ihnen angegebenen Konstantenwert fest.
<b>Feld</b>	Bindet den Standardwert des Elements an einen Parameter eines anderen Elements aus der Repräsentation.
<b>Bedingt</b>	Wendet eine Bedingung an. Mithilfe von Bedingungen können Sie verschiedene Klauseln und Ausdrücke erstellen und auf ein Element anwenden.
<b>Extern</b>	Wählen Sie eine vRealize Orchestrator-Skriptaktion aus, um den Wert zu definieren.

- 12 Auf der Registerkarte **Optionen** können Sie Optionen auf das Element anwenden.

Option	Beschreibung
<b>Nicht eingestellt</b>	Ruft den Wert des Elements ab, das Sie in der vRealize Orchestrator-Workflow-Präsentation bearbeiten.
<b>Konstante</b>	Legt den Standardwert des Elements, das Sie bearbeiten, auf einen von Ihnen angegebenen Konstantenwert fest.
<b>Feld</b>	Bindet den Standardwert des Elements an einen Parameter eines anderen Elements aus der Repräsentation.
<b>Bedingt</b>	Wendet eine Bedingung an. Mithilfe von Bedingungen können Sie verschiedene Klauseln und Ausdrücke erstellen und auf ein Element anwenden.
<b>Extern</b>	Wählen Sie eine vRealize Orchestrator-Skriptaktion aus, um den Wert zu definieren.

- 13 Fügen Sie auf der Registerkarte **Werte** einen oder mehrere Werte für das Element hinzu.

Die verfügbaren Optionen hängen vom bearbeiteten Elementtyp ab.

Option	Beschreibung
<b>Nicht eingestellt</b>	Ruft den Wert des Elements ab, das Sie in der vRealize Orchestrator-Workflow-Präsentation bearbeiten.
<b>Vordefinierte Werte</b>	<p>Wählen Sie in der vRealize Orchestrator-Bestandsliste Werte aus einer Liste mit verwandten Objekten aus.</p> <ol style="list-style-type: none"> <li>a Geben Sie in das Suchfeld <b>Vordefinierte Werte</b> einen Wert ein, um die vRealize Orchestrator-Bestandsliste zu durchsuchen.</li> <li>b Wählen Sie in den Suchergebnissen einen Wert aus und drücken Sie die Eingabetaste.</li> </ol>

Option	Beschreibung
<b>Wert</b>	<p>Definieren Sie benutzerdefinierte Werte mit Bezeichnungen.</p> <ol style="list-style-type: none"> <li>Geben Sie in das Textfeld <b>Wert</b> einen Wert ein.</li> <li>Geben Sie in das Textfeld <b>Bezeichnung</b> eine Bezeichnung für den Wert ein.</li> <li>Klicken Sie auf das Symbol <b>Hinzufügen</b> (+).</li> </ol>
<b>Externe Werte</b>	<p>Wählen Sie eine vRealize Orchestrator-Skriptaktion aus, um für den Wert Informationen zu definieren, die nicht direkt vom Workflow verfügbar gemacht werden.</p> <ul style="list-style-type: none"> <li>Wählen Sie <b>Externen Wert hinzufügen</b> aus.</li> <li>Wählen Sie Ihre vRealize Orchestrator-Skriptaktion aus.</li> <li>Klicken Sie auf <b>Übernehmen</b>.</li> </ul>

14 Klicken Sie auf **Übernehmen**.

15 Klicken Sie auf **Beenden**.

### Hinzufügen eines neuen Elements

Beim Bearbeiten des generierten Standardformulars eines XaaS-Blueprints können Sie dem Formular ein vordefiniertes neues Element hinzufügen. Wenn Sie beispielsweise ein standardmäßig generiertes Feld nicht verwenden möchten, können Sie es löschen und durch ein neues ersetzen.

#### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Erstellen Sie einen XaaS-Blueprint](#).

#### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > XaaS-Blueprints** aus.
- 2 Klicken Sie auf den XaaS-Blueprint, den Sie bearbeiten möchten.
- 3 Klicken Sie auf die Registerkarte **Blueprint-Formular**.
- 4 Ziehen Sie ein Element aus dem Bereich „Neue Felder“ und fügen Sie es im Bereich „Formularseite“ ein.
- 5 Geben Sie in das Textfeld **ID** die ID eines Workflow-Eingabeparameters ein.
- 6 Geben Sie in das Textfeld **Bezeichnung** eine Bezeichnung ein.  
Bezeichnungen sind für Verbraucher in den Formularen sichtbar.
- 7 (Optional) Wählen Sie aus dem Dropdown-Menü **Typ** einen Typ für das Feld aus.

- 8 Geben Sie ein vRealize Orchestrator-Objekt in das Textfeld **Entitätstyp** ein und drücken Sie die Eingabetaste.

Dieser Schritt ist nicht für alle Feldtypen erforderlich.

Option	Beschreibung
<b>Ergebnistyp</b>	Wenn Sie ein Skript zum Definieren eines externen Werts für das Feld verwenden, geben Sie den Ergebnistyp Ihrer vRealize Orchestrator-Skriptaktion ein.
<b>Eingabeparameter</b>	Wenn Sie das Feld zum Akzeptieren der Verbrauchereingaben und zum Übergeben von Parametern zurück an vRealize Orchestrator verwenden, geben Sie den Typ für den Eingabeparameter ein, der vom vRealize Orchestrator-Workflow akzeptiert wird.
<b>Ausgabeparameter</b>	Wenn Sie das Feld zum Anzeigen von Informationen für Verbraucher verwenden, geben Sie den Typ für den Ausgabeparameter des vRealize Orchestrator-Workflows ein.

- 9 (Optional) Aktivieren Sie das Kontrollkästchen **Mehrere Werte**, um Verbrauchern die Auswahl mehrerer Objekte zu erlauben.

Diese Option ist nicht für alle Feldtypen verfügbar.

- 10 Klicken Sie auf **Übernehmen**.

- 11 Klicken Sie auf **Aktualisieren**.

#### Weiter

Sie können das Element bearbeiten, um die Standardeinstellungen zu ändern und verschiedene Optionen und Werte anzuwenden.

#### Einfügen eines Abschnittstitels in ein XaaS -Blueprint-Formular

Sie können einen Abschnittstitel einfügen, um das Formular in Abschnitte aufzuteilen.

#### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Erstellen Sie einen XaaS-Blueprint](#).

#### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > XaaS-Blueprints** aus.
- 2 Klicken Sie auf den XaaS-Blueprint, den Sie bearbeiten möchten.
- 3 Klicken Sie auf die Registerkarte **Blueprint-Formular**.
- 4 Ziehen Sie das **Abschnittstitel**-Element aus dem Bereich „Formular“ in den Bereich „Formularseite“.
- 5 Geben Sie einen Namen für den Abschnitt ein.
- 6 Klicken Sie außerhalb des Elements, um die Änderungen zu speichern.
- 7 Klicken Sie auf **Aktualisieren**.

## Hinzufügen eines Textelements zu einem XaaS -Blueprint-Formular

Sie können ein Textfeld einfügen, um dem Formular beschreibenden Text hinzuzufügen.

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Erstellen Sie einen XaaS-Blueprint.](#)

### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > XaaS-Blueprints** aus.
- 2 Klicken Sie auf den XaaS-Blueprint, den Sie bearbeiten möchten.
- 3 Klicken Sie auf die Registerkarte **Blueprint-Formular**.
- 4 Ziehen Sie das **Text**-Element aus dem Bereich „Neue Felder“ in den Bereich „Formularseite“.
- 5 Geben Sie den Text ein, den Sie hinzufügen möchten.
- 6 Klicken Sie außerhalb des Elements, um die Änderungen zu speichern.
- 7 Klicken Sie auf **Aktualisieren**.

## Entwerfen eines Ressourcenaktionsformulars

Wenn Sie eine Ressourcenaktion erstellen, können Sie das Formular mit den Aktionen bearbeiten, indem Sie dem Formular neue Felder hinzufügen, die vorhandenen Felder bearbeiten oder Felder löschen und neu anordnen. Darüber hinaus können Sie neue Formulare und Formularseiten erstellen und per Drag & Drop neue Felder einfügen.

### Hinzufügen eines neuen Ressourcenaktionsformulars

Beim Bearbeiten des generierten Standardformulars eines Workflows, den Sie als Ressourcenaktion veröffentlichen möchten, können Sie ein neues Ressourcenaktionsformular hinzufügen.

Durch das Hinzufügen eines neuen Ressourcenaktionsformulars definieren Sie das Erscheinungsbild der Seite mit den übermittelten Aktionsdetails. Wenn Sie kein Formular für übermittelte Aktionsdetails hinzufügen, sieht der Verbraucher, was im Aktionsformular definiert ist.

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Erstellen einer Ressourcenaktion.](#)

### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Klicken Sie auf die Ressourcenaktion, die Sie bearbeiten möchten.
- 3 Klicken Sie auf die Registerkarte **Formular**.



- 4 Klicken Sie auf das Symbol **Neues Formular** (+).
- 5 Geben Sie einen Namen und optional eine Beschreibung ein.
- 6 Wählen Sie im Menü **Bildschirmtyp** den Bildschirmtyp aus.

Option	Beschreibung
<b>Aktionsformular</b>	Das standardmäßige Ressourcenaktionsformular, das Verbrauchern angezeigt wird, wenn sie die Aktion nach der Bereitstellung ausführen möchten.
<b>Übermittelte Aktionsdetails</b>	Eine Anforderungsdetailsseite, die Verbrauchern angezeigt wird, wenn sie die Aktion anfordern und die Anforderungsdetails auf der Registerkarte <b>Anforderung</b> anzeigen möchten.

- 7 Klicken Sie auf **Übernehmen**.

#### Weiter

Fügen Sie die gewünschten Felder hinzu, indem Sie sie aus dem Bereich „Neue Felder“ in den Bereich „Formularseite“ ziehen.

#### Hinzufügen eines neuen Elements zu einem Ressourcenaktionsformular

Beim Bearbeiten des generierten Standardformulars einer Ressourcenaktion können Sie dem Formular ein vordefiniertes neues Element hinzufügen. Wenn Sie beispielsweise ein standardmäßig generiertes Feld nicht verwenden möchten, können Sie es löschen und durch ein neues ersetzen.

#### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Erstellen einer Ressourcenaktion](#).

#### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Klicken Sie auf die Ressourcenaktion, die Sie bearbeiten möchten.
- 3 Klicken Sie auf die Registerkarte **Formular**.
- 4 Ziehen Sie ein Element aus dem Bereich „Neue Felder“ und fügen Sie es im Bereich „Formularseite“ ein.
- 5 Geben Sie in das Textfeld **ID** die ID eines Workflow-Eingabeparameters ein.
- 6 Geben Sie in das Textfeld **Bezeichnung** eine Bezeichnung ein.  
Bezeichnungen sind für Verbraucher in den Formularen sichtbar.
- 7 (Optional) Wählen Sie aus dem Dropdown-Menü **Typ** einen Typ für das Feld aus.

- 8 Geben Sie ein vRealize Orchestrator-Objekt in das Textfeld **Entitätstyp** ein und drücken Sie die Eingabetaste.

Dieser Schritt ist nicht für alle Feldtypen erforderlich.

Option	Beschreibung
<b>Ergebnistyp</b>	Wenn Sie ein Skript zum Definieren eines externen Werts für das Feld verwenden, geben Sie den Ergebnistyp Ihrer vRealize Orchestrator-Skriptaktion ein.
<b>Eingabeparameter</b>	Wenn Sie das Feld zum Akzeptieren der Verbrauchereingaben und zum Übergeben von Parametern zurück an vRealize Orchestrator verwenden, geben Sie den Typ für den Eingabeparameter ein, der vom vRealize Orchestrator-Workflow akzeptiert wird.
<b>Ausgabeparameter</b>	Wenn Sie das Feld zum Anzeigen von Informationen für Verbraucher verwenden, geben Sie den Typ für den Ausgabeparameter des vRealize Orchestrator-Workflows ein.

- 9 (Optional) Aktivieren Sie das Kontrollkästchen **Mehrere Werte**, um Verbrauchern die Auswahl mehrerer Objekte zu erlauben.

Diese Option ist nicht für alle Feldtypen verfügbar.

- 10 Klicken Sie auf **Übernehmen**.

- 11 Klicken Sie auf **Beenden**.

#### Weiter

Sie können das Element bearbeiten, um die Standardeinstellungen zu ändern und verschiedene Optionen und Werte anzuwenden.


#### Bearbeiten eines Ressourcenaktionselements

Auf der Seite mit dem Ressourcenaktionsformular können Sie bestimmte Merkmale eines Elements bearbeiten. Sie können den Elementtyp und dessen Standardwerte ändern und verschiedene Optionen und Werte anwenden.

#### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Erstellen einer Ressourcenaktion](#).

#### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Klicken Sie auf die Ressourcenaktion, die Sie bearbeiten möchten.
- 3 Klicken Sie auf die Registerkarte **Formular**.
- 4 Suchen Sie das Element, das Sie bearbeiten möchten.
- 5 Klicken Sie auf das Symbol **Bearbeiten** ().

- 6 Geben Sie in das Textfeld **Bezeichnung** einen neuen Namen für das Feld ein, um die den Verbrauchern angezeigte Bezeichnung zu ändern.
- 7 Geben Sie in das Textfeld **Beschreibung** eine Beschreibung ein.
- 8 Wählen Sie aus dem Dropdown-Menü **Typ** eine Option aus, um den Anzeigetyp des Elements zu ändern.

Die verfügbaren Optionen hängen vom bearbeiteten Elementtyp ab.

- 9 Wählen Sie aus dem Dropdown-Menü **Größe** eine Option aus, um die Größe des Elements zu ändern.
- 10 Wählen Sie aus dem Dropdown-Menü **Beschriftungsgröße** eine Option aus, um die Beschriftungsgröße zu ändern.
- 11 Bearbeiten Sie den Standardwert des Elements.

Option	Beschreibung
<b>Nicht eingestellt</b>	Ruft den Wert des Elements ab, das Sie in der vRealize Orchestrator-Workflow-Präsentation bearbeiten.
<b>Konstante</b>	Legt den Standardwert des Elements, das Sie bearbeiten, auf einen von Ihnen angegebenen Konstantenwert fest.
<b>Feld</b>	Bindet den Standardwert des Elements an einen Parameter eines anderen Elements aus der Repräsentation.
<b>Bedingt</b>	Wendet eine Bedingung an. Mithilfe von Bedingungen können Sie verschiedene Klauseln und Ausdrücke erstellen und auf ein Element anwenden.
<b>Extern</b>	Wählen Sie eine vRealize Orchestrator-Skriptaktion aus, um den Wert zu definieren.

- 12 Auf der Registerkarte **Optionen** können Sie Optionen auf das Element anwenden.

Option	Beschreibung
<b>Nicht eingestellt</b>	Ruft den Wert des Elements ab, das Sie in der vRealize Orchestrator-Workflow-Präsentation bearbeiten.
<b>Konstante</b>	Legt den Standardwert des Elements, das Sie bearbeiten, auf einen von Ihnen angegebenen Konstantenwert fest.
<b>Feld</b>	Bindet den Standardwert des Elements an einen Parameter eines anderen Elements aus der Repräsentation.
<b>Bedingt</b>	Wendet eine Bedingung an. Mithilfe von Bedingungen können Sie verschiedene Klauseln und Ausdrücke erstellen und auf ein Element anwenden.
<b>Extern</b>	Wählen Sie eine vRealize Orchestrator-Skriptaktion aus, um den Wert zu definieren.

### 13 Fügen Sie auf der Registerkarte **Werte** einen oder mehrere Werte für das Element hinzu.

Die verfügbaren Optionen hängen vom bearbeiteten Elementtyp ab.

Option	Beschreibung
<b>Nicht eingestellt</b>	Ruft den Wert des Elements ab, das Sie in der vRealize Orchestrator-Workflow-Präsentation bearbeiten.
<b>Vordefinierte Werte</b>	<p>Wählen Sie in der vRealize Orchestrator-Bestandsliste Werte aus einer Liste mit verwandten Objekten aus.</p> <ol style="list-style-type: none"> <li>Geben Sie in das Suchfeld <b>Vordefinierte Werte</b> einen Wert ein, um die vRealize Orchestrator-Bestandsliste zu durchsuchen.</li> <li>Wählen Sie in den Suchergebnissen einen Wert aus und drücken Sie die Eingabetaste.</li> </ol>
<b>Wert</b>	<p>Definieren Sie benutzerdefinierte Werte mit Bezeichnungen.</p> <ol style="list-style-type: none"> <li>Geben Sie in das Textfeld <b>Wert</b> einen Wert ein.</li> <li>Geben Sie in das Textfeld <b>Bezeichnung</b> eine Bezeichnung für den Wert ein.</li> <li>Klicken Sie auf das Symbol <b>Hinzufügen</b> (+).</li> </ol>
<b>Externe Werte</b>	<p>Wählen Sie eine vRealize Orchestrator-Skriptaktion aus, um für den Wert Informationen zu definieren, die nicht direkt vom Workflow verfügbar gemacht werden.</p> <ul style="list-style-type: none"> <li>Wählen Sie <b>Externen Wert hinzufügen</b> aus.</li> <li>Wählen Sie Ihre vRealize Orchestrator-Skriptaktion aus.</li> <li>Klicken Sie auf <b>Übernehmen</b>.</li> </ul>

### 14 Klicken Sie auf **Übernehmen**.

### 15 Klicken Sie auf **Aktualisieren**.

## Einfügen eines Abschnittstitels in ein Ressourcenaktionsformular

Sie können einen Abschnittstitel einfügen, um das Formular in Abschnitte aufzuteilen.

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Erstellen einer Ressourcenaktion](#).

### Vorgehensweise

- Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- Klicken Sie auf die Ressourcenaktion, die Sie bearbeiten möchten.
- Klicken Sie auf die Registerkarte **Formular**.
- Ziehen Sie das **Abschnittstitel**-Element aus dem Bereich „Formular“ in den Bereich „Formularseite“.
- Geben Sie einen Namen für den Abschnitt ein.
- Klicken Sie außerhalb des Elements, um die Änderungen zu speichern.
- Klicken Sie auf **Beenden**.

## Hinzufügen eines Textelements zu einem Ressourcenaktionsformular

Sie können ein Textfeld einfügen, um dem Formular beschreibenden Text hinzuzufügen.

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Erstellen einer Ressourcenaktion](#).

### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Klicken Sie auf die Ressourcenaktion, die Sie bearbeiten möchten.
- 3 Klicken Sie auf die Registerkarte **Formular**.
- 4 Ziehen Sie das **Text**-Element aus dem Bereich „Neue Felder“ in den Bereich „Formularseite“.
- 5 Geben Sie den Text ein, den Sie hinzufügen möchten.
- 6 Klicken Sie außerhalb des Elements, um die Änderungen zu speichern.
- 7 Klicken Sie auf **Beenden**.

## XaaS -Beispiele und -Szenarien

Die Beispiele und Szenarien enthalten Vorschläge, wie Sie vRealize Automation für häufige Aufgaben mit XaaS-Blueprints und Ressourcenaktionen verwenden können.

### Erstellen eines XaaS -Blueprints und einer Aktion zum Erstellen und Ändern eines Benutzers

Mithilfe von XaaS können Sie ein Katalogelement für die Bereitstellung eines Benutzers in einer Gruppe erstellen und veröffentlichen. Sie können dem bereitgestellten Benutzer auch einen neuen Vorgang nach erfolgter Bereitstellung zuordnen. Dies kann beispielsweise ein Vorgang sein, der den Verbrauchern das Ändern des Benutzerkennworts gestattet.

Als XaaS-Architekt erstellen Sie eine neue benutzerdefinierte Ressource, einen XaaS-Blueprint und veröffentlichen ein Katalogelement zum Erstellen eines Benutzers. Außerdem erstellen Sie eine Ressourcenaktion zum Ändern des Kennworts des Benutzers.

Als Katalogadministrator erstellen Sie einen Dienst und nehmen das Blueprint-Katalogelement in den Dienst auf. Darüber hinaus bearbeiten Sie die Workflow-Präsentation des Katalogelements mithilfe des Formulardesigners und ändern die Art und Weise, wie Verbrauchern das Anforderungsformular angezeigt wird.

Als Business-Gruppenmanager oder Mandantenadministrator erteilen Sie einem Verbraucher die Berechtigung für den neu erstellten Dienst, das Katalogelement und die Ressourcenaktion.

### Voraussetzungen

Überprüfen Sie, ob das Active Directory-Plug-In ordnungsgemäß konfiguriert ist und ob Sie über die Rechte zum Erstellen von Benutzern in Active Directory verfügen.

## Vorgehensweise

### 1 Erstellen eines Testbenutzers als benutzerdefinierte Ressource

Sie können eine benutzerdefinierte Ressource erstellen und dem vRealize Orchestrator-Objektyp AD:User zuordnen.

### 2 Erstellen eines XaaS-Blueprints zum Erstellen eines Benutzers

Nachdem Sie die benutzerdefinierte Ressource erstellt haben, können Sie den XaaS-Blueprint erstellen, um den Workflow „Benutzer in einer Gruppe erstellen“ als Katalogelement zu veröffentlichen.

### 3 Veröffentlichen des Blueprints „Benutzer erstellen“ als Katalogelement

Nachdem Sie den XaaS-Blueprint „Testbenutzer erstellen“ erstellt haben, können Sie ihn als Katalogelement veröffentlichen.

### 4 Erstellen einer Ressourcenaktion zum Ändern eines Benutzerkennworts

Sie können eine Ressourcenaktion erstellen, damit die Verbraucher des XaaS-Blueprints „Benutzer erstellen“ das Kennwort des Benutzers nach der Bereitstellung des Benutzers ändern können.

### 5 Veröffentlichen der Ressourcenaktion zum Ändern eines Kennworts

Um die Ressourcenaktion zum Ändern des Kennworts des Testbenutzers als Vorgang nach erfolgter Bereitstellung zu verwenden, müssen Sie es veröffentlichen.

### 6 Erstellen eines Katalogdienstes zum Erstellen eines Testbenutzers

Sie können einen Dienst erstellen, um das Katalogelement zum Erstellen eines Benutzers im Servicekatalog anzuzeigen und um es Verbrauchern zu ermöglichen, auf einfache Weise das Katalogelement aufzufinden, das sich auf das Erstellen des Testbenutzers bezieht.

### 7 Zuordnen des Katalogelements zum Dienst „Testbenutzer erstellen“

Um das Katalogelement „Testbenutzer erstellen“ in den Dienst „Testbenutzer erstellen“ einzubeziehen, müssen Sie es diesem Dienst zuordnen.

### 8 Erteilen der Berechtigung für den Dienst und die Ressourcenaktion an einen Verbraucher

Business-Gruppenmanager und Mandantenadministratoren können einem Benutzer oder einer Benutzergruppe die Berechtigung für den Dienst und die Ressourcenaktion erteilen, damit sie den Dienst in ihrem Katalog sehen und das im Dienst enthaltene Katalogelement „Testbenutzer erstellen“ anfordern können. Nachdem die Verbraucher das Element bereitgestellt haben, können sie die Änderung des Benutzerkennworts anfordern.

## Erstellen eines Testbenutzers als benutzerdefinierte Ressource

Sie können eine benutzerdefinierte Ressource erstellen und dem vRealize Orchestrator-Objektyp AD:User zuordnen.

## Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.

## Vorgehensweise

### 1 Wählen Sie **Design > XaaS > Benutzerdefinierte Ressourcen** aus.

- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Geben Sie im Textfeld **Orchestrator-Typ** Folgendes ein: **AD:User**. Drücken Sie dann die Eingabetaste.
- 4 Wählen Sie in der Liste **AD:User** aus.
- 5 Geben Sie einen Namen für die Ressource ein.  
Beispielsweise **Testbenutzer**.
- 6 Geben Sie eine Beschreibung für die Ressource ein.  
Beispielsweise  
**Dies ist eine benutzerdefinierte Testressource, die ich für mein Katalogelement zum Erstellen eines Benutzers in einer Gruppe verwenden werde.**
- 7 Klicken Sie auf **Weiter**.
- 8 Lassen Sie das Formular unverändert.
- 9 Klicken Sie auf **Fertig stellen**.

Sie haben die benutzerdefinierte Testressource erstellt, die auf der Seite „Benutzerdefinierte Ressourcen“ aufgeführt wird.

#### Weiter

Erstellen Sie einen XaaS-Blueprint.

#### Erstellen eines XaaS -Blueprints zum Erstellen eines Benutzers

Nachdem Sie die benutzerdefinierte Ressource erstellt haben, können Sie den XaaS-Blueprint erstellen, um den Workflow „Benutzer in einer Gruppe erstellen“ als Katalogelement zu veröffentlichen.

#### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.

#### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > XaaS-Blueprints** aus.
- 2 Klicken Sie auf **Hinzufügen** (+).
- 3 Navigieren Sie in der vRealize Orchestrator-Workflow-Bibliothek zu **Orchestrator > Bibliothek > Microsoft > Active Directory > Benutzer** und wählen Sie den Workflow **Benutzer in einer Gruppe erstellen** aus.
- 4 Klicken Sie auf **Weiter**.
- 5 Ändern Sie den Namen des Blueprints in **Testbenutzer erstellen** und übernehmen Sie die Beschreibung.
- 6 Klicken Sie auf **Weiter**.

**7** Bearbeiten Sie das Blueprint-Formular.

- a Klicken Sie auf **Der Domänenname im Win2000-Formular**.
- b Klicken Sie auf die Registerkarte **Optionen**.
- c Klicken Sie auf den Dropdown-Pfeil neben **Wert**, wählen Sie im Dropdown-Menü **Konstante** aus und geben Sie **test.domain** ein.

Sie haben für den Domännennamen einen Konstantenwert festgelegt.

- d Klicken Sie auf den Dropdown-Pfeil neben **Sichtbar**, wählen Sie im Dropdown-Menü **Konstante** aus und wählen Sie dann im Dropdown-Menü **Nein** aus.

Sie haben festgelegt, dass der Domänenname für den Verbraucher des Katalogelements nicht sichtbar ist.

- e Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

**8** Klicken Sie auf **Weiter**.

**9** Wählen Sie **newUser [Testbenutzer]** als bereitzustellenden Ausgabeparameter aus.

**10** Klicken Sie auf **Fertig stellen**.

Sie haben einen Blueprint zum Erstellen eines Testbenutzers erstellt, und der Blueprint wird auf der Seite mit den XaaS-Blueprints angezeigt.

## Weiter

Veröffentlichen Sie den Blueprint „Testbenutzer erstellen“, um ihn als aktives Katalogelement festzulegen.

## Veröffentlichen des Blueprints „Benutzer erstellen“ als Katalogelement

Nachdem Sie den XaaS-Blueprint „Testbenutzer erstellen“ erstellt haben, können Sie ihn als Katalogelement veröffentlichen.

## Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.

## Vorgehensweise

- 1** Wählen Sie **Design > XaaS > XaaS-Blueprints** aus.
- 2** Wählen Sie die Zeile des Blueprints „Testbenutzer erstellen“ aus und klicken Sie auf die Schaltfläche **Veröffentlichen**.

Der Status des Blueprints „Testbenutzer erstellen“ ändert sich zu „Veröffentlicht“. Sie können zu **Administration > Katalogmanagement > Katalogelemente** navigieren und anzeigen, dass der Blueprint „Testbenutzer erstellen“ als Katalogelement veröffentlicht wurde.

## Erstellen einer Ressourcenaktion zum Ändern eines Benutzerkennworts

Sie können eine Ressourcenaktion erstellen, damit die Verbraucher des XaaS-Blueprints „Benutzer erstellen“ das Kennwort des Benutzers nach der Bereitstellung des Benutzers ändern können.



## Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.

## Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Klicken Sie auf **Hinzufügen** (+).
- 3 Navigieren Sie in der vRealize Orchestrator-Workflow-Bibliothek zu **Orchestrator > Bibliothek > Microsoft > Active Directory > Benutzer** und wählen Sie den Workflow **Benutzerkennwort ändern** aus.
- 4 Klicken Sie auf **Weiter**.
- 5 Wählen Sie aus dem Dropdown-Menü **Ressourcentyp** den Eintrag **Testbenutzer** aus.  
Dies ist die benutzerdefinierte Ressource, die Sie zuvor erstellt haben.
- 6 Wählen Sie aus dem Dropdown-Menü **Eingabeparameter** den Eintrag **Benutzer** aus.
- 7 Klicken Sie auf **Weiter**.
- 8 Ändern Sie den Namen der Ressourcenaktion in **Kennwort des Testbenutzers ändern** und übernehmen Sie die Beschreibung auf der Registerkarte **Details**.
- 9 Klicken Sie auf **Weiter**.
- 10 (Optional) Lassen Sie das Formular unverändert.
- 11 Klicken Sie auf **Hinzufügen**.

Sie haben eine Ressourcenaktion erstellt, um das Kennwort eines Benutzers zu ändern, und die Ressourcenaktion wird auf der Seite „Ressourcenaktionen“ aufgeführt.

## Weiter

Veröffentlichen Sie die Ressourcenaktion „Kennwort des Testbenutzers ändern“.

## Veröffentlichen der Ressourcenaktion zum Ändern eines Kennworts

Um die Ressourcenaktion zum Ändern des Kennworts des Testbenutzers als Vorgang nach erfolgter Bereitstellung zu verwenden, müssen Sie es veröffentlichen.

## Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.

## Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Wählen Sie die Zeile der Aktion zum Ändern des Kennworts des Testbenutzers aus und klicken Sie auf die Schaltfläche **Veröffentlichen**.

Der Status der Aktion zum Ändern des Kennworts des Testbenutzers ändert sich zu „Veröffentlicht“.

## Weiter

Weisen Sie der Ressourcenaktion ein Symbol zu. Sie können anschließend beim Erstellen einer Berechtigung die Aktion verwenden. Weitere Informationen über das Zuweisen eines Symbols zu einer Ressourcenaktion finden Sie unter [Zuweisen eines Symbols zu einer Ressourcenaktion](#).

## Erstellen eines Katalogdienstes zum Erstellen eines Testbenutzers

Sie können einen Dienst erstellen, um das Katalogelement zum Erstellen eines Benutzers im Servicekatalog anzuzeigen und um es Verbrauchern zu ermöglichen, auf einfache Weise das Katalogelement aufzufinden, das sich auf das Erstellen des Testbenutzers bezieht.

### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **Katalogadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Katalogmanagement > Services** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Geben Sie **Testbenutzer erstellen** als Name für den Dienst ein.
- 4 Wählen Sie aus dem Dropdown-Menü **Status** den Eintrag **Aktiv** aus.
- 5 Lassen Sie die anderen Textfelder leer.
- 6 Klicken Sie auf **OK**.

Sie haben den Dienst „Testbenutzer erstellen“ erstellt, der auf der Seite mit den Diensten angezeigt wird.

## Weiter

Bearbeiten Sie das Katalogelement „Testbenutzer erstellen“, um es in den Dienst einzubeziehen.

## Zuordnen des Katalogelements zum Dienst „Testbenutzer erstellen“

Um das Katalogelement „Testbenutzer erstellen“ in den Dienst „Testbenutzer erstellen“ einzubeziehen, müssen Sie es diesem Dienst zuordnen.

### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **Katalogadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Katalogmanagement > Katalogelemente** aus.
- 2 Suchen Sie nach dem Katalogelement „Testbenutzer erstellen“ und klicken Sie auf den Namen des Katalogelements.
- 3 (Optional) Klicken Sie auf **Datei auswählen**, um das Symbol des Katalogelements zu ändern.

- 4 Wählen Sie aus dem Dropdown-Menü **Dienst** den Dienst **Testbenutzer erstellen** aus.
- 5 Klicken Sie auf **Beenden**.

Sie haben das Katalogelement „Testbenutzer erstellen“ dem Dienst „Testbenutzer erstellen“ zugeordnet.

#### Weiter

Business-Gruppenmanager und Mandantenadministratoren können einem Benutzer oder einer Benutzergruppe die Berechtigung für den Dienst und die Ressourcenaktion erteilen.

#### Erteilen der Berechtigung für den Dienst und die Ressourcenaktion an einen Verbraucher

Business-Gruppenmanager und Mandantenadministratoren können einem Benutzer oder einer Benutzergruppe die Berechtigung für den Dienst und die Ressourcenaktion erteilen, damit sie den Dienst in ihrem Katalog sehen und das im Dienst enthaltene Katalogelement „Testbenutzer erstellen“ anfordern können. Nachdem die Verbraucher das Element bereitgestellt haben, können sie die Änderung des Benutzerkennworts anfordern.

#### Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** oder **Business-Gruppenmanager** an.

#### Vorgehensweise

- 1 Wählen Sie **Administration > Katalogmanagement > Berechtigungen** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Geben Sie **Benutzer erstellen** in das Textfeld **Name** ein.
- 4 Lassen Sie die Textfelder **Beschreibung** und **Ablaufdatum** leer.
- 5 Wählen Sie aus dem Dropdown-Menü **Status** den Eintrag **Aktiv** aus.
- 6 Wählen Sie im Dropdown-Menü **Business-Gruppe** die Business-Zielgruppe aus.
- 7 Geben Sie in das Textfeld **Benutzer und Gruppen** einen Benutzernamen ein und drücken Sie die Eingabetaste.  
  
Die Person, die Sie auswählen, sieht den Dienst und die im Dienst enthaltenen Katalogelemente im Katalog.
- 8 Klicken Sie auf **Weiter**.
- 9 Geben Sie **Testbenutzer erstellen** in das Textfeld **Berechtigte Services** ein und drücken Sie die Eingabetaste.
- 10 Geben Sie **Kennwort des Testbenutzers ändern** in das Textfeld **Berechtigte Aktionen** ein und drücken Sie die Eingabetaste.
- 11 Klicken Sie auf **Hinzufügen**.

Sie haben eine aktive Berechtigung erstellt und den Dienst für den Katalog der Verbraucher verfügbar gemacht.

Wenn sich Verbraucher des Diensts an ihren vRealize Automation-Konsolen anmelden, wird der von Ihnen erstellte Dienst, „Testbenutzer erstellen“, auf der Registerkarte **Katalog** angezeigt. Sie können das Katalogelement „Benutzer in einer Gruppe erstellen“, das Sie erstellt und zum Dienst hinzugefügt haben, anfordern. Nachdem sie den Benutzer erstellt haben, können sie das Benutzerkennwort ändern.

### Erstellen und Veröffentlichen einer XaaS -Aktion zum Migrieren einer virtuellen Maschine

Sie können eine XaaS-Ressourcenaktion zum Erweitern der Vorgänge, die Verbraucher auf IaaS-bereitgestellten virtuellen vSphere-Maschinen durchführen können, erstellen und veröffentlichen.

In diesem Szenario erstellen Sie eine Ressourcenaktion für eine schnelle Migration einer virtuellen vSphere-Maschine.

#### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.

#### Vorgehensweise

##### 1 Erstellen einer Ressourcenaktion zum Migrieren einer virtuellen vSphere-Maschine

Das Erstellen einer benutzerdefinierten Ressourcenaktion erfolgt, damit die Verbraucher virtuelle vSphere-Maschinen migrieren können, nachdem sie die virtuellen vSphere-Maschinen mit IaaS bereitgestellt haben.

##### 2 Veröffentlichen der Aktion für das Migrieren einer virtuellen vSphere-Maschine

Um die Schnellmigration der Ressourcenaktion der virtuellen Maschine als Vorgang nach erfolgter Bereitstellung zu verwenden, müssen Sie sie veröffentlichen.

### Erstellen einer Ressourcenaktion zum Migrieren einer virtuellen vSphere-Maschine

Das Erstellen einer benutzerdefinierten Ressourcenaktion erfolgt, damit die Verbraucher virtuelle vSphere-Maschinen migrieren können, nachdem sie die virtuellen vSphere-Maschinen mit IaaS bereitgestellt haben.

#### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Klicken Sie auf **Hinzufügen (+)**.
- 3 Navigieren Sie in der vRealize Orchestrator-Workflow-Bibliothek zu **Orchestrator > Bibliothek > vCenter > VM-Verwaltung > Verschieben und migrieren** und wählen Sie den Workflow **Schnellmigration der virtuellen Maschine** aus.
- 4 Klicken Sie auf **Weiter**.
- 5 Wählen Sie aus dem Dropdown-Menü **Ressourcentyp** den Eintrag **IaaS VC VirtualMachine** aus.
- 6 Wählen Sie aus dem Dropdown-Menü **Eingabeparameter** den Eintrag **vm** aus.
- 7 Klicken Sie auf **Weiter**.

- 8 Übernehmen Sie den Namen der Ressourcenaktion und die Beschreibung auf der Registerkarte **Details**.
- 9 Klicken Sie auf **Weiter**.
- 10 Lassen Sie das Formular unverändert.
- 11 Klicken Sie auf **Beenden**.

Sie haben eine Ressourcenaktion erstellt, um eine virtuelle Maschine zu migrieren, und die Ressourcenaktion wird auf der Seite „Ressourcenaktionen“ aufgeführt.

#### Weiter

[Veröffentlichen der Aktion für das Migrieren einer virtuellen vSphere-Maschine](#)

#### Veröffentlichen der Aktion für das Migrieren einer virtuellen vSphere-Maschine

Um die Schnellmigration der Ressourcenaktion der virtuellen Maschine als Vorgang nach erfolgter Bereitstellung zu verwenden, müssen Sie sie veröffentlichen.

#### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Wählen Sie die Zeile der Schnellmigration der Ressourcenaktion der virtuellen Maschine aus und klicken Sie auf die Schaltfläche **Veröffentlichen**.

Sie haben einen vRealize Orchestrator-Workflow als Ressourcenaktion erstellt und veröffentlicht. Sie können zu **Administration > Katalogmanagement > Aktionen** navigieren, um die Ressourcenaktion „Schnellmigration der virtuellen Maschine“ in der Liste mit den Aktionen anzuzeigen. Der Ressourcenaktion kann ein Symbol zugewiesen werden. Siehe [Zuweisen eines Symbols zu einer Ressourcenaktion](#).

#### Weiter

Fügen Sie die Aktion den Berechtigungen hinzu, die die IaaS-bereitgestellten virtuellen vSphere-Maschinen enthalten. Siehe [Erteilen der Berechtigung für Dienste, Katalogelemente und Aktionen](#).

#### Erstellen einer XaaS -Aktion zum Migrieren einer virtuellen Maschine mit vMotion

Mithilfe von XaaS können Sie eine Ressourcenaktion erstellen und veröffentlichen, um eine IaaS-bereitgestellte virtuelle Maschine mit vMotion zu migrieren.

In diesem Szenario erstellen Sie eine Ressourcenaktion, um eine virtuelle vSphere-Maschine mit vMotion zu migrieren. Darüber hinaus bearbeiten Sie die Workflow-Präsentation mithilfe des Formulardesigners und ändern die Art und Weise, wie Verbrauchern die Aktion angezeigt wird, wenn sie diese anfordern.

#### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.

## Vorgehensweise

### 1 Erstellen einer Aktion zum Migrieren einer virtuellen vSphere-Maschine mit vMotion

Sie können eine benutzerdefinierte Ressourcenaktion erstellen, damit die Benutzer des Servicekatalogs eine virtuelle vSphere-Maschine mit vMotion migrieren können, nachdem sie die Maschine mit IaaS bereitgestellt haben.

### 2 Bearbeiten des Ressourcenaktionsformulars

Über das Formular der Ressourcenaktion wird die vRealize Orchestrator-Workflow-Präsentation zugeordnet. Sie können dieses Formular bearbeiten und definieren, was die Verbraucher der Ressourcenaktion sehen, wenn sie den Vorgang nach erfolgter Bereitstellung ausführen.

### 3 Hinzufügen eines übermittelten Aktions-Detailformulars und Speichern der Aktion

Sie können ein neues Formular zur Ressourcenaktion „Virtuelle Maschine mit vMotion migrieren“ hinzufügen, um festzulegen, was die Verbraucher sehen, nachdem sie die Ausführung des Vorgangs nach erfolgter Bereitstellung angefordert haben.

### 4 Veröffentlichen der Aktion für das Migrieren einer virtuellen Maschine mit vMotion

Um die Ressourcenaktion zum Migrieren einer virtuellen Maschine mit vMotion als Vorgang nach erfolgter Bereitstellung zu verwenden, müssen Sie sie veröffentlichen.

## Erstellen einer Aktion zum Migrieren einer virtuellen vSphere-Maschine mit vMotion

Sie können eine benutzerdefinierte Ressourcenaktion erstellen, damit die Benutzer des Servicekatalogs eine virtuelle vSphere-Maschine mit vMotion migrieren können, nachdem sie die Maschine mit IaaS bereitgestellt haben.

## Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Klicken Sie auf **Hinzufügen (+)**.
- 3 Navigieren Sie in der vRealize Orchestrator-Workflow-Bibliothek zu **Orchestrator > Bibliothek > vCenter > VM-Verwaltung > Verschieben und migrieren** und wählen Sie den Workflow **Virtuelle Maschine mit vMotion migrieren** aus.
- 4 Klicken Sie auf **Weiter**.
- 5 Wählen Sie aus dem Dropdown-Menü **Ressourcentyp** den Eintrag **IaaS VC VirtualMachine** aus.
- 6 Wählen Sie aus dem Dropdown-Menü **Eingabeparameter** den Eintrag **vm** aus.
- 7 Klicken Sie auf **Weiter**.
- 8 Übernehmen Sie den Namen der Ressourcenaktion und die Beschreibung auf der Registerkarte **Details**.
- 9 Klicken Sie auf **Weiter**.

## Weiter

[Bearbeiten des Ressourcenaktionsformulars.](#)

## Bearbeiten des Ressourcenaktionsformulars

Über das Formular der Ressourcenaktion wird die vRealize Orchestrator-Workflow-Präsentation zugeordnet. Sie können dieses Formular bearbeiten und definieren, was die Verbraucher der Ressourcenaktion sehen, wenn sie den Vorgang nach erfolgter Bereitstellung ausführen.

### Vorgehensweise

1 Klicken Sie auf das Symbol **Löschen** (✖), um das **Pool**-Element zu löschen.

2 Bearbeiten Sie das **Host**-Element.

- a Klicken Sie auf das Symbol **Bearbeiten** (✎) neben dem Feld **Host**.
- b Geben Sie **Zielhost** in das Textfeld **Bezeichnung** ein.
- c Wählen Sie aus dem Dropdown-Menü **Typ** den Eintrag **Suchen** aus.
- d Klicken Sie auf die Registerkarte **Optionen**.
- e Wählen Sie aus dem Dropdown-Menü **Erforderlich** den Eintrag **Konstante** aus und wählen Sie **Ja** aus.  
Sie haben das Feld „Host“ als „Immer erforderlich“ festgelegt.
- f Klicken Sie auf **Übernehmen**.

3 Bearbeiten Sie das **Priorität**-Element.

- a Klicken Sie auf das Symbol **Bearbeiten** (✎) neben dem Feld **Priorität**.
- b Geben Sie **Priorität der Aufgabe** in das Textfeld **Bezeichnung** ein.
- c Wählen Sie aus dem Dropdown-Menü **Typ** den Eintrag **Radio Buttons** aus.
- d Klicken Sie auf die Registerkarte **Werte** und deaktivieren Sie das Kontrollkästchen **Nicht festgelegt**.
- e Geben Sie **lowPriority** in das Suchtextfeld **Vordefinierte Werte** ein und drücken Sie die Eingabetaste.
- f Geben Sie **defaultPriority** in das Suchtextfeld **Vordefinierte Werte** ein und drücken Sie die Eingabetaste.
- g Geben Sie **highPriority** in das Suchtextfeld **Vordefinierte Werte** ein und drücken Sie die Eingabetaste.
- h Klicken Sie auf **Übernehmen**.

Wenn die Verbraucher die Ressourcenaktion anfordern, wird eine Optionsfeldgruppe mit den folgenden drei Optionsfeldern angezeigt: **lowPriority**, **defaultPriority** und **highPriority**.

4 Bearbeiten Sie das **Zustand**-Element.

- a Klicken Sie auf das Symbol **Bearbeiten** (✎) neben dem Feld **Zustand**.
- b Geben Sie **Zustand der virtuellen Maschine** in das Textfeld **Bezeichnung** ein.

- c Wählen Sie aus dem Dropdown-Menü **Typ** den Eintrag **Dropdown** aus.
- d Klicken Sie auf die Registerkarte **Werte** und deaktivieren Sie das Kontrollkästchen **Nicht festgelegt**.
- e Geben Sie **poweredOff** in das Suchtextfeld **Vordefinierte Werte** ein und drücken Sie die Eingabetaste.
- f Geben Sie **poweredOn** in das Suchtextfeld **Vordefinierte Werte** ein und drücken Sie die Eingabetaste.
- g Geben Sie **suspended** in das Suchtextfeld **Vordefinierte Werte** ein und drücken Sie die Eingabetaste.
- h Klicken Sie auf **Übernehmen**.

Wenn die Verbraucher die Ressourcenaktion anfordern, wird ein Dropdown-Menü mit den folgenden drei Optionen angezeigt: **poweredOff**, **poweredOn** und **suspended**.

Sie haben die Workflow-Präsentation des Workflows „Virtuelle Maschine mit vMotion migrieren“ bearbeitet.

## Weiter

[Hinzufügen eines übermittelten Aktions-Detailformulars und Speichern der Aktion.](#)

### Hinzufügen eines übermittelten Aktions-Detailformulars und Speichern der Aktion

Sie können ein neues Formular zur Ressourcenaktion „Virtuelle Maschine mit vMotion migrieren“ hinzufügen, um festzulegen, was die Verbraucher sehen, nachdem sie die Ausführung des Vorgangs nach erfolgter Bereitstellung angefordert haben.

#### Vorgehensweise

- 1 Klicken Sie auf das Symbol **Neues Formular** (+) neben dem Dropdown-Menü **Formular**.
- 2 Geben Sie **Übermittelte Aktion** in das Textfeld **Name** ein.
- 3 Lassen Sie das Feld **Beschreibung** leer.
- 4 Wählen Sie im Menü **Bildschirmtyp** die Option **Übermittelte Aktionsdetails** aus.
- 5 Klicken Sie auf **Übernehmen**.
- 6 Klicken Sie auf das Symbol **Bearbeiten** (✎) neben dem Dropdown-Menü **Formularseite**.
- 7 Geben Sie **Details** in das Textfeld **Überschrift** ein.
- 8 Klicken Sie auf **Übernehmen**.
- 9 Ziehen Sie das **Text**-Element aus dem Bereich „Formular“ und fügen Sie es auf der Seite **Formular** ein.
- 10 Geben Sie Folgendes ein:  
**Sie haben eine Anforderung zum Migrieren Ihrer Maschine mit vMotion übermittelt.  
 Warten Sie, bis der Vorgang erfolgreich abgeschlossen wurde.**



**11** Klicken Sie außerhalb des Textfelds, um die Änderungen zu speichern.

**12** Klicken Sie auf **Übernehmen**.

**13** Klicken Sie auf **Hinzufügen**.

Sie haben eine Ressourcenaktion erstellt, um eine virtuelle Maschine mit vMotion zu migrieren, und die Ressourcenaktion wird auf der Seite „Ressourcenaktionen“ aufgeführt.

#### Weiter

[Veröffentlichen der Aktion für das Migrieren einer virtuellen Maschine mit vMotion.](#)

#### Veröffentlichen der Aktion für das Migrieren einer virtuellen Maschine mit vMotion

Um die Ressourcenaktion zum Migrieren einer virtuellen Maschine mit vMotion als Vorgang nach erfolgter Bereitstellung zu verwenden, müssen Sie sie veröffentlichen.

#### Vorgehensweise

- 1** Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2** Wählen Sie die Zeile der Ressourcenaktion zum Migrieren einer virtuellen Maschine mit vMotion aus und klicken Sie auf die Schaltfläche **Veröffentlichen**.

Sie haben einen vRealize Orchestrator-Workflow als Ressourcenaktion erstellt und veröffentlicht. Sie können zu **Administration > Katalogmanagement > Aktionen** navigieren, um die Ressourcenaktion „Virtuelle Maschine mit vMotion migrieren“ in der Liste mit den Aktionen anzuzeigen. Der Ressourcenaktion kann ein Symbol zugewiesen werden. Siehe [Zuweisen eines Symbols zu einer Ressourcenaktion](#).

Darüber hinaus haben Sie die Präsentation des Workflows bearbeitet und das Erscheinungsbild der Aktion definiert.

#### Weiter

Business-Gruppenmanager und Mandantenadministratoren können die Ressourcenaktion „Virtuelle Maschine mit vMotion migrieren“ in eine Berechtigung einbeziehen. Weitere Informationen zum Erstellen und Veröffentlichen von IaaS-Blueprints für virtuelle Plattformen finden Sie unter [Entwerfen von Maschinen-Blueprints](#).

#### Erstellen und Veröffentlichen einer XaaS -Aktion zum Erstellen eines Snapshots

Mithilfe von XaaS können Sie eine Ressourcenaktion zum Erstellen eines Snapshots einer virtuellen vSphere-Maschine, die mit IaaS bereitgestellt wurde, erstellen und veröffentlichen.

In diesem Szenario erstellen Sie eine Ressourcenaktion zum Erstellen eines Snapshots einer virtuellen vSphere-Maschine, die mit IaaS bereitgestellt wurde. Darüber hinaus bearbeiten Sie die Workflow-Präsentation mithilfe des Formulardesigners und ändern die Art und Weise, wie Verbrauchern die Aktion angezeigt wird, wenn sie diese anfordern.

#### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.

## Vorgehensweise

### 1 Erstellen der Aktion zum Erstellen eines Snapshots einer virtuellen vSphere-Maschine

Sie können eine benutzerdefinierte Ressourcenaktion erstellen, damit die Verbraucher einen Snapshot einer virtuellen vSphere-Maschine erstellen können, nachdem sie die Maschine mit IaaS bereitgestellt haben.

### 2 Veröffentlichen der Aktion zum Erstellen eines Snapshots

Um die Ressourcenaktion „Snapshot erstellen“ als Vorgang nach erfolgter Bereitstellung zu verwenden, müssen Sie sie veröffentlichen.

## Erstellen der Aktion zum Erstellen eines Snapshots einer virtuellen vSphere-Maschine

Sie können eine benutzerdefinierte Ressourcenaktion erstellen, damit die Verbraucher einen Snapshot einer virtuellen vSphere-Maschine erstellen können, nachdem sie die Maschine mit IaaS bereitgestellt haben.

## Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Klicken Sie auf **Hinzufügen (+)**.
- 3 Navigieren Sie in der vRealize Orchestrator-Workflow-Bibliothek zu **Orchestrator > Bibliothek > vCenter > VM-Verwaltung > Snapshot** und wählen Sie den Workflow **Snapshot erstellen** aus.
- 4 Klicken Sie auf **Weiter**.
- 5 Wählen Sie aus dem Dropdown-Menü **Ressourcentyp** den Eintrag **IaaS VC VirtualMachine** aus.
- 6 Wählen Sie aus dem Dropdown-Menü **Eingabeparameter** den Eintrag **vm** aus.
- 7 Klicken Sie auf **Weiter**.
- 8 Übernehmen Sie den Namen der Ressourcenaktion und die Beschreibung auf der Registerkarte **Details**.
- 9 Klicken Sie auf **Weiter**.
- 10 Lassen Sie das Formular unverändert.
- 11 Klicken Sie auf **Hinzufügen**.

Sie haben eine Ressourcenaktion erstellt, um einen Snapshot einer virtuellen Maschine zu erstellen, und die Ressourcenaktion wird auf der Seite „Ressourcenaktionen“ aufgeführt.

## Weiter

[Veröffentlichen der Aktion zum Erstellen eines Snapshots.](#)

## Veröffentlichen der Aktion zum Erstellen eines Snapshots

Um die Ressourcenaktion „Snapshot erstellen“ als Vorgang nach erfolgter Bereitstellung zu verwenden, müssen Sie sie veröffentlichen.

## Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Wählen Sie die Zeile der Aktion „Snapshot erstellen“ aus und klicken Sie auf die Schaltfläche **Veröffentlichen**.

Sie haben einen vRealize Orchestrator-Workflow als Ressourcenaktion erstellt und veröffentlicht. Sie können zu **Administration > Katalogmanagement > Aktionen** navigieren, um die Ressourcenaktion „Snapshot erstellen“ in der Liste mit den Aktionen anzuzeigen. Der Ressourcenaktion kann ein Symbol zugewiesen werden. Siehe [Zuweisen eines Symbols zu einer Ressourcenaktion](#).

## Weiter

Business-Gruppenmanager und Mandantenadministratoren können die Ressourcenaktion „Snapshot erstellen“ in eine Berechtigung einbeziehen. Weitere Informationen zum Erstellen und Veröffentlichen von IaaS-Blueprints für virtuelle Plattformen finden Sie unter [Entwerfen von Maschinen-Blueprints](#).

## Erstellen und Veröffentlichen einer XaaS -Aktion zum Starten einer virtuellen Amazon-Maschine

Mithilfe von XaaS können Sie Aktionen zum Erweitern der Vorgänge, die Verbraucher auf von Drittanbietern bereitgestellten virtuellen Maschinen durchführen können, erstellen und veröffentlichen.

In diesem Szenario erstellen und veröffentlichen Sie eine Ressourcenaktion für den Schnellstart von virtuellen Amazon-Maschinen.

## Voraussetzungen

- Installieren Sie das vRealize Orchestrator-Plug-In für Amazon Web Services auf Ihrem standardmäßigen vRealize Orchestrator-Server.
- Erstellen oder importieren Sie einen vRealize Orchestrator-Workflow für Ressourcenzuordnungen von Amazon-Instanzen.

## Vorgehensweise

### 1 [Erstellen einer Ressourcenzuordnung für Amazon-Instanzen](#)

Sie können eine Ressourcenzuordnung erstellen, um Amazon-Instanzen, die mithilfe von IaaS bereitgestellt werden, dem vom Amazon Web Services-Plug-in verfügbar gemachten vRealize Orchestrator-Typ `AWS:EC2Instance` zuzuordnen.

### 2 [Erstellen einer Ressourcenaktion zum Starten einer virtuellen Amazon-Maschine](#)

Sie können eine Ressourcenaktion erstellen, damit die Verbraucher bereitgestellte virtuelle Amazon-Maschinen starten können.

### 3 [Veröffentlichen der Aktion für das Starten von Amazon-Instanzen](#)

Um die neu erstellte Ressourcenaktion zum Starten von Instanzen für Vorgänge nach erfolgter Bereitstellung auf virtuellen Amazon-Maschinen zu verwenden, müssen Sie sie veröffentlichen.

## Erstellen einer Ressourcenzuordnung für Amazon-Instanzen

Sie können eine Ressourcenzuordnung erstellen, um Amazon-Instanzen, die mithilfe von IaaS bereitgestellt werden, dem vom Amazon Web Services-Plug-in verfügbar gemachten vRealize Orchestrator-Typ `AWS:EC2Instance` zuzuordnen.

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.
- Erstellen oder importieren Sie einen Workflow oder eine Skriptaktion für die vRealize Orchestrator-Ressourcenzuordnung.

### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenzuordnungen** aus.
- 2 Klicken Sie auf **Hinzufügen** (+).
- 3 Geben Sie **EC2-Instanz** in das Textfeld **Name** ein.
- 4 Geben Sie **Cloud-Maschine** in das Textfeld **Katalogressourcentyp** ein.
- 5 Geben Sie **AWS:EC2Instance** in das Textfeld **Orchestrator-Typ** ein.
- 6 Wählen Sie **Immer verfügbar** aus.
- 7 Wählen Sie den zu verwendenden Ressourcenzuordnungstyp aus.
- 8 Wählen Sie in der vRealize Orchestrator-Bibliothek Ihre benutzerdefinierte Skriptaktion bzw. Ihren benutzerdefinierten Workflow für die Ressourcenzuordnung aus.
- 9 Klicken Sie auf **Hinzufügen**.

Mithilfe Ihrer Amazon-Ressourcenzuordnung können Sie Ressourcenaktionen für mithilfe von IaaS bereitgestellte Amazon-Maschinen erstellen.

### Weiter

[Erstellen einer Ressourcenaktion zum Starten einer virtuellen Amazon-Maschine.](#)

## Erstellen einer Ressourcenaktion zum Starten einer virtuellen Amazon-Maschine

Sie können eine Ressourcenaktion erstellen, damit die Verbraucher bereitgestellte virtuelle Amazon-Maschinen starten können.

### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.

### Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Klicken Sie auf **Hinzufügen** (+).

- 3 Navigieren Sie zu **Orchestrator > Bibliothek > Amazon Web Services > Elastic Cloud > Instanzen** und wählen Sie den Workflow **Instanzen starten** im Workflows-Ordner aus.
- 4 Klicken Sie auf **Weiter**.
- 5 Wählen Sie aus dem Dropdown-Menü **Ressourcentyp** den Eintrag **EC2-Instanz** aus.  
Dies ist der Name der Ressourcenzuordnung, die Sie zuvor erstellt haben.
- 6 Wählen Sie aus dem Dropdown-Menü **Eingabeparameter** den Eintrag **Instanz** aus.  
Dies ist der Eingabeparameter des Ressourcenaktionsworkflows für den Abgleich mit der Ressourcenzuordnung.
- 7 Klicken Sie auf **Weiter**.
- 8 Übernehmen Sie den Namen und die Beschreibung.  
Der Standardname der Ressourcenaktion lautet „Instanzen starten“.
- 9 Klicken Sie auf **Weiter**.
- 10 Übernehmen Sie die Felder auf der Registerkarte **Formular**.
- 11 Klicken Sie auf **Hinzufügen**.

Sie haben eine Ressourcenaktion erstellt, um virtuelle Amazon-Maschinen zu starten, und die Ressourcenaktion wird auf der Seite „Ressourcenaktionen“ aufgeführt.

## Weiter

[Veröffentlichen der Aktion für das Starten von Amazon-Instanzen.](#)

## Veröffentlichen der Aktion für das Starten von Amazon-Instanzen

Um die neu erstellte Ressourcenaktion zum Starten von Instanzen für Vorgänge nach erfolgter Bereitstellung auf virtuellen Amazon-Maschinen zu verwenden, müssen Sie sie veröffentlichen.

## Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **XaaS-Architekt** an.

## Vorgehensweise

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Wählen Sie die Zeile der Ressourcenaktion zum Starten von Instanzen aus und klicken Sie auf die Schaltfläche **Veröffentlichen**.

Der Status der Ressourcenaktion zum Starten von Instanzen ändert sich zu „Veröffentlicht“.

## Weiter

Fügen Sie die Aktion „Instanzen starten“ der Berechtigung hinzu, die das Amazon-Katalogelement enthält. Siehe [Erteilen der Berechtigung für Dienste, Katalogelemente und Aktionen](#).

## Fehlerbehebung für falsche Akzente und Sonderzeichen in XaaS -Blueprints

Wenn Sie XaaS-Blueprints für Sprachen erstellen, die Nicht-ASCII-Zeichenfolgen verwenden, werden die Akzente und Sonderzeichen als nicht verwendbare Zeichenfolgen dargestellt.

### Ursache

Eine vRealize Orchestrator-Konfigurationseigenschaft, die nicht standardmäßig festgelegt ist, kann aktiviert werden.

### Lösung

- 1 Navigieren Sie im Orchestrator-Serversystem zu `/etc/vco/app-server/`.
- 2 Öffnen Sie die Konfigurationsdatei `vmo.properties` in einem Texteditor.
- 3 Vergewissern Sie sich, dass die folgende Eigenschaft deaktiviert ist.

```
com.vmware.o11n.webview.htmlescaping.disabled
```

- 4 Speichern Sie die Datei `vmo.properties`.
- 5 Starten Sie den vRealize Orchestrator-Server neu.

## Veröffentlichen eines Blueprints

Blueprints werden im Entwurfszustand gespeichert. Sie können sie als Katalogelemente erst dann konfigurieren oder sie als Blueprint-Komponenten in der Design-Arbeitsfläche verwenden, wenn Sie sie manuell veröffentlicht haben.

Nach dem Veröffentlichen des Blueprints können Sie eine Berechtigung für ihn erteilen, um ihn für Bereitstellungsanforderungen im Servicekatalog zur Verfügung zu stellen.

Sie müssen einen Blueprint nur einmal veröffentlichen. Änderungen, die Sie an einem veröffentlichten Blueprint vornehmen, werden automatisch in den Katalog und in verschachtelte Blueprint-Komponenten übernommen.

## Veröffentlichen eines Blueprints

Sie können einen Blueprint für die Verwendung bei der Maschinenbereitstellung und optional für die Wiederverwendung in einem anderen Blueprint veröffentlichen. Um den Blueprint für die Anforderung einer Maschinenbereitstellung zu verwenden, müssen Sie dem Blueprint nach dem Veröffentlichen eine Berechtigung erteilen. Blueprints, die als Komponenten in anderen Blueprints genutzt werden, erfordern keine Berechtigung.

### Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Infrastrukturarchitekt** an.
- Erstellen Sie einen Blueprint. Siehe *Checkliste für das Erstellen von vRealize Automation-Blueprints*.

### Vorgehensweise

- 1 Klicken Sie auf die Registerkarte **Design**.
- 2 Klicken Sie auf **Blueprints**.
- 3 Zeigen Sie auf den zu veröffentlichenden Blueprint und klicken Sie auf **Veröffentlichen**.
- 4 Klicken Sie auf **OK**.

Der Blueprint wird als Katalogelement veröffentlicht. Sie müssen ihm jedoch zuerst eine Berechtigung erteilen, damit er Benutzern im Servicekatalog zur Verfügung steht.

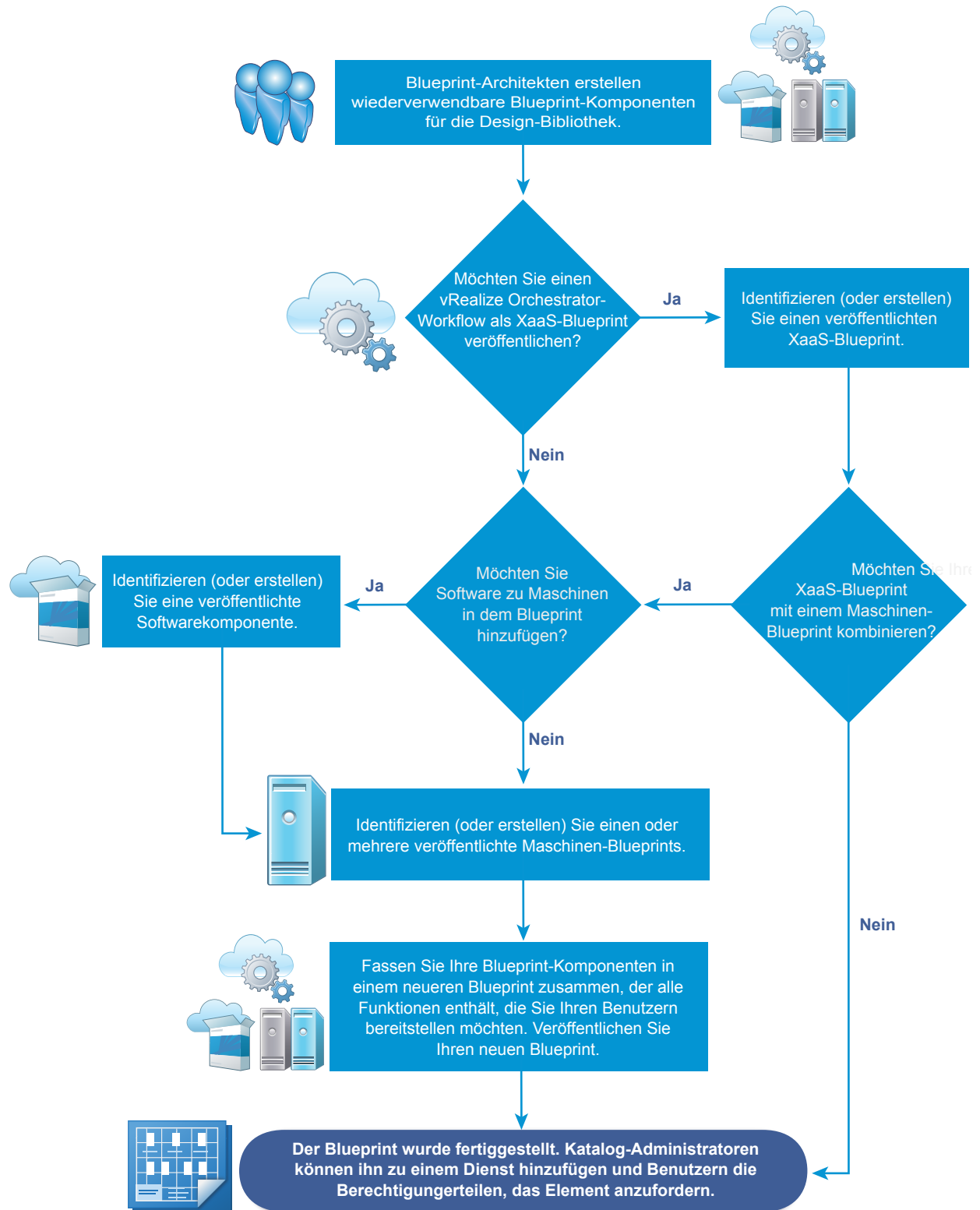
### Weiter

Fügen Sie den Blueprint dem Katalogdienst hinzu und erteilen Sie Benutzern die Berechtigung, das Katalogelement für die Maschinenbereitstellung anzufordern, wie im Blueprint definiert.

## Erstellen zusammengesetzter Blueprints

Sie können veröffentlichte Blueprints und Blueprint-Komponenten wiederverwenden und in neuer Art und Weise kombinieren, um IT-Dienstpakete zu erstellen, über die Ihren Benutzern ausgefeilte Funktionen bereitgestellt werden.

Abbildung 4-3. Workflow zum Erstellen zusammengesetzter Blueprints





- **Grundlegendes zum Verhalten von verschachtelten Blueprints**

Blueprints können wiederverwendet werden, indem Sie sie in einem anderen Blueprint als Komponente verschachteln. Blueprints verschachteln Sie zur Wiederverwendung und Modularitätskontrolle bei der Maschinenbereitstellung. Beim Arbeiten mit verschachtelten Blueprints gelten jedoch spezielle Regeln und Überlegungen.

- **Auswählen einer Maschinenkomponente, die Softwarekomponenten unterstützt**

Für die Bereitstellung von Softwarekomponenten platzieren Sie diese beim Zusammenstellen von Blueprints auf unterstützten Maschinenkomponenten.

- **Erstellen von Eigenschaftsbindungen zwischen Blueprint-Komponenten**

Bei verschiedenen Bereitstellungsszenarien ist für eine Komponente der Eigenschaftswert einer anderen Komponente erforderlich, damit sie selbst angepasst werden kann. Sie können Eigenschaften von XaaS, Maschinen und Software sowie benutzerdefinierte Eigenschaften in einem Blueprint an andere Eigenschaften binden.

- **Erstellen expliziter Abhängigkeiten und Steuern der Bereitstellungsreihenfolge**

Wenn Sie Informationen für eine Ihrer Blueprint-Komponenten benötigen, um die Bereitstellung einer anderen Komponente abzuschließen, können Sie auf der Design-Arbeitsfläche eine explizite Abhängigkeit erstellen. Auf diese Weise können Sie die Bereitstellung staffeln, damit die abhängige Komponente nicht vorzeitig bereitgestellt wird. Explizite Abhängigkeiten steuern die Bereitstellungsreihenfolge und lösen während eines vertikalen oder horizontalen Skalierungsvorgangs stets abhängige Aktualisierungen aus.

- **Szenario: Zusammenfügen und Testen eines Blueprints zur Bereitstellung von MySQL auf Rainpole-verknüpften Klon-Maschinen**

Mit Ihren Rechten als Anwendungs-, Software- oder IaaS-Architekt erstellen Sie einen Blueprint, um Ihre MySQL-Komponente mit dem CentOS-verknüpften Klon-Blueprint von vSphere zu kombinieren, den Sie erstellt haben.

## Grundlegendes zum Verhalten von verschachtelten Blueprints

Blueprints können wiederverwendet werden, indem Sie sie in einem anderen Blueprint als Komponente verschachteln. Blueprints verschachteln Sie zur Wiederverwendung und Modularitätskontrolle bei der Maschinenbereitstellung. Beim Arbeiten mit verschachtelten Blueprints gelten jedoch spezielle Regeln und Überlegungen.

Ein Blueprint, der ein oder mehrere verschachtelte Blueprints enthält, wird als äußerer Blueprint bezeichnet. Wenn Sie eine Blueprint-Komponente zur Design-Arbeitsfläche hinzufügen, während Sie einen anderen Blueprint erstellen oder bearbeiten, wird die Blueprint-Komponente als verschachtelter Blueprint bezeichnet, und der Container-Blueprint, zu dem er hinzugefügt wird, wird als äußerer Blueprint bezeichnet.

Die Verwendung von verschachtelten Blueprints bringt Überlegungen mit sich, die nicht immer offensichtlich sind. Es ist wichtig, die Regeln und Überlegungen zu verstehen, um die Möglichkeiten der Maschinenbereitstellung optimal zu nutzen.

## Allgemeine Regel und Überlegungen für das Verschachteln von Blueprints

- Als Best Practice zum Minimieren der Blueprint-Komplexität sollten Sie Blueprints nicht tiefer als drei Ebenen verschachteln, wobei der Blueprint der obersten Ebene als eine der drei Ebenen zählt.
- Wenn ein Benutzer Berechtigungen für den obersten Blueprint hat, so ist er zu allen Aspekten des Blueprints berechtigt, einschließlich verschachtelter Blueprints.
- Sie können eine Genehmigungsrichtlinie auf einen Blueprint anwenden. Nach der Genehmigung werden das Blueprint-Katalogelement und all seine Komponenten, einschließlich verschachtelter Blueprints, bereitgestellt. Sie können auch verschiedene Genehmigungsrichtlinien auf verschiedene Komponenten anwenden. Alle Genehmigungsrichtlinien müssen genehmigt werden, bevor der angeforderte Blueprint bereitgestellt wird.
- Beim Bearbeiten eines veröffentlichten Blueprints werden keine Bereitstellungen geändert, die bereits mithilfe dieses Blueprints bereitgestellt wurden. Zum Bereitstellungszeitpunkt liest die sich ergebende Bereitstellung aktuelle Werte aus dem Blueprint, einschließlich den verschachtelten Blueprints. Die einzigen Änderungen, die Sie an implementierte Bereitstellungen weitergeben können, sind Bearbeitungen von Softwarekomponenten, wie beispielsweise Bearbeitungen an Aktualisierungs- oder Deinstallationsskripts.
- Einstellungen, die Sie im äußeren Blueprint definieren, überschreiben in Ihren verschachtelten Blueprints konfigurierte Einstellungen, wobei die folgenden Ausnahmen gelten:
  - Sie können den Namen eines verschachtelten Blueprints ändern, nicht aber den Namen einer Maschinenkomponente oder einer anderen Komponente in einem verschachtelten Blueprint.
  - Sie können keine benutzerdefinierten Eigenschaften für eine Maschinenkomponente in einem verschachtelten Blueprint hinzufügen oder löschen. Sie können diese benutzerdefinierten Eigenschaften jedoch bearbeiten. Sie können keine Eigenschaftengruppen für eine Maschinenkomponente in einem verschachtelten Blueprint hinzufügen, bearbeiten oder löschen.
- Änderungen, die Sie oder ein anderer Architekt an den Einstellungen von verschachtelten Blueprints vornehmen, werden in Ihren äußeren Blueprints angezeigt, außer Sie haben diese Einstellungen im äußeren Blueprint überschrieben.
- Die Leasedauer eines verschachtelten Blueprints und des äußeren Blueprints kann auf einen beliebigen Wert festgelegt werden. Die maximale Leasedauer des äußeren Blueprints sollte aber auf den niedrigsten maximalen Leasewert eines verschachtelten Blueprints begrenzt werden. Auf diese Weise kann der Anwendungsarchitekt einen zusammengesetzten Blueprint mit einheitlichen und variablen Leasewerten entwerfen, der jedoch die durch den Infrastrukturarchitekt identifizierten Einschränkungen einhält. Wenn der für einen verschachtelten Blueprint definierte maximale Leasewert niedriger als der für den äußeren Blueprint definierte maximale Leasewert ist, schlägt die Bereitstellungsanforderung fehl.
- Bei der Arbeit an einem äußeren Blueprint können Sie die Einstellungen für die Maschineneinstellungen überschreiben, die für eine Maschinenkomponente in einem verschachtelten Blueprint konfiguriert sind.

- Bei der Arbeit an einem äußeren Blueprint können Sie eine Softwarekomponente auf eine Maschinenkomponente in einem verschachtelten Blueprint ziehen.

## Regeln und Überlegungen für das Verschachteln von Blueprints im Zusammenhang mit Netzwerken und der Sicherheit

- Alle Netzwerk- und Sicherheitskomponenten in äußeren Blueprints können Maschinen zugeordnet werden, die in verschachtelten Blueprints definiert sind.
- Wenn Anwendungsisolierung auf den äußeren Blueprint angewendet wird, überschreibt dieser die Anwendungsisolierungseinstellungen, die in verschachtelten Blueprints angegeben sind.
- Transportzoneneinstellungen, die im äußeren Blueprint definiert sind, überschreiben Transportzoneinstellungen, die in verschachtelten Blueprints angegeben werden.
- Bei der Arbeit an einem äußeren Blueprint können Sie Lastausgleichsdienst-Einstellungen relativ zu den Netzwerkkomponenteneinstellungen und Maschinenkomponenteneinstellungen konfigurieren, die in einem inneren bzw. verschachtelten Blueprint konfiguriert sind.
- Bei einem verschachtelten Blueprint, der eine On-Demand-NAT-Netzwerkkomponente enthält, können die in dieser On-Demand-NAT-Netzwerkkomponente angegebenen IP-Bereiche im äußeren Blueprint nicht bearbeitet werden.
- Der äußere Blueprint kann keinen inneren Blueprint enthalten, der Einstellungen für bedarfsgesteuerte Netzwerke oder Einstellungen für Lastenausgleich bei Bedarf enthält. Die Verwendung eines inneren Blueprints, der eine bedarfsgesteuerte NSX-Netzwerkkomponenten oder eine NSX-Lastausgleichsdienst-Komponente enthält, wird nicht unterstützt.
- Bei einem verschachtelten Blueprint, der NSX-Netzwerk- oder -Sicherheitskomponenten enthält, können Sie das Netzwerkprofil oder Sicherheitsrichtlinieninformationen, die im verschachtelten Blueprint angegeben sind, nicht ändern. Sie können diese Einstellungen aber für andere vSphere-Maschinenkomponenten wiederverwenden, die Sie dem äußeren Blueprint hinzufügen.
- Um sicherzustellen, dass NSX-Netzwerk- und -Sicherheitskomponenten in verschachtelten Blueprints in einem zusammengesetzten Blueprint eindeutig benannt werden, setzt vRealize Automation ein Präfix vor die ID des verschachtelten Blueprints für Netzwerk- und Sicherheitskomponentennamen, die nicht eindeutig sind. Wenn Sie z. B. einen Blueprint mit dem ID-Namen xbp\_1 zu einem äußeren Blueprint hinzufügen und beide Blueprints eine On-Demand-Sicherheitsgruppenkomponente mit dem Namen OD\_Security\_Group\_1 enthalten, wird die Komponente in dem verschachtelten Blueprint auf der Designarbeitsfläche des Blueprints in xbp\_1\_OD\_Security\_Group\_1 umbenannt. Die Namen von Netzwerk- und Sicherheitskomponenten im äußeren Blueprint erhalten kein Präfix.

## Überlegungen für das Verschachteln von Blueprints im Zusammenhang mit Softwarekomponenten

Für skalierbare Blueprints empfiehlt es sich, Einzel-Layer-Blueprints zu erstellen, die andere Blueprints nicht wiederverwenden. Normalerweise werden Aktualisierungsprozesse während Skalierungsvorgängen durch implizite Abhängigkeiten ausgelöst. Beispielsweise Abhängigkeiten, die Sie beim Binden einer Softwareeigenschaft an eine Maschineneigenschaft erstellen. Implizite Abhängigkeiten in einem verschach-

telten Blueprint lösen jedoch nicht immer Aktualisierungsprozesse aus. Wenn Sie verschachtelte Blueprints in einem skalierbaren Blueprint verwenden müssen, können Sie manuell Abhängigkeiten zwischen Komponenten in Ihrem verschachtelten Blueprint festlegen, um explizite Abhängigkeiten zu erstellen, die stets eine Aktualisierung auslösen.

## Auswählen einer Maschinenkomponente, die Softwarekomponenten unterstützt

Für die Bereitstellung von Softwarekomponenten platzieren Sie diese beim Zusammenstellen von Blueprints auf unterstützten Maschinenkomponenten.

Zur Unterstützung von Software-Komponenten muss der ausgewählte Maschinen-Blueprint eine Maschinenkomponente enthalten, die auf einer Vorlage, einem Snapshot oder einem Amazon-Maschinen-Image basiert, das den Guest-Agent und den Software-Bootstrap-Agent enthält, und er muss eine unterstützte Bereitstellungsmethode verwenden. Da die Software-Agents die Internetprotokollversion 6 (IPv6) nicht unterstützen, müssen Sie sicherstellen, dass die verwendeten Maschinen-Blueprints, Reservierungen und Netzwerk- und Sicherheitskomponenten für die Verwendung von IPv4 und nicht IPv6 konfiguriert sind. Wenn Sie Blueprints als skalierbar konfigurieren, empfiehlt es sich, Einzel-Layer-Blueprints zu erstellen, die andere Blueprints nicht wiederverwenden. Normalerweise werden Aktualisierungsprozesse während Skalierungsvorgängen durch implizite Abhängigkeiten ausgelöst. Beispielsweise Abhängigkeiten, die Sie beim Binden einer Softwareeigenschaft an eine Maschineneigenschaft erstellen. Implizite Abhängigkeiten in einem verschachtelten Blueprint lösen jedoch nicht immer Aktualisierungsprozesse aus.

IaaS-Architekten, Anwendungsarchitekten und Softwarearchitekten können Blueprints zusammenstellen, aber nur IaaS-Architekten können Maschinenkomponenten konfigurieren. Wenn Sie kein IaaS-Architekt sind, können Sie nicht Ihre eigenen Maschinenkomponenten konfigurieren. Sie können jedoch Maschinen-Blueprints wiederverwenden, die von Ihrem IaaS-Architekten erstellt und veröffentlicht wurden. Wenn Sie verschachtelte Blueprints in einem skalierbaren Blueprint verwenden müssen, können Sie manuell Abhängigkeiten zwischen Komponenten in Ihrem verschachtelten Blueprint festlegen, um explizite Abhängigkeiten zu erstellen, die stets eine Aktualisierung auslösen.

**Tabelle 4-47. Bereitstellungsmethoden, die Software unterstützen**

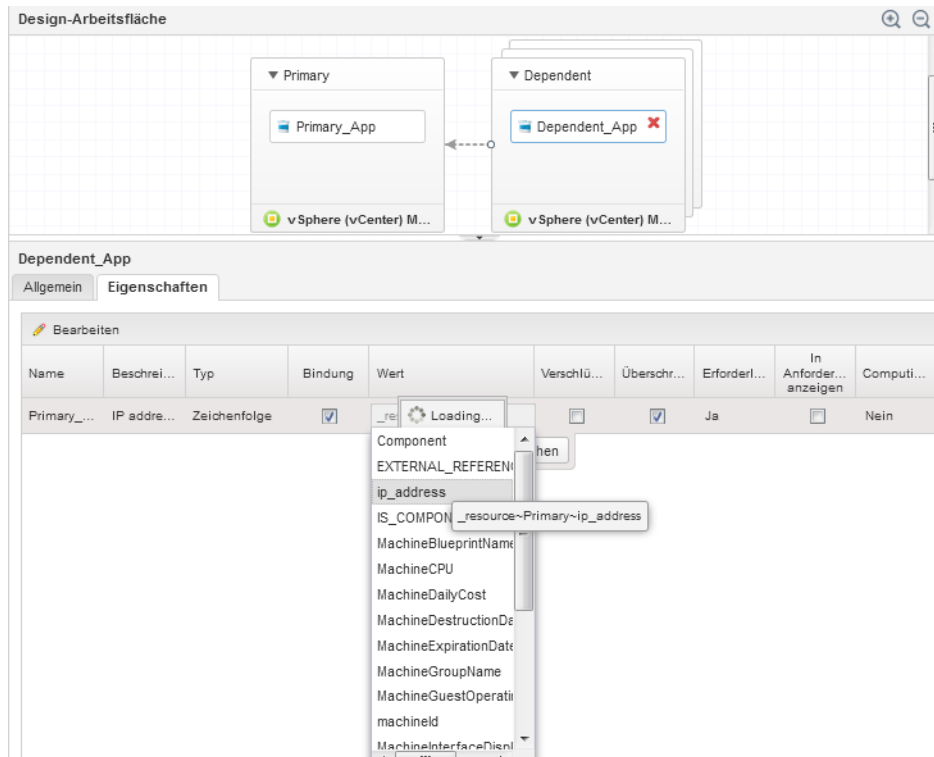
Maschinentyp	Bereitstellungsmethode
vSphere	Klonen
vSphere	Verknüpfter Klon
vCloud Director	Klonen
vCloud Air	Klonen
Amazon AWS	Amazon-Maschinen-Image

## Erstellen von Eigenschaftsbindungen zwischen Blueprint-Komponenten

Bei verschiedenen Bereitstellungsszenarien ist für eine Komponente der Eigenschaftswert einer anderen Komponente erforderlich, damit sie selbst angepasst werden kann. Sie können Eigenschaften von XaaS, Maschinen und Software sowie benutzerdefinierte Eigenschaften in einem Blueprint an andere Eigenschaften binden.

Ihr Softwarearchitekt kann beispielsweise Eigenschaftsdefinitionen in den Lebenszyklusskripts einer WAR-Komponente ändern. Eine WAR-Komponente kann den Installationsspeicherort der Apache Tomcat-Serverkomponente benötigen, damit Ihr Softwarearchitekt die WAR-Komponente so konfiguriert, dass diese den `server_home`-Eigenschaftswert auf den `install_path`-Eigenschaftswert des Apache Tomcat-Servers festlegt. Als den Blueprint zusammenfügender Architekt müssen Sie den `server_home`-Eigenschaftswert an den `install_path`-Eigenschaftswert des Apache Tomcat-Servers binden, damit die Software-Komponente erfolgreich bereitstellt.

Sie legen Eigenschaftsbindungen fest, wenn Sie Komponenten in einem Blueprint konfigurieren. Ziehen Sie auf der Seite „Blueprint“ Ihre Komponente auf die Arbeitsfläche und klicken Sie auf die Registerkarte **Eigenschaften**. Um eine Eigenschaft in einem Blueprint an eine andere Eigenschaft zu binden, aktivieren Sie das Kontrollkästchen **Binden**. Sie können `ComponentName~PropertyName` in das Textfeld „Wert“ eingeben oder mit dem Abwärtspfeil eine Liste verfügbarer Bindungsoptionen erstellen. Sie können ein Tilde-Schreibzeichen (~) als Trennzeichen zwischen Komponenten und Eigenschaften verwenden. Um beispielsweise an die `dp_port`-Eigenschaft anzubinden, können Sie in Ihrer MySQL-Softwarekomponente `mysql~db_port` eingeben. Um an Eigenschaften anzubinden, die während der Bereitstellung konfiguriert werden, wie z. B. die IP-Adresse einer Maschine oder der Hostname einer Software-Komponente, geben Sie `_resource~ComponentName~PropertyName` ein. Um beispielsweise an den Reservierungsnamen einer Maschine anzubinden, könnten Sie `_resource~vSphere_Machine_1~MachineReservationName` eingeben.

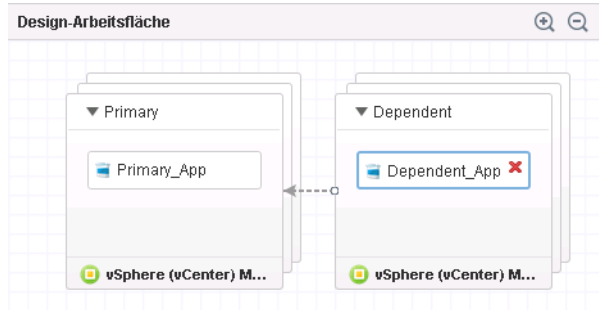
**Abbildung 4-4. Binden einer Softwareeigenschaft an die IP-Adresse einer Maschine**

## Erstellen expliziter Abhängigkeiten und Steuern der Bereitstellungsreihenfolge

Wenn Sie Informationen für eine Ihrer Blueprint-Komponenten benötigen, um die Bereitstellung einer anderen Komponente abzuschließen, können Sie auf der Design-Arbeitsfläche eine explizite Abhängigkeit erstellen. Auf diese Weise können Sie die Bereitstellung staffeln, damit die abhängige Komponente nicht vorzeitig bereitgestellt wird. Explizite Abhängigkeiten steuern die Bereitstellungsreihenfolge und lösen während eines vertikalen oder horizontalen Skalierungsvorgangs stets abhängige Aktualisierungen aus.

Wenn Sie Blueprints mit mehreren Maschinen und Anwendungen entwerfen, benötigen Sie unter Umständen Eigenschaften von einer Maschine, um eine Installation auf einer anderen Maschine abzuschließen. Wenn Sie beispielsweise einen Webserver erstellen, benötigen Sie unter Umständen den Hostnamen des Datenbankservers, bevor Sie die Anwendung installieren und Datenbanktabellen instanziiieren können. Wenn Sie eine explizite Abhängigkeit zuordnen, beginnt Ihr Datenbankserver mit der Bereitstellung, sobald Ihr Webserver die Bereitstellung abgeschlossen hat.

Um eine Abhängigkeit auf der Blueprint-Arbeitsfläche zuzuordnen, ziehen Sie eine Linie von der abhängigen Komponente zu der Komponente, von der Sie abhängig sind. Wenn Sie damit fertig sind, weist die als Zweites zu erstellende Komponente einen Pfeil auf, der auf die Komponente zeigt, die zuerst erstellt werden soll. In der Abbildung „Steuern der Buildreihenfolge durch Zuordnen von Abhängigkeiten“ wird die abhängige Maschine erst bereitgestellt, wenn die primäre Maschine erstellt ist. Alternativ können Sie beide Maschinen für die gleichzeitige Bereitstellung konfigurieren und eine Abhängigkeit zwischen den Softwarekomponenten zeichnen.

**Abbildung 4-5. Steuern der Buildreihenfolge durch Zuordnen von Abhängigkeiten**

Wenn Sie Blueprints als skalierbar konfigurieren, empfiehlt es sich, Einzel-Layer-Blueprints zu erstellen, die andere Blueprints nicht wiederverwenden. Normalerweise werden Aktualisierungsprozesse während Skalierungsvorgängen durch implizite Abhängigkeiten ausgelöst. Beispielsweise Abhängigkeiten, die Sie beim Binden einer Softwareeigenschaft an eine Maschineneigenschaft erstellen. Implizite Abhängigkeiten in einem verschachtelten Blueprint lösen jedoch nicht immer Aktualisierungsprozesse aus. Wenn Sie verschachtelte Blueprints in einem skalierbaren Blueprint verwenden müssen, können Sie manuell Abhängigkeiten zwischen Komponenten in Ihrem verschachtelten Blueprint festlegen, um explizite Abhängigkeiten zu erstellen, die stets eine Aktualisierung auslösen.

## Szenario: Zusammenfügen und Testen eines Blueprints zur Bereitstellung von MySQL auf Rainpole-verknüpften Klon-Maschinen

Mit Ihren Rechten als Anwendungs-, Software- oder IaaS-Architekt erstellen Sie einen Blueprint, um Ihre MySQL-Komponente mit dem CentOS-verknüpften Klon-Blueprint von vSphere zu kombinieren, den Sie erstellt haben.



### Voraussetzungen

- Erstellen Sie eine Softwarekomponente, um MySQL auf Linux-Maschinen zu installieren. Siehe [Szenario: Erstellen einer MySQL-Softwarekomponente für Rainpole](#).
- Melden Sie sich bei der vRealize Automation-Konsole als Mitglied der benutzerdefinierten Gruppe der Rainpole-Architekten an. Siehe [Szenario: Erstellen einer benutzerdefinierten Gruppe für Ihre Rainpole-Architekten](#).

## Vorgehensweise

### 1 Szenario: Erstellen eines Containers für Ihren Blueprint „MySQL unter CentOS“ für Rainpole

Erstellen Sie unter Verwendung Ihrer IaaS-, Software- oder Anwendungsarchitekten-Berechtigungen einen Blueprint-Container und konfigurieren Sie den Namen, die Beschreibung und den eindeutigen Bezeichner für Ihren vSphere-Blueprint „MySQL unter CentOS“.

### 2 Szenario: Hinzufügen von Software und einer Maschine zum Blueprint „MySQL unter CentOS“ für Rainpole

Mit Ihren Rechten als IaaS-, Software- oder Anwendungsarchitekt ziehen Sie den veröffentlichten Maschinen-Blueprint „CentOS für Softwaretests“ in Ihre Arbeitsfläche, um diesen Blueprint als Ihre Maschine wiederzuverwenden. Sie ziehen Ihre veröffentlichte Softwarekomponente auf die virtuelle Maschine und konfigurieren die Software-Eigenschaften, die Sie in der Software-Komponente angegeben haben.

### 3 Szenario: Hinzufügen von CentOS mit dem MySQL-Katalogelement zum Rainpole-Dienst

Mit Ihren Mandantenadministratorrechten fügen Sie Ihren neuen Blueprint zum Rainpole-Katalogdienst hinzu, sodass Sie Ihre Arbeit überprüfen können.

### 4 Szenario: Bereitstellen des CentOS mit dem MySQL-Katalogelement für Rainpole

Fordern Sie das Servicekatalogelement mit dem Testbenutzerkonto an, um eine CentOS-Maschine mit MySQL bereitzustellen.

## Szenario: Erstellen eines Containers für Ihren Blueprint „MySQL unter CentOS“ für Rainpole

Erstellen Sie unter Verwendung Ihrer IaaS-, Software- oder Anwendungsarchitekten-Berechtigungen einen Blueprint-Container und konfigurieren Sie den Namen, die Beschreibung und den eindeutigen Bezeichner für Ihren vSphere-Blueprint „MySQL unter CentOS“.

## Vorgehensweise

- 1 Wählen Sie **Design > Blueprints** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Geben Sie **MySQL unter CentOS** in das Textfeld **Name** ein.
- 4 Überprüfen Sie den generierten eindeutigen Bezeichner.

Das Feld „Bezeichner“ wird automatisch basierend auf dem von Ihnen eingegebenen Namen aufgefüllt. Sie können dieses Feld jetzt bearbeiten, aber nach der Speicherung des Blueprints kann es nicht mehr geändert werden. Bezeichner sind innerhalb Ihres Mandanten permanent und eindeutig, weshalb Sie damit programmgesteuert mit Blueprints interagieren und Eigenschaftsbindungen erstellen können.

- 5 Geben Sie **MySQL-Software auf vSphere CentOS-Maschine** in das Textfeld **Beschreibung** ein.



- 6 Konfigurieren Sie einen Lease-Bereich, aus dem Benutzer auswählen können, indem Sie **1** in das Textfeld **Minimum** und **7** in das Textfeld **Maximum** eingeben.

Benutzer haben die Möglichkeit, ihre angeforderten Maschinen für bis zu 7 Tage zu leasen, bevor sie ihre Leases verlängern müssen oder bevor ihre Maschinen gelöscht werden.

- 7 Klicken Sie auf **OK**.

#### Weiter

Ziehen Sie die MySQL-Komponente und das veröffentlichte CentOS für den Software-Maschinen-Blueprint in die Arbeitsfläche.

### Szenario: Hinzufügen von Software und einer Maschine zum Blueprint „MySQL unter CentOS“ für Rainpole

Mit Ihren Rechten als IaaS-, Software- oder Anwendungsarchitekt ziehen Sie den veröffentlichten Maschinen-Blueprint „CentOS für Softwaretests“ in Ihre Arbeitsfläche, um diesen Blueprint als Ihre Maschine wiederzuverwenden. Sie ziehen Ihre veröffentlichte Softwarekomponente auf die virtuelle Maschine und konfigurieren die Software-Eigenschaften, die Sie in der Software-Komponente angegeben haben.

#### Vorgehensweise

- 1 Klicken Sie in der Liste „Kategorien“ auf „Blueprints“.
- 2 Ziehen Sie **CentOS für Softwaretests** auf die Arbeitsfläche.
- 3 Klicken Sie in der Liste „Kategorien“ auf **Softwarekomponenten**.
- 4 Ziehen Sie **MySQL für virtuelle Linux-Maschinen** auf die vSphere-Maschine.
- 5 Klicken Sie auf die Registerkarte **Eigenschaften**.
- 6 Aktualisieren Sie die db\_port-Eigenschaft für diesen Blueprint.
  - a Wählen Sie die db\_port-Eigenschaft aus und klicken Sie auf **Bearbeiten**.
  - b Geben Sie im Textfeld **Wert** den Wert **3308** ein.

Wenn ein Servicekatalogbenutzer das Element anfordert, ist 3308 der Standardwert.
  - c Klicken Sie auf **OK**.
- 7 Klicken Sie auf **Beenden**.
- 8 Wählen Sie die Zeile aus, die „CentOS mit MySQL“ enthält, und klicken Sie auf **Veröffentlichen**.

Sie haben einen Blueprint veröffentlicht, der die CentOS-Maschinen- und MySQL-Softwarekomponente enthält.

### Szenario: Hinzufügen von CentOS mit dem MySQL-Katalogelement zum Rainpole-Dienst

Mit Ihren Mandantenadministratorrechten fügen Sie Ihren neuen Blueprint zum Rainpole-Katalogdienst hinzu, sodass Sie Ihre Arbeit überprüfen können.

**Vorgehensweise**

- 1 Wählen Sie **Administration > Katalogmanagement > Services** aus.
- 2 Wählen Sie die Zeile für den Rainpole-Katalogdienst in der Liste **Dienste** aus und klicken Sie auf **Katalogelemente verwalten**.
- 3 Klicken Sie auf das Symbol **Neu (+)**.
- 4 Wählen Sie **CentOS mit MySQL** aus.

Nur veröffentlichte Blueprints und Komponenten, die noch keinem Dienst zugewiesen sind, werden in der Liste angezeigt. Wenn der Blueprint nicht angezeigt wird, stellen Sie sicher, dass er veröffentlicht wurde oder dass er nicht Bestandteil eines anderen Diensts ist.

- 5 Klicken Sie auf **OK**.
- 6 Klicken Sie auf **Schließen**.

Sie können jetzt CentOS mit dem MySQL-Katalogelement anfordern. Sie müssen keine Berechtigung für das neue Katalogelement erteilen, da Sie eine Berechtigung für Ihre Rainpole-Business-Gruppe für den gesamten Rainpole-Dienst erteilt haben.

**Weiter**

Fordern Sie CentOS mit dem MySQL-Katalogelement an, um Ihre Arbeit zu überprüfen.

**Szenario: Bereitstellen des CentOS mit dem MySQL-Katalogelement für Rainpole**

Fordern Sie das Servicekatalogelement mit dem Testbenutzerkonto an, um eine CentOS-Maschine mit MySQL bereitzustellen.

**Vorgehensweise**

- 1 Melden Sie sich bei der vRealize Automation-Konsole ab.
- 2 Melden Sie sich erneut mit dem Benutzernamen **test\_user** und dem Kennwort **VMware1!** an.
- 3 Klicken Sie auf die Registerkarte **Katalog**.
- 4 Klicken Sie auf die Schaltfläche **Anforderung**, um ein Katalogelement anzufordern.
- 5 Geben Sie **Funktionalität überprüfen** in das Textfeld **Beschreibung** ein.
- 6 Klicken Sie auf **Einreichen**, um das Katalogelement anzufordern.
- 7 Klicken Sie auf die Registerkarte **Anforderungen**, um den Status Ihrer Anforderung zu überwachen.

Nach erfolgreicher Bereitstellung der Maschine wird die Statusmeldung **Erfolgreich** angezeigt.

**Weiter**

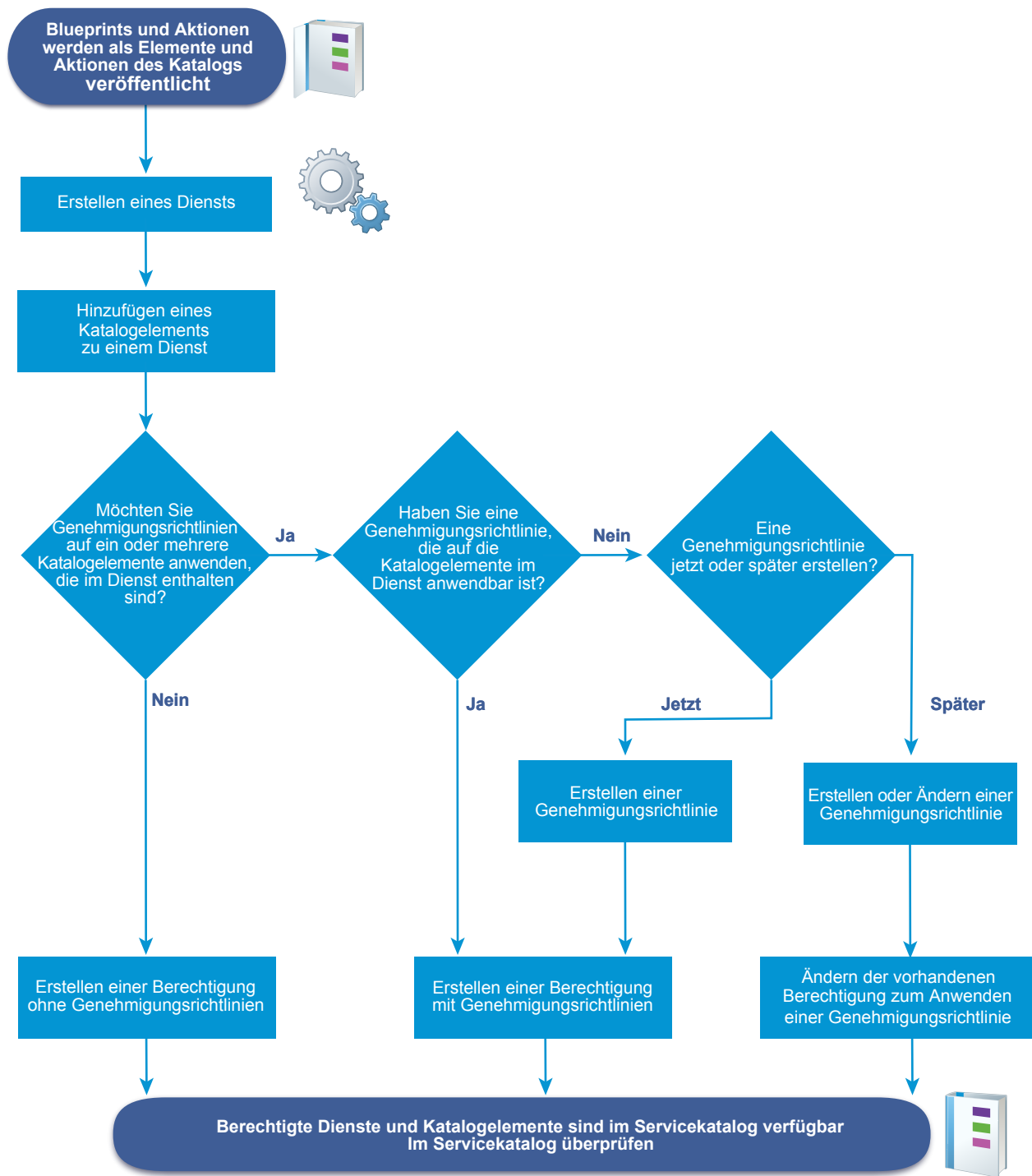
- Planen Sie die Installation einer Produktionsumgebung. Siehe *Referenzarchitektur*.

- Mehr über weitere Optionen zum Konfigurieren von vRealize Automation, zum Entwerfen und Exportieren von Blueprints und zum Verwalten Ihres Servicekatalogs. Siehe *Konfigurieren von vRealize Automation*.

## Verwalten des Servicekatalogs

Der Servicekatalog ist der Bereich, in dem Ihre Kunden Maschinen und andere Elemente für die Bereitstellung für ihre Nutzung anfordern. Sie verwalten den Benutzerzugriff auf die Servicekatalogelemente basierend darauf, wie Sie Services erstellen, Benutzern für mindestens ein Element Berechtigungen erteilen und Kontrolle anwenden.

Der Workflow zum Hinzufügen von Elementen zum Servicekatalog hängt davon ab, ob Sie Genehmigungsrichtlinien erstellen und anwenden.



## Checkliste für die Konfiguration des Servicekatalogs

Nachdem Sie Blueprints und Aktionen erstellt und veröffentlicht haben, können Sie einen vRealize Automation-Dienst erstellen, Katalogelemente konfigurieren und Berechtigungen und Genehmigungen zuweisen.

Die Checkliste für die Konfiguration des Servicekatalogs bietet eine allgemeine Übersicht über die Schritte, die für die Konfiguration von Katalogen erforderlich sind, und zeigt für jeden Schritt zu treffende Entscheidungen und detaillierte Anweisungen auf.

**Tabelle 4-48. Konfigurieren der Checkliste für den Servicekatalog**

Aufgabe	Erforderliche Rolle	Details
<input type="checkbox"/> Hinzufügen eines Diensts.	Mandantenadministrator oder Katalogadministrator	Siehe <a href="#">Hinzufügen eines Diensts</a> .
<input type="checkbox"/> Hinzufügen eines Katalogelements zu einem Dienst.	Mandantenadministrator oder Katalogadministrator	Siehe <a href="#">Hinzufügen von Katalogelementen zu einem Dienst</a> .
<input type="checkbox"/> Konfigurieren des Katalogelements im Dienst.	Mandantenadministrator oder Katalogadministrator	Siehe <a href="#">Konfigurieren eines Katalogelements</a> .
<input type="checkbox"/> Erstellen und Anwenden von Berechtigungen für das Katalogelement.	Mandantenadministrator oder Business-Gruppenmanager	Siehe <a href="#">Erteilen der Berechtigung für Dienste, Katalogelemente und Aktionen</a> .
<input type="checkbox"/> Erstellen und Anwenden von Genehmigungsrichtlinien für das Katalogelement.	Der Mandantenadministrator oder Genehmigungsadministrator kann Genehmigungsrichtlinien erstellen.  Der Mandantenadministrator oder Business-Gruppenmanager kann Genehmigungsrichtlinien anwenden.	Siehe <a href="#">Erstellen einer Genehmigungsrichtlinie</a> .

## Erstellen eines Diensts

Bei einem Dienst handelt es sich um eine Gruppe von Katalogelementen, die dem Servicekatalog hinzugefügt werden sollen. Sie können Berechtigungen für den Dienst erteilen, wodurch Business-Gruppenbenutzern die Berechtigung für alle zugehörigen Katalogelemente erteilt wird, und Sie können eine Genehmigungsrichtlinie auf den Dienst anwenden.

Ein Dienst fungiert als dynamische Gruppe von Katalogelementen. Wenn Sie Berechtigungen für einen Dienst erteilen, sind alle Katalogelemente des Diensts für die angegebenen Benutzer im Servicekatalog verfügbar, und alle Katalogelemente, die Sie in einem Dienst hinzufügen oder entfernen, werden im Servicekatalog entsprechend aktualisiert.

Den erstellten Dienst können Sie als Dienstkategorie verwenden, um Dienstangebote für Ihre Servicekatalogbenutzer zusammenzustellen. Beispielsweise einen Windows-Desktopdienst, der Katalogelemente für die Betriebssysteme Windows 7, 8 und 10 beinhaltet, oder einen Linux-Dienst, der CentOS- und RHEL-Betriebssystemelemente beinhaltet.

## Hinzufügen eines Diensts

Fügen Sie einen Dienst hinzu, um Katalogelemente für Ihre Benutzer von Servicekatalogen verfügbar zu machen. Alle Katalogelemente müssen einem Dienst zugeordnet sein, damit Sie Benutzern die Berechtigung für die Elemente erteilen können.

Wenn Benutzern die Berechtigung für den Dienst erteilt ist, werden die Katalogelemente gemeinsam im Servicekatalog angezeigt. Sie können Benutzern auch die Berechtigung für einzelne Katalogelemente erteilen.

### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **Katalogadministrator** an.

### Vorgehensweise

1 Wählen Sie **Administration > Katalogmanagement > Services** aus.

2 Klicken Sie auf das Symbol **Neu** (+).

3 Geben Sie einen Namen und eine Beschreibung ein.

Diese Werte werden im Servicekatalog für die Katalogbenutzer angezeigt.

4 Um ein bestimmtes Symbol für den Dienst im Servicekatalog hinzuzufügen, klicken Sie auf **Durchsuchen** und wählen ein Bild aus.

Die Bilddateitypen GIF, JPG und PNG werden unterstützt. Das angezeigte Bild weist 40 x 40 Pixel auf. Wenn Sie kein benutzerdefiniertes Bild auswählen, wird das Standardsymbol im Servicekatalog angezeigt.

5 Wählen Sie aus dem Dropdown-Menü **Status** einen Status aus.

Option	Beschreibung
<b>Inaktiv</b>	Der Dienst ist im Servicekatalog nicht verfügbar. Wenn sich ein Dienst in diesem Status befindet, können Sie dem Dienst Katalogelemente zuordnen, aber Sie können Benutzern nicht die Berechtigung für den Dienst erteilen. Wenn Sie <b>Inaktiv</b> für einen Dienst auswählen, der aktiv und berechtigt ist, wird dieser aus dem Servicekatalog entfernt, bis Sie ihn erneut aktivieren.
<b>Aktiv</b>	(Standard) Für den Dienst und die zugehörigen Katalogelemente kann Benutzern die Berechtigung erteilt werden und sie sind dann im Servicekatalog für diese Benutzer verfügbar.
<b>Gelöscht</b>	Entfernt den Dienst aus vRealize Automation. Alle zugehörigen Katalogelemente sind weiterhin vorhanden, aber alle dem Dienst im Servicekatalog zugeordneten Elemente sind für die Katalogbenutzer nicht verfügbar.

## 6 Konfigurieren der Diensteseinstellungen

Die folgenden Einstellungen liefern Informationen zu den Servicekatalogbenutzern. Diese Einstellungen haben keine Auswirkung auf die Dienstverfügbarkeit.

Option	Beschreibung
<b>Stunden</b>	Konfigurieren Sie die Zeit, in der das Support-Team verfügbar ist. Die Zeitangabe basiert auf der lokalen Uhrzeit.  Die Servicestunden dürfen sich nicht über mehrere Tage erstrecken. Beispielsweise können Sie nicht 16:00 Uhr bis 04:00 Uhr als Servicestunden festlegen. Bei Servicestunden, die über Mitternacht hinausgehen, müssen zwei Berechtigungen erstellt werden. Eine Berechtigung für die Zeit von 16:00 Uhr bis 00:00 Uhr sowie eine für die Zeit von 00:00 Uhr bis 04:00 Uhr.
<b>Besitzer</b>	Geben Sie den Benutzer oder die Benutzergruppe an, der bzw. die der primäre Besitzer des Diensts und der zugehörigen Katalogelemente ist.
<b>Support-Team</b>	Geben Sie die benutzerdefinierte Benutzergruppe oder den benutzerdefinierten Benutzer an, die bzw. der für den Support von Problemen verfügbar ist, die Servicekatalogbenutzer bei der Bereitstellung von Elementen mithilfe dieses Diensts haben.
<b>Änderungsfenster</b>	Wählen Sie das Datum und die Uhrzeit für eine geplante Änderung des Diensts aus. Diese Zeitangabe dient zu Informationszwecken und hat keine Auswirkungen auf die Verfügbarkeit des Diensts.

## 7 Klicken Sie auf **Hinzufügen**.

### Weiter

Ordnen Sie Katalogelemente einem Dienst zu, damit Sie Benutzern die Berechtigung für die Elemente erteilen können. Siehe [Hinzufügen von Katalogelementen zu einem Dienst](#).

## Hinzufügen von Katalogelementen zu einem Dienst

Fügen Sie Katalogelemente zu Diensten hinzu, um Benutzern die Berechtigung zum Anfordern der Elemente im Servicekatalog zu erteilen. Ein Katalogelement kann nur einem Dienst zugeordnet werden.

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **Katalogadministrator** an.
- Vergewissern Sie sich, dass ein Dienst vorhanden ist. Siehe [Hinzufügen eines Diensts](#).
- Vergewissern Sie sich, dass mindestens ein Katalogelement veröffentlicht wurde. Siehe [Konfigurieren eines Katalogelements](#).

### Vorgehensweise

- 1 Wählen Sie **Administration > Katalogmanagement > Services** aus.
- 2 Wählen Sie den Dienst aus, dem Sie Katalogelemente hinzufügen, und klicken Sie auf **Katalogelemente verwalten**.

### 3 Klicken Sie auf das Symbol **Katalogelemente** (+).

- a Wählen Sie die Katalogelemente aus, die in diesen Dienst aufgenommen werden sollen.

Im Dialogfeld „Katalogelemente auswählen“ werden nur die Elemente angezeigt, die noch keinem Dienst zugeordnet sind.

- b Klicken Sie auf **Hinzufügen**.

### 4 Klicken Sie auf **Schließen**.

#### Weiter

- Sie können dem Katalogelement ein benutzerdefiniertes Symbol hinzufügen, das zusammen mit dem Katalogelement im Servicekatalog angezeigt wird. Siehe [Konfigurieren eines Katalogelements](#).
- Erteilen Sie Benutzern die Berechtigung für die Dienste oder Katalogelemente, damit sie diese im Servicekatalog anfordern können. Siehe [Erstellen von Berechtigungen](#).

## Arbeiten mit Katalogelementen und Aktionen

Katalogelemente sind veröffentlichte Blueprints für Maschinen, Softwarekomponenten und andere Objekte. Aktionen im Katalogverwaltungsbereich sind veröffentlichte Aktionen, die Sie für die bereitgestellten Katalogelemente ausführen können. Sie können diese Liste verwenden, um festzulegen, welche Blueprints und Aktionen veröffentlicht werden, sodass Sie sie Nutzern des Dienstkatalogs zur Verfügung stellen können.

### Veröffentlichte Katalogelemente

Bei einem Katalogelement handelt es sich um einen veröffentlichten Blueprint. Veröffentlichte Blueprints können auch in anderen Blueprints verwendet werden. Die Wiederverwendung von Blueprints in anderen Blueprints wird in der Katalogelementliste nicht angezeigt.

Die veröffentlichten Katalogelemente können auch Elemente umfassen, die nur Komponenten von Blueprints sind. So werden veröffentlichte Softwarekomponenten beispielsweise als Katalogelemente aufgelistet, sie sind jedoch nur als Teil einer Bereitstellung verfügbar.

Bereitstellungskatalogelemente müssen einem Dienst zugeordnet sein, sodass Sie sie berechtigten Nutzern des Dienstkatalogs zur Verfügung stellen können. Nur aktive Elemente werden im Dienstkatalog angezeigt. Sie können Katalogelemente für einen anderen Dienst konfigurieren, sie zum vorübergehenden Entfernen aus dem Dienstkatalog deaktivieren sowie ein benutzerdefiniertes Symbol hinzufügen, das im Katalog angezeigt wird.

### Veröffentlichte Aktionen

Aktionen sind Änderungen, die Sie an bereitgestellten Katalogelementen vornehmen können. Sie können beispielsweise eine virtuelle Maschine neu starten.

Aktionen können integrierte Aktionen oder mithilfe von XaaS erstellte Aktionen enthalten. Integrierte Aktionen werden hinzugefügt, wenn Sie eine Maschine oder einen anderen bereitgestellten Blueprint hinzufügen. XaaS-Aktionen müssen erstellt und veröffentlicht werden.



Aktionen können nicht Diensten zugeordnet werden. Sie müssen eine Aktion in die Berechtigung einschließen, die das Katalogelement enthält, für das die Aktion ausgeführt wird. Aktionen, die Nutzern gewährt werden, werden im Dienstkatalog nicht angezeigt. Die Aktionen stehen für das bereitgestellte Element auf der Registerkarte **Elemente** des Benutzers des Dienstkatalogs bereit, je nachdem, ob sie auf das Element anwendbar sind und wie der aktuelle Status des Elements lautet.

Sie können ein benutzerdefiniertes Symbol zu der Aktion hinzufügen, die auf der Registerkarte **Elemente** angezeigt wird.

## Konfigurieren eines Katalogelements

Ein Katalogelement ist ein veröffentlichter Blueprint, für den Benutzern Berechtigungen erteilt werden können. Die Optionen der Katalogelemente dienen zum Ändern des Status oder zugehörigen Dienstes. Außerdem können Sie die Berechtigungen anzeigen, die das ausgewählte Katalogelement enthalten.

Im Servicekatalog werden nur Katalogelemente angezeigt, die einem Dienst zugeordnet sind und für die den Benutzern die entsprechende Berechtigung erteilt wurde. Katalogelemente können nur einem Dienst zugeordnet werden.

Wenn Sie nicht möchten, dass ein Katalogelement im Servicekatalog angezeigt wird, es aber weder aus einer Berechtigung noch aus der Liste der veröffentlichten Katalogelemente entfernen möchten, können Sie es deaktivieren. Der Status eines deaktivierten Katalogelements lautet „Zurückgezogen“ im Raster und „Inaktiv“ in den Konfigurationsdetails. Sie können das Element zu einem späteren Zeitpunkt aktivieren.

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **Katalogadministrator** an.
- Stellen Sie sicher, dass Sie mindestens ein als Katalogelement veröffentlichter Blueprint vorhanden ist. Siehe [Veröffentlichen eines Blueprints](#).

### Vorgehensweise

- 1 Wählen Sie **Administration > Katalogmanagement > Katalogelemente** aus.
- 2 Wählen Sie das Katalogelement aus und klicken Sie auf **Konfigurieren**.

### 3 Konfigurieren Sie die Einstellungen des Katalogelements.

Option	Beschreibung
<b>Symbol</b>	Suchen Sie nach einem Bild. Die Bilddateitypen GIF, JPG und PNG werden unterstützt. Das angezeigte Bild weist 40 x 40 Pixel auf. Wenn Sie kein benutzerdefiniertes Bild auswählen, wird das Standardkatalogsymbol im Servicekatalog angezeigt.
<b>Status</b>	<p>Mögliche Werte sind <b>Aktiv</b>, <b>Inaktiv</b> und <b>Staging</b>.</p> <ul style="list-style-type: none"> <li>■ <b>Aktiv</b>. Das Katalogelement wird im Dienstkatalog angezeigt und die berechtigten Benutzer können es zur Bereitstellung von Ressourcen verwenden. Das Element wird in der Liste der Katalogelemente als veröffentlicht angezeigt.</li> <li>■ <b>Inaktiv</b>. Das Katalogelement ist im Servicekatalog nicht verfügbar. Das Element wird in der Liste der Katalogelemente als zurückgezogen angezeigt.</li> <li>■ <b>Staging</b>. Das Katalogelement ist im Servicekatalog nicht verfügbar. Wählen Sie dieses Menüelement aus, wenn das Element einmal inaktiv war und Sie Staging verwenden, um anzugeben, dass Sie es möglicherweise erneut aktivieren möchten. Wird in der Liste der Katalogelemente als „Staging“ angezeigt.</li> </ul>
<b>Dienst</b>	Auswählen eines Dienstes. Alle Katalogelemente müssen einem Dienst zugeordnet sein, wenn dieser berechtigten Benutzern im Servicekatalog angezeigt werden soll. Die Liste beinhaltet aktive und inaktive Dienste.
<b>Neu und interessant</b>	Das Katalogelement wird auf der Startseite im Bereich „Neu und interessant“ angezeigt.

4 Klicken Sie zum Anzeigen der Berechtigungen, bei denen das Katalogelement den Benutzern zur Verfügung gestellt wird, auf die Registerkarte **Berechtigungen**.

5 Klicken Sie auf **Aktualisieren**.

#### Weiter

- Um das Katalogelement im Servicekatalog verfügbar zu machen, müssen Sie Benutzern die Berechtigung für den dem Element zugeordneten Dienst oder für das einzelne Element erteilen. Siehe [Erstellen von Berechtigungen](#).
- Um die Reihenfolge für die Verarbeitung der Berechtigungen anzugeben, damit die Genehmigungsrichtlinien für einzelne Benutzer richtig angewendet werden, müssen Sie die Prioritätsreihenfolge für mehrfache Berechtigungen für dieselbe Business-Gruppe festlegen. Siehe [Priorisieren von Berechtigungen](#).

### Konfigurieren einer Aktion für den Servicekatalog

Bei einer Aktion handelt es sich um eine Änderung oder einen Workflow, die bzw. der auf bereitgestellten Elementen ausgeführt werden kann. Sie können ein Symbol hinzufügen oder die Berechtigungen anzeigen, die die ausgewählte Aktion enthalten.

Eine Aktion ist entweder eine integrierte Aktion für eine bereitgestellte Maschine, ein Netzwerk oder andere Blueprint-Komponenten, oder sie ist eine veröffentlichte XaaS-Aktion.

Bei dem Symbol werden die Bilddateitypen GIF, JPG und PNG unterstützt. Das angezeigte Bild weist 40 x 40 Pixel auf. Wenn Sie kein benutzerdefiniertes Bild auswählen, wird das Standardsymbol für Aktionen auf der Registerkarte **Elemente** angezeigt.

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **Katalogadministrator** an.
- Stellen Sie sicher, dass Sie über mindestens eine veröffentlichte Aktion verfügen. Siehe [Veröffentlichen eines Blueprints](#) und [Veröffentlichen einer Ressourcenaktion](#).

### Vorgehensweise

- 1 Wählen Sie **Administration > Katalogmanagement > Aktionen** aus.
- 2 Wählen Sie die freigegebene Aktion aus und klicken Sie auf **Details anzeigen**.
- 3 Suchen Sie nach einem Bild.
- 4 Klicken Sie zum Anzeigen der Berechtigungen, bei denen die Aktion den Benutzern zur Verfügung gestellt wird, auf die Registerkarte **Berechtigungen**.
- 5 Klicken Sie auf **Aktualisieren**.

### Weiter

[Erteilen der Berechtigung für Dienste, Katalogelemente und Aktionen.](#)

## Erstellen von Berechtigungen

Berechtigungen bestimmen, welche Elemente und Aktionen im Servicekatalog für die Mitglieder der ausgewählten Business-Gruppe verfügbar sind. Eine Berechtigung muss aktiv sein, damit die Elemente im Servicekatalog angezeigt werden. Wenn Elemente kontrolliert werden müssen, können Sie mithilfe von Berechtigungen Genehmigungsrichtlinien auf verschiedene Elemente anwenden.

Zum Konfigurieren der Berechtigung müssen die Katalogelemente in einem Dienst enthalten sein. Berechtigungen können mehrere Dienste, Katalogelemente aus Diensten, die in anderen Berechtigungen enthalten sind, und Aktionen umfassen, die Sie in den bereitgestellten Katalogelementen ausführen können.

### Grundlegendes zur Interaktion von Berechtigungsoptionen

Die Art, wie Sie eine Berechtigung konfigurieren, bestimmt, was im Servicekatalog angezeigt wird. Die Interaktion von Diensten, Katalogelementen und Komponenten, Aktionen und Genehmigungsrichtlinien hat Auswirkungen darauf, was ein Benutzer des Servicekatalogs anfordern kann und wie Genehmigungsrichtlinien angewendet werden.

Beim Erstellen einer Berechtigung müssen Sie die Interaktion von Diensten, Katalogelementen, Aktionen und Genehmigungen berücksichtigen.

- **Dienste in Berechtigungen**

Ein berechtigter Dienst fungiert als dynamische Gruppe von Katalogelementen. Wenn ein Katalogelement zu einem Dienst hinzugefügt wird, nachdem ihm die Berechtigung erteilt wurde, ist das neue Katalogelement für die angegebenen Benutzer ohne zusätzliche Konfiguration verfügbar.

- **Katalogelemente und Komponenten in Berechtigungen**

Berechtigte Katalogelemente sind Blueprints, die Sie im Servicekatalog anfordern können. Berechtigte Komponenten sind Bestandteil der Blueprints, können aber nicht speziell im Servicekatalog angefordert werden.

- **Aktionen in Berechtigungen**

Aktionen werden für bereitgestellte Katalogelemente ausgeführt. Bereitgestellte Katalogelemente und die Aktionen, die Sie für diese Katalogelemente ausführen dürfen, werden auf der Registerkarte „Elemente“ angezeigt. Um Aktionen für ein bereitgestelltes Element auszuführen, muss die Aktion in der Berechtigung für das Katalogelement enthalten sein, mit dem das Element über den Servicekatalog bereitgestellt wurde.

- **Genehmigungsrichtlinien in Berechtigungen**

Genehmigungsrichtlinien werden in Berechtigungen angewendet, damit Sie Ressourcen in Ihrer Umgebung verwalten können.

## **Dienste in Berechtigungen**

Ein berechtigter Dienst fungiert als dynamische Gruppe von Katalogelementen. Wenn ein Katalogelement zu einem Dienst hinzugefügt wird, nachdem ihm die Berechtigung erteilt wurde, ist das neue Katalogelement für die angegebenen Benutzer ohne zusätzliche Konfiguration verfügbar.

Wenn Sie eine Genehmigungsrichtlinie auf einen Dienst anwenden, gilt für alle Elemente, wenn sie angefordert werden, dieselbe Genehmigungsrichtlinie.

## **Katalogelemente und Komponenten in Berechtigungen**

Berechtigte Katalogelemente sind Blueprints, die Sie im Servicekatalog anfordern können. Berechtigte Komponenten sind Bestandteil der Blueprints, können aber nicht speziell im Servicekatalog angefordert werden.

Berechtigte Katalogelemente und Komponenten können die folgenden Elemente umfassen:

### **Katalogelemente**

- Elemente aus jedem Dienst, den Sie berechtigten Benutzern bereitstellen möchten, und sogar Dienste, die nicht in der aktuellen Berechtigung enthalten sind.

Beispielsweise haben Sie als Katalog-Administrator mehrere unterschiedliche Versionen von Red Hat Enterprise Linux einem Red Hat-Dienst zugeordnet und erteilen den Qualitätsingenieuren für Produkt A die Berechtigung für diesen Dienst. Anschließend erhalten Sie eine Anforderung, Servicekatalogelemente zu erstellen, die nur die neueste Version von Linux-basierten Betriebssystemen für das

Schulungsteam enthalten. Sie erstellen eine Berechtigung für das Schulungsteam, die die neuesten Versionen der anderen Betriebssysteme in einem Dienst enthält. Sie haben bereits die neueste Version von RHEL einem anderen Dienst zugeordnet, weshalb Sie nicht den gesamten Red Hat-Dienst, sondern RHEL als Katalogelement hinzufügen.

- Elemente, die in einem Dienst enthalten sind, der Bestandteil der aktuellen Berechtigung ist, aber Sie möchten eine Genehmigungsrichtlinie auf das einzelne Katalogelement anwenden, das von der Richtlinie abweicht, die Sie auf den Dienst angewendet haben.

Beispielsweise erteilen Sie als Business-Gruppenmanager Ihrem Entwicklungsteam die Berechtigung für einen Dienst, der drei VM-Katalogelemente enthält. Sie wenden eine Genehmigungsrichtlinie an, die die Genehmigung des Virtual Infrastructure-Administrators für Maschinen mit mehr als vier CPUs erfordert. Eine der virtuellen Maschinen wird für Leistungstests verwendet, weshalb Sie sie als Katalogelement hinzufügen und eine weniger restriktive Genehmigungsrichtlinie für dieselbe Benutzergruppe anwenden.

## Komponenten

- Komponenten sind nicht anhand des Namens im Servicekatalog verfügbar, da sie Bestandteil eines Katalogelements sind. Sie erteilen ihnen separat Berechtigungen, sodass Sie eine bestimmte Genehmigungsrichtlinie anwenden können, die vom Katalogelement, in dem sie enthalten ist, abweicht.

Beispielsweise enthält ein Element eine Maschine und Software. Die Maschine ist als bereitstellbares Element verfügbar und weist eine Genehmigungsrichtlinie auf, die die Genehmigung des Standortmanagers erfordert. Die Software ist nicht als eigenständiges, bereitstellbares Element verfügbar, sondern nur im Rahmen einer Maschinenanforderung, aber die Genehmigungsrichtlinie für die Software erfordert die Genehmigung durch den Softwarelizenzierungsadministrator Ihrer Organisation. Wenn die Maschine im Servicekatalog angefordert wird, muss sie vom Standortadministrator und vom Softwarelizenzierungsadministrator genehmigt werden, bevor sie bereitgestellt wird. Nach der Bereitstellung wird die Maschine, mit dem Softwareeintrag, auf der Registerkarte „Elemente“ des Anforderers als Bestandteil der Maschine angezeigt.

## Aktionen in Berechtigungen

Aktionen werden für bereitgestellte Katalogelemente ausgeführt. Bereitgestellte Katalogelemente und die Aktionen, die Sie für diese Katalogelemente ausführen dürfen, werden auf der Registerkarte „Elemente“ angezeigt. Um Aktionen für ein bereitgestelltes Element auszuführen, muss die Aktion in der Berechtigung für das Katalogelement enthalten sein, mit dem das Element über den Servicekatalog bereitgestellt wurde.

Beispielsweise enthält die Berechtigung 1 eine virtuelle vSphere-Maschine und die Aktion „Snapshot erstellen“. Die Berechtigung 2 enthält nur eine virtuelle vSphere-Maschine. Wenn Sie eine vSphere-Maschine über die Berechtigung 1 bereitstellen, ist die Aktion „Snapshot erstellen“ verfügbar. Wenn Sie eine vSphere-Maschine über die Berechtigung 2 bereitstellen, ist keine Aktion verfügbar. Um die Aktion für Benutzer mit der Berechtigung 2 verfügbar zu machen, fügen Sie die Aktion „Snapshot erstellen“ zur Berechtigung 2 hinzu.

Wenn Sie eine Aktion auswählen, die auf keines der Katalogelemente in der Berechtigung anwendbar ist, wird sie nicht als Aktion auf der Registerkarte „Elemente“ angezeigt. Angenommen, Ihre Berechtigung enthält eine vSphere-Maschine und Sie erteilen die Berechtigung für die Aktion „Löschen“ für eine Cloud-Maschine. Die Aktion „Löschen“ ist nicht für die Ausführung auf der bereitgestellten Maschine verfügbar.

Sie können eine Genehmigungsrichtlinie auf eine Aktion anwenden, die von der Richtlinie abweicht, die auf das Katalogelement in der Berechtigung angewendet wird.

Wenn der Benutzer des Servicekatalogs Mitglied mehrerer Business-Gruppen ist und eine Gruppe nur zum Ein- und Ausschalten und die andere Gruppe nur zum Löschen berechtigt ist, stehen dem Benutzer alle drei Aktionen für die entsprechende bereitgestellte Maschine zur Verfügung.

### **Best Practices beim Erteilen der Berechtigung für Aktionen**

Blueprints sind komplex, und die Erteilung der Berechtigung zum Ausführen von Aktionen für bereitgestellte Blueprints kann zu unerwartetem Verhalten führen. Halten Sie sich an die folgenden Best Practices, wenn Sie Servicekatalogbenutzern die Berechtigung zum Ausführen von Aktionen für ihre bereitgestellten Elemente erteilen.

- Wenn Sie Benutzern die Berechtigung zum Löschen der Maschine erteilen, erteilen Sie ihnen die Berechtigung zum Löschen der Bereitstellung. Ein bereitgestellter Blueprint ist eine Bereitstellung.

Eine Bereitstellung kann eine Maschine enthalten. Angenommen, der Servicekatalogbenutzer ist berechtigt, die Aktion zum Löschen der Maschine auszuführen, aber er ist nicht berechtigt, die Aktion zum Löschen der Bereitstellung auszuführen. Wenn der Benutzer dann die Aktion zum Löschen der Maschine für die letzte oder einzige Maschine in einer Bereitstellung ausführt, wird eine Meldung mit dem Hinweis angezeigt, dass der Benutzer nicht über die Berechtigung zum Ausführen der Aktion verfügt. Wenn Sie die Berechtigung für beide Aktionen erteilen, wird sichergestellt, dass die Bereitstellung aus Ihrer Umgebung entfernt wird. Um die Kontrolle über die Aktion zum Löschen der Bereitstellung zu verwalten, können Sie eine Richtlinie vor der Genehmigung erstellen und auf die Aktion anwenden. Mithilfe dieser Richtlinie kann der entsprechende Genehmiger die Anforderung zum Löschen der Bereitstellung überprüfen, bevor sie ausgeführt wird.

- Wenn Sie Servicekatalogbenutzern die Berechtigungen „Lease ändern“, „Besitzer ändern“, „Ablauf“, „Neu konfigurieren“ und für andere Aktionen, die auf Maschinen und Bereitstellungen angewendet werden können, erteilen, sollten Sie ihnen die Berechtigung für beide Aktionen erteilen.

### **Genehmigungsrichtlinien in Berechtigungen**

Genehmigungsrichtlinien werden in Berechtigungen angewendet, damit Sie Ressourcen in Ihrer Umgebung verwalten können.

Um beim Erstellen der Berechtigung eine Genehmigungsrichtlinie anzuwenden, muss die Richtlinie bereits vorhanden sein. Ist dies nicht der Fall, können Sie dennoch die Berechtigung erstellen und im Entwurfszustand oder inaktiven Zustand belassen, bis Sie die erforderlichen Genehmigungsrichtlinien für die Katalogelemente und die Aktionen in dieser Berechtigung erstellt haben, und dann die Richtlinien später anwenden.

Sie müssen keine Genehmigungsrichtlinie auf Elemente oder Aktionen anwenden. Wenn keine Genehmigungsrichtlinie angewendet wird, werden die Elemente und Aktionen, wenn sie angefordert werden, bereitgestellt, ohne dass eine Genehmigungsanforderung ausgelöst wird.

## Erteilen der Berechtigung für Dienste, Katalogelemente und Aktionen

Wenn Sie einer Berechtigung Dienste, Katalogelemente oder Aktionen hinzufügen, erlauben Sie den in der Berechtigung identifizierten Benutzern und Gruppen, die bereitstellbaren Elemente im Servicekatalog anzufordern. Aktionen sind Elementen zugeordnet und werden auf der Registerkarte **Elemente** für den Anforderer angezeigt.

Es gibt mehrere Benutzerrollen, die das Erstellen von Berechtigungen für Business-Gruppen erlauben.

- Mandantenadministratoren können in ihrem Mandanten Berechtigungen für jede Business-Gruppe erstellen.
- Business-Gruppenmanager können Berechtigungen für die von ihnen verwalteten Gruppen erstellen.
- Katalogadministratoren können in ihrem Mandanten Berechtigungen für jede Business-Gruppe erstellen.

Wenn Sie eine Berechtigung erstellen, müssen Sie eine Business-Gruppe auswählen und die einzelnen Benutzer und Gruppen in der Business-Gruppe für die Berechtigung angeben.

Informationen zum Erstellen einer Berechtigung, sodass Sie durch die Interaktion von Diensten, Katalogelemente und Aktionen mit Genehmigungen, die entsprechenden Elemente im Servicekatalog bereitstellen können, finden Sie unter [Erstellen von Berechtigungen](#).

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **Katalogadministrator** an.
- Stellen Sie sicher, dass die Katalogelemente, für die Sie Benutzern die Berechtigung erteilen, einem Dienst zugeordnet sind. Siehe [Hinzufügen von Katalogelementen zu einem Dienst](#).
- Stellen Sie sicher, dass die Business-Gruppe, für die Sie die Berechtigung definieren, vorhanden ist und dass die Mitgliedsbenutzer und Benutzergruppen definiert sind. Siehe [Erstellen einer Business-Gruppe](#).
- Stellen Sie sicher, dass die Genehmigungsrichtlinien vorhanden sind, wenn Sie beim Erstellen dieser Berechtigung Genehmigungen hinzufügen möchten. Siehe [Erstellen einer Genehmigungsrichtlinie](#). Wenn Sie Benutzern die Berechtigung für die Elemente im Servicekatalog ohne Genehmigungen erteilen möchten, können Sie die Berechtigung später ändern, um Diensten, Katalogelementen und Aktionen Genehmigungen hinzuzufügen.

### Vorgehensweise

- 1 Wählen Sie **Administration > Katalogmanagement > Berechtigungen** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.

### 3 Konfigurieren Sie die Detailoptionen.

Details bestimmen, wie die Berechtigung in der Berechtigungsliste angezeigt wird und welche Benutzer Zugriff auf die Elemente im Servicekatalog haben.

Option	Beschreibung
<b>Name und Beschreibung</b>	Informationen zur Berechtigung, die in der Berechtigungsliste angezeigt wird.
<b>Ablaufdatum</b>	Legen Sie das Datum und die Uhrzeit fest, wenn die Berechtigung an einem bestimmten Datum inaktiv werden soll.
<b>Status</b>	<p>Mögliche Werte sind „Entwurf“, „Aktiv“ und „Inaktiv“.</p> <ul style="list-style-type: none"> <li>■ Entwurf. Elemente sind im Servicekatalog nicht verfügbar und waren niemals aktiv. Nach Aktivierung einer Berechtigung können Sie nicht mehr zum Entwurfsstatus zurückkehren.</li> <li>■ Aktiv. Elemente sind im Servicekatalog verfügbar. Diese Option ist verfügbar, wenn Sie Berechtigungen hinzufügen oder bearbeiten.</li> <li>■ Inaktiv. Elemente sind im Servicekatalog nicht verfügbar, aber die Berechtigung war einmal aktiv. Die Berechtigung wurde aufgrund des Ablaufdatums oder durch einen Benutzer deaktiviert.</li> </ul>
<b>Business-Gruppe</b>	<p>Wählen Sie eine Business-Gruppe aus. Sie können Berechtigungen nur für eine Business-Gruppe erstellen und berechtigte Benutzer müssen Mitglieder der Business-Gruppe sein.</p> <p>Wenn eine Berechtigung für alle Benutzer verfügbar sein soll, benötigen Sie entweder eine „Alle Benutzer“-Business-Gruppe und eine benutzerdefinierte Benutzergruppe, die alle Benutzer enthält, oder aber Sie müssen Berechtigungen für jede Business-Gruppe erstellen.</p> <p>Wenn Sie als Business-Gruppenmanager angemeldet sind, können Sie nur Berechtigungen für Ihre Business-Gruppe erstellen.</p>
<b>Benutzer und Gruppen</b>	<p>Fügen Sie mindestens einen Benutzer oder eine Gruppe hinzu. Die verfügbaren Benutzer oder Gruppen sind auf Mitglieder der ausgewählten Business-Gruppe beschränkt.</p> <p>Wenn der Status „Entwurf“ ist, müssen Sie keine Benutzer oder Gruppen angeben. Um eine Berechtigung zu aktivieren, müssen Sie mindestens einen Benutzer oder eine Gruppe angeben.</p>

### 4 Klicken Sie auf **Weiter**.



- 5 Klicken Sie auf das Symbol **Neu (+)**, um Benutzern die Berechtigung für Dienste, Katalogelemente oder Aktionen zu erteilen.

Sie können eine Berechtigung mit verschiedenen Kombinationen von Diensten, Elementen und Aktionen erstellen.

Option	Beschreibung
<b>Berechtigte Services</b>	<p>Fügen Sie einen Dienst hinzu, wenn Sie berechtigten Benutzern den Zugriff auf alle veröffentlichte Katalogelemente geben möchten, die mit dem Dienst verknüpft sind.</p> <p>Ein berechtigter Dienst ist eine dynamische Berechtigung. Wenn ein Element zu einem späteren Zeitpunkt zu dem Dienst hinzugefügt wird, wird es zum Servicekatalog für berechtigte Benutzer hinzugefügt. Berechtigungen können sowohl Dienste als auch individuelle Katalogelemente umfassen.</p>
<b>Berechtigte Katalogelemente und Komponenten</b>	<p>Fügen Sie einzelne Elemente hinzu, die für die berechtigten Benutzer verfügbar sind.</p> <p>Berechtigungen können sowohl Dienste als auch einzelne Katalogelemente enthalten. Um eine andere Richtlinie auf ein im Dienst enthaltenes Element anzuwenden, fügen Sie es als Katalogelement hinzu. Die Genehmigungsrichtlinie für ein Element hat Vorrang vor der Genehmigungsrichtlinie für den Dienst, zu dem sie gehört, wenn sich beide in der gleichen Berechtigung befinden. Wenn sie sich in unterschiedlichen Berechtigungen befinden, basiert die Reihenfolge auf der festgelegten Priorität.</p> <p>Katalogelemente müssen einem Dienst zugeordnet werden, um im Servicekatalog verfügbar zu sein. Das Katalogelement kann jedem Dienst zugeordnet werden, nicht nur einem Dienst in der aktuellen Berechtigung.</p> <p>Komponenten sind Bestandteile eines Katalogelements, sind aber nicht anhand des Namens im Servicekatalog verfügbar. Beispielsweise ist MySQL-Software eine Komponente eines CentOS-VM-Katalogelements. Berechtigungen für Komponenten werden zusammen mit dem Katalogelement erteilt. Wenn Sie eine Genehmigungsrichtlinie speziell für Software anwenden möchten, erteilen Sie separate Berechtigungen für das Element. Ansonsten müssen Sie einer Komponente keine Berechtigungen erteilen, damit sie zusammen mit dem übergeordneten Element bereitgestellt wird.</p>
<b>Berechtigte Aktionen</b>	<p>Fügen Sie Aktionen hinzu, wenn Sie Benutzern das Ausführen der Aktionen für ein bereitgestelltes Element erlauben möchten.</p> <p>Aktionen, die Sie für die über diese Berechtigung erteilten Elemente ausführen möchten, müssen in derselben Berechtigung vorhanden sein.</p> <p>Berechtigte Aktionen werden im Servicekatalog nicht angezeigt. Sie werden auf der Registerkarte „Elemente“ für ein bereitgestelltes Element angezeigt.</p>
<b>Aktionen gelten nur für die in dieser Berechtigung definierten Elemente</b>	<p>Bestimmt, ob die berechtigten Aktionen für alle zutreffenden Dienstkatalogelemente berechtigt sind oder nur die Elemente in dieser Berechtigung.</p> <p>Bei Auswahl der Option sind die Business-Gruppenmitglieder berechtigt, die Aktionen für die entsprechenden Elemente in dieser Berechtigung durchzuführen. Diese Methode zur Berechtigungserteilung für die Aktionen wird empfohlen, da Sie so die Aktionen für die spezifischen Elemente angeben können.</p> <p>Ist die Option nicht ausgewählt, sind die in dieser Berechtigung angegebenen Benutzer zur Durchführung der Aktionen für alle zutreffenden Katalogelemente berechtigt, unabhängig davon, ob die Elemente in dieser Berechtigung enthalten sind oder nicht. Alle angewendeten Genehmigungsrichtlinien für diese Aktionen sind ebenfalls aktiv.</p>

- 6 Verwenden Sie das Dropdown-Menü in den verschiedenen Abschnitten, um die verfügbaren Elemente zu filtern.
- 7 Aktivieren Sie Kontrollkästchen, um der Berechtigung Elemente hinzuzufügen.
- 8 Um dem ausgewählten Dienst, dem ausgewählten Element oder der ausgewählten Aktion eine Genehmigungsrichtlinie hinzuzufügen, wählen Sie aus dem Dropdown-Menü **Diese Richtlinie auf ausgewählte Elemente anwenden** eine Genehmigungsrichtlinie aus.

Wenn Sie eine Genehmigungsrichtlinie auf einen Dienst anwenden, gilt für alle Elemente des Diensts dieselbe Genehmigungsrichtlinie. Um eine andere Richtlinie auf ein Element anzuwenden, fügen Sie es als Katalogelement hinzu und wenden Sie die entsprechende Richtlinie an.

- 9 Klicken Sie auf **OK**.

Der Dienst, das Element bzw. die Aktion wird zur Berechtigung hinzugefügt.

- 10 Klicken Sie zum Speichern der Berechtigung auf **Fertig stellen**.

Wenn der Berechtigungsstatus „Aktiv“ lautet, werden der Dienst und die Elemente zum Servicekatalog hinzugefügt.

#### Weiter

Stellen Sie sicher, dass die berechtigten Dienste und Katalogelemente im Servicekatalog für die berechtigten Benutzer angezeigt werden und dass die angeforderten Elemente die Zielobjekte erwartungsgemäß bereitstellen. Sie können das Element im Namen der ausgewählten Benutzer anfordern.

## Priorisieren von Berechtigungen

Wenn mehrere Berechtigungen für dieselbe Business-Gruppe vorhanden sind, können Sie die Berechtigungen priorisieren, sodass die Berechtigung und die zugeordnete Genehmigungsrichtlinie in der angegebenen Reihenfolge verarbeitet werden, wenn eine Servicekatalogbenutzer eine Anforderung stellt.

Wenn Sie eine Genehmigungsrichtlinie für eine Benutzergruppe konfigurieren und ein Gruppenmitglied über eine eindeutige Richtlinie für mindestens einen der Services, Katalogelemente oder Aktionen verfügen soll, priorisieren Sie die Mitgliederberechtigung vor der Gruppenberechtigung. Wenn das Mitglied ein Element im Servicekatalog anfordert, basiert die angewendete Genehmigungsrichtlinie auf der Priorität der Berechtigungen für die Business-Gruppe. Wird der Name des Mitglieds zum ersten Mal gefunden, entweder als Teil einer benutzerdefinierten Benutzergruppe oder als individueller Benutzer, ist dies die angewendete Genehmigungsrichtlinie.

Beispiel: Sie erstellen zwei Berechtigungen für dasselbe Katalogelement, sodass Sie eine Genehmigungsrichtlinie für die Buchhaltungsbenutzergruppe und eine andere Genehmigungsrichtlinie für Connie, ein Mitglied dieser Gruppe, anwenden können.

**Tabelle 4-49. Beispielberechtigungen**

Berechtigung 1	Berechtigung 2
Business-Gruppe: Finanzen	Business-Gruppe: Finanzen
Benutzer und Gruppen: Buchhaltungsgruppe	Benutzer und Gruppen: Connie
Katalogelement 1: Richtlinie A	Katalogelement 1: Richtlinie C

Connie fordert Katalogelement 1 im Servicekatalog an. Abhängig von der Priorität der Berechtigungen für die Finanz-Business-Gruppe wird eine andere Richtlinie auf die Anfrage von Connie angewendet.


**Tabelle 4-50. Beispielergebnisse**

Konfiguration und Ergebnis	Priorität	Priorität
Priorität	1: Berechtigung 1 2: Berechtigung 2	1: Berechtigung 2 2: Berechtigung 1
Angewendete Richtlinie	Die Richtlinie A wird angewendet.  Connie ist ein Mitglied der Buchhaltungs-Benutzergruppe. Die Suche nach Connie als berechtigter Benutzer endet bei Berechtigung 1, und die Genehmigungsrichtlinie wird angewendet.	Die Richtlinie C wird angewendet.  Die Suche nach Connie als berechtigter Benutzer endet bei Berechtigung 2, und die Genehmigungsrichtlinie wird angewendet.

### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **Katalogadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Katalogmanagement > Berechtigungen** aus.
- 2 Klicken Sie auf das Symbol **Priorisieren** (  ).
- 3 Wählen Sie in der Dropdownliste **Business-Gruppe** eine Business-Gruppe aus.
- 4 Ziehen Sie eine Berechtigung an eine neue Position in der Liste, um ihre Priorität zu ändern.
- 5 Wählen Sie eine Aktualisierungsmethode aus.

Option	Beschreibung
<b>Aktualisieren</b>	Speichert die Änderungen.
<b>Aktualisieren und schließen</b>	Speichert die Änderungen und schließt das Fenster <b>Elemente priorisieren</b> .

## Arbeiten mit Genehmigungsrichtlinien

Genehmigungsrichtlinien sind ein Kontrollmechanismus, den Sie Servicekataloganforderungen hinzufügen, damit Sie Ressourcen in Ihrer Umgebung verwalten können. Jede Richtlinie stellt einen definierten Bedingungssatz dar, der auf Dienste, Katalogelemente und Aktionen angewendet werden kann, wenn Sie Benutzern die Berechtigung für diese Elemente erteilen.

### Genehmigungsrichtlinienprozess

Zunächst erstellt ein Mandantenadministrator oder Genehmigungsadministrator die Genehmigungsrichtlinien, für die die Bereitstellungskontrolle erforderlich ist.

Genehmigungsrichtlinien werden für Genehmigungsrichtlinientypen oder bestimmte Elemente erstellt. Wenn die Richtlinie auf einem Richtlinientyp basiert, können Sie sie auf übereinstimmende Katalogelementtypen anwenden. Wenn beispielsweise eine Richtlinie auf einem Softwarerichtlinientyp basiert, können Sie sie für beliebige Softwareelemente in den Berechtigungen definieren und darauf anwenden. Wenn die Richtlinie für ein bestimmtes Element ist, sollten Sie sie nur auf dieses Element anwenden. Wenn es sich beispielsweise bei dem Element um ein bestimmtes Softwareelement handelt, sollten Sie die Richtlinie nur auf dieses spezielle Datenbanksoftwareelement in der Berechtigung anwenden.

Richtlinien können Anforderungen vor und nach der Genehmigung beinhalten. Anforderungen vor der Genehmigung müssen genehmigt werden, bevor das angeforderte Element bereitgestellt wird. Für Richtlinien nach der Genehmigung muss der Genehmiger die Anforderung akzeptieren, bevor das bereitgestellte Element für den anfordernden Benutzer verfügbar gemacht wird.

Die Konfigurationen vor und nach der Genehmigung bestehen aus einer oder mehreren Ebenen, die bestimmen, wann die Genehmigungsrichtlinie ausgelöst wird und wer die Anforderung genehmigt bzw. wie die Anforderung genehmigt wird. Mehrere Ebenen sind möglich. Beispiel: Eine Genehmigungsrichtlinie kann eine Ebene für die Genehmigung durch den Manager enthalten, gefolgt von einer Ebene für die Genehmigung durch die Finanzabteilung.

Anschließend wendet ein Mandantenadministrator oder Business-Gruppenmanager die Genehmigungsrichtlinien auf die Dienste, Katalogelemente bzw. Aktionen an.

Wenn schließlich ein Servicekatalogbenutzer ein Element anfordert, auf das eine Genehmigungsrichtlinie angewendet ist, genehmigen die Genehmiger die Anforderung auf der Seite **Genehmigungen** über die Registerkarte **Posteingang** oder lehnen sie ab. Der anfordernde Benutzer kann den Genehmigungsstatus für eine bestimmte Anforderung auf der Registerkarte **Anforderungen** nachverfolgen.

## Beispiele für Genehmigungsrichtlinien basierend auf dem VM-Richtlinientyp

Sie können eine Genehmigungsrichtlinie erstellen, die Sie auf denselben Katalogelementtyp anwenden können. Es ergeben sich jedoch unterschiedliche Ergebnisse, wenn ein Element im Servicekatalog angefordert wird. In Abhängigkeit davon, wie die Genehmigungsrichtlinie definiert und angewendet wird, variieren die Auswirkungen auf den Servicekatalogbenutzer und den Genehmiger.

Die folgende Tabelle enthält Beispiele für verschiedene Genehmigungsrichtlinien, die alle auf demselben Genehmigungsrichtlinientyp basieren. Diese Beispiele veranschaulichen einige Konfigurationsmethoden für Genehmigungsrichtlinien, mit denen Sie einen unterschiedlichen Grad an Kontrolle erzielen.

Tabelle 4-51. Beispiele für Genehmigungsrichtlinien und Ergebnisse

Angestrebte Kontrolle	Ausgewählter Richtlinientyp	Vor oder nach der Genehmigung	Wann ist eine Genehmigung erforderlich?	Wer sind die Genehmiger?	Wie wird die Richtlinie in der Berechtigung angewendet?	Ergebnisse bei Anforderung des Elements im Servicekatalog
<p>Der Business-Gruppenmanager muss alle VM-Anforderungen genehmigen.</p> <p>Die Genehmigungsrichtlinie muss auf mehrere Business-Gruppen in mehreren Berechtigungen anwendbar sein.</p>	Servicekatalog – Katalogelementanforderung – virtuelle Maschine	Zur Registerkarte „Vor der Genehmigung“ hinzufügen	Wählen Sie „Immer erforderlich“ aus.	<p>Wählen Sie <b>Genehmiger aus der Anforderung bestimmen</b> aus.</p> <p>Wählen Sie die Bedingung <b>Business-Gruppe &gt; Manager &gt; Benutzer &gt; Manager</b> aus.</p> <p>Wählen Sie <b>Jeder kann genehmigen</b> aus.</p>	Berechtigungen basieren auf Business-Gruppen. Diese Genehmigung kann für jede Berechtigung verwendet werden, bei der die Genehmigung des Managers für die virtuelle Maschine erforderlich ist.	Wenn der Servicekatalogbenutzer eine virtuelle Maschine anfordert, auf die diese Genehmigung angewendet wurde, muss der Business-Gruppenmanager die Anforderung genehmigen, bevor die Maschine bereitgestellt wird.
Der Virtual Infrastructure-Administrator muss die ordnungsgemäße Bereitstellung der virtuellen Maschine sicherstellen und die Anforderung genehmigen, bevor die virtuelle Maschine für den anfordernden Benutzer freigegeben wird.	Servicekatalog – Katalogelementanforderung – virtuelle Maschine	Zur Registerkarte „Nach der Genehmigung“ hinzufügen	Wählen Sie „Immer erforderlich“ aus.	<p>Wählen Sie <b>Bestimmte Benutzer und Gruppen</b> aus.</p> <p>Wählen Sie die benutzerdefinierten Benutzergruppen des Virtual Infrastructure-Administrators aus.</p> <p>Wählen Sie <b>Jeder kann genehmigen</b> aus.</p>	Diese Genehmigung kann für jede Berechtigung verwendet werden, bei der der Virtual Infrastructure-Administrator die virtuelle Maschine auf dem vCenter Server nach der Bereitstellung überprüfen soll.	Wenn der Servicekatalogbenutzer eine virtuelle Maschine anfordert, auf die diese Genehmigung angewendet wurde, wird die virtuelle Maschine bereitgestellt. Wenn jedes Mitglied der VI-Admin-Gruppe die Anforderung genehmigt, wird die Maschine für den Benutzer freigegeben.

Tabelle 4-51. Beispiele für Genehmigungsrichtlinien und Ergebnisse (Fortsetzung)

Angestrebte Kontrolle	Ausgewählter Richtlinientyp	Vor oder nach der Genehmigung	Wann ist eine Genehmigung erforderlich?	Wer sind die Genehmiger?	Wie wird die Richtlinie in der Berechtigung angewendet?	Ergebnisse bei Anforderung des Elements im Servicekatalog
Um Virtual Infrastructure-Ressourcen zu verwalten und die Kosten zu kontrollieren, können Sie zwei Genehmigungsebenen „Vor der Bereitstellung“ hinzufügen, nämlich eine Genehmigung für Maschinenressourcen und eine zweite Genehmigung für die Kosten der Maschine pro Tag.	Servicekatalog – Katalogelementanforderung – virtuelle Maschine	Zur Registerkarte „Vor der Genehmigung“ hinzufügen	<p>Ebene 1</p> <p>Wählen Sie <b>Erforderlich basierend auf Bedingungen</b> aus.</p> <p>Konfigurieren Sie die Bedingungen: CPUs &gt; 6 oder Arbeitsspeicher &gt; 8 oder Speicher &gt; 100 GB.</p>	<p>Wählen Sie <b>Genehmiger aus der Anforderung bestimmen</b> aus.</p> <p>Wählen Sie die Bedingung „Angefordert von &gt; Manager“ aus. Klicken</p> <p>Sie auf <b>Systemeigenschaften</b> und wählen Sie <b>CPUs, Arbeitsspeicher und Speicher</b> aus, damit der Genehmiger den Wert auf ein akzeptables Niveau ändern kann.</p>	Diese Genehmigungsrichtlinie kann in einer Berechtigung verwendet werden, bei der der Manager des anfordernden Benutzers und ein Mitglied der Finanzabteilung die Anforderung genehmigen sollen.	<p>Wenn der Servicekatalogbenutzer eine virtuelle Maschine anfordert, wird die Anforderung ausgewertet und es wird bestimmt, ob die angeforderten Werte für CPU, Arbeitsspeicher oder Speicher über den in Ebene 1 angegebenen Werten liegen.</p> <p>Wenn dies nicht der Fall ist, wird die Bedingung für die Ebene 2 ausgewertet.</p> <p>Wenn die Anforderungen mindestens eine der Bedingungen der Ebene 1 überschreiten, muss der Manager die Anforderung genehmigen.</p> <p>Der Manager kann die angeforderten Konfigurationswerte reduzieren und die Anforderung genehmigen oder aber die Anforderung ablehnen.</p>
			<p>Ebene 2</p> <p>Wählen Sie <b>Erforderlich basierend auf Bedingungen</b> aus.</p> <p>Konfigurieren Sie die Bedingung „Kosten &gt; 15,00 pro Tag“.</p>	<p>Wählen Sie <b>Bestimmte Benutzer und Gruppen</b> aus.</p> <p>Wählen Sie die benutzerdefinierte Benutzergruppe „Finanzen“ aus.</p> <p>Wählen Sie <b>Jeder kann genehmigen</b> aus.</p>		

## Beispiel für Aktionen mit in einer zusammengesetzten Bereitstellung angewendeten Genehmigungsrichtlinien

Wenn Sie Genehmigungsrichtlinien auf Aktionen anwenden, die für verschiedene Komponenten in einem zusammengesetzten Blueprint ausgeführt werden können, ist der Genehmigungsprozess unterschiedlich, je nachdem, wie die Berechtigung konfiguriert ist und wie die Genehmigungsrichtlinien angewendet werden.

In diesem Beispiel werden bestimmte Details zum Erstellen des Blueprints verwendet und anschließend Genehmigungsrichtlinien auf Aktionen angewendet, die aus dem Servicekatalog für den bereitgestellten Blueprint in verschiedenen Berechtigungen ausgeführt werden können. Der Blueprint ist ein zusammengesetzter Blueprint, der einen anderen Blueprint enthält. Die verwendeten Aktionen dienen zum Löschen der bereitgestellten Elemente, zum Löschen einer Bereitstellung für die Blueprints und zum Löschen einer virtuellen Maschine für die Maschine. Durch das sich daraus ergebende Verhalten wird festgelegt, welche Elemente bzw. Komponenten gelöscht werden und wann durch die angewendeten Genehmigungsrichtlinien Genehmigungsanforderungen ausgelöst werden.

### Blueprint – Beispiel

In diesem Beispiel konfigurieren Sie einen Blueprint, der einen geschachtelten Blueprint mit einer virtuellen Maschine umfasst.

- Blueprint 1 – Blueprint für kontinuierliche Integration
  - Blueprint 2 – Vorproduktions-Blueprint
    - Virtuelle Maschine 1 – TestAsAService vSphere VM

### Genehmigungsrichtlinien für Löschaktionen

Sie können zwei Genehmigungsrichtlinien konfigurieren, um bereitgestellte Elemente zu löschen. Eine Aktion vom Typ „Löschen – Bereitstellung“ kann in diesem Beispiel für „Blueprint 1“ oder „Blueprint 2“ ausgeführt werden. Eine Aktion vom Typ „Löschen – Virtuelle Maschine“ kann für „Virtuelle Maschine 1“ ausgeführt werden. Sie erstellen die Genehmigungsrichtlinien, die Sie dann auf die Aktionen in der Berechtigung anwenden können.

Name der Genehmigungsrichtlinie	Genehmigungsrichtlinientyp
Genehmigungsrichtlinie A	Servicekatalog – Ressourcenaktionsanforderung – Löschen – Bereitstellung
Genehmigungsrichtlinie B	Servicekatalog – Ressourcenaktionsanforderung – Löschen – Virtuelle Maschine

### Auf Aktionen angewendete Berechtigungen und Genehmigungsrichtlinien

Sie konfigurieren drei Berechtigungen. Jede Berechtigung enthält den zusammengesetzten Blueprint. In jeder Berechtigung fügen Sie die Löschaktionen hinzu und wenden die Genehmigungsrichtlinien an.

Berechtigungsname	Berechtigte Aktion auf bereitgestellter Maschine	Angewendete Genehmigungsrichtlinie
Berechtigung 1	Löschen – Bereitstellung	Genehmigungsrichtlinie A
Berechtigung 2	Löschen – Virtuelle Maschine	Genehmigungsrichtlinie B

Berechtigungsname	Berechtigte Aktion auf bereitgestellter Maschine	Angewendete Genehmigungsrichtlinie
Berechtigung 3	Löschen – Bereitstellung	Genehmigungsrichtlinie A
	Löschen – Virtuelle Maschine	Genehmigungsrichtlinie B

## Benutzeraktionen im Servicekatalog

Wenn der Benutzer des Servicekatalogs die Aktion ausführt, werden Blueprints oder Maschinen abhängig von dem Element, das der Benutzer in der Aktion ausgeführt hat, gelöscht.

Benutzeraktionen im Servicekatalog	Ausgewählte Aktion	Gelöschte Blueprints oder Maschinen
Aktion 1	Die Aktion „Löschen – Bereitstellung“ wird auf „Blueprint 1 – Blueprint für kontinuierliche Integration“ ausgeführt.	Blueprint 1, Blueprint 2 und Virtuelle Maschine 1
Aktion 2	Die Aktion „Löschen – Bereitstellung“ wird auf dem geschachtelten „Blueprint 2 – Vorproduktions-Blueprint“ ausgeführt.	Blueprint 2 und Virtuelle Maschine 1
Aktion 3	Die Aktion „Löschen – Virtuelle Maschine“ wird auf der Maschine ausgeführt, die sich innerhalb einer Bereitstellung befindet, „Virtuelle Maschine 1 – TestAsAService vSphere VM“.	Virtuelle Maschine 1

## Auf Aktionen in den Berechtigungen angewendete Genehmigungsrichtlinien

Sie wenden die Genehmigungsrichtlinien an und die Genehmiger erhalten eine Genehmigungsanforderung abhängig vom dem Blueprint oder der Maschine, für den bzw. die der Servicekatalogbenutzer die Aktion ausgeführt hat.

Berechtigungsname	Genehmigungsrichtlinie für Aktionen	Benutzeraktion	Ausgelöste Genehmigungsanforderung	Wenn genehmigt, gelöschte Blueprints oder Maschinen
Berechtigung 1 – Genehmigungsrichtlinie „Löschen – Bereitstellung“	Richtlinie A (Genehmigungsrichtlinie „Löschen – Bereitstellung“ nur für Aktion „Löschen – Bereitstellung“)	Aktion 1 (Aktion „Löschen – Bereitstellung“ für „Blueprint 1“ ausführen)	Genehmigungsanforderungen werden nur für „Blueprint 1“ ausgelöst	Blueprint 1, Blueprint 2 und Virtuelle Maschine 1
		Aktion 2 (Aktion „Löschen – Bereitstellung“ für „Blueprint 2“ ausführen)	Genehmigungsanforderungen werden nur für „Blueprint 2“ ausgelöst	Blueprint 2 und Virtuelle Maschine 1
		Aktion 3 (Aktion „Löschen – Virtuelle Maschine“ wird für „Virtuelle Maschine 1“ ausgeführt)	Es werden keine Genehmigungsanforderungen ausgelöst	Virtuelle Maschine 1
Berechtigung 2	Richtlinie B (Richtlinie „Löschen – Virtuelle Maschine“) nur für Aktion „Löschen – Virtuelle Maschine“	Aktion 1 (Aktion „Löschen – Bereitstellung“ für „Blueprint 1“ ausführen)	Es werden keine Genehmigungsanforderungen ausgelöst	Blueprint 1, Blueprint 2 und Virtuelle Maschine 1



Berechtigungsname	Genehmigungsrichtlinie für Aktionen	Benutzeraktion	Ausgelöste Genehmigungsanforderung	Wenn genehmigt, gelöschte Blueprints oder Maschinen
		Aktion 2 (Aktion „Löschen – Bereitstellung“ für „Blueprint 2“ ausführen)	Es werden keine Genehmigungsanforderungen ausgelöst	Blueprint 2 und Virtuelle Maschine 1
		Aktion 3 (Aktion „Löschen – Virtuelle Maschine“ wird für „Virtuelle Maschine 1“ ausgeführt)	Genehmigungsanforderungen werden nur für „Virtuelle Maschine 1“ ausgelöst	Virtuelle Maschine 1
Berechtigung 3	Richtlinie A (Genehmigungsrichtlinie „Löschen – Bereitstellung“) für Aktion „Löschen – Bereitstellung“ und Richtlinie B (Richtlinie „Löschen – Virtuelle Maschine“) für Aktion „Löschen – Virtuelle Maschine“	Aktion 1 (Aktion „Löschen – Bereitstellung“ für „Blueprint 1“ ausführen)	Genehmigungsanforderungen werden nur für „Blueprint 1“ ausgelöst	Blueprint 1, Blueprint 2 und Virtuelle Maschine 1
		Aktion 2 (Aktion „Löschen – Bereitstellung“ für „Blueprint 2“ ausführen)	Genehmigungsanforderungen werden nur für „Blueprint 2“ ausgelöst	Blueprint 2 und Virtuelle Maschine 1
		Aktion 3 (Aktion „Löschen – Virtuelle Maschine“ wird für „Virtuelle Maschine 1“ ausgeführt)	Genehmigungsanforderungen werden nur für „Virtuelle Maschine 1“ ausgelöst	Virtuelle Maschine 1

## Beispiel für eine Genehmigungsrichtlinie in mehreren Berechtigungen

Wenn Sie eine Genehmigungsrichtlinie auf ein Element anwenden, das in mehreren Berechtigungen verwendet wird, die für die gleichen Benutzer in einer Business-Gruppe gelten, wird die Genehmigungsrichtlinie auch in dem Service für das Element ausgelöst, in dem die Genehmigungsrichtlinie nicht explizit in der Berechtigung angewendet ist.

Sie erstellen beispielsweise die folgenden Blueprints, Services, Genehmigungsrichtlinien und Berechtigungen.

### Blueprints

- Virtuelle RHEL vSphere-Maschine
- QE-Test beinhaltet virtuelle RHEL vSphere-Maschine
- QE-Schulung beinhaltet virtuelle RHEL vSphere-Maschine

### Dienste

- Der QE-Test-Blueprint ist dem Testdienst zugeordnet
- Der QE-Schulungs-Blueprint ist dem Schulungsdienst zugeordnet

## Berechtigungen

- Berechtigung 1
- Berechtigung 2

**Tabelle 4-52. Berechtigungskonfigurationen**

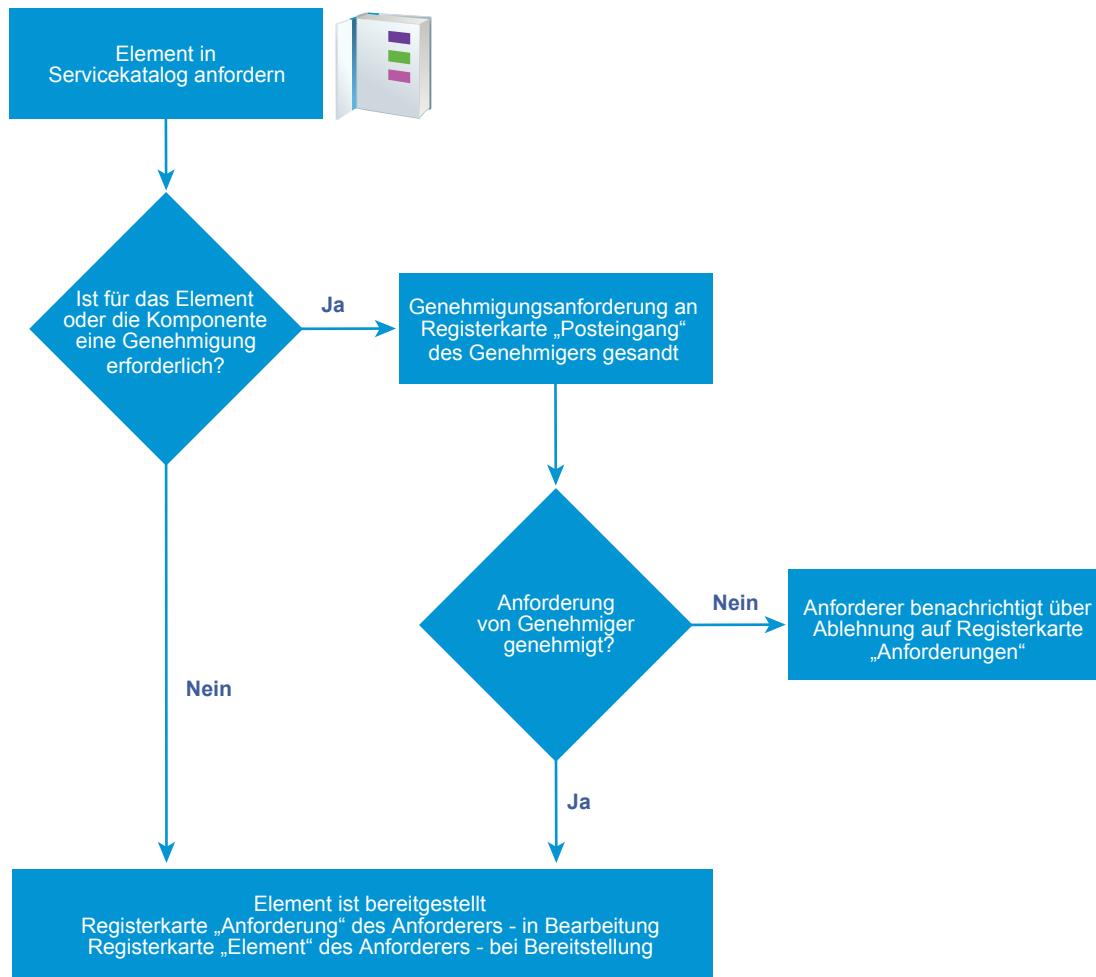
Berechtigungsname	Business-Gruppe	Berechtigter Service	Berechtigtes Element
Berechtigung 1	QE	Testen	Katalogelementanforderung – Virtuelle Maschine angewendet auf Komponente der virtuellen Maschine
Berechtigung 2	QE	Schulung	

## Ergebnisse

Wenn der Benutzer QE-Schulungen im Servicekatalog auswählt, wird die Genehmigungsrichtlinie für die virtuelle RHEL vSphere-Maschine ausgelöst, da es sich um einen Blueprint auf Basis einer virtuellen Maschinenkomponente handelt, die im QE-Schulungs-Blueprint verwendet wird.

**Vorbereiten von Genehmigungsrichtlinien im Servicekatalog**

Wenn ein Benutzer ein Element im Servicekatalog anfordert, dem eine Genehmigungsrichtlinie zugeordnet ist, wird die Anforderung durch den Genehmiger und den Anforderer in einem Workflow verarbeitet, der dem Folgenden ähnelt.



## Erstellen einer Genehmigungsrichtlinie

Mandantenadministratoren und Genehmigungsadministratoren können Genehmigungen definieren und diese in Berechtigungen verwenden. Sie können die Genehmigungsrichtlinien mit mehreren Ebenen für Ereignisse vor der Genehmigung und Ereignisse nach der Genehmigung konfigurieren.

Wenn Sie eine Einstellung in einem Softwarekomponenten-Blueprint ändern und diese Einstellung in einer Genehmigungsrichtlinie zum Auslösen einer Genehmigungsanforderung verwendet wird, funktioniert die Genehmigungsrichtlinie möglicherweise nicht erwartungsgemäß. Wenn Sie eine Einstellung in einer Komponente ändern müssen, sollten Sie überprüfen, ob sich Ihre Einstellungen nicht auf eine oder mehrere Genehmigungsrichtlinien auswirken.

### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **Genehmigungsadministrator** an.

## Vorgehensweise

### 1 Angabe von Informationen zu Genehmigungsrichtlinien

Definieren Sie beim Erstellen einer Genehmigungsrichtlinie den Genehmigungsrichtlinientyp, den Namen, die Beschreibung und den Status.

### 2 Erstellen einer Genehmigungsebene

Beim Erstellen einer Genehmigungsrichtlinie können Sie Ebenen vor oder nach der Genehmigung hinzufügen.

### 3 Konfigurieren des Genehmigungsformulars zum Hinzufügen von Systemeigenschaften und benutzerdefinierten Eigenschaften

Sie können Systemeigenschaften und benutzerdefinierte Eigenschaften hinzufügen, die auf einem Genehmigungsformular angezeigt werden. Wenn Sie diese Eigenschaften hinzufügen, können die Genehmiger die Werte der Systemeigenschaften für die Einstellungen der Maschinenressourcen (zum Beispiel CPU, Lease oder Arbeitsspeicher) ändern, bevor sie eine Genehmigungsanforderung abschließen.

### 4 Einstellungen für Genehmigungsrichtlinien

Beim Erstellen einer Genehmigungsrichtlinie werden verschiedene Optionen konfiguriert, mittels derer festgelegt wird, wann ein von einem Servicekatalogbenutzer angefordertes Element genehmigt werden muss. Die Genehmigung kann erforderlich sein, bevor die Anforderung mit der Bereitstellung beginnt oder nachdem das Element bereitgestellt wurde, jedoch bevor es für den anfordernden Benutzer freigegeben wird.

## Angabe von Informationen zu Genehmigungsrichtlinien

Definieren Sie beim Erstellen einer Genehmigungsrichtlinie den Genehmigungsrichtlinientyp, den Namen, die Beschreibung und den Status.

## Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **Genehmigungsadministrator** an.

## Vorgehensweise

- 1 Wählen Sie **Administration > Genehmigungsrichtlinien** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.

### 3 Wählen Sie einen Richtlinienentyp oder eine Softwarekomponente aus.

Option	Beschreibung
<b>Richtlinientyp auswählen</b>	<p>Erstellen einer Genehmigungsrichtlinie auf Basis des Richtlinienanforderungstyps.</p> <p>Wählen Sie diese Option aus, um eine Genehmigungsrichtlinie zu definieren, die auf alle Katalogelemente dieses Typs anwendbar ist. Der Anforderungstyp kann eine allgemeine Anforderung, eine Katalogelementanforderung oder eine Ressourcenaktionsanforderung sein.</p> <p>Die verfügbaren Bedingungskonfigurationsoptionen variieren je nach Typ. Je spezifischer der Typ, desto spezifischer die Konfigurationsfelder. Beispiel: „Servicekatalog - Katalogelementanforderung“ gibt nur die Felder zurück, die allen Katalogelementen gemeinsam sind, während „Servicekatalog - Katalogelementanforderung - Virtuelle Maschine“ auch die gemeinsamen Optionen und die spezifischen Optionen für virtuelle Maschinen enthält.</p> <p>Der Anforderungstyp begrenzt die Anzahl der Katalogelemente oder Aktionen, auf die sich die Genehmigungsrichtlinie anwenden lässt.</p>
<b>Ein Element auswählen</b>	<p>Erstellen einer Genehmigungsrichtlinie auf Basis eines bestimmten Elements.</p> <p>Wählen Sie diese Option aus, um eine Genehmigungsrichtlinie zu definieren, die auf bestimmte Elemente anwendbar ist, die im Servicekatalog nicht als einzelne Elemente, sondern nur als Teil einer Maschine oder einer anderen Bereitstellung verfügbar sind (beispielsweise Softwarekomponenten).</p> <p>Die verfügbaren Bedingungskonfigurationsfelder sind elementspezifisch und können detaillierter sein als die für ein Richtlinienentypen-element angegebenen Kriterien.</p>
<b>Liste</b>	<p>Bietet eine Auflistung der verfügbaren Richtlinienentyp- oder Katalogelemente.</p> <p>Suche oder Sortierung der Spalten, um ein bestimmtes Element oder einen bestimmten Typ zu finden.</p>

### 4 Klicken Sie auf **OK**.

### 5 Geben Sie einen Namen und optional eine Beschreibung ein.

### 6 Wählen Sie den Status der Richtlinie im Dropdown-Menü **Status** aus.

Option	Beschreibung
<b>Entwurf</b>	Speichert die Genehmigungsrichtlinie in einem bearbeitbaren Status.
<b>Aktiv</b>	Speichert die Genehmigungsrichtlinie in einem schreibgeschützten Status, den Sie in einer Berechtigung verwenden können.
<b>Inaktiv</b>	Speichert die Genehmigungsrichtlinie in einem schreibgeschützten Status, den Sie erst in einer Berechtigung verwenden können, nachdem Sie die Richtlinie aktiviert haben.

#### Weiter

Erstellen der Genehmigungsebenen „Vor der Genehmigung“ und „Nach der Genehmigung“.

#### Erstellen einer Genehmigungsebene

Beim Erstellen einer Genehmigungsrichtlinie können Sie Ebenen vor oder nach der Genehmigung hinzufügen.

Sie können mehrere Genehmigungsebenen für eine Genehmigungsrichtlinie erstellen. Wenn ein Servicekatalogbenutzer ein Element anfordert, dem eine Genehmigungsrichtlinie mit mehreren Ebenen zugeordnet ist, muss die erste Ebene akzeptiert werden, bevor die Genehmigungsanforderung an den nächsten Genehmiger gesendet wird. Siehe [Arbeiten mit Genehmigungsrichtlinien](#).

## Voraussetzungen

[Angabe von Informationen zu Genehmigungsrichtlinien](#).

## Vorgehensweise

- 1 Klicken Sie auf der Registerkarte **Vor der Genehmigung** oder **Nach der Genehmigung** auf das Symbol **Neu** (+).
- 2 Geben Sie einen Namen und optional eine Beschreibung ein.
- 3 Wählen Sie eine Genehmigungsanforderung aus.

Option	Beschreibung
<b>Immer erforderlich</b>	Die Genehmigungsrichtlinie wird bei jeder Anforderung ausgelöst.
<b>Erforderlich basierend auf Bedingungen</b>	<p>Die Genehmigungsrichtlinie basiert auf einer oder mehreren Bedingungsklauseln. Bei Auswahl dieser Option müssen Sie die Bedingungen erstellen. Wenn diese Genehmigungsrichtlinie auf die entsprechenden Dienste, Katalogelemente oder Aktionen in einer Berechtigung angewendet wird, werden die Bedingungen ausgewertet. Treffen die Bedingungen zu, muss die Anforderung vor Ihrer Bereitstellung mit der Methode des angegebenen Genehmigers genehmigt werden. Treffen die Bedingungen nicht zu, wird die Anforderung bereitgestellt, ohne dass eine Genehmigung erforderlich ist. Zum Beispiel müssen alle Anforderungen einer virtuellen Maschine mit 4 oder mehr CPUs vom Administrator der virtuellen Infrastruktur genehmigt werden.</p> <p>Die Verfügbarkeit der Felder, die als Basis für die Bedingungen dienen sollen, hängt davon ab, welcher Genehmigungsrichtlinientyp oder welches Katalogelement ausgewählt wurde.</p> <p>Wird ein Wert für eine Bedingung eingegeben, wird bei den Werten die Groß- und Kleinschreibung berücksichtigt.</p> <p>Um mehr als eine Bedingungsklausel zu konfigurieren, wählen Sie für die Klauseln die Boolesche Operation aus.</p>

- 4 Wählen Sie die Genehmiger aus.

Option	Aktion
<b>Bestimmte Benutzer und Gruppen</b>	Sendet die Genehmigungsanforderung an die ausgewählten Benutzer.
<b>Genehmiger aus der Anforderung bestimmen</b>	Sendet die Genehmigungsanforderung an die Benutzer auf der Grundlage der definierten Bedingung.
<b>Ereignisabonnement verwenden</b>	<p>Verarbeitet die Genehmigungsanforderung auf der Grundlage definierter Ereignisabonnements.</p> <p>Das Workflow-Abonnement muss unter <b>Administration &gt; Ereignisse &gt; Abonnements</b> definiert werden. Die entsprechenden Workflow-Abonnements gelten vor und nach Genehmigung.</p>

## 5 Geben Sie an, wer die Anforderung oder die Aktion genehmigen muss.

Option	Beschreibung
<b>Jeder kann genehmigen</b>	Nur einer der Genehmiger muss genehmigen, bevor die Anforderung verarbeitet wird.  Wenn das Element im Servicekatalog angefordert wird, werden Genehmigungsanforderungen an alle Genehmiger gesendet. Wird die Anforderung von einem Genehmiger genehmigt, ist die Anforderung genehmigt und die Genehmigungsanforderung wird aus den Posteingängen der übrigen Genehmiger entfernt.
<b>Alle müssen genehmigen</b>	Alle der angegebenen Genehmiger müssen genehmigen, bevor die Anforderung verarbeitet wird.

## 6 Fügen Sie einem Genehmigungsformular Eigenschaften hinzu oder speichern Sie die Ebene.

- Um dem Genehmigungsformular Eigenschaften hinzuzufügen, klicken Sie auf **Systemeigenschaften** oder **Benutzerdefinierte Eigenschaften**.
- Zum Speichern der Ebene klicken Sie auf **OK**.

### Weiter

Informationen zum Hinzufügen von Eigenschaften zum Genehmigungsformular finden Sie unter [Konfigurieren des Genehmigungsformulars zum Hinzufügen von Systemeigenschaften und benutzerdefinierten Eigenschaften](#).

### Konfigurieren des Genehmigungsformulars zum Hinzufügen von Systemeigenschaften und benutzerdefinierten Eigenschaften

Sie können Systemeigenschaften und benutzerdefinierte Eigenschaften hinzufügen, die auf einem Genehmigungsformular angezeigt werden. Wenn Sie diese Eigenschaften hinzufügen, können die Genehmiger die Werte der Systemeigenschaften für die Einstellungen der Maschinenressourcen (zum Beispiel CPU, Lease oder Arbeitsspeicher) ändern, bevor sie eine Genehmigungsanforderung abschließen.

Die verfügbaren Systemeigenschaften richten sich nach dem Typ der Genehmigungsrichtlinie und danach, wie der Blueprint konfiguriert ist. Bei einigen Eigenschaften muss dem konfigurierten Feld im Blueprint ein Mindest- und ein Höchstwert hinzugefügt werden, bevor die Eigenschaft in der Liste der Systemeigenschaften angezeigt wird.

Benutzerdefinierte Eigenschaften können hinzugefügt werden, wenn Sie die Genehmigungsebene hinzufügen. Wenn eine benutzerdefinierte Eigenschaft konfiguriert und in einen Blueprint eingefügt wird, überschreiben die benutzerdefinierten Eigenschaften, die Sie dem Genehmigungsformular hinzufügen, alle anderen Instanzen dieser benutzerdefinierten Eigenschaft, beispielsweise in Blueprints, Eigenschaftengruppen oder Endpoints.

Der Genehmiger kann ausgewählte oder konfigurierte Eigenschaften im Genehmigungsformular ändern.

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **Genehmigungsadministrator** an.
- [Erstellen einer Genehmigungsebene](#).

## Vorgehensweise

- 1 Klicken Sie auf der Registerkarte **Vor der Genehmigung** oder **Nach der Genehmigung** auf das Symbol **Neu** (+).
- 2 Klicken Sie auf die Registerkarte **Systemeigenschaften**.
- 3 Aktivieren Sie das Kontrollkästchen für jede Systemeigenschaft, die der Genehmiger während des Genehmigungsprozesses konfigurieren soll.
- 4 Konfigurieren Sie die benutzerdefinierten Eigenschaften.

Fügen Sie eine oder mehrere benutzerdefinierte Eigenschaften hinzu, die der Genehmiger während des Genehmigungsprozesses konfigurieren soll.

- a Klicken Sie auf die Registerkarte **Benutzerdefinierte Eigenschaften**.
- b Klicken Sie auf das Symbol **Neu** (+).
- c Geben Sie die benutzerdefinierten Eigenschaftswerte ein.

Option	Beschreibung
<b>Name</b>	Eingabe des Eigenschaftsnamens.
<b>Bezeichnung</b>	Eingabe der Bezeichnung, die dem Genehmiger im Genehmigungsformular angezeigt wird.
<b>Beschreibung</b>	Eingabe der erweiterten Informationen für den Genehmiger. Diese Informationen werden im Formular als Feld-Tooltip angezeigt.

- d Klicken Sie auf **Speichern**.
  - e Zum Löschen mehrerer benutzerdefinierter Eigenschaften wählen Sie die entsprechenden Zeilen aus und klicken Sie auf **Löschen**.
- 5 Klicken Sie auf **OK**.

## Weiter

- Fügen Sie weitere Ebenen vor oder nach der Genehmigung hinzu.
- Speichern Sie die Genehmigungsrichtlinie. Die Richtlinie muss aktiv sein, damit sie auf Dienste, Elemente oder Aktionen in den **Berechtigungen** angewendet werden kann.

## Einstellungen für Genehmigungsrichtlinien

Beim Erstellen einer Genehmigungsrichtlinie werden verschiedene Optionen konfiguriert, mittels derer festgelegt wird, wann ein von einem Servicekatalogbenutzer angefordertes Element genehmigt werden muss. Die Genehmigung kann erforderlich sein, bevor die Anforderung mit der Bereitstellung beginnt oder nachdem das Element bereitgestellt wurde, jedoch bevor es für den anfordernden Benutzer freigegeben wird.

Wählen Sie **Administration > Genehmigungsrichtlinien** aus. Klicken Sie auf **Neu**.



- **Einstellungen für Genehmigungsrichtlinien-Typen**

Über den Genehmigungsrichtlinien-Typ wird festgelegt, wie die Genehmigungsrichtlinie konfiguriert wird und auf welche Elemente oder Aktionen sie sich in der Berechtigung anwenden lässt. Wenn Sie Genehmigungsebenen hinzufügen, wirkt sich der Richtlinientyp oder das Element darauf aus, welche Felder verfügbar sind, um Bedingungen für die Genehmigungsebenen zu schaffen.

- **Hinzufügen von Einstellungen für Genehmigungsrichtlinien**

Sie konfigurieren die grundlegenden Informationen zur Genehmigungsrichtlinie, einschließlich des Richtlinienstatus, damit Sie die Richtlinie verwalten können.

- **Hinzufügen von Ebeneninformationen zu Einstellungen für Genehmigungsrichtlinien**

Eine Genehmigungsebene enthält die Bedingungen, die einen Genehmigungsprozess auslösen, wenn der Servicekatalogbenutzer das Element anfordert, sowie Systemeigenschaften und benutzerdefinierte Eigenschaften, die Sie hinzufügen möchten. Wenn die Genehmigungsrichtlinie ausgelöst wird, werden die Genehmigungsanforderungen an die entsprechenden Genehmiger gesendet.

- **Hinzufügen von Systemeigenschaften zu Einstellungen für Genehmigungsrichtlinien**

Sie haben Systemeigenschaften ausgewählt, die Sie dem Genehmigungsformular hinzufügen möchten, und erlauben dem Genehmiger das Ändern des Werts.

- **Hinzufügen von benutzerdefinierten Eigenschaften zu Einstellungen für Genehmigungsrichtlinien**

Sie konfigurieren benutzerdefinierte Eigenschaften, die Sie dem Genehmigungsformular hinzufügen möchten, damit der Genehmiger den Wert ändern kann.

## **Einstellungen für Genehmigungsrichtlinien-Typen**

Über den Genehmigungsrichtlinien-Typ wird festgelegt, wie die Genehmigungsrichtlinie konfiguriert wird und auf welche Elemente oder Aktionen sie sich in der Berechtigung anwenden lässt. Wenn Sie Genehmigungsebenen hinzufügen, wirkt sich der Richtlinientyp oder das Element darauf aus, welche Felder verfügbar sind, um Bedingungen für die Genehmigungsebenen zu schaffen.

Wählen Sie **Administration > Genehmigungsrichtlinien** aus. Klicken Sie auf **Neu**.

**Tabelle 4-53. Optionen für Typen von Genehmigungsrichtlinien**

Option	Beschreibung
<b>Richtlinientyp auswählen</b>	<p>Erstellen einer Genehmigungsrichtlinie auf Basis des Richtlinientypen- oder Anforderungstyps.</p> <p>Wählen Sie diese Option aus, um eine Genehmigungsrichtlinie zu definieren, die auf alle Katalogelemente dieses Typs anwendbar ist. Der Anforderungstyp kann eine allgemeine Anforderung, eine Katalogelementanforderung oder eine Ressourcenaktionsanforderung sein.</p> <p>Die verfügbaren Bedingungskonfigurationsoptionen variieren je nach Typ. Je spezifischer der Typ, desto spezifischer die Konfigurationsfelder. Beispiel: „Servicekatalog - Katalogelementanforderung“ gibt nur die Felder zurück, die allen Katalogelementen gemeinsam sind, während „Servicekatalog - Katalogelementanforderung - Virtuelle Maschine“ auch die gemeinsamen Optionen und die spezifischen Optionen für virtuelle Maschinen enthält.</p> <p>Der Anforderungstyp begrenzt die Anzahl der Katalogelemente oder Aktionen, auf die sich die Genehmigungsrichtlinie anwenden lässt.</p>
<b>Ein Element auswählen</b>	<p>Erstellen einer Genehmigungsrichtlinie auf Basis eines bestimmten Elements.</p> <p>Wählen Sie diese Option aus, um eine Genehmigungsrichtlinie zu definieren, die auf bestimmte Elemente anwendbar ist, die im Servicekatalog nicht als einzelne Elemente, sondern nur als Teil einer Maschine oder einer anderen Bereitstellung verfügbar sind (beispielsweise Softwarekomponenten).</p> <p>Die verfügbaren Bedingungskonfigurationsoptionen sind element-spezifisch und können detaillierter sein als die für ein Richtlinientypen- oder Katalogelement angegebenen Kriterien.</p>
<b>Liste</b>	<p>Bietet eine Auflistung der verfügbaren Richtlinientyp- oder Katalogelemente.</p> <p>Suche oder Sortierung der Spalten, um ein bestimmtes Element oder einen bestimmten Typ zu finden.</p>

### Hinzufügen von Einstellungen für Genehmigungsrichtlinien

Sie konfigurieren die grundlegenden Informationen zur Genehmigungsrichtlinie, einschließlich des Richtlinienstatus, damit Sie die Richtlinie verwalten können.

Zum Definieren der grundlegenden Informationen für die Genehmigungsrichtlinie wählen Sie **Administration > Richtlinien** aus. Klicken Sie auf **Neu**. Wählen Sie den Richtlinientyp aus und klicken Sie auf **OK**.

**Tabelle 4-54. Optionen für Genehmigungsrichtlinien**

Option	Beschreibung
Name	Der Name, der angezeigt wird, wenn die Genehmigungsrichtlinie in einer Berechtigung angewendet wird.
Beschreibung	Geben Sie eine ausführliche Beschreibung für die Genehmigungsrichtlinie ein. Diese Informationen vereinfachen die Verwaltung Ihrer Genehmigungsrichtlinien.

**Tabelle 4-54. Optionen für Genehmigungsrichtlinien (Fortsetzung)**

Option	Beschreibung
Status	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>■ Entwurf. Die Genehmigungsrichtlinie kann nicht in Berechtigungen angewendet werden. Nach der Aktivierung einer Richtlinie kann sie nicht mehr auf den Entwurfsstatus zurückgesetzt werden.</li> <li>■ Aktiv. Die Genehmigungsrichtlinie kann in Berechtigungen angewendet werden.</li> <li>■ Inaktiv. Die Genehmigungsrichtlinie kann nicht in Berechtigungen angewendet werden. Wenn die Richtlinie nicht auf Berechtigungen angewendet wurde und von Ihnen deaktiviert wird, können Sie die Richtlinie zwar löschen, aber nicht erneut aktivieren. Wenn die Richtlinie angewendet wurde und von Ihnen deaktiviert wird, müssen die betreffenden Elemente mit einer anderen Richtlinie verknüpft werden, da die Elemente andernfalls nicht verknüpft sind. Nicht verknüpfte Elemente und Aktionen werden weiterhin Benutzern gewährt, aber sie weisen keine angewendete Genehmigungsrichtlinie auf.</li> </ul>
Richtlinientyp	<p>Zeigt den Anforderungstyp der Genehmigungsrichtlinie an. Wenn Sie ein Katalogelement als Basis für die Genehmigungsrichtlinie ausgewählt haben, wird der zugehörige Anforderungstyp angezeigt.</p>
Element	<p>Zeigt das ausgewählte Katalogelement an. Wenn Sie einen Anforderungstyp als Basis für die Genehmigungsrichtlinie ausgewählt haben, ist dieses Feld leer.</p>
Zuletzt aktualisiert von	<p>Der Name des Benutzers, der Änderungen an der Genehmigungsrichtlinie vorgenommen hat.</p>
Zuletzt aktualisiert am	<p>Das Datum der letzten Änderung an der Genehmigungsrichtlinie.</p>
Vor Genehmigung – Ebene	<p>Um eine Genehmigung anzufordern, bevor die angeforderten Elemente bereitgestellt oder die Aktionen ausgeführt werden, konfigurieren Sie eine oder mehrere Bedingungen, die einen Genehmigungsprozess auslösen, wenn der Servicekatalogbenutzer das Element anfordert.</p>

**Tabelle 4-54. Optionen für Genehmigungsrichtlinien (Fortsetzung)**

Option	Beschreibung
Nach Genehmigung – Ebene	Um eine Genehmigung anzufordern, nachdem das Element bereitgestellt wurde, aber bevor das bereitgestellte oder geänderte Element für den anfordernden Servicekatalogbenutzer freigegeben wird, konfigurieren Sie eine oder mehrere Bedingungen, die einen Genehmigungsprozess auslösen. Beispielsweise überprüft der Virtual Infrastructure-Administrator, ob die virtuelle Maschine einen funktionsfähigen Status aufweist, bevor sie für den Servicekatalogbenutzer freigegeben wird.
Verknüpfte Berechtigungen anzeigen	Zeigt alle Berechtigungen an, für die die Genehmigungsrichtlinie auf Dienste, Katalogelemente oder Aktionen angewendet wurde. Sie können die Elemente in einer Berechtigung mit einer anderen Richtlinie verknüpfen. Diese Option ist nur verfügbar, wenn Sie eine aktive Genehmigungsrichtlinie anzeigen.

### Hinzufügen von Ebeneninformationen zu Einstellungen für Genehmigungsrichtlinien

Eine Genehmigungsebene enthält die Bedingungen, die einen Genehmigungsprozess auslösen, wenn der Servicekatalogbenutzer das Element anfordert, sowie Systemeigenschaften und benutzerdefinierte Eigenschaften, die Sie hinzufügen möchten. Wenn die Genehmigungsrichtlinie ausgelöst wird, werden die Genehmigungsanforderungen an die entsprechenden Genehmiger gesendet.

Zum Definieren der grundlegenden Informationen für die Genehmigungsrichtlinie wählen Sie **Administration > Richtlinien** aus. Klicken Sie auf **Neu**. Wählen Sie den Richtlinientyp aus und klicken Sie auf **OK**. Klicken Sie auf der Registerkarte „Vor der Genehmigung“ oder „Nach der Genehmigung“ auf das Symbol **Neu (+)**.

Die Ebenen priorisieren Sie basierend auf der Reihenfolge, in der sie verarbeitet werden sollen. Wenn die Genehmigungsrichtlinie ausgelöst wird und die erste Genehmigungsebene abgelehnt wird, wird die Anforderung abgelehnt.

**Tabelle 4-55. Optionen für Ebeneninformationen**

Option	Beschreibung
Name	Geben Sie einen Namen ein. Der Name der Ebene wird beim Überprüfen von Anforderungen mit Genehmigungsrichtlinien angezeigt.
Beschreibung	Eingabe einer Ebenenbeschreibung. Beispiel: CPU>4 to VI Admin.
Wann ist eine Genehmigung erforderlich?	Auswählen, wann die Genehmigungsrichtlinie ausgelöst wird.

Tabelle 4-55. Optionen für Ebeneninformationen (Fortsetzung)

Option	Beschreibung
Immer erforderlich	<p>Die Genehmigungsrichtlinie wird bei jeder Anforderung ausgelöst.</p> <p>Wenn Sie diese Option auswählen und diese Genehmigungsrichtlinie auf die entsprechenden Dienste, Katalogelemente oder Aktionen in einer Berechtigung anwenden, muss die Anforderung vor Ihrer Bereitstellung mit der angegebenen Genehmigmethode genehmigt werden. Zum Beispiel müssen alle Anforderungen vom Manager des anfordernden Benutzers genehmigt werden.</p>
Erforderlich basierend auf Bedingungen	<p>Die Genehmigungsrichtlinie basiert auf einer oder mehreren Bedingungsklauseln.</p> <p>Bei Auswahl dieser Option müssen Sie die Bedingungen erstellen. Wenn diese Genehmigungsrichtlinie auf die entsprechenden Dienste, Katalogelemente oder Aktionen in einer Berechtigung angewendet wird, werden die Bedingungen ausgewertet. Treffen die Bedingungen zu, muss die Anforderung vor Ihrer Bereitstellung mit der Methode des angegebenen Genehmigers genehmigt werden. Treffen die Bedingungen nicht zu, wird die Anforderung bereitgestellt, ohne dass eine Genehmigung erforderlich ist. Zum Beispiel müssen alle Anforderungen einer virtuellen Maschine mit 4 oder mehr CPUs vom Administrator der virtuellen Infrastruktur genehmigt werden.</p> <p>Die Verfügbarkeit der Felder, die als Basis für die Bedingungen dienen sollen, hängt davon ab, welcher Genehmigungsrichtlinientyp oder welches Katalogelement ausgewählt wurde.</p> <p>Wird ein Wert für eine Bedingung eingegeben, wird bei den Werten die Groß- und Kleinschreibung berücksichtigt.</p> <p>Um mehr als eine Bedingungsklausel zu konfigurieren, wählen Sie für die Klauseln die Boolesche Operation aus.</p> <ul style="list-style-type: none"> <li>■ Alle folgenden Optionen. Die Genehmigung wird ausgelöst, wenn alle Klauseln zutreffen. Hierbei gibt es einen Booleschen UND-Operator zwischen jeder Klausel.</li> <li>■ Eine der folgenden Optionen. Die Genehmigungsebene wird ausgelöst, wenn mindestens eine der Klauseln zutrifft. Hierbei gibt es einen Booleschen ODER-Operator zwischen jeder Klausel.</li> <li>■ Nicht die folgende. Die Genehmigungsebene wird ausgelöst, wenn keine der Klauseln zutrifft. Hierbei gibt es einen Booleschen NICHT-Operator zwischen jeder Klausel.</li> </ul>
Genehmiger	Auswählen der Genehmigmethode.
Bestimmte Benutzer und Gruppen	<p>Sendet die Genehmigungsanforderung an die ausgewählten Benutzer.</p> <p>Wählen Sie die Benutzer oder Benutzergruppen aus, die die Servicekataloganforderung genehmigen müssen, bevor diese bereitgestellt wird oder eine Aktion ausgeführt wird. Beispiel: Die Anforderung wird bei Auswahl von <b>Jeder kann genehmigen</b> an die Administratorgruppe für die virtuelle Infrastruktur gesendet.</p>

**Tabelle 4-55. Optionen für Ebeneninformationen (Fortsetzung)**

Option	Beschreibung
<b>Benutzer aus der Anforderung bestimmen</b>	<p>Sendet die Genehmigungsanforderung an die Benutzer auf der Grundlage der definierten Bedingung.</p> <p>Beispiel: Wenn Sie diese Genehmigungsrichtlinie auf alle Business-Gruppen anwenden möchten und die Anforderung vom Business-Gruppenmanager genehmigt werden soll, wählen Sie <b>Business-Gruppe &gt; Verbraucher &gt; Benutzer &gt; Manager</b> aus.</p>
<b>Ereignisabonnement verwenden</b>	<p>Verarbeitet die Genehmigungsanforderung auf der Grundlage definierter Ereignisabonnements.</p> <p>Das Workflow-Abonnement muss unter <b>Administration &gt; Ereignisse &gt; Abonnements</b> definiert werden. Die entsprechenden Workflow-Abonnements gelten vor und nach Genehmigung.</p>
<b>Jeder kann genehmigen</b>	<p>Nur einer der Genehmiger muss genehmigen, bevor die Anforderung verarbeitet wird.</p> <p>Wenn das Element im Servicekatalog angefordert wird, werden Genehmigungsanforderungen an alle Genehmiger gesendet. Wird die Anforderung von einem Genehmiger genehmigt, ist die Anforderung genehmigt und die Genehmigungsanforderung wird aus den Posteingängen der übrigen Genehmiger entfernt.</p> <p>Wenn der erste Genehmiger die Anforderung ablehnt, wird der anfordernde Benutzer über die Ablehnung benachrichtigt und die Genehmigungsanforderung wird aus den Posteingängen der übrigen Genehmiger entfernt.</p> <p>Wenn der erste Genehmiger seine Genehmigung gibt und die Genehmigungsanforderung in der Konsole des zweiten Genehmigers offen ist, darf der Genehmiger die Genehmigungsanforderung nicht übermitteln, da davon ausgegangen wird, dass deren Bearbeitung durch die Antwort des ersten Genehmigers abgeschlossen wurde.</p> <p>Wenn Sie <b>Bestimmte Benutzer und Gruppen</b> oder <b>Genehmiger aus der Anforderung bestimmen</b> auswählen und es mehr als einen Genehmiger gibt, ist dies eine der zusätzlichen Optionen. Wenn es nur einen Genehmiger gibt, ist diese Option nicht anwendbar.</p>
<b>Alle müssen genehmigen</b>	<p>Alle der angegebenen Genehmiger müssen genehmigen, bevor die Anforderung verarbeitet wird.</p> <p>Wenn Sie <b>Bestimmte Benutzer und Gruppen</b> oder <b>Genehmiger aus der Anforderung bestimmen</b> auswählen und es mehr als einen Genehmiger gibt, ist dies eine der zusätzlichen Optionen. Wenn es nur einen Genehmiger gibt, ist diese Option nicht anwendbar.</p>

### Hinzufügen von Systemeigenschaften zu Einstellungen für Genehmigungsrichtlinien

Sie haben Systemeigenschaften ausgewählt, die Sie dem Genehmigungsformular hinzufügen möchten, und erlauben dem Genehmiger das Ändern des Werts.

Wählen Sie beispielsweise für die Genehmigung einer virtuellen Maschine „CPU“ aus, wenn Sie dem Genehmiger das Ändern einer Anforderung für 6 CPUs in 4 CPUs erlauben möchten.

Für die Auswahl von Systemeigenschaften wählen Sie **Administration > Richtlinien** aus. Klicken Sie auf **Neu**. Wählen Sie den Richtlinienotyp aus und klicken Sie auf **OK**. Klicken Sie auf der Registerkarte „Vor der Genehmigung“ oder „Nach der Genehmigung“ auf das Symbol **Neu (+)** und klicken Sie auf die Registerkarte **Systemeigenschaften**.

**Tabelle 4-56. Systemeigenschaften-Optionen**

Option	Beschreibung
<b>Eigenschaften</b>	<p>Die Liste der verfügbaren Systemeigenschaften hängt vom ausgewählten Anforderungstyp oder Katalogelement ab und davon, ob für das betreffende Element Systemeigenschaften vorhanden sind.</p> <p>Manche Eigenschaften sind nur verfügbar, wenn der Blueprint auf eine bestimmte Art und Weise konfiguriert ist (beispielsweise CPUs). Der Blueprint, auf den die Genehmigungsrichtlinie mit der CPU-Systemeigenschaft angewendet wird, muss als Bereich konfiguriert werden. Beispiel: Der CPU-Mindestwert beträgt 2, der Maximalwert 8.</p>

### Hinzufügen von benutzerdefinierten Eigenschaften zu Einstellungen für Genehmigungsrichtlinien

Sie konfigurieren benutzerdefinierte Eigenschaften, die Sie dem Genehmigungsformular hinzufügen möchten, damit der Genehmiger den Wert ändern kann.

Fügen Sie beispielsweise für die Genehmigung einer virtuellen Maschine

**VMware.VirtualCenter.Folder** hinzu, wenn Sie dem Genehmiger die Angabe des Ordners erlauben möchten, dem die Maschine in vCenter Server hinzugefügt wird.

Sie können auch eine benutzerdefinierte Eigenschaft speziell für dieses Genehmigungsrichtlinienformular hinzufügen.

Für die Auswahl von Systemeigenschaften wählen Sie **Administration > Richtlinien** aus. Klicken Sie auf **Neu**. Wählen Sie den Richtlinienotyp aus und klicken Sie auf **OK**. Klicken Sie auf der Registerkarte „Vor der Genehmigung“ oder „Nach der Genehmigung“ auf das Symbol **Neu (+)** und klicken Sie auf die Registerkarte **Benutzerdefinierte Eigenschaften**.

**Tabelle 4-57. Benutzerdefinierte Eigenschaften**

Option	Beschreibung
<b>Name</b>	Eingabe des Eigenschaftsnamens.
<b>Bezeichnung</b>	Eingabe der Bezeichnung, die dem Genehmiger im Genehmigungsformular angezeigt wird.
<b>Beschreibung</b>	<p>Eingabe der erweiterten Informationen für den Genehmiger.</p> <p>Diese Informationen werden im Formular als Feld-Tooltip angezeigt.</p>

## Ändern einer Genehmigungsrichtlinie

Sie können eine aktive oder inaktive Genehmigungsrichtlinie nicht ändern. Sie müssen eine Kopie der Originalrichtlinie erstellen und die Richtlinie ersetzen, die nicht die erforderlichen Ergebnisse erbringt. Aktive und inaktive Genehmigungsrichtlinien sind schreibgeschützt. Genehmigungsrichtlinien im Entwurfsstatus können geändert werden.


Wenn Sie eine Kopie der Genehmigungsrichtlinie erstellen, basiert die neue Richtlinie auf dem Typ der Originalrichtlinie. Sie können alle Attribute außer dem Richtlinientyp bearbeiten. Bearbeitungen nehmen Sie vor, wenn Sie die Genehmigungsebenen zum Ändern, Hinzufügen oder Entfernen von Ebenen ändern oder System- bzw. benutzerdefinierte Eigenschaften zu den Formularen hinzufügen möchten.

Sie können Ebenen vor und nach der Genehmigung erstellen. Anweisungen zum Erstellen einer Genehmigungsebene finden Sie unter [Erstellen einer Genehmigungsebene](#).

### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **Genehmigungsadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Genehmigungsrichtlinien** aus.
- 2 Wählen Sie die Zeile der zu kopierenden Genehmigungsrichtlinie aus.
- 3 Klicken Sie auf das Symbol **Kopieren** .
 

Es wird eine Kopie der Genehmigungsrichtlinie erstellt.
- 4 Wählen Sie die neue zu bearbeitende Genehmigungsrichtlinie aus.
- 5 Geben Sie im Textfeld **Name** einen Namen ein.
- 6 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.
- 7 Wählen Sie den Status der Richtlinie im Dropdown-Menü **Status** aus.

Option	Beschreibung
<b>Entwurf</b>	Speichert die Genehmigungsrichtlinie in einem bearbeitbaren Status.
<b>Aktiv</b>	Speichert die Genehmigungsrichtlinie in einem schreibgeschützten Status, den Sie in einer Berechtigung verwenden können.
<b>Inaktiv</b>	Speichert die Genehmigungsrichtlinie in einem schreibgeschützten Status, den Sie erst in einer Berechtigung verwenden können, nachdem Sie die Richtlinie aktiviert haben.

- 8 Erstellen Sie die Ebenen vor und nach der Genehmigung.
- 9 Klicken Sie auf **OK**.

Sie haben eine neue Genehmigungsrichtlinie basierend auf einer vorhandenen Genehmigungsrichtlinie erstellt.



## Weiter

Wenden Sie die neue Genehmigungsrichtlinie in einer Berechtigung an. Siehe [Erteilen der Berechtigung für Dienste, Katalogelemente und Aktionen](#).

## Deaktivieren einer Genehmigungsrichtlinie

Wenn Sie feststellen, dass eine Genehmigungsrichtlinie veraltet ist, können Sie die Richtlinie deaktivieren, damit sie während der Bereitstellung nicht verfügbar ist.

Zum Deaktivieren einer Genehmigungsrichtlinie müssen Sie für jede Berechtigung, auf die die Genehmigungsrichtlinie aktuell angewendet wird, eine neue Richtlinie zuweisen.

Später können Sie eine deaktivierte Genehmigungsrichtlinie erneut aktivieren oder aber löschen.

### Voraussetzungen

Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **Genehmigungsadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Genehmigungsrichtlinien** aus.
- 2 Klicken Sie auf den Namen der Genehmigungsrichtlinie.
- 3 Klicken Sie auf **Verknüpfte Berechtigungen anzeigen**.
  - a Wählen Sie im Dropdown-Menü **Alle ersetzen durch** die neue Genehmigungsrichtlinie aus.

Enthält die Liste mehr als eine Berechtigung, wird die neue Genehmigungsrichtlinie auf alle aufgelisteten Berechtigungen angewendet.
  - b Klicken Sie auf **OK**.
- 4 Nachdem Sie überprüft haben, dass keine Berechtigungen mit der Genehmigungsrichtlinie verknüpft sind, wählen Sie im Dropdown-Menü „Status“ die Option **Inaktiv** aus.
- 5 Klicken Sie auf **OK**.
- 6 Um eine Genehmigungsrichtlinie zu löschen, wählen Sie die Zeile aus, die die inaktive Richtlinie enthält.
  - a Klicken Sie auf **Löschen**.
  - b Klicken Sie auf **OK**.

Die Verknüpfung der Genehmigungsrichtlinie mit Berechtigungen, in denen sie verwendet wird, wird entfernt und die Genehmigungsrichtlinie wird deaktiviert. Die Genehmigungsrichtlinie können Sie später erneut aktivieren und erneut auf Elemente in einer Berechtigung anwenden.

## Weiter

Falls Sie die Genehmigungsrichtlinie nicht mehr benötigen, können Sie sie löschen. Siehe [Löschen einer Genehmigungsrichtlinie](#).

## Löschen einer Genehmigungsrichtlinie

Wenn Genehmigungsrichtlinien vorhanden sind, die Sie deaktiviert haben und nicht mehr benötigen, können Sie sie aus vRealize Automation löschen.

### Voraussetzungen

- Sie müssen die Verknüpfung von Genehmigungsrichtlinien entfernen und sie deaktivieren. Siehe [Deaktivieren einer Genehmigungsrichtlinie](#).
- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **Genehmigungsadministrator** an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Genehmigungsrichtlinien** aus.
- 2 Wählen Sie die Zeile aus, die die inaktive Richtlinie enthält.
- 3 Klicken Sie auf **Löschen**.
- 4 Klicken Sie auf **OK**.

Die Genehmigungsrichtlinie wird gelöscht.

## Szenario: Konfigurieren des Katalogs für Rainpole-Architekten zum Testen von Blueprints

Mit Ihren Mandantenadministratorrechten erstellen Sie einen speziellen Katalogdienst, der sehr wenig Kontrolle enthält, in dem Ihre Rainpole-Architekten ihre Arbeit effizient testen können, bevor Blueprints in Ihre Produktionsumgebung exportiert werden. Sie erstellen einen Blueprint-Test-Dienst, fügen den CentOS-Blueprint von vSphere zum Dienst hinzu und erteilen Ihren Rainpole-Architekten die Berechtigung für alle Katalogelemente und für alle Aktionen, die mit dem Dienst verbunden sind, sodass Ihre Architekten ihre Arbeit überprüfen können, indem Katalogelemente bereitgestellt werden.



### Vorgehensweise

#### 1 [Szenario: Erstellen eines Katalogdiensts für Rainpole – Blueprint-Tests](#)

Mit Ihren Mandantenadministratorrechten erstellen Sie einen Katalogdienst namens Rainpole-Dienst. Sie weisen sich selbst als Besitzer und Support-Kontakt für diesen Dienst zu, sodass sich Ihre Rainpole-Architekten mit allen Problemen an Sie wenden können.

## 2 Szenario: Hinzufügen Ihres vSphere CentOS-Katalogelements zum Rainpole-Dienst

Mit Ihren Mandantenadministratorrechten fügen Sie den veröffentlichten Blueprint Ihrer vSphere CentOS-Maschine zum Rainpole-Dienst hinzu.

## 3 Szenario: Erteilen der Berechtigung für Ihre Rainpole-Architekten für das Anfordern von Katalogelementen

Mit Ihren Mandantenadministratorrechten erteilen Sie Ihren Rainpole-Architekten die Berechtigung für alle Aktionen und Elemente, die zum Rainpole-Dienst gehören.

## Szenario: Erstellen eines Katalogdiensts für Rainpole – Blueprint-Tests

Mit Ihren Mandantenadministratorrechten erstellen Sie einen Katalogdienst namens Rainpole-Dienst. Sie weisen sich selbst als Besitzer und Support-Kontakt für diesen Dienst zu, sodass sich Ihre Rainpole-Architekten mit allen Problemen an Sie wenden können.

### Vorgehensweise

- 1 Wählen Sie **Administration > Katalogmanagement > Services** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Geben Sie den Namen **Rainpole-Dienst** ein.
- 4 Wählen Sie im Dropdown-Menü „Status“ die Option **Aktiv** aus.
- 5 Verwenden Sie als Mandantenadministrator, der den Dienst erstellt, die Suchoption, um sich selbst als Besitzer und Supportteam hinzuzufügen.
- 6 Klicken Sie auf **OK**.

### Weiter

Mit Ihren Mandantenadministratorrechten fügen Sie den veröffentlichten Blueprint Ihrer vSphere CentOS-Maschine zum Rainpole-Dienst hinzu.

## Szenario: Hinzufügen Ihres vSphere CentOS-Katalogelements zum Rainpole-Dienst

Mit Ihren Mandantenadministratorrechten fügen Sie den veröffentlichten Blueprint Ihrer vSphere CentOS-Maschine zum Rainpole-Dienst hinzu.

Alle veröffentlichten Blueprints, die Sie bereitstellen möchten, müssen als Katalogelement Teil eines Diensts sein, aber jeder Blueprint kann nur ein Katalogelement in jeweils einem Dienst sein. Wenn Sie Ihren Blueprint in mehreren Katalogdiensten gleichzeitig veröffentlichen müssen, erstellen Sie Kopien Ihres Blueprints.

### Vorgehensweise

- 1 Wählen Sie **Administration > Katalogmanagement > Services** aus.
- 2 Wählen Sie in der Liste „Services“ die Zeile „Blueprint Testing“ aus und klicken Sie auf **Katalogelemente verwalten**.

3 Klicken Sie auf das Symbol **Neu** (+).

4 Aktivieren Sie das Kontrollkästchen **CentOS in vSphere**.

Nur veröffentlichte Blueprints und Komponenten, die noch keinem Dienst zugewiesen sind, werden in der Liste angezeigt. Wenn der Blueprint nicht angezeigt wird, stellen Sie sicher, dass er veröffentlicht wurde oder dass er nicht Bestandteil eines anderen Diensts ist.

5 Klicken Sie auf **OK**.

6 Klicken Sie auf **Schließen**.

#### Weiter

Mit Ihren Mandantenadministratorrechten erteilen Sie Ihren Rainpole-Architekten die Berechtigung, Katalogelemente vom Rainpole-Dienst abzurufen.

### Szenario: Erteilen der Berechtigung für Ihre Rainpole-Architekten für das Anfordern von Katalogelementen

Mit Ihren Mandantenadministratorrechten erteilen Sie Ihren Rainpole-Architekten die Berechtigung für alle Aktionen und Elemente, die zum Rainpole-Dienst gehören.

Indem Sie Ihren Rainpole-Architekten die Berechtigung für alle Aktionen und Elemente im Dienst erteilen, ist es einfacher für diese, neue Katalogelemente dem Dienst zu Testzwecken hinzuzufügen. In einer Produktionsumgebung verwenden Sie möglicherweise Berechtigungen unterschiedlich und konfigurieren eine strenge Kontrolle. Sie möchten möglicherweise verwalten, welche Katalogelemente jeder Benutzer anfordern darf und welche Aktionen sie für bestimmte Katalogelemente ausführen können, die sie besitzen.

#### Vorgehensweise

1 Wählen Sie **Administration > Katalogmanagement > Berechtigungen** aus.

2 Klicken Sie auf das Symbol **Neu** (+).

3 Konfigurieren Sie die Details.

- a Geben Sie den Namen **Berechtigung für Rainpole-Architekt** ein.
- b Wählen Sie aus dem Dropdown-Menü **Status** den Eintrag **Aktiv** aus.
- c Wählen Sie im Dropdown-Menü **Business-Gruppe** Ihre Rainpole-Business-Gruppe aus.
- d Fügen Sie Ihre Rainpole-Architekten unter Verwendung des Suchfelds **Benutzer und Gruppen** hinzu.
- e Klicken Sie auf **Weiter**.

#### 4 Erteilen Sie die Berechtigung für den Rainpole-Katalogdienst.

- a Klicken Sie auf das Symbol **Services hinzufügen** (+) neben der Überschrift „Berechtigte Services“.
- b Wählen Sie **Rainpole-Dienst** aus.
- c Klicken Sie auf **OK**.

Alle Benutzer, die Sie der Berechtigung hinzugefügt haben, sind jetzt für alle Katalogelemente im Rainpole-Dienst berechtigt.

#### 5 Gewähren Sie Berechtigungen für alle Benutzeraktionen.

- a Klicken Sie auf das Symbol **Aktionen hinzufügen** (+) neben der Überschrift „Berechtigte Aktionen“.
- b Aktivieren Sie das Kontrollkästchen in der Spaltenüberschrift, um Berechtigungen für alle Aktionen zu gewähren.
- c Aktivieren Sie das Kontrollkästchen **Aktionen gelten nur für die in dieser Berechtigung definierten Elemente**, damit Sie später eine strengere Kontrolle über diese Benutzer in anderen Katalogdiensten ausüben können.
- d Klicken Sie auf **OK**.

Ihre Architekten sind berechtigt, alle anwendbaren Aktionen in Katalogelementen auszuführen, die sie aus Ihrem Rainpole-Dienst bereitstellen. Sie sind nicht berechtigt, diese Aktionen in Elementen auszuführen, die sie möglicherweise aus einem anderen Dienst oder über eine andere Berechtigung bereitstellen.

#### 6 Klicken Sie auf **Beenden**.

Alle Ihre Architekten können jetzt den CentOS-Maschinen-Blueprint von vSphere und alle neuen Katalogelemente anzeigen und anfordern, die zu ihrem Dienst hinzugefügt wurden.

#### Weiter

Fordern Sie mit dem von Ihnen eingerichteten lokalen Benutzerkonto die Bereitstellung des CentOS-Katalogelements von vSphere an, um den Blueprint und die Katalogkonfiguration zu testen.

## Szenario: Testen der Rainpole-CentOS-Maschine

Sie fordern mit dem von Ihnen erstellten lokalen Testbenutzerkonto an, die CentOS-Maschine vSphere bereitzustellen. Sie melden sich bei der bereitgestellten Maschine an und vergewissern sich, dass sie wie erwartet funktioniert.



## Vorgehensweise

### 1 Szenario: Anfordern der virtuellen Rainpole-Maschine

Sie fordern mit Ihrem Testbenutzerkonto das Servicekatalogelement an, um CentOS auf der virtuellen vSphere-Maschine bereitzustellen.

### 2 Szenario: Anmelden bei der bereitgestellten Rainpole-Maschine

Melden Sie sich mit dem Testbenutzerkonto bei der erfolgreich bereitgestellten CentOS-Maschine von vSphere an.

## Szenario: Anfordern der virtuellen Rainpole-Maschine

Sie fordern mit Ihrem Testbenutzerkonto das Servicekatalogelement an, um CentOS auf der virtuellen vSphere-Maschine bereitzustellen.

### Vorgehensweise

- 1 Melden Sie sich bei der vRealize Automation-Konsole ab.
- 2 Melden Sie sich erneut mit dem Benutzernamen **test\_user** und dem Kennwort **VMware1!** an.
- 3 Klicken Sie auf die Registerkarte **Katalog**.
- 4 Klicken Sie auf die Schaltfläche **Anforderung**, um ein Katalogelement anzufordern.
- 5 Geben Sie **Funktionalität überprüfen** in das Textfeld **Beschreibung** ein.
- 6 Klicken Sie auf **Einreichen**, um das Katalogelement anzufordern.
- 7 Klicken Sie auf die Registerkarte **Anforderungen**, um den Status Ihrer Anforderung zu überwachen.

Nach erfolgreicher Bereitstellung der Maschine wird die Statusmeldung **Erfolgreich** angezeigt.

### Weiter

Melden Sie sich bei der bereitgestellten Maschine an.

## Szenario: Anmelden bei der bereitgestellten Rainpole-Maschine

Melden Sie sich mit dem Testbenutzerkonto bei der erfolgreich bereitgestellten CentOS-Maschine von vSphere an.

### Vorgehensweise

- 1 Wählen Sie **Elemente > Maschinen** aus.

- 2 Wählen Sie den Pfeil neben CentOS auf dem vSphere-Element aus.  
Die bereitgestellte Maschine wird unter dem erweiterten Element angezeigt.
- 3 Klicken Sie auf die bereitgestellte Maschine.
- 4 Klicken Sie im rechten Fensterbereich auf **Remote bei der Maschine anmelden**.
- 5 Melden Sie sich bei der Maschine an.

Sie haben vRealize Automation in einer Minimalbereitstellung installiert, einen Proof-of-Concept eingerichtet und die Umgebung für eine fortlaufende Entwicklung von Blueprints konfiguriert.

#### Weiter

- Wenn Sie eine vRealize Automation Enterprise-Lizenz erworben haben, können Sie hier weiterlesen, um weitere Informationen über die Bereitstellung von Maschinen mit Softwarekomponenten zu erhalten.
- Planen Sie die Installation einer Produktionsumgebung. Siehe *Referenzarchitektur*.
- Mehr über weitere Optionen zum Konfigurieren von vRealize Automation, zum Entwerfen und Exportieren von Blueprints und zum Verwalten Ihres Servicekatalogs. Siehe *Konfigurieren von vRealize Automation*.

## Szenario: Den Anwendungs-Blueprint vom Typ „CentOS mit MySQL“ im Servicekatalog verfügbar machen

Als Mandantenadministrator haben Sie verlangt, dass die Blueprint-Architekten ein Katalogelement erstellen, um virtuelle Maschinen vom Typ „MySQL unter CentOS“ zur Ausführung von Testfällen für Ihre Entwicklungs- und Qualitätsingenieurgruppe bereitzustellen. Der Softwarearchitekt hat Sie darüber informiert, dass das Katalogelement für die Benutzer bereit steht. Um das Element für die Unternehmensbenutzer zur Verfügung zu stellen, müssen Sie die Blueprints und die Software-Komponente einem Katalogdienst zuordnen und anschließend den Mitgliedern der Business-Gruppe die Berechtigung zum Anfordern des Katalogelements erteilen.

#### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** oder **Katalogadministrator** an.
- Veröffentlichen Sie einen Blueprint, um virtuelle „MySQL unter vSphere CentOS“-Maschinen bereitzustellen. Siehe [Szenario: Zusammenfügen und Testen eines Blueprints zur Bereitstellung von MySQL auf Rainpole-verknüpften Klon-Maschinen](#).
- Wenn Sie Blueprints in einer Entwicklungsumgebung erstellen, importieren Sie Ihren Blueprint in Ihre Produktionsumgebung. Siehe [Exportieren und Importieren von Blueprints](#).
- Erstellen Sie eine Reservierung, um vSphere-Ressourcen Ihrer Dev- und QE-Business-Gruppe zuzuteilen. Siehe [Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer](#).

## Vorgehensweise

### 1 Szenario: Erstellen des Katalogdiensts „Dev and QE Service“

Als Mandantenadministrator möchten Sie einen separaten Katalogdienst für Ihre Entwicklungs- und Qualitätssicherungsabteilung erstellen, damit Ihre anderen Abteilungen wie z. B. die Finanz- und Personalabteilungen die speziellen Katalogelemente nicht sehen. Sie erstellen einen Katalogdienst mit dem Namen „Dev and QE Service“, um alle Katalogelemente zu veröffentlichen, die die Entwicklungs- und Qualitätssicherungsabteilung für das Ausführen der Testfälle benötigt.

### 2 Szenario: Hinzufügen von CentOS mit MySQL zu Ihrem Dev- und QE-Service

Als Mandantenadministrator möchten Sie das Katalogelement „CentOS mit MySQL“ zum Dev- und QE-Service hinzufügen.

### 3 Szenario: Erteilen von Berechtigungen für Benutzer zum Anfordern von „Dev and QE Service“-Elementen als ein Katalogelement

Als Mandantenadministrator erstellen Sie eine „Dev and QE“-Berechtigung und fügen die Katalogelemente und einige relevante Aktionen hinzu, damit Ihre Benutzer in der Entwicklungs- und Qualitätssicherungsabteilung das Katalogelement „CentOS with MySQL“ anfordern und Aktionen für die Maschine und die Bereitstellung ausführen können.

## Szenario: Erstellen des Katalogdiensts „Dev and QE Service“

Als Mandantenadministrator möchten Sie einen separaten Katalogdienst für Ihre Entwicklungs- und Qualitätssicherungsabteilung erstellen, damit Ihre anderen Abteilungen wie z. B. die Finanz- und Personalabteilungen die speziellen Katalogelemente nicht sehen. Sie erstellen einen Katalogdienst mit dem Namen „Dev and QE Service“, um alle Katalogelemente zu veröffentlichen, die die Entwicklungs- und Qualitätssicherungsabteilung für das Ausführen der Testfälle benötigt.

## Vorgehensweise

- 1 Wählen Sie **Administration > Katalogmanagement > Services** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Geben Sie den Namen **Dev and QE Service** im Textfeld **Name** ein.
- 4 Geben Sie die Beschreibung **Dev and QE application catalog items for test cases** im Textfeld **Beschreibung** ein.
- 5 Wählen Sie aus dem Dropdown-Menü **Status** den Eintrag **Aktiv** aus.
- 6 Als Katalogadministrator, der den Dienst erstellt, fügen Sie mithilfe der Suchoption Ihren Namen als Besitzer hinzu.
- 7 Fügen Sie die benutzerdefinierte Benutzergruppe „Support-Team“ hinzu.

Fügen Sie beispielsweise eine benutzerdefinierte Benutzergruppe hinzu, die die IaaS-Architekten und Software-Architekten enthält, sodass Sie und die Servicekatalogbenutzer über jemanden verfügen, an den Sie sich wenden können, wenn es bei der Bereitstellung der Katalogelemente zu Problemen kommen sollte.



## 8 Klicken Sie auf **OK**.

Sie haben einen Katalogdienst „Dev and QE“ erstellt und aktiviert, aber er enthält noch keine Katalogelemente.

### Szenario: Hinzufügen von CentOS mit MySQL zu Ihrem Dev- und QE-Service

Als Mandantenadministrator möchten Sie das Katalogelement „CentOS mit MySQL“ zum Dev- und QE-Service hinzufügen.

#### Vorgehensweise

- 1 Wählen Sie **Administration > Katalogmanagement > Services** aus.
- 2 Wählen Sie die Zeile „Dev- und QE-Service“ in der Liste **Services** aus und klicken Sie auf **Katalogelemente verwalten**.
- 3 Klicken Sie auf das Symbol **Neu (+)**.
- 4 Wählen Sie **CentOS mit MySQL** aus.  
  
Nur veröffentlichte Blueprints und Komponenten, die noch keinem Dienst zugewiesen sind, werden in der Liste angezeigt. Wenn der Blueprint nicht angezeigt wird, stellen Sie sicher, dass er veröffentlicht wurde oder dass er nicht Bestandteil eines anderen Diensts ist.
- 5 Klicken Sie auf **OK**.
- 6 Klicken Sie auf **Schließen**.

Sie haben das Katalogelement „CentOS mit MySQL“ für den Dev- und QE-Service veröffentlicht. Benutzer können das Element jedoch erst dann anzeigen oder anfordern, wenn Sie ihnen Berechtigungen für das Element oder den Service erteilt haben.

### Szenario: Erteilen von Berechtigungen für Benutzer zum Anfordern von „Dev and QE Service“-Elementen als ein Katalogelement

Als Mandantenadministrator erstellen Sie eine „Dev and QE“-Berechtigung und fügen die Katalogelemente und einige relevante Aktionen hinzu, damit Ihre Benutzer in der Entwicklungs- und Qualitätssicherungsabteilung das Katalogelement „CentOS with MySQL“ anfordern und Aktionen für die Maschine und die Bereitstellung ausführen können.

In diesem Szenario erteilen Sie dem Dienst Berechtigungen, weil die Benutzer Berechtigungen für alle zukünftigen Katalogelemente haben sollen, die diesem Dienst hinzugefügt werden. Darüber hinaus möchten Sie es Ihren Benutzern erlauben, ihre zur Verfügung gestellte Bereitstellung zu verwalten. Deshalb fügen Sie der Berechtigung Aktionen wie das Ein- und Ausschalten, das Erstellen von Snapshots und das Löschen der Bereitstellung hinzu.

#### Vorgehensweise

- 1 Wählen Sie **Administration > Katalogmanagement > Berechtigungen** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.

### 3 Konfigurieren Sie die Details.

- a Geben Sie den Namen **Dev and QE Entitlement** im Textfeld **Name** ein.
- b Wählen Sie im Dropdown-Menü **Status** die Option **Aktiv** aus.
- c Wählen Sie im Dropdown-Menü **Business-Gruppe** die Gruppe **Dev and QE** aus.
- d Fügen Sie im Bereich „Benutzer und Gruppen“ einen oder mehrere Benutzer hinzu.

Fügen Sie sich selbst nur hinzu, wenn Sie sicher sind, dass der Blueprint erwartungsgemäß funktioniert. Wenn dies der Fall ist, können Sie einzelne Benutzer und benutzerdefinierte Benutzergruppen hinzufügen.

- e Klicken Sie auf **Weiter**.

### 4 Fügen Sie den Dienst hinzu.

Obwohl Sie die CentOS- und MySQL-Katalogelemente separat hinzufügen, wird durch das Hinzufügen des Diensts sichergestellt, dass alle Elemente, die Sie dem Dienst zu einem späteren Zeitpunkt hinzufügen, für die Mitglieder der Business-Gruppe im Servicekatalog verfügbar sind.

- a Klicken Sie auf das Symbol **Services hinzufügen** (+) neben der Überschrift „Berechtigte Services“.
- b Wählen Sie **Dev and QE Service** aus.
- c Klicken Sie auf **OK**.

„Dev and QE Service“ wird zur Liste „Berechtigte Services“ hinzugefügt.

## 5 Fügen Sie Aktionen hinzu.

- a Klicken Sie auf das Symbol **Aktionen hinzufügen** (+) neben der Überschrift „Berechtigte Aktionen“.
- b Klicken Sie auf die Spaltenüberschrift „Typ“, um die Liste zu sortieren.

Wählen Sie die folgenden Aktionen basierend auf dem Typ aus. Diese Aktionen sind hilfreich für die Benutzer in der Entwicklungs- und Qualitätssicherungsabteilung, die mit den Testmaschinen arbeiten. Dies sind die einzigen Aktionen, die diese Business-Gruppenmitglieder verwenden sollen.

Typ	Aktionsname
Maschine	Einschalten
Maschine	Ausschalten
Virtuelle Maschine	Snapshot erstellen
Virtuelle Maschine	Snapshot wiederherstellen
Bereitstellung	Löschen Mit der Aktion zum Löschen der Bereitstellung wird nicht nur die virtuelle Maschine, sondern die gesamte Bereitstellung gelöscht.

- c Klicken Sie auf **OK**.

Diese fünf Aktionen werden zur Liste „Berechtigte Aktionen“ hinzugefügt.

## 6 Klicken Sie auf **Beenden**.

Damit haben Sie das Katalogelement „CentOS with MySQL“ zu Ihrem neuen Katalogdienst „Dev and QE“ hinzugefügt und den Mitgliedern der Business-Gruppe die Berechtigung zum Anfordern und Verwalten des Elements erteilt.

### Weiter

Nachdem Sie Ihre Arbeit durch Bereitstellen des Katalogelements „CentOS with MySQL“ überprüft haben, können Sie der Berechtigung zusätzliche Benutzer hinzufügen, um das Katalogelement für Ihre Benutzer in der Entwicklungs- und Qualitätssicherungsabteilung öffentlich verfügbar zu machen. Wenn Sie die Bereitstellung von Ressourcen in Ihrer Umgebung noch stärker kontrollieren möchten, können Sie Genehmigungsrichtlinien für die MySQL-Software-Komponente und die Maschine „CentOS für Softwaretests“ erstellen. Siehe [Szenario: Erstellen und Anwenden von CentOS with MySQL-Genehmigungsrichtlinien](#).

## Szenario: Erstellen und Anwenden von CentOS with MySQL-Genehmigungsrichtlinien

Als Mandantenadministrator für die Entwicklungs- und Qualitätssicherungsabteilung möchten Sie Anforderungen von Katalogelementen streng kontrollieren. Bevor Ihre Benutzer das CentOS with MySQL-Katalogelement bereitstellen können, muss Ihr vSphere Virtual Infrastructure-Administrator die Maschinenanforderung genehmigen und Ihr Softwaremanager muss die Softwareanforderung genehmigen.

Sie erstellen also eine Genehmigungsrichtlinie für die vSphere CentOS with MySQL-Servicekataloganforderung und wenden sie an, um die Genehmigung durch einen vSphere Virtual Infrastructure-Administrator basierend auf bestimmten Bedingungen einzuholen. Sie erstellen außerdem eine weitere Genehmigungsrichtlinie für die MySQL-Software-Komponente, um die Genehmigung durch Ihren Softwaremanager für jede Anforderung einzuholen.

Genehmigungsadministratoren können nur die Genehmigungen erstellen. Ein Business-Gruppenmanager kann diese dann auf Berechtigungen anwenden. Als Mandantenadministrator können Sie die Genehmigungen sowohl erstellen als auch auf Berechtigungen anwenden.

### Voraussetzungen

- Melden Sie sich bei der vRealize Automation-Konsole als **Mandantenadministrator** an. Nur ein Mandantenadministrator kann Genehmigungsrichtlinien sowohl erstellen als auch anwenden.
- Stellen Sie sicher, dass das CentOS with MySQL-Katalogelement in einem Dienst enthalten ist. Siehe [Szenario: Den Anwendungs-Blueprint vom Typ „CentOS mit MySQL“ im Servicekatalog verfügbar machen](#).

### Vorgehensweise

#### 1 [Szenario: Erstellen einer Genehmigungsrichtlinie für eine virtuelle CentOS-Maschine mit MySQL](#)

Als Mandantenadministrator möchten Sie sicherzustellen, dass die Gruppe für Entwicklung und Qualitätstechnik virtuelle Maschinen erhält, die in Ihrer Umgebung angemessen bereitgestellt sind. Daher erstellen Sie eine Genehmigungsrichtlinie, die eine vorherige Genehmigung für Anforderungen erfordert, welche bestimmte Anforderungen erfüllen.

#### 2 [Szenario: Erstellen einer Genehmigungsrichtlinie für MySQL-Softwarekomponenten](#)

Als Mandantenadministrator wurden Sie von Ihren Softwaremanagern gebeten, Genehmigungsrichtlinien für MySQL-Installationen zu erstellen und anzuwenden, um die Lizenznutzung nachzuverfolgen. Sie erstellen eine Richtlinie, um den Softwarelizenzmanager zu benachrichtigen, sobald die Softwarekomponente „MySQL for Linux Virtual Machines“ angefordert wird.

#### 3 [Szenario: Anwenden von Genehmigungsrichtlinien auf CentOS mit MySQL-Komponenten](#)

Sie können als der Mandantenadministrator Genehmigungsrichtlinien und Berechtigungen erstellen. Sie ändern die Berechtigung „Dev and QE“, um die Genehmigungsrichtlinien anzuwenden, die Sie erstellt haben, sodass Genehmigungen ausgelöst werden, wenn ein Benutzer des Servicekatalogs das Element anfordert.

## Szenario: Erstellen einer Genehmigungsrichtlinie für eine virtuelle CentOS-Maschine mit MySQL

Als Mandantenadministrator möchten Sie sicherzustellen, dass die Gruppe für Entwicklung und Qualitätstechnik virtuelle Maschinen erhält, die in Ihrer Umgebung angemessen bereitgestellt sind. Daher erstellen Sie eine Genehmigungsrichtlinie, die eine vorherige Genehmigung für Anforderungen erfordert, welche bestimmte Anforderungen erfüllen.

Da die virtuelle CentOS-Maschine mit MySQL vCenter Server-Ressourcen belegt, soll der Administrator der virtuellen vSphere-Infrastruktur Anforderungen genehmigen, wenn der angeforderte Arbeitsspeicher mehr als 2048 MB bzw. mehr als 2 CPUs beträgt, um sicherzustellen, dass die Ressourcen vernünftig belegt werden. Sie geben dem Genehmiger auch die Möglichkeit, die angeforderten CPU- und Arbeitsspeicherwerte vor der Genehmigung einer Anforderung zu ändern.

### Vorgehensweise

- 1 Wählen Sie **Administration > Genehmigungsrichtlinien** aus.
- 2 Erstellen Sie eine Genehmigungsrichtlinie für die Bereitstellung von virtuellen Maschinen.

- a Klicken Sie auf das Symbol **Neu (+)**.
- b Wählen Sie **Richtlinientyp auswählen** aus.
- c Wählen Sie in der Liste **Servicekatalog - Katalogelementanforderung - Virtuelle Maschine** aus.
- d Klicken Sie auf **OK**.
- e Konfigurieren Sie die folgenden Optionen:

Option	Konfiguration
<b>Name</b>	Geben Sie <b>CentOS auf vSphere CPU oder Arbeitsspeicher VM</b> ein.
<b>Beschreibung</b>	Geben Sie <b>Erfordert VI-Admin-Genehmigung für CPU&gt;2 oder Arbeitsspeicher&gt;2048</b> ein.
<b>Status</b>	Wählen Sie <b>Aktiv</b> aus.

- 3 Klicken Sie auf der Registerkarte **Vor der Genehmigung** auf das Symbol **Hinzufügen (+)**.
- 4 Konfigurieren Sie die Registerkarte **Ebeneninformationen** mit den Auslöserkriterien und den Genehmigungsaktionen.
  - a Geben Sie im Textfeld **Name CPU>2 oder Arbeitsspeicher>2048 – VI-Admin** ein.
  - b Geben Sie im Textfeld **Beschreibung VI-Admin-Genehmigung für CPU und Arbeitsspeicher** ein.
  - c Wählen Sie **Erforderlich basierend auf Bedingungen** aus.
  - d Wählen Sie in der Dropdown-Liste „Klausel“ **Eine der folgenden Optionen** aus.
  - e Wählen Sie in der neuen Dropdown-Liste „Klausel“ den Eintrag **CPUs** aus und konfigurieren Sie die Klausel mit den Werten **CPU > 2**.
  - f Klicken Sie auf **Ausdruck hinzufügen** und konfigurieren Sie die Klausel mit den Werten **Arbeitsspeicher (MB) > 2048**.
  - g Wählen Sie **Bestimmte Benutzer und Gruppen** aus.
  - h Geben Sie den Namen des Administrators für virtuelle vSphere-Infrastruktur bzw. der Administratorgruppe in das Suchtextfeld ein und klicken Sie auf das Suchsymbol (🔍).

- i Wählen Sie den Benutzer oder die Gruppe aus.
- j Wählen Sie **Jeder kann genehmigen** aus.

Für die Genehmigung ist nur ein Administrator für virtuelle Infrastruktur erforderlich, um die Ressourcen zu überprüfen und die Anforderung zu genehmigen.

- 5 Klicken Sie auf die Registerkarte **Systemeigenschaften** und wählen Sie die Eigenschaften aus, mit denen der Genehmiger die angeforderten CPU- und Arbeitsspeicherwerte vor der Genehmigung einer Anforderung ändern kann.
  - a Aktivieren Sie die Kontrollkästchen **CPUs** und **Arbeitsspeicher (MB)**.
  - b Klicken Sie auf **OK**.

- 6 Klicken Sie auf **OK**.

Sie haben eine Genehmigungsrichtlinie für Anforderungen virtueller Maschinen erstellt, müssen aber noch eine Genehmigung für die MySQL-Komponente erstellen. Genehmigungen werden erst ausgelöst, nachdem Sie die Richtlinien auf eine Berechtigung angewendet haben.

## Szenario: Erstellen einer Genehmigungsrichtlinie für MySQL- Softwarekomponenten

Als Mandantenadministrator wurden Sie von Ihren Softwaremanagern gebeten, Genehmigungsrichtlinien für MySQL-Installationen zu erstellen und anzuwenden, um die Lizenznutzung nachzuverfolgen. Sie erstellen eine Richtlinie, um den Softwarelizenzmanager zu benachrichtigen, sobald die Softwarekomponente „MySQL for Linux Virtual Machines“ angefordert wird.

Diese Art von Genehmigung ist möglicherweise in manchen Umgebungen erforderlich, da Lizenzschlüssel vom Softwaremanager bereitgestellt werden müssen. In diesem Szenario muss nur der Softwaremanager die Anforderung nachverfolgen und genehmigen. Nachdem Sie die Genehmigungsrichtlinie erstellt haben, wenden Sie die Richtlinie auf das Katalogelement „MySQL for Linux Virtual Machines“ an. Diese Genehmigungsrichtlinie ist sehr spezifisch und kann nur auf die Softwarekomponente „MySQL for Linux Virtual Machines“ in den Berechtigungen angewendet werden.

### Vorgehensweise

- 1 Wählen Sie **Administration > Genehmigungsrichtlinien** aus.
- 2 Erstellen Sie eine Genehmigungsrichtlinie für die MySQL-Softwarekomponente.
  - a Klicken Sie auf das Symbol **Neu (+)**.
  - b Wählen Sie **Ein Element auswählen** aus.
  - c Wählen Sie **MySQL for Linux Virtual Machines** aus.

- d Klicken Sie auf **OK**.
- e Konfigurieren Sie die folgenden Optionen:

Option	Konfiguration
Name	Geben Sie <b>MySQL tracking approval</b> ein.
Beschreibung	Geben Sie <b>Approval request sent to software manager</b> ein.
Status	Wählen Sie <b>Aktiv</b> aus.

- 3 Klicken Sie auf der Registerkarte **Vor der Genehmigung** auf das Symbol **Hinzufügen (+)**.
- 4 Konfigurieren Sie die Registerkarte **Ebeneninformationen** mit den Auslöserkriterien und den Genehmigungsaktionen.
  - a Geben Sie im Feld **Name** die Zeichenfolge **MySQL software deployment notice** ein.
  - b Geben Sie im Feld **Beschreibung** die Zeichenfolge **Software mgr approval of software installation** ein.
  - c Wählen Sie **Immer erforderlich** aus.
  - d Wählen Sie **Bestimmte Benutzer und Gruppen** aus.
  - e Geben Sie im Suchtextfeld den Namen des Softwaremanagers ein, klicken Sie auf das Suchsymbol (🔍) und wählen Sie den Benutzer aus.
  - f Wählen Sie **Jeder kann genehmigen** aus.

Für diese Anforderung ist nur ein Softwaremanager zum Genehmigen der Anforderung erforderlich.

Klicken Sie auf **OK**.

- 5 Klicken Sie auf **OK**.

Sie haben die Genehmigungsrichtlinien für virtuelle Maschinen und für die Softwarekomponente „MySQL for Linux Virtual Machines“ erstellt. Genehmigungen werden erst ausgelöst, nachdem Sie die Genehmigungsrichtlinien auf eine Berechtigung angewendet haben.

## Szenario: Anwenden von Genehmigungsrichtlinien auf CentOS mit MySQL-Komponenten

Sie können als der Mandantenadministrator Genehmigungsrichtlinien und Berechtigungen erstellen. Sie ändern die Berechtigung „Dev and QE“, um die Genehmigungsrichtlinien anzuwenden, die Sie erstellt haben, sodass Genehmigungen ausgelöst werden, wenn ein Benutzer des Servicekatalogs das Element anfordert.

Es mag zwar einfacher sein, Ihrer Business-Gruppe die Berechtigung für den gesamten Katalogdienst zu erteilen, allerdings haben Sie dann nicht dieselbe Kontrolle wie beim Erstellen einzelner Berechtigungen für Katalogelemente. Wenn Sie beispielsweise Benutzern die Berechtigung für einen Dienst erteilen, können sie alle in diesem Dienst enthaltenen Katalogelemente sowie alle Elemente, die dem Dienst in Zukunft hinzugefügt werden, anfordern. Dies bedeutet auch, dass Sie nur sehr allgemeine Genehmigungs-

richtlinien verwenden können, die für jedes Katalogelement des Diensts gelten, wie beispielsweise immer die Genehmigung von einem Manager anzufordern. Wenn Sie die Berechtigung für Katalogelemente einzeln erteilen, können Sie für jedes Element ganz spezielle Genehmigungsrichtlinien erstellen und anwenden und genau kontrollieren, wer welche Elemente in dem Dienst anfordern kann. Wenn Sie die Berechtigung für die einzelnen Komponenten von Katalogelementen erteilen, haben Sie sogar noch mehr Kontrolle.

Wenn Sie nicht wissen, welche Genehmigungsrichtlinien Sie auf Elemente in einer Berechtigung anwenden möchten, können Sie zu einem späteren Zeitpunkt zurückkehren und sie anwenden. In diesem Szenario wenden Sie unterschiedliche Genehmigungsrichtlinien auf zwei Komponenten desselben veröffentlichten Anwendungs-Blueprints an.

### Vorgehensweise

- 1 Wählen Sie **Administration > Katalogmanagement > Berechtigungen** aus.
- 2 Klicken Sie auf die **Berechtigung „Dev and QE“**.
- 3 Klicken Sie auf die Registerkarte **Elemente und Genehmigungen**.
- 4 Fügen Sie CentOS mit der MySQL-Maschine hinzu und wenden Sie die Genehmigungsrichtlinie an.
  - a Klicken Sie auf das Symbol **Elemente hinzufügen** (+) neben der Überschrift „Berechtigte Elemente“.
  - b Aktivieren Sie das Kontrollkästchen **CentOS mit MySQL**.
  - c Klicken Sie auf den Dropdown-Pfeil **Diese Richtlinie auf ausgewählte Elemente anwenden**.  
Die Richtlinie „CentOS on vSphere CPU and Memory“ ist nicht in der Liste aufgeführt.
  - d Klicken Sie auf **Alle anzeigen** und anschließend auf den Pfeil nach unten, um alle Genehmigungsrichtlinien anzuzeigen.
  - e Wählen Sie **CentOS on vSphere CPU and Memory [Servicekatalog – Katalogelementanforderung – Virtuelle Maschine]** aus.  
Die vSphere CentOS-Maschine ist ein Maschinen-Blueprint in einem Anwendungs-Blueprint. Überprüfen Sie die Richtliniennamen, damit Sie die für Ihren Katalogelementtyp passende Richtlinie auswählen. Wenn Sie die falsche Richtlinie anwenden, schlägt die Genehmigungsrichtlinie fehl oder löst Genehmigungsanfragen basierend auf falschen Bedingungen aus.
  - f Klicken Sie auf **OK**.
- 5 Fügen Sie MySQL für die Softwarekomponente der virtuellen Linux-Maschine als ein Element hinzu und wenden Sie eine Genehmigungsrichtlinie auf das MySQL-Element an.
  - a Klicken Sie auf das Symbol **Katalogelemente und Komponenten hinzufügen** (+) neben der Überschrift „Berechtigte Katalogelemente und Komponenten“.
  - b Wählen Sie **Nein** aus dem Dropdown-Menü **Katalogelemente und Komponenten** aus.  
Softwarekomponenten sind immer mit einer Maschine verbunden. Sie sind nicht für individuelle Anforderungen im Servicekatalog verfügbar.



- c Aktivieren Sie das Kontrollkästchen **MySQL für virtuelle Linux-Maschinen**.
- d Klicken Sie auf den Dropdown-Pfeil **Diese Richtlinie auf ausgewählte Elemente anwenden**.
- e Wählen Sie **MySQL tracking approval [Servicekatalog – Katalogelementanforderung – Softwarekomponente]** aus.

Sie benötigen die erweiterte Option nicht, da die Genehmigungsrichtlinie für diese spezielle Softwarekomponente erstellt wurde, die einer virtuellen Maschine hinzugefügt wird.

- f Klicken Sie auf **OK**.

## 6 Fügen Sie Aktionen hinzu, die die Benutzer auf der bereitgestellten Maschine ausführen können.

Genehmigungsrichtlinien werden nicht auf Aktionen in diesem Szenario angewendet.

- a Klicken Sie auf das Symbol **Aktionen hinzufügen** (+) neben der Überschrift „Berechtigte Aktionen“.
- b Wählen Sie die folgenden Aktionen aus.

Name / Typ	Beschreibung
<b>Snapshot erstellen / Virtuelle Maschine</b>	Erstellt einen Snapshot der virtuellen Maschine, einschließlich der installierten Software. Ermöglicht den Entwicklern, Snapshots zu erstellen, auf die sie bei der Entwicklung wiederherstellen können.
<b>Löschen / Bereitstellung</b>	Löscht den gesamten bereitgestellten Blueprint, nicht nur die Maschine. Verwenden Sie diese Aktion, um verwaiste Komponenten zu vermeiden.
<b>Ausschalten / Maschine</b>	Schaltet die virtuelle Maschine aus.
<b>Einschalten / Maschine</b>	Schaltet die virtuelle Maschine ein.
<b>Auf Snapshot wiederherstellen / Virtuelle Maschine</b>	Stellt auf den zuvor erstellten Snapshot wieder her.

- c Klicken Sie auf **OK**.

## 7 Klicken Sie auf **Beenden**.

Diese Berechtigung ermöglicht es Ihnen, verschiedene Genehmigungen auf unterschiedlichen Blueprint-Komponenten anzufordern.

### Weiter

Fordern Sie CentOS mit dem MySQL-Element im Servicekatalog als ein Mitglied der Business-Gruppe an, um sicherzustellen, dass sich die Berechtigung und die Genehmigungen wie erwartet verhalten.