

Konfigurieren von vRealize Automation

28. Dezember 2020

vRealize Automation 7.4

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

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

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

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

Copyright © 2015-2020 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise.](#)

Inhalt

Konfigurieren von vRealize Automation 6

Aktualisierte Informationen 7

1 Externe Vorbereitungen für die Blueprint-Bereitstellung 8

- Vorbereiten Ihrer Umgebung für die Verwaltung durch vRealize Automation 8
 - Checkliste für das Vorbereiten der NSX-Netzwerk- und -Sicherheitskonfiguration 10
 - Checkliste für die Unterstützung eines externen IPAM-Anbieters 15
 - Prüfliste für die Konfiguration von Container für vRealize Automation 19
 - Vorbereiten Ihrer vCloud Director-Umgebung für vRealize Automation 20
 - Vorbereiten Ihrer vCloud Air-Umgebung für vRealize Automation 21
 - Vorbereiten Ihrer Amazon AWS-Umgebung 21
 - Vorbereiten von Netzwerk- und Sicherheitsfunktionen für Red Hat OpenStack 29
 - Vorbereiten Ihrer SCVMM-Umgebung 29
- Konfigurieren der Netzwerk-zu-Azure-VPC-Konnektivität 30
- Vorbereiten für Maschinenbereitstellung 32
 - Auswählen einer vorzubereitenden Methode zur Maschinenbereitstellung 32
 - Checkliste für die Ausführung von Visual Basic-Skripts während der Bereitstellung 36
 - Verwenden des vRealize Automation-Gast-Agent bei der Bereitstellung 38
 - Checkliste für das Vorbereiten für die Bereitstellung durch Klonen 46
 - Vorbereiten für die vCloud Air- und vCloud Director-Bereitstellung 63
 - Vorbereiten für die Linux Kickstart-Bereitstellung 64
 - Vorbereiten für SCCM-Bereitstellung 67
 - Vorbereiten für die WIM-Bereitstellung 69
 - Vorbereiten für die Image-Bereitstellung der virtuellen Maschine 77
 - Vorbereiten für die Bereitstellung von Amazon-System-Images 77
 - Szenario: Vorbereiten von vSphere -Ressourcen für Maschinenbereitstellung in Rainpole 80
- Vorbereiten für Software-Bereitstellung 83
 - Vorbereiten der Bereitstellung von Maschinen mit Software 84
 - Szenario: Vorbereiten einer vSphere CentOS-Vorlage für Klonmaschinen- und Softwarekomponenten-Blueprints 88
 - Szenario: Vorbereiten auf den Import des vSphere-Beispielanwendungs-Blueprints „Dukes Bank“ 92

2 Vorbereitungen für Mandanten und Ressourcen für die Bereitstellung von Blueprints 98

- Konfigurieren der Mandanteneinstellungen 98
 - Auswählen der Verzeichnisverwaltungs-Konfigurationsoptionen 99

Durchführen eines Upgrades von externen Konnektoren für die Verzeichnisverwaltung	174
Szenario: Konfigurieren eines Active Directory-Links für hochverfügbare vRealize Automation-Bereitstellung	183
Konfigurieren von externen Konnektoren für Smartcard- und Drittanbieter-Identitätsanbieter-Authentifizierung in vRealize Automation	185
Erstellen eines Links für Active Directory mit mehreren Domänen oder mit mehreren Gesamtstrukturen	193
Konfigurieren von Gruppen und Benutzerrollen	196
Erstellen weiterer Mandanten	203
Löschen eines Mandanten	205
Konfigurieren von Sicherheitseinstellungen für mehrere Mandanten	206
Konfigurieren des benutzerdefinierten Brandings	206
Checkliste für die Konfiguration von Benachrichtigungen	209
Erstellen einer benutzerdefinierten RDP-Datei zur Unterstützung von RDP-Verbindungen für bereitgestellte Maschinen	221
Szenario: Hinzufügen von Datacenter-Standorten für regionsübergreifende Bereitstellungen	222
Konfigurieren von vRealize Orchestrator	223
Konfigurieren von Ressourcen	229
Checkliste für die Konfiguration von IaaS-Ressourcen	229
Konfigurieren von XaaS-Ressourcen	371
Erstellen und Konfigurieren von Containern	386
Installieren zusätzlicher Plug-Ins auf dem vRealize Orchestrator-Standardserver	407
Arbeiten mit Active Directory-Richtlinien	407
Benutzereinstellungen für Benachrichtigungen und Stellvertretungen	411

3 Bereitstellen von Dienst-Blueprints für Benutzer 413

Entwerfen von Blueprints	413
Erstellen Ihrer Design-Bibliothek	416
Entwerfen von Maschinen-Blueprints	419
Entwerfen von Software-Komponenten	527
Entwerfen von XaaS-Blueprints und Ressourcenaktionen	542
Veröffentlichen eines Blueprints	612
Arbeiten mit von Entwicklern gesteuerten Blueprints	613
Exportieren und Importieren von Blueprints und Inhalten	613
Herunterladen und Konfigurieren des bereitgestellten eigenständigen Blueprints	620
Erstellen von Blueprints und anderem IaaS-Inhalt in einer Umgebung mit mehreren Entwicklern	620
Erstellen zusammengesetzter Blueprints	621
Grundlegendes zum Verhalten von verschachtelten Blueprints	623
Verwenden von Maschinenkomponenten und Software-Komponenten beim Zusammenfügen von Blueprints	627
Erstellen von Eigenschaftsbindungen zwischen Blueprint-Komponenten	628
Erstellen von Abhängigkeiten und Steuern der Bereitstellungsreihenfolge	629

Anpassen von Blueprint-Anforderungsformularen	631
Erstellen eines benutzerdefinierten Anforderungsformulars mit Active Directory-Optionen	634
Benutzerdefinierte Formulardesigner-Feldeigenschaften	641
Verwenden von vRealize Orchestrator-Aktionen im Designer für benutzerdefinierte Formulare	647
Verwenden des Datenrasterelements im Designer für benutzerdefinierte Formulare	649
Verwenden der externen Validierung im Designer für benutzerdefinierte Formulare	652
Verwalten des Servicekatalogs	656
Checkliste für die Konfiguration des Servicekatalogs	657
Erstellen eines Diensts	658
Arbeiten mit Katalogelementen und Aktionen	661
Erstellen von Berechtigungen	664
Arbeiten mit Genehmigungsrichtlinien	673
Anfordern der Maschinenbereitstellung mit einem parametrisierten Blueprint	704
Szenario: Den Anwendungs-Blueprint vom Typ „CentOS mit MySQL“ im Servicekatalog verfügbar machen	706
Verwalten von bereitgestellten Katalogelementen	710
Ausführen von Aktionen für bereitgestellte Ressourcen	711
Angaben von Einstellungen für die Neukonfiguration von Maschinen und Überlegungen bei der Neukonfiguration	738
Erneutes Konfigurieren eines Lastausgleichsdiensts in einer Bereitstellung	746
Ändern von NAT-Regeln in einer Bereitstellung	748
Hinzufügen oder Entfernen von Sicherheitselementen in einer Bereitstellung	750
Anzeigen aller NAT-Regeln für einen vorhandenen NSX Edge	751

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.

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 Datencentern 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
16. November 2018	Geringfügige Änderungen.
5. Oktober 2018	Geringfügige Änderungen.
15. Juni 2018	<ul style="list-style-type: none">■ Konfigurieren einer OpenLDAP Directory-Verbindung wurde aktualisiert■ Der Abschnitt Verzeichnisverwaltung für Hochverfügbarkeit konfigurieren wurde aktualisiert und der Abschnitt Aktivieren der Verzeichnissynchronisierung auf einem sekundären Connector wurde hinzugefügt, um weitere Informationen zum Arbeiten mit Konnektoren in einer Hochverfügbarkeitskonfiguration (HA, High Availability) bereitzustellen.■ Erstellen eines Puppet-Endpoints wurde aktualisiert.■ Geringfügige Änderungen.
3. Mai 2018	<ul style="list-style-type: none">■ Geringfügige Änderungen.■ Informationen zu Von Azure unterstützte Regionen wurden hinzugefügt.
12. April 2018	Erstversion.

Externe Vorbereitungen für die Blueprint-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 enthält die folgenden Themen:

- [Vorbereiten Ihrer Umgebung für die Verwaltung durch vRealize Automation](#)
- [Konfigurieren der Netzwerk-zu-Azure-VPC-Konnektivität](#)
- [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
	<p>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 Checkliste für das Vorbereiten der NSX-Netzwerk- und -Sicherheitskonfiguration.</p>
 vCloud Director	<p>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 Vorbereiten Ihrer vCloud Director-Umgebung für vRealize Automation.</p>
 vCloud Air	<p>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 Vorbereiten für die vCloud Air- und vCloud Director-Bereitstellung.</p>
 Amazon AWS	<p>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 Vorbereiten Ihrer Amazon AWS-Umgebung.</p>
Microsoft Azure	<p>Konfigurieren des Netzwerks zur Verwendung von VPN-Tunneln zwecks Unterstützung von Softwarekomponenten auf Azure-Blueprints. Siehe Konfigurieren der Netzwerk-zu-Azure-VPC-Konnektivität.</p>
 Red Hat OpenStack	<p>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 Vorbereiten von Netzwerk- und Sicherheitsfunktionen für Red Hat OpenStack.</p>

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

Umgebung	Vorbereitungen
 SCVMM	Konfigurieren Sie den Speicher und das Netzwerk und machen Sie sich mit den Einschränkungen bei der Namensgebung von Vorlagen- und Hardwareprofilen vertraut. Siehe Vorbereiten Ihrer SCVMM-Umgebung .
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 Checkliste für die Unterstützung eines externen IPAM-Anbieters .
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 Vorbereiten für Maschinenbereitstellung .

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.

Ab vRealize Automation 7.3 brauchen Sie das NSX-Plug-In nicht mehr zu installieren, um integrierte NSX-Funktionalität zu erhalten. Die gesamte integrierte NSX-Funktionalität wird nun direkt aus den NSX-APIs und nicht mehr aus dem NSX-Plug-In bezogen. Wenn Sie jedoch XaaS zum Erweitern Ihrer Integration von vRealize Automation und NSX verwenden möchten, müssen Sie das NSX-Plug-In in vRealize Orchestrator wie hier beschrieben installieren.

Bei der Vorbereitung für die Verwendung der Netzwerk-, Sicherheits- und Lastausgleichsdienstfunktionen von NSX in vRealize Automation unter Verwendung von NSX-Manager-Anmeldedaten müssen Sie das NSX-Manager-Administratorkonto verwenden.

Weitere Informationen zu NSX finden Sie in der NSX-Dokumentation unter https://www.vmware.com/support/pubs/nsx_pubs.html sowie in öffentlichen Blogs und Artikeln wie zum Beispiel [Integrieren von NSX in vRealize Automation](#).

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 für vRealize Automation-Blueprints konfigurierbaren NSX-Einstellungen 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"/> 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-Lastausgleichseinstellungen.	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> .
<input type="checkbox"/> Stellen Sie für Cross-vCenter-Bereitstellungen sicher, dass der NSX Manager über die Rolle des primären NSX Manager verfügt.	Für die Bereitstellung von vRealize Automation benötigt der NSX Manager für die Region, in der sich die Maschinen befinden, die Rolle des primären NSX Manager.	Siehe Administratoranforderungen für die Bereitstellung von globalen NSX-Objekten . Informationen zur Cross-vCenter-Bereitstellung, zu globalen Objekten und zur Rolle des primären NSX Manager finden Sie im <i>Installationshandbuch für NSX</i> und im <i>Administratorhandbuch für NSX</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.

Allgemeine Informationen zum Plug-In-Update und zur Fehlerbehebung finden Sie in der vRealize Orchestrator-[Dokumentation](#).

Voraussetzungen

Ab vRealize Automation 7.3 brauchen Sie das NSX-Plug-In nicht mehr zu installieren, um integrierte NSX-Funktionalität zu erhalten. Die gesamte integrierte NSX-Funktionalität wird nun direkt aus den NSX-APIs und nicht mehr aus dem NSX-Plug-In bezogen. Wenn Sie jedoch XaaS zum Erweitern Ihrer Integration von vRealize Automation und NSX verwenden möchten, müssen Sie das NSX-Plug-In in vRealize Orchestrator wie hier beschrieben installieren.

Wenn Sie einen eingebetteten vRealize Orchestrator verwenden, der bereits ein installiertes NSX-Plug-In enthält, können Sie diesen Vorgang überspringen.

- 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 den vRealize Orchestrator-Client installiert haben und dass Sie sich mit Administratoranmeldedaten anmelden können.
- Vergewissern Sie sich anhand der vRealize Automation-[Support-Matrix](#), dass die Version des NSX-Plug-Ins korrekt ist.

Verfahren

- 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 `o11nplugin-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.

Nächste Schritte

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.

Verfahren

- 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.

Ergebnisse

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.

Nächste Schritte

Wenden Sie die entsprechenden Sicherheitsfunktionen für den Blueprint an.

Administratoranforderungen für die Bereitstellung von globalen NSX-Objekten

Zur Bereitstellung von Maschinen in einer Cross-vCenter NSX-Umgebung bei Verwendung von globalen NSX-Objekten müssen Sie die Bereitstellung in einem vCenter vornehmen, in dem der NSX-Computing-Manager die primäre Rolle einnimmt.

In einer Cross-vCenter NSX-Umgebung können Sie mehrere vCenter Server haben, denen jeweils ein eigener NSX Manager zugeordnet werden muss. Einem NSX Manager wird die Rolle des primären NSX Manager zugewiesen, die übrigen erhalten die Rolle eines sekundären NSX Manager.

Der primäre NSX Manager kann globale Objekte wie etwa globale logische Switches erstellen. Diese Objekte werden mit den sekundären NSX Managern synchronisiert. Sie können diese Objekte von einem sekundären NSX Manager anzeigen lassen, können diese dort jedoch nicht bearbeiten. Zur Verwaltung globaler Objekte müssen Sie den primären NSX Manager verwenden. Der primäre NSX Manager kann für die Konfiguration von jedem beliebigen sekundären NSX Manager in der Umgebung verwendet werden.

Weitere Informationen zur Cross-vCenter NSX-Umgebung finden Sie unter *Übersicht über Cross-vCenter Networking and Security* im *Administratorhandbuch für NSX* in der [Produktdokumentation zu NSX](#).

Bei einem vSphere (vCenter)-Endpoint, der dem NSX-Endpoint eines primären NSX Managers zugeordnet ist, unterstützt vRealize Automation lokale NSX-Objekte, wie lokale logische Switches, lokale Edge-Gateways sowie lokale Lastausgleichsmodule, Sicherheitsgruppen und Sicherheits-Tags. Es unterstützt auch 1:1- und 1:n-NAT-Netzwerke mit globaler Transportzone, geroutete Netzwerke mit globaler Transportzone und universelle verteilte logische Router (DLRs) sowie einen Lastausgleichsdienst in Verbindung mit jedem beliebigen Netzwerktyp.

vRealize Automation unterstützt keine universellen vorhandenen oder bedarfsgesteuerten NSX-Sicherheitsgruppen oder -Tags.

Verwenden Sie zum Bereitstellen lokaler bedarfsgesteuerter Netzwerke als primärer NSX Manager eine vCenter-spezifische lokale Transportzone. Für vRealize Automation-Reservierungen können Sie konfigurieren, dass die lokale Transportzone und virtuelle Verbindungen für Bereitstellungen in diesem lokalen vCenter verwendet werden.

Wenn Sie einen vSphere (vCenter)-Endpoint mit einem entsprechenden sekundären NSX Manager-Endpoint verbinden, können Sie nur lokale Objekte bereitstellen und verwenden.

Sie können einen NSX-Endpoint nur einem vSphere-Endpoint zuordnen. Die Zuordnungseinschränkung bedeutet, dass Sie kein universelles bedarfsgesteuertes Netzwerk bereitstellen und es an vSphere-Maschinen anhängen können, die auf verschiedenen vCentern bereitgestellt wurden.

vRealize Automation kann einen universellen logischen NSX-Switch als externes Netzwerk verwenden. Wenn ein universeller Switch vorhanden ist, wird er zum Erfassen von Daten verwendet und dann an jede virtuelle Maschine in der Bereitstellung angehängt oder von jeder dieser virtuellen Maschinen belegt.

- Durch Bereitstellen eines bedarfsgesteuerten Netzwerks in einer universellen Transportzone kann ein neuer universeller logischer Switch erstellt werden.
- Durch Bereitstellen eines bedarfsgesteuerten Netzwerks in einer universellen Transportzone auf dem primären NSX Manager wird ein neuer universeller logischer Switch erstellt.
- Das Bereitstellen eines bedarfsgesteuerten Netzwerks in einer universellen Transportzone auf einem sekundären NSX Manager schlägt fehl, da NSX keinen universellen logischen Switch auf einem sekundären NSX Manager erstellen kann.

Weitere Informationen zu universellen NSX-Objekten finden Sie im VMware Knowledgebase-Artikel *Deployment of vRealize Automation blueprints with NSX objects fail (2147240)* unter <http://kb.vmware.com/kb/2147240>.

Checkliste für die Unterstützung eines externen IPAM-Anbieters

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

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

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

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

Aufgabe	Beschreibung	Details
<input type="checkbox"/> Unterstütztes vRealize Orchestrator-Plug-In für den externen IPAM-Anbieter beziehen und importieren.	<p>Laden Sie das Plug-In bzw. Paket des IPAM-Anbieters, zum Beispiel das Infoblox-IPAM-Plug-In für vRealize Orchestrator und zugehörige Dokumentation, von VMware Solution Exchange (https://solutionexchange.vmware.com/store/category_groups/cloud-management) herunter und importieren Sie das Plug-In oder Paket in vRealize Orchestrator.</p> <p>Wenn VMware Solution Exchange das benötigte IPAM-Anbieterpaket nicht enthält, können Sie mithilfe des SDKs eines externen IPAM-Lösungsanbieters und der zugehörigen Dokumentation Ihr eigenes Paket erstellen.</p> <p>Ein für vRealize Automation versionsspezifisches SDK eines externen IPAM-Lösungsanbieters, zugehörige Dokumentation und zugehöriges Starterpaket für vRealize Orchestrator und vRealize Automation sind unter https://code.vmware.com/sdks oder https://code.vmware.com/samples verfügbar.</p>	<p>Siehe Abrufen und Importieren eines IPAM-Drittanbieterpakets in vRealize Orchestrator.</p>
<input type="checkbox"/> Die erforderlichen Konfigurationsworkflows ausführen und die externe IPAM-Lösung als vRealize Automation-Endpoint registrieren.	<p>Führen Sie die vRealize Orchestrator-Konfigurationsworkflows aus und registrieren Sie den Endpoint-Typ des IPAM-Anbieters in vRealize Orchestrator.</p>	<p>Siehe Führen Sie den Workflow zur Registrierung des Drittanbieter-IPAM-Endpoint-Typs aus in vRealize Orchestrator.</p>

Abrufen und Importieren eines IPAM-Drittanbieterpakets in vRealize Orchestrator

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

Sie können ein vorhandenes Drittanbieter-Plug-In für das IP-Adressmanagement herunterladen und verwenden, z. B. Infoblox IPAM. Sie können auch Ihr eigenes IPAM-Drittanbieter-Plug-In oder -paket erstellen, indem Sie ein von VMware bereitgestelltes Starterpaket und die begleitende SDK-Dokumentation für die Verwendung mit einem anderen IPAM-Lösungsdrittanbieter, wie z. B. BlueCat, verwenden.

- Laden Sie das vorhandene Plug-In [Infoblox-IPAM-Plug-In für vRealize Orchestrator](#) und die unterstützende Dokumentation von marketplace.vmware.com herunter. Der Download enthält auch die Dokumentation für das Installieren und Verwenden des Plug-Ins.

- Erstellen Sie Ihre eigene Drittanbieter-IPAM-Lösung, indem Sie ein SDK eines IPAM-Lösungsdrittanbieters, die zugehörige Dokumentation und ein zugeordnetes Starterpaket für vRealize Orchestrator und vRealize Automation beziehen und verwenden. Weitere Informationen finden Sie auf der Seite [vRealize Automation-Beispielpaket eines IPAM-Drittanbieters](#) unter code.vmware.com/web/sdk.

Sobald Sie das Plug-In bzw. Paket des IPAM-Drittanbieters in vRealize Orchestrator importieren, müssen Sie die erforderlichen Workflows ausführen und den IPAM-Endpoint-Typ in vRealize Orchestrator registrieren.

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

Bei diesen Schritten wird das Infoblox-IPAM-Plug-In als Beispiel verwendet. Ihre Schrittabfolge unterscheidet sich möglicherweise in Abhängigkeit von Ihrer vRealize Automation- oder Plug-In-Version.

Voraussetzungen

- Laden Sie das Paket oder Plug-In von marketplace.vmware.com herunter.
- Melden Sie sich bei vRealize Orchestrator mit Administratorrechten für das Importieren, Konfigurieren und Registrieren eines vRealize Orchestrator-Plug-Ins bzw. Pakets an.

Verfahren

- 1 Öffnen Sie die Website marketplace.vmware.com.
- 2 Suchen Sie das Plug-In bzw. Paket und laden Sie es herunter.

Importieren Sie z. B. das Infoblox-Plug-In, das den Drittanbieter-IPAM-Endpoint von Infoblox in vRealize Orchestrator und vRealize Automation 7.1 und höher unterstützt.

- a Wählen Sie in der Kategorie **Veröffentlicher** die Option **Infoblox** aus und klicken Sie auf **Übernehmen**.
- b Wählen Sie [The Infoblox Plug-in for vRealize Orchestrator](#).
- c Klicken Sie auf **Tech Specs** (Technische Daten) und überprüfen Sie die Voraussetzungen.
- d Klicken Sie auf **Try**, um weitere Informationen und eine E-Mail mit einem Link zum Download zu erhalten.
- e Laden Sie die ZIP-Datei gemäß den Anweisungen in der E-Mail herunter.

Version 4.0 und höher des Plug-Ins unterstützt vRealize Automation 7.1 und höher. Die ZIP-Datei enthält auch Dokumentation zum Plug-In.

- 3 Klicken Sie in vRealize Orchestrator auf die Registerkarte **Administrator** und klicken Sie auf **Paket importieren**.

- 4 Wählen Sie das zu importierende Paket aus.
- 5 Wählen Sie alle Workflows und Artefakte aus und klicken Sie auf **Ausgewählte Elemente importieren**.

Nächste Schritte

[Führen Sie den Workflow zur Registrierung des Drittanbieter-IPAM-Endpoint-Typs aus in vRealize Orchestrator](#).

Führen Sie den Workflow zur Registrierung des Drittanbieter-IPAM-Endpoint-Typs aus in vRealize Orchestrator

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

Voraussetzungen

- [Abrufen und Importieren eines IPAM-Drittanbieterpakets in vRealize Orchestrator](#)
- Vergewissern Sie sich, dass Sie bei vRealize Orchestrator mit der Berechtigung zum Ausführen von Registrierungs-Workflows angemeldet sind.
- Bereiten Sie sich darauf vor, bei Aufforderung durch den Registrierungs-Workflow die vRealize Automation-Administratoranmeldedaten einzugeben. Wenn Sie IPAM-Endpoint-Typen in vRealize Orchestrator registrieren, werden Sie aufgefordert, vRealize Automation-Administratoranmeldedaten einzugeben.

Verfahren

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

Jedes IPAM-Anbieterpaket weist einen eindeutigen Namen auf und enthält spezielle Workflows. Jeder Anbieter stellt seinen eigenen Registrierungsworkflow zur Verfügung. Die Workflow-Namen in den Anbieterpaketen können ähnlich sein, aber der Speicherort der Workflows in vRealize Orchestrator kann unterschiedlich sein und ist anbieterspezifisch.

- 2 Führen Sie in diesem Beispiel den Register IPAM Endpoint-Registrierungsworkflow aus und geben Sie den IPAM-Infoblox-Endpoint-Typ an.
- 3 Geben Sie bei der Eingabeaufforderung für vRealize Automation-Anmeldedaten Ihre vRealize Automation-Administratoranmeldedaten ein, beispielsweise Fabric-Administratoranmeldedaten.

Sie müssen im Registrierungs-Workflow vRealize Automation-Anmeldedaten für den Systemadministrator angeben. Selbst wenn ein Benutzer ohne Systemadministratorrechte beim vRealize Orchestrator-Client angemeldet ist, wird die Registrierung bei Eingabe der vRealize Automation-Systemadministrator-Anmeldedaten für den Workflow erfolgreich durchgeführt.

Ergebnisse

In diesem Beispiel registriert das Paket Infoblox als neuen IPAM-Endpoint-Typ im vRealize Automation-Endpoint-Dienst und stellt den Endpoint-Typ zur Verfügung, wenn Sie Endpoints in vRealize Automation erstellen oder bearbeiten.

Hinweis Es ist möglich, dass die Infoblox IPAM-Verbindung nicht mehr auf der vRealize Orchestrator Registerkarte **Bestandsliste** angezeigt wird, nachdem Sie den vRealize Orchestrator-Server im vRealize Orchestrator Control Center neu gestartet haben. Um das Problem zu beheben, führen Sie den Create IPAM Connection-Workflow vom Menü **vRO Admin > Bibliothek > Infoblox > vRA > Helfer** aus. Sie können anschließend die Registerkarte vRealize Orchestrator **Bestandsliste** aufrufen, **Infoblox IPAM** auswählen und die Seite aktualisieren, um die Infoblox IPAM-Verbindung anzuzeigen.

Nächste Schritte

Sie können jetzt in vRealize Automation einen IPAM-Infoblox-Endpoint-Typ oder einen Endpoint für das Paket oder Plug-In eines Drittanbieters erstellen, das Sie gerade registriert haben. Siehe [Erstellen eines Endpoints eines IPAM-Drittanbieters](#).

Prüfliste für die Konfiguration von Container für vRealize Automation

Um mit Container zu beginnen, müssen Sie die Funktion zur Unterstützung der vRealize Automation-Benutzerrollen konfigurieren.

Nachdem Sie die Containerdefinitionen in Container konfiguriert haben, können Sie Containerkomponenten in einem Blueprint hinzufügen und konfigurieren.

Tabelle 1-4. Prüfliste für die Konfiguration von Container für vRealize Automation

Aufgabe	Details
Weisen Sie die die Rollen Containeradministrator und Containerarchitekt zu.	Siehe die Informationen zu Containerrollen unter <i>Grundlagen und Konzepte</i> .
Definieren Sie Containerdefinitionen auf der Registerkarte Container in vRealize Automation.	Siehe <i>Konfigurieren von vRealize Automation</i> .
Fügen Sie auf der Registerkarte Design in vRealize Automation Containerkomponenten und Container-Netzwerkkomponenten zu Blueprints hinzu.	Siehe <i>Konfigurieren von vRealize Automation</i> .

Konfigurieren von Container mit der vRealize Automation-Appliance

Xenon-Dienstinformationen sind über die vRealize AutomationvRealize Automation-Appliance (**vRA-Einstellungen > Xenon**) zugänglich.

Sie enthält Informationen zur Xenon-HostVM, zum Überwachungsport und zum Dienststatus. Sie zeigt auch Informationen zu den in einem Cluster gruppierten Xenon-Knoten an.

Sie können den Xenon Linux-Dienst mit den folgenden Befehlszeilenbefehlen in der vRealize Automation-Appliance verwalten.

Befehl	Beschreibung
service xenon-service status	Zeigt den Status (ausgeführt oder beendet) des Diensts an.
service xenon-service start	Startet den Dienst.
service xenon-service stop	Beendet den Dienst.
service xenon-service restart	Startet den Dienst neu.
service xenon-service get_host	Zeigt den Namen des Hosts an, auf dem der Dienst ausgeführt wird.
service xenon-service get_port	Zeigt den Dienstport an.
service xenon-service status_cluster	Zeigt Informationen zu allen in einem Cluster gruppierten Knoten im JSON-Format an.
service xenon-service reset	Löscht das Verzeichnis, in dem Xenon alle Konfigurationsdateien speichert, und startet den Dienst neu.

Gruppieren von Containern in einem Cluster

Sie können den Xenon-Dienst zusammen mit Container für vRealize Automation verwenden, um Knoten in einem Cluster zu verbinden. Wenn die Knoten in einem Cluster gruppiert sind, werden andere Knoten beim Starten des Xenon-Diensts automatisch verbunden.

Sie können den Clusterstatus auf der Registerkarte **Xenon** in der vRealize Automation-Appliance oder anhand der Ausführung des folgenden Befehls auf einer Befehlszeilenoberfläche überwachen:

```
service xenon-service status_cluster
```

Xenon kann für Quorum-basierte Cluster verwendet werden. Das Quorum wird mit der Formel $(\text{number of nodes} / 2) + 1$ berechnet.

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 Datencenter 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.

vRealize Automation erfordert Zugriffsschlüssel als Endpoint-Anmeldedaten und unterstützt keine Benutzernamen und Kennwörter.

■ Rollen- und Berechtigungsautorisierung in Amazon Web Services

Mit der Hauptbenutzerrolle in AWS erhält ein(e) AWS Directory Services-Benutzer bzw. -Gruppe den Vollzugriff auf AWS-Dienste und -Ressourcen, was jedoch nicht erforderlich ist. Benutzerrollen mit geringeren Berechtigungen werden ebenfalls unterstützt. Die folgende AWS-Sicherheitsrichtlinie erfüllt die Anforderungen der vRealize Automation-Funktionalität:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeImages",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeVolumes",

      "ec2:DescribeVpcAttribute",
      "ec2:DescribeAddresses",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeImageAttribute",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeVolumeStatus",
      "ec2:DescribeVpnConnections",
      "ec2:DescribeRegions",
      "ec2:DescribeTags",
      "ec2:DescribeVolumeAttribute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeNetworkInterfaceAttribute",

      "ec2:DisassociateAddress",
      "ec2:GetPasswordData",

      "ec2:ImportKeyPair",
      "ec2:ImportVolume",

      "ec2:CreateVolume",
      "ec2>DeleteVolume",
      "ec2:AttachVolume",
      "ec2:ModifyVolumeAttribute",
      "ec2:DetachVolume",

      "ec2:AssignPrivateIpAddresses",
      "ec2:UnassignPrivateIpAddresses",

      "ec2:CreateKeyPair",
      "ec2>DeleteKeyPair",
```

```

        "ec2:CreateTags",
        "ec2:AssociateAddress",
        "ec2:ReportInstanceState",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:MonitorInstances",
        "ec2:RebootInstances",
        "ec2:RunInstances",
        "ec2:TerminateInstances",

        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth"
    ],
    "Resource": "*"
}
}]

```

■ Anmeldedaten für die Authentifizierung in Amazon Web Services

Für die Verwaltung von Amazon Identity and Access Management (IAM)-Benutzern und -Gruppen benötigen Sie Anmeldedaten als AWS-Administrator mit Vollzugriff.

Wenn Sie einen AWS-Endpoint in vRA erstellen, werden Sie zur Eingabe eines Schlüssels und eines geheimen Schlüssels aufgefordert. Für den Abruf des erforderlichen Zugriffsschlüssels zum Erstellen des Amazon-Endpoints muss der Administrator 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. Siehe [Erstellen eines Amazon-Endpoints](#).

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 demund 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 EC2-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 Speichervolumen auf Blockebene mit einer Amazon-Maschineninstanz und Amazon Virtual Private Cloud verwendet werden. Das Speichervolumen 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.

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

Als mit der Einrichtung einer Umgebung zur Evaluierung von vRealize Automation beauftragter IT-Experte möchten Sie die VPC-Konnektivität zwischen Netzwerk und Amazon 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

- 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.

Verfahren

- 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 \
User of Amazon tunnel machine@Public IP Address of Amazon tunnel machine
```

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

Nächste Schritte

- 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 Sicherheitsgruppen in einer Reservierung angeben, wenn Sie eine Maschine anfordern. Darüber hinaus können Sie eine vorhandene oder bedarfsgesteuerte NSX-Sicherheitsgruppe in der Design-Arbeitsfläche 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.

Verwandte Informationen über das Vorbereiten der Umgebung finden Sie unter den SCVMM-Anforderungen im Handbuch *Installieren von vRealize Automation*.

Verwandte Informationen über das Bereitstellen von Maschinen finden Sie unter [Erstellen eines Hyper-V \(SCVMM\)-Endpoints](#).

vRealize Automation unterstützt keine Bereitstellungsumgebung, die eine private SCVMM-Cloud-Konfiguration verwendet. vRealize Automation kann derzeit keine Datenerfassung, Datenzuordnung oder Datenbereitstellung basierend auf privaten SCVMM-Clouds durchführen.

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 Begriffe werden beispielsweise 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.

Konfigurieren der Netzwerk-zu-Azure-VPC-Konnektivität

Wenn Sie Softwarekomponenten in Azure-Blueprints verwenden möchten, müssen Sie Netzwerk-zu-Azure-Konnektivität konfigurieren.

Voraussetzungen

- Erstellen Sie eine Azure-Sicherheitsgruppe namens „TunnelGroup“ und konfigurieren Sie sie so, dass der Zugriff auf Port 22 zulässig ist.
- Erstellen oder bestimmen Sie eine Maschine, beispielsweise eine CentOS-Maschine, in der Azure-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.

Verfahren

- 1 Melden Sie sich bei Ihrer Azure-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 Azure-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 \
User of Azure tunnel machine@Public IP Address of Azure tunnel machine
```

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

Nächste Schritte

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

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.

Weitere Informationen zum Festlegen von Ports während der Vorbereitung zur Bereitstellung von Maschinen finden Sie in den Dokumenten *Handbuch zur sicheren Konfiguration* und *Referenzarchitektur* auf der Webseite [Informationen zu VMware vRealize Automation](#).

Auswählen einer vorzubereitenden Methode zur Maschinenbereitstellung

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

Tabelle 1-5. Auswählen einer vorzubereitenden Methode zur Maschinenbereitstellung

Szenario	Unterstützter Endpoint	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.	Checkliste für die Ausführung von Visual Basic-Skripts während der Bereitstellung
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"> ■ vSphere ■ vCloud Air ■ vCloud Director ■ Amazon AWS 	<ul style="list-style-type: none"> ■ (Erforderlich) Gast-Agent ■ (Erforderlich) Software-Bootstrap-Agent und Gast-Agent 	<ul style="list-style-type: none"> ■ Klonen ■ Klon (für vCloud Air oder vCloud Director) ■ Verknüpfter Klon ■ Amazon-Maschinen-Image 	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 Vorbereiten für Software-Bereitstellung .
Weiteres Anpassen von Maschinen nach der Bereitstellung mithilfe des Gast-Agent.	Alle virtuellen Endpoints und Amazon AWS.	<ul style="list-style-type: none"> ■ (Erforderlich) Gast-Agent ■ (Optional) Software-Bootstrap-Agent und Gast-Agent 	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.
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.

Tabelle 1-5. Auswählen einer vorzubereitenden Methode zur Maschinenbereitstellung (Fortsetzung)

Szenario	Unterstützter Endpoint	Agent-Unterstützung	Bereitstellungsmethode	Vorbereitungen vor der Bereitstellung
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.	vSphere	<ul style="list-style-type: none"> ■ (Optional) Gast-Agent ■ (Optional) Software-Bootstrap-Agent und Gast-Agent 	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> <p>Der im Blueprint angegebene VM-Snapshot sollte vor der Bereitstellung der verknüpften Klon-VMs ausgeschaltet werden.</p>
Stellen Sie eine speichereffiziente Kopie einer virtuellen Maschine durch Verwendung der Net App FlexClone-Technologie bereit.	vSphere	(Optional) Gast-Agent	NetApp FlexClone	Siehe Checkliste für das Vorbereiten für die Bereitstellung durch Klonen .
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"> ■ vSphere ■ KVM (RHEV) ■ SCVMM 	<ul style="list-style-type: none"> ■ (Optional) Gast-Agent ■ (Nur für vSphere optional) Software-Bootstrap-Agent und Gast-Agent 	Klonen	<p>Siehe Checkliste für das Vorbereiten für die Bereitstellung durch Klonen.</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"> ■ vCloud Air ■ vCloud Director 	<ul style="list-style-type: none"> ■ (Optional) Gast-Agent ■ (Optional) Software-Bootstrap-Agent und Gast-Agent 	Klonen von vCloud Air oder vCloud Director	<p>Siehe Vorbereiten für die vCloud Air- und vCloud Director-Bereitstellung.</p> <p>Wenn Software unterstützt werden soll, müssen Sie eine Vorlage erstellen, die den Gast-Agent und den Software-Bootstrap-Agent enthält.</p> <p>Konfigurieren Sie für vCloud Air die Netzwerkverbindung zwischen Ihrer vRealize Automation-Umgebung und Ihrer vCloud Air-Umgebung.</p>

Tabelle 1-5. Auswählen einer vorzubereitenden Methode zur Maschinenbereitstellung (Fortsetzung)

Szenario	Unterstützter Endpoint	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"> ■ Alle virtuellen Endpoints ■ Red Hat OpenStack 	Der Gast-Agent wird im Rahmen der Vorbereitungsanweisungen installiert.	Linux Kickstart	Vorbereiten für die Linux Kickstart-Bereitstellung
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	Vorbereiten für SCCM-Bereitstellung
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"> ■ Alle virtuellen Endpoints ■ Red Hat OpenStack 	Gast-Agent ist erforderlich. Wenn Sie das WinPE-Image erstellen, müssen Sie den Gast-Agent manuell einfügen.	WIM	Vorbereiten für die WIM-Bereitstellung

Tabelle 1-5. Auswählen einer vorzubereitenden Methode zur Maschinenbereitstellung (Fortsetzung)

Szenario	Unterstützter Endpoint	Agent-Unterstützung	Bereitstellungsmethode	Vorbereitungen vor der Bereitstellung
Starten Sie eine Instanz von einem VM-Image.	Red Hat OpenStack	Nicht unterstützt	VM-Image	Siehe Vorbereiten für die Image-Bereitstellung der virtuellen Maschine .
Starten Sie eine Instanz von einem Amazon-System-Image.	Amazon AWS	<ul style="list-style-type: none"> ■ (Optional) Gast-Agent ■ (Optional) Software-Bootstrap-Agent und Gast-Agent 	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 1-6. 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</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. 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> <hr/> <p>Hinweis 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"> ■ 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>. ■ 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.

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.

Hinweis Der Linux-Gast-Agent weist während der Erstellungs- und Klonaktionen für Linux Kickstart- und PXE-Bereitstellungen statische IP-Adressen zu, die auf den benutzerdefinierten Eigenschaften von vRealize Automation in Arbeitselementen basieren. Der Gast-Agent kann die neuere konsistente Netzwerknamenskonvention (wie z. B. in Ubuntu 16.x) nicht übernehmen, wenn er statische IP-Adressen zuweist.

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.

Sie können Sicherheitseinstellungen für die bereitzustellenden virtuellen Maschinen konfigurieren, indem Sie Informationen in einem Reservierungs-, Blueprint- oder Gast-Agent-Skript angeben. Wenn die bereitzustellenden Maschinen einen Gast-Agent benötigen, müssen Sie eine Sicherheitsregel, die diese Anforderung enthält, zur Reservierung oder zum Blueprint hinzufügen. Wenn Sie z. B. eine Standardsicherheitsrichtlinie verwenden, die die Kommunikation zwischen allen Maschinen nicht zulässt, und Sie sich auf eine separate Sicherheitsrichtlinie verlassen, die die Kommunikation zwischen bestimmten Maschinen, kann der Gast-Agent während der Anpassungsphase möglicherweise mit vRealize Automation kommunizieren. Um dieses Problem während der Bereitstellung von Maschinen zu vermeiden, verwenden Sie eine Standardsicherheitsrichtlinie, die während der Anpassungsphase die Kommunikation ermöglicht.

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 1-7. Benutzerdefinierte Eigenschaften für das Ändern von IP-Adressen auf einer bereitgestellten Maschine mithilfe eines Gast-Agents

Benutzerdefinierte Eigenschaft	Beschreibung
<code>VirtualMachine.Admin.UseGuestAgent</code>	Setzen Sie den Wert auf true , um den Gast-Agent beim Start der bereitgestellten Maschine zu initialisieren.
<code>VirtualMachine.Customize.WaitComplete</code>	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 1-7. Benutzerdefinierte Eigenschaften für das Ändern von IP-Adressen auf einer bereitgestellten Maschine mithilfe eines Gast-Agents (Fortsetzung)

Benutzerdefinierte Eigenschaft	Beschreibung
VirtualMachine.SoftwareN.ScriptPath	<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 <code>{CustomPropertyName}</code> in der Pfadzeichenfolge einfügen. Angenommen, Sie haben eine benutzerdefinierte Eigenschaft <code>ActivationKey</code> mit dem Wert <code>1234</code>. 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> <p>Fügen Sie <code>{Owner}</code> ein, um den Namen des Maschinenbesitzers an das Skript zu übergeben.</p> <p>Sie können auch benutzerdefinierte Eigenschaftswerte als Parameter an das Skript weitergeben, indem Sie <code>{YourCustomProperty}</code> in die Pfadzeichenfolge einfügen. Wenn Sie beispielsweise den Wert <code>\\vra-scripts.mycompany.com\scripts\changeIP.bat</code> eingeben, wird das Skript <code>changeIP.bat</code> von einem gemeinsam genutzten Speicherort ausgeführt. Wenn Sie jedoch den Wert <code>\\vra-scripts.mycompany.com\scripts\changeIP.bat {VirtualMachine.Network0.Address}</code> eingeben, wird das Skript für die Änderung der IP-Adresse ausgeführt, aber auch der Wert der Eigenschaft <code>VirtualMachine.Network0.Address</code> als Parameter an das Skript weitergegeben.</p>
VirtualMachine.ScriptPath.Decrypt	<p>Ermöglicht vRealize Automation das Abrufen einer verschlüsselten Zeichenfolge, die als ordnungsgemäß formatierte benutzerdefinierte Eigenschaftsanweisung <code>VirtualMachine.SoftwareN.ScriptPath</code> an die gagent-Befehlszeile übergeben wird.</p> <p>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 <code>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat Kennwort</code> nicht sicher, da sie ein tatsächliches Kennwort enthält.</p>

Tabelle 1-7. Benutzerdefinierte Eigenschaften für das Ändern von IP-Adressen auf einer bereitgestellten Maschine mithilfe eines Gast-Agents (Fortsetzung)

Benutzerdefinierte Eigenschaft	Beschreibung
	<p>Zum Entschlüsseln des Kennworts können Sie eine benutzerdefinierte vRealize Automation-Eigenschaft erstellen, wie beispielsweise <code>MyPassword = password</code>, und die Verschlüsselung durch Aktivieren des verfügbaren Kontrollkästchens aktivieren. Der Gast-Agent entschlüsselt den Eintrag [MyPassword] in den Wert in der benutzerdefinierten Eigenschaft <code>MyPassword</code> und führt das Skript als <code>c:\dosomething.bat password</code> aus.</p> <ul style="list-style-type: none"> ■ Erstellen Sie die benutzerdefinierte Eigenschaft <code>MyPassword = Kennwort</code>, wobei <i>Kennwort</i> der Wert Ihres tatsächlichen Kennworts ist. Aktivieren Sie die Verschlüsselung durch Aktivieren des verfügbaren Kontrollkästchens. ■ Legen Sie die benutzerdefinierte Eigenschaft <code>VirtualMachine.ScriptPath.Decrypt</code> als <code>VirtualMachine.ScriptPath.Decrypt = true</code> fest. ■ Legen Sie die benutzerdefinierte Eigenschaft <code>VirtualMachine.Software0.ScriptPath</code> als <code>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat [MyPassword]</code> fest. <p>Wenn Sie <code>VirtualMachine.ScriptPath.Decrypt</code> auf „False“ festlegen oder die benutzerdefinierte Eigenschaft <code>VirtualMachine.ScriptPath.Decrypt</code> 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*.

Konfigurieren des Vertrauensverhältnisses zu einem Server für den Gast-Agent

Die Installation der PEM-Datei für öffentliche Schlüssel für den vRealize Automation Manager Service-Host im richtigen Gast-Agent-Ordner stellt die sicherste Methode für die Konfiguration des Vertrauensverhältnisses zu einem Server für den Gast-Agent dar.

Suchen Sie den Gast-Agent-Ordner auf jeder Vorlage für die PEM-Datei `cert.pem` Vertrauensverhältnis zu einem Server für den Manager Service-Host.

- Windows-Gast-Agent-Ordner auf jeder Vorlage, die die `gugent`-Befehlszeile verwendet

```
C:\VRMGuestAgent\cert.pem
```

- Linux-Gast-Agent-Ordner auf jeder Vorlage, die die `gugent`-Befehlszeile verwendet

```
/usr/share/gugent/cert.pem
```

Wenn Sie die Datei `cert.pem` nicht an diesem Speicherort ablegen, kann die Vorlagenreferenzmaschine den Gast-Agent nicht verwenden. Wenn Sie beispielsweise nach dem Starten der VM mit geänderten Skripts versuchen, Informationen zum öffentlichen Schlüssel zu sammeln, setzen Sie den Sicherheitszustand außer Kraft.

Je nach konfigurierter Umgebung sind zudem diese Faktoren zu berücksichtigen:

- Für WIM-Installationen müssen Sie die Inhalte der PEM-Datei für öffentliche Schlüssel zur ausführbaren Datei für die Konsole und zur Benutzeroberfläche hinzufügen. Die Konsolenmarkierung lautet **/cert filename**.
- Für RedHat kickstart-Installationen müssen Sie den öffentlichen Schlüssel ausschneiden und in die Beispieldatei einfügen. Andernfalls schlägt die Ausführung des Gast-Agent fehl.
- Für SCCM-Installationen muss sich die `cert.pem`-Datei im Ordner `VRMGuestAgent` befinden.
- Für Linux vSphere-Installationen muss sich die `cert.pem`-Datei im Ordner `/usr/share/gugent` befinden.

Hinweis Wahlweise können Sie Software und Gast-Agents zusammen installieren, indem Sie das folgende Skript über <https://APPLIANCE/software/index.html> herunterladen. Mit diesem Skript können Sie die Akzeptanz von SSL-Zertifikat-Fingerprints verarbeiten, während Sie die Vorlagen erstellen.

- Linux
`prepare_vra_template.sh`
- Windows
`prepare_vra_template.ps1`

Wenn Sie die Software und den Gast-Agent zusammen installieren, müssen Sie die Anweisungen unter [Installieren des Gast-Agents auf einer Linux-Referenzmaschine](#) oder [Installieren des Gast-Agents auf einer Windows-Referenzmaschine](#) nicht befolgen.

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.
- Stellen Sie eine sichere vertrauenswürdige Verbindung zwischen den Gast-Agenten und Ihrer Manager Service-Maschine her. Siehe [Konfigurieren des Vertrauensverhältnisses zu einem Server für den Gast-Agent](#).

Verfahren

- 1 Navigieren Sie zur Seite für die Verwaltungskonsole der vRealize Automation-Appliance.

Beispiel: `https://va-hostname.domain.com`.

- 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 Klicken Sie auf dieser Seite im Abschnitt mit den Installationsprogrammen für Gast-Agents auf **Linux-Gast-Agent-Pakete**, um die Datei `LinuxGuestAgentPkgs.zip` herunterzuladen und zu speichern.

- 4 Entpacken Sie die heruntergeladene Datei `LinuxGuestAgentPkgs.zip`, in den Ordner `VraLinuxGuestAgent`.

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

- a Navigieren Sie zum Unterverzeichnis `VraLinuxGuestAgent`, das dem während der Bereitstellung bereitzustellenden Gastbetriebssystem entspricht, z. B. `rhel32`.
- 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 gurent-gurent-7.1.0-4201531.i386.rpm` aus.

- 6 Konfigurieren Sie den Gast-Agent zum Kommunizieren mit dem Manager Service durch Ausführen von `installgurent.sh Manager_Service_Hostname_fdqn:portnumber ssl platform`.

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

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

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

- 8 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>

Nächste Schritte

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 vRealize Automation-Windows-Gast-Agent auf einer Windows-Referenzmaschine als Windows-Dienst und sorgen Sie für die weitere Anpassung der Maschinen.

Voraussetzungen

- Bestimmen oder erstellen Sie die Referenzmaschine.
- Stellen Sie eine sichere vertrauenswürdige Verbindung zwischen den Gast-Agenten und Ihrer Manager Service-Maschine her. Siehe [Konfigurieren des Vertrauensverhältnisses zu einem Server für den Gast-Agent](#).

Verfahren

- 1 Navigieren Sie zur vRealize Automation-Appliance-Seite **Gast- und Software-Agent-Installationsprogramme**:

<https://vRealize-Automation-Appliance-FQDN/software>

- 2 Laden Sie unter **Gast-Agent-Installationsprogramme** die ausführbare 32-Bit- oder 64-Bit-Datei herunter und speichern Sie sie im Stammverzeichnis des Laufwerks C:.

Hinweis Es gibt eine Befehlszeilenalternative für dieses Gast-Agent-Installationsverfahren. Anstatt die ausführbaren Dateien herunterzuladen, können Sie auf der Seite „Gast- und Software-Agent-Installationsprogramme“ zu **Windows-Software-Installationsprogramme** navigieren. Dort können Sie das PowerShell-Skript `prepare_vra_template.ps1` herunterladen und ausführen:

```
PowerShell -NoProfile -ExecutionPolicy Bypass -Command prepare_vra_template.ps1
```

- 3 Extrahieren Sie die Windows-Gast-Agent-Dateien, indem Sie die ausführbare Datei ausführen. Bei der Extrahierung wird das Verzeichnis `C:\VRMGuestAgent` erstellt, und die Dateien werden diesem Verzeichnis hinzugefügt.

Benennen Sie `C:\VRMGuestAgent` 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 Legen Sie die vertrauenswürdige PEM-Datei des Manager Service im Verzeichnis `C:\VRMGuestAgent\` ab, um den Gast-Agent so zu konfigurieren, dass er Ihre Manager Service-Maschine als vertrauenswürdig einstuft.
- 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
Wenn Sie einen Lastausgleichsdienst verwenden	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> .
Wenn Sie keinen Lastausgleichsdienst verwenden	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> .
Wenn Sie ein Amazon-System-Image vorbereiten	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>

Ergebnisse

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

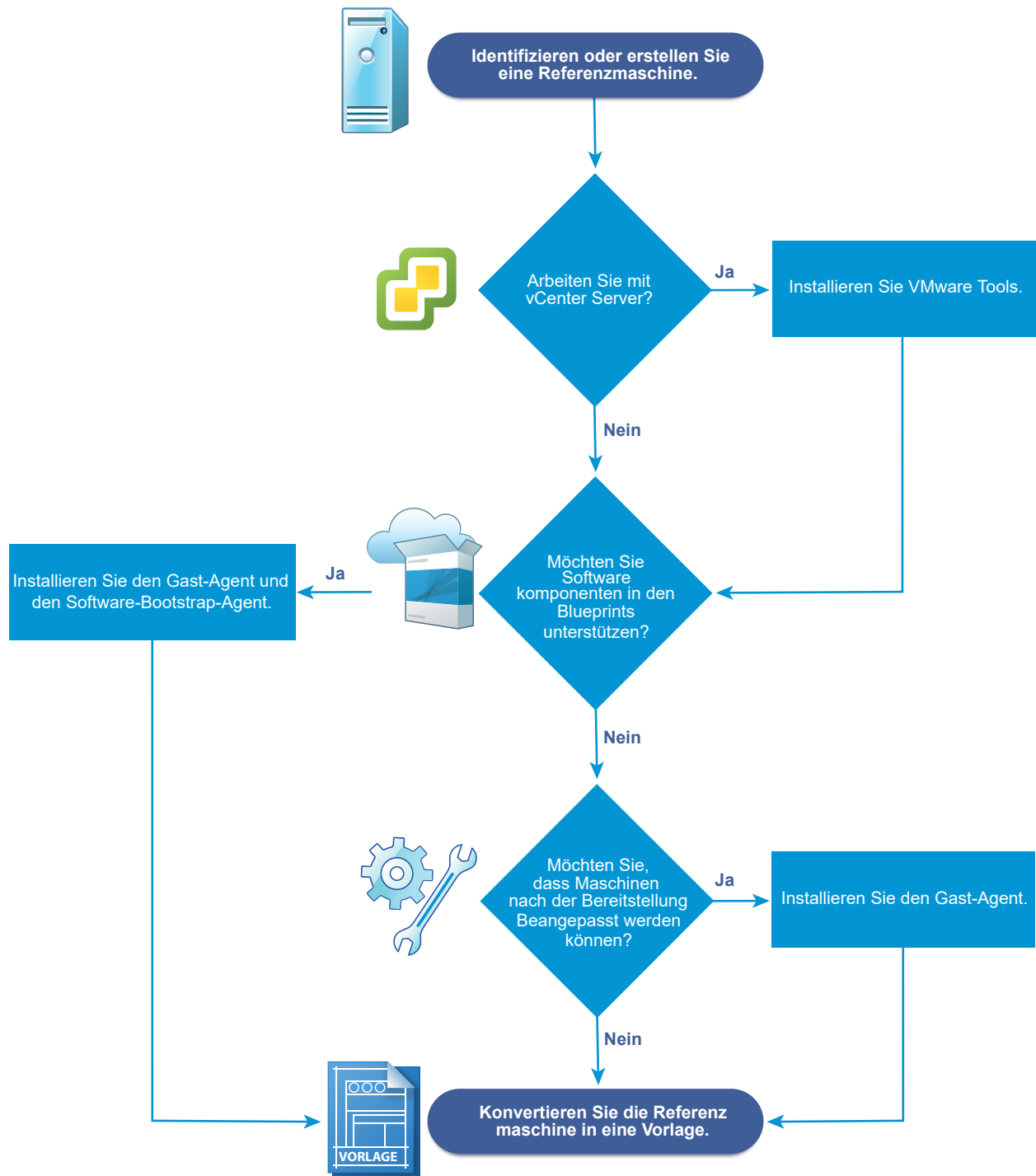
Nächste Schritte

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.

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 1-8. 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	<p>Weitere Informationen zu Windows-Referenzmaschinen finden Sie unter Vorbereiten einer Windows-Referenzmaschine für die Unterstützung von Software.</p> <p>Weitere Informationen zu Linux-Referenzmaschinen finden Sie unter Vorbereiten einer Linux-Referenzmaschine für die Unterstützung von Software.</p>
<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 Verwenden des vRealize Automation-Gast-Agent bei der Bereitstellung .
<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	<p>Die Referenzmaschine kann ein- oder ausgeschaltet sein. Wenn Sie in vCenter Server klonen, können Sie eine Referenzmaschine direkt verwenden, ohne eine Vorlage zu erstellen.</p> <p>Informieren Sie sich in der von Ihrem Hypervisor bereitgestellten Dokumentation.</p>
<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	<p>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.</p> <p>Informieren Sie sich in der von Ihrem Hypervisor bereitgestellten Dokumentation.</p>
<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-Architekten.	Siehe Arbeitsblatt zur virtuellen Bereitstellung durch Klonen .

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 Arbeitsblattr Tabellen und fügen sie zur Bearbeitung in ein Textverarbeitungstool ein.

Erforderliche Vorlagen- und Reservierungsinformationen

Tabelle 1-9. 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"> ■ Klonen ■ Verknüpfter Klon ■ NetApp FlexClone
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 1-10. vCenter Server-Betriebssystem

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
VMware.VirtualCenter.OperatingSystem		Gibt die Version des vCenter Server-Gastbetriebssystems (VirtualMachineGuestOsIdentifier) 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 1-11. 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 \SendEmail.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 \SendEmail.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 Skripts in den Blueprint einschließen.

Tabelle 1-12. Arbeitsblatt für Informationen zum Linux-Gast-Agent-Anpassungsskript

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
Linux.ExternalScript.Name		<p>Gibt den Namen eines optionalen Anpassungsskripts an, wie beispielsweise config.sh, 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.</p> <p>Wenn Sie ein externes Skript angeben, müssen Sie auch mithilfe der Eigenschaften Linux.ExternalScript.LocationType und Linux.ExternalScript.Path dessen Speicherort definieren.</p>
Linux.ExternalScript.LocationType		<p>Gibt den Speicherorttyp des in der Eigenschaft Linux.ExternalScript.Name benannten Anpassungsskripts an. Mögliche Werte sind „local“ oder „nfs“.</p> <p>Darüber hinaus müssen Sie mit der Eigenschaft Linux.ExternalScript.Path den Skriptspeicherort angeben. Wenn der Speicherorttyp „nfs“ lautet, sollten Sie auch die Eigenschaft Linux.ExternalScript.Server verwenden.</p>
Linux.ExternalScript.Server		<p>Gibt den Namen des NFS-Servers an, wie beispielsweise „lab-ad.lab.local“, auf dem das in Linux.ExternalScript.Name angegebene externe Linux-Anpassungsskript gespeichert ist.</p>
Linux.ExternalScript.Path		<p>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 /scripts/linux/config.sh.</p>

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 1-13. Arbeitsblatt für benutzerdefinierte Eigenschaften zum Anpassen geklonter Maschinen mit einem Gast-Agent

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
<code>VirtualMachine.Admin.AddOwnerToAdmins</code>		Legen Sie diese Eigenschaft auf „True“ (Standardwert) fest, um den Besitzer der Maschine, gemäß der Eigenschaft <code>VirtualMachine.Admin.Owner</code> , zur lokalen Administratorengruppe auf der Maschine hinzuzufügen.
<code>VirtualMachine.Admin.AllowLogin</code>		Legen Sie diese Eigenschaft auf „True“ (Standardwert) fest, um den Maschinenbesitzer zur Gruppe der lokalen Remotedesktopbenutzer, gemäß der Eigenschaft <code>VirtualMachine.Admin.Owner</code> , hinzuzufügen.
<code>VirtualMachine.Admin.UseGuestAgent</code>		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 <code>VMwareCloneWorkflow</code> 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.
<code>VirtualMachine.DiskN.Active</code>		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.
<code>VirtualMachine.DiskN.Label</code>		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 1-13. Arbeitsblatt für benutzerdefinierte Eigenschaften zum Anpassen geklonter Maschinen mit einem Gast-Agent (Fortsetzung)

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
<code>VirtualMachine.DiskN.Letter</code>		Gibt den Laufwerkbuchstaben oder Mount-Punkt der Festplatte <i>N</i> einer Maschine an. Der Standardwert ist C. Um beispielsweise den Buchstaben D für die Festplatte 1 anzugeben, definieren Sie die benutzerdefinierte Eigenschaft als <code>VirtualMachine.Disk1.Letter</code> 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 <i>N</i> vom Gast-Agent im Gastbetriebssystem gemountet wird.
<code>VirtualMachine.Admin.CustomizeGuestOSDelay</code>		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.
<code>VirtualMachine.Customize.WaitCompletion</code>		Legen Sie diese Eigenschaft auf „True“ fest, um zu verhindern, dass der Bereitstellungsworkflow Arbeitselemente an den Gast-Agent sendet, bevor alle Anpassungen abgeschlossen wurden.
<code>VirtualMachine.SoftwareN.Name</code>		Gibt den beschreibenden Namen der Softwareanwendung <i>N</i> 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 1-13. Arbeitsblatt für benutzerdefinierte Eigenschaften zum Anpassen geklonter Maschinen mit einem Gast-Agent (Fortsetzung)

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
VirtualMachine.SoftwareN.ScriptPath		<p>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>Sie können benutzerdefinierte Eigenschaftswerte als Parameter an das Skript übergeben, indem Sie <code>{CustomPropertyName}</code> in der Pfadzeichenfolge einfügen. Angenommen, Sie haben eine benutzerdefinierte Eigenschaft <code>ActivationKey</code> 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 <code>/Ordnername/Unterordnername/Dateiname.iso</code>. 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

Sie können die Konfiguration für bestimmte Netzwerkgeräte auf einer Maschine angeben, indem Sie benutzerdefinierte Eigenschaften verwenden.

Gängige, netzwerkbezogene benutzerdefinierte Eigenschaften sind in der folgenden Tabelle aufgelistet. Informationen über zusätzliche und verwandte benutzerdefinierte Eigenschaften finden Sie unter *Benutzerdefinierte Eigenschaften für Klon-Blueprints* und *Benutzerdefinierte Eigenschaften für Netzwerke* in *Referenz für benutzerdefinierte Eigenschaften*.

Tabelle 1-14. 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. Für bedarfsgesteuerte NAT-Netzwerke oder bedarfsgesteuerte geroutete Netzwerke wird diese Eigenschaft nicht unterstützt.</p>

Tabelle 1-14. 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. Für bedarfsgesteuerte NAT-Netzwerke oder bedarfsgesteuerte geroutete Netzwerke wird diese Eigenschaft nicht unterstützt.</p>

Tabelle 1-14. 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 <code>N= 0</code> und <code>1</code> 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. Für bedarfsgesteuerte NAT-Netzwerke oder bedarfsgesteuerte geroutete Netzwerke wird diese Eigenschaft nicht unterstützt.</p> <p>Ein Beispiel dafür, wie Sie diese benutzerdefinierte Eigenschaft verwenden können, um <code>VirtualMachine.Network0.Name</code> basierend auf der Auswahl des Konsumenten aus einer Liste der vordefinierten verfügbaren Netzwerke dynamisch festzulegen, finden Sie im</p>

Tabelle 1-14. Konfiguration benutzerdefinierter Eigenschaften für Netzwerke (Fortsetzung)

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
		Blog Adding a Network Selection Drop-Down in vRA 7 (Hinzufügen eines Dropdown-Menüs für die Netzwerkauswahl in vRA 7).
<code>VirtualMachine.NetworkN.PortID</code>		<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 <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. Für bedarfsgesteuerte NAT-Netzwerke oder bedarfsgesteuerte geroutete Netzwerke wird diese Eigenschaft nicht unterstützt.</p>
<code>VirtualMachine.NetworkN.NetworkProfileName</code>		<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=0</i> für das erste Gerät, 1 für das zweite Gerät usw.</p> <p>Das Netzwerkprofil, auf das die Eigenschaft verweist, wird zum Zuweisen einer IP-Adresse verwendet. Die Eigenschaft bestimmt das Netzwerk, an das die Maschine angeschlossen ist, basierend auf der Reservierung.</p>

Tabelle 1-14. Konfiguration benutzerdefinierter Eigenschaften für Netzwerke (Fortsetzung)

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
■ VirtualMachine.NetworkN.SubnetMask		<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"> ■ VCNS.LoadBalancerEdgePool.Names ■ VCNS.LoadBalancerEdgePool.Names.moderate ■ VCNS.LoadBalancerEdgePool.Names.high ■ VCNS.LoadBalancerEdgePool.Names.low <p>Konfiguriert Attribute des in VirtualMachine.NetworkN.NetworkProfileName angegebenen Netzwerkprofils.</p>
■ VirtualMachine.NetworkN.Gateway		
■ VirtualMachine.NetworkN.PrimaryDns		
■ VirtualMachine.NetworkN.SecondaryDns		
■ VirtualMachine.NetworkN.PrimaryWins		
■ VirtualMachine.NetworkN.SecondaryWins		
■ VirtualMachine.NetworkN.DnsSuffix		
■ VirtualMachine.NetworkN.DnsSearchSuffixes		

Tabelle 1-14. Konfiguration benutzerdefinierter Eigenschaften für Netzwerke (Fortsetzung)

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
VCNS.LoadBalancerEdgePool.Names. <i>name</i>		<p>Gibt die NSX-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"> ■ VCNS.LoadBalancerEdgePool.Names ■ VCNS.LoadBalancerEdgePool.Names.moderate ■ VCNS.LoadBalancerEdgePool.Names.high ■ VCNS.LoadBalancerEdgePool.Names.low

Tabelle 1-14. Konfiguration benutzerdefinierter Eigenschaften für Netzwerke (Fortsetzung)

Benutzerdefinierte Eigenschaft	Mein Wert	Beschreibung
VCNS.SecurityGroup.Names.name		<p>Gibt die NSX-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"> ■ VCNS.SecurityGroup.Names ■ VCNS.SecurityGroup.Names.sales ■ VCNS.SecurityGroup.Names.support
VCNS.SecurityTag.Names.name		<p>Gibt das NSX-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"> ■ VCNS.SecurityTag.Names ■ VCNS.SecurityTag.Names.sales ■ VCNS.SecurityTag.Names.support

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.

Der folgende Überblick zeigt die Schritte, die Sie ausführen müssen, bevor Sie vRealize Automation zum Erstellen von Endpoints und zum Definieren von Reservierungen und Blueprints verwenden können. 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.

Verfahren

- 1 Navigieren Sie zur Seite für die Verwaltungskonsole der vRealize Automation-Appliance.

Beispiel: `https://va-hostname.domain.com`.

- 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 Klicken Sie auf dieser Seite im Abschnitt mit den Installationsprogrammen für Gast-Agents auf **Linux-Gast-Agent-Pakete**, um die Datei `LinuxGuestAgentPkgs.zip` herunterzuladen und zu speichern.

- 4 Entpacken Sie die heruntergeladene Datei `LinuxGuestAgentPkgs.zip`, in den Ordner `VraLinuxGuestAgent`.

- 5 Navigieren Sie zum entsprechenden Unterverzeichnis `VraLinuxGuestAgent` für das bereitzustellende Gastbetriebssystem.

Beispiel: `rhel32`.

- 6 Öffnen Sie eine Datei im entsprechenden Unterverzeichnis „samples“ für Ihr Zielsystem.

Beispielsweise `samples/sample-https-rhel6-x86.cfg`.

- 7 Ersetzen Sie alle Instanzen der Zeichenfolge `host=dcac.example.net` durch die IP-Adresse oder den vollqualifizierten Domännennamen und die Portnummer für den Manager Service oder den Lastausgleichsdienst für den Manager Service.

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>

- 8 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
```

- 9 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.

Verfahren

- 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
```

Ergebnisse

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 Die Kommunikation mit SCCM erfordert den NetBIOS-Namen des SCCM-Servers.
Arbeiten Sie mit Ihrem Netzwerkadministrator zusammen, um sicherzustellen, dass mindestens ein Distributed Execution Manager (DEM) den FQDN des SCCM-Servers in seinen NetBIOS-Namen auflösen kann.
Sie müssen DEMs nicht direkt im selben Netzwerk wie der SCCM-Server platzieren, sondern sie müssen den SCCM-Server über IP erreichen können.
- 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.

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.

Verfahren

- 1 Navigieren Sie zur Seite für die Verwaltungskonsole der vRealize Automation-Appliance.

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

- 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 Klicken Sie auf dieser Seite im Abschnitt für die Komponenteninstallation auf Windows-Gast-Agent-Dateien (**32-Bit**) oder (**64-Bit**), um die Datei GuestAgentInstaller.exe oder GuestAgentInstaller_x64.exe herunterzuladen und zu speichern.

- 4 Extrahieren Sie die Dateien für den Windows-Gast-Agent in einen für SCCM verfügbaren Speicherort.

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

- 5 Erstellen Sie anhand der Definitionsdatei SCCMPackageDefinitionFile.sms ein Softwarepaket.

- 6 Stellen Sie das Softwarepaket für Ihren Verteilungspunkt zur Verfügung.
- 7 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. Den Staging-Bereich muss ein Netzwerkverzeichnis sein, das als UNC-Pfad angegeben oder über folgende Instanz als Netzwerklaufwerk gemountet werden kann:
 - Der Referenzmaschine.
 - Dem System, auf dem Sie das WinPE-Image erstellen.
 - Dem Virtualisierungshost, auf dem Sie die Maschinen bereitstellen.
- 2 Vergewissern Sie sicher, dass das Netzwerk über einen DHCP-Server verfügt. vRealize Automation kann keine Maschinen unter Verwendung mit einem WIM-Image 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.
 - (Optional) Erstellen Sie beliebige benutzerdefinierte Skripts, die Sie zur Anpassung bereitgestellter Maschinen verwenden möchten, und legen Sie sie im entsprechenden Arbeitselementverzeichnis ab.
 - 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](#).

Wenn Sie das WinPE-Image erstellen, müssen Sie 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, schauen Sie in Ihrer Hypervisor-Dokumentation nach.
- 8 Rufen Sie die folgenden Informationen ab, um den Blueprint einzuschließen:
 - 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.

Verfahren

1 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.

2 SysPrep-Anforderungen an die Referenzmaschine

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

3 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).

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

Sie müssen den vRealize Automation-Gast-Agent manuell in Ihr WinPE-Image einfügen.

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*.

SysPrep-Anforderungen an die Referenzmaschine

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

Tabelle 1-15. Erforderliche SysPrep-Einstellungen für Windows Server- oder Windows XP-Referenzmaschine

GuiUnattended-Einstellungen	Wert
AutoLogon	Ja
AutoLogonCount	1
AutoLogonUsername	<i>Benutzername</i> (Benutzername und Kennwort 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 entspricht AutoLogonUsername.</i>

Tabelle 1-16. 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> (Benutzername und Kennwort 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> (Benutzername und Kennwort 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.)
Hinweis 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.	

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):

- 1 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.
- 2 Kopieren Sie die VirtIO-Treiberdateien und fügen Sie die Treiber in ein WinPE-Image ein.
- 3 Laden Sie das WinPE-Image ISO auf die ISO-Speicherdomänen von Red Hat Enterprise Virtualization unter Verwendung des `rhev-m-iso-uploader`-Befehls hoch. Weitere Informationen zum Verwalten von ISO-Images in RHEV finden Sie in der Red Hat-Dokumentation.

- 4 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.

Manuelles Einfügen des Gast-Agent in ein WinPE-Image

Sie müssen den vRealize Automation-Gast-Agent manuell in Ihr 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.

Verfahren

1 Installieren des Gast-Agents in einem WinPE

Sie müssen die Gast-Agent-Dateien manuell in Ihr WinPE-Image kopieren.

2 Konfigurieren der Datei „doagent.bat“

Sie müssen die Datei `doagent.bat` manuell konfigurieren.

3 Konfigurieren der Datei „doagentc.bat“

Sie müssen die Datei `doagentc.bat` manuell konfigurieren.

4 Konfigurieren der Gast-Agent-Eigenschaftendateien

Sie müssen die Gast-Agent-Eigenschaftendateien manuell konfigurieren.

Verfahren

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

Sie müssen die Gast-Agent-Dateien manuell in Ihr WinPE-Image kopieren.

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.

Verfahren

- ◆ Laden Sie den vRealize Automation-Gast-Agent über 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.

Nächste Schritte

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

Konfigurieren der Datei „doagent.bat“

Sie müssen die Datei `doagent.bat` manuell konfigurieren.

Voraussetzungen

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

Verfahren

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

Beispiel: `C:\Programme (x86)\VMware\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.

- Ersetzen Sie alle Instanzen der Zeichenfolge `#Dcac Hostname#` durch den vollqualifizierten Domännennamen und die Portnummer des IaaS Manager Service-Hosts.

Option	Beschreibung
Wenn Sie einen Lastausgleichsdienst verwenden	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>
Wenn Sie keinen Lastausgleichsdienst verwenden	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>

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

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

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

Nächste Schritte

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

Konfigurieren der Datei „doagentc.bat“

Sie müssen die Datei `doagentc.bat` manuell konfigurieren.

Voraussetzungen

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

Verfahren

- Navigieren Sie zum Verzeichnis `VRMGuestAgent` in Ihrem WinPE-Image.
Beispiel: `C:\Programme (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent`.
- Erstellen Sie eine Kopie der Datei `doagentsvc-template.bat` und benennen Sie sie `doagentc.bat`.
- Öffnen Sie `doagentc.bat` in einem Texteditor.
- 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
Wenn Sie einen Lastausgleichsdienst verwenden	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>
Wenn Sie keinen Lastausgleichsdienst verwenden	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.

Nächste Schritte

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

Konfigurieren der Gast-Agent-Eigenschaftendateien

Sie müssen die Gast-Agent-Eigenschaftendateien manuell konfigurieren.

Voraussetzungen

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

Verfahren

- 1 Navigieren Sie zum Verzeichnis `VRMGuestAgent` in Ihrem WinPE-Image.
Beispiel: `C:\Programme (x86)\VMware\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*.
- 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 bei vRealize Automation als **IaaS-Administrator** an.

Verfahren

- 1 Klicken Sie auf **Infrastruktur > Administration > Instanztypen**.
- 2 Klicken Sie auf **Neu**.
- 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** (✓).

Ergebnisse

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

Nächste Schritte

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.

Verfahren

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-aaS-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-aaS-Architekten, die als Grundlage für deren Klon-Blueprints dient.

Verfahren

- 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.

Ergebnisse

vCenter Server markiert Ihre Referenzmaschine „Rainpole_centos_63_x86“ als Vorlage und zeigt die Aufgabe im Fensterbereich „Kürzlich bearbeitete Aufgaben“ an.

Nächste Schritte

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-IaaS-Architekten beim Erstellen von Klon-Blueprints für Linux-Maschinen verwenden können.

Verfahren

- 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**.

Ergebnisse

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

Nächste Schritte

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.

Weitere Informationen zum Festlegen von Ports während der Vorbereitung zur Bereitstellung finden Sie in den Dokumenten *Handbuch zur sicheren Konfiguration* und *Referenzarchitektur* auf der Webseite [Informationen zu VMware vRealize Automation](#).

Tabelle 1-17. 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 Checkliste für das Vorbereiten für die Bereitstellung durch Klonen .
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 Checkliste für das Vorbereiten für die Bereitstellung durch Klonen .

Tabelle 1-17. 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 Checkliste für das Vorbereiten für die Bereitstellung durch Klonen .
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

Für die Installation der Java-Laufzeitumgebung, des Gast-Agent und des Software-Bootstrap-Agents auf Ihrer Windows-Referenzmaschine verwenden Sie ein einzelnes Skript. Auf der Referenzmaschine können Sie eine Vorlage zum Klonen, einen Snapshot oder ein Amazon-Maschinen-Image zwecks Unterstützung der Software-Komponenten erstellen.

Software unterstützt die Skripterstellung mit Windows CMD und PowerShell 2.0.

Wichtig Der Startvorgang darf nicht unterbrochen werden. Konfigurieren Sie die virtuelle Maschine so, dass der Startvorgang der virtuellen Maschine bis zur Anzeige der Anmeldeaufforderung nicht unterbrochen wird. Stellen Sie z. B. sicher, dass beim Start der virtuellen Maschine durch keine Prozesse oder Skripte Benutzereingaben angefordert werden.

Voraussetzungen

- Identifizieren oder erstellen Sie eine Windows-Referenzmaschine.
- Stellen Sie eine sichere vertrauenswürdige Verbindung zwischen der Referenzmaschine und Ihrem IaaS Manager Service-Host her. Siehe [Konfigurieren des Vertrauensverhältnisses zu einem Server für den Gast-Agent](#).

- Wenn Sie Remotezugriff auf die Maschine zwecks Fehlerbehebung oder aus anderen Gründen wünschen, installieren Sie Remote Desktop Services (RDS).
- Entfernen Sie die Artefakte der Netzwerkkonfiguration aus den Netzwerkkonfigurationsdateien.

Verfahren

- 1 Melden Sie sich als Administrator beim Windows-Referenzserver an.
- 2 Öffnen Sie einen Browser zur Software-Downloadseite auf der vRealize Automation-Appliance.

`https://vRealize-Automation-Appliance-FQDN/software`
- 3 Speichern Sie die Vorlagen-ZIP-Datei auf dem Windows-Server.

`prepare_vra_template_windows.zip`
- 4 Extrahieren Sie die ZIP-Inhalte in einen Ordner und führen Sie die Batchdatei aus.

`.\prepare_vra_template.bat`
- 5 Folgen Sie den Anweisungen am Bildschirm.
- 6 Wenn Sie fertig sind, fahren Sie die virtuelle Windows-Maschine herunter.

Ergebnisse

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

Nächste Schritte

Konvertieren Sie die Referenzmaschine in eine Vorlage zum Klonen, einen Snapshot oder ein Amazon-Maschinen-Image. Alle Software-Komponenten werden unterstützt und können von Infrastrukturarchitekten beim Erstellen von Blueprints verwendet werden.

Vorbereiten einer Linux-Referenzmaschine für die Unterstützung von Software

Für die Installation der Java-Laufzeitumgebung, des Gast-Agent und des Software-Bootstrap-Agent auf Ihrer Linux-Referenzmaschine verwenden Sie ein einzelnes Skript. Auf der Referenzmaschine können Sie eine Vorlage zum Klonen, einen Snapshot oder ein Amazon-Maschinen-Image zwecks Unterstützung der Software-Komponenten erstellen.

Software unterstützt Skripting mit Bash.

Wichtig Der Startvorgang darf nicht unterbrochen werden. Konfigurieren Sie die virtuelle Maschine so, dass der Startvorgang der virtuellen Maschine bis zur Anzeige der Anmeldeaufforderung nicht unterbrochen wird. Stellen Sie z. B. sicher, dass beim Start der virtuellen Maschine durch keine Prozesse oder Skripte Benutzereingaben angefordert werden.

Voraussetzungen

- Identifizieren oder erstellen Sie eine Linux-Referenzmaschine.
- Stellen Sie sicher, dass die folgenden Befehle je nach Ihrem Linux-System 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

Sie können auch einen Editor verwenden, um das heruntergeladene `prepare_vra_template.sh`-Skript zu untersuchen, das die verwendeten Befehle bereitstellt.

- Wenn Sie Remotezugriff auf die Maschine zwecks Fehlerbehebung oder aus anderen Gründen wünschen, installieren Sie OpenSSH.
- Entfernen Sie die Artefakte der Netzwerkkonfiguration aus den Netzwerkkonfigurationsdateien.

Verfahren

- 1 Melden Sie sich bei Ihrer Referenzmaschine als Root-Benutzer an.
- 2 Laden Sie das tar.gz-Vorlagenpaket von der vRealize Automation-Appliance herunter.

```
wget https://vrealize-automation-appliance-FQDN/software/download/prepare_vra_template.tar.gz
```

Wenn Ihre Umgebung selbstsignierte Zertifikate verwendet, benötigen Sie möglicherweise die Option `--no-check-certificate`.

```
wget --no-check-certificate https://vrealize-automation-appliance-FQDN/software/download/prepare_vra_template.tar.gz
```

- 3 Dekomprimieren Sie das Paket.
- 4 Suchen Sie in der dekomprimierten Ausgabe das Installationsprogrammskript und führen Sie es aus.

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

- 5 Führen Sie das Installationsskript aus.

```
./prepare_vra_template.sh
```

Informationen zu nicht interaktiven Optionen und erwarteten Werten finden Sie in der Hilfe zum Skript.

```
./prepare_vra_template.sh --help
```

6 Folgen Sie den Anweisungen am Bildschirm.

Bei erfolgreicher Installation wird eine Bestätigung angezeigt. Wenn Fehlermeldungen und Protokolle angezeigt werden, beheben Sie die Fehler und führen Sie das Skript erneut aus.

7 Wenn Sie fertig sind, fahren Sie die virtuelle Linux-Maschine herunter.

Ergebnisse

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

Nächste Schritte

Wandeln Sie die Referenzmaschine auf Ihrem Hypervisor oder Cloud-Anbieter in eine Vorlage zum Klonen, einen Snapshot oder ein Amazon-Maschinen-Image um. Alle Software-Komponenten werden unterstützt und können von Infrastrukturarchitekten beim Erstellen von Blueprints verwendet werden.

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\appd_bootstrap_removal.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.

Verfahren

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.

Ergebnisse

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 Ausführung 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.

Nächste Schritte

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 *Installieren und Konfigurieren von vRealize Automation für das Rainpole-Szenario*.

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`.

Verfahren

- 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.

Ergebnisse

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.

Verfahren

- 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**.

Ergebnisse

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.

Verfahren

- 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**.

Ergebnisse

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

- 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.

Verfahren

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.

Ergebnisse

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.

Verfahren

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

- 2 Laden Sie das Installationsskript von Ihrer 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.

Ergebnisse

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 anhand 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.

Verfahren

- 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**.

Ergebnisse

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.

Verfahren

- 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**.

Ergebnisse

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

Nächste Schritte

- 1 Erstellen Sie ein externes Netzwerkprofil zum Bereitstellen eines Gateways und eines Bereichs von IP-Adressen. Siehe [Erstellen eines externen Netzwerkprofils mithilfe eines IPAM-Drittanbieters](#).
- 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](#).

Vorbereitungen für Mandanten und Ressourcen für die Bereitstellung von Blueprints

2

Sie können mehrere Mandantenumgebungen konfigurieren, jede mit eigenen Gruppen von Benutzern und einem eindeutigen Zugriff auf Ressourcen, die von vRealize Automation verwaltet werden.

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren der Mandanteneinstellungen](#)
- [Konfigurieren von Ressourcen](#)
- [Benutzereinstellungen für Benachrichtigungen und Stellvertretungen](#)

Konfigurieren der Mandanteneinstellungen

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 <i>Installieren und Konfigurieren von vRealize Automation für das Rainpole-Szenario</i> .
<input type="checkbox"/> Konfigurieren der Verzeichnisverwaltung zum Einrichten der Mandanten-Identitätsverwaltung und für den Zugriff auf Steuerungseinstellungen.	Mandantenadministrator	Auswählen der Verzeichnisverwaltungs-Konfigurationsoptionen

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

Aufgabe	vRealize Automation-Rolle	Details
<input type="checkbox"/> Erstellen von Business-Gruppen und benutzerdefinierten Gruppen und Erteilen von Zugriffsrechten für Benutzer auf die vRealize Automation-Konsole.	Mandantenadministrator	Konfigurieren von Gruppen und Benutzerrollen
<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 or	Erstellen weiterer Mandanten
<input type="checkbox"/> (Optional) Konfigurieren von benutzerdefiniertem Branding auf den Anmeldeseiten von Mandanten und auf Anwendungsseiten der vRealize Automation-Konsole.	<input checked="" type="checkbox"/> Systemadministrator <input checked="" type="checkbox"/> Mandantenadministrator	Konfigurieren des benutzerdefinierten Brandings
<input type="checkbox"/> (Optional) Konfigurieren von vRealize Automation, sodass Benachrichtigungen an Benutzer gesendet werden, wenn bestimmte Ereignisse auftreten.	<input checked="" type="checkbox"/> Systemadministrator <input checked="" type="checkbox"/> Mandantenadministrator	Checkliste für die Konfiguration von Benachrichtigungen
<input type="checkbox"/> (Optional) Konfigurieren von vRealize Orchestrator zur Unterstützung von XaaS und weiteren Optionen zur Erweiterbarkeit.	<input checked="" type="checkbox"/> Systemadministrator <input checked="" type="checkbox"/> Mandantenadministrator	Konfigurieren von vRealize Orchestrator
<input type="checkbox"/> (Optional) Erstellen einer benutzerdefinierten Remotedesktop-Protokolldatei, die von IaaS-Architekten in Blueprints zum Konfigurieren von RDP-Einstellungen verwendet wird.	Systemadministrator or	Erstellen einer benutzerdefinierten RDP-Datei zur Unterstützung von RDP-Verbindungen für bereitgestellte Maschinen
<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 or	Ein Beispiel über das Hinzufügen von Datacenter-Standorten finden Sie unter Szenario: Hinzufügen von Datacenter-Standorten für regionsübergreifende Bereitstellungen .

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"> 1 Konfigurieren eines Links zu Active Directory. Siehe Konfigurieren eines Active Directory über LDAP/IWA-Links. 2 Wenn Sie vRealize Automation für Hochverfügbarkeit konfiguriert haben, finden Sie weitere Informationen unter Verzeichnisverwaltung für Hochverfügbarkeit konfigurieren.
(Optional) Erhöhen der Sicherheit eines auf Benutzer-ID und Kennwort basierenden Verzeichnis-Links durch Konfiguration einer bidirektionalen Integration mit Active Directory-Verbindungen.	Konfigurieren einer bidirektionalen Vertrauensstellung zwischen vRealize Automation und Active Directory
(Optional) Hinzufügen von Benutzern und Gruppen zu einem vorhandenen Active Directory-Link.	Hinzufügen von Benutzern oder Gruppen zu einer Active Directory-Verbindung .
(Optional) Bearbeiten der Standardrichtlinie, um benutzerdefinierte Regeln für einen Active Directory-Link anzuwenden.	Verwalten der Benutzerzugriffsrichtlinie .
(Optional) Konfigurieren von Netzwerkbereichen, um die IP-Adressen einzuschränken, über die die Benutzer sich beim System anmelden können, und Verwalten von Anmeldeeinschränkungen (Zeitüberschreitung, Anzahl der Anmeldeversuche vor einer Kontosperrung).	Hinzufügen oder Bearbeiten eines Netzwerkbereichs .

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 Jetzt synchronisieren, um die Verzeichnissynchronisierung manuell zu starten.</p> <p>Siehe Konfigurieren der Verzeichnisverwaltung zum Erstellen eines Active Directory-Links.</p> <p>Wenn Sie auf ein Verzeichnis und dann auf die Schaltfläche Synchronisierungseinstellungen 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 Connector. Siehe Verwalten von Konnektoren und Konnektorclustern.</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 Auswahl der mit dem Verzeichnis zu synchronisierenden Attribute.</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 Hinzufügen oder Bearbeiten eines Netzwerkbereichs.</p>
Identitätsanbieter	<p>Auf der Seite „Identitätsanbieter“ sind die Identitätsanbieter aufgeführt, die in Ihrem System zur Verfügung stehen. vRealize Automation-Systeme enthalten einen Connector, der als standardmäßiger Identitätsanbieter dient und für viele Benutzeranforderungen ausreichend ist. Sie können externe Identitätsanbieterinstanzen hinzufügen oder eine Kombination von Connector und externen Identitätsanbietern verwenden.</p> <p>Siehe Konfigurieren einer Identitätsdrittanbieter-Verbindung.</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 Verwalten der Benutzerzugriffsrichtlinie.</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 zwischen Active Directory und 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 Selbst bei Verwendung eines externen Identitätsanbieters müssen Sie den Connector zum Synchronisieren von Benutzer- und Gruppendaten konfigurieren.

Verzeichnis

Der Directories Management-Dienst verfügt über ein eigenes Verzeichniskonzept, in dem Active Directory-Attribute und -Parameter zum Definieren von Benutzern und Gruppen verwendet werden. Sie können ein oder mehrere Verzeichnisse erstellen und diese Verzeichnisse mit Ihrer Active Directory-Bereitstellung synchronisieren. Im Dienst können die folgenden Verzeichnistypen erstellt werden.

- 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.

Der Dienst hat keinen direkten Zugriff auf Active Directory. Nur der Connector hat direkten Zugriff auf Active Directory. 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 Active Directory und dem Dienst über mindestens einen Worker.

Eine Connector-Instanz kann nicht mit zwei Workern 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 Active Directory über LDAP/IWA-Links](#) . 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 Active Directory über LDAP/IWA-Links](#) . 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 Active Directory über LDAP/IWA-Links](#) . 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 Active Directory über LDAP/IWA-Links](#) . 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.

Es gibt beim Konfigurieren einer Active Directory-Verbindung mithilfe der Verzeichnisverwaltung drei Protokolloptionen für die Active Directory-Kommunikation.

- Active Directory über LDAP – Das Protokoll „Active Directory über LDAP“ unterstützt standardmäßig die DNS-Dienstidentifizierungssuche.
- Active Directory (integrierte Windows-Authentifizierung) - Mit Active Directory (integrierte Windows-Authentifizierung) können Sie die beizutretende Domäne 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.
- OpenLDAP - Sie können die Open Source-Version von LDAP verwenden, um die Benutzerauthentifizierung der Verzeichnisverwaltung zu unterstützen.

Nachdem Sie ein Kommunikationsprotokoll ausgewählt und einen Active Directory-Link konfiguriert 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.

Konfigurieren eines Active Directory über LDAP/IWA-Links

Sie können ein Active Directory über LDAP/IWA-Link zur Unterstützung der Benutzerauthentifizierung unter Verwendung der Directories Management-Funktion konfigurieren, um einen Link zum Active Directory zur Unterstützung von

Benutzerauthentifizierung für alle Mandanten sowie zur Auswahl von Benutzern und Gruppen einzurichten, die mit dem Directories Management-Verzeichnis synchronisiert werden.

Informationen und Anweisungen zum Verwenden von OpenLDAP mit der Verzeichnisverwaltung finden Sie unter [Konfigurieren einer OpenLDAP Directory-Verbindung](#).

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 lokalen Domänengruppe enthält. Wenn Sie diesen Schritt nicht durchführen, fehlen diese Mitglieder in der lokalen Domänengruppe.

Voraussetzungen

- 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.
- Wenn Ihr Active Directory einen Zugriff über SSL oder STARTTLS erfordert, ist das Stamm-Zertifizierungsstellenzertifikat des Active Directory-Domänencontrollers erforderlich.
- Melden Sie sich bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 1 Wählen Sie **Administration > Verwaltung der Verzeichnisse > Verzeichnisse** aus.
- 2 Klicken Sie auf **Verzeichnis hinzufügen** und wählen Sie **Active Directory über LDAP/IWA hinzufügen** aus.
- 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 Active Directory (Integrierte Windows-Authentifizierung) aus. Für die integrierte Windows-Authentifizierung von Active Directory werden die Bind-Benutzer-UPN-Adresse und das entsprechende Kennwort benötigt.
LDAP	Wählen Sie Active Directory über LDAP aus. Für Active Directory über LDAP gehören zu den erforderlichen Informationen der Basis-DN, der Bind-DN und das Bind-DN-Kennwort.

- 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
Synchronisierungs-Connector	Wählen Sie den gewünschten Connector aus, der für Ihr System verwendet werden soll. Jede vRealize Automation-Appliance enthält einen Standardkonnektor. Wenden Sie sich an Ihren Systemadministrator, falls Sie Hilfe bei der Auswahl des geeigneten Connectors benötigen.
Authentifizierung	<p>Klicken Sie auf das entsprechende Optionsfeld, um anzugeben, ob der ausgewählte Connector auch Authentifizierung durchführt.</p> <p>Wenn Sie Active Directory (integrierte Windows-Authentifizierung) mit einem externen Identitätsanbieter zur Authentifizierung von Benutzern verwenden, klicken Sie auf Nein. Nachdem Sie die Active Directory-Verbindung zur Synchronisierung von Benutzern und Gruppen konfiguriert haben, öffnen Sie die Seite „Identitätsanbieter“, um den externen Identitätsanbieter zur Authentifizierung hinzuzufügen.</p> <p>Informationen zur Verwendung von Authentifizierungsadaptern wie PasswordIpddAdapter, SecurIDAdapter und RadiusAuthAdapter finden Sie im <i>Administratorhandbuch für VMware Identity Manager</i>.</p>
Verzeichnissuchattribut	<p>Geben Sie das gewünschte Kontoattribut ein, das den Benutzernamen enthält. Es wird empfohlen, das Attribut „sAMAccount“ anstelle von „userPrincipalName“ zu verwenden. Bei Verwendung von „userPrincipalName“ für Synchronisierungsvorgänge kann es vorkommen, dass die Integration von Software von Zweit- und Drittanbietern, die einen Benutzernamen benötigt, nicht ordnungsgemäß funktioniert.</p> <p>Hinweis Wenn Sie „sAMAccountName“ auswählen, wenn Sie einen globalen Katalog verwenden (aktiviertes Kontrollkästchen Dieses Verzeichnis verfügt über einen globalen Katalog im Bereich „Serverspeicherort“), können sich Benutzer nicht anmelden.</p>

- 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
Serverspeicherort - Wird bei Auswahl von „Active Directory über LDAP“ angezeigt	<p>■ Wenn Sie die DNS-Dienstidentifizierung für die Suche nach Active Directory-Domänen verwenden, behalten Sie die Aktivierung des Kontrollkästchens Dieses Verzeichnis unterstützt die DNS-Dienstidentifizierung bei.</p> <p>Hinweis Wenn Sie diese Option auswählen, können Sie die Portzuweisung nicht in 636 ändern.</p> <p>Gemeinsam mit dem Verzeichnis wird eine automatisch mit einer Liste von Domänencontrollern aufgefüllte <code>domain_krb.properties</code>-Datei erstellt. Siehe Informationen über die Auswahl von Domänencontrollern.</p> <p>Wenn Active Directory eine STARTTLS-Verschlüsselung erfordert, aktivieren Sie das Kontrollkästchen Dieses Verzeichnis erfordert für alle Verbindungen die Verwendung von STARTTLS im Abschnitt „Zertifikate“, kopieren Sie das Active Directory-Stammzertifizierungsstellen-Zertifikat und fügen Sie es in das Feld SSL-Zertifikat ein.</p> <p>■ Falls das angegebene Active Directory keine DNS-Dienstidentifizierungssuche verwendet, deaktivieren Sie in den Server-Speicherort-Feldern das Kontrollkästchen neben Dieses Verzeichnis unterstützt die DNS-Dienstidentifizierung und geben Sie den Hostnamen und die Portnummer für Active Directory ein.</p> <p>Aktivieren Sie das Kontrollkästchen Dieses Verzeichnis verfügt über einen globalen Katalog, wenn das zugeordnete Active Directory einen globalen Katalog verwendet. Ein globaler Katalog enthält eine Darstellung aller Objekte in jeder Domäne einer Active Directory-Gesamtstruktur mit mehreren Domänen.</p> <p>Wenn Sie das Verzeichnis als globalen Katalog konfigurieren möchten, lesen Sie den Abschnitt „Active Directory-Umgebung mit mehreren Domänen in einer einzelnen Struktur“ unter Active Directory-Umgebungen.</p> <p>Wenn Active Directory Zugriff über SSL benötigt, aktivieren Sie unter der Überschrift „Zertifikate“ das Kontrollkästchen Für dieses Verzeichnis müssen alle Verbindungen SSL verwenden und stellen Sie das Active Directory-SSL-Zertifikat bereit.</p> <p>Wenn Sie diese Option auswählen, wird Port 636 automatisch verwendet und kann nicht geändert werden.</p> <p>Vergewissern Sie sich, dass das Zertifikat im PEM-Format vorliegt und die Zeilen „BEGIN CERTIFICATE“ und „END CERTIFICATE“ enthält.</p>
Domänenbeitrittsdetails – Wird bei Auswahl von „Active Directory (Integrierte Windows-Authentifizierung)“ angezeigt.	Geben Sie die entsprechenden Anmeldedaten ein in den Textfeldern Domänenname , Benutzername des Domänenadministrators und Kennwort des Domänenadministrators ein.

Option	Beschreibung
	<p>Wenn Active Directory eine STARTTLS-Verschlüsselung erfordert, aktivieren Sie das Kontrollkästchen Dieses Verzeichnis erfordert für alle Verbindungen die Verwendung von STARTTLS im Abschnitt „Zertifikate“, kopieren Sie das Active Directory-Stammzertifizierungsstellen-Zertifikat und fügen Sie es in das Feld SSL-Zertifikat ein.</p> <p>Vergewissern Sie sich, dass das Zertifikat im PEM-Format vorliegt und die Zeilen „BEGIN CERTIFICATE“ und „END CERTIFICATE“ enthält.</p> <p>Wenn das Verzeichnis mehrere Domänen verwendet, fügen Sie die Stammzertifizierungsstellen-Zertifikate für alle Domänen nacheinander hinzu.</p> <p>Hinweis Wenn für Active Directory STARTTLS erforderlich ist, können Sie das Verzeichnis nicht erstellen, wenn Sie das Zertifikat nicht bereitstellen.</p>

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

Für Active Directory über LDAP:

Option	Beschreibung
Basis-DN	Geben Sie den Basis-Distinguished-Name für die Suche ein. Beispiel: cn=users,dc=corp,dc=local.
Bind-DN	Geben Sie den Bind-Distinguished-Name ein. Beispiel: cn=fritz_infra,cn=users,dc=corp,dc=local

Für Active Directory (Integrierte Windows-Authentifizierung):

Option	Beschreibung
Bind-Benutzer-UPN	Geben Sie den User Principal Name (Benutzername des Prinzipals) des Benutzers ein, der die Domäne authentifizieren kann. Beispiel: Benutzername@example.com.
Bind-DN-Kennwort	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. Wenn Sie eine Gruppe synchronisieren, werden alle Benutzer, für die „Domänenbenutzer“ nicht die primäre Gruppe in Active Directory darstellt, nicht synchronisiert.

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 Arbeitsspeichermenge 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.

Die entsprechenden Werte lauten wie folgt:

- Ein Benutzer: **CN=Benutzername,CN=Users,OU=Users,DC=myCorp,DC=com**

- Mehrere Benutzer: **OU=Users,OU=myUnit,DC=myCorp,DC=com**

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.

Hinweis Stellen Sie sicher, dass Sie Benutzer-DNs angeben, die sich unter dem zuvor angegebenen Basis-DN befinden. Wenn sich der Benutzer-DN außerhalb des Basis-DN befindet, werden die Benutzer dieses DN zwar synchronisiert, können sich aber nicht anmelden.

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

Ergebnisse

Die Verbindung zu Active Directory-Server ist abgeschlossen und die ausgewählten Benutzer und Gruppen werden dem Verzeichnis hinzugefügt. Sie können jetzt Benutzer und Gruppen zu den jeweiligen vRealize Automation-Rollen hinzufügen, indem Sie **Verwaltung > Benutzer und Gruppen > Verzeichnisbenutzer und -gruppen** auswählen. Weitere Informationen hierzu finden Sie unter [Zuweisen von Rollen zu Directory-Benutzern oder -Gruppen Rollen zuweisen](#).

Nächste Schritte

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 Verwaltungskonsolle, die Benutzerportalseiten und den Anmeldebildschirm an.

Konfigurieren einer OpenLDAP Directory-Verbindung

Sie können eine OpenLDAP Directory-Verbindung mit der Verzeichnisverwaltung konfigurieren.

Obwohl es viele unterschiedliche LDAP-Protokolle gibt, ist OpenLDAP das einzige Protokoll, das mit der vRealize Automation-Verzeichnisverwaltung getestet und genehmigt wurde.

Zum Integrieren Ihres LDAP-Verzeichnisses erstellen Sie ein entsprechendes Directories Management-Verzeichnis und synchronisieren Benutzer und Gruppen aus Ihrem LDAP-Verzeichnis mit dem Directories Management-Verzeichnis. Sie können eine regelmäßige Synchronisierung für spätere Aktualisierungen einrichten.

Sie können auch die LDAP-Attribute auswählen, die für Benutzer synchronisiert werden sollen, und diese den Directories Management-Attributen zuordnen.

Ihre LDAP-Verzeichniskonfiguration kann auf Standardschemata basieren; Sie können aber auch benutzerdefinierte Schemata erstellen. Sie können auch benutzerdefinierte Attribute festlegen. Damit Directories Management Ihr LDAP-Verzeichnis nach Benutzer- oder Gruppenobjekten abfragen kann, müssen Sie die LDAP-Suchfilter und Attributnamen angeben, die für Ihr LDAP-Verzeichnis gelten.

Insbesondere müssen Sie folgende Informationen angeben:

- LDAP-Suchfilter zum Abfragen von Gruppen, Benutzern und des Verbindungsbenutzers
- LDAP-Attributnamen für Gruppenmitgliedschaft, UUID und Distinguished Name

Hinweis Verzeichnisverwaltung verwendet die Standardseitengröße von 1.500 für LDAP-Abfragen. Wenn Sie eine Verbindung zu einem OpenLDAP-Verzeichnis konfigurieren, müssen Sie die einfache Erweiterung der Seitenergebnissteuerung für OpenLDAP aktivieren, um die Anzahl der angezeigten Ergebnisse einzuschränken. Wenn Sie diese Erweiterung nicht verwenden, kann es zu Synchronisierungsfehlern bei Benutzern und Gruppen kommen.

Voraussetzungen

- Prüfen Sie die Konfiguration auf der Seite „Benutzerattribute“, und fügen Sie alle weiteren Attribute hinzu, die synchronisiert werden sollen. Sie ordnen die Directories Management-Attribute den Attributen Ihres LDAP-Verzeichnisses beim Erstellen des Verzeichnisses zu. Diese Attribute werden für die im Verzeichnis aufgeführten Benutzer synchronisiert.

Hinweis Wenn Sie Änderungen an Benutzerattributen vornehmen, sollten Sie die Auswirkungen auf andere Verzeichnisse im Dienst berücksichtigen. Wenn Sie sowohl Active Directory als auch LDAP-Verzeichnisse hinzufügen möchten, dürfen Sie mit Ausnahme des Attributs **userName** kein Attribut als erforderlich markieren. Die Einstellungen auf der Seite „Benutzerattribute“ gelten für alle Verzeichnisse im Dienst. Wenn ein Attribut als erforderlich markiert ist, werden Benutzer ohne dieses Attribut nicht mit dem Directories Management-Dienst synchronisiert.

- Ein Bind-DN-Benutzerkonto. Es empfiehlt sich, ein Bind-DN-Benutzerkonto zu verwenden, bei dem das Kennwort nicht abläuft.
- In Ihrem LDAP-Verzeichnis muss die UUID von Benutzern und Gruppen reines Textformat haben.
- In Ihrem LDAP-Verzeichnis muss ein Domänenattribut für alle Benutzer und Gruppen vorhanden sein.

Dieses Attribut ordnen Sie dem Attribut Directories Management-**Domäne** beim Erstellen des Directories Management-Verzeichnisses zu.

- Benutzernamen dürfen keine Leerzeichen enthalten. Wenn ein Benutzername ein Leerzeichen enthält, wird der Benutzer zwar synchronisiert, verfügt jedoch nicht über Berechtigungen.
- Bei Verwendung der zertifikatbasierten Authentifizierung müssen Benutzer Werte für die Attribute „userPrincipalName“ und „E-Mail-Adresse“ haben.

Verfahren

- 1 Wählen Sie **Administration > Verwaltung der Verzeichnisse > Verzeichnisse** aus.
- 2 Klicken Sie auf **Verzeichnis hinzufügen** und wählen Sie **LDAP-Verzeichnis hinzufügen** aus.

3 Geben Sie die erforderlichen Informationen auf der Seite „LDAP-Verzeichnis hinzufügen“ ein.

Option	Beschreibung
Verzeichnisname	Geben Sie einen Namen für das Directories Management-Verzeichnis ein.
Verzeichnissynchronisierung und -authentifizierung	<p>a Wählen Sie im Feld Synchronisierungs-Konnektor den Connector aus, der für die Synchronisierung von Benutzern und Gruppen aus Ihrem LDAP-Verzeichnis mit dem Directories Management-Verzeichnis verwendet werden soll.</p> <p>Standardmäßig ist immer eine Konnektorkomponente mit dem Directories Management-Dienst verfügbar. Dieser Konnektor wird in der Dropdown-Liste angezeigt. Wenn Sie mehrere Directories Management-Appliances für eine Hochverfügbarkeit installieren, erscheint die Konnektorkomponente jeder Appliance in der Liste.</p> <p>Sie benötigen keinen separaten Konnektor für ein LDAP-Verzeichnis. Ein Konnektor kann mehrere Verzeichnisse unterstützen – unabhängig davon, ob es sich dabei um Active Directory oder LDAP-Verzeichnisse handelt.</p> <p>b Wählen Sie im Feld Authentifizierung die Option Ja, wenn Sie dieses LDAP-Verzeichnis für die Authentifizierung von Benutzern verwenden möchten.</p> <p>Wenn die Authentifizierung der Benutzer durch einen externen Identitätsanbieter erfolgen soll, wählen Sie Nein. Öffnen Sie nach dem Hinzufügen der Verzeichnisverbindung zur Synchronisierung von Benutzern und Gruppen die Seite Verwaltung > Verzeichnisverwaltung > Identitätsanbieter, um den externen Identitätsanbieter zur Authentifizierung hinzuzufügen.</p> <p>c Behalten Sie für die meisten Konfigurationen die Standardeinstellung Benutzerdefiniert im Textfeld Verzeichnissuchattribut bei. Geben Sie im Feld Benutzerdefiniertes Verzeichnissuchattribut das für den Benutzer- und Gruppennamen zu verwendende LDAP-Verzeichnisattribut an. Mit diesem Attribut werden Entitäten wie Benutzer und Gruppen vom LDAP-Server eindeutig identifiziert. z. B. cn.</p>
Server-Speicherort	<p>Geben Sie den Host und die Portnummer des LDAP-Verzeichnisseservers ein. Für den Server-Host können Sie entweder den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse angeben. Z. B. meinLDAPserver.beispiel.com oder 100.00.00.0.</p> <p>Wenn sich hinter einem Lastausgleichsdienst ein Server-Cluster befindet, geben Sie stattdessen die Informationen zum Lastausgleichsdienst ein.</p>

Option	Beschreibung
LDAP-Konfiguration	<p>Geben Sie die LDAP-Suchfilter und -Attribute an, die Directories Management zur Abfrage Ihres LDAP-Verzeichnisses verwenden kann. Standardwerte werden auf Basis des LDAP-Grundschemas bereitgestellt.</p> <p>Filterabfragen</p> <ul style="list-style-type: none"> ■ Gruppen: Der Suchfilter zum Abrufen von Gruppenobjekten. Beispiel: (objectClass=group) ■ Verbindungsbenutzer: Der Suchfilter zum Abrufen des Objekts Verbindungsbenutzer, d. h. des Benutzers, der eine Verbindung zum Verzeichnis herstellen kann. Beispiel: (objectClass=person) ■ Benutzer: Der Suchfilter zum Abrufen der zu synchronisierenden Benutzer. Beispiel: (&(objectClass=user)(objectCategory=person)) <p>Attribute</p> <ul style="list-style-type: none"> ■ Mitgliedschaft: Das Attribut, das in Ihrem LDAP-Verzeichnis zum Definieren der Mitglieder einer Gruppe verwendet wird. Beispiel: Mitglied ■ Objekt-UUID: Das Attribut, das in Ihrem LDAP-Verzeichnis zum Definieren der UUID eines Benutzers oder einer Gruppe verwendet wird. Beispiel: entryUUID ■ Distinguished Name: Das Attribut, das in Ihrem LDAP-Verzeichnis zum Definieren des Distinguished Name (definierten Namens) eines Benutzers oder einer Gruppe verwendet wird. Beispiel: entryDN
Zertifikate	<p>Wenn Ihr LDAP-Verzeichnis den Zugriff über SSL erfordert, aktivieren Sie das Kontrollkästchen Dieses Verzeichnis erfordert für alle Verbindungen die Verwendung von SSL. Kopieren Sie dann das CA SSL-Stammzertifikat des LDAP-Verzeichnisseservers in das Textfeld SSL-Zertifikat. Stellen Sie sicher, dass das Zertifikat im PEM-Format vorliegt, und fügen Sie die Zeilen „BEGIN CERTIFICATE“ und „END CERTIFICATE“ ein.</p> <p>Stellen Sie schließlich sicher, dass im Feld Serverport des Seitenabschnitts „Serverspeicherort“ die richtige Portnummer angegeben ist.</p>
Bind-Benutzerdetails	<p>Basis-DN: Geben Sie den DN ein, ab dem die Suche starten soll. Z. B.: cn=Benutzer,dc=Beispiel,dc=com</p> <p>Alle entsprechenden Benutzer müssen sich unter dem Basis-DN befinden. Wenn sich ein bestimmter Benutzer nicht unter dem Basis-DN befindet, kann sich dieser Benutzer auch dann nicht anmelden, wenn er Mitglied einer Gruppe ist, die sich unter diesem Basis-DN befindet.</p> <p>Bind-DN: Geben Sie den für die Verbindung zum LDAP-Verzeichnis zu verwendenden Domänennamen (DN) ein. Sie können auch Benutzernamen eingeben, in den meisten Bereitstellungen ist ein Domänenname jedoch geeigneter.</p> <p>Hinweis Es empfiehlt sich, ein Bind-DN-Benutzerkonto zu verwenden, bei dem das Kennwort nicht abläuft.</p> <p>Bind-DN-Kennwort: Geben Sie das Kennwort für den Bind-DN-Benutzer ein.</p>

- 4 Zum Testen der Verbindung zum LDAP-Verzeichnisserver klicken Sie auf **Verbindung testen**.

Wenn keine Verbindung hergestellt werden kann, prüfen Sie die von Ihnen eingegebenen Informationen, und nehmen Sie entsprechende Änderungen vor.

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

- 6 Stellen Sie sicher, dass auf der Seite „Domänen auswählen“ die richtige Domäne ausgewählt ist, und klicken Sie auf **Weiter**.

- 7 Prüfen Sie auf der Seite „Attribute zuordnen“, ob die Directories Management-Attribute den richtigen LDAP-Attributen zugeordnet sind.

Diese Attribute werden für Benutzer synchronisiert.

Wichtig Sie müssen eine Zuordnung für das Attribut -Domäne angeben.

Sie können der Liste Attribute von der Seite „Benutzerattribute“ hinzufügen.

- 8 Klicken Sie auf **Weiter**.

- 9 Klicken Sie auf **+**, um die Gruppen auszuwählen, die Sie vom LDAP-Verzeichnis in das Directories Management-Verzeichnis auf der Seite „Zu synchronisierende Gruppen (Benutzer) auswählen“ synchronisieren möchten.

Wenn Ihr LDAP-Verzeichnis mehrere Gruppen mit dem gleichen Namen enthält, müssen Sie für sie eindeutige Namen auf der Seite „Gruppen“ angeben.

Enthält eine aus Active Directory hinzugefügte Gruppe Mitglieder, die nicht in der Benutzerliste enthalten sind, werden sie hinzugefügt. Wenn Sie eine Gruppe synchronisieren, werden alle Benutzer, für die „Domänenbenutzer“ nicht die primäre Gruppe in Active Directory darstellt, nicht synchronisiert.

Die Option **Mitglieder verschachtelter Gruppen synchronisieren** ist standardmäßig aktiviert. Wenn diese Option aktiviert ist, werden alle Benutzer synchronisiert, die direkt zu der von Ihnen ausgewählten Gruppe gehören, sowie alle Benutzer, die zu darin vorhandenen verschachtelten Gruppen gehören. Beachten Sie, dass die verschachtelten Gruppen selbst nicht synchronisiert werden. Es werden nur die Benutzer synchronisiert, die zu den verschachtelten Gruppen gehören. Im Directories Management-Verzeichnis werden diese Benutzer als Mitglieder der obersten Gruppe angezeigt, die Sie für die Synchronisierung ausgewählt haben. Tatsächlich wird die Hierarchie unter einer ausgewählten Gruppe geglättet; Benutzer aus allen Ebenen in Directories Management werden als Mitglieder der ausgewählten Gruppe angezeigt.

Wenn diese Option deaktiviert ist und Sie eine Gruppe für die Synchronisierung festlegen, werden alle Benutzer, die direkt zu dieser Gruppe gehören, synchronisiert. Benutzer, die zu verschachtelten Gruppen gehören, werden in diesem Fall nicht synchronisiert. Das Deaktivieren dieser Option ist bei großen Verzeichniskonfigurationen sinnvoll, bei denen die Durchsicht eines Gruppenstrukturbaums ressourcen- und zeitintensiv ist. Wenn Sie diese Option deaktivieren, stellen Sie sicher, dass Sie alle Gruppen auswählen, deren Benutzer Sie synchronisieren möchten.

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-Verzeichnisverwaltung die erforderliche Arbeitsspeichermenge zugeteilt hat. Wenn das Problem weiterhin besteht, erhöhen Sie die Arbeitsspeicherzuteilung für die Verzeichnisverwaltung nach Bedarf. Bei Systemen mit einer großen Anzahl von Benutzern und Gruppen muss möglicherweise die Arbeitsspeicherzuteilung für die Verzeichnisverwaltung auf bis zu 24 GB erhöht werden.

10 Klicken Sie auf **Weiter**.

11 Um zusätzliche Benutzer hinzuzufügen, klicken Sie auf **+**. Geben Sie beispielsweise **CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com** ein.

Sie können Organisationseinheiten sowie Einzelbenutzer hier hinzufügen.

Sie können einen Filter für den Ausschluss bestimmter Benutzertypen erstellen. Dazu wählen Sie das Benutzerattribut für den Filter, die Abfragerregel und den Wert aus.

12 Klicken Sie auf **Weiter**.

13 Überprüfen Sie auf der Seite, wie viele Benutzer und Gruppen mit dem Verzeichnis synchronisiert werden und wie die Standardsynchronisierung terminiert ist.

Um Änderungen für Benutzer und Gruppen oder für die Synchronisierungshäufigkeit durchzuführen, klicken Sie jeweils auf **Bearbeiten**.

14 Klicken Sie auf **Verzeichnis synchronisieren**, um die Verzeichnissynchronisierung zu starten.

Ergebnisse

Die Verbindung zum LDAP-Verzeichnis ist hergestellt. Benutzer und Gruppen werden aus dem LDAP-Verzeichnis mit dem Directories Management-Verzeichnis synchronisiert.

Sie können jetzt Benutzer und Gruppen zu den jeweiligen vRealize Automation-Rollen hinzufügen, indem Sie **Verwaltung > Benutzer und Gruppen > Verzeichnisbenutzer und -gruppen** auswählen. Weitere Informationen hierzu finden Sie unter [Zuweisen von Rollen zu Directory-Benutzern oder -Gruppen Rollen zuweisen](#).

Einschränkungen bei der Integration von LDAP-Verzeichnissen

Es gibt mehrere wichtige Einschränkungen im Zusammenhang mit der Integration von LDAP-Verzeichnissen in der Verzeichnisverwaltung.

- Sie können nur eine Domäne aus einem LDAP-Verzeichnis integrieren.
Zur Integration mehrerer Domänen aus einem LDAP-Verzeichnis müssen Sie zusätzliche Directories Management-Verzeichnisse erstellen, jeweils ein Verzeichnis pro Domäne.
- Folgende Authentifizierungsmethoden werden nicht für Directories Management-Verzeichnisse des Typs LDAP-Verzeichnis unterstützt:
 - Kerberos-Authentifizierung
 - Adaptive RSA-Authentifizierung
 - ADFS als externer Identitätsanbieter
 - SecurID
 - Radius-Authentifizierung mit Vasco- und SMS-Kennungsserver
- Sie können einer LDAP-Domäne nicht beitreten.
- Die Integration in View oder von Citrix veröffentlichte Ressourcen wird für Directories Management-Verzeichnisse des Typs LDAP-Verzeichnis nicht unterstützt.
- Benutzernamen dürfen keine Leerzeichen enthalten. Wenn ein Benutzername ein Leerzeichen enthält, wird der Benutzer zwar synchronisiert, verfügt jedoch nicht über Berechtigungen.
- Wenn Sie sowohl Active Directory als auch LDAP-Verzeichnisse hinzufügen möchten, dürfen Sie mit Ausnahme des Attributs `userName`, das als erforderlich markiert werden kann, kein Attribut als erforderlich auf der Seite „Benutzerattribute“ markieren. Die Einstellungen auf der Seite „Benutzerattribute“ gelten für alle Verzeichnisse im Dienst. Wenn ein Attribut als erforderlich markiert ist, werden Benutzer ohne dieses Attribut nicht mit dem Directories Management-Dienst synchronisiert.
- Wenn Ihr LDAP-Verzeichnis mehrere Gruppen mit dem gleichen Namen enthält, müssen Sie für sie eindeutige Namen im Directories Management-Dienst angeben. Sie können die Namen bei der Auswahl der zu synchronisierenden Gruppen angeben.
- Die Option, Benutzern das Zurücksetzen von abgelaufenen Kennwörtern zu gestatten, ist nicht verfügbar.
- Die Datei `domain_krb.properties` wird nicht unterstützt.

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 manuell 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.

Ein Connector wird auch für die Benutzersynchronisierung verwendet. Es ist jedoch nur ein Connector für die Verzeichnissynchronisierung konfiguriert. Synchronisierte Benutzer werden in der Appliance-Datenbank gespeichert, die von allen geclusterten Knoten gelesen werden kann. Wenn der für die Verzeichnissynchronisierung zuständige Connector fehlschlägt, funktioniert die Verzeichnissynchronisierung nicht mehr. Zur Wiederherstellung muss der Mandantenadministrator manuell einen anderen Connector zum Ausführen der Verzeichnissynchronisierung über die vRealize Automation-Benutzeroberfläche auffordern. Siehe [Aktivieren der Verzeichnissynchronisierung auf einem sekundären Connector](#).

Weitere Informationen zum Arbeiten mit Connectors finden Sie unter [Verwalten von Konnektoren und Konnektorclustern](#).

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 [Konfigurieren der Mandanteneinstellungen](#).

Verfahren

- 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 derzeit 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 aus, der Ihrer sekundären vRealize Automation-Appliance entspricht.
- 5 Geben Sie das entsprechende Kennwort in das 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.

Aktivieren der Verzeichnissynchronisierung auf einem sekundären Connector

Wenn Ihr primärer Connector fehlschlägt, wird die Authentifizierung automatisch durch eine andere Connector-Instanz verarbeitet. Im Falle eines Fehlers bei der Verzeichnissynchronisierung müssen Sie die Verzeichniseinstellungen in der Verzeichnisverwaltung ändern, um die entsprechende sekundäre Connector-Instanz zu verwenden. Sie können die Verzeichnissynchronisierung jeweils nur auf einem Connector aktivieren.

Verfahren

- 1 Wählen Sie **Verwaltung > Verzeichnisverwaltung > Verzeichnisse** aus.
- 2 Wählen Sie das Verzeichnis aus, das der ursprünglichen Connector-Instanz zugeordnet war.

Hinweis Sie können diese Informationen auf der Seite **Verzeichnisse > Connectors** anzeigen.

- 3 Wählen Sie im Abschnitt „Verzeichnissynchronisierung und Authentifizierung“ der Seite „Verzeichnis“ eine andere Connector-Instanz in der Dropdown-Liste **Synchronisierungs-Connector** aus.
- 4 Geben Sie im Abschnitt „Bind-Benutzerdetails“ das Kennwort für Ihr Active Directory-Bind-Konto in das Textfeld **Bindungs-DN-Kennwort** ein.
- 5 Klicken Sie auf **Speichern**.

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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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
Name des Identitätsanbieters	Einen Namen für den neuen Identitätsanbieter eingeben
Metadaten des Identitätsanbieters (URI oder XML)	Fügen Sie die Inhalte der Metadatendatei der Active Directory-Verbindungsdienste hier ein.
Richtlinien für Namen-ID in SAML-Anforderung (optional)	Geben Sie bei Bedarf einen Namen für die SAML-Anforderung der Identitätsrichtlinien ein.
Benutzer	Wählen Sie die Domains aus, auf die Benutzer Zugriff haben sollen.
IDP-Metadaten verarbeiten	Klicken Sie, um die hinzugefügte Metadatendatei zu verarbeiten.
Netzwerk	Wählen Sie die Netzwerkbereiche aus, auf die Benutzer Zugriff haben sollen.
Authentifizierungsmethoden	Geben Sie einen Namen für die Authentifizierungsmethode ein, die von diesem Identitätsanbieter verwendet wird.
SAML-Kontext	Wählen Sie für das System den entsprechenden Kontext aus.
SAML-Signaturzertifikat	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 Ihr Netzwerkbereich **Mein Computer** ist und Sie auf Inhalte über **Alle Gerätetypen** zugreifen müssen, dann müssen Sie sich 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 Verwaltungskonsole 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 abgerufen Attribute in der „Attribute abrufen“-Regel in das gewünschte SAML-Format umwandeln. Nachdem Sie die Regel erstellt haben, bearbeiten Sie die Regel, indem Sie den 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. Komponentenkonfiguration 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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

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

Hinzufügen von Benutzern oder Gruppen zu einer Active Directory-Verbindung

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

Das Benutzerauthentifizierungssystem der Verzeichnisverwaltung importiert beim Hinzufügen von Gruppen und Benutzern Daten aus Active Directory. Die Geschwindigkeit des Imports wird durch die Active Directory-spezifischen Datenübertragungsmöglichkeiten beschränkt. Dies führt dazu, dass Aktionen je nach Anzahl der Gruppen und Benutzer, die hinzugefügt werden, viel Zeit in Anspruch nehmen können. Um Probleme zu minimieren, begrenzen Sie die Gruppen und Benutzer auf diejenigen, die für eine vRealize Automation-Aktion erforderlich sind. Falls Probleme auftreten, schließen Sie nicht benötigte Anwendungen und vergewissern Sie sich, dass Active Directory ausreichend Arbeitsspeicher von Ihrer Bereitstellung zugeteilt wurde. Sollten weiterhin Probleme auftreten, erhöhen Sie die Active Directory zugeteilte Menge an Arbeitsspeicher. Bei Bereitstellungen mit einer großen Anzahl von Benutzern und Gruppen muss möglicherweise die Arbeitsspeicherzuteilung für Active Directory auf bis zu 24 GB erhöht werden.

Wenn Sie eine vRealize Automation-Bereitstellung mit vielen Benutzern und Gruppen synchronisieren, kann eine Verzögerung eintreten, bevor die Protokolldetails verfügbar sind. Der Zeitstempel der Protokolldatei kann von dem auf der Konsole angezeigten Zeitpunkt der Fertigstellung abweichen.

Wenn Sie eine Gruppe aus Active Directory hinzufügen und Mitglieder der Gruppe nicht in der Benutzerliste enthalten sind, werden diese Mitglieder zur Liste hinzugefügt. Wenn Sie eine Gruppe synchronisieren, werden Benutzer, für die „Domänenbenutzer“ nicht die primäre Gruppe in Active Directory darstellt, nicht synchronisiert.

Hinweis Sie können eine Synchronisierungsaktion nicht abbrechen, nachdem Sie sie gestartet haben.

Voraussetzungen

- Installierter Connector mit aktiviertem Aktivierungscode. Auf der Seite „Benutzerattribute“ können Sie die erforderlichen Standardattribute auswählen und zusätzliche Attribute hinzufügen.

Weitere Informationen finden Sie unter *Auswählen von Attributen zur Verzeichnissynchronisierung* in *Konfigurieren von vRealize Automation*.

- 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.

- Wenn Sie Active Directory mit mehreren Gesamtstrukturen und integrierter Windows-Authentifizierung nutzen und die lokale Gruppe der Domäne Mitglieder aus verschiedenen Gesamtstrukturen umfasst, führen Sie die folgenden Schritte aus. Fügen Sie den Bind-Benutzer zur Gruppe „Administratoren“ der lokalen Gruppe der Domäne hinzu. Ohne Hinzufügen des Bind-Benutzers fehlen diese Mitglieder in der lokalen Gruppe der Domäne.
- Melden Sie sich bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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 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 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 die Änderungen zu speichern, ohne die Aktualisierungen sofort zu synchronisieren. Klicken Sie auf **Speichern und synchronisieren**, um die Änderungen zu speichern und die Aktualisierungen sofort zu synchronisieren.

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.

Verfahren

- 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**.

Ergebnisse

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 vielezählreiche 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.

Der Arbeitsspeicher für die Verzeichnisverwaltung wird basierend auf dem der vRealize Automation-Appliance zugeordneten Gesamtarbeitsspeicher berechnet. In der folgenden Tabelle finden Sie Arbeitsspeicherzuteilungen für die relevanten Komponenten.

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

Arbeitsspeicher für die virtuellen Appliance	Arbeitsspeicher für den vRA-Dienst	Arbeitsspeicher für den vDM-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.

Verfahren

- 1 Beenden Sie alle Maschinen, auf denen eine vRealize Automation-Appliance ausgeführt wird.
- 2 Erhöhen Sie auf jeder Maschine die Arbeitsspeicherzuteilung für die virtuelle Appliance.
Wenn Sie eine Standard-Arbeitsspeicherzuteilung von 18 GB verwenden, empfiehlt VMware die 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.

Verfahren

- 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.

Konfigurieren der Just-in-Time-Benutzerbereitstellung

Sie können die Just-in-Time-Bereitstellung (JIT) konfigurieren, um das Hinzufügen von Benutzern ohne Synchronisierung von Active Directory zu unterstützen.

Zur Unterstützung der Just-in-Time-Bereitstellung müssen Sie einen externen Identitätsanbieter hinzufügen und dann eine Verbindung dazu innerhalb Ihrer vRealize Automation-Bereitstellung konfigurieren, um die Verzeichnisverwaltung in andere SSO-Anbieter über ein SAML-Protokoll zu integrieren. Darüber hinaus müssen Sie ein neues Verzeichnis mit dem entsprechenden Namen erstellen, wie z. B. JIT-Verzeichnis.

Wenn Sie die Just-in-Time-Bereitstellung aktivieren, können Sie Just-in-Time-Benutzer zu einer designierten benutzerdefinierten Gruppe hinzufügen. Um diese Funktionalität zu unterstützen, erstellen Sie eine benutzerdefinierte Gruppe mit den entsprechenden Mitgliedern. Siehe [Hinzufügen von Just-in-Time-Benutzern mit benutzerdefinierten Gruppen und Regeln](#).

Hinweis Konfigurieren Sie als Best Practice keine Just-in-Time-Bereitstellung auf dem Standardmandanten „`vsphere.local`“.

Voraussetzungen

Konfigurieren Sie einen entsprechenden externen Identitätsanbieter für die Verwendung mit JIT-Bereitstellung.

Verfahren

- 1 Erstellen Sie einen Identitätsanbieter für die Just-in-Time-Bereitstellung.
 - a Wählen Sie **Administration > Verzeichnisverwaltung > Identitätsanbieter** aus.
 - b Klicken Sie auf **Identitätsanbieter hinzufügen** und bearbeiten Sie die Einstellungen für die Identitätsanbieterinstanz nach Bedarf.
 - Erstellen Sie für die Just-in-Time-Bereitstellung einen externen Identitätsanbieter.
 - Geben Sie im Abschnitt „Just-in-Time-Verzeichnis erstellen“ Namen für das Verzeichnis und eine oder mehrere Domänen ein.
 - Sie müssen ein Netzwerk für die Konfiguration des externen Identitätsanbieters auswählen.
 - Wenn Sie einen externen VMware Identity Manager als externen Identitätsanbieter verwenden und Benutzer mit `userPrincipalName` authentifizieren, müssen Sie die Konfiguration der Namen-ID-Zuordnung für `userPrincipalName` vom Standardwert `x509SubjectName` in `unspecified` ändern.

Unter [Konfigurieren einer Identitätsdrittanbieter-Verbindung](#) finden Sie weitere Informationen zum Erstellen von Identitätsanbietern.
- 2 Konfigurieren Sie SAML für den Just-in-Time-Identitätsanbieter.
 - a Kopieren Sie Identitätsanbieter-Metadaten aus Ihrem Identitätsanbieter.
 - b Wählen Sie in vRealize Automation Ihren Identitätsanbieter aus und fügen Sie die Identitätsanbieter-Metadaten in das Textfeld **Identitätsanbieter-Metadaten (URL oder XML)** ein.
 - c Klicken Sie auf **Speichern**.
 - d Wählen Sie im Dropdown-Menü **Namen-ID-Richtlinien in SAML-Anforderung (optional)** das entsprechende Format aus.

Wenn Sie beispielsweise die E-Mail-Adresse als eindeutige Benutzer-ID verwenden, würden Sie `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress` auswählen.
 - e Wählen Sie das entsprechende Verzeichnis unter der Überschrift „Benutzer“ aus.
 - f Wählen Sie die Netzwerke für diesen Identitätsanbieter unter der Überschrift „Netzwerk“ aus.
 - g Geben Sie einen geeigneten Namen in das Textfeld **Authentifizierungsmethoden** ein.
 - h Wählen Sie in der Dropdown-Liste **SAML-Kontext** die Option `urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport` aus.
 - i Klicken Sie mit der rechten Maustaste auf den Link **Metadaten des Dienstanbieters (SP)** und öffnen Sie diesen in einer separaten Browserregisterkarte.
 - j Verwenden Sie diese Metadaten, um die SAML-Verbindung für Ihren Identitätsanbieter zu konfigurieren.

Wenn Sie VMware Identity Manager verwenden, finden Sie in der VMware Identity Manager-Dokumentation vollständige Anweisungen zur Konfiguration von SAML.

3 Klicken Sie auf **Hinzufügen**.

Das neue Verzeichnis wird mit dem angegebenen Verzeichnisnamen erstellt.

4 Konfigurieren Sie die vRealize Automation-Zugriffsrichtlinie.

- a Wählen Sie **Administration > Richtlinien** aus.
- b Klicken Sie auf das grüne +-Symbol in der oberen rechten Ecke der Richtlinienregeltabelle.
- c Legen Sie die Richtlinienregel für die entsprechenden Bereiche und Gerätetypen fest.
- d Wählen Sie die Authentifizierungsmethode aus, die Sie beim Konfigurieren des externen Identitätsanbieters für JIT-Bereitstellung erstellt haben.

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 Sie auf der Seite „Benutzerattribute“ vornehmen und speichern, werden der Seite „Zugeordnete Attribute“ im Directories Management-Verzeichnis hinzugefügt. Bei der nächsten Synchronisierung mit Active Directory werden die Attributänderungen im Verzeichnis aktualisiert.

Auf der Seite „Benutzerattribute“ sind die Standardverzeichnisattribute aufgelistet, die Sie den Active Directory-Attributen zuordnen 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 hinzu.
disabled (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

Tabelle 2-6. Standardzuordnung von Verzeichnisattributen zu Active Directory-Attributen (Fortsetzung)

Verzeichnisattributname	Standardzuordnung zu Active Directory-Attribut
firstName	givenName
email	mail
userName	sAMAccountName

Auf der Seite „Benutzerattribute“ sind die Standardverzeichnisattribute aufgelistet, die Sie den Active Directory-Attributen zuordnen 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 hinzu.
disabled (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 und Konnektorclustern

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 aus, 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 Identitätsdrittanbieter-Verbindung](#).
- 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.

Konnektoren in einer Clusterumgebung

In einer verteilten vRealize Automation-Bereitstellung führen alle verfügbare Konnektoren die gesamte erforderliche Benutzerautorisierung durch, während ein einzelner festgelegter Konnektor für die gesamte Konfigurationssynchronisierung zuständig ist. In der Regel beinhaltet die Synchronisierung Erweiterungen, Löschvorgänge oder Änderungen an der Benutzerkonfiguration, und die Synchronisierung erfolgt automatisch unter der Voraussetzung, dass alle Konnektoren verfügbar sind. Es gibt bestimmten Situationen, in denen die automatische Synchronisierung nicht stattfindet.

Bei Änderungen im Zusammenhang mit der Verzeichniskonfiguration, wie z. B. bei Änderungen am Basis-DN, versucht vRealize Automation, Updates automatisch an alle Konnektoren in einem Cluster weiterzugeben. Wenn ein Konnektor aus irgendeinem Grund ausgefallen oder nicht erreichbar ist, erhält dieser Konnektor auch dann nicht das Update, wenn er im Online-Betrieb fortgesetzt wird. Um Konfigurationsänderungen in Konnektoren zu implementieren, an die diese Änderungen möglicherweise nicht automatisch weitergegeben wurden, müssen Systemadministratoren die Änderungen in allen anwendbaren Konnektoren manuell speichern.

Bei Änderungen am Profil der Verzeichnissynchronisierung versucht vRealize Automation ebenfalls, die Updates an alle Konnektoren weiterzugeben. Wenn der Synchronisierungskonnektor funktionsfähig ist, wird das Update gespeichert und an alle verfügbaren Autorisierungskonnektoren weitergegeben. Wenn mindestens ein Konnektor nicht erreichbar ist, empfängt der Systemadministrator eine Warnmeldung darüber, dass nicht alle Konnektoren aktualisiert wurden. Wenn der Synchronisierungskonnektor aus anderen Gründen nicht funktionsfähig ist, schlägt das Update fehl und ein Fehler tritt auf. Wenn der Systemadministrator den als Synchronisierungskonnektor festgelegten Konnektor ändert, empfängt der neue Synchronisierungskonnektor die neuesten verfügbaren Profilinformationen, und diese Informationen werden an alle anwendbaren und verfügbaren Konnektoren weitergegeben.

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.

Verfahren

- 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.

Verfahren

- 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](#).

Verfahren

- 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 Domännennamen 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.

Name der Richtlinie STANDARDRICHTLINIE

Beschreibung

Gültig für

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)	✗ +

- 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 Identitätsdrittanbieter-Verbindung](#).
- 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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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**.

Konfigurieren von zusätzlichen Identitätsanbieterverbindungen

Sie können bei Bedarf zusätzliche Identitätsanbieterverbindungen konfigurieren, um unterschiedliche Identitätsverwaltungsszenarien zu unterstützen, einschließlich zusätzlicher integrierter Identitätsanbieter und Identitätsanbieter von Drittunternehmen.

Sie können drei Typen von Identitätsanbieterverbindungen mithilfe der Verzeichnisverwaltung erstellen.

- **Drittanbieter-IDP erstellen** – Verwenden Sie dieses Element, um eine Verbindung mit einem externen Identitätsanbieter eines Drittunternehmens zu erstellen. Stellen Sie sicher, dass Sie Folgendes haben, bevor Sie eine Identitätsanbieter-Instanz eines Drittunternehmens hinzufügen.
 - 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 Metadateninformationen 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.

- **Arbeitsumgebungs-IDP erstellen** – Wenn Sie einen Konnektor zur Authentifizierung von Benutzern während der Konfiguration der Verzeichnisverwaltung aktivieren, wird ein Arbeitsumgebungs-IDP als Identitätsanbieter erstellt und die Kennwort-Authentifizierung wird aktiviert. Sie können zusätzliche Arbeitsumgebungsidentitätsanbieter hinter unterschiedlichen Lastausgleichsdiensten konfigurieren.
- **Integrierten IDP erstellen** – Integrierte Identitätsanbieter verwenden die internen Verzeichnisverwaltungsmechanismen zur Unterstützung der Authentifizierung. Sie können konfigurieren, dass die integrierten Identitätsanbieter Authentifizierungsmethoden verwenden, die nicht die Verwendung eines lokalen Konnektors erfordern. Wenn Sie den integrierten Anbieter konfigurieren, weisen Sie die Authentifizierungsmethoden zu, die mit dem Anbieter verwendet werden sollen.
- **Konfigurieren einer Identitätsdrittanbieter-Verbindung**
vRealize Automation enthält eine Identitätsanbieter-Verbindungs-Standardinstanz. Benutzer können zusätzliche Identitätsanbieter-Verbindungen erstellen, um Just-in-time-Benutzerbereitstellungen oder andere benutzerdefinierte Konfigurationen zu unterstützen.
- **Konfigurieren zusätzlicher Arbeitsumgebungsidentitätsanbieter**
Wenn Sie einen Verzeichnisverwaltungskonnektor zum Authentifizieren von Benutzern konfigurieren, wird ein Arbeitsumgebungsidentitätsanbieter erstellt und die Kennwortauthentifizierung aktiviert.
- **Konfigurieren einer integrierten Identitätsanbieter-Verbindung**
Sie können mehrere integrierte Identitätsanbieter konfigurieren und ihnen Authentifizierungsmethoden zuordnen.

Konfigurieren einer Identitätsdrittanbieter-Verbindung

vRealize Automation enthält eine Identitätsanbieter-Verbindungs-Standardinstanz. Benutzer können zusätzliche Identitätsanbieter-Verbindungen erstellen, um Just-in-time-Benutzerbereitstellungen oder andere benutzerdefinierte Konfigurationen zu unterstützen.

vRealize Automation enthält einen Standard-Identitätsanbieter. In den meisten Fällen werden die Kundenbedürfnisse mit dem Standardanbieter ausreichend abgedeckt. Wenn Sie eine vorhandene Identitätsverwaltungslösung für Unternehmen verwenden, können Sie einen benutzerdefinierten Identitätsanbieter so einrichten, dass die Benutzer zu Ihrer vorhandenen Identitätslösung umgeleitet werden.

Wenn Sie einen benutzerdefinierten Identitätsanbieter verwenden, verwendet die Verzeichnisverwaltung SAML-Metadaten von diesem Anbieter, um eine Vertrauensbeziehung mit dem Anbieter einzurichten. Nachdem diese Beziehung eingerichtet ist, ordnet die Verzeichnisverwaltung die Benutzer von der SAML-Assertion zur Liste der internen vRealize Automation-Benutzer basierend auf der Subjektnamen-ID zu.

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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Identitätsanbieter** aus.
Auf der Seite werden alle konfigurierten Identitätsanbieter angezeigt.
- 2 Klicken Sie auf **Identitätsanbieter hinzufügen**.
Ein Menü mit Identitätsanbieteroptionen wird angezeigt.
- 3 Wählen Sie **Create Third Party IDP** (IDP Dritter erstellen) aus.
- 4 Geben Sie die entsprechenden Informationen ein, um den Identitätsanbieter zu konfigurieren.

Option	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"> 1 Geben Sie die SAML-Metadaten-URL oder den xml-Inhalt in das Textfeld ein. 2 Klicken Sie auf IDP-Metadaten verarbeiten. Die von IdP unterstützten Formate der Namens-ID werden aus den Metadaten extrahiert und der Tabelle mit den Formaten der Namens-ID hinzugefügt. 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. 4 (Optional) Wählen Sie das Zeichenfolgenformat für den NameIDPolicy-Antwortbezeichner aus.
Benutzer	Wählen Sie die Directories Management-Verzeichnisse der Benutzer aus, die sich mit diesem Identitätsanbieter authentifizieren können.
Just-in-Time-Benutzerbereitstellung	<p>Wählen Sie die entsprechenden Optionen zur Unterstützung der Just-in-Time-Bereitstellung mit einem entsprechenden externen Identitätsanbieter aus.</p> <p>Geben Sie den Verzeichnisnamen für die Verwendung in der Just-in-Time-Bereitstellung ein.</p> <p>Geben Sie eine oder mehrere Domänen ein, die innerhalb des externen Identitätsanbieters vorhanden sind, der für die Just-in-Time-Bereitstellung verwendet wird.</p>
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>

Option	Beschreibung
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 Metadaten des Dienstanbieters , 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 Hostname 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: myco.example.com:8443.

5 Klicken Sie auf **Hinzufügen**.

Nächste Schritte

- 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*.

Konfigurieren zusätzlicher Arbeitsumgebungsidentitätsanbieter

Wenn Sie einen Verzeichnisverwaltungskonnektor zum Authentifizieren von Benutzern konfigurieren, wird ein Arbeitsumgebungsidentitätsanbieter erstellt und die Kennwortauthentifizierung aktiviert.

Sie können zusätzliche Konnektoren für den Betrieb hinter mehreren Lastausgleichsdiensten konfigurieren. Wenn Ihre Bereitstellung mehr als einen Lastausgleichsdienst enthält, können Sie in jeder Lastausgleichsdienstkonfiguration einen anderen Arbeitsumgebungsidentitätsanbieter für die Authentifizierung verwenden.

Verfahren

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Identitätsanbieter** aus.
Auf der Seite werden alle konfigurierten Identitätsanbieter angezeigt.
- 2 Klicken Sie auf **Identitätsanbieter hinzufügen**.
Ein Menü mit Identitätsanbieteroptionen wird angezeigt.
- 3 Wählen Sie **Arbeitsumgebungsidentitätsanbieter erstellen**.

4 Geben Sie die entsprechenden Informationen ein, um den Identitätsanbieter zu konfigurieren.

Option	Beschreibung
Name des Identitätsanbieters	Geben Sie den Namen für diese Instanz des integrierten Identitätsanbieters ein.
Benutzer	Wählen Sie die zu authentifizierenden Benutzer aus. Die konfigurierten Verzeichnisse werden aufgeführt.
Benutzer	Wählen Sie die Verzeichnisse der Benutzer aus, die sich mit diesem Arbeitsumgebungsidentitätsanbieter authentifizieren können.
Netzwerk	Die im Dienst konfigurierten vorhandenen Netzwerkbereiche werden aufgeführt. Wählen Sie den Netzwerkbereich für die Benutzer anhand der IP-Adressen aus, die Sie zu dieser Identitätsanbieter-Instanz für die Authentifizierung umleiten möchten.
Authentifizierungsmethoden	Die Authentifizierungsmethoden, die für den Dienst konfiguriert sind, werden angezeigt. Aktivieren Sie das Kontrollkästchen für die Authentifizierungsmethoden, um sie diesem Identitätsanbieter zuzuweisen. Für die Konformität des Geräts und des Kennworts stellen Sie bei AirWatch und AirWatch Connector sicher, dass die Option auf der AirWatch-Konfigurationsseite aktiviert ist.

5 Klicken Sie auf **Hinzufügen**.

Konfigurieren einer integrierten Identitätsanbieter-Verbindung

Sie können mehrere integrierte Identitätsanbieter konfigurieren und ihnen Authentifizierungsmethoden zuordnen.

Voraussetzungen

Wenn Sie die integrierte Kerberos-Authentifizierung verwenden, laden Sie das Zertifikat des KDC-Serverzertifikatsausstellers für die AirWatch-Konfiguration des iOS-Geräteverwaltungsprofils herunter.

Verfahren

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Identitätsanbieter** aus.
Auf der Seite werden alle konfigurierten Identitätsanbieter angezeigt.
- 2 Klicken Sie auf **Identitätsanbieter hinzufügen**.
Ein Menü mit Identitätsanbieteroptionen wird angezeigt.
- 3 Wählen Sie **Integrierten Identitätsanbieter erstellen** aus.
- 4 Geben Sie die entsprechenden Informationen ein, um den Identitätsanbieter zu konfigurieren.

Option	Beschreibung
Name des Identitätsanbieters	Geben Sie den Namen für diese Instanz des integrierten Identitätsanbieters ein.
Benutzer	Wählen Sie die zu authentifizierenden Benutzer aus. Die konfigurierten Verzeichnisse werden aufgeführt.

Option	Beschreibung
Netzwerk	Die im Dienst konfigurierten vorhandenen Netzwerkbereiche werden aufgeführt. Wählen Sie den Netzwerkbereich für die Benutzer anhand der IP-Adressen aus, die Sie zu dieser Identitätsanbieter-Instanz für die Authentifizierung umleiten möchten.
Authentifizierungsmethoden	<p>Die Authentifizierungsmethoden, die für den Dienst konfiguriert sind, werden angezeigt. Aktivieren Sie das Kontrollkästchen für die Authentifizierungsmethoden, um sie diesem Identitätsanbieter zuzuweisen.</p> <p>Für die Konformität des Geräts und des Kennworts stellen Sie bei AirWatch und AirWatch Connector sicher, dass die entsprechende Option auf der AirWatch-Konfigurationsseite aktiviert ist.</p>

5 Klicken Sie auf **Hinzufügen**.

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 ManagementConnector-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 Benutzernamen 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.

Verfahren

- 1 Fügen Sie den Directories Management Connector auf einer unterstützten Version des RSA SecurID-Servers als Authentifizierungs-Agent hinzu. Geben Sie die folgenden Informationen ein.

Option	Beschreibung
Hostname	Hostname von Directories Management.
IP-Adresse	IP-Adresse von Directories Management.
Alternative IP-Adresse	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.

Nächste Schritte

Wechseln Sie zur Verwaltungskonsolle 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.

Verfahren

- 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 „SecurIDdpAdapter“. 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 IP-Adresse 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 <code>sdconf.rec</code> 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**.

Nächste Schritte

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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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.

Option	Aktion
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.
Gemeinsamer geheimer Schlüssel	Geben Sie den gemeinsamen geheimen Schlüssel ein, der zwischen dem RADIUS-Server und dem VMware Identity Manager-Dienst wird.
Server-Timeout 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 innerhalb 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 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. Der Standardtextstring ist RADIUS-Passcode .

- 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**.

Nächste Schritte

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-Verwaltungskonsole aktivieren und konfigurieren.

Voraussetzungen

- Abrufen des Root-Zertifikats und der Zwischen-Zertifikate von der Zertifizierungsstelle (CA), die die Zertifikate der Benutzer signiert hat.
- (Optional) OID-Liste (Objektkennungsliste) der gültigen Zertifikatsrichtlinien für die Zertifikatauthentifizierung.
- Für Sperrprüfungen: Den CRL-Speicherort und die URL des OCSP-Servers.
- (Optional) Speicherort des OCSP-Antwortsignaturzertifikats.
- Inhalt des Zustimmungformulars, wenn vor der Authentifizierung ein Zustimmungformulars angezeigt werden soll.

Verfahren

- 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 Klicken Sie in der Zeile „CertificateAuthAdapter“ auf **Bearbeiten**.
- 5 Konfigurieren Sie die Seite „Zertifikat-Authentifizierungsadapter“.

Hinweis Ein Asterisk (*) gibt an, welche Felder erforderlich sind. Alle anderen Felder sind optional auszufüllen.

Option	Beschreibung
*Name	Der Name ist erforderlich. Der Standardname lautet „CertificateAuthAdapter“. Sie können diesen Namen ändern.
Zertifikatsadapter aktivieren	Aktivieren Sie das Kontrollkästchen, um die Zertifikatauthentifizierung zu aktivieren.
*Root- und Zwischen-CA-Zertifikate	Wählen Sie die hochzuladenden Zertifikatsdateien aus. Sie können mehrere Root- und Zwischen-CA-Zertifikate auswählen, die im DER- oder PEM-Format codiert sind.

Option	Beschreibung
Hochgeladene CA-Zertifikate	<p>Die hochgeladenen Zertifikatsdateien sind im Abschnitt „Hochgeladene CA-Zertifikate“ des Formulars aufgeführt.</p> <p>Sie müssen den Dienst neu starten, damit die neuen Zertifikate verfügbar sind.</p> <p>Klicken Sie auf Web-service neu starten, um den Dienst neu zu starten, und die Zertifikate in die Liste der vertrauenswürdigen Dienste aufzunehmen.</p> <p>Hinweis Ein Neustart des Dienstes aktiviert nicht die Zertifikatauthentifizierung. Fahren Sie mit der Konfiguration dieser Seite fort, nachdem der Dienst erneut gestartet wurde. Wenn Sie am Ende der Seite auf Speichern klicken, wird die Zertifikatauthentifizierung des Dienstes aktiviert.</p>
E-Mail verwenden, wenn kein UPN im Zertifikat vorhanden ist	Wenn der Benutzer-Prinzipalname (User Principal Name = UPN) nicht im Zertifikat existiert, aktivieren Sie dieses Kontrollkästchen, um das Attribut „emailAddress“ als Erweiterung des Alternativer Antragstellernamens für die Validierung der Benutzerkonten zu verwenden.
Zertifikatsrichtlinien wurden akzeptiert	<p>Erstellen Sie eine Liste mit Objektkennungen, die in den Erweiterungen der Zertifikatsrichtlinien akzeptiert werden.</p> <p>Geben Sie die Objekt-ID-Nummern (OID) für die Zertifikatausstellungsrichtlinie ein. Klicken Sie auf Weiteren Wert hinzufügen, um weitere OIDs hinzuzufügen.</p>
Zertifikatsperrung aktivieren	Aktivieren Sie das Kontrollkästchen, um die Zertifikatsperrüberprüfung zu aktivieren. Dies verhindert, dass sich Benutzer authentifizieren können, die über gesperrte Zertifikate verfügen.
CRL von Zertifikaten verwenden	Aktivieren Sie das Kontrollkästchen, um die von der Zertifizierungsstelle veröffentlichte Zertifikatsperrliste (CRL, Certificate Revocation Lists) zu verwenden, um den Status eines Zertifikats (gesperrt oder nicht gesperrt) zu validieren.
CRL-Speicherort	Geben Sie den Serverdateipfad oder den lokalen Dateipfad ein, von dem die CRL geladen werden kann.
OCSP-Sperrung aktivieren	Aktivieren Sie das Kontrollkästchen, um das Zertifikatvalidierungsprotokoll „Online Certificate Status Protocol (OCSP)“ zu verwenden, um den Sperrstatus des Zertifikats zu erfahren.
CRL im Falle eines OCSP-Fehlers verwenden	Wenn Sie sowohl CRL als auch OCSP konfigurieren, können Sie dieses Kontrollkästchen aktivieren, um wieder CRL zu verwenden, wenn die OCSP-Prüfung nicht verfügbar ist.
OCSP-Nonce senden	Aktivieren Sie dieses Kontrollkästchen, wenn Sie den eindeutigen Bezeichner der OCSP-Anfrage in der Antwort übermitteln möchten.
OCSP-URL	Wenn Sie OCSP-Widerruf aktiviert haben, geben Sie die OCSP-Serveradresse für die Widerrufsprüfung ein.
Signaturzertifikat des OCSP-Antwortdienstes	Geben Sie den Pfad des OCSP-Zertifikats für den Antwortdienst: <i>/path/to/file.cer</i> ein.

Option	Beschreibung
Zustimmungsformular vor der Authentifizierung aktivieren	Aktivieren Sie dieses Kontrollkästchen, um eine Seite mit einem Zustimmungsformular anzuzeigen, bevor sich die Benutzer mit der Zertifikatauthentifizierung bei ihrem „Meine Apps“-Portal anmelden.
Inhalt des Zustimmungsformulars	Geben Sie hier den Text ein, der im Zustimmungsformular angezeigt werden soll.

6 Klicken Sie auf **Speichern**.

Nächste Schritte

- 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 ManagementConnector 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 Identitätsdrittanbieter-Verbindung

vRealize Automation enthält eine Identitätsanbieter-Verbindungs-Standardinstanz. Benutzer können zusätzliche Identitätsanbieter-Verbindungen erstellen, um Just-in-time-Benutzerbereitstellungen oder andere benutzerdefinierte Konfigurationen zu unterstützen.

vRealize Automation enthält einen Standard-Identitätsanbieter. In den meisten Fällen werden die Kundenbedürfnisse mit dem Standardanbieter ausreichend abgedeckt. Wenn Sie eine vorhandene Identitätsverwaltungslösung für Unternehmen verwenden, können Sie einen benutzerdefinierten Identitätsanbieter so einrichten, dass die Benutzer zu Ihrer vorhandenen Identitätslösung umgeleitet werden.

Wenn Sie einen benutzerdefinierten Identitätsanbieter verwenden, verwendet die Verzeichnisverwaltung SAML-Metadaten von diesem Anbieter, um eine Vertrauensbeziehung mit dem Anbieter einzurichten. Nachdem diese Beziehung eingerichtet ist, ordnet die Verzeichnisverwaltung die Benutzer von der SAML-Assertion zur Liste der internen vRealize Automation-Benutzer basierend auf der Subjektnamen-ID zu.

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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Identitätsanbieter** aus.
Auf der Seite werden alle konfigurierten Identitätsanbieter angezeigt.
- 2 Klicken Sie auf **Identitätsanbieter hinzufügen**.
Ein Menü mit Identitätsanbieteroptionen wird angezeigt.
- 3 Wählen Sie **Create Third Party IDP** (IDP Dritter erstellen) aus.
- 4 Geben Sie die entsprechenden Informationen ein, um den Identitätsanbieter zu konfigurieren.

Option	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"> 1 Geben Sie die SAML-Metadaten-URL oder den xml-Inhalt in das Textfeld ein. 2 Klicken Sie auf IDP-Metadaten verarbeiten. Die von IdP unterstützten Formate der Namens-ID werden aus den Metadaten extrahiert und der Tabelle mit den Formaten der Namens-ID hinzugefügt. 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. 4 (Optional) Wählen Sie das Zeichenfolgenformat für den NameIDPolicy-Antwortbezeichner aus.

Option	Beschreibung
Benutzer	Wählen Sie die Directories Management-Verzeichnisse der Benutzer aus, die sich mit diesem Identitätsanbieter authentifizieren können.
Just-in-Time-Benutzerbereitstellung	Wählen Sie die entsprechenden Optionen zur Unterstützung der Just-in-Time-Bereitstellung mit einem entsprechenden externen Identitätsanbieter aus. Geben Sie den Verzeichnisnamen für die Verwendung in der Just-in-Time-Bereitstellung ein. Geben Sie eine oder mehrere Domänen ein, die innerhalb des externen Identitätsanbieters vorhanden sind, der für die Just-in-Time-Bereitstellung verwendet wird.
Netzwerk	Die im Dienst konfigurierten vorhandenen Netzwerkbereiche werden aufgeführt. Wählen Sie die Netzwerkbereiche der Benutzer anhand ihrer IP-Adressen aus, die Sie zu dieser Identitätsanbieter-Instanz für die Authentifizierung umleiten möchten.
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 Metadaten des Dienstanbieters , 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 Hostname 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: myco.example.com:8443.

5 Klicken Sie auf **Hinzufügen**.

Nächste Schritte

- 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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Netzwerkbereiche** aus.

- 2 Bearbeiten Sie einen vorhandenen Netzwerkbereich oder fügen Sie einen neuen Netzwerkbereich hinzu.

Option	Beschreibung
Vorhandenen Bereich bearbeiten	Klicken Sie zum Bearbeiten auf den Namen des Netzwerkbereichs.
Bereich hinzufügen	Klicken Sie auf Netzwerkbereich hinzufügen , 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.

Nächste Schritte

- 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.

Verfahren

- 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**.

Ergebnisse

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](#).

Verfahren

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Richtlinien** aus.
- 2 Klicken Sie zur Bearbeitung auf die Standardzugriffsrichtlinie.
- 3 Um eine Richtlinienregel zu bearbeiten, klicken Sie auf die entsprechende Authentifizierungsmethode in der Spalte „Richtlinienregeln/Authentifizierungsmethode“.
Um eine neue Richtlinienregel hinzuzufügen, klicken Sie auf das **+**-Symbol.
- 4 Klicken Sie auf **Speichern** und auf der Richtlinienseite erneut auf **Speichern**.

Richtlinienregel bearbeiten

The screenshot shows the 'Richtlinienregel bearbeiten' (Edit Policy Rule) configuration form. It includes the following fields and options:

- Ist der Netzwerkbereich eines Benutzers...**: A dropdown menu with the value 'ALLE BEREICHE'.
- und der Benutzer versucht, auf Inhalte zuzugreifen von...**: A dropdown menu with the value 'Web-Browser'.
- muss der Benutzer die Authentifizierung mit der folgenden Methode durchführen...**: A dropdown menu with the value 'Password'.
- Wenn die vorangegangene Authentifizierungsmethode fehlschlägt, dann:**: A dropdown menu with the value '-Authentifizierungsmethode auswählen-'.
- +** **Fallback-Methode(n)**: A button to add a fallback authentication method.
- Erneute Authentifizierung nach:**: A text input field with the value '8' and a unit dropdown menu with the value '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.

Verfahren

- 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 Hostnamen umleiten ein. Meist ist dies der Hostname des Dienstes.

- 7** Klicken Sie auf **Speichern**.

Nächste Schritte

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.

Verfahren

- 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

Ergebnisse

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.

Verfahren

- 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.

Ergebnisse

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.

Verfahren

- 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.

Ergebnisse

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.

Durchführen eines Upgrades von externen Konnektoren für die Verzeichnisverwaltung

Wenn Sie mit Ihrer vRealize Automation-Verzeichnisverwaltungskonfiguration einen externen Konnektor verwenden, müssen Sie möglicherweise diesen Konnektor ab und zu aktualisieren.

Sie müssen möglicherweise einen externen Konnektor aktualisieren, wenn Sie ein Upgrade der Version Ihrer vRealize Automation-Bereitstellung durchführen oder wenn ein neuer Konnektor-Build eine Funktion enthält, die Sie gerne verwenden möchten.

Diese Dokumentation gilt nur für Benutzer, die zusätzliche eigenständige externe Connector-Appliances bereitgestellt haben. In vRealize Automation werden externe Connector-Appliances beispielsweise mit der Smartcard-Authentifizierung verwendet.

Standardmäßig verwendet der Connector die VMware-Website für das Upgrade-Verfahren. Hierfür muss die Connector-Appliance über eine Verbindungsmöglichkeit zum Internet verfügen. Sie müssen ggf. auch Proxy-Server-Einstellungen für die Connector-Appliance konfigurieren.

Wenn Ihre Connector-Instanz nicht über eine Internetverbindung verfügt, können Sie das Upgrade offline durchführen. Für ein Offline-Upgrade laden Sie das Upgrade-Paket herunter und richten einen lokalen Webserver ein, auf dem die Upgrade-Datei gehostet werden soll.

Zielgruppe

Diese Informationen sind für alle Personen bestimmt, die Installationen, Upgrades und Konfigurationen der Verzeichnisverwaltung durchführen. Die Informationen sind für erfahrene Windows- oder Linux-Systemadministratoren bestimmt, die mit der VM-Technologie vertraut sind.

Vorbereiten auf das Durchführen eines Upgrades eines externen Konnektors

Um die Durchführung eines Konnektor-Upgrades vorzubereiten, müssen Sie nach verfügbaren Upgrades suchen und ggfs. die Proxy-Server-Einstellungen für die Appliance konfigurieren.

■ Überprüfen der Verfügbarkeit eines Online-Upgrades des externen Konnektors

Wenn Ihre Connector-Appliance über eine Verbindungsmöglichkeit zum Internet verfügt, können Sie von der Appliance aus prüfen, ob Upgrades online verfügbar sind.

■ Konfigurieren von Proxy-Server-Einstellungen für die externe Connector-Appliance

Die Connector-Appliance greift über das Internet auf die VMware-Update-Server zu. Wenn Ihre Netzwerkkonfiguration Internetzugriff über einen HTTP-Proxy bereitstellt, müssen Sie die Proxy-Einstellungen für die -Appliance anpassen.

Überprüfen der Verfügbarkeit eines Online-Upgrades des externen Konnektors

Wenn Ihre Connector-Appliance über eine Verbindungsmöglichkeit zum Internet verfügt, können Sie von der Appliance aus prüfen, ob Upgrades online verfügbar sind.

Verfahren

- 1 Melden Sie sich bei der Connector-Appliance als Root-Anwender an.
- 2 Führen Sie folgenden Befehl aus.

```
/usr/local/horizon/update/updatemgr.hznupdateinstaller
```

- 3 Führen Sie den folgenden Befehl aus, um zu überprüfen, ob ein Online-Upgrade vorhanden ist.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

Konfigurieren von Proxy-Server-Einstellungen für die externe Connector-Appliance

Die Connector-Appliance greift über das Internet auf die VMware-Update-Server zu. Wenn Ihre Netzwerkkonfiguration Internetzugriff über einen HTTP-Proxy bereitstellt, müssen Sie die Proxy-Einstellungen für die -Appliance anpassen.

Aktivieren Sie den Proxy, damit dieser nur den Internetdatenverkehr verarbeitet. Um sicherzustellen, dass der Proxy korrekt eingerichtet ist, legen Sie den Parameter für internen Datenverkehr innerhalb der Domäne auf „no-proxy“ fest.

Hinweis Proxy-Server, die eine Authentifizierung erfordern, werden nicht unterstützt.

Voraussetzungen

- Stellen Sie sicher, dass Sie über das Root-Kennwort für die Connector-Appliance verfügen.
- Stellen Sie sicher, dass Sie über die Informationen für den Proxy-Server verfügen.

Verfahren

- 1 Melden Sie sich bei der Connector-Appliance als Root-Anwender an.
- 2 Geben Sie in die Befehlszeile YaST ein, um das Hilfsprogramm YaST auszuführen.
- 3 Wählen Sie im linken Fensterbereich **Netzwerkdienste** und dann **Proxy** aus.

- 4 Geben Sie die URLs der Proxy-Server in die Felder **URL für HTTP-Proxy** und **URL für HTTPS-Proxy** ein.
- 5 Wählen Sie **Fertig stellen** aus und beenden Sie das Hilfsprogramm YaST.
- 6 Führen Sie auf der virtuellen Connector-Appliance einen Neustart des Tomcat-Servers aus, um die neuen Proxy-Einstellungen anzuwenden.

```
service horizon-workspace restart
```

Ergebnisse

Die VMware-Update-Server sind jetzt für die Connector-Appliance verfügbar.

Durchführen eines Upgrades eines externen Konnektors online

Sie können einen externen Verzeichnisverwaltungskonnektor online aktualisieren, wenn Sie über eine entsprechende Verbindung verfügen.

Voraussetzungen

- Vergewissern Sie sich, dass die Connector-Appliance vapp-updates.vmware.com an Port 80 über HTTP auflösen und erreichen kann.
- Vergewissern Sie sich, dass ein Connector-Upgrade vorhanden ist. Führen Sie den entsprechenden Befehl aus, um zu überprüfen, ob Upgrades vorhanden sind. Weitere Informationen finden Sie unter „Überprüfen, ob ein Directories Management Connector-Upgrade online verfügbar ist“.
- Vergewissern Sie sich, dass mindestens 2 GB Festplattenspeicher auf der primären Root-Partition der Appliance verfügbar sind.
- Vergewissern Sie sich, dass der Connector ordnungsgemäß konfiguriert ist.
- Erstellen Sie einen Snapshot Ihrer Connector-Appliance als Backup. Informationen zum Erstellen von Snapshots finden Sie in der vSphere-Dokumentation.
- Wenn für den ausgehenden HTTP-Zugriff ein HTTP-Proxy-Server erforderlich ist, konfigurieren Sie die Proxy-Server-Einstellungen für die Connector-Appliance. Weitere Informationen finden Sie unter „Konfigurieren von Proxy-Server-Einstellungen für die Directories Management Connector-Appliance“.

Verfahren

- 1 Melden Sie sich bei der Connector-Appliance als Root-Anwender an.
- 2 Führen Sie folgenden Befehl aus.

```
/usr/local/horizon/update/updatemgr.hznupdateinstaller
```

- 3 Führen Sie den folgenden Befehl aus, um zu überprüfen, ob ein Online-Upgrade vorhanden ist.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- 4 Aktualisieren Sie mit dem folgenden Befehl die Appliance.

```
/usr/local/horizon/update/updatemgr.hznupdate
```

Während des Upgrades ausgegebene Meldungen werden in der Datei `update.log` unter dem Pfad `/opt/vmware/var/log/update.log` gespeichert.

- 5 Führen Sie erneut den `updatemgr.hzn check`-Befehl aus, um sich zu vergewissern, dass kein neueres Update vorhanden ist.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- 6 Überprüfen Sie die Version der Appliance nach dem Upgrade.

```
vami-cli version --appliance
```

Die neue Version wird angezeigt.

- 7 Starten Sie die Connector-Appliance neu.

```
reboot
```

Offline-Upgrade eines externen Konnektors

Wenn Ihre vorhandene Connector-Appliance der vRealize Automation-Verzeichnisverwaltung keine Verbindung zum Internet herstellen kann, um ein Upgrade durchzuführen, können Sie ein Offline-Upgrade durchführen. Sie müssen ein Upgrade-Repository auf einem lokalen Webserver einrichten und die Connector-Appliance konfigurieren, um den lokalen Webserver für Upgrades zu verwenden.

Voraussetzungen

- Vergewissern Sie sich, dass ein Connector-Upgrade vorhanden ist. Prüfen Sie, ob auf der My VMware-Download-Website unter my.vmware.com Upgrades vorhanden sind.
- Vergewissern Sie sich, dass mindestens 2 GB Festplattenspeicher auf der primären Root-Partition der Appliance verfügbar sind.
- Vergewissern Sie sich, dass der Connector ordnungsgemäß konfiguriert ist.
- Erstellen Sie einen Snapshot Ihrer Connector-Appliance als Backup. Informationen zum Erstellen von Snapshots finden Sie in der vSphere-Dokumentation.

- Konfigurieren Sie die Connector-Appliance so, dass sie einen lokalen Webserver als Host für die Upgrade-Datei verwendet. Weitere Informationen finden Sie unter „Vorbereiten eines lokalen Webserver für ein Offline-Upgrade“.

Verfahren

1 Vorbereiten eines lokalen Webserver für ein Offline-Upgrade

Bevor Sie mit dem Offline-Connector-Upgrade beginnen, bereiten Sie den lokalen Webserver vor, indem Sie eine Verzeichnisstruktur erstellen, die ein Unterverzeichnis für die Connector-Appliance enthält.

2 Konfigurieren des Connectors und Durchführen von Offline-Upgrades

Konfigurieren Sie die Connector-Appliance so, dass sie auf den lokalen Webserver zeigt, um ein Offline-Upgrade durchzuführen. Führen Sie dann ein Upgrade für die Appliance durch.

Vorbereiten eines lokalen Webserver für ein Offline-Upgrade

Bevor Sie mit dem Offline-Connector-Upgrade beginnen, bereiten Sie den lokalen Webserver vor, indem Sie eine Verzeichnisstruktur erstellen, die ein Unterverzeichnis für die Connector-Appliance enthält.

Voraussetzungen

- Laden Sie die Datei `identity-manager-connector-versionNumber-buildNumber-updaterepo.zip` von My VMware herunter. Wechseln Sie zu my.vmware.com und zur VMware Identity Manager-Download-Seite und laden Sie die unter **VMware Identity Manager Connector-Offline-Upgrade-Paket** aufgeführte Datei herunter.
- Wenn Sie einen IIS-Webserver verwenden, konfigurieren Sie den Webserver für die Verwendung von Sonderzeichen in Dateinamen. Diese Konfiguration erfolgt im Abschnitt **Filter anfordern** durch Auswahl der Option **Doppeltes Escape-Zeichen zulassen**.

Verfahren

- 1 Erstellen Sie ein Verzeichnis auf dem Webserver unter `http://YourWebServer/VM/` und kopieren Sie die heruntergeladene ZIP-Datei hinein.
- 2 Stellen Sie sicher, dass Ihr Webserver MIME-Typen für `.sig` (text/plain) und `.sha256` (text/plain) enthält.

Ohne diese MIME-Typen kann Ihr Server nicht nach Updates suchen.

- 3 Entpacken Sie die ZIP-Datei.

Server für den Inhalt der extrahierten ZIP-Datei ist `http://YourWebServer/VM/`.

Der extrahierte Inhalt der Datei enthält die folgenden Unterverzeichnisse: `/manifest` und `/package-pool`.

- 4 Führen Sie den folgenden `updateLocal.hzn`-Befehl aus, um zu prüfen, ob die URL gültige Aktualisierungsinhalte aufweist.

```
/usr/local/horizon/update/updatesLocal.hzn checkurl http://YourWebServer/VM
```

Konfigurieren des Connectors und Durchführen von Offline-Upgrades

Konfigurieren Sie die Connector-Appliance so, dass sie auf den lokalen Webserver zeigt, um ein Offline-Upgrade durchzuführen. Führen Sie dann ein Upgrade für die Appliance durch.

Voraussetzungen

Bereiten Sie einen lokalen Webserver zur Durchführung eines Offline-Upgrades vor.

Verfahren

- 1 Melden Sie sich bei der Connector-Appliance als Root-Anwender an.
- 2 Führen Sie den folgenden Befehl aus, um ein Upgrade-Repository zu konfigurieren, das einen lokalen Webserver verwendet.

```
/usr/local/horizon/update/updatesLocal.hzn seturl http://YourWebServer/VM/
```

Hinweis Um die Konfiguration rückgängig zu machen und die Möglichkeit wiederherzustellen, ein Online-Upgrade durchzuführen, können Sie den folgenden Befehl ausführen.

```
/usr/local/horizon/update/updatesLocal.hzn setdefault
```

- 3 Führen Sie das Upgrade durch.
 - a Führen Sie folgenden Befehl aus.

```
/usr/local/horizon/update/updatesmgr.hznupdateinstaller
```

- b Führen Sie folgenden Befehl zur Überprüfung der Version des verfügbaren Upgrades aus.

```
/usr/local/horizon/update/updatesmgr.hzncheck
```

- c Aktualisieren Sie mit dem folgenden Befehl den Connector.

```
/usr/local/horizon/update/updatesmgr.hznupdate
```

Während des Upgrades ausgegebene Meldungen werden in der Datei `update.log` unter dem Pfad `/opt/vmware/var/log/update.log` gespeichert.

- d Führen Sie den Befehl `updatesmgr.hzn check` erneut aus.

```
/usr/local/horizon/update/updatesmgr.hzncheck
```

- e Überprüfen Sie die Version der Appliance nach dem Upgrade.

```
vamcli version --appliance
```

Der Befehl sollte die neue Version anzeigen.

- f Starten Sie die Connector-Appliance neu.

Führen Sie beispielsweise an der Befehlszeile den folgenden Befehl aus.

```
reboot
```

Ergebnisse

Das Upgrade des Connectors ist nun abgeschlossen.

Konfigurieren der Einstellungen nach dem Upgrade eines externen Konnektors

Nach dem Upgrade auf Connector 2016.3.1.0 oder höher müssen Sie einige Einstellungen vornehmen:

Erneutes Beitreten zur Domäne mit Kerberos-Authentifizierung

Wenn Sie die Kerberos-Authentifizierung oder Active Directory-Verzeichnisse (integrierte Windows-Authentifizierung) verwenden, müssen Sie die Domäne verlassen und dann erneut beitreten. Dies ist für alle virtuellen Connector-Appliances Ihrer Bereitstellung erforderlich.

- 1 Wählen Sie **Administration > Verzeichnisverwaltung > Konnektoren** aus.
- 2 Klicken Sie auf der Seite „Konnektoren“ für jeden Konnektor, der für die Kerberos-Authentifizierung oder für das Active Directory-Verzeichnis (integrierte Windows-Authentifizierung) verwendet wird, auf **Domäne verlassen**.
- 3 Für den Beitritt benötigen Sie Active Directory-Anmeldedaten mit Rechten für den Domänenbeitritt. Weitere Informationen hierzu finden Sie unter [Hinzufügen einer Konnektormaschine zu einer Domäne](#).
- 4 Wenn Sie die Kerberos-Authentifizierung verwenden, aktivieren Sie erneut den Kerberos-Authentifizierungsadapter. Um auf die Seite „Authentifizierungsadapter“ zuzugreifen, klicken Sie auf der Seite „Konnektoren“ auf den entsprechenden Link in der Spalte **Worker** und wählen Sie die Registerkarte **Authentifizierungsadapter** aus.
- 5 Stellen Sie sicher, dass die anderen verwendeten Authentifizierungsadapter aktiviert sind.

Seite „Domänen aktualisieren“

Wenn Sie Active Directory (integrierte Windows-Authentifizierung) oder Active Directory über LDAP mit aktivierter Option **Dieses Verzeichnis unterstützt den DNS-Dienstspeicherort** verwenden, speichern Sie die Domänenseite des Verzeichnisses.

- 1 Wählen Sie **Verwaltung > Verzeichnisverwaltung > Verzeichnisse** aus.
- 2 Wählen Sie das passende Verzeichnis aus, um es zu bearbeiten.

- 3 Geben Sie das Kennwort für den Bind-DN-Benutzer ein und klicken Sie auf **Speichern**.
- 4 Klicken Sie links auf der Seite auf **Synchronisierungseinstellungen** und wählen Sie die Registerkarte **Domänen** aus.
- 5 Klicken Sie auf **Speichern**.

DNS-Dienstspeicherort und Domänencontroller

Hinweis In Connector 2016.3.1.0 und höher wird automatisch eine Datei `domain_krb.properties` erstellt. Darin werden automatisch Domänencontroller eingetragen, wenn ein Verzeichnis mit aktiviertem DNS-Dienstspeicherort erstellt wird. Wenn Sie die Domänenseite nach dem Upgrade speichern und Ihre ursprüngliche Bereitstellung eine Datei `domain_krb.properties` enthält, wird die Datei eventuell mit Domänen aktualisiert, die Sie nachträglich hinzugefügt haben und die deshalb nicht in der Datei enthalten sind. Wenn Ihre ursprüngliche Bereitstellung die Datei `domain_krb.properties` nicht enthält, wird diese Datei angelegt und automatisch mit Domänencontrollern gefüllt. Unter [Informationen über die Auswahl von Domänencontrollern](#) finden Sie weitere Informationen zur `domain_krb.properties`-Datei.

Beheben von Aktualisierungsfehlern bei externen Konnektoren

Sie können durch Durchsehen der Fehlerprotokolle Aktualisierungsprobleme bei externen Konnektoren der vRA-Verzeichnisverwaltung beheben. Wenn der Connector nicht gestartet wird, können Sie eine frühere Instanz per Rollback auf einen Snapshot wiederherstellen.

■ Überprüfen der Upgrade-Fehlerprotokolle

Um Fehler zu beheben, die während des Upgrades auftreten, überprüfen Sie die Fehlerprotokolle. Upgrade-Protokolldateien befinden sich im Verzeichnis `/opt/vmware/var/log`.

■ Rollback auf Snapshots des Connectors

Wenn nach einem Upgrade der Konnektor nicht ordnungsgemäß startet und Sie das Problem nicht durch Überprüfen der Upgrade-Fehlerprotokolle und erneutes Ausführen des Upgrade-Befehls beheben können, können Sie ein Rollback auf eine vorherige Konnektorinstanz durchführen.

■ Erfassen eines Pakets von Protokolldateien

Sie können ein Paket von Protokolldateien erfassen, um es an den VMware-Support zu senden. Sie beziehen das Paket von der Konfigurationsseite für den Connector.

Überprüfen der Upgrade-Fehlerprotokolle

Um Fehler zu beheben, die während des Upgrades auftreten, überprüfen Sie die Fehlerprotokolle. Upgrade-Protokolldateien befinden sich im Verzeichnis `/opt/vmware/var/log`.

Falls Fehler aufgetreten sind, startet der Konnektor nach dem Upgrade möglicherweise nicht.

Verfahren

- 1 Melden Sie sich bei der Connector-Appliance an.

- 2 Wechseln Sie in das Verzeichnis `/opt/vmware/var/log`.
- 3 Öffnen Sie die Datei `update.log` und überprüfen Sie die Fehlermeldungen.
- 4 Beheben Sie die Fehler und führen Sie den Upgrade-Befehl erneut aus. Der Upgrade-Befehl wird an dem Punkt fortgesetzt, an dem er angehalten wurde.

Hinweis Alternativ können Sie auch einen Snapshot wiederherstellen und die Aktualisierung erneut ausführen.

Rollback auf Snapshots des Connectors

Wenn nach einem Upgrade der Konnektor nicht ordnungsgemäß startet und Sie das Problem nicht durch Überprüfen der Upgrade-Fehlerprotokolle und erneutes Ausführen des Upgrade-Befehls beheben können, können Sie ein Rollback auf eine vorherige Konnektorinstanz durchführen.

Verfahren

- ◆ Stellen Sie einen der Snapshots wieder her, die Sie als Backup Ihrer ursprünglichen Connector-Instanz erstellt haben. Weitere Informationen finden Sie in der vSphere-Dokumentation.

Erfassen eines Pakets von Protokolldateien

Sie können ein Paket von Protokolldateien erfassen, um es an den VMware-Support zu senden. Sie beziehen das Paket von der Konfigurationsseite für den Connector.

Die folgenden Protokolldateien werden im Paket erfasst.

Tabelle 2-9. Protokolldateien

Komponente	Speicherort der Protokolldatei	Beschreibung
Apache Tomcat-Protokolle (catalina.log)	<code>/opt/vmware/horizon/workspace/logs/catalina.log</code>	Apache Tomcat zeichnet Meldungen auf, die in den anderen Protokolldateien nicht aufgezeichnet werden.
Konfigurator-Protokolle (configurator.log)	<code>/opt/vmware/horizon/workspace/logs/configurator.log</code>	Anforderungen, die der Konfigurator vom REST-Client und der Web-Benutzeroberfläche empfängt
Connector-Protokolle (connector.log)	<code>/opt/vmware/horizon/workspace/logs/connector.log</code>	Ein Datensatz für jede von der Webschnittstelle empfangene Anforderung. Jeder Protokolleintrag enthält zudem die Anforderungs-URL, den Zeitstempel und Ausnahmen. Synchronisierungsaktionen werden nicht erfasst.

Verfahren

- 1 Melden Sie sich bei der Connector-Konfigurationsseite unter `https://connectorURL:8443/cfg/logs` an.

- 2 Klicken Sie auf **Protokollpaket vorbereiten**.
- 3 Laden Sie das Paket herunter und senden Sie es an den VMware-Support.

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*.
- Melden Sie sich bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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
Verzeichnisname	Fügen Sie die IP-Adresse des Active Directory-Domänennamens hinzu.
Synchronisierungs-Connector	Jede vRealize Automation-Appliance enthält einen Connector. Sie können alle verfügbaren Connectoren verwenden.
Basis-DN	Geben Sie den definierten Namen (DN, Distinguished Name) des Startpunkts für Verzeichnisserversuchen ein. Beispiel: cn=users,dc=corp,dc=local .

Option	Beispieleingabe
Bind-DN	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: cn=config_admin infra,cn=users,dc=corp,dc=local .
Bind-DN-Kennwort	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 Abfrageregeln 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 sekundären 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.

Ergebnisse

Sie haben das Active Directory Ihres Unternehmens mit vRealize Automation verbunden und die Verzeichnisverwaltung für Hochverfügbarkeit konfiguriert.

Nächste Schritte

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 von externen Konnektoren für Smartcard- und Drittanbieter-Identitätsanbieter-Authentifizierung in vRealize Automation

Ein Systemadministrator muss einen externen Konnektor für Ihre vRealize Automation-Bereitstellung mithilfe der Verzeichnisverwaltung konfigurieren, wenn Sie externe Identitätsanbieter wie z. B. Kerberos oder die Smartcard-Authentifizierung verwenden.

Mit Verzeichnisverwaltung werden mehrere Identitätsanbieter und Konnektor-Cluster für jedes konfigurierte Active Directory unterstützt. Sie können für die Verwendung eines externen Identitätsanbieters oder der Smartcard-Authentifizierung entweder einen einzelnen externen Konnektor oder einen Konnektor-Cluster mit einem entsprechenden Identitätsanbieter hinter einem Lastausgleichsdienst, der SSL-Passthrough zulässt, einrichten. Weitere Informationen hierzu finden Sie unter [Verwalten von Konnektoren und Konnektorclustern](#).

Informationen zur Aktualisierung eines externen Konnektors finden Sie unter [Durchführen eines Upgrades von externen Konnektoren für die Verzeichnisverwaltung](#).

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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

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-Identitätsanbieter](#)

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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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.

Verfahren

- 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
Quelle	Navigieren Sie zum Speicherort des OVA-Pakets oder geben Sie eine URL ein.
Details der OVA-Vorlage	Überprüfen Sie, ob Sie die richtige Version ausgewählt haben.

Seite	Beschreibung
Lizenz	Lesen Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf Akzeptieren .
Name und Speicherort	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:
Host/Cluster	Wählen Sie den Host oder Cluster zum Ausführen der bereitgestellten Vorlage aus.
Ressourcenpool	Wählen Sie den Ressourcenpool aus.
Speicher	Wählen Sie den Speicherort aus, an dem die Dateien der virtuellen Maschine gespeichert werden sollen.
Festplattenformat	Wählen Sie das Festplattenformat für die Dateien aus. Wählen Sie für Produktionsumgebungen das Format Thick Provision aus. Verwenden Sie für Evaluierungen und Tests das Format Thin Provision aus.
Netzwerkzuordnung	Ordnen Sie die Netzwerke in Ihrer Umgebung den Netzwerken der OVF-Vorlage zu.
Eigenschaften	<ul style="list-style-type: none"> a Wählen Sie im Feld Einstellung der Zeitzone die richtige Zeitzone aus. 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. c Geben Sie im Textfeld „Hostname“ den zu verwendenden Hostnamen ein. Wenn dieses Feld leer ist, wird zum Suchen des Hostnamens Reverse-DNS verwendet. 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>Wichtig 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>
Bereit zum Abschließen	Überprüfen Sie Ihre Auswahl und klicken Sie auf Beenden .

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.

Nächste Schritte

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.

Verfahren

- 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
Appliance-Administrator	Erstellen Sie das Administratorkennwort für die Appliance. Der Benutzername lautet admin 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. Wichtig Das Kennwort des Benutzers admin muss aus mindestens sechs Zeichen bestehen.
Root-Konto	Für die Installation der Connector-Appliance wird ein Standard-VMware-Root-Kennwort verwendet. Erstellen Sie ein neues Root-Kennwort.
sshuser-Konto	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 auf dem internen vRealize Automation-Connector verwenden, können Sie das entsprechende Zertifikat abrufen, indem Sie den folgenden Befehl auf der vRealize Automation-Appliance ausführen: `cat /etc/apache2/server-cert.pem`

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.

Nächste Schritte

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.

Wenn die Verzeichnisverwaltung auf einen Lastausgleichsdienst verweist, wird das SSL-Zertifikat auf den Lastausgleichsdienst angewendet.

Sie müssen die Option **Mark this key as exportable** (Diesen Schlüssel als exportierbar markieren) aktivieren, wenn Sie ein Zertifikat importieren.

Sie müssen nur den CN oder den Domännennamen der Site der Zertifizierungsstelle angeben, wenn Sie eine CSR für ein benutzerdefiniertes Zertifikat generieren.

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.

Verfahren

- 1 Melden Sie sich bei der Administratorseite für die Connector-Appliance als ein Admin-Benutzer unter dem folgenden Speicherort an:
`https://myconnector.mycompany:8443/cfg`
- 2 Klicken Sie in der Verwaltungskonsole auf **Appliance-Einstellungen**.
Standardmäßig ist „VA-Konfiguration“ ausgewählt.
- 3 Klicken Sie auf **Konfigurationen verwalten**.
- 4 Geben Sie das Admin-Benutzerkennwort für den VMware Identity Manager-Server 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

```
-----BEGIN CERTIFICATE-----
jIQt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+
...
...
...
W53+O05j5xsxzDJfWr1lqBIFF/OkiYCPcyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
WdR9Vpg3WQT5+C3HU17bUOwvhp/rjIQt90+
...
...
...
O05j5xsxzDJfWr1lqBIFF/OkiYCPW53+cyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
dR9Vpg3WQTjIQt9W5+C3HU17bUOwvhp/r0+
...
...
...
5j5xsxzDJfWr1lqW53+O0BIFF/OkiYCPcyK1
-----END CERTIFICATE-----
```

Beispiel für einen privaten Schlüssel

-----BEGIN RSA PRIVATE KEY-----

jIQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+

...

...

...

1lqBIFFW53+O05j5xsxzDJfWr/OklYCPcyK1

-----END RSA PRIVATE KEY-----

Erstellen eines Arbeitsbereichs-Identitätsanbieters

Sie müssen einen Arbeitsbereichs-Identitätsanbieter für die Verwendung mit einem externen Konnektor erstellen.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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 Domännennamen 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 Zertifikatsauthentifizierung 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*.
- Melden Sie sich bei vRealize Automation als **Mandantenadministrator** an.
- Konfigurieren Sie die entsprechenden Domänen und Active Directory-Gesamtstrukturen für Ihre Bereitstellung.

Verfahren

- 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
Synchronisierungs-Connector	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.
Authentifizierung	Klicken Sie auf das entsprechende Optionsfeld, um anzugeben, ob der ausgewählte Connector auch Authentifizierung durchführt.
Verzeichnissuchattribut	Geben Sie das gewünschte Kontoattribut ein, das den Benutzernamen enthält.

Abhängig von der Bereitstellungskonfiguration 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
Bind-Benutzer-UPN	Geben Sie den User Principal Name (Benutzername des Prinzipals) des Benutzers ein, der die Domäne authentifizieren kann. Beispiel: Benutzername@example.com.
Bind-DN-Kennwort	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 Arbeitsspeichermenge 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**.

Nächste Schritte

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 gewähren Benutzern Zugriffsrechte, indem sie Benutzern und Gruppen Rollen zuweisen.

Damit Benutzer oder Gruppen eine Pipeline ändern oder auslösen können, müssen Sie diesen Benutzern und Gruppen Berechtigungen zuweisen. Wenn Sie Benutzern und Gruppen die Rolle „Versionsmanager“ zuweisen, können sie die Pipeline ändern und auslösen. Wenn Sie Benutzern und Gruppen die Rolle „Versionsentwickler“ zuweisen, können sie die Pipeline auslösen. Weitere Informationen finden Sie im Handbuch zur *Verwendung von vRealize Code Stream*.

Voraussetzungen

Melden Sie sich bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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 Führen Sie auf der Seite **Benutzerdetails** auf der Registerkarte **Allgemein** einen Bildlauf durch die Liste der Rollen durch, um den Benutzer hinzuzufügen.
 - a Um die Benutzerberechtigungen zum Ändern und Auslösen einer Pipeline zu erteilen, aktivieren Sie das Kontrollkästchen **Versionsmanager**.
 - b Um die Benutzerberechtigungen zum Auslösen einer Pipeline zu erteilen, aktivieren Sie das Kontrollkästchen **Versionsentwickler**.
- 7 Klicken Sie auf **Aktualisieren**.

Ergebnisse

Benutzer, die aktuell bei vRealize Automation angemeldet sind, müssen sich abmelden und wieder bei vRealize Automation anmelden, bevor sie auf die Seiten navigieren können, auf die ihnen Zugriff gewährt wurde.

Nächste Schritte

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. Benutzerdefinierte Gruppen ermöglichen eine präzisere Steuerung des Zugriffs innerhalb von vRealize Automation als Business-Gruppen, die einem Geschäftszweig, einer Abteilung oder einer anderen Organisationseinheit entsprechen.

Benutzerdefinierte Gruppen ermöglichen Ihnen, Zugriffsrechte für Aufgaben präziser als standardmäßige vRealize Automation-Gruppenzuweisungen zu gewähren. Es ist beispielsweise ratsam, eine benutzerdefinierte Gruppe zu erstellen, damit Mandantenadministratoren steuern können, wer über bestimmte Berechtigungen innerhalb des Mandanten verfügt.

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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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**.

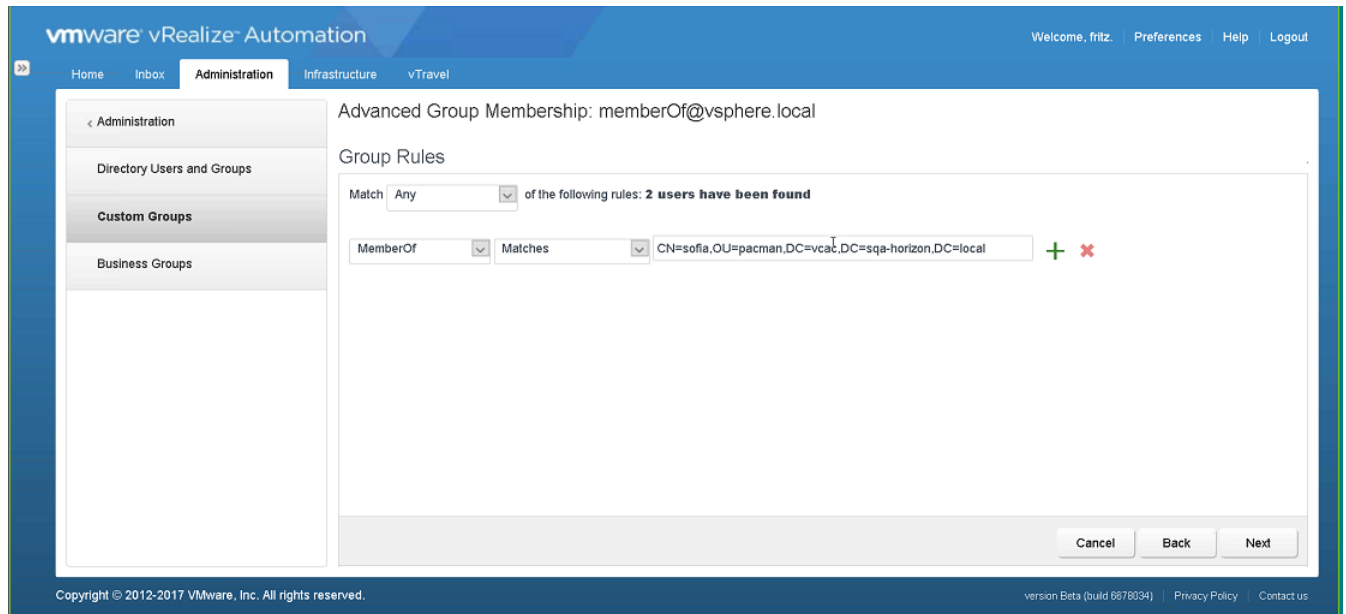
Ergebnisse

Benutzer, die aktuell bei vRealize Automation angemeldet sind, müssen sich abmelden und wieder bei vRealize Automation anmelden, bevor sie auf die Seiten navigieren können, auf die ihnen Zugriff gewährt wurde.

Hinzufügen von Just-in-Time-Benutzern mit benutzerdefinierten Gruppen und Regeln

Mit der Just-in-Time-Benutzerbereitstellung können Sie ohne Zugriff auf das Active Directory vRealize Automation-Benutzer zu einer Bereitstellung hinzufügen. Um die Just-in-Time-Bereitstellung für erstmalige Benutzer aufzurufen, müssen Sie Regeln zum Auffüllen der anwendbaren benutzerdefinierten Gruppe erstellen.

Bei der ersten Anmeldung wird Just-in-Time-Benutzern die Gruppenmitgliedschaft dynamisch basierend auf Regeln zugewiesen, die Sie auf der Assistentenseite für erweiterte Gruppenmitgliedschaft erstellen. Nach der ersten Anmeldung können Sie die Gruppenmitgliedschaft auf die übliche Weise zuweisen. Diese zweite Seite des Assistenten enthält vier Auswahlfelder zum Erstellen von Regeln basierend auf einer Reihe von Kriterien, die Just-in-Time-Benutzer definieren.



Beispielsweise können Sie im ersten Auswahlfeld „Domäne“ als ein Kriterium und anschließend „Übereinstimmungen“ im zweiten Feld auswählen. Anschließend können Sie in das dritte Regelfeld eine Domäne eingeben. Diese Auswahlen erstellen eine Regel, die eine Just-in-Time-Mitgliedschaft basierend auf Benutzern erstellt, die der angegebenen Domäne zugeordnet sind. Das dritte Auswahlfeld ist ein Freiform-Eingabefeld, und Sie können alle Informationen eingeben, die einen logischen Bezug zu den Auswahlen in den ersten beiden Auswahlfeldern haben.

Hinweis Sie können mehrere Regeln erstellen, um Just-in-Time-Benutzer basierend auf einer Reihe von Kriterien aufzufüllen. Wenn Sie mehrere Regeln erstellen, können Sie das Regelauswahlfeld **Übereinstimmung** oberhalb der Hauptregelfelder verwenden, um anzugeben, ob vRealize Automation beim Auffüllen von Just-in-Time-Benutzern mit bestimmten oder mit allen Regeln abgeglichen werden soll.

Verfahren

- 1 Wählen Sie **Administration > Benutzer & Gruppen > Benutzerdefinierte Gruppen** aus und erstellen oder suchen Sie eine passende benutzerdefinierte Gruppe für Just-in-Time-Benutzer.

Weitere Informationen hierzu finden Sie unter [Erstellen einer benutzerdefinierten Gruppe](#).

- 2 Klicken Sie auf die Schaltfläche **Erweiterte Mitgliedschaft**.
Bei Bedarf können Sie einzelne Benutzern auf der Seite hinzufügen.
- 3 Klicken Sie auf **Weiter**, um die Seite „Gruppenregeln“ anzuzeigen.
- 4 Klicken Sie in den drei wichtigsten Auswahlfeldern für Regeln unter dem Regelauswahlfeld **Übereinstimmung** auf die Pfeile nach unten und geben Sie die Informationen zum Aktivieren der Dropdown-Menüs ein, mit denen Sie die gewünschte Regel erstellen können.

- 5 Erstellen Sie mithilfe der Regelauswahlfelder eine oder mehrere Regeln entsprechend den Anforderungen für Ihre Benutzerkonfiguration.
- 6 (Optional) Wenn Sie mehrere Regeln erstellen, können Sie das Regelauswahlfeld **Übereinstimmung** verwenden, um die Verarbeitung der Regeln durch vRealize Automation festzulegen.
- 7 Klicken Sie auf **Weiter**.
- 8 Wenn Sie Benutzer aus der Gruppe ausschließen möchten, suchen Sie diese Benutzer auf der Seite „Benutzer aus Gruppe ausschließen“ und fügen Sie sie hinzu.
- 9 Klicken Sie auf **Weiter**.
- 10 Überprüfen Sie die Gruppenkonfiguration auf der Überprüfungsseite und klicken Sie auf **Speichern**, um Ihre Regeln und Ihre Konfiguration zu speichern und zu implementieren.

Ergebnisse

Just-in-Time-Benutzer werden auf der Grundlage der Regeln hinzugefügt, die Sie erstellt haben.

Erstellen einer Business-Gruppe

Business-Gruppen werden verwendet, um einen Satz von Diensten und Ressourcen einer Gruppe von Benutzern zuzuordnen. Diese Gruppen entsprechen häufig einer Sparte, einer Abteilung oder einer anderen Organisationseinheit. 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 bei vRealize Automation 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 für die Gruppe bereitstellen möchten, das den Namen von bereitgestellten Maschinen vorangestellt wird, fordern Sie ein Präfix von einem Fabric-Administrator an. Siehe [Konfigurieren von Maschinenpräfixen](#). Maschinenpräfixe sind nicht für XaaS-Anforderungen anwendbar.

Verfahren

- 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
Name	Geben Sie den Namen für die Business-Gruppe ein.
Beschreibung	Geben Sie die Beschreibung ein.
Manager E-Mails senden an	Geben Sie eine oder mehrere E-Mail-Adressen der Benutzer ein, die Benachrichtigungen zu Kapazitätswarnungen empfangen müssen. E-Mail-Alias-Adressen werden nicht unterstützt. Jede E-Mail-Adresse muss für einen bestimmten Benutzer vorgesehen sein. Trennen Sie mehrere Einträge durch Kommas voneinander. Beispielsweise JoeAdmin@mycompany.com,WeiMgr@mycompany.com .
Active Directory-Richtlinie	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. Sie können die Benutzer jetzt angeben, oder Sie können leere Business-Gruppen erstellen und diese später auffüllen.

Option	Beschreibung
Gruppenmanagerrolle	Kann für die Gruppe Berechtigungen erstellen und Genehmigungsrichtlinien zuweisen.
Supportrolle	Kann Katalogelemente im Namen von anderen Mitgliedern der Business-Gruppe anfordern und verwalten.
Rolle mit gemeinsam genutztem Zugriff	Kann Ressourcen, die von anderen Mitgliedern der Business-Gruppe bereitgestellt wurden, verwenden und Aktionen darauf ausführen.
Benutzerrolle	Kann Dienstkatalogelemente anfordern, für die sie über eine Berechtigung verfügt.

6 Klicken Sie auf **Weiter**.

7 Konfigurieren Sie die Standard-Infrastrukturoptionen.

Option	Beschreibung
Standardmaschinenpräfix	<p>Auswählen eines vorkonfigurierten Maschinenpräfixes für die Business-Gruppe.</p> <p>Dieses Präfix wird von Maschinen-Blueprints verwendet. Wenn der Blueprint das Standardpräfix verwendet und Sie es hier nicht angeben, wird ein Maschinenpräfix basierend auf dem Namen 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.</p> <p>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.</p>
Active Directory-Container	<p>Eingabe eines Active Directory-Containers. Diese Option ist nur für die WIM-Bereitstellung anwendbar.</p> <p>Andere Bereitstellungsmethoden erfordern zusätzliche Konfiguration, um bereitgestellte Maschinen zu einem AD-Container hinzuzufügen.</p>

8 Klicken Sie auf **Hinzufügen**.

Ergebnisse

Fabric-Administratoren können Ihrer Business-Gruppe durch Erstellen einer Reservierung Ressourcen zuteilen. Business-Gruppenmanager können Berechtigungen für Mitglieder der Business-Gruppe erstellen.

Nächste Schritte

- 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 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.

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 Basiskonfiguration 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.

Verfahren

1 (Optional) 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 (Optional) Konfigurieren von lokalen Benutzern

Der vRealize Automation-Systemadministrator muss die lokalen Benutzer für jeden anwendbaren Mandanten konfigurieren.

3 (Optional) 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.

Verfahren

- 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.

Verfahren

- 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.

Ergebnisse

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*.

Verfahren

- 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.

Verfahren

- 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**.

Ergebnisse

Der Mandant wird aus Ihrer vRealize Automation-Bereitstellung gelöscht.

Konfigurieren von Sicherheitseinstellungen für mehrere Mandanten

Sie können die Verfügbarkeit von NSX-Sicherheitsobjekten für Mandanten in einer Umgebung mit mehreren Mandanten steuern.

Wenn Sie ein NSX-Sicherheitsobjekt in vRealize Automation erstellen, kann seine Standardverfügbarkeit entweder auf „Global“, d. h. verfügbar in allen Mandanten, für die der zugehörige Endpoint eine Reservierung aufweist, oder auf „Verborgen“ für alle Benutzer mit Ausnahme des Administrators gesetzt sein.

Die mandantenübergreifende Verfügbarkeit von Sicherheitsobjekten richtet sich auch danach, ob der zugehörige Endpoint eine Reservierung oder Reservierungsrichtlinie im Mandanten aufweist.

Die Hilfsmittel, mit denen Sie die Verfügbarkeit neuer Sicherheitsobjekte für mehrere Mandanten steuern, und das Verhalten, das in vorhandenen Sicherheitsobjekten nach der Aktualisierung auf diese vRealize Automation-Version in Bezug auf Mandanten beobachtet werden kann, werden im verwandten Thema [Steuern des Mandantenzugriffs für Sicherheitsobjekte](#) zusammengefasst.

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.

Verfahren

- 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.

Ergebnisse

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.

Verfahren

- 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.

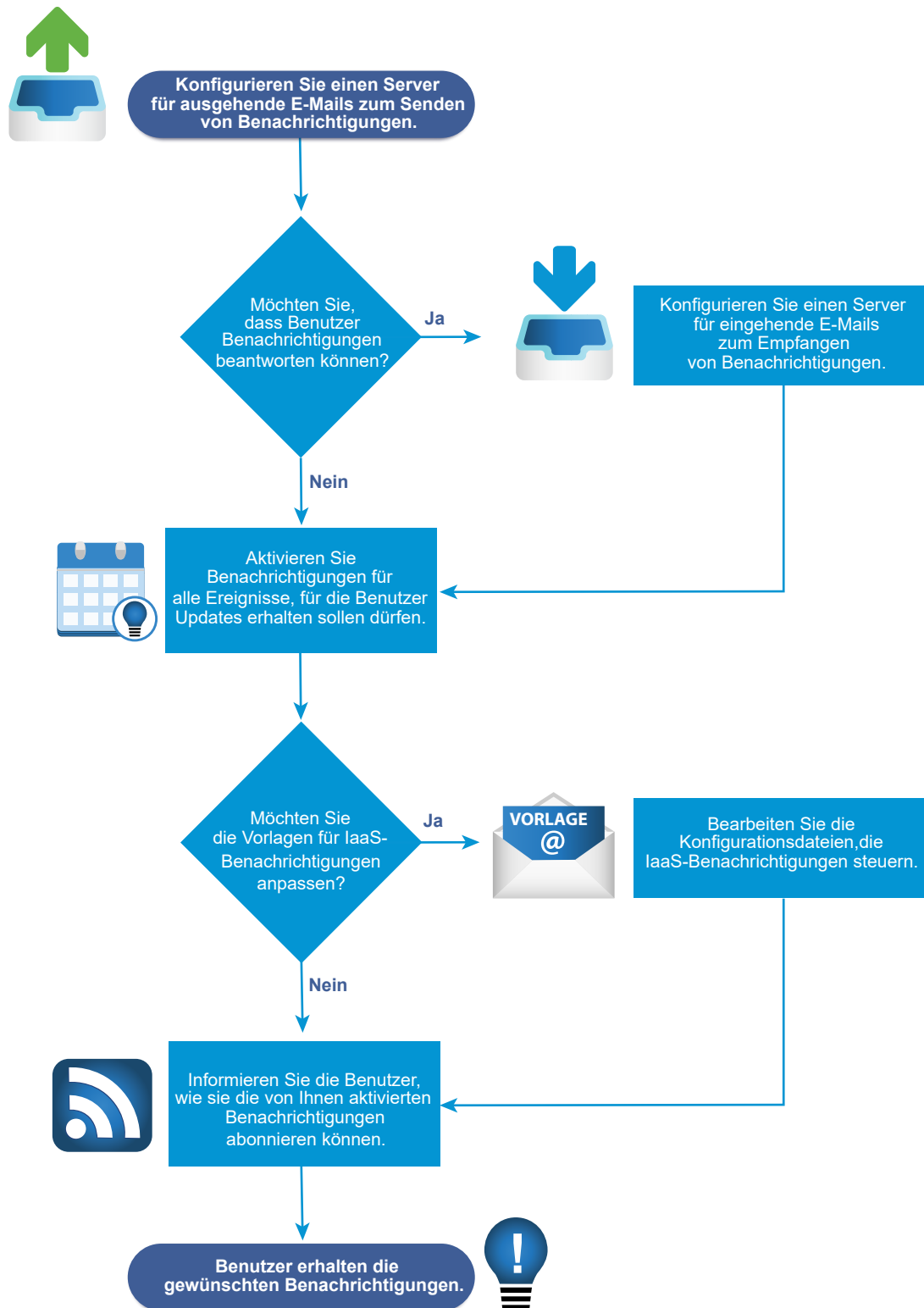
7 Klicken Sie auf **Aktualisieren**, um Ihre Konfiguration des Brandings zu implementieren.

Ergebnisse

Bei Mandantenbenutzern wird das benutzerdefinierte Branding auf deren Anwendungsseiten angezeigt.

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 2-10. 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"> ■ Systemadministratoren konfigurieren globale Standardserver. ■ Mandantenadministratoren konfigurieren Server für ihre Mandanten. 	<p>Informationen zum ersten Konfigurieren eines Servers für einen Mandanten finden Sie unter Hinzufügen eines mandantenspezifischen Postausgangsservers. Informationen zur Vorgehensweise, wenn Sie einen globale Standardserver überschreiben müssen, finden Sie unter Überschreiben eines Standard-Ausgangs-E-Mail-Servers des Systems. Informationen zum Konfigurieren globaler Standardserver für alle Mandanten finden Sie unter Erstellen eines globalen Postausgangsservers.</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"> ■ Systemadministratoren konfigurieren globale Standardserver. ■ Mandantenadministratoren konfigurieren Server für ihre Mandanten. 	<p>Informationen zum ersten Konfigurieren eines Servers für einen Mandanten finden Sie unter Hinzufügen eines mandantenspezifischen Posteingangsservers. Informationen zur Vorgehensweise, wenn Sie einen globale Standardserver überschreiben müssen, finden Sie unter Überschreiben eines Standard-Eingangs-E-Mail-Servers des Systems. Informationen zum Konfigurieren eines globalen Standardservers für alle Mandanten finden Sie unter Erstellen eines globalen Posteingangsservers.</p>
<input type="checkbox"/> (Optional) Geben Sie an, wann eine E-Mail-Benachrichtigung vor Ablauf einer Maschine verschickt werden soll.	Systemadministrator	Siehe Anpassen des Datums für E-Mail-Benachrichtigungen wegen des Ablaufs von Maschinen .
<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	Siehe Konfigurieren der Benachrichtigungen .

Tabelle 2-10. 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\VMware\VCAC\Server) kann die Vorlagen für diese E-Mail-Benachrichtigungen konfigurieren.	Siehe Konfigurieren von Vorlagen für automatische IaaS-E-Mails .
<input type="checkbox"/> Ihre Benutzer werden automatisch auf die konfigurierten Benachrichtigungen abonniert. Stellen Sie Ihren Benutzern, falls nötig, 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 Abonnieren von Benachrichtigungen .

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.

Verfahren

- 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.

Verfahren

- 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 bei vRealize Automation 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.

Verfahren

- 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 bei vRealize Automation als **Mandantenadministrator** an.
- Stellen Sie sicher, dass der angegebene Benutzer in einer Identitätsquelle und in der Business-Gruppe vorhanden ist.

Verfahren

- 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
Name	Geben Sie einen Namen für den Posteingangsserver ein.
Beschreibung	Geben Sie eine Beschreibung für den Posteingangsserver ein.
Sicherheit	Aktivieren Sie das Kontrollkästchen SSL verwenden .
Protokoll	Wählen Sie ein Serverprotokoll aus.
Servername	Geben Sie den Servernamen ein.
Server-Port	Geben Sie die Server-Portnummer ein.

- 5 Geben Sie den Ordnernamen 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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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
Name	Geben Sie den Namen des Eingangs-E-Mail-Servers ein.
Beschreibung	Geben Sie eine Beschreibung für den Posteingangsserver ein.
Sicherheit	Aktivieren Sie das Kontrollkästchen SSL , um als Sicherheitsoption SSL zu verwenden.
Protokoll	Wählen Sie ein Serverprotokoll aus.
Servername	Geben Sie den Servernamen ein.
Server-Port	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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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 bei vRealize Automation als **Mandantenadministrator** an.
- Stellen Sie sicher, dass ein Mandantenadministrator oder Systemadministrator einen Postausgangsserver konfiguriert hat. Siehe [Hinzufügen eines mandantenspezifischen Postausgangsservers](#).

Verfahren

- 1 Wählen Sie **Administration > Benachrichtigungen > Szenarien** aus.
- 2 Wählen Sie eine oder mehrere Benachrichtigungen aus.
- 3 Klicken Sie auf **Aktivieren**.

Ergebnisse

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.

Verfahren

- 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
```

Nächste Schritte

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:

- [E-Mail-Anpassung in vRealize Automation](#)
- [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, werden Sie automatisch darauf abonniert. Benachrichtigungsereignisse können den erfolgreichen Abschluss einer Kataloganforderung oder einer erforderlichen Genehmigung beinhalten.

Wenn Sie manuell abonnieren müssen, können Sie Ihre Benachrichtigungen aktivieren.

Voraussetzungen

Melden Sie sich bei vRealize Automation an.

Verfahren

- 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**.

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.

Verfahren

- 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\Server\Website\Rdp`.
- 7 Fügen Sie die benutzerdefinierte `VirtualMachine.Rdp.File`-Eigenschaft einem Blueprint hinzu.

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](#).

Szenario: Hinzufügen von Datacenter-Standorten für regionsübergreifende 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.



Sie können nicht Datacenter-Standorte in der XML-Datei basierend auf der Mandanten- oder Business-Gruppe filtern. Wenn Sie in einer Umgebung mit mehreren Mandanten arbeiten, können Sie Eigenschaftsdefinitionen verwenden, um basierend auf der Mandanten- oder Business-Gruppe zu filtern. Informationen zur Verwendung von Eigenschaftsdefinitionen finden im Blog-Beitrag [How to use dynamic property definitions](#).

Verfahren

- 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.

Ergebnisse

Ihr Fabric-Administrator kann für die in den einzelnen Datencentern vorhandenen Computing-Ressourcen den geeigneten Standort anwenden. Siehe [Szenario: Anwenden eines Standorts auf eine Computing-Ressource für regionsenübergreifende Bereitstellungen](#).

Nächste Schritte

Sie können die `Vrm.DataCenter.Location`-Eigenschaft zu einem Blueprint hinzufügen oder die Option **Standort in Anforderung anzeigen** im Blueprint aktivieren, damit Benutzer beim Anfordern einer Maschinenbereitstellung einen Datacenter-Standort angeben müssen.

Konfigurieren von vRealize Orchestrator

vRealize Orchestrator ist eine Automatisierungs- und Verwaltungs-Engine, die vRealize Automation für die Unterstützung von XaaS und weiteren Erweiterungsmöglichkeiten erweitert. Sie können den vRealize Orchestrator-Server konfigurieren und verwenden, der in der vRealize Automation-Appliance vorkonfiguriert ist, oder Sie können vRealize Orchestrator als externe Serverinstanz bereitstellen und diese externe Instanz vRealize Automation zuordnen.

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.

Wenn vRealize Automation für die Verwendung von vRealize Orchestrator konfiguriert wird, können Orchestrator-Workflows im vRealize Orchestrator-Servicekatalog als Teil der XaaS-Blueprint-Verwaltung veröffentlicht werden.

Wenn Sie Orchestrator-Workflows ausführen möchten, um die Verwaltung von IaaS-Maschinen zu erweitern, müssen Sie vRealize Orchestrator als Endpoint konfigurieren.

Konfigurationsrechte

System- und Mandantenadministratoren können vRealize Automation für die Verwendung eines externen oder des eingebetteten 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"> ■ Konfigurieren des vRealize Orchestrator-Servers für alle Mandanten. ■ Definieren des standardmäßigen vRealize Orchestrator-Workflow-Ordners für einen Mandanten.
Mandantenadministratoren	<ul style="list-style-type: none"> ■ Konfigurieren des vRealize Orchestrator-Servers für ihren eigenen Mandanten. ■ Hinzufügen von vRealize Orchestrator-Plug-ins als Endpoints.

Konfigurieren des eingebetteten vRealize Orchestrator-Servers

Die vRealize Automation-Appliance enthält eine vorkonfigurierte Instanz von vRealize Orchestrator. Der vRealize Orchestrator-Serverdienst wird standardmäßig ausgeführt. Sie müssen den Konfigurationsdienst jedoch manuell starten, um auf das Control Center zugreifen zu können.

Voraussetzungen

Stellen Sie die vRealize Automation-Appliance bereit. Einzelheiten dazu finden Sie unter *Bereitstellung der vRealize Automation-Appliance* in *Installieren von vRealize Automation*.

Verfahren

- 1 Melden Sie sich an der vRealize Automation-Konsole als **Systemadministrator** oder **Mandantenadministrator** an.
- 2 Wählen Sie **Administration > VRO-Konfiguration > Serverkonfiguration** aus.
- 3 Klicken Sie auf **Standard-Orchestrator-Server verwenden**.

Ergebnisse

Verbindung zum eingebetteten vRealize Orchestrator-Server werden jetzt konfiguriert. Der Ordner für **VCAC**-Workflows und die zugehörigen Dienstprogrammaktionen werden automatisch importiert. Der Workflows-Ordner **VCAC > ASD** enthält Workflows zum Konfigurieren von Endpoints und zum Erstellen von Ressourcenzuordnungen.

Konfigurieren des standardmäßigen Workflow-Ordnern 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.

Verfahren

- 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**.

Ergebnisse

Sie haben den standardmäßigen vRealize Orchestrator-Workflow-Ordner für einen Mandanten definiert.

Nächste Schritte

Wiederholen Sie diese Schritte für alle Mandanten, für die Sie einen Standard-Workflow-Ordner definieren möchten.

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.

Verfahren

- 1 Starten Sie den vRealize Orchestrator-Konfigurationsdienst.
 - a Melden Sie sich bei 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 Stellen Sie eine Verbindung zur vRealize Automation-URL in einem Webbrowser her.

3 Klicken Sie auf **vRealize Orchestrator Control Center**.

Sie werden zu „https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter“ umgeleitet.

4 Melden Sie sich beim vRealize Orchestrator Control Center an.

Der Benutzername wird vom Administrator der vRealize Automation-Appliance konfiguriert.

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.

Verfahren

1 Stellen Sie eine Verbindung zur vRealize Automation-URL in einem Webbrowser her.

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 Domänennamen der vRealize Automation-Appliance im Textfeld **Hostname** und **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
Ignorieren	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 vRealize Orchestrator-Remoteserver zu synchronisieren.
Abbrechen	Schließen Sie das Fenster und beenden Sie den Anmeldevorgang.
Dieses Zertifikat installieren und keine Sicherheitswarnungen für dieses mehr anzeigen.	Wählen Sie dieses Kontrollkästchen und klicken Sie auf Ignorieren , um das Zertifikat zu installieren und um den Empfang von Sicherheitswarnungen zu beenden.

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

Nächste Schritte

Sie können ein Paket importieren, Workflows 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 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 „vcoadmins“-Gruppe sein.

Voraussetzungen

- Installieren und konfigurieren Sie eine externe vRealize Orchestrator-Appliance. Weitere Informationen finden Sie unter *Installieren und Konfigurieren von vRealize Orchestrator* im vRealize Orchestrator-Informationscenter unter https://www.vmware.com/support/pubs/orchestrator_pubs.html.
- Melden Sie sich an der vRealize Automation-Konsole als **Systemadministrator** oder **Mandantenadministrator** an.
- Konfigurieren Sie den standardmäßigen Workflow-Ordner. Siehe [Konfigurieren des standardmäßigen Workflow-Ordners für einen Mandanten](#).

Verfahren

- 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.

Hinweis Wenn der externe Orchestrator-Server für das Arbeiten im Clustermodus konfiguriert ist, geben Sie die IP-Adresse oder den Hostnamen des virtuellen Lastausgleich-Servers ein, der die Client-Anforderungen über die Orchestrator-Server im Cluster verteilt.

- 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
Single Sign On	<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>
Einfach	<p>Stellt mit dem Benutzernamen und dem Kennwort, die Sie in das Textfeld Benutzername bzw. Kennwort 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 **OK**.

Ergebnisse

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.

Nächste Schritte

[Anmelden beim vRealize Orchestrator-Client](#)

Konfigurieren von Ressourcen

Sie können Ressourcen konfigurieren, wie z. B. Endpoints, Reservierungen und Netzwerkprofile, um Blueprint-Definitionen und Maschinenbereitstellungen durch vRealize Automation zu unterstützen.

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.

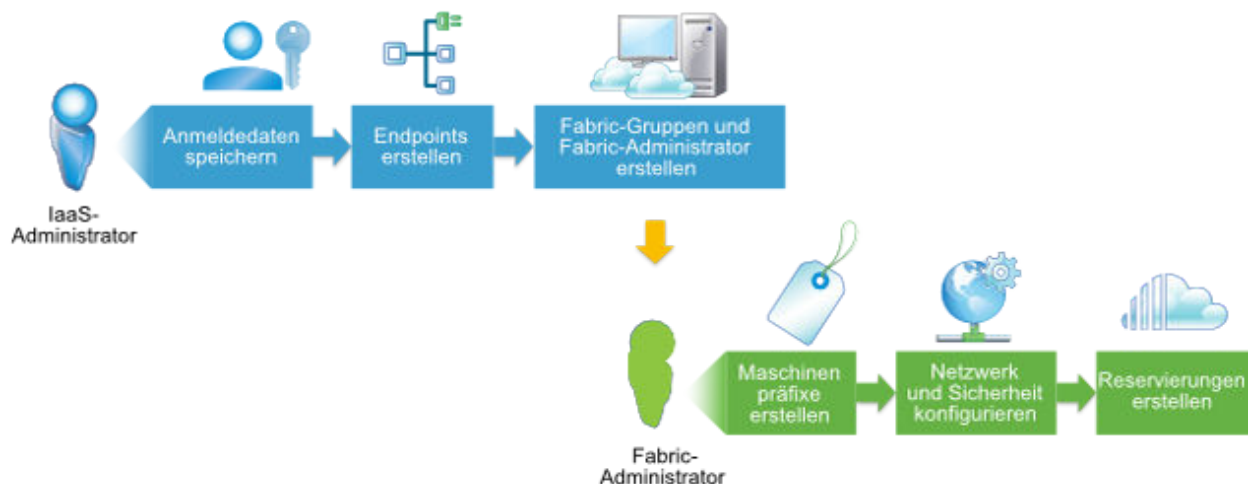


Tabelle 2-11. Checkliste für die Konfiguration von IaaS-Ressourcen

Aufgabe	vRealize Automation-Rolle	Details
<input type="checkbox"/> Erstellen Sie Endpoints für Ihre Infrastruktur, um Ressourcen mit vRealize Automation verwalten zu können.	IaaS-Administrator	Auswählen eines Endpoint-Szenarios.
<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	Erstellen einer Fabric-Gruppe.
<input type="checkbox"/> Konfigurieren Sie Maschinenpräfixe, die für die Erstellung von Namen für durch vRealize Automation bereitgestellte Maschinen verwendet werden.	Fabric-Administrator	Konfigurieren von Maschinenpräfixen.
<input type="checkbox"/> (Optional) Erstellen Sie Netzwerkprofile, um Netzwerkeinstellungen für bereitgestellte Maschinen zu konfigurieren.	Fabric-Administrator	Erstellen eines Netzwerkprofils.
<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"> ■ IaaS-Administrator, wenn dieser auch als Fabric-Administrator konfiguriert wurde ■ Fabric-Administrator 	Konfigurieren von Reservierungen und Reservierungsrichtlinien.

Konfigurieren von Endpoints

Sie erstellen und konfigurieren die Endpoints, mit denen vRealize Automation mit Ihrer Infrastruktur kommunizieren kann.

Die Kategorisierung der Endpoint-Definitionen basiert auf dem Typ:

- Cloud

Die Cloud-Kategorie enthält die Endpoint-Typen vCloud Air, vCloud Director, Amazon EC2 und OpenStack
- IPAM

Diese Kategorie wird nur angezeigt, wenn Sie einen IPAM-Endpoint-Typ eines Drittanbieters, wie beispielsweise Infoblox IPAM, in einem vRealize Orchestrator-Workflow registriert haben.
- Verwaltung

Diese Kategorie enthält nur den vRealize Operations Manager-Endpoint.
- Netzwerk und Sicherheit

Diese Kategorie enthält die Proxy- und NSX-Endpoint-Typen.

Ein Proxy-Endpoint kann mit einem Amazon-, vCloud Air- oder vCloud Director-Endpoint verknüpft werden.

Ein NSX-Endpoint kann mit einem vSphere-Endpoint verknüpft werden.

- **Orchestrierung**

Diese Kategorie enthält nur den vRealize Orchestrator-Endpoint.

- **Speicher**

Diese Kategorie enthält den NetApp ONTAP-Endpoint.

- **Virtuell**

Die virtuelle Kategorie enthält die Endpoint-Typen vSphere, Hyper-V (SCVMM) und KVM (RHEV).

Sie können weitere Endpoint-Typen in vRealize Orchestrator konfigurieren und mit unterstützten Endpoint-Typen in vRealize Automation verwenden. Sie können Endpoints auch programmgesteuert importieren und exportieren.

Informationen zum Arbeiten mit Endpoints nach einem Upgrade oder einer Migration finden Sie unter [Überlegungen beim Arbeiten mit aktualisierten oder migrierten Endpoints](#).

Auswählen eines Endpoint-Szenarios

Wählen Sie ein Endpoint-Szenario basierend auf dem Typ des Ziel-Endpoints aus.

Weitere Informationen zu den verfügbaren Endpoint-Einstellungen finden Sie unter [Endpoint-Einstellungen – Referenz](#).

Tabelle 2-12. Auswählen eines Endpoint-Szenarios

Endpoint	Weitere Informationen
vSphere	Erstellen eines vSphere-Endpoints
NSX	Erstellen eines NSX-Endpoints und Zuordnen zu einem vSphere-Endpoint
vCloud Air (Abonnement oder OnDemand)	Erstellen eines vCloud Air-Endpoints
vCloud Director	Erstellen eines vCloud Director-Endpoints
vRealize Orchestrator	Erstellen eines vRealize Orchestrator-Endpoints
vRealize Operations	Erstellen eines vRealize Operations Manager-Endpoints
IPAM-Drittanbieter	Erstellen eines Endpoints eines IPAM-Drittanbieters
Microsoft Azure	Erstellen eines Microsoft Azure-Endpoints
Puppet	Erstellen eines Puppet-Endpoints
Amazon	<ul style="list-style-type: none"> ■ Erstellen eines Amazon-Endpoints ■ (Optional) Hinzufügen eines Amazon-Instanztyps
OpenStack	Erstellen eines OpenStack-Endpoints
Proxy	Erstellen eines Proxy-Endpoints und Zuordnen dieses Endpoints zu einem Cloud-Endpoint

Tabelle 2-12. Auswählen eines Endpoint-Szenarios (Fortsetzung)

Endpoint	Weitere Informationen
Hyper-V (SCVMM)	Erstellen eines Hyper-V (SCVMM)-Endpoints
KVM (RHEV)	Endpoint-Einstellungen – Referenz
NetApp ONTAP	<ul style="list-style-type: none"> ■ Platzsparende Speicher für die virtuelle Bereitstellung ■ Endpoint-Einstellungen – Referenz
Hyper-V (Standalone), XenServer oder Xen Pool Master	Erstellen eines Hyper-V-, XenServer- oder Xen-Pool-Endpoints
Importieren von Endpoints	Programmgesteuertes Importieren oder Exportieren von Endpoints

Endpoint-Einstellungen – Referenz

Verwenden Sie Endpoint-Einstellungen, um Anmeldedaten für den Speicherort und den Zugriff für die Bereitstellung der Datenerfassung und des Servicekatalogs festzulegen.

Registerkarte „Allgemein“

Die meisten vRealize Automation-Endpoints enthalten die folgenden Optionen. Einstellungen, die für einen bestimmten Endpoint-Typ eindeutig sind, werden nicht aufgelistet.

Tabelle 2-13. Einstellungen auf der Registerkarte **Allgemein**

Einstellung	Beschreibung
Name	Geben Sie den Endpoint-Namen ein.
Beschreibung	Geben Sie die Endpoint-Beschreibung ein.

Tabelle 2-13. Einstellungen auf der Registerkarte **Allgemein** (Fortsetzung)

Einstellung	Beschreibung
Adresse	<p>Geben Sie die Endpoint-Adresse im für Endpoints spezifischen Adressformat ein.</p> <ul style="list-style-type: none"> Für einen KVM (RHEV)- oder NetApp ONTAP-Endpoint muss die Adresse in einem der folgenden Formate vorliegen: <ul style="list-style-type: none"> <code>https://FQDN</code> <code>https://IP_address</code> Beispiel: <code>https://mycompany-kvmrhev1.mycompany.local</code> oder <code>netapp-1.mycompany.local</code>. Für einen OpenStack-Endpoint muss die Adresse das Format <code>https://FQDN/powervc/openstack/ service</code> aufweisen. Beispiel: <code>https://openstack.mycompany.com/powervc/openstack/admin</code>. Für einen OpenStack-Endpoint muss die Adresse eines der folgenden Formate aufweisen: <ul style="list-style-type: none"> <code>https://FQDN:500</code> <code>https://IP_address:500</code> Für einen vSphere-Endpoint muss die Adresse das Format <code>https://host/sdk</code> aufweisen. Für einen NSX-Endpoint muss die Adresse das Format <code>https://host</code> aufweisen. Für einen vRealize Orchestrator-Endpoint muss die Adresse das Format des HTTPS-Protokolls, den vollqualifizierten Namen oder die IP-Adresse des vRealize Orchestrator-Servers und die vRealize Orchestrator-Portnummer (z. B. <code>https://vrealize-automation-appliance-hostname:443/vco</code>) aufweisen. Für einen vRealize Operations-Endpoint muss die Adresse das Format <code>https://host/suite-api</code> aufweisen.
Integrierte Anmeldedaten	<p>Wenn Sie Ihre integrierten vSphere-Anmeldedaten verwenden möchten, müssen Sie keinen Benutzernamen und kein Kennwort eingeben. Diese Einstellung gilt nur für vSphere-Endpoints.</p>
Benutzername	<p>Geben Sie den Benutzernamen auf Administratorebene ein, den Sie für den Endpoint im Endpoint-spezifischen Format wie in der Benutzeroberfläche vorgeschlagen gespeichert haben.</p>
Kennwort	<p>Geben Sie das Administratorkennwort ein, das Sie für den Endpoint gespeichert haben.</p>
OpenStack-Projekt	<p>Geben Sie einen OpenStack-Mandantennamen ein. Diese Einstellung gilt nur für OpenStack-Endpoints.</p>
Organisation	<p>Wenn Sie ein Organisationsadministrator sind, können Sie einen vCloud Director-Organisationsnamen eingeben. Diese Eigenschaft gilt nur für vCloud Director.</p>
Zugriffsschlüssel-ID	<p>Geben Sie die Amazon AWS-Schlüssel-ID ein. Diese Einstellung gilt nur für Amazon-Endpoints.</p>
Geheimer Zugriffsschlüssel	<p>Geben Sie den geheimen Amazon AWS-Zugriffsschlüssel ein. Diese Einstellung gilt nur für Amazon-Endpoints.</p>

Tabelle 2-13. Einstellungen auf der Registerkarte **Allgemein** (Fortsetzung)

Einstellung	Beschreibung
Port	Geben Sie den Portwert ein, um eine Verbindung zur Endpoint-Proxy-Adresse herzustellen. Diese Einstellung gilt nur für Proxy-Endpoints.
Priorität	Geben Sie einen Prioritätswert als Ganzzahl größer oder gleich 1 ein. Ein niedriger Wert gibt eine höhere Priorität an. Der Prioritätswert ist mit der eingebetteten benutzerdefinierten Eigenschaft VMware.VCenterOrchestrator.Priority verknüpft. Diese Einstellung gilt nur für vRealize Orchestrator-Endpoints.

Registerkarte „Eigenschaften“

Alle Endpoint-Typen verwenden eine Eigenschaften-Registerkarte, um benutzerdefinierte Eigenschaften oder Eigenschaftsgruppen und Einstellungen zu erfassen. Beispiele für benutzerdefinierte Eigenschaften für bestimmte Endpoint-Typen finden Sie unter *Referenz für benutzerdefinierte Eigenschaften*.

Registerkarte „Zuordnung“

Sie können eine Zuordnung zu einem NSX-Endpoint oder einem Proxy-Endpoint erstellen. Dies richtet sich nach dem jeweiligen Endpoint, von dem aus die Zuordnung erstellt wird. Sie können einen vSphere-Endpoint einem NSX-Endpoint zuordnen, um NSX-Einstellungen zum vSphere-Endpoint zuzuweisen. Sie können auch einen vCloud Air-, vCloud Director- oder Amazon-Endpoint einem Proxy-Endpoint zuordnen, um die Proxyeinstellungen zum vCloud Air-, vCloud Director- oder Amazon-Endpoint zuzuweisen.

Verbindung testen

Sie können eine Testverbindung zwecks Überprüfung der Anmeldedaten, der Host-Endpoint-Adresse und des Zertifikats für einen vSphere-, NSX- oder vRealize Operations Manager-Endpoint verwenden. Siehe [Überlegungen bei der Verwendung einer Testverbindung](#).

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. Wahlweise können Sie NSX-Einstellungen mit dem vSphere-Endpoint verknüpfen, indem Sie eine Zuordnung zu einem NSX-Endpoint herstellen.

Wenn Sie einen vSphere-Endpoint aktualisiert oder migriert haben, der einen NSX-Manager verwendet hat, wird ein neuer NSX-Endpoint erstellt, der eine Zuordnung zwischen dem vSphere-Quell-Endpoint und einem neuen NSX-Endpoint enthält.

Wenn Ihre vSphere-Umgebung in NSX integriert ist, finden Sie weitere Informationen unter [Erstellen eines NSX-Endpoints und Zuordnen zu einem vSphere-Endpoint](#).

Weitere Informationen zur Überprüfung der Verbindung und des vertrauenswürdigen Zertifikats finden Sie unter [Überlegungen bei der Verwendung einer Testverbindung](#).

Voraussetzungen

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

- Um Ihren vSphere-Endpoint zu verwalten, müssen Sie einen vSphere-Proxy-Agent installieren, und Sie müssen den exakt selben Namen für den Endpoint und den Agent verwenden. Informationen zum Installieren des Agents finden Sie unter *Installieren von vRealize Automation*.
- Wenn Sie einen vSphere-Endpoint zum Bereitstellen von VMs über OVF-Vorlagen verwenden möchten, vergewissern Sie sich, dass Ihre Anmeldedaten das vSphere-Recht `VApp.Import` im dem Endpoint zugeordneten vCenter umfassen.

Mit dem Recht `VApp.Import` können Sie eine vSphere-Maschine bereitstellen, indem Sie die aus einer OVF-Datei importierten Einstellungen importieren. Details zu diesem vSphere-Recht finden Sie in der [vSphere SDK-Dokumentation](#).

Wenn die OVF-Datei auf einer Website gehostet wird, finden Sie weitere Informationen unter [Erstellen eines Proxy-Endpoints für eine OVF-Host-Website](#).

- Wenn Sie zusätzliche NSX-Netzwerkeinstellungen und -Sicherheitseinstellungen für den vSphere-Endpoint konfigurieren möchten, erstellen Sie einen NSX-Endpoint. Sie können eine Zuordnung zum NSX-Endpoint herstellen, während Sie einen vSphere-Endpoint erstellen. Siehe [Erstellen eines NSX-Endpoints und Zuordnen zu einem vSphere-Endpoint](#).

Verfahren

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.

- 2 Wählen Sie **Neu > Virtuell > vSphere** aus.

- 3 Geben Sie im Textfeld **Name** einen Namen ein.

Der Name 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 Geben Sie Ihre Administratoranmeldedaten (Benutzername und Kennwort für vSphere) ein oder verwenden Sie stattdessen Ihre integrierten Anmeldedaten für vSphere.

Geben Sie die Anmeldedaten mit der Berechtigung zum Ändern benutzerdefinierter Attribute ein.

Das Format des Benutzernamens ist *domain\username*.

Wählen Sie **Integrierte Anmeldedaten verwenden**, um das Dienstkonto des vSphere-Proxy-Agents zu verwenden, mit dem Sie sich mit dem vCenter Server verbinden.

Wenn Sie Ihre integrierten vSphere-Anmeldedaten verwenden möchten, müssen Sie keinen Benutzernamen und kein Kennwort eingeben.

- 7 (Optional) Klicken Sie auf **Eigenschaften** und fügen Sie benutzerdefinierte Eigenschaften, Eigenschaftsgruppen oder Ihre eigenen Eigenschaftsdefinitionen für den Endpoint hinzu.
- 8 (Optional) Um NSX-Netzwerk- und -Sicherheitseinstellungen für den Endpoint zu konfigurieren, klicken Sie auf **Zuordnungen** und stellen Sie eine Zuordnung zu einem vorhandenen NSX-Endpoint her.

Sie benötigen mindestens einen NSX-Endpoint, um eine Zuordnung zu erstellen.

- 9 (Optional) Klicken Sie auf **Verbindung testen**, um die Anmeldedaten, die Host-Endpoint-Adresse und das vertrauenswürdige Zertifikat zu validieren. Mit dieser Aktion wird ebenfalls überprüft, ob der Manager-Dienst und der Agent zum Erfassen von Daten vom Endpoint ausgeführt werden. Mit der Aktion **OK** werden dieselben Bedingungen getestet.

Die Aktion **Testverbindung** gibt Informationen zu einer der folgenden Bedingungen zurück:

- **Zertifikatfehler**

Wenn das Zertifikat nicht gefunden wird, nicht als vertrauenswürdig eingestuft wird oder abgelaufen ist, werden Sie aufgefordert, einen Zertifikat-Fingerabdruck zu akzeptieren. Wenn Sie den Fingerabdruck nicht akzeptieren, können Sie weiterhin den Endpoint speichern, aber die Bereitstellung von Maschinen schlägt möglicherweise fehl.

- **Agent-Fehler**

Der zugeordnete vSphere-Agent wurde nicht gefunden. Der Agent muss für den Test erfolgreich ausgeführt werden.

- **Hostfehler**

Die angegebene Endpoint-Adresse ist nicht erreichbar oder der zugeordnete Manager-Dienst wird nicht ausgeführt. Der Manager-Dienst muss für den Test erfolgreich ausgeführt werden.

- **Anmeldedatenfehler**

Die angegebene Kombination aus Benutzername und Kennwort ist für den Endpoint unter der angegebenen Adresse ungültig.

- **Zeitüberschreitung**

Die Testaktion konnte nicht im zulässigen Zeitraum von zwei Minuten abgeschlossen werden.

Wenn die Aktion **Testverbindung** fehlschlägt, können Sie weiterhin den Endpoint speichern, aber die Bereitstellung von Maschinen schlägt möglicherweise fehl.

Wenn ein Problem mit dem vertrauenswürdigen Zertifikat vorliegt (zum Beispiel, wenn das Zertifikat abgelaufen ist), werden Sie aufgefordert, einen Zertifikat-Fingerabdruck zu akzeptieren.

10 Klicken Sie auf **OK**, um den Endpoint zu speichern.

Mit der Aktion **OK** werden dieselben Bedingungen wie mit der Aktion **Verbindung testen** getestet. Wenn eine der oben genannten Bedingungen gefunden wird, wird eine Meldung zurückgegeben. Wenn der Endpoint gespeichert werden kann, wird die Fehlermeldung weiterhin zwecks Überprüfung auf dem Bildschirm angezeigt.

Ergebnisse

vRealize Automation erfasst Daten Ihres Endpoints und ermittelt Ihre Computing-Ressourcen.

Hinweis Benennen Sie vSphere-Datencenter nach der Datenerfassung nicht um, da andernfalls möglicherweise die Bereitstellung fehlschlägt.

Nächste Schritte

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

Erstellen eines NSX-Endpoints und Zuordnen zu einem vSphere-Endpoint

Sie können einen NSX-Endpoint erstellen und seine NSX-Einstellungen einem vorhandenen vSphere-Endpoint zuordnen.

Wenn Sie einen vSphere-Endpoint aktualisiert oder migriert haben, der einen NSX-Manager verwendet hat, wird ein neuer NSX-Endpoint erstellt, der eine Zuordnung zwischen dem vSphere-Quell-Endpoint und einem neuen NSX-Endpoint enthält.

Informationen zur Überprüfung der NSX-Verbindung und zur Vertrauensstellung des Zertifikats finden Sie unter [Überlegungen bei der Verwendung einer Testverbindung](#).

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **IaaS-Administrator** an.
- Um Ihren vSphere-Endpoint zu verwalten, müssen Sie einen vSphere-Proxy-Agent installieren, und Sie müssen den exakt selben Namen für den Endpoint und den Agent verwenden. Informationen zum Installieren des Agents finden Sie unter *Installieren von vRealize Automation*.
- Konfigurieren Sie die NSX-Netzwerkeinstellungen. Siehe [Konfigurieren der Einstellungen für Netzwerk- und Sicherheitskomponenten](#).
- [Erstellen eines vSphere-Endpoints](#).

Bei der Vorbereitung für die Verwendung der Netzwerk-, Sicherheits- und Lastausgleichsdienstfunktionen von NSX in vRealize Automation unter Verwendung von NSX-Manager-Anmeldedaten müssen Sie das NSX-Manager-Administratorkonto verwenden.

Verfahren

- 1** Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2** Wählen Sie **Neu > Netzwerk und Sicherheit > NSX** 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 die NSX-Instanz ein.

Die URL muss folgenden Typ aufweisen: **https://hostname** oder **https://IP_address**.

Beispiel: **https://nsx-manager.local**.

- 6 Geben Sie den NSX-Administratorbenutzernamen und das zugehörige Kennwort ein, die für den NSX-Endpoint gespeichert sind.
- 7 (Optional) Klicken Sie auf **Eigenschaften** und fügen Sie benutzerdefinierte Eigenschaften, Eigenschaftsgruppen oder Ihre eigenen Eigenschaftsdefinitionen für den Endpoint hinzu.
- 8 Um die NSX-Netzwerk- und Sicherheitseinstellungen zu einem vorhandenen vSphere-Endpoint zuzuordnen, klicken Sie auf **Zuordnungen** und wählen Sie einen vorhandenen vSphere-Endpoint aus.

Bevor Sie die Zuordnung erstellen können, müssen Sie den vSphere-Endpoint erstellen.

Sie können einen NSX-Endpoint nur einem vSphere-Endpoint zuordnen. Die Zuordnungseinschränkung bedeutet, dass Sie kein universelles bedarfsgesteuertes Netzwerk bereitstellen und es an vSphere-Maschinen anhängen können, die auf verschiedenen vCentern bereitgestellt wurden.

- 9 (Optional) Klicken Sie auf **Verbindung testen**, um die Anmeldedaten, die Host-Endpoint-Adresse und das vertrauenswürdige Zertifikat zu validieren. Mit dieser Aktion wird ebenfalls überprüft, ob der Manager-Dienst und der Agent zum Erfassen von Daten vom Endpoint ausgeführt werden. Mit der Aktion **OK** werden dieselben Bedingungen getestet.

Die Aktion **Testverbindung** gibt Informationen zu einer der folgenden Bedingungen zurück:

- **Zertifikatfehler**

Wenn das Zertifikat nicht gefunden wird, nicht als vertrauenswürdig eingestuft wird oder abgelaufen ist, werden Sie aufgefordert, einen Zertifikat-Fingerabdruck zu akzeptieren. Wenn Sie den Fingerabdruck nicht akzeptieren, können Sie weiterhin den Endpoint speichern, aber die Bereitstellung von Maschinen schlägt möglicherweise fehl.

- **Agent-Fehler**

Der zugeordnete vSphere-Agent wurde nicht gefunden. Der Agent muss für den Test erfolgreich ausgeführt werden.

- **Hostfehler**

Die angegebene Endpoint-Adresse ist nicht erreichbar oder der zugeordnete Manager-Dienst wird nicht ausgeführt. Der Manager-Dienst muss für den Test erfolgreich ausgeführt werden.

- **Anmeldedatenfehler**

Die angegebene Kombination aus Benutzername und Kennwort ist für den Endpoint unter der angegebenen Adresse ungültig.

- **Zeitüberschreitung**

Die Testaktion konnte nicht im zulässigen Zeitraum von zwei Minuten abgeschlossen werden.

Wenn die Aktion **Testverbindung** fehlschlägt, können Sie weiterhin den Endpoint speichern, aber die Bereitstellung von Maschinen schlägt möglicherweise fehl.

Wenn ein Problem mit dem vertrauenswürdigen Zertifikat vorliegt (zum Beispiel, wenn das Zertifikat abgelaufen ist), werden Sie aufgefordert, einen Zertifikat-Fingerabdruck zu akzeptieren.

10 Klicken Sie auf **OK**, um den Endpoint zu speichern.

Mit der Aktion **OK** werden dieselben Bedingungen wie mit der Aktion **Verbindung testen** getestet. Wenn eine der oben genannten Bedingungen gefunden wird, wird eine Meldung zurückgegeben. Wenn der Endpoint gespeichert werden kann, wird die Fehlermeldung weiterhin zwecks Überprüfung auf dem Bildschirm angezeigt.

Ergebnisse

vRealize Automation erfasst Daten Ihres Endpoints und ermittelt Ihre Computing-Ressourcen.

Nächste Schritte

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. Sie können dem vCloud Director-Endpoint auch Proxyeinstellungen zuordnen, indem Sie eine Zuordnung zu einem Proxy-Endpoint festlegen.

Informationen zur vCloud Air-Managementkonsole finden Sie in der vCloud Air-Dokumentation.

Hinweis Bei für vCloud Air-Endpoints und vCloud Director-Endpoints definierten Reservierungen wird die Verwendung von Netzwerkprofilen für die Bereitstellung von Maschinen nicht unterstützt.

Für vCloud Air-Endpoints müssen der Name der Organisation und der Name des vDC für eine vCloud Air-Abonnementinstanz identisch sein.

Weitere Informationen zum Zuordnen von Proxyeinstellungen zu Ihrem Endpoint finden Sie unter [Erstellen eines Proxy-Endpoints und Zuordnen dieses Endpoints zu einem Cloud-Endpoint](#).

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **laaS-Administrator** an.

- Stellen Sie sicher, dass Sie über die Berechtigung **Virtual Infrastructure-Administrator** für Ihr vCloud Air-Abonnementdienst- bzw. OnDemand-Konto verfügen.
- Wenn Sie zusätzliche Sicherheit konfigurieren und Verbindungen über einen Proxy-Server erzwingen möchten, erstellen Sie einen Proxy-Endpoint. Beim Erstellen eines vCloud Director-Endpoints können Sie eine Zuordnung zu dem Proxy-Endpoint festlegen. Siehe [Erstellen eines Proxy-Endpoints und Zuordnen dieses Endpoints zu einem Cloud-Endpoint](#).

Verfahren

- 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 Geben Sie Ihren Benutzernamen und Ihr Kennwort auf Administratorebene ein.

Sie müssen sich als vCloud Air-Abonnementdienst- bzw. OnDemand-Kontoadministrator anmelden.

Das Format des Benutzernamens ist `domain\username`.

Geben Sie die Anmeldedaten für einen Organisationsadministrator mit Berechtigungen zur Verbindungsherstellung durch Verwendung von VMware Remote Console ein.

- 6 (Optional) Klicken Sie auf **Eigenschaften** und fügen Sie benutzerdefinierte Eigenschaften, Eigenschaftsgruppen oder Ihre eigenen Eigenschaftsdefinitionen für den Endpoint hinzu.
- 7 (Optional) Um zusätzliche Sicherheit zu konfigurieren und Verbindungen über einen Proxyserver zu erzwingen, klicken Sie auf **Zuordnungen** und stellen Sie eine Zuordnung zu einem vorhandenen Proxy-Endpoint her.

Sie müssen mindestens über einen Proxy-Endpoint verfügen, um eine Zuordnung zu erstellen.
- 8 Klicken Sie auf **OK**.

Nächste Schritte

[Erstellen einer Fabric-Gruppe](#).

Erstellen eines vCloud Director-Endpoints

Sie können einen vCloud Director-Endpoint für die Verwaltung aller vCloud Director-vDCs (virtuelle Datencenter) in Ihrer Umgebung erstellen, oder Sie erstellen separate Endpoints für die Verwaltung jeder vCloud Director-Organisation. Sie können dem vCloud Director-Endpoint auch Proxyeinstellungen zuordnen, indem Sie eine Zuordnung zu einem Proxy-Endpoint festlegen.

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 Bei für vCloud Air-Endpoints und vCloud Director-Endpoints definierten Reservierungen wird die Verwendung von Netzwerkprofilen für die Bereitstellung von Maschinen nicht unterstützt.

Weitere Informationen zum Zuordnen von Proxyeinstellungen zu Ihrem Endpoint finden Sie unter [Erstellen eines Proxy-Endpoints und Zuordnen dieses Endpoints zu einem Cloud-Endpoint](#).

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **laaS-Administrator** an.
- Wenn Sie zusätzliche Sicherheit konfigurieren und Verbindungen über einen Proxy-Server erzwingen möchten, erstellen Sie einen Proxy-Endpoint. Beim Erstellen eines vCloud Director-Endpoints können Sie eine Zuordnung zu dem Proxy-Endpoint festlegen. Siehe [Erstellen eines Proxy-Endpoints und Zuordnen dieses Endpoints zu einem Cloud-Endpoint](#).

Verfahren

- 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 Geben Sie Ihren Benutzernamen und Ihr Kennwort auf Administratorebene ein.
 - 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
Alle Organisations-vCDs erkennen	Wenn Sie vCloud Director in einer Private Cloud implementiert haben, können Sie das Textfeld Organisation leer lassen, um der Anwendung die Erkennung von allen verfügbaren Organisations-vDCs zu erlauben.
Separate Endpoints für jedes Organisations-vCD	Geben Sie in das Textfeld Organisation 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 für den Endpoint eingeben, benötigen Sie einen Benutzer, der in dieser Organisation über Anmeldedaten des Organisationsadministrators verfügt.

Geben Sie die Anmeldedaten mit Berechtigungen zur Verbindungsherstellung durch Verwendung von VMware Remote Console ein.

- Geben Sie zum Verwalten aller Organisationen mit einem einzelnen Endpoint die Anmeldedaten für einen Systemadministrator ein.
- Erstellen Sie zum Verwalten eines jeden virtuellen Datencenters einer Organisation (vDC) mit einem separaten Endpoint separate Anmeldedaten für Organisationsadministratoren für jedes vDC.

Erstellen Sie nicht einen einzelnen Endpoint auf Systemebene und einzelne Organisations-Endpoints für dieselbe vCloud Director-Instanz.

- 7 (Optional) Klicken Sie auf **Eigenschaften** und fügen Sie benutzerdefinierte Eigenschaften, Eigenschaftsgruppen oder Ihre eigenen Eigenschaftsdefinitionen für den Endpoint hinzu.
- 8 (Optional) Um zusätzliche Sicherheit zu konfigurieren und Verbindungen über einen Proxyserver zu erzwingen, klicken Sie auf **Zuordnungen** und stellen Sie eine Zuordnung zu einem vorhandenen Proxy-Endpoint her.

Sie müssen mindestens über einen Proxy-Endpoint verfügen, um eine Zuordnung zu erstellen.

- 9 Klicken Sie auf **OK**.

Nächste Schritte

[Erstellen einer Fabric-Gruppe.](#)

Erstellen eines Amazon-Endpoints

Sie können einen Endpoint zum Herstellen einer Verbindung zu einer Amazon-Instanz verwenden. Wahlweise können Sie Proxyeinstellungen auch dem Amazon-Endpoint zuordnen, indem Sie eine Zuordnung zum Proxy-Endpoint erstellen.

vRealize Automation stellt mehrere -Instanztypen bereit, die Sie beim Erstellen von Blueprints verwenden können. Informationen zum Importieren eigener Instanztypen finden Sie unter [Hinzufügen eines Amazon-Instanztyps](#).

Weitere Informationen zum Zuordnen von Proxyeinstellungen zu Ihrem Endpoint finden Sie unter [Erstellen eines Proxy-Endpoints und Zuordnen dieses Endpoints zu einem Cloud-Endpoint](#).

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **IaaS-Administrator** an.
- Wenn Sie zusätzliche Sicherheit konfigurieren und Verbindungen über einen Proxy-Server erzwingen möchten, erstellen Sie einen Proxy-Endpoint. Beim Erstellen eines Amazon-Endpoints können Sie eine Zuordnung zu dem Proxy-Endpoint festlegen. Siehe [Erstellen eines Proxy-Endpoints und Zuordnen dieses Endpoints zu einem Cloud-Endpoint](#).

Verfahren

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-Konto für diesen Endpoint.

4 Geben Sie die Zugriffsschlüssel-ID auf Administratorebene für das Amazon-Konto ein.

Nur einem Endpoint kann eine Amazon-Zugriffsschlüssel-ID zugeordnet werden.

Für den Abruf des erforderlichen Zugriffsschlüssels zum Erstellen des Amazon-Endpoints müssen Sie 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 finden Sie in der Dokumentation zu Amazon.

5 Geben Sie den geheimen Zugriffsschlüssel für den Amazon-Endpoint ein.

6 (Optional) Klicken Sie auf **Eigenschaften** und fügen Sie benutzerdefinierte Eigenschaften, Eigenschaftsgruppen oder Ihre eigenen Eigenschaftsdefinitionen für den Endpoint hinzu.

7 (Optional) Um zusätzliche Sicherheit zu konfigurieren und Verbindungen über einen Proxyserver zu erzwingen, klicken Sie auf **Zuordnungen** und stellen Sie eine Zuordnung zu einem vorhandenen Proxy-Endpoint her.

Sie müssen mindestens über einen Proxy-Endpoint verfügen, um eine Zuordnung zu erstellen.

8 Klicken Sie auf **OK**.

Ergebnisse

Nach der Erstellung des Endpoints beginnt vRealize Automation mit der Erfassung von Daten aus den Amazon Web Services-Regionen.

Nächste Schritte

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 bei vRealize Automation als **IaaS-Administrator** an.

Verfahren

1 Klicken Sie auf **Infrastruktur > Administration > Instanztypen**.

2 Klicken Sie auf **Neu**.

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** (✔).

Ergebnisse

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

Nächste Schritte

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

Erstellen eines Proxy-Endpoints und Zuordnen dieses Endpoints zu einem Cloud-Endpoint

Sie können einen Proxy-Endpoint erstellen und dessen Proxyeinstellungen einem vCloud Air-, vCloud Director- oder Amazon-Endpoint zuordnen.

Wenn Sie einen vCloud Air-, vCloud Director- oder Amazon-Endpoint aktualisieren oder migrieren, der einen Proxymanager verwendet hat, wird ein neuer vCloud Air-, vCloud Director- oder Amazon-Endpoint erstellt, der eine Zuordnung zwischen dem vCloud Air-, vCloud Director- oder Amazon-Endpoint und einem neuen Proxy-Endpoint enthält.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **IaaS-Administrator** an.
- Erstellen Sie einen der folgenden Endpoint-Typen:
 - [Erstellen eines vCloud Air-Endpoints](#)
 - [Erstellen eines Amazon-Endpoints](#)
 - [Erstellen eines vCloud Director-Endpoints](#)

Sie benötigen mindestens einen vCloud Air-, vCloud Director- oder Amazon-Endpoint, um eine Zuordnung über den Proxy-Endpoint zu erstellen.

Verfahren

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Wählen Sie **Neu > Netzwerk und Sicherheit > Proxy** 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 installierten Proxy-Agent ein.
- 6 Geben Sie in das Textfeld **Port** die zu verwendende Portnummer für die Verbindung mit dem Proxy-Server ein.
- 7 Geben Sie Ihren Benutzernamen und Ihr Kennwort auf Administratorebene ein.
- 8 (Optional) Klicken Sie auf **Eigenschaften** und fügen Sie benutzerdefinierte Eigenschaften, Eigenschaftsgruppen oder Ihre eigenen Eigenschaftsdefinitionen für den Endpoint hinzu.

- 9 Um die Proxyeinstellungen zu einem vCloud Air-, vCloud Director- oder Amazon-Endpoint zuzuordnen, klicken Sie auf **Zuordnungen** und wählen Sie einen oder mehrere Endpoints aus.

Sie müssen mindestens über einen vCloud Air-, vCloud Director- oder Amazon-Endpoint verfügen, um eine Zuordnung zu erstellen.

Sie können den Proxy-Endpoint mehreren Endpoints zuordnen.

- 10 Klicken Sie auf **OK**.

Ergebnisse

vRealize Automation erfasst Daten Ihres Endpoints und ermittelt Ihre Computing-Ressourcen.

Nächste Schritte

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

Erstellen eines Proxy-Endpoints für eine OVF-Host-Website

Sie können einen Proxy-Endpoint erstellen, um ihn beim Importieren von OVF in eine vSphere-Maschinenkomponente in einem Blueprint oder als Wertsatz für ein Image-Komponentenprofil zu verwenden, wenn die OVF-Datei auf einer Website gehostet wird.

Weitere Informationen zum Konfigurieren für die OVF-Bereitstellung finden Sie unter [Erstellen eines vSphere-Endpoints](#) und [Konfigurieren eines bereitzustellenden Blueprints in einer OVF-Datei](#).

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **laaS-Administrator** an.

Verfahren

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Wählen Sie **Neu > Netzwerk und Sicherheit > Proxy** aus.
- 3 Geben Sie im Textfeld **Name** einen Namen ein.
- 4 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein.
- 5 Geben Sie im Textfeld **Adresse** die URL für die Website ein, die die OVF-Datei hostet.
- 6 Geben Sie im Textfeld **Port** die zu verwendende Portnummer für die Verbindung mit dem Proxyserver der Website ein.
- 7 Geben Sie Ihren Benutzernamen und Ihr Kennwort auf Administratorebene ein.
- 8 (Optional) Klicken Sie auf **Eigenschaften** und fügen Sie benutzerdefinierte Eigenschaften, Eigenschaftsgruppen oder Ihre eigenen Eigenschaftsdefinitionen für den Endpoint hinzu.
- 9 Klicken Sie auf **OK**.

Ergebnisse

Sie können nun den Endpoint zum Definieren der Website, von der OVF bezogen werden soll, verwenden. Weitere Informationen finden Sie unter [Definieren von Blueprint-Einstellungen für eine vSphere-Komponente unter Verwendung einer OVF-Datei](#) und [Definieren eines Image-Wertsatzes für ein Komponentenprofil unter Verwendung einer OVF-Datei](#).

Erstellen eines vRealize Orchestrator-Endpoints

Sie können einen vRealize Orchestrator-Endpoint für die Verbindung zu einem vRealize Orchestrator-Server erstellen.

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 bei vRealize Automation als **laaS-Administrator** an.

Verfahren

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Wählen Sie **Neu > Orchestrierung > vRealize 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 Geben Sie Ihre vRealize Orchestrator-Anmeldedaten in den Feldern **Benutzername** und **Kennwort** ein, um eine Verbindung zum vRealize Orchestrator-Endpoint herzustellen.

Die verwendeten Anmeldedaten sollten für alle vRealize Orchestrator-Workflows von laaS über Berechtigungen zum Ausführen verfügen.

Um die in der vRealize Automation-Appliance eingebettete vRealize Orchestrator-Standardinstanz zu verwenden, lautet der Benutzername **`administrator@vsphere.local`** und das Kennwort ist das Administratorkennwort, das bei der Konfiguration von SSO angegeben wurde.

- 6 Geben Sie eine ganze Zahl größer oder gleich 1 in das Textfeld **Priorität** ein.

Ein niedrigerer Wert gibt eine höhere Priorität an.

- 7 (Optional) Klicken Sie auf **Eigenschaften** und fügen Sie benutzerdefinierte Eigenschaften, Eigenschaftsgruppen oder Ihre eigenen Eigenschaftsdefinitionen für den Endpoint hinzu.
- 8 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 die eingebettete Instanz als vRealize Orchestrator-Endpoint für das Ausführen von vRealize Automation-Workflows in einer Produktions- oder Testumgebung oder für das Erstellen eines Proof-of-Concepts verwenden.

Die Verwendung dieses vRealize Orchestrator-Endpoints für die Ausführung von vRealize Automation-Workflows in einer Produktionsumgebung wird ebenfalls empfohlen.

Das vRealize Orchestrator-Plug-In wird automatisch mit vRealize Orchestrator 7.1 und höher installiert. Es muss kein separates vRealize Orchestrator-Plug-In installiert werden.

Erstellen eines vRealize Operations Manager-Endpoints

Sie können einen vRealize Operations Manager-Endpoint für die Verbindung zu einer vRealize Operations Manager-Host-Suite-API erstellen.

Informationen zur Überprüfung der vRealize Operations Manager-Verbindung und zur Vertrauensstellung des Zertifikats finden Sie unter [Überlegungen bei der Verwendung einer Testverbindung](#).

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **laaS-Administrator** an.

Verfahren

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Wählen Sie **Neu > Management > vRealize Operations Manager** aus.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 Geben Sie die URL für den vRealize Operations Manager-Server in das Textfeld **Adresse** ein.
Die URL muss folgendes Format aufweisen: **https://hostname/suite-api**.
- 5 Geben Sie Ihren Benutzernamen und Ihr Kennwort für vRealize Operations Manager ein.

- 6 (Optional) Klicken Sie auf **Eigenschaften** und fügen Sie benutzerdefinierte Eigenschaften, Eigenschaftsgruppen oder Ihre eigenen Eigenschaftsdefinitionen für den Endpoint hinzu.
- 7 (Optional) Klicken Sie auf **Verbindung testen**, um die Anmeldedaten, die Host-Endpoint-Adresse und das vertrauenswürdige Zertifikat zu validieren. Mit dieser Aktion wird ebenfalls überprüft, ob der Manager-Dienst und der Agent zum Erfassen von Daten vom Endpoint ausgeführt werden. Mit der Aktion **OK** werden dieselben Bedingungen getestet.

Die Aktion **Testverbindung** gibt Informationen zu einer der folgenden Bedingungen zurück:

- **Zertifikatfehler**

Wenn das Zertifikat nicht gefunden wird, nicht als vertrauenswürdig eingestuft wird oder abgelaufen ist, werden Sie aufgefordert, einen Zertifikat-Fingerabdruck zu akzeptieren. Wenn Sie den Fingerabdruck nicht akzeptieren, können Sie weiterhin den Endpoint speichern, aber die Bereitstellung von Maschinen schlägt möglicherweise fehl.

- **Agent-Fehler**

Der zugeordnete vSphere-Agent wurde nicht gefunden. Der Agent muss für den Test erfolgreich ausgeführt werden.

- **Hostfehler**

Die angegebene Endpoint-Adresse ist nicht erreichbar oder der zugeordnete Manager-Dienst wird nicht ausgeführt. Der Manager-Dienst muss für den Test erfolgreich ausgeführt werden.

- **Anmeldedatenfehler**

Die angegebene Kombination aus Benutzername und Kennwort ist für den Endpoint unter der angegebenen Adresse ungültig.

- **Zeitüberschreitung**

Die Testaktion konnte nicht im zulässigen Zeitraum von zwei Minuten abgeschlossen werden.

Wenn die Aktion **Testverbindung** fehlschlägt, können Sie weiterhin den Endpoint speichern, aber die Bereitstellung von Maschinen schlägt möglicherweise fehl.

Wenn ein Problem mit dem vertrauenswürdigen Zertifikat vorliegt (zum Beispiel, wenn das Zertifikat abgelaufen ist), werden Sie aufgefordert, einen Zertifikat-Fingerabdruck zu akzeptieren.

- 8 Klicken Sie auf **OK**.

Erstellen eines Endpoints eines IPAM-Drittanbieters

Wenn Sie in vRealize Orchestrator einen IPAM Endpoint-Typ eines Drittanbieters registriert und konfiguriert haben, können Sie in vRealize Automation einen Endpoint für diesen IPAM-Lösungsanbieter 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 Sie über die VMware Solution Exchange-Site herunterladen können. Sie können dieses Verfahren auch verwenden, wenn Sie Ihr eigenes IPAM-Anbieterpaket mithilfe des im Lieferumfang von VMware enthaltenen IPAM-Lösungs-SDK 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 in vRealize Orchestrator den Endpoint-Typ für das Plug-In des IPAM-Lösungsanbieters registrieren.

Voraussetzungen

- [Abrufen und Importieren eines IPAM-Drittanbieterpakets in vRealize Orchestrator.](#)
- [Führen Sie den Workflow zur Registrierung des Drittanbieter-IPAM-Endpoint-Typs aus in vRealize Orchestrator.](#)
- Melden Sie sich bei vRealize Automation als **laaS-Administrator** an.

Erstellen Sie für dieses Beispiel einen Infoblox-IPAM-Endpoint unter Verwendung eines Endpoint-Typs, den Sie in vRealize Orchestrator für Ihr IPAM-Drittanbieter-Plug-In oder -Paket registriert haben.

Verfahren

1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.

2 Wählen Sie **Neu > IPAM > IPAM-Endpoint-Typ**.

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 auf **Eigenschaften** und fügen Sie Endpoint-Eigenschaften hinzu, die für den jeweiligen 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**.

Nächste Schritte

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

Erstellen eines Microsoft Azure-Endpoints

Sie können einen Microsoft Azure-Endpoint erstellen, um die Einrichtung einer authentifizierten Verbindung zwischen vRealize Automation und einer Azure-Bereitstellung zu erleichtern.

Ein Endpoint stellt eine Verbindung zu einer Ressource her, in diesem Fall eine Azure-Instanz, mit der Sie Blueprints für virtuelle Maschine erstellen können. Sie müssen über einen Azure-Endpoint verfügen, der als Basis von Blueprints für die Bereitstellung von virtuellen Azure-Maschinen verwendet wird. Wenn Sie mehrere Azure-Abonnements verwenden, benötigen Sie Endpoints für jede Abonnement-ID.

Als Alternative können Sie mithilfe des Befehls zum Hinzufügen einer Azure-Verbindung eine solche direkt aus vRealize Orchestrator erstellen. Dieser befindet sich unter **Bibliothek > Azure- > Konfiguration** in der Workflow-Struktur von vRealize Orchestrator. In den meisten Fällen ist das Erstellen einer Verbindung über die Endpoint-Konfiguration wie in diesem Dokument beschrieben die bevorzugte Option.

Azure-Endpoints werden von vRealize Orchestrator und der XaaS-Funktionalität unterstützt. Sie können einen Azure-Endpoint erstellen, löschen oder bearbeiten. Bitte beachten Sie: Wenn Sie Änderungen an einem bestehenden Endpoint vornehmen und einige Stunden lang keine Updates an dem Azure-Portal über die aktualisierte Verbindung durchführen, müssen Sie den vRealize Orchestrator-Dienst über den Befehl `service vco-service restart` neu starten. Wird der Dienst nicht neu gestartet, kann dies zu Fehlern führen.

Voraussetzungen

- Konfigurieren Sie eine Instanz von Microsoft Azure und rufen Sie ein gültiges Microsoft Azure-Abonnement ab, dessen Abonnement-ID verwendet werden kann. Weitere Informationen über das Konfigurieren von Azure und das Abrufen einer Abonnement-ID finden Sie unter <http://www.vaficionado.com/2016/11/using-new-microsoft-azure-endpoint-vrealize-automation-7-2/>.
- Stellen Sie sicher, dass Ihre vRealize Automation-Bereitstellung über mindestens einen Mandanten und eine Business-Gruppe verfügt.
- Erstellen Sie ein Active Directory-Verzeichnis für eine Anwendung, wie in <https://azure.microsoft.com/de-de/documentation/articles/resource-group-create-service-principal-portal> beschrieben.
- Notieren Sie sich die folgenden Informationen im Zusammenhang mit Azure, da Sie sie während der Endpoint- und Blueprint-Konfiguration benötigen.
 - Abonnement-ID
 - Mandanten-ID
 - Name des Speicherkontos
 - Name der Ressourcengruppe
 - Speicherort
 - Name des virtuellen Netzwerks
 - Client-Anwendungs-ID
 - Geheimer Schlüssel der Client-Anwendung
 - URN des VM-Images

- Es gibt eindeutige Einstellungen für das Erstellen und Bereitstellen von Cloudanwendungen für Azure in der China-Umgebung. Weitere Informationen finden Sie unter <https://docs.microsoft.com/en-us/azure/china/china-get-started-developer-guide>. Wenn Sie einen vRealize Automation Azure-Endpoint für China erstellen, müssen die Dienst-URL, die Anmelde-URL und die Speicher-URL wie folgt angegeben werden:

- Dienst-URL: `https://management.chinacloudapi.cn`
- Anmelde-URL: `https://login.chinacloudapi.cn/`
- Speicher-URL: `https://storage_account_name.blob.core.chinacloudapi.cn/`

Die Azure-Implementierung innerhalb von vRealize Automation unterstützt einen Teil der von Microsoft Azure unterstützten Regionen. Siehe [Von Azure unterstützte Regionen](#).

- Melden Sie sich bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 1 Wählen Sie **Administration > vRO-Konfiguration > Endpoints** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Klicken Sie auf der Registerkarte „Plugin“ auf das Dropdown-Menü **Plugin** und wählen Sie das **Azure-Plugin** aus.
- 4 Klicken Sie auf **Weiter**.
- 5 Geben Sie einen Namen und optional eine Beschreibung ein.
- 6 Klicken Sie auf **Weiter**.
- 7 Befüllen Sie die Textfelder auf der Registerkarte **Details** entsprechend den Anforderungen des Endpoints.

Parameter	Beschreibung
Verbindungseinstellungen	
Azure-Verbindung	
Name der Verbindung	Eindeutiger Name für die neue Endpoint-Verbindung. Dieser Name wird in der vRealize Orchestrator-Schnittstelle angezeigt, um Ihnen das Identifizieren einer bestimmten Verbindung zu erleichtern.
Azure-Abonnement-ID	Der Bezeichner für Ihr Azure-Abonnement. Mit der ID werden die Speicherkonten, virtuellen Maschinen und andere Azure-Ressourcen angegeben, auf die Sie zugreifen können.
Einstellungen des Ressourcenmanagers	
URI des Azure-Diensts	Der URI, über den Sie Zugriff auf die Azure-Instanz erhalten. Der Standardwert von <code>https://management.azure.com/</code> eignet sich für viele gängige Implementierungen.

Parameter	Beschreibung
URI des Azure-Speichers	Der URI, über den Sie Zugriff auf die Azure-Speicherinstanz erhalten.
Mandanten-ID	Die ID des Azure-Mandanten, die vom Endpoint verwendet werden soll.
Client-ID	Der Bezeichner des Azure-Clients, der vom Endpoint verwendet werden soll. Dieser wird zugewiesen, wenn Sie eine Active Directory-Anwendung erstellen.
Geheimer Client-Schlüssel	Der Schlüssel, der mit einer Azure-Client-ID verwendet wird. Dieser Schlüssel wird zugewiesen, wenn Sie eine Active Directory-Anwendung erstellen.
Anmelde-URL	Die für den Zugriff auf die Azure-Instanz verwendete URL. Der Standardwert von <code>https://login.windows.net/</code> eignet sich für viele gängige Implementierungen.
Proxy-Einstellungen	
Proxy-Host	Wenn Ihr Unternehmen einen Proxy-Webserver verwendet, geben Sie den Namen dieses Servers ein.
Proxy-Port	Wenn Ihr Unternehmen einen Proxy-Webserver verwendet, geben Sie die Portnummer dieses Servers ein.

8 (Optional) Klicken Sie auf „Eigenschaften“ und fügen Sie benutzerdefinierte Eigenschaften, Eigenschaftsgruppen oder Ihre eigenen Eigenschaftsdefinitionen hinzu.

9 Klicken Sie auf **Fertig stellen**.

Nächste Schritte

Erstellen Sie in Azure geeignete Ressourcengruppen, Speicherkonten und Netzwerksicherheitsgruppen. Sie sollten ggf. auch Lastausgleichsmodule für Ihre Implementierung erstellen.

Aktion	Optionen
Erstellen einer Azure-Ressourcengruppe	<ul style="list-style-type: none"> ■ Erstellen Sie die Ressourcengruppe mithilfe des Azure-Portals. Spezielle Anweisungen finden Sie in der Azure-Dokumentation. ■ Verwenden Sie den geeigneten vRealize Orchestrator-Workflow, der sich in der Ressourcengruppe unter <code>Library/Azure/Resource/Create</code> befindet. ■ Erstellen und veröffentlichen Sie in vRealize Automation einen XaaS-Blueprint, der den vRealize Orchestrator-Workflow enthält. Sie können die Ressourcengruppe anfordern, nachdem Sie sie an den Dienst und die Berechtigungen angehängt haben. Beachten Sie, dass der Ressourcentyp der Ressourcengruppe von vRealize Automation nicht unterstützt oder verwaltet wird.
Erstellen eines Azure-Speicherkontos	<ul style="list-style-type: none"> ■ Verwenden Sie Azure, um ein Speicherkonto zu erstellen. Spezielle Anweisungen finden Sie in der Azure-Dokumentation. ■ Verwenden Sie den geeigneten vRealize Orchestrator-Workflow, der sich im Speicherkonto unter <code>Library/Azure/Storage/Create</code> befindet. ■ Erstellen und veröffentlichen Sie in vRealize Automation einen XaaS-Blueprint, der den vRealize Orchestrator-Workflow enthält. Sie können das Speicherkonto anfordern, nachdem Sie es an den Dienst und die Berechtigungen angehängt haben.
Erstellen einer Azure-Netzwerk-Sicherheitsgruppe	<ul style="list-style-type: none"> ■ Verwenden Sie Azure, um eine Sicherheitsgruppe zu erstellen. Spezielle Anweisungen finden Sie in der Azure-Dokumentation. ■ Verwenden Sie den geeigneten vRealize Orchestrator-Workflow, der sich in der Netzwerksicherheitsgruppe unter <code>Library/Azure/Network/Create</code> befindet. ■ Erstellen und veröffentlichen Sie in vRealize Automation einen XaaS-Blueprint, der den vRealize Orchestrator-Workflow enthält. Sie können die Sicherheitsgruppe anfordern, nachdem Sie sie zu dem Dienst und den Berechtigungen hinzugefügt haben.

Von Azure unterstützte Regionen

Die Azure-Implementierung innerhalb von vRealize Automation unterstützt einen Teil der von Microsoft Azure unterstützten Regionen.

Die folgenden Azure-Regionen werden durch die Azure-Implementierung innerhalb von vRealize Automation unterstützt.

- | | |
|---------------------|------------------------|
| ■ Asien, Osten | ■ Australien, Osten |
| ■ Asien, Südosten | ■ Australien, Südosten |
| ■ USA, Mitte | ■ Indien, Süden |
| ■ USA, Osten | ■ Indien, Mitte |
| ■ USA, Osten 2 | ■ Indien, Westen |
| ■ USA, Westen | ■ Kanada, Mitte |
| ■ USA, Westen 2 | ■ Kanada, Osten |
| ■ USA, Norden-Mitte | ■ USA, Westen-Mitte |
| ■ USA, Süden-Mitte | ■ Korea, Mitte |
| ■ Europa, Norden | ■ Korea, Süden |
| ■ Europa, Westen | ■ UK, Westen |
| ■ Japan, Westen | ■ UK, Süden |
| ■ Japan, Osten | ■ China, Osten |
| ■ Brasilien, Süden | ■ China, Norden |

Erstellen eines Puppet-Endpoints

Sie können einen Puppet-Endpoint erstellen, um das Hinzufügen von Puppet-Konfigurationsverwaltungskomponenten zu virtuellen vSphere-Maschinen zu unterstützen. Diese Komponenten ermöglichen es Ihnen, einen Puppet-Master zu verwenden, um die Verwaltung der Konfiguration auf virtuellen Maschinen zu erzwingen.

Ein Endpoint stellt eine Verbindung zu einer externen Ressource her, in diesem Fall zu einer Puppet-Master-Instanz. Der Endpoint ermöglicht es Ihnen, Puppet-Konfigurationsverwaltungskomponenten auf Blueprints der virtuellen vSphere-Maschinen zu platzieren. Bereitgestellte virtuelle Maschinen, die auf diesen Blueprints basieren, enthalten einen Puppet-Agent, der die Steuerung durch den zugeordneten Puppet Master vereinfacht.

Weitere Informationen über das Puppet-Plug-In und eine Demo seiner Konfiguration finden Sie unter <https://www.youtube.com/watch?v=P-VglzE9o-o>.

Voraussetzungen

- Installieren und konfigurieren Sie Puppet Enterprise gemäß den Anforderungen Ihrer Umgebung.
- Laden Sie das Puppet-Plug-In, Version 3.0, für Ihre vRealize Orchestrator-Bereitstellung herunter und installieren Sie es. Sie können das Plug-In über <https://marketplace.vmware.com/vsx/solutions/puppet-plugin-for-vrealize-automation?ref=search> herunterladen. Informationen zur Installation und Verwendung des Plug-Ins finden Sie unter https://docs.puppet.com/pe/latest/vro_intro.html.

Verfahren

- 1 Wählen Sie **Administration > vRO-Konfiguration > Endpoints** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Klicken Sie auf der Registerkarte „Plug-In“ auf das Dropdown-Menü **Plug-In** und wählen Sie das **Puppet-Plug-In** aus.
- 4 Klicken Sie auf **Weiter**.

- 5 Geben Sie einen Namen und optional eine Beschreibung ein.
- 6 Klicken Sie auf **Weiter**.
- 7 Befüllen Sie die Textfelder auf der Registerkarte **Details** entsprechend den Anforderungen des Endpoints.

Parameter	Beschreibung
Anzeigename für diesen Puppet-Master	Der Name des Puppet-Masters, der der Endpoint-Verbindung zugeordnet ist. Dieser Name wird in der vRealize Orchestrator-Schnittstelle angezeigt, um Ihnen das Identifizieren einer bestimmten Verbindung zu erleichtern.
Hostname oder IP-Adresse	Der FQDN oder die IP-Adresse des Puppet-Masters, der von diesem Endpoint verwendet wird.
SSH-Port	Der Port, der für die Verwendung durch die sichere Kommunikation für diesen Puppet-Master definiert ist.
SSH RBAC und Benutzername	Der Benutzername für die rollenbasierte Zugriffssteuerung, der für die Verbindung mit dem Puppet-Master erforderlich ist.
SSH und Kennwort für RBAC	Das Kennwort für die rollenbasierte Zugriffssteuerung, das für die Verbindung mit dem Puppet-Master erforderlich ist.
Sudo für Shell-Befehle auf diesem Master verwenden?	Wählen Sie diese Option, wenn Administratoren Sudo-Befehle auf Linux-Servern für Sicherheitsoptionen auf virtuellen Maschinen, die auf diesem Endpoint basieren, verwenden können sollen.

- 8 Klicken Sie auf **OK**.

Ergebnisse

Sie können jetzt Puppet-Konfigurationsverwaltungskomponenten zu vSphere-Blueprints hinzufügen, damit Sie virtuelle vSphere-Maschinen bereitstellen können, die Puppet-Agents enthalten.

Erstellen eines Hyper-V (SCVMM)-Endpoints

Sie können Endpoints für die Kommunikation zwischen vRealize Automation und Ihrer SCVMM-Umgebung erstellen und Computing-Ressourcen identifizieren, Daten sammeln und Maschinen bereitstellen.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **laaS-Administrator** an.
- Sie müssen einen DEM-Agent zum Verwalten Ihres Hyper-V (SCVMM)-Endpoints installieren und konfigurieren. Weitere Informationen finden Sie bei den SCVMM-Anforderungen im Handbuch *Installieren von vRealize Automation*.

Informationen hierzu finden Sie unter [Vorbereiten Ihrer SCVMM-Umgebung](#).

Verfahren

- 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 Geben Sie den Administratorbenutzernamen und das zugehörige Kennwort ein, den bzw. das Sie für diesen Endpoint gespeichert haben.
 Falls Sie die Anmeldedaten noch nicht gespeichert haben, können Sie sie nun speichern.
- 7 (Optional) Klicken Sie auf **Eigenschaften** und fügen Sie benutzerdefinierte Eigenschaften, Eigenschaftsgruppen oder Ihre eigenen Eigenschaftsdefinitionen für den Endpoint hinzu.
- 8 Klicken Sie auf **OK**.

Ergebnisse

vRealize Automation erfasst Daten Ihres Endpoints und ermittelt Ihre Computing-Ressourcen.

Nächste Schritte

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

Erstellen eines OpenStack-Endpoints

Sie erstellen einen Endpoint, damit vRealize Automation mit der OpenStack-Instanz kommunizieren kann.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **laaS-Administrator** an.
- 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*.
- Stellen Sie sicher, dass der verwendete Openstack-Typ aktuell unterstützt wird. Siehe *Übersicht über die Unterstützung von vRealize Automation*.

Wenn Sie ein Upgrade oder eine Migration von einer früheren vRealize Automation-Installation durchgeführt haben und die Datenerfassung für OpenStack-Endpoints fehlschlägt, können Sie die benutzerdefinierte Eigenschaft `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` zu jedem Keystone V3 OpenStack-Endpoint hinzufügen, um einen gültigen Domänennamen anzugeben und die Datenerfassung zu aktivieren.

Verfahren

- 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
PowerVC	Die URL muss das Format http://myPowerVC.com:5000 oder http://FQDN:5000 aufweisen.
OpenStack	Die URL muss das Format FQDN:5000 oder IP_address:5000 aufweisen. Geben Sie das Suffix /v2.0 nicht für die Endpoint-Adresse an.

- 5 Geben Sie Ihren Administratorbenutzernamen und das zugehörige Kennwort ein.
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 Klicken Sie auf **Eigenschaften** und fügen Sie benutzerdefinierte Eigenschaften, Eigenschaftsgruppen oder Ihre eigenen Eigenschaftsdefinitionen für den Endpoint hinzu.
Wenn Keystone V3 aktiv ist, fügen Sie die benutzerdefinierte Eigenschaft `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` hinzu, um eine bestimmte Domäne zuzuweisen.
- 8 Klicken Sie auf **OK**.

Ergebnisse

vRealize Automation erfasst Daten Ihres Endpoints und ermittelt Ihre Computing-Ressourcen.

Nächste Schritte

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

Erstellen eines Hyper-V-, XenServer- oder Xen-Pool-Endpoints

Sie können Endpoints erstellen, um vRealize Automation die Kommunikation mit der Hauptumgebung von Hyper-V, XenServer oder Xen-Pool zu ermöglichen, die Computing-Ressourcen zu identifizieren, Daten zu erfassen und Maschinen bereitzustellen.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **laaS-Administrator** an.

- Ein Systemadministrator muss einen Proxy-Agent mit entsprechenden gespeicherten Anmeldedaten für Ihren Endpoint erstellen. Siehe *Installieren von vRealize Automation*.

Verfahren

- 1 Wählen Sie **Infrastruktur > Endpoints > Agents** aus.
- 2 Geben Sie den vollqualifizierten DNS-Namen Ihres Hyper-V-Servers, Xen-Servers oder Ihres Xen-Hauptpools im Textfeld **Computing-Ressource** ein.

Hinweis Für einen Xen-Pool-Endpoint müssen Sie den Namen des Hauptpools eingeben. Um doppelte Einträge in der vRealize Automation-Computing-Ressourcentabelle zu vermeiden, geben Sie eine Adresse an, die der konfigurierten Hauptadresse des Xen-Pools entspricht. Wenn als Hauptadresse des Xen-Pools beispielsweise der Hostname verwendet wird, geben Sie den Hostnamen ein und nicht den FQDN. Wenn der FQDN als Hauptadresse des Xen-Pools 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**.

Ergebnisse

vRealize Automation erfasst Daten Ihres Endpoints und ermittelt Ihre Computing-Ressourcen.

Nächste Schritte

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

Überlegungen bei der Verwendung einer Testverbindung

Sie können eine Testverbindung zwecks Überprüfung der Anmeldedaten, der Host-Endpoint-Adresse und des Zertifikats für einen vSphere-, NSX- oder vRealize Operations Manager-Endpoint verwenden.

Mit dieser Aktion wird ebenfalls überprüft, ob der Manager-Dienst und der Agent zum Erfassen von Daten vom Endpoint ausgeführt werden.

Die Aktion **Testverbindung** gibt Informationen zu einer der folgenden Bedingungen zurück:

- **Zertifikatsfehler**
Wenn das Zertifikat nicht gefunden wird, nicht als vertrauenswürdig eingestuft wird oder abgelaufen ist, werden Sie aufgefordert, einen Zertifikat-Fingerabdruck zu akzeptieren. Wenn Sie den Fingerabdruck nicht akzeptieren, können Sie weiterhin den Endpoint speichern, aber die Bereitstellung von Maschinen schlägt möglicherweise fehl.
- **Agent-Fehler**

Der zugeordnete vSphere-Agent wurde nicht gefunden. Der Agent muss für den Test erfolgreich ausgeführt werden.

- **Hostfehler**

Die angegebene Endpoint-Adresse ist nicht erreichbar oder der zugeordnete Manager-Dienst wird nicht ausgeführt. Der Manager-Dienst muss für den Test erfolgreich ausgeführt werden.

- **Anmeldedatenfehler**

Die angegebene Kombination aus Benutzername und Kennwort ist für den Endpoint unter der angegebenen Adresse ungültig.

- **Zeitüberschreitung**

Die Testaktion konnte nicht im zulässigen Zeitraum von zwei Minuten abgeschlossen werden.

Wenn Fehler beim Ausführen einer **Testverbindung** auf aktualisierten oder migrierten Endpoints auftreten, finden Sie die Schritte zum Einrichten einer Zertifikatvertrauensstellung unter [Überlegungen beim Arbeiten mit aktualisierten oder migrierten Endpoints](#).

Programmgesteuertes Importieren oder Exportieren von Endpoints

Um Endpoints in vRealize Automation 7.3 oder höher programmgesteuert zu importieren oder zu exportieren, müssen Sie entweder die neuen endpoint-configuration-service-REST-APIs von vRealize Automation oder vRealize CloudClient verwenden.

Die vRealize CloudClient-Dokumentation enthält alle Informationen zur anwendbaren Formatierung, Beispiele und Informationen zur Verwendung.

Sie können die vRealize CloudClient-Anwendung und die zugehörige Dokumentation von der vRealize CloudClient-Produktseite unter <https://developercenter.vmware.com/tool/cloudclient> herunterladen.

Anzeigen von Endpoint-Quellen und Ausführen der Datenerfassung

Sie können die Maschinen- und Computing-Ressource anzeigen, die einem bestimmten Endpoint zugeordnet sind. Sie können die Datenerfassung auch manuell starten.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **laaS-Administrator** an.
- Stellen Sie sicher, dass Sie mindestens über einen Endpoint verfügen.

Verfahren

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Wählen Sie eine vorhandene Endpoint-Zeile aus und klicken Sie auf **Aktionen**.

Wählen Sie eine der folgenden verfügbaren Aktionen aus.

- Klicken Sie auf **Computing-Ressourcen anzeigen**, um die Seite **Infrastruktur > Computing-Ressource** zu öffnen. Auf dieser Seite können Sie die Einstellungen für die Computing-Ressource anzeigen und bearbeiten.

- Klicken Sie auf **Maschinen anzeigen**, um die Seite **Infrastruktur > Verwaltete Maschinen** zu öffnen.
- Klicken Sie auf **Datenerfassung**, um die Seite „Datenerfassung“ zu öffnen und die Datenerfassung für den Endpoint zu starten. Sie können die Seite aktualisieren, um den aktuellen Status der Anforderung anzuzeigen.

Überlegungen beim Arbeiten mit aktualisierten oder migrierten Endpoints

Nachdem Sie ein Upgrade oder eine Migration von einer Betaversion von vRealize Automation 7.3 durchgeführt haben, sind für ein Verständnis des Vorgangs und entsprechendes Handeln folgende wichtigen Überlegungen zu beachten.

Diese Informationen beziehen sich auf Endpoints, die auf diese Version von vRealize Automation aktualisiert oder migriert wurden.

- Wenn Sie ein Upgrade oder eine Migration von einer Version vor vRealize Automation 7.3 durchführen, werden alle vCloud Air-, vCloud Director- und Amazon-Endpoints, die Proxyeinstellungen enthalten, einem neuen Proxy-Endpoint zugeordnet, der deren Proxyeinstellungen enthält.

Nach dem Upgrade oder der Migration lautet der Name des Proxy-Endpoints Proxy_YYYYY, wobei YYYYY ein Hash der URL, des Ports und der Anmeldedaten des Proxy ist. Wenn Sie dieselben Proxyeinstellungen (zum Beispiel dieselbe URL, denselben Port und dieselben Anmeldedaten) für einen anderen Endpoint (zum Beispiel für einen vCloud Air- oder Amazon-Endpoint) verwendet haben, sind nach dem Upgrade bzw. der Migration nur ein Proxy-Endpoint und eine Zuordnung zwischen dem vCloud Air- und dem Amazon-Endpoint und dem neuen Proxy-Endpoint vorhanden. Ein Proxy-Endpoint kann mehreren Amazon-, vCloud Air- oder vCloud Director-Endpoints zugeordnet werden.

- Wenn Sie vSphere-Endpoints aktualisieren oder migrieren, die NSX Manager-Einstellungen enthalten, werden alle vSphere-Endpoints einem neuen NSX-Endpoint zugeordnet, der dessen NSX Manager-Einstellungen enthält.

Nach dem Upgrade oder der Migration lautet der Name des NSX-Endpoints NSX_XXXXX, wobei XXXXX der Name des übergeordneten vSphere-Endpoints in der vRealize Automation-Version vor 7.3 ist.

- Nach Abschluss eines Upgrades bzw. einer Migration von vRealize Automation kann ein Infrastrukturadministrator die Namen für den neuen NSX- und für den Proxy-Endpoint ändern.
- Die Standardsicherheitseinstellung für aktualisierte oder migrierte Endpoints ist, nicht vertrauenswürdige Zertifikate nicht zu akzeptieren.
- Wenn Sie nicht vertrauenswürdige Zertifikate verwendet haben, müssen Sie nach dem Upgrade oder der Migration von einer früheren vRealize Automation-Installation die folgenden Schritte für alle vSphere- und NSX-Endpoints ausführen, um die Validierung des Zertifikats durchzuführen. Andernfalls schlagen die Endpoint-Vorgänge mit Zertifikatsfehlern fehl. Weitere Informationen finden Sie in den VMware Knowledgebase-Artikeln *Endpoint*

communication is broken after upgrade to vRA 7.3 (2150230) unter <http://kb.vmware.com/kb/2150230> und *How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings (2108294)* unter <http://kb.vmware.com/kb/2108294>.

- a Melden Sie sich nach dem Upgrade bzw. der Migration bei der vRealize AutomationvSphere-Agent-Maschine an und starten Sie Ihre vSphere-Agents mithilfe der Registerkarte **Dienste** neu.

Im Fall einer Migration werden möglicherweise nicht alle Agents neu gestartet. Starten Sie diese bei Bedarf manuell neu.

- b Warten Sie, bis mindestens ein Ping-Bericht abgeschlossen ist. Es dauert eine oder zwei Minuten, bis ein Ping-Bericht abgeschlossen ist.
- c Wenn die vSphere-Agents die Datenerfassung gestartet haben, melden Sie sich bei vRealize Automation als IaaS-Administrator an.
- d Klicken Sie auf **Infrastruktur > Endpoints > Endpoints**.
- e Bearbeiten Sie einen vSphere-Endpoint und klicken Sie auf **Verbindung testen**.
- f Wenn eine Zertifikataufforderung angezeigt wird, klicken Sie auf **OK**, um das Zertifikat zu akzeptieren.

Wenn keine Zertifikataufforderung angezeigt wird, kann es sein, dass das Zertifikat derzeit korrekt in einer vertrauenswürdigen Rootzertifizierungsstelle der Windows-Maschine gespeichert ist, die Dienste für den Endpoint hostet, z. B. als Proxy-Agent-Maschine oder DEM-Maschine.

- g Klicken Sie auf **OK**, um die Zertifikatsannahme anzuwenden und den Endpoint zu speichern.
- h Wiederholen Sie diesen Vorgang für jeden vSphere-Endpoint.
- i Wiederholen Sie diesen Vorgang für jeden NSX-Endpoint.

Wenn die Aktion **Verbindung testen** erfolgreich war, aber einige Datenerfassungs- bzw. Bereitstellungsvorgänge fehlschlagen, können Sie dasselbe Zertifikat auf allen Agent-Maschinen installieren, die den Endpoint bedienen, sowie auf allen DEM-Maschinen. Alternativ dazu können Sie das Zertifikat von vorhandenen Maschinen deinstallieren und den oben genannten Vorgang für den fehlerhaften Endpoint wiederholen.

- Die vRealize Automation-REST-APIs, die verwendet wurden, um in vRealize Automation 7.2 und früheren Versionen Endpoints programmgesteuert zu erstellen, zu bearbeiten und zu löschen, werden in vRealize Automation 7.3 und höher nicht mehr unterstützt. Um Endpoints in vRealize Automation 7.3 oder höher programmgesteuert zu erstellen, zu bearbeiten und zu löschen, müssen Sie entweder die neuen REST-APIs für den vRealize Automation-Endpoint-Konfigurationsdienst oder vRealize CloudClient verwenden.

- Wenn Sie ein Upgrade oder eine Migration von einer früheren vRealize Automation-Installation durchgeführt haben und die Datenerfassung für OpenStack-Endpoints fehlschlägt, können Sie die benutzerdefinierte Eigenschaft `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` zu jedem Keystone V3 OpenStack-Endpoint hinzufügen, um einen gültigen Domänennamen anzugeben und die Datenerfassung zu aktivieren.
- Beim Upgrade eines IPAM-Endpoints eines Drittanbieters, wie zum Beispiel Infoblox-IPAM, wird das vRealize Orchestrator-Paket mit dem `RegisterIPAMEndpoint-Workflow` aktualisiert. Möglicherweise müssen Sie den Workflow in vRealize Orchestrator nach Abschluss des vRealize Automation-Upgrade erneut ausführen.
- Um die Anmeldedaten für mehrere Endpoints zu ändern, können Sie die Endpoints entweder manuell bearbeiten oder mit vRealize CloudClient ein Massenupdate durchführen.
- Bestimmte Endpoint-Typen, wie z. B. vCloud Air und vCloud Director, können nicht direkt von vRealize Automation 6.2.x auf vRealize Automation 7.3 oder höher aktualisiert oder migriert werden.
- Für den Fall, dass nach einem erfolgreichen Upgrade bzw. einer erfolgreichen Migration auf vRealize Automation 7.3 die Seite **Infrastruktur > Endpoints** nicht angezeigt wird oder nur einige der Endpoint-Typen und Endpoints zeigt, finden Sie im [Knowledge Base-Artikel 2150252](#) einen Vorschlag zur Umgehung dieses Problems.

Überlegungen beim Löschen von Endpoints

Sie können bestimmte Endpoint-Typen unter bestimmten Bedingungen löschen.

- Sie können Endpunkte löschen, für die keine Daten erfasst wurden.
- Sie können einen OpenStack-, Amazon- und VRO-Endpoint löschen, wenn Daten für diesen erfasst wurden, wobei er jedoch nicht über Reservierungen verfügt. Andere Endpoint-Typen können nicht gelöscht werden, wenn Daten für sie erfasst wurden.
- Sie können einen IPAM-Endpoint eines Drittanbieters löschen, wenn er keine Zuordnung zu einem Netzwerkprofil hat.
- Beim Löschen eines vSphere-Endpoints werden in der Bestätigungsaufforderung die folgenden Abhängigkeiten aufgelistet:
 - Auf dem Endpoint wurden Daten erfasst.
 - Auf den Endpoint wird in einer Reservierung verwiesen, die einer Computing-Ressource zugeordnet ist. Ein Endpoint, auf den in einer Reservierung verwiesen wird, kann nicht gelöscht werden. Reservierungen erfordern eine Computing-Ressource.
 - Der Endpoint enthält eine Vorlage, auf die in einem vorhandenen Blueprint verwiesen wird.
Der Blueprint wird nicht gelöscht, wenn Sie den Endpoint löschen.
- Der Endpoint wird von virtuellen Maschinen verwendet, die in Gebrauch sind.

- Sie können Endpoints programmgesteuert mit den in vRealize Automation 7.3 eingeführten neuen endpoint-configuration-service-REST-APIs (CREATE, EDIT und DELETE) von vRealize Automation oder mithilfe von vRealize CloudClient löschen. Mithilfe der endpoint-configuration-service-REST-APIs vor vRealize Automation 7.3 können keine Endpoints gelöscht werden.

Fehlerbehebung – Verbundener vSphere-Endpoint kann nicht gefunden werden

Wenn die Datenerfassung für einen vSphere-Endpoint fehlschlägt, kann dies auf die Nichtübereinstimmung des Proxynamens mit dem Endpoint-Namen zurückzuführen sein.

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 der 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**.

Lösung

Der Proxy-Agent kann mit dem Endpoint kommunizieren und die Datenerfassung ist erfolgreich.

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 bei vRealize Automation als **laaS-Administrator** an.
- Erstellen Sie mindestens einen Endpoint. Siehe [Auswählen eines Endpoint-Szenarios](#).

Verfahren

- 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**.

Ergebnisse

Fabric-Administratoren können nun Maschinenpräfixe konfigurieren. Siehe [Konfigurieren von Maschinenpräfixen](#).

Benutzer, die aktuell bei vRealize Automation angemeldet sind, müssen sich abmelden und wieder bei vRealize Automation 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 bei vRealize Automation als **Fabric-Administrator** an.

Verfahren

- 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 an, ob das Maschinenpräfix in allen Mandanten oder nur im aktuellen Mandanten in der Spalte **Sichtbarkeit** angezeigt werden soll.
- 5 Geben Sie in das Textfeld **Anzahl der Ziffern** die Anzahl der laufenden Ziffern ein.
- 6 Geben Sie in das Textfeld **Nächste Nummer** die laufende Startnummer ein.

7 Klicken Sie auf das Symbol **Speichern** (✔).

Ergebnisse

Mandantenadministratoren können Business-Gruppen erstellen, sodass Benutzer für das Anfordern von Maschinen auf vRealize Automation zugreifen können.

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 Profile von bedarfsgesteuerten NAT- und gerouteten Netzwerken, 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 auch IPAM-Drittanbieter, 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 Netzwerkprofil zu definieren.

Hinweis Wenn Sie einen IPAM-Drittanbieter nutzen und angeben möchten, in welchem Netzwerk Ihre Maschine bereitgestellt werden soll, verwenden Sie für jedes VLAN ein separates Netzwerkprofil, um das im [Knowledgebase-Artikel 2148656](#) beschriebene bekannte Problem zu vermeiden.

Wenn Sie statt eines IPAM-Drittanbieters den von vRealize Automation bereitgestellten IPAM-Endpoint verwenden, können Sie die IP-Adressbereiche angeben, die Netzwerkprofile verwenden 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. 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.

Sie können ein Netzwerkprofil einem bestimmten Netzwerkpfad in einer Reservierung zuweisen. Bestimmten Typen von Maschinenkomponenten, wie z. B. vSphere, können Sie ein Netzwerkprofil zuweisen, wenn Sie Blueprints erstellen oder bearbeiten.

Hinweis Obwohl Sie das Netzwerkprofil einer bereitgestellten virtuellen Maschine nicht ändern können, können Sie das Netzwerk ändern, mit dem die virtuelle Maschine verbunden ist. Wenn das Netzwerk einem anderen Netzwerkprofil zugeordnet ist, weist vRealize Automation eine IP-Adresse aus diesem Netzwerkprofil zur virtuellen Maschine zu. Die virtuelle Maschine verwendet jedoch weiterhin die alte IP-Adresse, bis Sie die IP-Adresse auf dem Gastbetriebssystem aktualisieren. Alternativ können Sie die Aktion für die Neukonfiguration auf der bereitgestellten virtuellen Maschine verwenden. Dafür ist auch die Aktualisierung der IP-Adresse auf dem Gastbetriebssystem erforderlich.

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.

Weitere Informationen zu diesen Netzwerktypen finden Sie im *NSX-Administratorhandbuch* im NSX-Informationscenter unter https://www.vmware.com/support/pubs/nsx_pubs.html.

Tabelle 2-14. Verfügbare Netzwerktypen für ein vRealize Automation-Netzwerkprofil

Netzwerktyp	Beschreibung
Extern	<p>Vorhandenes Netzwerk, das auf dem vSphere-Server konfiguriert ist. 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 IP-Bereiche verwenden, die vom bereitgestellten VMware-IPAM-Endpoint oder vom Endpoint eines externen IPAM-Diensteanbieters bezogen werden, den Sie in vRealize Orchestrator registriert und konfiguriert haben, wie z. B. Infoblox IPAM. Ein IP-Bereich wird während der Zuteilung aus einem IP-Block erstellt.</p> <p>Ein externes Netzwerkprofil mit einem statischen IP-Bereich ist die Voraussetzung für NAT- und geroutete Netzwerke.</p> <p>Siehe Erstellen eines externen Netzwerkprofils für ein vorhandenes Netzwerk.</p>
NAT	<p>Bedarfsgesteuertes Netzwerk, das während der Bereitstellung erstellt wurde. NAT-Netzwerke, die einen IP-Adressensatz für die externe Kommunikation und einen anderen IP-Adressensatz für die interne Kommunikation verwenden.</p> <p>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>Sie können IP-Bereiche verwenden, die vom bereitgestellten VMware-IPAM-Endpoint oder vom Endpoint eines externen IPAM-Diensteanbieters bezogen werden, den Sie in vRealize Orchestrator registriert und konfiguriert haben, wie z. B. Infoblox IPAM. Ein IP-Bereich wird während der Zuteilung aus einem IP-Block erstellt.</p> <p>Ein NAT-Netzwerkprofil definiert lokale und externe Netzwerke, die eine Übersetzungstabelle für die wechselseitige Kommunikation verwenden.</p> <p>Siehe Erstellen eines NAT-Netzwerkprofils für ein bedarfsgesteuertes Netzwerk.</p>
Weitergeleitet	<p>Bedarfsgesteuertes Netzwerk, das während der Bereitstellung erstellt wurde. Geroutete Netzwerke enthalten einen routingfähigen IP-Adressbereich, der in Subnetze aufgeteilt ist, die mittels DLR (Distributed Logical Router) miteinander verknüpft sind.</p> <p>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>Sie können IP-Bereiche verwenden, die vom bereitgestellten VMware-IPAM-Endpoint oder vom Endpoint eines externen IPAM-Diensteanbieters bezogen werden, den Sie in vRealize Orchestrator registriert und konfiguriert haben, wie z. B. Infoblox IPAM. Ein IP-Bereich wird während der Zuteilung aus einem IP-Block erstellt.</p> <p>Ein geroutetes Netzwerkprofil definiert einen routingfähigen Bereich und verfügbare Subnetze.</p> <p>Siehe Erstellen eines Profils eines gerouteten Netzwerks für ein bedarfsgesteuertes Netzwerk.</p>

Verwenden von Netzwerkprofilen zum Steuern von IP-Adressbereichen

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.

Sie können optional das bereitgestellte vRealize Automation IPAM oder einen registrierten und konfigurierten Endpoint eines externen IPAM-Dienstanbieters in Ihrem Netzwerkprofil verwenden, um IP-Adressen zu beziehen und zu konfigurieren. Informationen zu Anforderungen für externe IPAM-Anbieter finden Sie unter [Checkliste für die Unterstützung eines externen IPAM-Anbieters](#).

Wenn Sie einen Endpoint eines externen IPAM-Dienstanbieters 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. Die angegebene Bereichssubnetzmaske wird verwendet, um Subnetze aus dem IP-Block zuzuteilen.

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.

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 status nicht den Wert „Zugewiesen“ aufweisen.

CSV-Feld	Beschreibung
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 <code>machine_name</code> nicht leer sein.
NIC_offset	Eine nicht negative ganze Zahl. Optional.

Mit dem folgenden Beispieleintrag wird kein NIC-Versatz festgelegt:

```
100.10.100.1,mymachine01,Allocated
```

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. Alternativ dazu können Sie einem IPAM-Drittanbieter erlauben, die IP-Adressen bereitzustellen.

- Importieren Sie zunächst einen Bereich von IP-Adressen in ein vRealize Automation-Netzwerkprofil.
- Wenden Sie die importierten Werte an, um einen 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 zu prüfen, wie sich die Netzwerkbereichswerte ändern.

Sie können nicht die Option **Aus CSV importieren** für Netzwerkprofile verwenden, die einen IPAM-Endpoint eines Drittanbieters verwenden, weil die IP-Adressen vom IPAM-Drittanbieter und nicht von vRealize Automation verwaltet werden.

Voraussetzungen

- Melden Sie sich bei vRealize Automation 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 IPAM-Drittanbieters](#) und [Grundlegendes zum CSV-Dateiformat für den Import von Netzwerkprofil-IP-Adressen](#).

Verfahren

- 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 **Neu**.

- a Geben Sie einen Namen für den Netzwerkbereich ein.
- b Geben Sie eine Beschreibung für den Netzwerkbereich ein.
- c Geben Sie die IP-Startadresse des Bereichs ein.
- d Geben Sie 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,Allocated
```

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.

CSV-Feld	Beschreibung
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 <code>machine_name</code> nicht leer sein.
NIC_offset	Eine nicht negative ganze Zahl. Optional.

- 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.

Nächste Schritte

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 für ein vorhandenes Netzwerk

Sie können externe Netzwerkprofile erstellen, um die Netzwerkeinstellungen für das Konfigurieren von bestehenden Netzwerken für die Bereitstellung von Maschinen anzugeben, einschließlich der Konfiguration von während der Bereitstellung zu verwendenden NSX-Edge-Geräten.

Sie können den bereitgestellten vRealize Automation-IPAM-Anbieter-Endpoint oder den Endpoint eines IPAM-Drittanbieters, wie z. B. Infoblox, verwenden, den Sie in vRealize Orchestrator registriert haben.

Erstellen eines externen Netzwerkprofils mithilfe des bereitgestellten IPAM-Endpoints

Sie können ein externes Netzwerkprofil erstellen, um Netzwerkeigenschaften und einen Bereich von statischen IP-Adressen zu definieren, die für das Bereitstellen von Maschinen auf einem vorhandenen Netzwerk verwendet werden können.

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.

Weitere Informationen über das Erstellen eines externen Netzwerkprofils und das Verwenden eines externen IPAM-Anbieter-Endpoints finden Sie unter [Erstellen eines externen Netzwerkprofils mithilfe eines IPAM-Drittanbieters](#).

Verfahren

1 [Angaben von Informationen für ein externes Netzwerkprofil unter Verwendung des bereitgestellten IPAM-Endpoints](#)

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 ein externes Netzwerkprofil unter Verwendung des bereitgestellten IPAM-Endpoints](#)

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.

Nächste Schritte

Sie können einem Netzwerkpfad in einer Reservierung ein Netzwerkprofil zuweisen, während ein Blueprint-Architekt das Netzwerkprofil in einem Blueprint angeben kann. Sie können das externe Netzwerkprofil verwenden, wenn Sie ein bedarfsgesteuertes NAT-Profil oder das Profil eines gerouteten Netzwerks erstellen.

Angaben von Informationen für ein externes Netzwerkprofil unter Verwendung des bereitgestellten IPAM-Endpoints

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 für die Unterstützung eines externen IPAM-Anbieters](#) und [Erstellen eines externen Netzwerkprofils mithilfe eines IPAM-Drittanbieters](#). Erstellen Sie anhand des folgenden Verfahrens ein Netzwerkprofil mithilfe des VMware-internen IPAM-Endpoints.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Fabric-Administrator** an.

Verfahren

- 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 Übernehmen Sie den standardmäßigen **IPAM-Endpoint** für den bereitgestellten **vRealize Automation IPAM-Endpoint**.
- 5 Geben Sie eine IP-Subnetzmaske in das Textfeld **Subnetzmaske** ein.
 Die Subnetzmaske gibt die Größe des ganzen routingfähigen Adressbereichs an, den Sie für Ihr Netzwerkprofil definieren möchten.
 Beispielsweise 255.255.0.0.
- 6 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.
 Die im Netzwerkprofil festgelegte Gateway-IP-Adresse wird während der Zuteilung der Netzwerkkarte (NIC) zugewiesen. Wenn im Textfeld **Gateway** im Netzwerkprofil kein Wert zugewiesen wird, müssen Sie beim Bereitstellen der Edge-Maschine die benutzerdefinierte Eigenschaft `VirtualMachine.Network0.Gateway` verwenden.
- 7 Klicken Sie auf die Registerkarte **DNS**.
- 8 Geben Sie bei Bedarf DNS- und WINS-Werte ein.
 Für die Registrierung und Auflösung von DNS-Namen werden DNS-Werte verwendet. 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 IPAM-Drittanbieter 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 die **DNS-Suffixe** ein.
 - d (Optional) Geben Sie einen Wert für die **DNS-Suchsuffixe** ein.
 - e (Optional) Geben Sie einen Wert für **Bevorzugter WINS** ein.
 - f (Optional) Geben Sie einen Wert für **Alternativer WINS** ein.

Nächste Schritte

Sie können IP-Bereiche für statische IP-Adressen konfigurieren. Siehe [Konfigurieren von IP-Bereichen für ein externes Netzwerkprofil unter Verwendung des bereitgestellten IPAM-Endpoints](#).

Konfigurieren von IP-Bereichen für ein externes Netzwerkprofil unter Verwendung des bereitgestellten IPAM-Endpoints

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 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. Sie können manuell definierte IP-Bereiche und über CSV importierte IP-Adressen kombinieren. Beispielsweise können Sie einige Bereiche über die Benutzeroberfläche und andere über den Import aus einer CSV-Datei definieren.

Wenn Sie aus einer CSV-Datei ein zweites Mal importieren, unabhängig vom CSV-Dateinamen, werden die vom vorherigen CSV-Dateiimport importierten IP-Bereiche gelöscht und die neuen IP-Bereichsinformationen hinzugefügt. Dadurch wird der vorherige Import überschrieben, wenn Sie ein zweites Mal oder noch öfter importieren. Sie können den Vorgang der Aktualisierung einer CSV-Datei und des erneuten Imports dieser CSV-Datei in das Netzwerkprofil unbegrenzt wiederholen.

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.

Voraussetzungen

[Angaben von Informationen für ein externes Netzwerkprofil unter Verwendung des bereitgestellten IPAM-Endpoints.](#)

Verfahren

- 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 **Neu**.
 - a Geben Sie einen Namen für den Netzwerkbereich ein.
 - b Geben Sie eine Beschreibung für den Netzwerkbereich ein.
 - c Geben Sie die IP-Startadresse des Bereichs ein.
 - d Geben Sie 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,Allocated
```

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. Optional.

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 Statureinstellungen 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.

Ergebnisse

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 IPAM-Drittanbieters

Sie können eine IPAM-Lösung eines Drittanbieters verwenden, die Sie in vRealize Orchestrator importiert, konfiguriert und registriert haben, um von diesem Drittanbieter IP-Adressen abzurufen.

Sie können ein externes Netzwerkprofil erstellen, das den Endpoint eines registrierten IPAM-Lösungsdrittanbieters 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 mithilfe des bereitgestellten IPAM-Endpoints](#).

Verfahren

1 [Angaben von externen Netzwerkprofilinformationen durch Verwendung eines IPAM-Endpoints eines Drittanbieters](#)

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 unter Verwendung eines IPAM-Endpoints von einem Drittanbieter](#)

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.

Nächste Schritte

Sie können einem Netzwerkpfad in einer Reservierung ein Netzwerkprofil zuweisen, während ein Blueprint-Architekt das Netzwerkprofil in einem Blueprint angeben kann. Sie können das externe Netzwerkprofil verwenden, wenn Sie ein bedarfsgesteuertes NAT-Profil oder das Profil eines gerouteten Netzwerks erstellen.

Angeben von externen Netzwerkprofilinformationen durch Verwendung eines IPAM-Endpoints eines Drittanbieters

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 für die Unterstützung eines externen IPAM-Anbieters](#).
- [Erstellen eines Endpoints eines IPAM-Drittanbieters](#).
- 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 bei vRealize Automation als **Fabric-Administrator** an.

Verfahren

- 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 oder mehrere IPAM-Anbieter-Endpoints von Drittanbietern konfiguriert haben, wählen Sie im Dropdown-Menü **IPAM-Endpoint** einen IPAM-Endpoint eines Drittanbieters aus.

Wenn Sie den Endpoint eines IPAM-Drittanbieters wählen, den Sie in vRealize Orchestrator registriert haben, werden die IP-Adressen vom angegebenen IPAM-Dienstanbieter bezogen. IP-Spezifikationen wie die Subnetzmaske und DNS/WINS-Optionen sind nicht verfügbar, da ihre Funktionen vom ausgewählten Drittanbieter-IPAM-Endpoint kontrolliert werden.

Nächste Schritte

Nun können Sie Netzwerkbereiche für IP-Adressen definieren, um die Netzwerkprofildefinition abzuschließen.

Konfigurieren von IP-Bereichen für ein externes Netzwerkprofil unter Verwendung eines IPAM-Endpoints von einem Drittanbieter

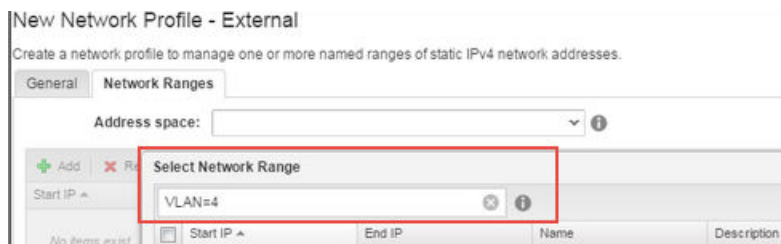
Sie können im Netzwerkprofil mindestens einen Netzwerkbereich mit statischen IP-Adressen für die Bereitstellung einer Maschine konfigurieren. Wenn Sie keinen Bereich angeben, können Sie ein Netzwerkprofil als Netzwerk-Reservierungsrichtlinie zur Auswahl eines Reservierungs-Netzwerkpfads für die Netzwerkkarte einer virtuellen Maschine (vNIC) verwenden.

Sie können die IP-Bereiche definieren, indem Sie die von einem IPAM-Drittanbieter bereitgestellten IP-Adressen verwenden.

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 zu erhalten.

Hinweis Es gibt ein bekanntes Problem bei einigen IPAM-Drittanbietern, bei dem es zu einer Zeitüberschreitung bei einer Abfrage beim Zurückgeben von Netzwerkbereichen kommen kann. Dies führt zu einer leeren Liste. Um dieses Problem zu umgehen, können Sie Suchkriterien angeben, um die Zeitüberschreitung zu vermeiden und die Netzwerkbereichsinformationen zu erhalten.

Sie können beispielsweise je nach IPAM-Anbieter möglicherweise jedem Netzwerk in der IPAM-Anbieter-Anwendung eine Eigenschaft namens VLAN hinzufügen und dieser Eigenschaft einen Wert hinzufügen, z. B. 4. Sie können dann die Eigenschaft und den Wert filtern, z. B. VLAN=4 im Textfeld **Netzwerkbereich auswählen** auf der Seite für das Netzwerkprofil von vRealize Automation.



Als Alternative können Sie die Einstellung für die Zeitüberschreitung mit dem folgenden Verfahren erhöhen:

- 1 Öffnen Sie auf jedem der vRealize Automation-Appliance-Knoten die Datei `/etc/vcac/webapps/o11n-gateway-service/WEB-INF/classes/META-INF/spring/root/o11n-gateway-service-context.xml`.
- 2 Ändern Sie den Wert der Zeitüberschreitung von 30 Sekunden auf eine höhere Zahl.
- 3 Starten Sie den vCAC-Server durch Eingabe von `service vcac-server restart` neu.

Voraussetzungen

[Angaben von externen Netzwerkprofilinformationen durch Verwendung eines IPAM-Endpoints eines Drittanbieters.](#)

Verfahren

- 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.

Bei Verwendung eines IPAM-Drittanbieters kann bei der Auswahl eines Netzwerkbereichs eine leere Liste generiert werden. Einzelheiten dazu finden Sie im Knowledgebase-Artikel 2148656 unter <http://kb.vmware.com/kb/2148656>.

- 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.

Nächste Schritte

Sie können einem Netzwerkpfad in einer Reservierung ein Netzwerkprofil zuweisen, während ein Blueprint-Architekt das Netzwerkprofil in einem Blueprint angeben kann.

Erstellen eines Profils eines gerouteten Netzwerks für ein bedarfsgesteuertes Netzwerk

Sie können ein bedarfsgesteuertes geroutetes Netzwerkprofil erstellen, das den angegebenen vRealize Automation-IPAM-Endpoint oder einen ordnungsgemäß konfigurierten und registrierten Drittanbieter-IPAM-Endpoint verwendet.

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. Jedes geroutete Subnetz kann auf alle anderen von demselben Netzwerkprofil erstellten Subnetze zugreifen.

Bei Verwendung eines IPAM-Drittanbieters wird der routingfähige IP-Bereich vom IPAM-Drittanbieter erstellt und verwaltet. Der Netzwerkadministrator verwendet einen IPAM-Drittanbieter zum Definieren eines routingfähigen IP-Bereichs und zum Erstellen eines entsprechenden IP-Blocks. Sie können mindestens einen über den IPAM-Drittanbieter abgerufenen IP-Block auswählen, wenn Sie ein geroutetes Netzwerkprofil erstellen oder bearbeiten.

Wenn vom IPAM-Drittanbieter eine neue Instanz eines Profils eines gerouteten Netzwerks zuteilt, setzt sich vRealize Automation mit dem Anbieter in Verbindung, um das nächste verfügbare Subnetz zu reservieren und einen Bereich unter Verwendung von IP-Blöcken, die anhand des Profils des gerouteten Netzwerks und der Subnetzgröße bestimmt werden, zu erstellen. Der resultierende Bereich wird verwendet, um Maschinen IP-Adressen zuzuweisen, die dem gerouteten Netzwerk in der gleichen Bereitstellung zugewiesen sind.

Erstellen eines Profils eines gerouteten Netzwerks durch Verwendung des bereitgestellten IPAM-Endpoints

Beim Verwenden eines Profils eines gerouteten Netzwerks mit dem bereitgestellten IPAM-Endpoint können Sie einen routingfähigen IP-Adressbereich und die verfügbaren Subnetze für ein geroutetes bedarfsgesteuertes Netzwerk definieren.

Sie können mithilfe des bereitgestellten vRealize Automation-IPAM-Endpoints einem Profil eines gerouteten Netzwerks statische IP-Adressbereiche sowie eine Basis-IP-Adresse zuweisen.

Sie können IP-Bereiche verwenden, die vom bereitgestellten VMware-IPAM-Endpoint oder vom Endpoint eines externen IPAM-Diensteanbieters bezogen werden, den Sie in vRealize Orchestrator registriert und konfiguriert haben, wie z. B. Infoblox IPAM. Ein IP-Bereich wird während der Zuteilung aus einem IP-Block erstellt.

Verfahren

1 [Angabe der Informationen eines Profils eines gerouteten Netzwerks mit dem vRealize Automation-IPAM-Endpoint](#)

Die Netzwerkprofilinformationen identifizieren die Eigenschaften eines gerouteten Netzwerks, sein zugrunde liegendes externes Netzwerkprofil sowie weitere Werte, die zum Bereitstellen des Netzwerks mithilfe des mitgelieferten IPAM-Endpoints verwendet werden.

2 [Konfigurieren von IP-Bereichen von Profilen eines gerouteten Netzwerks mit dem vRealize Automation-IPAM-Endpoint](#)

Sie können einen oder mehrere statische-IP-Adressbereiche für die Bereitstellung eines Netzwerks konfigurieren.

Angabe der Informationen eines Profils eines gerouteten Netzwerks mit dem vRealize Automation-IPAM-Endpoint

Die Netzwerkprofilinformationen identifizieren die Eigenschaften eines gerouteten Netzwerks, sein zugrunde liegendes externes Netzwerkprofil sowie weitere Werte, die zum Bereitstellen des Netzwerks mithilfe des mitgelieferten IPAM-Endpoints verwendet werden.

Informationen zum Erstellen eines gerouteten Netzwerkprofils mithilfe eines Drittanbieter-IPAM-Endpoints finden Sie unter [Angabe von Informationen für das Profil eines gerouteten Netzwerks mit einem IPAM-Endpoint eines Drittanbieters](#).

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Fabric-Administrator** an.
- Erstellen Sie ein externes Netzwerkprofil. Siehe [Erstellen eines externen Netzwerkprofils mithilfe des bereitgestellten IPAM-Endpoints](#).

Verfahren

- 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 Übernehmen Sie den standardmäßigen **IPAM-Endpoint** für den bereitgestellten **vRealize Automation IPAM-Endpoint**.
- 5 Wählen Sie aus dem Dropdown-Menü **Externes Netzwerkprofil** ein vorhandenes Netzwerkprofil aus.

- 6 Geben Sie die Subnetzmaske in das Textfeld **Subnetzmaske** ein, das dem externen Netzwerkprofil zugeordnet ist.

Die Subnetzmaske gibt die Größe des ganzen routingfähigen Adressbereichs an, den Sie für Ihr Netzwerkprofil definieren möchten.

Beispielsweise 255.255.0.0.

- 7 Wählen Sie aus dem Dropdown-Menü des Textfelds **Bereichssubnetzmaske** einen Wert aus, um festzulegen, wie Bereiche durch die Option **Bereiche generieren** auf der Seite **IP-Bereiche** generiert werden.

Beispielsweise 255.255.255.0.

Die Bereichssubnetzmaske legt fest, wie Sie diesen Adressbereich in einzelne Adressblöcke unterteilen möchten, die jeder Bereitstellungsinstanz dieses Netzwerkprofils zugeteilt werden. Berücksichtigen Sie bei der Auswahl eines Werts für die Bereichssubnetzmaske die Anzahl der Bereitstellungen, für die Sie das geroutete Netzwerk verwenden möchten.

Ein Bereich wird für jede Bereitstellung verwendet, die das Profil eines gerouteten Netzwerks verwendet. Die Anzahl der verfügbaren gerouteten Bereiche ist gleich die Subnetzmaske dividiert durch die Bereichssubnetzmaske, z. B. $255.255.0.0/255.255.255.0 = 256$.

- 8 Geben Sie die erste verfügbare IP-Adresse in das Textfeld **Basis-IP** ein.

Diese Option ist nicht verfügbar, wenn Sie den Endpoint eines Drittanbieters auswählen.

Geben Sie z. B. 120.120.0.1 ein.

- 9 Klicken Sie auf die Registerkarte **DNS**.
- 10 Geben Sie bei Bedarf DNS- und WINS-Werte ein.

Für die Registrierung und Auflösung von DNS-Namen werden DNS-Werte verwendet. 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 IPAM-Drittanbieter 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 die **DNS-Suffixe** ein.

- d (Optional) Geben Sie einen Wert für die **DNS-Suchsuffixe** ein.
- e (Optional) Geben Sie einen Wert für **Bevorzugter WINS** ein.
- f (Optional) Geben Sie einen Wert für **Alternativer WINS** ein.

Nächste Schritte

[Konfigurieren von IP-Bereichen von Profilen eines gerouteten Netzwerks mit dem vRealize Automation-IPAM-Endpoint.](#)

Konfigurieren von IP-Bereichen von Profilen eines gerouteten Netzwerks mit dem vRealize Automation-IPAM-Endpoint

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 der Informationen eines Profils eines gerouteten Netzwerks mit dem vRealize Automation-IPAM-Endpoint.](#)

Verfahren

- 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**.

Erstellen eines Profils eines gerouteten Netzwerks mithilfe eines IPAM-Endpoints eines Drittanbieters

Wenn Sie ein geroutetes Netzwerkprofil mit einem IPAM-Endpoint eines Drittanbieters verwenden, wird ein routingfähiger IP-Bereich erstellt und von einem IPAM-Drittanbieter verwaltet.

Wenn Sie im gerouteten Netzwerkprofil einen IPAM-Endpoint eines Drittanbieters verwenden, erstellt der Anbieter neue IP-Bereiche für jede Instanz des bedarfsgesteuerten Netzwerks.

Sie können IP-Bereiche verwenden, die vom bereitgestellten VMware-IPAM-Endpoint oder vom Endpoint eines externen IPAM-Dienstansbieters bezogen werden, den Sie in vRealize Orchestrator registriert und konfiguriert haben, wie z. B. Infoblox IPAM. Ein IP-Bereich wird während der Zuteilung aus einem IP-Block erstellt.

Verfahren

1 [Angaben von Informationen für das Profil eines gerouteten Netzwerks mit einem IPAM-Endpoint eines Drittanbieters](#)

Die Informationen zum Netzwerkprofil identifizieren die gerouteten Netzwerkeigenschaften, das zugrunde liegende externe Netzwerkprofil und sonstige Werte, die bei der Bereitstellung des Netzwerks mithilfe eines IPAM-Endpoints eines Drittanbieters verwendet werden.

2 [Konfigurieren von IP-Bereichen für das Profil eines gerouteten Netzwerks mit einem IPAM-Endpoint eines Drittanbieters](#)

Sie können einen oder mehrere benannte Bereiche statischer IPv4-Netzwerkadressen für die Bereitstellung eines Netzwerks verwalten.

Angaben von Informationen für das Profil eines gerouteten Netzwerks mit einem IPAM-Endpoint eines Drittanbieters

Die Informationen zum Netzwerkprofil identifizieren die gerouteten Netzwerkeigenschaften, das zugrunde liegende externe Netzwerkprofil und sonstige Werte, die bei der Bereitstellung des Netzwerks mithilfe eines IPAM-Endpoints eines Drittanbieters verwendet werden.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Fabric-Administrator** an.
- Erstellen Sie ein externes Netzwerkprofil. Siehe [Erstellen eines externen Netzwerkprofils mithilfe des bereitgestellten IPAM-Endpoints](#) oder [Erstellen eines externen Netzwerkprofils mithilfe eines IPAM-Drittanbieters](#).
- Erstellen und konfigurieren Sie einen IPAM-Endpoint eines Drittanbieters. Siehe [Erstellen eines Endpoints eines IPAM-Drittanbieters](#).

Verfahren

- 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 Wenn Sie einen oder mehrere IPAM-Anbieter-Endpoints von Drittanbietern konfiguriert haben, wählen Sie im Dropdown-Menü **IPAM-Endpoint** einen IPAM-Endpoint eines Drittanbieters aus.

Wenn Sie den Endpoint eines IPAM-Drittanbieters wählen, den Sie in vRealize Orchestrator registriert haben, werden die IP-Adressen vom angegebenen IPAM-Dienstanbieter bezogen. IP-Spezifikationen wie die Subnetzmaske und DNS/WINS-Optionen sind nicht verfügbar, da ihre Funktionen vom ausgewählten Drittanbieter-IPAM-Endpoint kontrolliert werden.

- 5 Wählen Sie aus dem Dropdown-Menü **Externes Netzwerkprofil** ein vorhandenes Netzwerkprofil aus.

Nur externe Netzwerkprofile, die für die Verwendung des angegebenen IPAM-Endpoints konfiguriert sind, werden aufgelistet und können ausgewählt werden.

- 6 Wählen Sie einen Wert aus dem Dropdown-Menü des Textfelds **Bereichssubnetzmaske** aus, um die Anzahl der für die Bereitstellung zu erstellenden Netzwerksubnetzen anzugeben.

Beispielsweise 255.255.255.0.

Die Bereichssubnetzmaske legt fest, wie Sie diesen Adressbereich in einzelne Adressblöcke unterteilen möchten, die jeder Bereitstellungsinstanz dieses Netzwerkprofils zugeteilt werden. Berücksichtigen Sie bei der Auswahl eines Werts für die Bereichssubnetzmaske die Anzahl der Bereitstellungen, für die Sie das geroutete Netzwerk verwenden möchten.

Ein Bereich wird für jede Bereitstellung verwendet, die das Profil eines gerouteten Netzwerks verwendet. Die Anzahl der verfügbaren gerouteten Bereiche ist gleich die Subnetzmaske dividiert durch die Bereichssubnetzmaske, z. B. $255.255.0.0/255.255.255.0 = 256$.

- 7 Klicken Sie auf die Registerkarte **IP-Blöcke**, um einen Adressbereich zu definieren und eine oder mehrere benannten Bereiche von statischen IPv4-Netzwerkadressen zu verwalten.

Die verfügbaren IP-Blöcke stellen die Quelle für IP-Bereiche dar, die für das bedarfsgesteuerte Routing erstellt oder zugeteilt werden.

Nächste Schritte

[Konfigurieren von IP-Bereichen für das Profil eines gerouteten Netzwerks mit einem IPAM-Endpoint eines Drittanbieters.](#)

Konfigurieren von IP-Bereichen für das Profil eines gerouteten Netzwerks mit einem IPAM-Endpoint eines Drittanbieters

Sie können einen oder mehrere benannte Bereiche statischer IPv4-Netzwerkadressen für die Bereitstellung eines Netzwerks verwalten.

Während der Bereitstellung teilt jedes neue geroutete Netzwerk den nächsten verfügbaren Bereich zu und verwendet diesen zugeteilten Adressbereich als IP-Bereich. Die IP-Blöcke werden vom IPAM-Drittanbieter bezogen. Während der Bereitstellung wird ein geroutetes Netzwerk vom Block mit einer Subnetzmaske zugeteilt, die der Subnetzmaske des angegebenen Bereichs entspricht.

Voraussetzungen

Angeben von Informationen für das Profil eines gerouteten Netzwerks mit einem IPAM-Endpoint eines Drittanbieters.

Verfahren

- 1 Wählen Sie aus dem Dropdown-Menü **Adressbereich** einen Adressbereich aus, um die für die Bereitstellung verfügbaren IP-Blöcke zu begrenzen.

Sobald Sie im Abschnitt unter dem Textfeld „Adressbereich“ einen oder mehrere IP-Blöcke hinzugefügt haben, können Sie keinen **Adressbereich**-Wert mehr auswählen. Das Profil eines gerouteten Netzwerks kann nicht mehr als einen Adressbereich enthalten.

- 2 Fügen Sie einen oder mehrere IP-Blöcke bzw. IPAM-Anbieterbereiche hinzu, indem Sie die anbieterspezifische Suchsyntax verwenden oder eine Auswahl im Dropdown-Menü „Suche“ vornehmen.

Die IP-Blöcke werden vom IPAM-Drittanbieter abgerufen.

Bei Verwendung eines IPAM-Drittanbieters kann bei der Auswahl eines Netzwerkbereichs eine leere Liste generiert werden. Einzelheiten dazu finden Sie im Knowledgebase-Artikel 2148656 unter <http://kb.vmware.com/kb/2148656>.

- a Klicken Sie auf **Hinzufügen**.
- b Klicken Sie auf **Suchen**.
- c Geben Sie die Suchsyntax ein oder wählen Sie einen oder mehrere IP-Blöcke aus dem Dropdown-Menü aus.
- d Klicken Sie auf **OK**.

- 3 Klicken Sie auf **Übernehmen**.

- 4 Klicken Sie auf **OK**.

Erstellen eines NAT-Netzwerkprofils für ein bedarfsgesteuertes Netzwerk

Sie können ein NAT-Netzwerkprofil für ein bedarfsgesteuertes Netzwerk erstellen, das entweder den bereitgestellten vRealize Automation-IPAM-Endpoint oder einen ordnungsgemäß konfigurierten und registrierten IPAM-Endpoint eines Drittanbieters verwendet.

Erstellen eines NAT-Netzwerkprofils unter Verwendung des bereitgestellten IPAM-Endpoints

Sie können ein bedarfsgesteuertes NSXNAT-Netzwerkprofil basierend auf einem externen Netzwerkprofil erstellen. Wenn Sie den bereitgestellten vRealize Automation-IPAM-Endpoint verwenden, können Sie dem NAT-Netzwerkprofil Bereiche mit statischen IP- und DHCP-Adressen zuweisen.

NAT-Netzwerke verwenden eine IP-Adressengruppe für die externe Kommunikation und eine andere IP-Adressengruppe für die interne Kommunikation. Externe IP-Adressen werden von einem externen Netzwerkprofil zugeteilt und interne NAT-IP-Adressen durch ein NAT-Netzwerkprofil definiert. Wenn Sie ein neues NAT-Netzwerk bereitstellen, wird eine neue Instanz des NAT-Netzwerkprofils erstellt und für das Zuteilen von Maschinen-IP-Adressen verwendet.

Sie können IP-Bereiche verwenden, die vom bereitgestellten VMware-IPAM-Endpoint oder vom Endpoint eines externen IPAM-Dienstansbieters bezogen werden, den Sie in vRealize Orchestrator registriert und konfiguriert haben, wie z. B. Infoblox IPAM. Ein IP-Bereich wird während der Zuteilung aus einem IP-Block erstellt.

Für ein NAT-Netzwerk vom Typ 1:n können Sie NAT-Regeln definieren, die konfiguriert werden können, wenn Sie eine NAT-Netzwerkkomponente dem Blueprint hinzufügen, und die geändert werden können, wenn Sie das NAT-Netzwerk in einer Bereitstellung bearbeiten.

Verfahren

1 [Angabe der Informationen eines NAT-Netzwerkprofils mit dem vRealize Automation-IPAM-Endpoint](#)

Das Netzwerkprofil identifiziert die Eigenschaften eines NAT-Netzwerks, sein zugrunde liegendes externes Netzwerkprofil, den NAT-Typ sowie weitere Werte, die zum Bereitstellen des Netzwerks mithilfe des eingebetteten vRealize Automation-IPAM verwendet werden.

2 [Konfigurieren von IP-Bereichen für das NAT-Netzwerkprofil mit dem vRealize Automation-IPAM-Endpoint](#)

Sie können einen oder mehrere statische-IP-Adressbereiche für die Bereitstellung eines Netzwerks konfigurieren.

Angabe der Informationen eines NAT-Netzwerkprofils mit dem vRealize Automation-IPAM-Endpoint

Das Netzwerkprofil identifiziert die Eigenschaften eines NAT-Netzwerks, sein zugrunde liegendes externes Netzwerkprofil, den NAT-Typ sowie weitere Werte, die zum Bereitstellen des Netzwerks mithilfe des eingebetteten vRealize Automation-IPAM verwendet werden.

Informationen zum Erstellen eines NAT-Netzwerkprofils, das einen IPAM-Endpoint eines Drittanbieters verwendet, finden Sie unter [Angabe von Informationen für das Profil eines NAT-Netzwerks mit einem IPAM-Endpoint eines Drittanbieters](#).

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Fabric-Administrator** an.
- Erstellen Sie ein externes Netzwerkprofil. Siehe [Erstellen eines externen Netzwerkprofils mithilfe des bereitgestellten IPAM-Endpoints](#).

Verfahren

- 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 bereitgestellten **vRealize Automation IPAM-Endpoint**.

- 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
Eins-zu-Eins	<p>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.</p> <p>Alle externen IP-Adressen, die einem NSX Edge-Uplink zugewiesen werden, muss Teil des im selben Subnetz befinden. Wenn NAT 1:1 in vRealize Automation verwendet wird, darf das entsprechende externe Netzwerkprofil nur IP-Bereiche enthalten, die in einem einzelnen Subnetz vorhanden sind.</p>
Eins-zu-Viele	<p>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 Aktiviert in der DHCP-Gruppe aktiviert.</p> <p>Der NAT-Übersetzungstyp 1:n ermöglicht Ihnen die Definition der NAT-Regeln, wenn Sie eine NAT-Netzwerkkomponente einem Blueprint hinzufügen.</p>

- 7 Geben Sie eine IP-Subnetzmaske in das Textfeld **Subnetzmaske** ein.

Die Subnetzmaske gibt die Größe des ganzen routingfähigen Adressbereichs an, den Sie für Ihr Netzwerkprofil definieren möchten.
 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.

Die im Netzwerkprofil festgelegte Gateway-IP-Adresse wird während der Zuteilung der Netzwerkkarte (NIC) zugewiesen. Wenn im Textfeld **Gateway** im Netzwerkprofil kein Wert zugewiesen wird, müssen Sie beim Bereitstellen der Edge-Maschine die benutzerdefinierte Eigenschaft `VirtualMachine.Network0.Gateway` verwenden.
- 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 DHCP-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.

Für die Registrierung und Auflösung von DNS-Namen werden DNS-Werte verwendet. 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 IPAM-Drittanbieter 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 die **DNS-Suffixe** ein.
- d (Optional) Geben Sie einen Wert für die **DNS-Suchsuffixe** ein.
- e (Optional) Geben Sie einen Wert für **Bevorzugter WINS** ein.
- f (Optional) Geben Sie einen Wert für **Alternativer WINS** ein.

Nächste Schritte

[Konfigurieren von IP-Bereichen für das NAT-Netzwerkprofil mit dem vRealize Automation-IPAM-Endpoint.](#)

Konfigurieren von IP-Bereichen für das NAT-Netzwerkprofil mit dem vRealize Automation-IPAM-Endpoint

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 der Informationen eines NAT-Netzwerkprofils mit dem vRealize Automation-IPAM-Endpoint.](#)

Verfahren

- 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 **Neu**.
 - a Geben Sie einen Namen für den Netzwerkbereich ein.
 - b Geben Sie eine Beschreibung für den Netzwerkbereich ein.

- c Geben Sie die IP-Startadresse des Bereichs ein.
- d Geben Sie 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,Allocated
```

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. Optional.

- 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 Statureinstellungen sind „Zuteilt“, „Nicht zuteilt“, „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 „Zuteilt“ geändert wird.

- 7 Klicken Sie auf **OK**.

Erstellen eines NAT-Netzwerkprofils unter Verwendung eines IPAM-Endpoints eines Drittanbieters

Sie können ein bedarfsgesteuertes NSXNAT-Netzwerkprofil basierend auf einem externen Netzwerkprofil erstellen. Wenn Sie ein NSX NAT-Netzwerkprofil mit einem IPAM-Endpoint eines Drittanbieters verwenden, wird ein IP-Bereich erstellt und vom IPAM-Drittanbieter verwaltet.

Wenn Sie einen IPAM-Endpoint eines Drittanbieters in Ihrem NAT-Netzwerkprofil verwenden, erstellt der Anbieter neue IP-Bereiche für jede Instanz des bedarfsgesteuerten Netzwerks. Ein interner Satz von IP-Adressen, die mit einem oder mehreren Bereichen definiert sind, werden am Endpoint des IPAM-Drittanbieters für jede Instanz im NAT-Netzwerk erstellt. Diese IP-Bereiche werden verwendet, um Maschinen IP-Adressen zuzuteilen, die dem NAT-Netzwerk in derselben Bereitstellung zugeordnet sind. Da es keine doppelten IP-Adressen innerhalb eines einzigen Adressbereichs geben darf, erstellt der Anbieter für jede Instanz des NAT-Netzwerks einen neuen Adressbereich. Wenn ein NAT-Netzwerk gelöscht wird, werden seine Bereiche im IPAM-Anbieter-Endpoint und im neuen Adressbereich gelöscht.

Sie können IP-Bereiche verwenden, die vom bereitgestellten VMware-IPAM-Endpoint oder vom Endpoint eines externen IPAM-Dienstanbieters bezogen werden, den Sie in vRealize Orchestrator registriert und konfiguriert haben, wie z. B. Infoblox IPAM. Ein IP-Bereich wird während der Zuteilung aus einem IP-Block erstellt.

Für ein NAT-Netzwerk vom Typ 1:n können Sie NAT-Regeln definieren, die konfiguriert werden können, wenn Sie eine NAT-Netzwerkkomponente dem Blueprint hinzufügen, und die geändert werden können, wenn Sie das NAT-Netzwerk in einer Bereitstellung bearbeiten.

Verfahren

- 1 [Angaben von Informationen für das Profil eines NAT-Netzwerks mit einem IPAM-Endpoint eines Drittanbieters](#)

Die Informationen zum Netzwerkprofil identifizieren die NAT-Netzwerkeigenschaften, das zugrunde liegende externe Netzwerkprofil und sonstige Werte, die bei der Bereitstellung des Netzwerks mithilfe eines IPAM-Endpoints eines Drittanbieters verwendet werden.

- 2 [Konfigurieren von IP-Bereichen für das NAT-Netzwerkprofil mit einem IPAM-Endpoint eines Drittanbieters](#)

Mithilfe von NAT können Sie einen oder mehrere IP-Adressbereiche für die Bereitstellung eines Netzwerks definieren.

Angeben von Informationen für das Profil eines NAT-Netzwerks mit einem IPAM-Endpoint eines Drittanbieters

Die Informationen zum Netzwerkprofil identifizieren die NAT-Netzwerkeigenschaften, das zugrunde liegende externe Netzwerkprofil und sonstige Werte, die bei der Bereitstellung des Netzwerks mithilfe eines IPAM-Endpoints eines Drittanbieters verwendet werden.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Fabric-Administrator** an.
- Erstellen Sie ein externes Netzwerkprofil. Siehe [Erstellen eines externen Netzwerkprofils mithilfe des bereitgestellten IPAM-Endpoints](#) oder [Erstellen eines externen Netzwerkprofils mithilfe eines IPAM-Drittanbieters](#).
- Erstellen und konfigurieren Sie einen IPAM-Endpoint eines Drittanbieters. Siehe [Erstellen eines Endpoints eines IPAM-Drittanbieters](#).

Verfahren

- 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 Wenn Sie einen oder mehrere IPAM-Anbieter-Endpoints von Drittanbietern konfiguriert haben, wählen Sie im Dropdown-Menü **IPAM-Endpoint** einen IPAM-Endpoint eines Drittanbieters aus.

Wenn Sie den Endpoint eines IPAM-Drittanbieters wählen, den Sie in vRealize Orchestrator registriert haben, werden die IP-Adressen vom angegebenen IPAM-Dienstleister bezogen. IP-Spezifikationen wie die Subnetzmaske und DNS/WINS-Optionen sind nicht verfügbar, da ihre Funktionen vom ausgewählten Drittanbieter-IPAM-Endpoint kontrolliert werden.

- 5 Wählen Sie aus dem Dropdown-Menü **Externes Netzwerkprofil** ein vorhandenes Netzwerkprofil aus.

Nur externe Netzwerkprofile, die für die Verwendung des angegebenen IPAM-Endpoints konfiguriert sind, werden aufgelistet und können ausgewählt werden.

- 6 Wählen Sie aus dem Dropdown-Menü **NAT-Typ** einen 1:1- oder 1:n-NAT-Typ (Network Address Translation, Netzwerkadressübersetzung) aus.

Option	Beschreibung
Eins-zu-Eins	<p>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.</p> <p>Alle externen IP-Adressen, die einem NSX Edge-Uplink zugewiesen werden, muss Teil des im selben Subnetz befinden. Wenn NAT 1:1 in vRealize Automation verwendet wird, darf das entsprechende externe Netzwerkprofil nur IP-Bereiche enthalten, die in einem einzelnen Subnetz vorhanden sind.</p>
Eins-zu-Viele	<p>Eine externe IP-Adresse wird von allen Maschinen auf dem Netzwerk gemeinsam genutzt. Eine interne Maschine kann nur statische IP-Adressen verwenden. Jede Maschine kann auf das externe Netzwerk zugreifen, aber es kann vom externen Netzwerk aus auf keine Maschine zugegriffen werden.</p> <p>DHCP wird nicht unterstützt, wenn NAT mit einem Drittanbieter-IPAM-Anbieter verwendet wird.</p> <p>Der NAT-Übersetzungstyp 1:n ermöglicht Ihnen die Definition der NAT-Regeln, wenn Sie eine NAT-Netzwerkkomponente einem Blueprint hinzufügen.</p>

- 7 Geben Sie eine IP-Subnetzmaske in das Textfeld **Subnetzmaske** ein.

Die Subnetzmaske gibt die Größe des ganzen routingfähigen Adressbereichs an, den Sie für Ihr Netzwerkprofil definieren möchten.

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.

Die im Netzwerkprofil festgelegte Gateway-IP-Adresse wird während der Zuteilung der Netzwerkkarte (NIC) zugewiesen. Wenn im Textfeld **Gateway** im Netzwerkprofil kein Wert zugewiesen wird, müssen Sie beim Bereitstellen der Edge-Maschine die benutzerdefinierte Eigenschaft `VirtualMachine.Network0.Gateway` verwenden.

- 9 Klicken Sie auf die Registerkarte **DNS**.

- 10 Geben Sie bei Bedarf DNS- und WINS-Werte ein.

Für die Registrierung und Auflösung von DNS-Namen werden DNS-Werte verwendet. 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 IPAM-Drittanbieter 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 die **DNS-Suffixe** ein.
- d (Optional) Geben Sie einen Wert für die **DNS-Suchsuffixe** ein.

- e (Optional) Geben Sie einen Wert für **Bevorzugter WINS** ein.
- f (Optional) Geben Sie einen Wert für **Alternativer WINS** ein.

Nächste Schritte

[Konfigurieren von IP-Bereichen für das NAT-Netzwerkprofil mit einem IPAM-Endpoint eines Drittanbieters.](#)

Konfigurieren von IP-Bereichen für das NAT-Netzwerkprofil mit einem IPAM-Endpoint eines Drittanbieters

Mithilfe von NAT können Sie einen oder mehrere IP-Adressbereiche für die Bereitstellung eines Netzwerks definieren.

Voraussetzungen

[Angaben von Informationen für das Profil eines NAT-Netzwerks mit einem IPAM-Endpoint eines Drittanbieters.](#)

Verfahren

- 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** und definieren Sie einen Netzwerkbereich.
 - a Geben Sie einen Namen und eine Beschreibung für den Netzwerkbereich ein.
 - b Geben Sie den Anfang und das Ende der IP-Adresse, um diese zu definieren.
 - c 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 Stauseinstellungen 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**.

Freigeben von IP-Adressen durch Löschen bereitgestellter Maschinen

Wenn Sie eine Bereitstellung löschen, werden ihre IP-Adressen gelöscht. Die zugewiesenen IP-Adressen, z. B. die IP-Adressen in einem Netzwerkprofilbereich, werden freigegeben und für die nachfolgende Bereitstellung zur Verfügung gestellt.

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, da der Vorgang zur Rückforderung statischer IP-Adressen alle 30 Minuten ausgeführt wird.

Wenn Sie einen IPAM-Drittanbieter verwenden, löscht vRealize Automation die zugehörigen IP-Adressen mithilfe des vRealize Orchestrator-Workflows im Plug-In bzw. Paket des IPAM-Drittanbieters.

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.

Für eine erfolgreiche Bereitstellung muss die Reservierung über ausreichend verfügbaren Speicher verfügen. Die Speicherverfügbarkeit der Reservierung hängt von Folgendem ab:

- Wie viel Speicher im Datenspeicher/Cluster verfügbar ist
- Wie viel von diesem Speicher für diesen Datenspeicher/Cluster reserviert ist
- Wie viel von diesem Speicher bereits in vRealize Automation zugewiesen ist

Beispiel: Selbst wenn der vCenter Server verfügbaren Speicher für den Datenspeicher/Cluster aufweist, schlägt die Bereitstellung mit einem Fehler des Typs „Keine Reservierung verfügbar für Zuteilung...“ fehl, wenn in der Reservierung nicht genügend Speicher reserviert ist. Der zugewiesene Speicher in einer Reservierung hängt von der Anzahl der VMs (unabhängig von ihrem Zustand) in dieser spezifischen Reservierung ab. Weitere Informationen finden Sie im VMware Knowledgebase-Artikel *Machine XXX: No reservation is available to allocate within the group XXX. Total XX GB of storage was requested (2151030)* unter <http://kb.vmware.com/kb/2151030>.

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 Speicher und Arbeitsspeicher, die mittels einer Reservierung einer bereitgestellten Maschine zugewiesen sind, werden freigegeben, wenn die Maschine, der der Speicher oder Arbeitsspeicher zugewiesen ist, in vRealize Automation mithilfe der Aktion „Löschen“ gelöscht wird. Der Speicher und der Arbeitsspeicher werden 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 EC2
- Azure
- Hyper V (SCVMM)
- Hyper-V Standalone
- KVM (RHEV)
- OpenStack
- XenServer

Sie können Sicherheitseinstellungen für die bereitzustellenden virtuellen Maschinen konfigurieren, indem Sie Informationen in einem Reservierungs-, Blueprint- oder Gast-Agent-Skript angeben.

Wenn die bereitzustellenden Maschinen einen Gast-Agent benötigen, müssen Sie eine Sicherheitsregel, die diese Anforderung enthält, zur Reservierung oder zum Blueprint hinzufügen. Wenn Sie z. B. eine Standardsicherheitsrichtlinie verwenden, die die Kommunikation zwischen allen Maschinen nicht zulässt, und Sie sich auf eine separate Sicherheitsrichtlinie verlassen, die die Kommunikation zwischen bestimmten Maschinen, kann der Gast-Agent während der Anpassungsphase möglicherweise mit vRealize Automation kommunizieren. Um dieses Problem während der Bereitstellung von Maschinen zu vermeiden, verwenden Sie eine Standardsicherheitsrichtlinie, die während der Anpassungsphase die Kommunikation ermöglicht.

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 2-15. Auswählen eines Reservierungsszenarios

Szenario	Prozedur
Erstellen einer vSphere-Reservierung.	Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer
Erstellen einer Reservierung, um für einen vCloud Air-Endpoint Ressourcen zuzuteilen.	Erstellen einer vCloud Air-Reservierung
Erstellen einer Reservierung, um für einen vCloud Director-Endpoint Ressourcen zuzuteilen.	Erstellen einer vCloud Director-Reservierung
Erstellen einer Reservierung, um Ressourcen auf einer Amazon-Ressource zuzuteilen (mit oder ohne Amazon Virtual Private Cloud).	Erstellen einer Amazon EC2-Reservierung
Erstellen einer Reservierung, um Ressourcen auf einer OpenStack-Ressource zuzuteilen.	Erstellen einer OpenStack-Reservierung
Erstellen einer Reservierung, um Ressourcen für Hyper-V zuzuteilen.	Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer
Erstellen einer Reservierung, um Ressourcen für KVM zuzuteilen.	Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer
Erstellen einer Reservierung, um Ressourcen auf einer OpenStack-Ressource zuzuteilen.	Erstellen einer OpenStack-Reservierung
Erstellen einer Reservierung, um Ressourcen für SCVMM zuzuteilen.	Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer
Erstellen einer Reservierung, um Ressourcen für XenServer zuzuteilen.	Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer
Erstellen einer Reservierung, um Ressourcen für Microsoft Azure zuzuteilen.	Erstellen einer Reservierung für Microsoft Azure

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.

Für eine erfolgreiche Bereitstellung muss die Reservierung über ausreichend verfügbaren Speicher verfügen. Die Speicherverfügbarkeit der Reservierung hängt von Folgendem ab:

- Wie viel Speicher im Datenspeicher/Cluster verfügbar ist
- Wie viel von diesem Speicher für diesen Datenspeicher/Cluster reserviert ist
- Wie viel von diesem Speicher bereits in vRealize Automation zugeteilt ist

Beispiel: Selbst wenn der vCenter Server verfügbaren Speicher für den Datenspeicher/Cluster aufweist, schlägt die Bereitstellung mit einem Fehler des Typs „Keine Reservierung verfügbar für Zuteilung...“ fehl, wenn in der Reservierung nicht genügend Speicher reserviert ist. Der zugeteilte Speicher in einer Reservierung hängt von der Anzahl der VMs (unabhängig von ihrem Zustand) in dieser spezifischen Reservierung ab. Weitere Informationen finden Sie im VMware Knowledgebase-Artikel *Machine XXX: No reservation is available to allocate within the group XXX. Total XX GB of storage was requested (2151030)* unter <http://kb.vmware.com/kb/2151030>.

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 Plattfortyp 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 Datacenter, 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.

Erstellen einer Amazon EC2-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 .

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

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.

Verfahren

1 [Angaben 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 [Angaben von Ressourcen- und Netzwerkeinstellungen für Amazon-Reservierungen](#)

Geben Sie Ressourcen- und Netzwerkeinstellungen für die Bereitstellung von Maschinen über die vRealize Automation-Reservierung ein.

3 [Angaben 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.

Angaben 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 bei vRealize Automation 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](#).

Verfahren

- 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 EC2** 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.

Ergebnisse

Verlassen Sie diese Seite nicht. Ihre Reservierung ist noch nicht abgeschlossen.

Angaben von Ressourcen- und Netzwerkeinstellungen für Amazon-Reservierungen

Geben Sie Ressourcen- und Netzwerkeinstellungen für die Bereitstellung von Maschinen über die vRealize Automation-Reservierung ein.

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. 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 (VPN) für ein Amazon VPN einrichten. Weitere Informationen zur Erstellung und Verwendung von Sicherheitsgruppen in Amazon Web Services finden Sie in der Dokumentation zu Amazon.

Weitere Informationen zu Lastausgleichsdiensten finden Sie unter *Konfigurieren von vRealize Automation*.

Voraussetzungen

[Angeben von Informationen zu Amazon-Reservierungen.](#)

Verfahren

- 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
Nicht angegeben	Das Verhalten von Schlüsselpaaren wird auf der Blueprint-Ebene anstatt auf der Reservierungsebene gesteuert.
Automatisch generiert pro Business-Gruppe	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.
Automatisch generiert pro Maschine	Jede Maschine weist ein eindeutiges Schlüsselpaar auf. Dies stellt die sicherste Methode dar, da keine Schlüsselpaare von Maschinen gemeinsam genutzt werden.
Bestimmtes Schlüsselpaar	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.

Geben Sie für eine VPC-Reservierung die Sicherheitsgruppen und Subnetze für jede VPC an, die bei der Reservierung zulässig ist.

- 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. Jede verfügbare Region erfordert mindestens eine angegebene Sicherheitsgruppe.
- 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.

Ergebnisse

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

[Angaben von Ressourcen- und Netzwerkeinstellungen für Amazon-Reservierungen.](#)

Verfahren

- 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 die Namen der AD-Benutzer oder -Gruppen (keine E-Mail-Adressen) ein, um Benachrichtigungen im Textfeld **Empfänger** zu erhalten.

Geben Sie jeweils einen Namen pro Zeile ein. 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.

Die E-Mail-Warnungen werden an die in der Liste der Business-Gruppe **Manager E-Mails senden an** enthaltenen Benutzer gesendet.
- 12 Legen Sie eine Erinnerungshäufigkeit (in Tagen) fest.
- 13 Klicken Sie auf **Speichern**.

Ergebnisse

Die Reservierung wird gespeichert und in der Liste „Reservierungen“ angezeigt.

Nächste Schritte

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.

Verfahren

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.

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.

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 bei vRealize Automation 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.

Verfahren

- 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.

Ergebnisse

Verlassen Sie diese Seite nicht. Ihre Reservierung ist noch nicht abgeschlossen.
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.

Voraussetzungen

Angeben von Informationen zu OpenStack-Reservierungen.

Verfahren

- 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
Nicht angegeben	Das Verhalten von Schlüsselpaaren wird auf der Blueprint-Ebene anstatt auf der Reservierungsebene gesteuert.
Automatisch generiert pro Business-Gruppe	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.
Automatisch generiert pro Maschine	Jede Maschine weist ein eindeutiges Schlüsselpaar auf. Dies stellt die sicherste Methode dar, da keine Schlüsselpaare von Maschinen gemeinsam genutzt werden.
Bestimmtes Schlüsselpaar	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 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.

Ergebnisse

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.](#)

Verfahren

- 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 die Namen der AD-Benutzer oder -Gruppen (keine E-Mail-Adressen) ein, um Benachrichtigungen im Textfeld **Empfänger** zu erhalten.

Geben Sie jeweils einen Namen pro Zeile ein. 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.

Die E-Mail-Warnungen werden an die in der Liste der Business-Gruppe **Manager E-Mails senden an** enthaltenen Benutzer gesendet.
- 12 Legen Sie eine Erinnerungshäufigkeit (in Tagen) fest.
- 13 Klicken Sie auf **Speichern**.

Ergebnisse

Die Reservierung wird gespeichert und in der Liste „Reservierungen“ angezeigt.

Nächste Schritte

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.

Verfahren

1 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.

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.

Nächste Schritte

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 bei vRealize Automation 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.

Verfahren

- 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.

Ergebnisse

Verlassen Sie diese Seite nicht. Ihre Reservierung ist noch nicht abgeschlossen.

Angaben 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 Bei für vCloud Air-Endpoints und vCloud Director-Endpoints definierten Reservierungen wird die Verwendung von Netzwerkprofilen für die Bereitstellung von Maschinen nicht unterstützt.

Voraussetzungen

[Angaben von Reservierungsinformationen für vCloud Director.](#)

Verfahren

- 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.

Ergebnisse

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 Vorauszahlungs-Reservierungen, die ohne angegebene Grenzwerte erstellt wurden, sind Warnungen nicht verfügbar.

Voraussetzungen

Angeben von Ressourcen- und Netzwerkeinstellungen für eine vCloud Air-Reservierung

Verfahren

- 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 die Namen der AD-Benutzer oder -Gruppen (keine E-Mail-Adressen) ein, um Benachrichtigungen im Textfeld **Empfänger** zu erhalten.

Geben Sie jeweils einen Namen pro Zeile ein. 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.

Die E-Mail-Warnungen werden an die in der Liste der Business-Gruppe **Manager E-Mails senden an** enthaltenen Benutzer gesendet.
- 14 Legen Sie eine Erinnerungshäufigkeit (in Tagen) fest.
- 15 Klicken Sie auf **Speichern**.

Ergebnisse

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.

Verfahren

1 [Angaben 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 [Angaben 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 [Angaben 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.

Nächste Schritte

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 bei vRealize Automation 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.

Verfahren

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.

Ergebnisse

Verlassen Sie diese Seite nicht. Ihre Reservierung ist noch nicht abgeschlossen.

Angaben 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 Bei für vCloud Air-Endpoints und vCloud Director-Endpoints definierten Reservierungen wird die Verwendung von Netzwerkprofilen für die Bereitstellung von Maschinen nicht unterstützt.

Voraussetzungen

Angeben von Reservierungsinformationen für vCloud Director.

Verfahren

- 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.

Ergebnisse

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.](#)

Verfahren

- 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 die Namen der AD-Benutzer oder -Gruppen (keine E-Mail-Adressen) ein, um Benachrichtigungen im Textfeld **Empfänger** zu erhalten.

Geben Sie jeweils einen Namen pro Zeile ein. 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.

Die E-Mail-Warnungen werden an die in der Liste der Business-Gruppe **Manager E-Mails senden an** enthaltenen Benutzer gesendet.
- 14 Legen Sie eine Erinnerungshäufigkeit (in Tagen) fest.
- 15 Klicken Sie auf **Speichern**.

Ergebnisse

Die Reservierung wird gespeichert und in der Liste „Reservierungen“ angezeigt.

Erstellen einer Reservierung für Microsoft Azure

Erstellen Sie eine Azure-Reservierung für eine bestimmte Business-Gruppe, um Benutzern in dieser Gruppe die Möglichkeit zu bieten, virtuelle Azure-Maschinen in einer angegebenen Computing-Ressource anzufordern.

Wenn Ihre Bereitstellung Single Sign-On über einen VPN-Tunnel unterstützt, können Sie Unterstützung für diese Funktion mit virtuellen Azure-Maschinen mit den Einstellungen auf der Registerkarte „Eigenschaften“ konfigurieren.

Hinweis Ignorieren Sie die Registerkarte „Warnungen“, wenn Sie eine Azure-Reservierung erstellen, da sie in diesem Zusammenhang keine Anwendung findet. Nach dem Erstellen einer Reservierung können Sie die Zuordnungen der Business-Gruppen nicht mehr ändern. Zudem besteht im Gegensatz zu anderen Maschinentypen zwischen einer Azure-Reservierung und einem Blueprint keine direkte Verbindung.

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 bei vRealize Automation als **Fabric-Administrator** an.
- Stellen Sie sicher, dass der Mandantenadministrator mindestens eine Business-Gruppe erstellt hat.
- (Optional) Konfigurieren Sie die Informationen zum Netzwerkprofil.
- Vergewissern Sie sich, dass Sie Zugriff auf alle erforderlichen Azure-Ressourcen haben.
- Stellen Sie sicher, dass erforderliche Schlüsselpaare vorhanden sind. Informationen über Schlüsselpaare finden Sie unter *Konfigurieren von vRealize Automation*.
- Rufen Sie eine gültige Azure-Abonnement-ID ab, die mit der für den jeweiligen Azure-Endpoint verwendeten übereinstimmt. Wenn Sie mehrere Azure-Abonnements verwenden, müssen Sie für jedes Abonnement eine Reservierung erstellen.
- Wenn Ihre Bereitstellung Single Sign-On über einen VPN-Tunnel unterstützt, müssen Sie die entsprechende VPC-Konnektivität konfigurieren, bevor Sie eine Reservierung erstellen. Siehe [Konfigurieren der Netzwerk-zu-Azure-VPC-Konnektivität](#).

Konfigurieren der grundlegenden Reservierungsinformationen für Microsoft Azure
Geben Sie die grundlegenden Informationen für eine Microsoft Azure-Reservierung an.

Alle Informationen auf der Seite „Reservierungsinformationen“ außer der Reservierungsrichtlinie müssen angegeben werden. Die Angabe der Informationen auf den nachfolgenden Azure-Reservierungsseiten ist optional.

Verfahren

- 1 Wählen Sie **Infrastruktur > Verwaltung > Reservierungen**.
- 2 Klicken Sie auf das Symbol **Neu** (+) und wählen Sie den zu erstellenden Reservierungstyp aus.
Wählen Sie **Azure** 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 **Business-Gruppe** eine Business-Gruppe aus.
Nur Benutzer in dieser Business-Gruppe können Maschinen mit dieser Reservierung bereitstellen.
- 6 Ignorieren Sie das Textfeld **Reservierungsrichtlinie**, da es nicht für Azure-Reservierungen gilt.
- 7 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.
- 8 (Optional) Deaktivieren Sie das Kontrollkästchen **Diese Reservierung aktivieren**, wenn Sie nicht möchten, dass diese Reservierung aktiv ist.
- 9 Klicken Sie auf **OK**.

Konfigurieren von Ressourceninformationen für die Azure-Reservierung

Beim Einrichten einer Azure-Reservierung können Sie Informationen zu Ressourcengruppen und Speicherkonten basierend auf der von Ihnen verwendeten Azure-Instanz zuweisen. Wenn Sie eine Reservierung einrichten, versucht die vRealize Automation-Bereitstellungslogik während der Bereitstellung einer virtuellen Maschine Ressourcen gemäß der von der Reservierung angegebenen Ressourceninformationen zuzuteilen, wie zum Beispiel Ressourcengruppen und Speicherkonten.

Sie können Informationen zu Ressourcengruppen und Speicherkonten für eine Azure-VM in der Reservierung konfigurieren, Sie können diese Felder in der Reservierung aber auch leer lassen. Wenn Sie die Felder leer lassen, werden die Ressourcengruppen- und Speicherkonten-Standardinformationen, die sich auf die angegebene Azure-Abonnement-ID beziehen, für alle verbundenen Blueprints verwendet. Sie können diese Informationen auch beim Erstellen eines Blueprints oder während der Bereitstellung einer virtuellen Maschine aktualisieren.

Voraussetzungen

Rufen Sie die Abonnement-ID für Ihre Azure-Instanz ab.

Verfahren

- 1 Geben oder fügen Sie Ihre Azure-Abonnement-ID im Textfeld **Abonnement-ID** ein.

- 2 Wählen Sie den Speicherort für die Reservierung aus, indem Sie auf das Dropdown-Menü **Speicherort** klicken.

Sie können dieses Feld frei lassen oder eine Reservierung mit Erkennung des Speicherplatzes erstellen. Wenn Sie allerdings einen Blueprint erstellen oder eine Azure-VM bereitstellen, müssen Speicherortinformationen eingegeben werden.

- 3 Klicken Sie in der Tabelle „Ressourcengruppe“ auf **Neu**.

- a Fügen Sie im Textfeld **Name** die entsprechenden Informationen zum Ressourcengruppennamen aus Ihrer Azure-Instanz ein.

Hinweis Das Feld **Name** darf nicht leer sein.

- b Weisen Sie im Textfeld **Priorität** einen numerischen Prioritätswert zu.

Diese Zuweisung legt die Priorität fest, wenn eine Reservierung mehr als eine Ressourcengruppe aufweist, wobei niedrigere Zahlen Vorrang haben.

- c Klicken Sie auf **Speichern**, um die Ressourcengruppe zur Reservierung hinzuzufügen.

- 4 Klicken Sie in der Tabelle „Speicherkonten“ auf **Neu**.

- a Fügen Sie im Textfeld **Name** die entsprechenden Informationen zum Speicherkontonamen aus Ihrer Azure-Instanz ein.

Hinweis Das Feld **Name** darf nicht leer sein.

- b Weisen Sie im Textfeld **Priorität** einen numerischen Prioritätswert zu.

- c Klicken Sie auf **Speichern**, um das Speicherkonto zur Reservierung hinzuzufügen.

Diese Zuweisung legt die Priorität fest, wenn eine Reservierung mehr als ein Speicherkonto aufweist, wobei niedrigere Zahlen Vorrang haben.

- 5 Klicken Sie auf **OK**, um mit der nächsten Registerkarte fortzufahren.

Konfigurieren von Azure-Eigenschaften

Sie können benutzerdefinierte Eigenschaften zu einer Azure-Reservierung hinzufügen, um Optionen wie VPN-Tunnel zur Kommunikation zwischen mehreren Netzwerken zu unterstützen. Diese Funktionalität ermöglicht auch das Hinzufügen von Softwarekomponenten zu Blueprints.

Sie müssen benutzerdefinierte Eigenschaften erstellen, die die entsprechenden URLs zur Unterstützung von VPN-Tunneln in Ihrem Netzwerk definieren. Darüber hinaus müssen Sie Eigenschaften erstellen, die den Pfad zu den Azure-Tunnelkonfigurationsskripts definieren, die Sie zuvor heruntergeladen haben.

Verwenden Sie die private IP-Adresse Ihrer physischen Azure-Tunnelmaschine sowie Port 1443, den Sie beim Aufrufen des SSH-Tunnels für *vRealize_automation_appliance_fqdn* zugewiesen haben.

Die folgende Tabelle zeigt die Namen und die Werte für die Eigenschaften, die für die Unterstützung von VPN-Tunneln erforderlich sind.

Name	Wert
Azure.Windows.ScriptPath	Gibt den Pfad zum heruntergeladenen Skript an, mit die Verwendung von Tunneln für Windows-basierte Systeme konfiguriert wird. Aktualisieren Sie den Pfad entsprechend den Anforderungen Ihrer Bereitstellung.
Azure.Linux.ScriptPath	Gibt den Pfad zum heruntergeladenen Skript an, mit dem die Verwendung von Tunneln für Linux-basierte Systeme konfiguriert wird. Aktualisieren Sie den Pfad entsprechend den Anforderungen Ihrer Bereitstellung.
agent.download.url	Gibt die URL für den VPN-Agent in Ihrer Bereitstellung an. Das URL-Format lautet <code>https:// Private_IP:1443/software-service/resources/noble-agent.jar</code>
software.agent.service.url	Geben Sie die Agent-Dienst-URL für die VPN-Software für Ihre Bereitstellung ein. Das URL-Format lautet <code>https:// Private_IP:1443/software-service/api</code>
software.ebs.url	Geben Sie die Ereignis-Broker-Dienst-URL für Ihre Bereitstellung ein. Das URL-Format lautet <code>https:// Private_IP:1443/event-broker-service/api</code>

Voraussetzungen

- Laden Sie die von VMware bereitgestellten Azure-Skripts auf der Seite **Installationsprogramme für Gast- und Software-Agents** auf Ihre vRealize Automation-Appliance herunter.

Diese Skripts installieren Azure-Erweiterungen, die für die Unterstützung von VPN-Tunneln erforderlich sind. Es gibt zwei Skripts: `script.ps1` und `script.sh`. Die Datei `.ps1` ist für Windows-Systeme, die Datei `.sh` für Linux-Systeme vorgesehen.

- Führen Sie `https://vrealize-automation-appliance-fqdn/software` aus, um die VMware vRealize Automation Appliance-Seite zu öffnen.
- Klicken Sie auf den Link **Gast- und Software-Agents** unter der Überschrift „To install vRealize Automation components (IaaS, Guest and Software Agents, Tools)“.
- Laden Sie die Azure Skriptdateien unter der Überschrift „Azure Machines“ herunter. Speichern Sie die Skript-Dateien an einem geeigneten Speicherort. Sie müssen auf diesen Speicherort verweisen, wenn Sie benutzerdefinierte Eigenschaften für Azure-Reservierungen konfigurieren.

Verfahren

- 1 Klicken Sie auf die Registerkarte **Eigenschaften**.
- 2 Klicken Sie auf **Neu**.
- 3 Geben Sie den entsprechenden Namen und Wert für die benutzerdefinierte Eigenschaft im Dialogfeld „Eigenschaften“ ein.

- 4 Klicken Sie nach dem Erstellen jeder Eigenschaft auf **OK**, um die betreffende Eigenschaft hinzuzufügen.
- 5 Wenn Sie alle erforderlichen Eigenschaften hinzugefügt haben, klicken Sie auf **OK**, um Ihre Einstellungen zu speichern.

Nächste Schritte

Nachdem Sie die benutzerdefinierten Eigenschaften zur Unterstützung von VPN-Tunneln erstellt haben, können Sie Softwarekomponenten für Ihre Azure-Blueprints erstellen. Weitere Informationen hierzu finden Sie unter *Konfigurieren von vRealize Automation*.

Wenn Sie eine Softwarekomponente für Azure einrichten möchten, wählen Sie **Virtuelle Azure-Maschine** im Dropdown-Menü „Container“ auf der Seite „Neue Software“ aus.

Konfigurieren von Netzwerkinformationen für die Azure-Reservierung

Sie können Informationen über das virtuelle Netzwerk und den Lastausgleichsdienst für eine Azure-VM in der Reservierung konfigurieren.

Sie können diese Seite auch teilweise oder komplett leer lassen und Informationen über das virtuelle Netzwerk und den Lastausgleichsdienst dann konfigurieren, wenn Sie eine virtuelle Maschine bereitstellen.

Wenn Sie ein Netzwerkprofil angeben, aber kein Subnetz, wird der Name des ersten vorhandenen Netzwerkbereichs des angegebenen Netzwerkprofils als Subnetzname verwendet. Wenn ein Netzwerkprofil angegeben ist, können Sie das vNet-Textfeld auch leer lassen. In diesem Fall wird der Name des ersten Netzwerkbereichs im angegebenen Netzwerkprofil als Subnetzname verwendet und der vNet-Name wird als erstes Azure-vNet aufgelöst, das ein geeignetes Subnetz enthält.

Voraussetzungen

Rufen Sie die entsprechenden Informationen über das virtuelle Netzwerk und den Lastausgleichsdienst aus Ihrer Azure-Instanz (falls zutreffend) ab.

Verfahren

- 1 Klicken Sie in der Tabelle „Netzwerke“ auf **Neu**, um das geeignete virtuelle Azure-Netzwerk zur Verwendung mit Ihrer virtuellen Maschine zu konfigurieren.
 - a Fügen Sie im Textfeld **vNet** die entsprechenden Informationen zum vNet-Namen aus Ihrer Azure-Instanz ein.
 - b Fügen Sie im Textfeld **Subnetz** die entsprechenden Informationen zum Subnetznamen aus Ihrer Azure-Instanz ein.

Die Angabe des Subnetzes ist optional. Wenn Sie dieses Feld leer lassen, wird standardmäßig das Subnetz des angegebenen vNet verwendet.

- c Geben oder fügen Sie im Textfeld **Netzwerkprofil** den passenden Namen ein. Sie können das Netzwerkprofil im Blueprint verwenden, um eine Netzwerkkarte einem Netzwerk zuzuordnen.

Die Angabe des Netzwerkprofils ist optional. Verwenden Sie diese Option, wenn Sie einen Blueprint basierend auf dem in vRealize Automation definierten Netzwerkprofil erstellen möchten und keine Anbindung an Azure-Netzwerkstrukturen wünschen.

- d Weisen Sie im Textfeld **Priorität** einen numerischen Prioritätswert zu (falls anwendbar).

Diese Zuweisung legt die Priorität fest, wenn ein virtuelles Netzwerk mehr als eine Reservierung aufweist, wobei niedrigere Zahlen Vorrang haben.

- e Klicken Sie auf **Speichern**, um die Ressourcengruppe zur Reservierung hinzuzufügen.

- 2 Klicken Sie in der Tabelle „Lastausgleichsdienste“ auf **Neu**, wenn Sie mehrere Maschinen bereitstellen und einen Lastausgleichsdienst verwenden.

- a Fügen Sie im Textfeld **Name** den entsprechenden Namen für den Lastausgleichsdienst aus Ihrer Azure-Instanz ein.

- b Fügen Sie im Textfeld **Back-End-Adressenpool** den entsprechenden Namen aus Ihrer Azure-Instanz ein.

- c Weisen Sie im Textfeld **Priorität** einen numerischen Prioritätswert zu (falls anwendbar).

Diese Zuweisung legt die Priorität fest, wenn ein virtuelles Netzwerk mehr als einen Lastausgleichsdienst aufweist, wobei niedrigere Zahlen Vorrang haben.

- d Klicken Sie auf **Speichern**, um den Lastausgleichsdienst zur Reservierung hinzuzufügen.

- 3 Klicken Sie in der Tabelle „Sicherheitsgruppen“ auf **Neu**, wenn Sie mehrere Maschinen bereitstellen möchten, die über eine Firewall kommunizieren müssen.

- a Fügen Sie im Textfeld **Name** den Namen der Sicherheitsgruppe aus Ihrer Azure-Instanz ein.

- b Weisen Sie im Textfeld **Priorität** einen numerischen Prioritätswert zu (falls anwendbar).

Diese Zuweisung legt die Priorität fest, wenn ein virtuelles Netzwerk mehr als eine Sicherheitsgruppe aufweist, wobei niedrigere Zahlen Vorrang haben.

- c Klicken Sie auf **Speichern**, um die Sicherheitsgruppe zur Reservierung hinzuzufügen.

- 4 Klicken Sie auf **OK**.

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 bei vRealize Automation 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 [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.

Verfahren

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.

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.

Verfahren

- 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.

Ergebnisse

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.

Verfahren

- 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.

Ergebnisse

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 Tunneleigenschaften hinzufügen, um die Agents für den Zugriff auf diese Ports zu konfigurieren.

Hinweis Wenn Sie ein PAT- oder NAT-Systemnetzwerk zwischen dem Netzwerk Ihres Unternehmens und dem vRealize Automation-Netzwerk verwenden, können Sie mithilfe dieser Eigenschaften auf Ihre private IP-Adresse und den Port zugreifen.

Verfahren

- 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**.

Ergebnisse

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.

Für eine erfolgreiche Bereitstellung muss die Reservierung über ausreichend verfügbaren Speicher verfügen. Die Speicherverfügbarkeit der Reservierung hängt von Folgendem ab:

- Wie viel Speicher im Datenspeicher/Cluster verfügbar ist
- Wie viel von diesem Speicher für diesen Datenspeicher/Cluster reserviert ist
- Wie viel von diesem Speicher bereits in vRealize Automation zugeteilt ist

Beispiel: Selbst wenn der vCenter Server verfügbaren Speicher für den Datenspeicher/Cluster aufweist, schlägt die Bereitstellung mit einem Fehler des Typs „Keine Reservierung verfügbar für Zuteilung...“ fehl, wenn in der Reservierung nicht genügend Speicher reserviert ist. Der zugeteilte Speicher in einer Reservierung hängt von der Anzahl der VMs (unabhängig von ihrem Zustand) in dieser spezifischen Reservierung ab. Weitere Informationen finden Sie im VMware Knowledgebase-Artikel *Machine XXX: No reservation is available to allocate within the group XXX. Total XX GB of storage was requested (2151030)* unter <http://kb.vmware.com/kb/2151030>.
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 Plattformtyp 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 die Standardeinstellung.

- Wenn der Blueprint oder die Anforderung die benutzerdefinierte Eigenschaft `VirtualMachine.Host.TpmEnabled` angibt, muss auf der Computing-Ressource für die 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 ausreichender 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 NSX konfiguriert haben, können Sie beim Erstellen oder Bearbeiten eines Blueprints Einstellungen für NSX-Transportzonen, Reservierungsrichtlinien für Edge und das geroutete Gateway sowie Anwendungsisolierungen angeben. Diese Einstellungen sind auf der Registerkarte **NSX-Einstellungen** auf den Seiten **Blueprint** und **Blueprint-Eigenschaften** verfügbar.

Die Netzwerk- und Sicherheitskomponenteneinstellungen, die Sie zur Design-Arbeitsfläche hinzufügen, werden von der NSX-Konfiguration abgeleitet. Dafür muss die Datenerfassung für den NSX-Bestand für vSphere-Cluster 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.

Verfahren

1 [Angaben 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 [Angaben 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 bei vRealize Automation 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.

Verfahren

- 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.

Ergebnisse

Verlassen Sie diese Seite nicht. Ihre Reservierung ist noch nicht abgeschlossen.

Angaben 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.

Für eine erfolgreiche Bereitstellung muss die Reservierung über ausreichend verfügbaren Speicher verfügen. Die Speicherverfügbarkeit der Reservierung hängt von Folgendem ab:

- Wie viel Speicher im Datenspeicher/Cluster verfügbar ist
- Wie viel von diesem Speicher für diesen Datenspeicher/Cluster reserviert ist
- Wie viel von diesem Speicher bereits in vRealize Automation zugeteilt ist

Beispiel: Selbst wenn der vCenter Server verfügbaren Speicher für den Datenspeicher/Cluster aufweist, schlägt die Bereitstellung mit einem Fehler des Typs „Keine Reservierung verfügbar für Zuteilung...“ fehl, wenn in der Reservierung nicht genügend Speicher reserviert ist. Der zugeteilte Speicher in einer Reservierung hängt von der Anzahl der VMs (unabhängig von ihrem Zustand) in dieser spezifischen Reservierung ab. Weitere Informationen finden Sie im VMware Knowledgebase-Artikel *Machine XXX: No reservation is available to allocate within the group XXX. Total XX GB of storage was requested (2151030)* unter <http://kb.vmware.com/kb/2151030>.

Voraussetzungen

Angeben von Informationen zu virtuellen Reservierungen.

Verfahren

- 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.

Sie können entweder einzelne Festplatten im Cluster oder einen Speichercluster wählen, aber nicht beides. Wenn Sie einen Speichercluster wählen, steuert SDRS die Speicherplatzierung und den Lastausgleich für Maschinen, die von dieser Reservierung aus bereitgestellt werden.

- 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.

Ergebnisse

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.](#)

Verfahren

- 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 die Namen der AD-Benutzer oder -Gruppen (keine E-Mail-Adressen) ein, um Benachrichtigungen im Textfeld **Empfänger** zu erhalten.

Geben Sie jeweils einen Namen pro Zeile ein. 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.

Die E-Mail-Warnungen werden an die in der Liste der Business-Gruppe **Manager E-Mails senden an** enthaltenen Benutzer gesendet.
- 13 Legen Sie eine Erinnerungshäufigkeit (in Tagen) fest.
- 14 Klicken Sie auf **Speichern**.

Ergebnisse

Die Reservierung wird gespeichert und in der Liste „Reservierungen“ angezeigt.

Nächste Schritte

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 bei vRealize Automation als **Fabric-Administrator** an.
- Erstellen Sie ein Netzwerkprofil. Siehe [Erstellen eines Netzwerkprofils](#).

Verfahren

- 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 Bei für vCloud Air-Endpoints und vCloud Director-Endpoints definierten 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. Verwandte Informationen zu Bereitstellung und SDRS finden Sie in der benutzerdefinierten Eigenschaft `VirtualMachine.Admin.Datastore.Cluster.ResourceLeaseDurationSec`.

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.

Verfahren

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 bei vRealize Automation als **Fabric-Administrator** an.

Verfahren

- 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.](#)

Verfahren

- 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. Verwandte Informationen zu Bereitstellung und SDRS finden Sie in der benutzerdefinierten Eigenschaft `VirtualMachine.Admin.Datastore.Cluster.ResourceLeaseDurationSec`.

Speicher und Arbeitsspeicher, die mittels einer Reservierung einer bereitgestellten Maschine zugewiesen sind, werden freigegeben, wenn die Maschine, der der Speicher oder Arbeitsspeicher zugewiesen ist, in vRealize Automation mithilfe der Aktion „Löschen“ gelöscht wird. Der Speicher und der Arbeitsspeicher werden nicht freigegeben, wenn die Maschine auf dem vCenter Server gelöscht wird.

Sie können beispielsweise Reservierungen, die Maschinen in einer vorhandenen Bereitstellung zugeordnet sind, nicht löschen. Wenn Sie bereitgestellte Maschinen manuell im vCenter Server verschieben oder löschen, erkennt vRealize Automation die bereitgestellten Maschinen weiterhin als aktiv und verhindert das Löschen von zugeordneten Reservierungen.

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.

Verfahren

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 bei vRealize Automation als **Fabric-Administrator** an.

Verfahren

- 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.](#)

Verfahren

- 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.

Arbeitslastplatzierung

Wenn Sie einen Blueprint bereitstellen, verwendet die Arbeitslastplatzierung erfasste Daten, um eine Empfehlung zu geben, wo der Blueprint basierend auf den verfügbaren Ressourcen bereitgestellt werden soll. vRealize Automation und vRealize Operations Manager arbeiten zusammen, um Platzierungsempfehlungen für die Arbeitslasten bei der Bereitstellung von neuen Blueprints bereitzustellen.

Während vRealize Automation Unternehmensrichtlinien verwaltet, wie z. B. Business-Gruppen, Reservierungen und Kontingente, findet eine Integration der Kapazitätsanalysen von vRealize Operations Manager statt, um die Maschinen zu platzieren. Die Arbeitslastplatzierung ist nur für vSphere-Endpoints verfügbar.

Im Zusammenhang mit der Arbeitslastplatzierung verwendete Begriffe

Mehrere Begriffe werden im Zusammenhang mit der Arbeitslastplatzierung verwendet.

- Cluster in vSphere verweisen auf Computing-Ressourcen in vRealize Automation.
- Reservierungen umfassen Computing-Ressource und Speicher, wobei der Speicher aus einzelnen Datenspeichern oder Datenspeicher-Clustern bestehen kann. Eine Reservierung kann mehrere Datenspeicher oder Datenspeicher-Cluster bzw. beides enthalten.
- Mehrere Reservierungen können auf denselben Cluster verweisen.
- Virtuelle Maschinen können auf mehrere Cluster verschoben werden.
- Wenn die Arbeitslastplatzierung aktiviert ist, verwendet der Bereitstellungsworkflow die Platzierungsrichtlinie, um eine Empfehlung für den Bereitstellungsort des Blueprints zu geben.

Bereitstellen von Blueprints mit Arbeitslastplatzierung

Wenn Sie die Arbeitslastplatzierung zum Bereitstellen von Blueprints verwenden, nutzt der Bereitstellungsworkflow die Reservierungen in vRealize Automation und die Platzierungsoptimierung von vRealize Operations Manager.

- 1 vRealize Automation stellt die Kontrollregeln bereit, um die Platzierung von Zielen zu ermöglichen.
- 2 vRealize Operations Manager gibt Empfehlungen für die Platzierungsoptimierung entsprechend den Analysedaten.
- 3 vRealize Automation setzt den Bereitstellungsprozess gemäß den Platzierungsempfehlungen von vRealize Operations Manager fort.

Wenn vRealize Operations Manager keine Empfehlung geben oder die Empfehlung nicht verwendet werden kann, verwendet vRealize Automation die standardmäßige Platzierungslogik.

Wenn ein Entwickler ein Katalogelement auswählt und das Formular zur Anforderung des Katalogelements ausfüllt, geht vRealize Automation bei der Bereitstellung der virtuellen Maschinen von folgenden Überlegungen aus.

Tabelle 2-16. Überlegungen zum Bereitstellen von virtuellen Maschinen

Überlegung	Auswirkung
Richtlinien	Die vRealize Automation-Reservierungsrichtlinie weist möglicherweise auf mehr als eine Reservierung hin.
Reservierungen	<p>vRealize Automation wertet die Anforderung aus und legt fest, welche Reservierungen die in der Anforderung vorgegebenen Einschränkungen erfüllen können.</p> <ul style="list-style-type: none"> ■ Wenn die Platzierung aktiviert ist und auf vRealize Operations Manager-Analysen basiert, übergibt vRealize Automation die Liste der Reservierungen an vRealize Operations Manager, um anhand der operativen Metriken die am besten geeignete Reservierung zu ermitteln. ■ Basiert die Platzierung nicht auf vRealize Operations Manager, entscheidet vRealize Automation auf Grundlage der Prioritäten und der Verfügbarkeit über die Platzierung. <p>Die Reservierungen werden aktualisiert, um nachzuverfolgen, dass Ressourcen verbraucht wurden.</p> <p>Wenn vRealize Operations Manager einen Cluster oder einen Datenspeicher empfiehlt, den vRealize Automation als ausgelastet oder nicht mehr anwendbar betrachtet, protokolliert vRealize Automation die Ausnahme. vRealize Automation ermöglicht die Bereitstellung, um den Standard-Platzierungsmechanismen gemäß fortzufahren.</p>

Um Ressourcen für eine virtuelle Maschine zu identifizieren, stellt vRealize Automation eine Liste der Kandidatenreservierungen bereit. Jeder Kandidat in der Liste kann einen Cluster und mindestens einen Datenspeicher oder Datenspeicher-Cluster enthalten. vRealize Operations Manager verwendet die Kandidatenreservierungen, um die Liste der Zielkandidaten zu erstellen und das beste Ziel zu suchen.

Die Richtlinie in vRealize Operations Manager legt den Grad des Lastausgleichs, der Nutzung und des Pufferspeichers für den Cluster fest. Für eine einzelne Reservierung, bei der es sich um einen Cluster oder Datenspeicher-Cluster handelt, validiert vRealize Automation, ob die Empfehlung ein geeignetes Platzierungsziel ist.

- Wenn das Ziel geeignet ist, stellt vRealize Automation den Blueprint entsprechend der Empfehlung bereit.
- Wenn das Ziel nicht geeignet ist, verwendet vRealize Automation die Standardmethode für die Platzierung der virtuellen Maschinen.

Bei den Überlegungen zur Platzierung müssen auch Probleme hinsichtlich Zustand und Nutzung berücksichtigt werden. Während der Cloud-Administrator und der Administrator der virtuellen Infrastruktur die Infrastruktur verwalten, kümmern sich Entwickler um den Zustand der Anwendungen. Zur Unterstützung der Entwickler müssen bei der Strategie für die Arbeitslastplatzierung auch Probleme im Hinblick auf Zustand und Nutzung berücksichtigt werden.

Tabelle 2-17. Überlegungen zu Problemen im Hinblick auf Zustand und Nutzung

Arbeitslastproblem	Platzierungslösung
Ein Entwickler stellt ein Zustandsproblem in der Umgebung fest.	vRealize Automation stellt Blueprints in Clustern bereit, die fehlerhaft oder aufgrund von großen Arbeitslasten überlastet sind. vRealize Automation muss die Kapazitätsanalysen in vRealize Operations Manager integrieren, um sicherzustellen, dass Blueprints in Clustern mit ausreichender Kapazität bereitgestellt werden.
Ein Entwickler bemerkt ein Nutzungsproblem.	Die Cluster in der Umgebung sind unzureichend ausgelastet. vRealize Automation muss die von vRealize Operations Manager bereitgestellte Kapazitätsanalyse integrieren, um sicherzustellen, dass Blueprints in einem Cluster mit maximaler Nutzung bereitgestellt werden.

Benutzer, die Blueprints bereitstellen

Die folgenden Benutzer führen Aktionen zum Bereitstellen von Blueprints aus.

Tabelle 2-18. Benutzer und Rollen für die Bereitstellung von Blueprints

Schritt	Benutzer	Aktion	Erforderliche Rolle
1	Cloud-Administrator oder Virtual Infrastructure-Administrator (VI)	Stellt sicher, dass die anfängliche Platzierung von virtuellen Maschinen den Unternehmensrichtlinien entspricht und dass diese gemäß den operativen Analysedaten optimiert sind.	IaaS-Admin-Rolle
1	Fabric-Administrator	Definiert die Reservierungen, die Reservierungsrichtlinien und die Platzierungsrichtlinie in vRealize Automation.	Fabric-Administrator-Rolle, Infrastrukturarchitekt
1	IaaS-Administrator	Definiert die Endpoints für vSphere und vRealize Operations Manager, die für die Platzierung der Arbeitslast erforderlich sind.	IaaS-Admin-Rolle
2	Infrastrukturarchitekt	Blueprint-Architekt, der direkt mit den Komponententypen der virtuellen Maschine arbeitet. Weist die Reservierungsrichtlinien für virtuelle Maschinen bei der Erstellung eines Blueprints zu. Gibt die Reservierungsrichtlinie als Eigenschaft der Maschinenkomponente im Blueprint an.	Infrastrukturarchitekt

Tabelle 2-18. Benutzer und Rollen für die Bereitstellung von Blueprints (Fortsetzung)

Schritt	Benutzer	Aktion	Erforderliche Rolle
3	Infrastrukturarchitekt, Anwendungsarchitekt, Softwarearchitekt und XaaS-Architekt	<p>Erstellt und veröffentlicht den Blueprint zum Bereitstellen der virtuellen Maschinen. Nur der Infrastrukturarchitekt arbeitet direkt mit den Maschinenkomponenten. Die anderen Architekt-Rollen können Infrastruktur-Blueprints bei der Verschachtelung wiederverwenden, jedoch die Einstellungen der Maschinenkomponenten nicht bearbeiten.</p> <p>Der Blueprint kann eine einzelne Komponente oder verschachtelte Blueprints, XaaS-Komponenten, mehrere virtuelle Maschinen in einer Multi-Tier-Anwendung usw. enthalten.</p> <p>vRealize Automation platziert die virtuellen Maschinen entsprechend der Konfiguration der Reservierungen und umfasst optional die Reservierungsrichtlinie auf der Ebene der Maschinenkomponente für den Blueprint. Beispielsweise kann Ihr Blueprint zwei Maschinen umfassen, wobei jeder Maschine eine andere Richtlinie zugewiesen wurde.</p> <p>vRealize Automation optimiert die virtuellen Maschinen zudem gemäß den von vRealize Operations Manager bereitgestellten operativen Analysedaten.</p>	Infrastrukturarchitekt
4	Cloud-Administrator oder VI-Administrator	<p>Wählt die Richtlinien für die anfängliche Platzierung der von vRealize Automation bereitgestellten virtuellen Maschinen aus.</p> <p>Der Administrator kann folgende Aktionen durchführen:</p> <ul style="list-style-type: none"> ■ Auswählen der Richtlinien mit einer API ■ Verwenden der Standardplatzierungsrichtlinie, die zur Verteilung der Arbeitslasten jeden Server in vRealize Automation einzeln nacheinander verwendet. Bei dieser Methode ist keine Eingabe von vRealize Operations Manager erforderlich. 	IaaS-Admin-Rolle, Infrastrukturarchitekt
5	VI-Administrator	Erstellt das benutzerdefinierte Datacenter und die benutzerdefinierten Gruppen in vRealize Operations Manager. Anschließend wendet der VI-Administrator die Richtlinie an, um die Arbeitslasten zu konsolidieren und gleichmäßig auf diese benutzerdefinierten Datacenter zu verteilen.	IaaS-Admin-Rolle, Infrastrukturarchitekt
6	Fabric-Administrator	<p>Wählt die Platzierungsrichtlinie in vRealize Automation aus.</p> <p>Verwenden der Richtlinie zur Arbeitslastplatzierung, damit vRealize Automation festlegen kann, wo die Maschinen beim Bereitstellen von neuen Blueprints platziert werden sollen. Die Platzierungsrichtlinie erfordert eine Benutzereingabe in vRealize Operations Manager.</p>	Fabric-Administratorrolle

Tabelle 2-18. Benutzer und Rollen für die Bereitstellung von Blueprints (Fortsetzung)

Schritt	Benutzer	Aktion	Erforderliche Rolle
7	Entwickler	Fordert einen Blueprint zur Bereitstellung von virtuellen Maschinen an. Der Blueprint kann zum Ausführen einer Three-Tier-Anwendung aus mehreren Maschinen bestehen.	
8	Entwickler	Wenn der Entwickler den Blueprint bereitstellt, sucht vRealize Operations Manager für die Anforderung eine Platzierungsrichtlinie, die den jeweiligen Clustern entspricht.	

Weitere Informationen zur Platzierungsrichtlinie finden Sie unter [Platzierungsrichtlinie](#).

Informationen zum Konfigurieren der Arbeitslastplatzierung finden Sie unter [Konfigurieren der Platzierung der Arbeitslast](#).

Distributed Resource Scheduler (DRS) ist zum Platzieren von virtuellen Maschinen erforderlich

vSphere DRS ist das Platzierungsmodul, das vRealize Automation und vRealize Operations Manager zum Bereitstellen und Platzieren virtueller Maschinen verwenden.

Damit vRealize Automation die beste Platzierung für die virtuellen Maschinen vorschlägt, müssen Sie DRS auf dem Cluster aktivieren und als vollständig automatisiert festlegen. vRealize Automation verwendet dann vSphere DRS-APIs, um die richtige Platzierung für die virtuellen Maschinen zu bestimmen.

vRealize Automation ist im vRealize Operations Manager-Platzierungsdienst integriert. vRealize Operations Manager bietet nur Empfehlungen zur Platzierung für Cluster, für die DRS aktiviert ist und die voll automatisiert sind.

Auswirkung der vRealize Automation-Speicherreservierungsrichtlinien

Das Vorhandensein von vRealize Automation-Speicherreservierungsrichtlinien wirkt sich auf die Arbeitslastverteilung mit vRealize Operations Manager aus.

Wenn die Arbeitslastverteilung mit vRealize Operations Manager aktiviert ist, übergibt vRealize Automation eine Liste der verfügbaren Reservierungen an vRealize Operations Manager, und vRealize Operations Manager wertet diese bezüglich der Speicherplatzierung basierend auf der Betriebsanalyse aus.

Wenn ein Blueprint Speicherreservierungsrichtlinien enthält, ändern sich Empfehlungen zur Workload-Verteilung von vRealize Operations Manager auf folgende Arten.

Hinweis Die Arbeitslastverteilung mit vRealize Operations Manager unterstützt nur virtuelle Maschinen mit einer oder mehreren Festplatten, wo nur eine Speicherreservierungsrichtlinie vorhanden ist. Kombinationen aus mehreren Richtlinien werden für die Festplattenplatzierung nicht unterstützt, da die Platzierung einzelner Festplatten nicht unterstützt wird.

- Virtuelle Maschinen mit einer oder mehreren Festplatten, von denen keine eine Speicherreservierungsrichtlinie angibt:

Die Platzierung erfolgt wie gewohnt. vRealize Operations Manager wertet die vollständige, ungefilterte Liste der Kandidatenreservierungen aus.

- Virtuelle Maschinen mit einer oder mehreren Festplatten, von denen alle dieselbe Speicherreservierungsrichtlinie angeben:

Kandidatenreservierungen werden auf Speicherebene gefiltert, damit vRealize Operations Manager nur Datenspeicher auswertet, die mit dieser Speicherreservierungsrichtlinie übereinstimmen.

- Virtuelle Maschinen mit mehreren Festplatten, von denen einige dieselbe Speicherrichtlinie, aber andere keine Speicherreservierungsrichtlinie angeben:
 - Wenn der Speicherzuteilungstyp „ERFASST“ lautet (Standard), werden alle Festplatten so behandelt, als ob sie dieselbe Richtlinie verwenden würden. vRealize Operations Manager wertet Datenspeicher aus, die mit dieser Speicherreservierungsrichtlinie übereinstimmen.
 - Wenn der Speicherzuteilungstyp „VERTEILT“ lautet, können virtuelle Maschinen nicht entsprechend vRealize Operations Manager-Empfehlungen platziert werden, da die Platzierung einzelner Festplatten nicht unterstützt wird. Die Platzierung erfolgt stattdessen standardmäßig mit vRealize Automation-Platzierungsalgorithmen.

Sie können den Speicherzuteilungstyp mit einer benutzerdefinierten Eigenschaft festlegen.

- Virtuelle Maschinen mit mehreren Festplatten, die jeweils unterschiedliche Speicherreservierungsrichtlinien angeben:

Da sie in Konflikt stehende Anforderungen zur Speicherreservierung aufweisen, können diese virtuellen Maschinen nicht entsprechend vRealize Operations Manager-Empfehlungen platziert werden. Die Platzierung erfolgt stattdessen standardmäßig mit vRealize Automation-Platzierungsalgorithmen.

- Virtuelle Maschinen, die einen bestimmten Speicherpfad erfordern:

Diese virtuellen Maschinen werden nicht über eine vRealize Operations Manager-Empfehlung platziert, da Sie bereits einen Speicherpfad angegeben haben. Die Platzierung entspricht eventuell den vRealize Operations Manager-Empfehlungen, vielleicht aber auch nicht.

Sie können den Speicherpfad mithilfe einer benutzerdefinierten Eigenschaft festlegen.

Platzierungsfehler: Wenn die vRealize Operations Manager-basierte Platzierung nicht durchgeführt werden kann, wird der Grund in einem Fehler beschrieben. Gründe können die nicht unterstützten Bedingungen in der obigen Liste oder Umgebungsfaktoren wie etwa fehlgeschlagene Kommunikation zwischen vRealize Operations Manager und vRealize Automation umfassen.

Um Fehler zu prüfen, gehen Sie zu **Anforderungen > Ausführung**. Klicken Sie oben rechts auf **Platzierungsfehler anzeigen**.

Einschränkungen bei der Platzierung der Arbeitslast

Wenn Sie bei der Bereitstellung von neuen Blueprints die Platzierungsrichtlinie für die Platzierung der Arbeitslast verwenden, um Maschinen zu platzieren, beachten Sie die Einschränkungen.

- In vRealize Operations Manager identifiziert die vRealize Automation-Lösung die Cluster und virtuelle Maschinen, die von vRealize Automation verwaltet werden.
- Wenn vRealize Automation die untergeordneten Objekte eines Datencenters oder eines benutzerdefinierten Datencenter-Containers in vRealize Operations Manager verwaltet, können diese Objekte nicht neu verteilt oder verschoben werden. Sie können den Ausschluss von Aktionen für verwaltete vRealize Automation-Objekte nicht aktivieren oder deaktivieren.
- Das Verhalten der Platzierung der Arbeitslast für Objekte, die von vRealize Automation verwaltet werden, lautet wie folgt:
 - Wenn ein benutzerdefiniertes Datencenter oder ein Datencenter einen Cluster enthält, der von vRealize Automation verwaltet wird, lässt die Platzierung der Arbeitslast nicht zu, dass der Cluster neu verteilt wird.
 - Wenn ein Cluster virtuelle Maschinen beinhaltet, die von vRealize Automation verwaltet werden, lässt die Platzierung der Arbeitslast nicht zu, dass diese virtuellen Maschinen verschoben werden.
- vRealize Operations Manager unterstützt nicht die Platzierung der Arbeitslast auf Ressourcenpools in vCenter Server.
- vSAN wird von vRealize Operations Manager in der aktuellen Version nicht unterstützt.

Berechtigungen für das Konfigurieren der Arbeitslastplatzierung

Sie benötigen Berechtigungen in vRealize Automation und vRealize Operations Manager, um die Arbeitslastplatzierung und die Platzierungsrichtlinie zu konfigurieren.

In vRealize Automation benötigen Sie die Fabric-Administrator-Rolle für das Konfigurieren der Arbeitslastplatzierung. Weitere Informationen finden Sie in der Übersicht über Benutzerrollen im vRealize Automation-Informationscenter.

In vRealize Operations Manager müssen Sie eine Benutzerrolle für die Arbeitslastplatzierung erstellen und der Rolle die Berechtigungen zuweisen.

- Weisen Sie im Benutzerkonto vSphere-Hosts und -Clustern und vSphere Storage die Nur-Lese-Berechtigung in der Objekthierarchie zu.
- Damit die Benutzerrolle API-Aufrufe in Arbeitslastplatzierungen verwenden kann, weisen Sie Lese- und Schreibberechtigungen für APIs zu. Wählen Sie **Administration > Zugriffssteuerung > Berechtigungen** aus und wählen Sie **REST-APIs > Alle übrigen Lese-, Schreib-APIs** aus.

vRealize Automation verwendet die vRealize Operations Manager-Rolle, wenn Sie den Endpoint registrieren und die Platzierungsempfehlungen während der Bereitstellung im Namen von Benutzern anfordern, die Katalogelemente anfordern.

Weitere Informationen finden Sie im Abschnitt zur Zugriffssteuerung im vRealize Operations Manager-Informationscenter.

Platzierungsrichtlinie

Sie können die Platzierungsrichtlinie verwenden, damit vRealize Automation festlegen kann, wo die Maschinen beim Bereitstellen von neuen Blueprints platziert werden sollen. Die Platzierungsrichtlinie verwendet die Analysen von vRealize Operations Manager, um die Arbeitslasten auf Ihren Clustern zu ermitteln und Platzierungsziele vorzuschlagen.

Sie müssen mehrere Schritte durchführen, bevor Sie die Platzierungsrichtlinie verwenden können. In vRealize Automation erstellen Sie Endpoints für vRealize Operations Manager- und vCenter Server-Instanzen. Anschließend erstellen Sie eine Fabric-Gruppe und fügen Ihrem vCenter Server-Endpoint Reservierungen hinzu.

Um sicherzustellen, dass vRealize Operations Manager Analysen für die Platzierung der Arbeitslast für vRealize Automation bereitstellt, müssen Sie folgende Aktionen durchführen:

- Installieren Sie die vRealize Automation-Lösung in der vRealize Operations Manager-Instanz, die für die Platzierung der Arbeitslast verwendet wird.
- Konfigurieren Sie vRealize Operations Manager, um den vCenter Server zu überwachen.

Informationen zum Konfigurieren von vRealize Automation und vRealize Operations Manager für die Platzierung der Arbeitslast finden Sie unter [Konfigurieren der Platzierung der Arbeitslast](#).

Suchen der Platzierungsrichtlinie

Wählen Sie in Ihrer vRealize Automation-Instanz **Infrastruktur > Reservierungen > Platzierungsrichtlinie** aus.

Um die von vRealize Operations Manager bereitgestellten Analysen für die Platzierung der Arbeitslast zu verwenden, wählen Sie **vRealize Operations Manager für Platzierungsempfehlungen verwenden** aus.

Wenn Sie die Richtlinie zur Platzierung der Arbeitslast nicht verwenden, verwendet vRealize Automation die Standardmethode für die Platzierung.

Konfigurieren der Platzierung der Arbeitslast

Um die Platzierungsrichtlinie zum Platzieren von Maschinen zu verwenden, wenn Sie neue Blueprints bereitstellen, konfigurieren Sie vRealize Automation für die Verwendung der von vRealize Operations Manager bereitgestellten Analysen. Sie können vRealize Operations Manager auch zum Anwenden einer Richtlinie für die Konsolidierung und Verteilung von Arbeitslasten auf Ihren Cluster-Computing-Ressourcen konfigurieren.

In vRealize Automation konfigurieren Sie Endpoints, erstellen eine Fabric-Gruppe und fügen Reservierungen hinzu. In vRealize Operations Manager konfigurieren Sie eine Richtlinie zur Unterstützung der Arbeitslastverteilung und wenden diese Richtlinie auf eine benutzerdefinierte Gruppe an, die Ihre benutzerdefinierten Computing-Ressourcen enthält.

Voraussetzungen

Bevor die Platzierungsrichtlinie Platzierungsziele für Blueprints vorschlagen kann, müssen Sie mehrere Schritte durchführen.

- Machen Sie sich mit der Platzierungsrichtlinie vertraut. Siehe [Platzierungsrichtlinie](#).
- Stellen Sie sicher, dass in vRealize Automation ein Endpoint für die vRealize Operations Manager-Instanz vorhanden ist, die für die Platzierung der Arbeitslast verwendet wird. Siehe [Erstellen eines vRealize Operations Manager-Endpoints](#).
- Stellen Sie sicher, dass ein Endpoint in vRealize Automation für die vCenter Server-Instanz vorhanden ist. Siehe [Erstellen eines vSphere-Endpoints](#).
- Fügen Sie Reservierungen zum vCenter Server-Endpoint hinzu. Siehe [Reservierungen](#).
- Fügen Sie eine Fabric-Gruppe hinzu, und stellen Sie sicher, dass der Benutzer ein Administrator der Fabric-Gruppe ist. Siehe [Erstellen einer Fabric-Gruppe](#).
- Stellen Sie sicher, dass vRealize Operations Manager dieselbe Infrastruktur überwacht, die vRealize Automation überwacht, um sicherzustellen, dass sie die gleichen vCenter Server-Instanzen enthalten. Weitere Informationen finden Sie unter [VMware vSphere-Lösung in vRealize Operations Manager](#) im vRealize Operations Manager-Informationscenter.
- Machen Sie sich mit Reservierungen, Speicherreservierungen, Blueprints und Delegieren von Anbietern vertraut. Weitere Informationen finden Sie im vRealize Automation-Informationscenter.
- Machen Sie sich mit den Füll- und Ausgleichseinstellungen in der vRealize Operations Manager-Richtlinie vertraut, die für die Platzierung der Arbeitslasten verwendet werden, und definieren Sie diese. Weitere Informationen finden Sie unter [Details zur Arbeitslast-Automatisierung](#) im vRealize Operations Manager-Informationscenter.

Verfahren

1 Konfigurieren von vRealize Automation für die Platzierung der Arbeitslast

Um Analysen für die Platzierung der Arbeitslast zum Platzieren von Maschinen zu verwenden, wenn Sie neue Blueprints bereitstellen, müssen Sie die vRealize Automation-Instanz vorbereiten.

2 Konfigurieren von vRealize Operations Manager für die Platzierung der Arbeitslast in vRealize Automation

Um Analysen für die Platzierung von Arbeitslasten auf vRealize Automation bereitzustellen, wenn Sie Maschinen beim Bereitstellen neuer Blueprints platzieren möchten, müssen Sie die vRealize Operations Manager-Instanz vorbereiten.

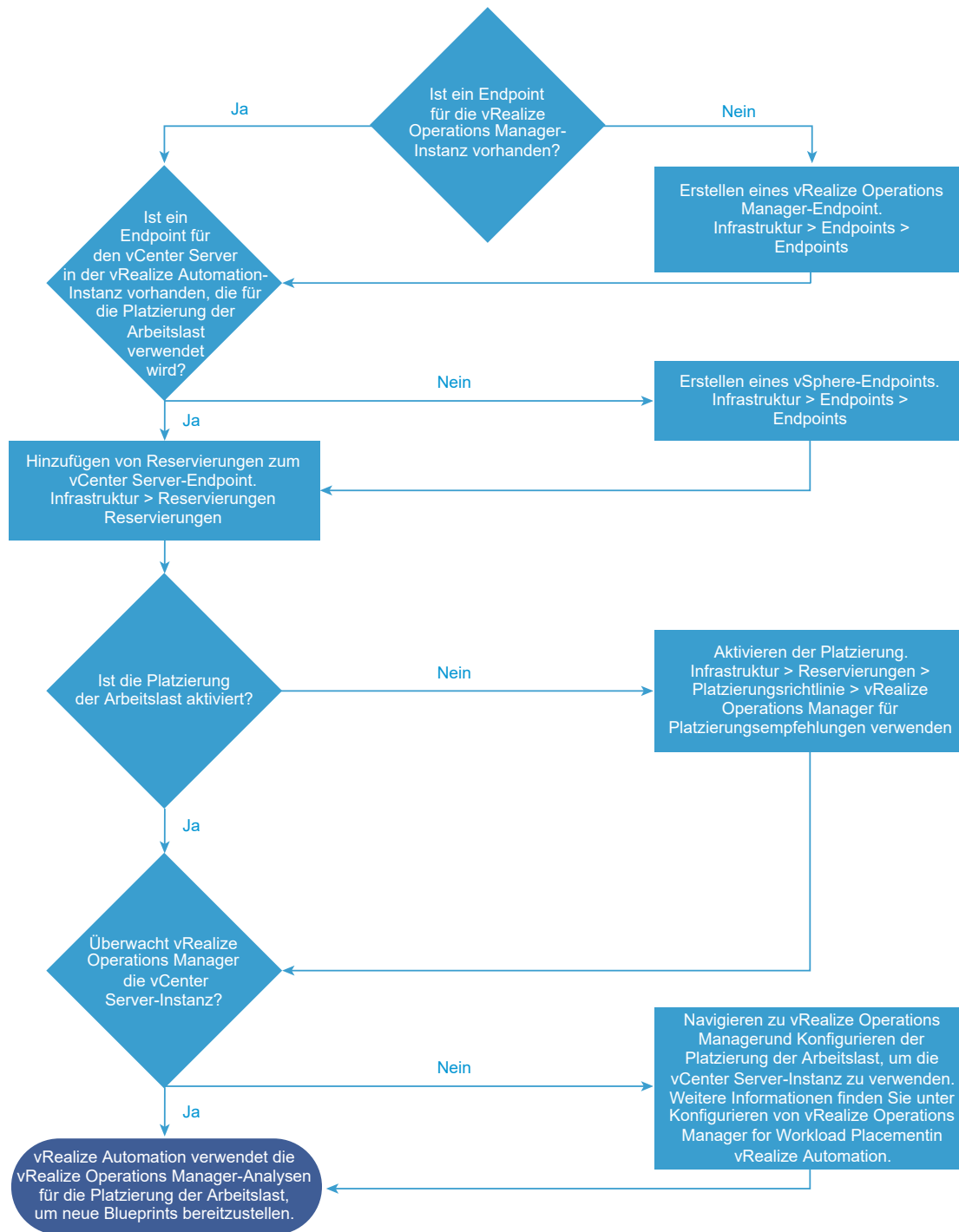
Ergebnisse

Sie haben vRealize Automation und vRealize Operations Manager für die Verwendung der Analysen zum Platzieren von Arbeitslasten konfiguriert, um Platzierungsziele für neue Blueprints vorzuschlagen.

Konfigurieren von vRealize Automation für die Platzierung der Arbeitslast

Um Analysen für die Platzierung der Arbeitslast zum Platzieren von Maschinen zu verwenden, wenn Sie neue Blueprints bereitstellen, müssen Sie die vRealize Automation-Instanz vorbereiten.

Um Ihre vRealize Automation-Instanz auf die Platzierungsrichtlinie vorzubereiten, konfigurieren Sie Endpoints, erstellen eine Fabric-Gruppe und fügen Reservierungen hinzu.



Voraussetzungen

- Um die Platzierung der Arbeitslast verwenden zu können, müssen Sie die Anforderungen verstehen. Siehe [Konfigurieren der Platzierung der Arbeitslast](#).
- Fügen Sie in vRealize Automation eine bestimmte Benutzerrolle und Berechtigungen für vRealize Operations Manager hinzu, um die Anmeldeinformationen zu validieren. Weitere Informationen finden Sie in der Übersicht über Benutzerrollen im vRealize Automation-Informationscenter.

Verfahren

- 1 Fügen Sie in Ihrer vRealize Automation-Instanz einen Endpoint für die vRealize Operations Manager-Instanz hinzu und klicken Sie auf **OK**.
 - a Wählen Sie **Infrastruktur > Endpoint > Endpoints** aus.
 - b Wählen Sie **Neu > Management > vRealize Operations Manager** aus.
 - c Geben Sie die allgemeinen Informationen für den **vRealize Operations Manager**-Endpoint ein.

Sie brauchen keine Eigenschaften für den Endpoint anzugeben.
- 2 Fügen Sie in Ihrer vRealize Automation-Instanz einen Endpoint für die vCenter Server-Instanz hinzu und klicken Sie auf **OK**.
 - a Wählen Sie **Infrastruktur > Endpoint > Endpoints** aus.
 - b Wählen Sie **Neu > Virtuell > vSphere (vCenter)** aus.
 - c Geben Sie die allgemeinen Informationen, Eigenschaften und Zuordnungen für den vCenter Server-Endpoint ein.

Nachdem Sie Endpoints hinzugefügt haben und vRealize Automation Daten daraus erfasst, sind die Computing-Ressourcen für diese Endpoints verfügbar. Sie können diese Computing-Ressourcen dann der Fabric-Gruppe hinzufügen, die Sie erstellen.

- 3 Erstellen Sie eine Fabric-Gruppe, damit andere Benutzer Reservierungen erstellen und die Platzierungsrichtlinie aktivieren können.
 - a Wählen Sie **Infrastruktur > Endpoint > Fabric-Gruppen** aus.
 - b Klicken Sie auf **Neu**, und geben Sie Informationen zu der Fabric-Gruppe ein.

Option	Beschreibung
Name	Geben Sie einen aussagekräftigen Namen für die Fabric-Gruppe ein.
Beschreibung	Geben Sie eine sinnvolle Beschreibung ein.
Fabric-Administratoren	Geben Sie die E-Mail-Adresse für jeden Benutzer ein, der als Fabric-Administrator fungieren soll.
Computing-Ressourcen	Wählen Sie die Computing-Ressourcen-Cluster aus, die die Administratoren verwalten können.

Nachdem Sie Computing-Ressourcen zu einer Fabric-Gruppe hinzugefügt haben und vRealize Automation Daten daraus erfasst, können Fabric-Administratoren Reservierungen für die Computing-Ressourcen erstellen.

- 4 Erstellen Sie Reservierungen für die Computing-Ressourcen in der vCenter Server-Instanz.
 - a Wählen Sie **Infrastruktur > Reservierungen > Reservierungen** aus.
 - b Wählen Sie **Neu > vSphere (vCenter)** aus.
 - c Geben Sie auf jeder Registerkarte die Informationen für die Reservierung ein.

Option	Aktion
Allgemein	Wählen Sie eine Reservierungsrichtlinie und die Priorität für die Richtlinie aus, und klicken Sie auf Diese Reservierung aktivieren .
Ressourcen	Wählen Sie das Maschinenkontingent, den Arbeitsspeicher und den Speicher aus. Sie brauchen keinen Ressourcenpool auszuwählen.
Netzwerk	Wählen Sie den Netzwerkadapter aus. Sie brauchen kein Netzwerkprofil auszuwählen.
Eigenschaften	Fügen Sie bei Bedarf benutzerdefinierte Eigenschaften für die Reservierung hinzu.
Alarm	Wählen Sie bei Bedarf Kapazitätswarnungen aus, um Empfänger zu benachrichtigen, wenn die Kapazität den Schwellenwert für die Reservierung überschreitet.

- 5 Aktivieren Sie die Platzierungsrichtlinie.
 - a Wählen Sie **Infrastruktur > Reservierungen > Platzierungsrichtlinie** aus.
 - b Aktivieren Sie das Kontrollkästchen mit dem Namen **vRealize Operations Manager für Reservierungsempfehlungen verwenden**.

Ergebnisse

Sie haben vRealize Automation für die Verwendung der Analysen von vRealize Operations Manager konfiguriert, um Maschinen zu platzieren, wenn Benutzer Blueprints bereitstellen.

Nächste Schritte

Konfigurieren Sie vRealize Operations Manager zum Überwachen der vCenter Server-Instanz und wenden Sie eine Arbeitslast-Platzierungsrichtlinie auf die Computing-Ressourcen Ihres Clusters an. Siehe [Konfigurieren von vRealize Operations Manager für die Platzierung der Arbeitslast in vRealize Automation](#).

Konfigurieren von vRealize Operations Manager für die Platzierung der Arbeitslast in vRealize Automation

Um Analysen für die Platzierung von Arbeitslasten auf vRealize Automation bereitzustellen, wenn Sie Maschinen beim Bereitstellen neuer Blueprints platzieren möchten, müssen Sie die vRealize Operations Manager-Instanz vorbereiten.

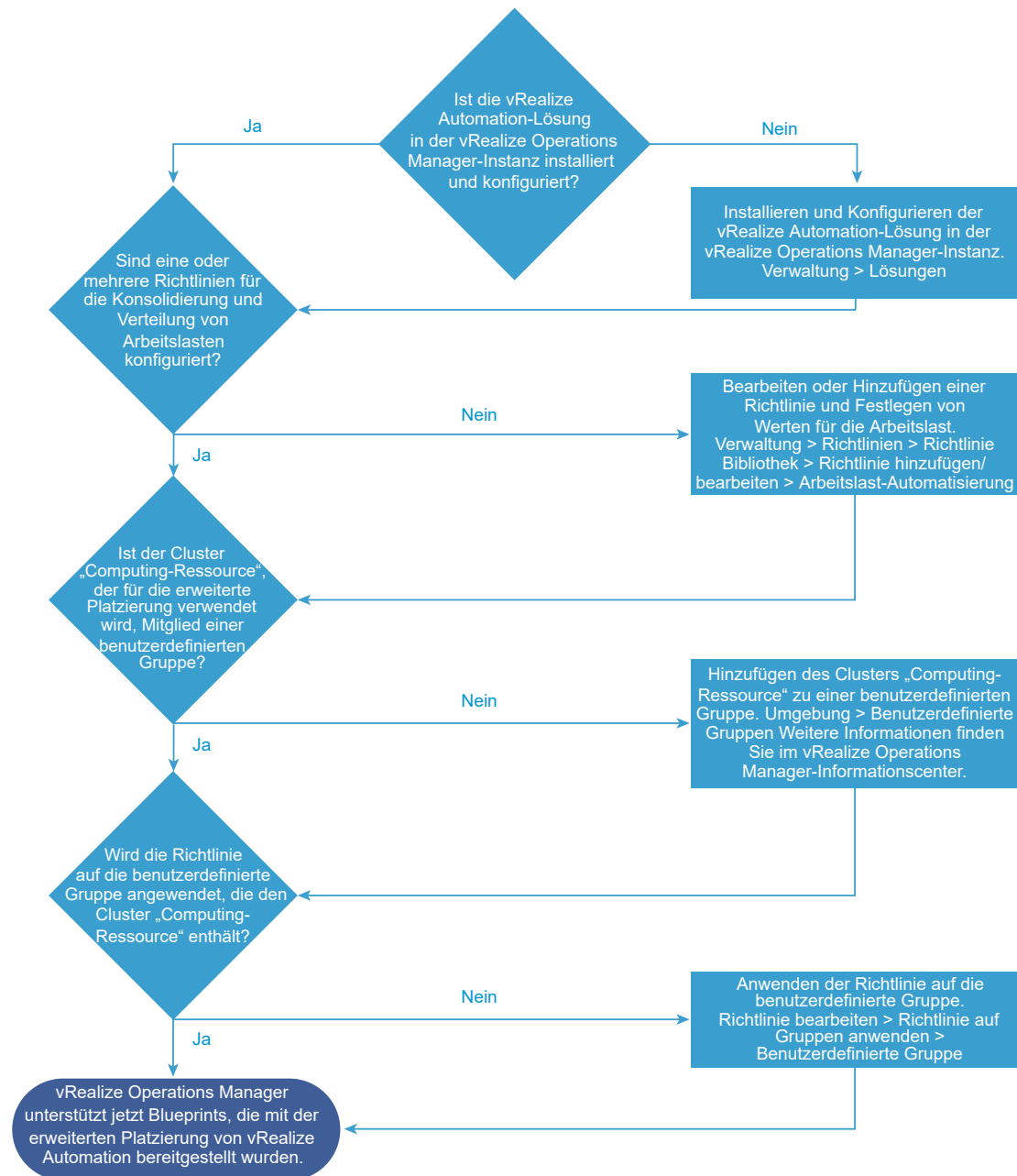
Vorsicht Sie dürfen die vRealize Automation-Lösung, die das Management Pack enthält, nur auf einer einzelnen vRealize Operations Manager-Instanz installieren.

Um Ihre vRealize Operations Manager-Instanz vorzubereiten, damit Analysen an vRealize Automation bereitgestellt werden, installieren und konfigurieren Sie die vRealize Automation-Lösung. Sie müssen auch eine Richtlinie konfigurieren und die Richtlinie auf Ihre Cluster-Computing-Ressourcen anwenden.

Nachdem Sie die vRealize Automation-Lösung konfiguriert haben, können Sie keine von vRealize Automation verwalteten virtuellen Maschinen verschieben oder neu verteilen.

Wenn die vRealize Automation-Lösung nicht in der vRealize Operations Manager-Instanz installiert ist, kann sich die Platzierung der Arbeitslast nach wie vor verschieben oder es kann zu einer Neuverteilung der von vRealize Automation verwalteten virtuellen Maschinen kommen.

Um das Verschieben von virtuellen Maschinen mithilfe der Arbeitslastplatzierung zuzulassen, müssen sich diese virtuelle Maschinen in einem Datacenter oder einem benutzerdefinierten Datacenter befinden.



Voraussetzungen

- Konfigurieren Sie vRealize Automation zur Verwendung von Analysen für die Platzierung von Arbeitslasten. Siehe [Konfigurieren von vRealize Automation für die Platzierung der Arbeitslast](#).
- Stellen Sie sicher, dass die vRealize Automation-Lösung auf der vRealize Operations Manager-Instanz installiert und konfiguriert ist, die für die Platzierung der Arbeitslast verwendet wird. Weitere Informationen zu dieser Lösung finden Sie unter [Management Pack for vRealize Automation auf Solution Exchange](#). Informationen dazu, wie die Platzierung der Arbeitslast in vRealize Operations Manager funktioniert, finden Sie in [Workload Automation Details](#) und verwandten Themen in der vRealize Operations Manager-Dokumentation.

Verfahren

- 1 Installieren und konfigurieren Sie die vRealize Automation-Lösung auf der Instanz von vRealize Operations Manager, die die Arbeitslastplatzierung verwaltet.

Die Lösung ist möglicherweise bereits installiert.

- a Um die Lösungen anzuzeigen, die in vRealize Operations Manager installiert sind, klicken Sie auf **Verwaltung > Lösungen**.
- b Überprüfen Sie, ob die vRealize Automation-Lösung bereits installiert ist.

Wenn die vRealize Automation-Lösung nicht in der Liste angezeigt wird, laden Sie die Lösung herunter und installieren Sie sie. Weitere Informationen finden Sie unter [Management Pack for vRealize Automation auf Solution Exchange](#).

- c Wenn die Lösung in der Liste angezeigt wird, wählen Sie die **VMware vRealize Automation-Lösung** aus und klicken Sie auf **Konfigurieren**.
- d Konfigurieren Sie die vRealize Automation-Lösung, und speichern Sie die Einstellungen.

Weitere Informationen zum Konfigurieren der Lösung finden Sie unter [Solutions in vRealize Operations Manager](#) im vRealize Operations Manager-Informationscenter.

- 2 Wenn Sie nicht die vRealize Operations Manager-Standardrichtlinie verwenden, müssen Sie eine benutzerdefinierte Gruppe erstellen. Anschließend fügen Sie die Computing-Ressourcen Ihres Clusters zur benutzerdefinierten Gruppe hinzu.

Um eine andere als die Standardrichtlinie auf Ihre Cluster anzuwenden, fügen Sie eine benutzerdefinierte Gruppe hinzu. Wenden Sie dann die Richtlinie auf die benutzerdefinierte Gruppe an. Wenn Sie die Standardrichtlinie verwenden, brauchen Sie keine benutzerdefinierte Gruppe zu erstellen, da die Standardrichtlinie für alle Objekte gilt.

- a Klicken Sie auf **Umgebung > Benutzerdefinierte Gruppen**.
- b Wenn keine benutzerdefinierte Gruppe für den Cluster vorhanden ist, erstellen Sie eine benutzerdefinierte Gruppe.

Einzelheiten dazu finden Sie unter [Benutzerszenario: Erstellen benutzerdefinierter Objektgruppen](#) im vRealize Operations Manager-Informationscenter.

- c Fügen Sie den Cluster zur benutzerdefinierten Gruppe hinzu, und speichern Sie die benutzerdefinierte Gruppe.

- 3 Konfigurieren Sie eine Richtlinie zum Konsolidieren und Verteilen von Arbeitslasten auf Ihren Clustern, und wenden Sie diese Richtlinie auf die benutzerdefinierte Gruppe an.

Sie konfigurieren eine Richtlinie in vRealize Operations Manager, um die Einstellungen für Konsolidierung, Lastausgleich, Ausfüllen, CPU, Arbeitsspeicher und Festplattenspeicher einzurichten. Beispiel: Sie ändern die Einstellung mit dem Namen „Arbeitslasten konsolidieren“, um die beste Platzierung für neue verwaltete Arbeitslasten basierend auf

Clusterstatus und Kapazität zu bestimmen. Sie ändern auch die Einstellung für den Schwellenwert für die Verteilung von Arbeitslasten auf der Ebene der Aggressivität, die zum Platzieren von Arbeitslasten erforderlich ist. Sie können eine oder mehrere Richtlinien konfigurieren und auf Ihre Cluster-Computing-Ressourcen anwenden.

- a Um die Richtlinien zu suchen, klicken Sie auf **Administration > Richtlinien > Richtlinienbibliothek**.
- b Um Werte für die Arbeitslast festzulegen, klicken Sie auf **Richtlinie hinzufügen/bearbeiten** und dann auf **Arbeitslast-Automatisierung**.

Die Einstellungen mit den Namen „Arbeitslasten konsolidieren“ und „Cluster-Spielraum“ gelten für die anfängliche Platzierung der virtuellen Maschinen.

- Wenn Sie „Arbeitslasten konsolidieren“ auf **keine** festlegen, wird die Arbeitslast bei ihrer Platzierung auf alle Cluster verteilt, für die die Richtlinie gilt. Wenn Sie „Arbeitslasten konsolidieren“ auf einen anderen Wert festlegen, wird bei der Platzierung der Arbeitslast der Cluster mit der höchsten Auslastung zuerst gefüllt.
 - Der Cluster-Spielraum ist der in einem Cluster reservierte Pufferspeicher (als Prozentsatz der Gesamtkapazität). Wenn Sie den Cluster-Spielraum zum Beispiel auf 20 % festlegen, verhindert die Arbeitslastplatzierung möglicherweise die Platzierung von virtuellen Maschinen auf diesen Clustern. Die Ursache für das Verhindern der Platzierung ist darauf zurückzuführen, dass der Cluster 20 % weniger freie Kapazität für CPU, Arbeitsspeicher und Festplattenspeicher hat.
- c Klicken Sie im Richtlinienbereich auf **Richtlinie auf Gruppen anwenden**.
 - d Wählen Sie die benutzerdefinierte Gruppe aus.
 - e Speichern Sie die Richtlinie.

Ergebnisse

Sie haben vRealize Operations Manager konfiguriert, sodass vRealize Automation die Analysen für die Platzierung von Arbeitslasten verwendet, um Platzierungsziele für Maschinen vorzuschlagen, wenn Benutzer Blueprints bereitstellen.

Nächste Schritte

Warten Sie, bis vRealize Automation und vRealize Operations Manager Daten von den Endpoints und Objekten in Ihrer Umgebung erfasst haben. Wenn Sie dann neue Blueprints bereitstellen, zeigt vRealize Automation die Empfehlungen für die Platzierung von Arbeitslasten, Zielkandidaten und ausgewählte Platzierung an, damit Sie diese bestätigen.

Fehlerbehebung bei der Platzierung der Arbeitslast

Wenn bei der Platzierung der Arbeitslast Probleme auftreten, verwenden Sie die Informationen zur Fehlerbehebung, um diese zu beheben.

Die vRealize Automation-Lösung ist erforderlich, damit die Platzierung der Arbeitslast ordnungsgemäß ausgeführt wird.

Die Platzierung der Arbeitslast basiert auf einzelnen Maschinen, und die Platzierung wird auf Maschinenebene durchgeführt. Wenn vRealize Automation und vRealize Operations Manager zusammen installiert sind, muss ebenfalls eine vRealize Automation-Lösung installiert werden.

Die Lösung, die das Management Pack und den Adapter enthält, identifiziert die Cluster, auf denen die Aktionen `Container neu verteilen` oder `VM verschieben` deaktiviert sind. Die Neuverteilung ist in dem benutzerdefinierten Datencenter deaktiviert, zu dem der Cluster gehört.

- Für nicht verwaltete vRealize Automation-Cluster, die zu einem benutzerdefinierten Datencenter ohne verwaltete vRealize Automation-Cluster gehören, werden die Aktionen `VM verschieben` und `Container neu verteilen` aktiviert. Für verwaltete vRealize Automation-Cluster werden diese Aktionen deaktiviert.
- In vRealize Operations Manager führt der vRealize Automation-Adapter dazu, dass VMs in Clustern, die Reservierungen zuordnen, nicht verschoben oder neu verteilt werden können.

Vorsicht Die vRealize Automation-Lösung darf nur auf einer einzelnen vRealize Operations Manager-Instanz installiert werden.

Hochverfügbarkeit (High Availability, HA) ist aktiviert, muss jedoch deaktiviert werden

Wenn HA bei Ausfall von vRealize Operations Manager nicht aktiviert ist, schlägt die Zeitüberschreitung für die Platzierung der Arbeitslast zum Aufrufen von vRealize Operations Manager möglicherweise fehl.

vRealize Automation protokolliert Fehler bei der Platzierung der Arbeitslast in der `catalina.out`-Protokolldatei.

vSphere-Endpoints in vRealize Automation werden nicht überwacht

vRealize Operations Manager überwacht die vSphere vCenter Server-Instanz nicht, die die Reservierungs-Cluster enthält.

Wenn vRealize Operations Manager die vRealize Automation-Kandidatenreservierungen für Cluster, Datenspeicher oder Datenspeicher-Cluster bei der Platzierung nicht erkennt, werden sie ignoriert. In der Platzierungsantwort kommuniziert vRealize Operations Manager an vRealize Automation, dass diese Elemente nicht erkannt wurden.

In der Folge zeigt vRealize Automation in den Platzierungsdetails der Anforderung ein Warnsymbol bei der Kandidatenreservierung an, um anzugeben, dass diese nicht erkannt wird.

Wenn Nichtübereinstimmungen auftreten, wird vRealize Automation am Anfang der Liste angezeigt

vRealize Automation und vRealize Operations Manager verwalten unterschiedliche Ansichten der Infrastruktur. Sie müssen beide jedoch dieselben vCenter Server-Instanzen in derselben Infrastruktur verwalten.

Muss Trennungen und Nichtübereinstimmungen identifizieren und Details anzeigen.

Was tun, wenn der vRealize Automation-Adapter inaktiv ist?

Die anfängliche Platzierung berücksichtigt immer die Liste der Zielkandidaten, die von vRealize Operations Manager empfangen werden, wie zum Beispiel, wenn ein Benutzer sofort nach der Installation einen Cluster hinzufügt.

Wenn die vRealize Automation-Lösung, die das Management Pack und den Adapter enthält, im vRealize Operations Manager nicht verfügbar ist, sind die Aktionen VM verschieben und Container neu verteilen verfügbar.

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 bei vRealize Automation 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](#).

Verfahren

- 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** (✅).

Ergebnisse

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 bei vRealize Automation als **Fabric-Administrator** an.
- Sie müssen bereits über ein Schlüsselpaar verfügen. Siehe [Erstellen eines Schlüsselpaars](#).

Verfahren

- 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 bei vRealize Automation als **Fabric-Administrator** an.
- Ein Schlüsselpaar mit einem privaten Schlüssel muss vorhanden sein. Siehe [Hochladen des privaten Schlüssels für ein Schlüsselpaar](#).

Verfahren

- 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**.

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 bei vRealize Automation als **Fabric-Administrator** an.
- Als Systemadministrator definieren Sie die Datacenter-Standorte. Siehe [Szenario: Hinzufügen von Datacenter-Standorten für regionsübergreifende Bereitstellungen](#).

Verfahren

- 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.

Ergebnisse

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](#).

Bereitstellen einer vRealize Automation-Bereitstellung mithilfe eines IPAM-Drittanbieters

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

Die IP-Adressbereiche im Netzwerkprofil werden in einer verknüpften Reservierung verwendet, die Sie in einem Blueprint festlegen. Wenn ein berechtigter Benutzer eine Maschinenbereitstellung unter Verwendung des Blueprint-Katalogelements anfordert, wird eine IP-Adresse für den vom IPAM-Drittanbieter angegebenen IP-Adressbereich bezogen. 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 2-19. Vorbereitungen für die Bereitstellung einer vRealize Automation-Bereitstellung mithilfe der IPAM-Checkliste von Infoblox.

Aufgabe	Beschreibung	Details
Beziehen, importieren und konfigurieren Sie das Plug-In oder Paket des Drittanbieters einer IPAM-Lösung.	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 (https://marketplace.vmware.com/vsx) das benötigte IPAM-Anbieterpaket nicht enthält, können Sie mit dem SDK des IPAM-Lösungsanbieters und der zugehörigen Dokumentation Ihr eigenes Paket erstellen. Weitere Informationen finden Sie auf der Seite vRealize Automation-Beispielpaket eines IPAM-Drittanbieters unter code.vmware.com/web/sdk .	Siehe Checkliste für die Unterstützung eines externen IPAM-Anbieters .
Erstellen Sie einen Endpoint für einen Drittanbieter einer IPAM-Lösung.	Erstellen Sie einen neuen IPAM-Endpoint in vRealize Automation.	Siehe Erstellen eines Endpoints eines IPAM-Drittanbieters .
Geben Sie die Endpoint-Einstellungen für den Drittanbieter einer IPAM-Lösung in einem externen Netzwerkprofil an.	Erstellen Sie ein externes Netzwerkprofil und geben Sie den definierten IPAM-Endpoint in vRealize Automation an.	Siehe Erstellen eines externen Netzwerkprofils mithilfe eines IPAM-Drittanbieters .

Tabelle 2-19. Vorbereitungen für die Bereitstellung einer vRealize Automation-Bereitstellung mithilfe der IPAM-Checkliste von Infoblox. (Fortsetzung)

Aufgabe	Beschreibung	Details
Geben Sie optional Endpoint-Einstellungen für den Drittanbieter einer IPAM-Lösung in einem gerouteten Netzwerkprofil an.	Erstellen Sie ein bedarfsgesteuertes Netzwerkprofil und geben Sie den definierten IPAM-Endpoint in vRealize Automation an.	Siehe Erstellen eines Profils eines gerouteten Netzwerks mithilfe eines IPAM-Endpoints eines Drittanbieters oder Erstellen eines NAT-Netzwerkprofils unter Verwendung eines IPAM-Endpoints eines Drittanbieters .
Definieren Sie eine Reservierung, um das Netzwerkprofil zu verwenden.	Erstellen Sie eine Reservierung, die das Netzwerkprofil in vRealize Automation aufruft.	Siehe Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer .
Definieren Sie einen Blueprint, der das externe Netzwerkprofil verwendet.	Erstellen Sie einen Blueprint, der die Reservierung in vRealize Automation verwendet.	Siehe Kapitel 3 Bereitstellen von Dienst-Blueprints für Benutzer .
Veröffentlichen Sie den Blueprint im Katalog, um ihn zur Nutzung verfügbar zu machen.	Veröffentlichen Sie den Blueprint im Katalog in vRealize Automation. Fügen Sie alle erforderlichen Berechtigungen hinzu.	Siehe Veröffentlichen eines Blueprints .
Fordern Sie die Bereitstellung einer Maschine mithilfe des Blueprint-Katalogelements an.	Verwenden Sie das Blueprint-Katalogelement, um die Bereitstellung einer Maschine in vRealize Automation anzufordern.	Siehe Verwalten des Servicekatalogs .

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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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 eingengt 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**.

Ergebnisse

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.

Nächste Schritte

- 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 bei vRealize Automation als **Mandantenadministrator** an.
- Stellen Sie sicher, dass Sie Zugriff auf einen REST-Host haben.

Verfahren

- 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
Keine	Es ist keine Authentifizierung erforderlich.
OAuth 1.0	<p>Verwendet das Protokoll OAuth 1.0. Sie müssen die erforderlichen Authentifizierungsparameter unter OAuth 1.0 angeben.</p> <ul style="list-style-type: none"> a Geben Sie im Textfeld Consumer-Schlüssel den Schlüssel ein, der den Consumer als Dienstanbieter identifiziert. b Geben Sie im Textfeld Consumer-Geheimnis das Geheimnis zum Nachweis der Nutzungsberechtigung für den Consumer-Schlüssel ein. c (Optional) Geben Sie im Textfeld Zugriffstoken den Zugriffstoken ein, den der Consumer für den Zugriff auf die geschützten Ressourcen verwendet. d (Optional) Geben Sie im Textfeld Zugriffstoken-Geheimnis das Geheimnis ein, das dem Consumer als Nachweis der Nutzungsberechtigung für einen Token dient.
OAuth 2.0	<p>Verwendet das Protokoll OAuth 2.0.</p> <p>Geben Sie im Textfeld Token das Authentifizierungstoken ein.</p>
Einfach	<p>Bietet eine Standardauthentifizierung für den Zugriff. Die Kommunikation mit dem Host erfolgt im Modus „Gemeinsame Sitzung“.</p> <ul style="list-style-type: none"> a Geben Sie im Textfeld Authentifizierungs-Benutzername den Benutzernamen für die gemeinsame Sitzung ein. b Geben Sie im Textfeld Authentifizierungskennwort das Kennwort für die gemeinsame Sitzung ein.
Digest	<p>Bietet eine Digest-Zugriffsauthentifizierung mit Verschlüsselung. Die Kommunikation mit dem Host erfolgt im Modus „Gemeinsame Sitzung“.</p> <ul style="list-style-type: none"> a Geben Sie im Textfeld Authentifizierungs-Benutzername den Benutzernamen für die gemeinsame Sitzung ein. b Geben Sie im Textfeld Authentifizierungskennwort das Kennwort für die gemeinsame Sitzung ein.

Option	Aktion
NTLM	<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"> Geben Sie die Anmeldedaten für die gemeinsame Sitzung an. <ul style="list-style-type: none"> ■ Geben Sie im Textfeld Authentifizierungs-Benutzername den Benutzernamen für die gemeinsame Sitzung ein. ■ Geben Sie im Textfeld Authentifizierungskennwort das Kennwort für die gemeinsame Sitzung ein. Konfigurieren der NTLM-Angaben <ul style="list-style-type: none"> ■ (Optional) Geben Sie im Textfeld Workstation für die NTLM-Authentifizierung den Workstation-Namen ein. ■ Geben Sie im Textfeld Domäne für die NTLM-Authentifizierung den Domänennamen ein.
Kerberos	<p>Bietet Kerberos-Zugriffsauthentifizierung. Die Kommunikation mit dem Host erfolgt im Modus „Gemeinsame Sitzung“.</p> <ol style="list-style-type: none"> Geben Sie im Textfeld Authentifizierungs-Benutzername den Benutzernamen für die gemeinsame Sitzung ein. Geben Sie im Textfeld Authentifizierungskennwort das Kennwort für die gemeinsame Sitzung ein.

11 Klicken Sie auf **Beenden**.

Ergebnisse

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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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"> a Geben Sie im Textfeld Port unter den Details zum PowerShell-Host die Portnummer für die Kommunikation mit dem Host ein. b Wählen Sie aus dem Dropdown-Menü Transportprotokoll ein Transportprotokoll aus. <p>Hinweis 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"> c Wählen Sie den Authentifizierungstyp aus dem Dropdown-Menü Authentifizierung aus. <p>Hinweis 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**.

Ergebnisse

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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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
Ja	Geben Sie im Textfeld WSDL-Inhalte den WSDL-Text ein.
Nein	Geben Sie im Textfeld WSDL-URL 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
Keine	Es ist keine Authentifizierung erforderlich.
Einfach	<p>Bietet eine Standardauthentifizierung für den Zugriff. Die Kommunikation mit dem Host erfolgt im Modus „Gemeinsame Sitzung“.</p> <ul style="list-style-type: none"> a Geben Sie im Textfeld Benutzername den Benutzernamen für die gemeinsame Sitzung ein. b Geben Sie im Textfeld Kennwort das Kennwort für die gemeinsame Sitzung ein.
Digest	<p>Bietet eine Digest-Zugriffsauthentifizierung mit Verschlüsselung. Die Kommunikation mit dem Host erfolgt im Modus „Gemeinsame Sitzung“.</p> <ul style="list-style-type: none"> a Geben Sie im Textfeld Benutzername den Benutzernamen für die gemeinsame Sitzung ein. b Geben Sie im Textfeld Kennwort das Kennwort für die gemeinsame Sitzung ein.
NTLM	<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> <ul style="list-style-type: none"> a Geben Sie die Anmeldedaten an. <ul style="list-style-type: none"> ■ Geben Sie im Textfeld Benutzername den Benutzernamen für die gemeinsame Sitzung ein. ■ Geben Sie im Textfeld Kennwort das Kennwort für die gemeinsame Sitzung ein. b Geben Sie die NTLM-Einstellungen an. <ul style="list-style-type: none"> ■ Geben Sie im Textfeld NTLM-Domäne den Domänennamen ein. ■ (Optional) Geben Sie im Textfeld NTLM-Workstation den Workstation-Namen ein.
Negotiate	<p>Bietet Kerberos-Zugriffsauthentifizierung. Die Kommunikation mit dem Host erfolgt im Modus „Gemeinsame Sitzung“.</p> <ul style="list-style-type: none"> a Geben Sie die Anmeldedaten an. <ul style="list-style-type: none"> 1 Geben Sie im Textfeld Benutzername den Benutzernamen für die gemeinsame Sitzung ein. 2 Geben Sie im Textfeld Kennwort das Kennwort für die gemeinsame Sitzung ein. b Geben Sie im Textfeld SPN des Kerberos-Diensts den SPN des Kerberos-Diensts ein.

11 Klicken Sie auf **Beenden**.**Ergebnisse**

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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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**.

Ergebnisse

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.

Erstellen eines Microsoft Azure-Endpoints

Sie können einen Microsoft Azure-Endpoint erstellen, um die Einrichtung einer authentifizierten Verbindung zwischen vRealize Automation und einer Azure-Bereitstellung zu erleichtern.

Ein Endpoint stellt eine Verbindung zu einer Ressource her, in diesem Fall eine Azure-Instanz, mit der Sie Blueprints für virtuelle Maschine erstellen können. Sie müssen über einen Azure-Endpoint verfügen, der als Basis von Blueprints für die Bereitstellung von virtuellen Azure-Maschinen verwendet wird. Wenn Sie mehrere Azure-Abonnements verwenden, benötigen Sie Endpoints für jede Abonnement-ID.

Als Alternative können Sie mithilfe des Befehls zum Hinzufügen einer Azure-Verbindung eine solche direkt aus vRealize Orchestrator erstellen. Dieser befindet sich unter **Bibliothek > Azure- > Konfiguration** in der Workflow-Struktur von vRealize Orchestrator. In den meisten Fällen ist das Erstellen einer Verbindung über die Endpoint-Konfiguration wie in diesem Dokument beschrieben die bevorzugte Option.

Azure-Endpoints werden von vRealize Orchestrator und der XaaS-Funktionalität unterstützt. Sie können einen Azure-Endpoint erstellen, löschen oder bearbeiten. Bitte beachten Sie: Wenn Sie Änderungen an einem bestehenden Endpoint vornehmen und einige Stunden lang keine Updates an dem Azure-Portal über die aktualisierte Verbindung durchführen, müssen Sie den vRealize Orchestrator-Dienst über den Befehl `service vco-service restart` neu starten. Wird der Dienst nicht neu gestartet, kann dies zu Fehlern führen.

Voraussetzungen

- Konfigurieren Sie eine Instanz von Microsoft Azure und rufen Sie ein gültiges Microsoft Azure-Abonnement ab, dessen Abonnement-ID verwendet werden kann. Weitere Informationen über das Konfigurieren von Azure und das Abrufen einer Abonnement-ID finden Sie unter <http://www.vaficionado.com/2016/11/using-new-microsoft-azure-endpoint-vrealize-automation-7-2/>.
- Stellen Sie sicher, dass Ihre vRealize Automation-Bereitstellung über mindestens einen Mandanten und eine Business-Gruppe verfügt.
- Erstellen Sie ein Active Directory-Verzeichnis für eine Anwendung, wie in <https://azure.microsoft.com/de-de/documentation/articles/resource-group-create-service-principal-portal> beschrieben.
- Notieren Sie sich die folgenden Informationen im Zusammenhang mit Azure, da Sie sie während der Endpoint- und Blueprint-Konfiguration benötigen.
 - Abonnement-ID
 - Mandanten-ID
 - Name des Speicherkontos
 - Name der Ressourcengruppe
 - Speicherort
 - Name des virtuellen Netzwerks
 - Client-Anwendungs-ID
 - Geheimer Schlüssel der Client-Anwendung
 - URN des VM-Images
- Es gibt eindeutige Einstellungen für das Erstellen und Bereitstellen von Cloudanwendungen für Azure in der China-Umgebung. Weitere Informationen finden Sie unter <https://docs.microsoft.com/en-us/azure/china/china-get-started-developer-guide>. Wenn Sie einen vRealize Automation Azure-Endpoint für China erstellen, müssen die Dienst-URL, die Anmelde-URL und die Speicher-URL wie folgt angegeben werden:
 - Dienst-URL: <https://management.chinacloudapi.cn>
 - Anmelde-URL: <https://login.chinacloudapi.cn/>
 - Speicher-URL: https://storage_account_name.blob.core.chinacloudapi.cn/

Die Azure-Implementierung innerhalb von vRealize Automation unterstützt einen Teil der von Microsoft Azure unterstützten Regionen. Siehe [Von Azure unterstützte Regionen](#).
- Melden Sie sich bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 1 Wählen Sie **Administration > vRO-Konfiguration > Endpoints** aus.

- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Klicken Sie auf der Registerkarte „Plugin“ auf das Dropdown-Menü **Plugin** und wählen Sie das **Azure-Plugin** aus.
- 4 Klicken Sie auf **Weiter**.
- 5 Geben Sie einen Namen und optional eine Beschreibung ein.
- 6 Klicken Sie auf **Weiter**.
- 7 Befüllen Sie die Textfelder auf der Registerkarte **Details** entsprechend den Anforderungen des Endpoints.

Parameter	Beschreibung
Verbindungseinstellungen	
Azure-Verbindung	
Name der Verbindung	Eindeutiger Name für die neue Endpoint-Verbindung. Dieser Name wird in der vRealize Orchestrator-Schnittstelle angezeigt, um Ihnen das Identifizieren einer bestimmten Verbindung zu erleichtern.
Azure-Abonnement-ID	Der Bezeichner für Ihr Azure-Abonnement. Mit der ID werden die Speicherkonten, virtuellen Maschinen und andere Azure-Ressourcen angegeben, auf die Sie zugreifen können.
Einstellungen des Ressourcenmanagers	
URI des Azure-Diensts	Der URI, über den Sie Zugriff auf die Azure-Instanz erhalten. Der Standardwert von <code>https://management.azure.com/</code> eignet sich für viele gängige Implementierungen.
URI des Azure-Speichers	Der URI, über den Sie Zugriff auf die Azure-Speicherinstanz erhalten.
Mandanten-ID	Die ID des Azure-Mandanten, die vom Endpoint verwendet werden soll.
Client-ID	Der Bezeichner des Azure-Clients, der vom Endpoint verwendet werden soll. Dieser wird zugewiesen, wenn Sie eine Active Directory-Anwendung erstellen.
Geheimer Client-Schlüssel	Der Schlüssel, der mit einer Azure-Client-ID verwendet wird. Dieser Schlüssel wird zugewiesen, wenn Sie eine Active Directory-Anwendung erstellen.
Anmelde-URL	Die für den Zugriff auf die Azure-Instanz verwendete URL. Der Standardwert von <code>https://login.windows.net/</code> eignet sich für viele gängige Implementierungen.
Proxy-Einstellungen	

Parameter	Beschreibung
Proxy-Host	Wenn Ihr Unternehmen einen Proxy-Webserver verwendet, geben Sie den Namen dieses Servers ein.
Proxy-Port	Wenn Ihr Unternehmen einen Proxy-Webserver verwendet, geben Sie die Portnummer dieses Servers ein.

8 (Optional) Klicken Sie auf „Eigenschaften“ und fügen Sie benutzerdefinierte Eigenschaften, Eigenschaftsgruppen oder Ihre eigenen Eigenschaftsdefinitionen hinzu.

9 Klicken Sie auf **Fertig stellen**.

Nächste Schritte

Erstellen Sie in Azure geeignete Ressourcengruppen, Speicherkonten und Netzwerksicherheitsgruppen. Sie sollten ggf. auch Lastausgleichsmodule für Ihre Implementierung erstellen.

Aktion	Optionen
Erstellen einer Azure-Ressourcengruppe	<ul style="list-style-type: none"> ■ Erstellen Sie die Ressourcengruppe mithilfe des Azure-Portals. Spezielle Anweisungen finden Sie in der Azure-Dokumentation. ■ Verwenden Sie den geeigneten vRealize Orchestrator-Workflow, der sich in der Ressourcengruppe unter <code>Library/Azure/Resource/Create</code> befindet. ■ Erstellen und veröffentlichen Sie in vRealize Automation einen XaaS-Blueprint, der den vRealize Orchestrator-Workflow enthält. Sie können die Ressourcengruppe anfordern, nachdem Sie sie an den Dienst und die Berechtigungen angehängt haben. Beachten Sie, dass der Ressourcentyp der Ressourcengruppe von vRealize Automation nicht unterstützt oder verwaltet wird.
Erstellen eines Azure-Speicherkontos	<ul style="list-style-type: none"> ■ Verwenden Sie Azure, um ein Speicherkonto zu erstellen. Spezielle Anweisungen finden Sie in der Azure-Dokumentation. ■ Verwenden Sie den geeigneten vRealize Orchestrator-Workflow, der sich im Speicherkonto unter <code>Library/Azure/Storage/Create</code> befindet. ■ Erstellen und veröffentlichen Sie in vRealize Automation einen XaaS-Blueprint, der den vRealize Orchestrator-Workflow enthält. Sie können das Speicherkonto anfordern, nachdem Sie es an den Dienst und die Berechtigungen angehängt haben.
Erstellen einer Azure-Netzwerk-Sicherheitsgruppe	<ul style="list-style-type: none"> ■ Verwenden Sie Azure, um eine Sicherheitsgruppe zu erstellen. Spezielle Anweisungen finden Sie in der Azure-Dokumentation. ■ Verwenden Sie den geeigneten vRealize Orchestrator-Workflow, der sich in der Netzwerksicherheitsgruppe unter <code>Library/Azure/Network/Create</code> befindet. ■ Erstellen und veröffentlichen Sie in vRealize Automation einen XaaS-Blueprint, der den vRealize Orchestrator-Workflow enthält. Sie können die Sicherheitsgruppe anfordern, nachdem Sie sie zu dem Dienst und den Berechtigungen hinzugefügt haben.

Von Azure unterstützte Regionen

Die Azure-Implementierung innerhalb von vRealize Automation unterstützt einen Teil der von Microsoft Azure unterstützten Regionen.

Die folgenden Azure-Regionen werden durch die Azure-Implementierung innerhalb von vRealize Automation unterstützt.

- | | |
|---------------------|------------------------|
| ■ Asien, Osten | ■ Australien, Osten |
| ■ Asien, Südosten | ■ Australien, Südosten |
| ■ USA, Mitte | ■ Indien, Süden |
| ■ USA, Osten | ■ Indien, Mitte |
| ■ USA, Osten 2 | ■ Indien, Westen |
| ■ USA, Westen | ■ Kanada, Mitte |
| ■ USA, Westen 2 | ■ Kanada, Osten |
| ■ USA, Norden-Mitte | ■ USA, Westen-Mitte |
| ■ USA, Süden-Mitte | ■ Korea, Mitte |
| ■ Europa, Norden | ■ Korea, Süden |
| ■ Europa, Westen | ■ UK, Westen |
| ■ Japan, Westen | ■ UK, Süden |
| ■ Japan, Osten | ■ China, Osten |
| ■ Brasilien, Süden | ■ China, Norden |
-

Erstellen und Konfigurieren von Containern

Über die Registerkarte Container in vRealize Automation können Sie die integrierte Container für vRealize Automation-Anwendung öffnen und die Container und Container-Netzwerkeinstellungen erstellen und konfigurieren, damit sie vRealize Automation-Blueprint-Architekten zur Verfügung stehen.

Sie können Container mithilfe von neuen und vorhandenen Vorlagen und Images in der integrierten Container-Anwendung definieren. Sie können dann Containerkomponenten und ihre zugehörigen Netzwerkeinstellungen zu vRealize Automation-Blueprints hinzufügen.

Verwalten von Containerhosts und Clustern

Sie können die Hosts anzeigen und verwalten, die Sie über die Seite „Cluster“ hinzufügen. Im Kontext von Container ist der Host eine virtuelle Maschine oder Infrastruktur, mit der Sie Container ausführen können.

Die Seite „Cluster“ auf der Registerkarte „Infrastruktur“ enthält die Steuerelemente zum Hinzufügen von neuen Clustern und Hosts. Zum Hinzufügen eines Hosts zur Containerumgebung müssen Sie ihn zu einem Cluster hinzufügen. Sie können den Status der Bereitstellungsanforderungen vorhandener Hosts überwachen und Ereignisprotokolle für Ihre Container über eine beliebige Seite auf den Registerkarten „Bibliothek“ und „Bereitstellungen“ anzeigen. Die Bereiche „Anforderungen“ und „Ereignisprotokoll“ befinden sich rechts auf der Seite.

Hinzufügen eines Containerhosts zu einem neuen Cluster

Sie müssen einen Host zu einem Cluster hinzufügen, um Container bereitzustellen.

Voraussetzungen

Wählen Sie oben links auf der Registerkarte „Container“ eine Business-Gruppe aus.

Verfahren

- 1 Melden Sie sich bei der vRealize Automation-Konsole als **Containeradministrator** an.
- 2 Klicken Sie auf die Registerkarte **Container**.
- 3 Klicken Sie auf **Infrastruktur > Cluster**.
- 4 Klicken Sie auf **Neu**.
- 5 Geben Sie einen Namen für den Cluster ein.
- 6 Geben Sie eine Beschreibung für den Cluster ein.
- 7 Wählen Sie unter **Typ** aus, ob Sie die Adresse eines Docker-Hosts oder eines virtuellen Containerhosts (VCH) eingegeben haben.

Hinweis Nur VCH-Hosts der Version 1.2 und 1.3 werden in Containern für vRealize Automation 7.4 unterstützt.

- 8 Geben Sie die IP-Adresse oder den Namen des Hosts im Format **http(s)://<hostname>:<port>** ein.
- 9 Wählen Sie Ihre Anmeldeinformationen aus der Liste aus.

Container unterstützt die Authentifizierung mit Anmeldeinformationen und die Authentifizierung mit öffentlichen bzw. privaten Schlüsseln. Sie können die auf der Seite **Identitätsverwaltung** verfügbaren Anmeldedaten hinzufügen.
- 10 Klicken Sie auf **Speichern**.

Ergebnisse

Sie haben erfolgreich einen neuen Cluster erstellt und ihm einen Host hinzugefügt.

Verwenden von Container-Bereitstellungsrichtlinien

Sie können Bereitstellungsrichtlinien mit Hosts und Containerdefinitionen verknüpfen. Sie verwenden Bereitstellungsrichtlinien in Container für vRealize Automation, um eine Präferenz für den spezifischen Host und die Kontingente festzulegen, wenn Sie einen Container bereitstellen.

Bereitstellungsrichtlinien, die auf einen Container angewendet werden, haben eine höhere Priorität als Platzierungen, die auf Containerhosts angewendet werden.

Hinweis Bereitstellungsrichtlinien sind veraltet und werden in einer künftigen Version von vRealize Automation entfernt.

Festlegen einer Bereitstellungsrichtlinie auf einem Host

Legen Sie eine Präferenz für den spezifischen Host und die Kontingente fest, wenn Sie einen Container bereitstellen.

Hinweis Bereitstellungsrichtlinien sind veraltet und werden in einer künftigen Version von vRealize Automation entfernt.

Voraussetzungen

Fügen Sie einem Cluster einen Host hinzu.

Verfahren

- 1 Melden Sie sich bei der vRealize Automation-Konsole als **Containeradministrator** an.
- 2 Klicken Sie auf die Registerkarte **Container**.
- 3 Klicken Sie auf **Infrastruktur > Cluster**.
- 4 Klicken Sie auf den Cluster, der den zu bearbeitenden Host enthält.
- 5 Klicken Sie auf **Ressourcen**.
- 6 Klicken Sie bei dem zu konfigurierenden Host auf das Optionssymbol und dann auf **Bearbeiten**.
- 7 Wählen Sie die Bereitstellungsrichtlinie aus und klicken Sie auf **Aktualisieren**.

Festlegen einer Bereitstellungsrichtlinie für eine Containerdefinition

Legen Sie eine Bereitstellungsrichtlinie für eine Containerdefinition fest.

Hinweis Bereitstellungsrichtlinien sind veraltet und werden in einer künftigen Version von vRealize Automation entfernt.

Verfahren

- 1 Klicken Sie auf die Registerkarte **Container**.
- 2 Klicken Sie auf **+Container**, um die Bereitstellung des Containers zu starten.
- 3 Klicken Sie in den Bereitstellungsoptionen auf **Richtlinie**.
- 4 Wählen Sie in der Dropdown-Liste **Bereitstellungsrichtlinie** eine vorhandene Richtlinie aus.
- 5 Stellen Sie den Container bereit oder speichern Sie ihn als Vorlage.

Konfigurieren der Containereinstellungen

Sie können eine Anwendung mit einem Container oder mit mehreren Containern definieren, indem Sie neue und vorhandene Container-Konfigurationseinstellungen verwenden.

Neben den zentralen Container für vRealize Automation-Einstellungen sind die folgenden vRealize Automation-Einstellungen für Bereitstellungen unter Verwendung von Containerkomponenten verfügbar:

- Integritätskonfiguration
- Links
- Bereitgestellte Dienste
- Parameter für Clustergröße und horizontale und vertikale Skalierung

Konfigurieren von Integritätsprüfungen in Container

Sie können eine Integritätsprüfungsmethode konfigurieren, um den Status eines Containers basierend auf benutzerdefinierten Kriterien zu aktualisieren.

Sie können HTTP- oder TCP-Protokolle verwenden, wenn Sie einen Befehl für einen Container ausführen. Sie können ebenfalls eine Integritätsprüfungsmethode angeben.

Voraussetzungen

- Stellen Sie sicher, dass Container für vRealize Automation in Ihrer unterstützten vRealize Automation-Bereitstellung aktiviert ist.
- Stellen Sie sicher, dass Sie über die Berechtigungen für die Rolle **Containeradministrator** oder **Containerarchitekt** verfügen.

Verfahren

- 1 Melden Sie sich bei vRealize Automation an.
- 2 Klicken Sie auf die Registerkarte **Container**.
- 3 Wählen Sie im linken Bereich **Bibliothek > Vorlagen** aus.
- 4 Bearbeiten Sie die Vorlage oder das Image.

Option	Beschreibung
So bearbeiten Sie eine Vorlage:	<ol style="list-style-type: none"> a Klicken Sie im oberen rechten Bereich der zu öffnenden Vorlage auf Bearbeiten. b Klicken Sie im oberen rechten Bereich des zu öffnenden Containers auf Bearbeiten.
So bearbeiten Sie ein Image:	Klicken Sie auf den Pfeil neben der Schaltfläche Bereitstellen des Images und dann auf Weitere Informationen eingeben .

- 5 Klicken Sie auf die Registerkarte **Integritätskonfiguration**.

6 Wählen Sie einen Integritätsmodus aus.

Tabelle 2-20. Integritätskonfigurationsmodi

Modus	Beschreibung
Keine	Standard. Keine Integritätsprüfungen sind konfiguriert.
HTTP	<p>Wenn Sie HTTP auswählen, müssen Sie eine API für den Zugriff sowie eine zu verwendende HTTP-Methode und -Version angeben. Die API ist relativ und Sie müssen nicht die Adresse des Containers eingeben. Sie können auch einen Wert für eine Zeitüberschreitung des Vorgangs und Integritätsschwellenwerte festlegen.</p> <p>Beispiel: Ein Fehlerfrei-Schwellenwert von 2 bedeutet, dass zwei hintereinander durchgeführte Aufrufe erfolgreich sein müssen, damit der Container als fehlerfrei und als ausgeführt betrachtet wird (Status: WIRD AUSGEFÜHRT). Beispiel: Ein Fehlerhaft-Schwellenwert von 2 bedeutet, dass zwei hintereinander durchgeführte Aufrufe nicht erfolgreich sein müssen, damit der Container als fehlerhaft (Status: FEHLER) betrachtet wird. Für alle Zustände zwischen diesen Schwellenwerten ist der Containerstatus „HERABGESTUFT“.</p>
TCP-Verbindung	<p>Wenn Sie TCP-Verbindung auswählen, müssen Sie nur einen Port für den Container eingeben. Die Integritätsprüfung versucht, eine TCP-Verbindung mit dem Container über den bereitgestellten Port herzustellen. Sie können auch einen Zeitüberschreitungswert für den Vorgang angeben und ähnlich wie bei HTTP Fehlerfrei- bzw. Fehlerhaft-Schwellenwerte festlegen.</p>
Befehl	<p>Wenn Sie Befehl auswählen, müssen Sie einen Befehl eingeben, der für den Container ausgeführt wird. Der Erfolg der Integritätsprüfung wird durch den Exitcode des Befehls angegeben.</p>
Integritätsprüfung bei Bereitstellung ignorieren	<p>Deaktivieren Sie diese Option, um eine Integritätsprüfung bei der Bereitstellung zu erzwingen. Dadurch wird erreicht, dass ein Container erst nach einer erfolgreichen Integritätsprüfung als bereitgestellt gilt.</p>
Autodeploy	<p>Ermöglicht automatische erneute Bereitstellung von Containern, wenn sie den Status FEHLER aufweisen.</p>

7 Klicken Sie auf **Speichern**.

Konfigurieren von Verknüpfungen in Container

Verknüpfungen und bereitgestellte Dienste dienen der Kommunikation für die Clusterdienste und den Lastausgleich auf den Hosts. Sie können Verknüpfungseinstellungen für Ihre Container in Container konfigurieren.

Sie können Verknüpfungen verwenden, um die Kommunikation zwischen mehreren Diensten in Ihrer Anwendung zu aktivieren. Verknüpfungen in Container weisen eine Ähnlichkeit mit Docker-Verknüpfungen auf, verbinden aber Container auf allen Hosts. Eine Verknüpfung besteht aus zwei Teilen: einem Dienstnamen und einem Alias. Der Dienstname ist der Name des Diensts oder der Vorlage, der bzw. die aufgerufen wird. Der Alias ist der Hostname, den Sie zur Kommunikation mit diesem Dienst verwenden.

Beispiel: Wenn Sie über eine Anwendung mit einem Web- und einem Datenbankdienst verfügen und unter Verwendung des Alias **my-db** eine Verknüpfung im Webdienst zum Datenbankdienst definieren, öffnet die Webdienstanwendung eine TCP-Verbindung zum `my-db:{PORT_OF_DB}`. Der `PORT_OF_DB` ist der Port, den die Datenbank unabhängig von dem öffentlichen Port abhört, der dem Host anhand der Containereinstellungen zugewiesen wurde. Wenn MySQL über den Standardport 3306 nach Updates sucht und es sich bei dem veröffentlichten Port für den Containerhost um Port 32799 handelt, greift die Webanwendung über `my-db:3306` auf die Datenbank zu.

Hinweis Die Verwendung von Netzwerken anstelle von Verknüpfungen wird empfohlen. Verknüpfungen werden mittlerweile als alte Docker-Funktion betrachtet, da sie bei der Verknüpfung von Containerclustern erhebliche Beschränkungen aufweisen. Dazu zählen:

- Docker unterstützt nicht mehrere Verknüpfungen mit demselben Alias. Das Zulassen von Container für vRealize Automation wird zum Generieren von Verknüpfungsaliasen empfohlen.
 - Sie können die Verknüpfungen einer Containerlaufzeit nicht aktualisieren. Bei der horizontalen oder vertikalen Skalierung eines verknüpften Clusters werden die Verknüpfungen des abhängigen Containers nicht aktualisiert.
-

Voraussetzungen

- Stellen Sie sicher, dass Container für vRealize Automation in Ihrer unterstützten vRealize Automation-Bereitstellung aktiviert ist.
- Stellen Sie sicher, dass Sie über die Berechtigungen für die Rolle **Containeradministrator** oder **Containerarchitekt** verfügen.
- Stellen Sie sicher, dass den Verknüpfungsdiensten ein Bridge-Netzwerk zur Verfügung steht.
- Stellen Sie sicher, dass der interne Port des Zieldiensts veröffentlicht wurde. Für die übergreifende Kommunikation kann der Dienst jedem anderen Port zugewiesen werden, er muss aber außerhalb des Hosts zugänglich sein.
- Stellen Sie den gegenseitigen Zugriff der Service-Hosts sicher.

Verfahren

- 1 Melden Sie sich bei vRealize Automation an.
- 2 Wählen Sie im linken Bereich **Bibliothek > Vorlagen** aus.

3 Bearbeiten Sie die Vorlage oder das Image.

Option	Beschreibung
So bearbeiten Sie eine Vorlage:	a Klicken Sie im oberen rechten Bereich der zu öffnenden Vorlage auf Bearbeiten . b Klicken Sie im oberen rechten Bereich des zu öffnenden Containers auf Bearbeiten .
So bearbeiten Sie ein Image:	Klicken Sie auf den Pfeil neben der Schaltfläche Bereitstellen des Images und dann auf Weitere Informationen eingeben .

4 Klicken Sie auf die Registerkarte **Standard**.

5 Geben Sie im Textfeld **Dienste** eine durch Komma getrennte Liste mit Diensten ein, von denen der Container abhängt.

6 Geben Sie im Feld **Alias** einen beschreibenden Namen für den Dienst oder die durch Komma getrennte Liste mit Diensten ein.

7 Klicken Sie auf **Speichern**.

Konfigurieren von bereitgestellten Diensten in Container

Sie können einen eindeutigen Hostnamen für einen Lastausgleichsdienst verwenden, indem Sie eine Adresse und einen Platzhalter in Ihren Containereinstellungen angeben.

Der Platzhalter bestimmt den Speicherort eines automatisch generierten Teils der URL. Dieser Wert ist für jeden Hostnamen eindeutig. Die Adresse unterstützt das %s-Formatzeichen, um den Speicherort des Platzhalters anzugeben.

Hinweis Wenn der Platzhalter nicht verwendet wird, ist er abhängig von der Systemkonfiguration als Präfix oder Suffix des Hostnamens positioniert.

Es wird empfohlen, dass Sie einen Lastausgleichsdienst verwenden, der Anfragen an jeden Knoten leiten kann, wenn Sie eine Anwendung erstellen, die einen Dienst beinhaltet, der öffentlich bereitgestellt und horizontal und vertikal skaliert werden muss. Nach der Bereitstellung der Anwendung wird die Konfiguration des Lastausgleichsdienst immer dann aktualisiert, wenn der Dienst von vRealize Automation horizontal und vertikal skaliert wird.

Voraussetzungen

- Stellen Sie sicher, dass Container für vRealize Automation in Ihrer unterstützten vRealize Automation-Bereitstellung aktiviert ist.
- Stellen Sie sicher, dass Sie über die Berechtigungen für die Rolle **Containeradministrator** oder **Containerarchitekt** verfügen.

Verfahren

1 Melden Sie sich bei vRealize Automation an.

2 Klicken Sie auf die Registerkarte **Container**.

- 3 Wählen Sie im linken Bereich **Bibliothek > Vorlagen** aus.
- 4 Bearbeiten Sie die Vorlage oder das Image.

Option	Beschreibung
So bearbeiten Sie eine Vorlage:	<ol style="list-style-type: none"> a Klicken Sie im oberen rechten Bereich der zu öffnenden Vorlage auf Bearbeiten. b Klicken Sie im oberen rechten Bereich des zu öffnenden Containers auf Bearbeiten.
So bearbeiten Sie ein Image:	Klicken Sie auf den Pfeil neben der Schaltfläche Bereitstellen des Images und dann auf Weitere Informationen eingeben .

- 5 Klicken Sie auf die Registerkarte **Netzwerk**.
- 6 Geben Sie im Feld **Adresse** den Speicherort für den Platzhalter ein.
Der Adresshost agiert als virtueller Host. Um auf den Adresshost zuzugreifen, können Sie Zuordnungsinformationen in der Datei etc/hosts hinzufügen oder einen DNS verwenden, der die Containeradresse dem Hostnamen zuordnet.
- 7 Geben Sie im Textfeld **Containerport** die für die Bereitstellung des Diensts verwendete Portnummer ein.
Verwenden Sie das im Formular angegebene Beispielformat. Wenn Ihre Containeranwendung mehr als einen Port bereitstellt, geben Sie an, welche internen Ports den Dienst bereitstellen können.
- 8 Klicken Sie auf **Speichern**.

Konfigurieren der Clustergröße und der Skalierung in Container

Sie können Containercluster erstellen, indem Sie die Container-Platzierungseinstellung zur Angabe der Clustergröße verwenden.

Wenn Sie einen Cluster konfigurieren, stellt der Container die angegebene Anzahl an Containern bereit. Anforderungen werden per Lastausgleich auf alle Container im Cluster verteilt.

Sie können die Clustergröße für einen bereitgestellten Container oder eine bereitgestellte Anwendung mit einem Wert von 1 erhöhen oder reduzieren. Wenn Sie die Clustergröße zur Laufzeit ändern, werden alle Affinitätsfilter und Platzierungsregeln berücksichtigt.

Voraussetzungen

- Stellen Sie sicher, dass Container für vRealize Automation in Ihrer unterstützten vRealize Automation-Bereitstellung aktiviert ist.
- Stellen Sie sicher, dass Sie über die Berechtigungen für die Rolle **Containeradministrator** oder **Containerarchitekt** verfügen.

Verfahren

- 1 Melden Sie sich bei vRealize Automation an.

- 2 Klicken Sie auf die Registerkarte **Container**.
- 3 Wählen Sie im linken Bereich **Bibliothek > Vorlagen** aus.
- 4 Bearbeiten Sie die Vorlage oder das Image.

Option	Beschreibung
So bearbeiten Sie eine Vorlage:	<ol style="list-style-type: none"> a Klicken Sie im oberen rechten Bereich der zu öffnenden Vorlage auf Bearbeiten. b Klicken Sie im oberen rechten Bereich des zu öffnenden Containers auf Bearbeiten.
So bearbeiten Sie ein Image:	Klicken Sie auf den Pfeil neben der Schaltfläche Bereitstellen des Images und dann auf Weitere Informationen eingeben .

- 5 Klicken Sie auf die Registerkarte **Richtlinien**.
- 6 Legen Sie die Clustergröße für den Container fest.
- 7 Klicken Sie auf **Speichern**.

Konfigurieren und Verwenden von Vorlagen und Images in Container

Container verwendet Vorlagen zum Bereitstellen von Containern.

Bei einer Vorlage handelt es sich um eine wiederverwendbare Konfiguration, die zum Bereitstellen eines Containers oder einer Reihe von Containern verwendet werden kann. In einer Vorlage können Sie eine Multi-Tier-Anwendung definieren, die aus verlinkten Diensten besteht.

Ein Dienst wird als ein oder mehrere Container desselben Typs oder Images definiert.

Sie können eine benutzerdefinierte Containervorlage auf der Grundlage einer vorhandenen Vorlage auf der Seite **Vorlagen** erstellen oder eine ordnungsgemäß formatierte YAML-Datei importieren. Sie können auch eine Containervorlage oder ein Container-Image bereitstellen.

Erstellen einer benutzerdefinierten Containervorlage

Sie können eine benutzerdefinierte Vorlage zum Definieren eines Containers erstellen.

Bei einer Vorlage handelt es sich um eine wiederverwendbare Konfiguration, die Sie zum Bereitstellen eines Containers oder einer Reihe von Containern verwenden können.

Auf der Seite „Vorlagen“ werden verfügbare Vorlagen-Images basierend auf den von Ihnen definierten Registrierungen angezeigt. Sie können eine benutzerdefinierte Vorlage basierend auf einem vorhandenen Vorlage-Image erstellen oder eine Vorlage bzw. eine Docker Compose-Datei importieren. Siehe [Importieren einer Container-Vorlage oder Docker Compose-Datei](#).

Sie können eine benutzerdefinierte Vorlage oder ein Image auch erstellen, indem Sie die Option **Bereitstellen > Zusätzliche Informationen eingeben** verwenden, die unter [Bereitstellen eines Containers von einer Vorlage oder einem Image aus](#) beschrieben ist.

Voraussetzungen

- Stellen Sie sicher, dass Sie über Berechtigungen für die Rolle **Containeradministrator** verfügen.

Verfahren

- 1 Melden Sie sich bei der vRealize Automation-Konsole als **Containeradministrator** an.
- 2 Klicken Sie auf die Registerkarte **Container**.
- 3 Wählen Sie im linken Bereich **Bibliothek > Vorlagen** aus.

In einer Liste werden die zur Bereitstellung verfügbaren Vorlagen und Images angezeigt.

- Konfigurierte Vorlagen in der Ansicht „Images“.
- Vorhandene oder benutzerdefinierte Vorlagen in der Ansicht **Vorlage**.
- Alle basierend auf Ihren angegebenen Registrierungen in der Ansicht **Alle** verfügbaren Vorlagen und Images.

Die Optionen **Importieren** und **Exportieren** sind ebenfalls für den Import oder Export von Vorlagen und Images verfügbar.

- 4 Klicken Sie auf den Pfeil neben der Schaltfläche **Bereitstellen** eines Image, das Sie in die Vorlage übernehmen möchten.
- 5 Klicken Sie auf **Zusätzliche Informationen eingeben**.
- 6 Klicken Sie auf **Als Vorlage speichern**, um Ihre Änderungen als neue Containervorlage in Containers for vRealize Automation zu speichern.

Nächste Schritte

Sie können eine Vorlage für künftige Bereitstellungen bearbeiten. Vorhandene Anwendungen, die von der Vorlage bereitgestellt wurden, sind nicht von Änderungen betroffen, die Sie nach der Bereitstellung an der Vorlage vornehmen.

Importieren einer Container-Vorlage oder Docker Compose-Datei

Sie können eine importierte Docker-Containervorlage oder eine Docker Compose YAML-Datei als benutzerdefiniert Vorlage in den Container für vRealize Automation verwenden.

Wenn Sie eine YAML-Datei verwenden, geben Sie den Inhalt der YAML-Datei als Text ein oder navigieren Sie zur YAML-Datei und laden Sie sie hoch. Die YAML-Datei repräsentiert die Vorlage, die Konfiguration für die verschiedenen Container und ihre Verbindungen. Die unterstützten Formattypen sind Docker Compose YAML und Container für vRealize Automation YAML.

Container für vRealize Automation YAML ähnelt Docker Compose, verwendet aber das YAML-Format des vRealize Automation-Blueprints, das in der vRealize Automation REST-API oder in vRealize CloudClient sichtbar ist. Mithilfe der Container für vRealize Automation-YAML können Sie vorhandene Docker Compose-Anwendungen importieren und sie mithilfe von Container ändern, bereitstellen und verwalten.

Voraussetzungen

- Stellen Sie sicher, dass Container für vRealize Automation in Ihrer unterstützten vRealize Automation-Bereitstellung aktiviert ist.
- Melden Sie sich bei vRealize Automation als **Containeradministrator** an.

Weitere Informationen zu dem von den vRealize Automation-Dienst-REST APIs verwendeten YAML-Format finden Sie unter *Referenz für vRealize Automation-API*.

Verfahren

1 Klicken Sie auf die Registerkarte **Container**.

2 Wählen Sie im linken Bereich **Bibliothek > Vorlagen** aus.

In einer Liste werden die zur Bereitstellung verfügbaren Vorlagen und Images angezeigt.

- Konfigurierte Vorlagen in der Ansicht „Images“.
- Vorhandene oder benutzerdefinierte Vorlagen in der Ansicht **Vorlage**.
- Alle basierend auf Ihren angegebenen Registrierungen in der Ansicht **Alle** verfügbaren Vorlagen und Images.

Die Optionen **Importieren** und **Exportieren** sind ebenfalls für den Import oder Export von Vorlagen und Images verfügbar.

3 Klicken Sie auf das Symbol **Vorlage oder Docker Compose importieren**.

Die Seite „Vorlage importieren“ wird angezeigt.

4 Geben Sie den Inhalt der YAML-Datei an.

Option	Beschreibung
Laden aus Datei	Klicken Sie auf Laden aus Datei , um zum Verzeichnis mit der YAML-Datei zu navigieren und diese auszuwählen.
Vorlage oder Docker Compose eingeben	Geben Sie den Inhalt einer ordnungsgemäß formatierten YAML-Datei im Textfeld Vorlage oder Docker Compose eingeben ein.

5 Klicken Sie auf **Importieren**.

Die neue Vorlage wird in der Ansicht **Vorlagen** angezeigt.

Bereitstellen eines Containers von einer Vorlage oder einem Image aus

Sie können in Ihrer Vorlagenansicht einen Container von einer Vorlage oder einem Image aus bereitstellen.

Beim Bereitstellungsprozess wird basierend auf den Konfigurationseinstellungen in der Vorlage oder dem Image, von der bzw. dem aus Sie die Bereitstellung durchführen, ein Container erstellt.

Sie können einen Container von einer Vorlage oder einem Image aus bereitstellen, indem Sie entweder vorhandene Konfigurationseinstellungen verwenden oder Konfigurationseinstellungen bearbeiten und anschließend bereitstellen.

Sie können auch Konfigurationseinstellungen bearbeiten und speichern, um eine neue, benutzerdefinierte Containervorlage oder ein Image zu erstellen.

Voraussetzungen

- Stellen Sie sicher, dass Container für vRealize Automation in Ihrer unterstützten vRealize Automation-Bereitstellung aktiviert ist.
- Melden Sie sich bei vRealize Automation als **Containeradministrator** an.

Verfahren

- 1 Klicken Sie auf die Registerkarte **Container**.
- 2 Wählen Sie im linken Bereich **Bibliothek > Vorlagen** aus.

In einer Liste werden die zur Bereitstellung verfügbaren Vorlagen und Images angezeigt.

- Konfigurierte Vorlagen in der Ansicht „Images“.
- Vorhandene oder benutzerdefinierte Vorlagen in der Ansicht **Vorlage**.
- Alle basierend auf Ihren angegebenen Registrierungen in der Ansicht **Alle** verfügbaren Vorlagen und Images.

Die Optionen **Importieren** und **Exportieren** sind ebenfalls für den Import oder Export von Vorlagen und Images verfügbar.

- 3 Verwenden Sie die Ansichtsoptionen **Alle**, **Images** bzw. **Vorlagen**, um das bereitzustellende Image bzw. die bereitzustellende Vorlage bereitzustellen.
- 4 Die Vorlage bzw. das Image bereitstellen

Option	Beschreibung
Bereitstellen anhand vorhandener Einstellungen	<ol style="list-style-type: none"> a Klicken Sie auf Bereitstellen. <p>In der Ansicht „Bereitstellungsanforderungen“ werden Informationen über den Erfolg der Bereitstellung angezeigt.</p>
Bereitstellen durch Bearbeiten von Einstellungen	<ol style="list-style-type: none"> a Klicken Sie auf den Pfeil neben der Schaltfläche Bereitstellen. b Klicken Sie auf Zusätzliche Informationen eingeben. c Geben Sie im Formular Bereitstellen eines Containers die Zusatzinformationen für den Behälter ein. d Sobald Sie die Informationen in das Formular eingegeben haben, klicken Sie auf Bereitstellen, um die Bereitstellung anhand der geänderten Einstellungen durchzuführen. e Klicken Sie auf Als Vorlage speichern, um Ihre Änderungen als neue Containervorlage in Container für vRealize Automation zu speichern. <p>In der Ansicht „Bereitstellungsanforderungen“ werden Informationen über den Erfolg der Bereitstellung angezeigt.</p>

Exportieren einer Containervorlage oder Docker Compose-Datei

Sie können eine Containervorlage als Docker Compose YAML-Datei oder als Container für vRealize Automation YAML-Datei exportieren.

Sie können eine Vorlage importieren und sie unter Verwendung der vRealize Automation REST-API oder von vRealize CloudClient per Programmierung oder grafisch in Container ändern. Sie können dann die geänderte Datei exportieren. Sie können z. B. in das Docker Compose-Format importieren und in das Blueprint-YAML-Format exportieren, das in der vRealize Automation Composition-Service-API verwendet wird. Manche Container-spezifischen Konfigurationen, z. B. Systemzustandskonfiguration und Affinitätseinschränkungen, werden jedoch nicht aufgenommen, wenn Sie die Vorlage im Docker Compose-Format exportieren.

Voraussetzungen

- Stellen Sie sicher, dass Container für vRealize Automation in Ihrer unterstützten vRealize Automation-Bereitstellung aktiviert ist.
- Melden Sie sich bei vRealize Automation als **Containeradministrator** an.

Weitere Informationen zu dem von den vRealize Automation-Dienst-REST APIs verwendeten YAML-Format finden Sie unter *Referenz für vRealize Automation-API*.

Verfahren

- 1 Klicken Sie auf die Registerkarte **Container**.

- 2 Wählen Sie im linken Bereich **Bibliothek > Vorlagen** aus.

In einer Liste werden die zur Bereitstellung verfügbaren Vorlagen und Images angezeigt.

- Konfigurierte Vorlagen in der Ansicht „Images“.
- Vorhandene oder benutzerdefinierte Vorlagen in der Ansicht **Vorlage**.
- Alle basierend auf Ihren angegebenen Registrierungen in der Ansicht **Alle** verfügbaren Vorlagen und Images.

Die Optionen **Importieren** und **Exportieren** sind ebenfalls für den Import oder Export von Vorlagen und Images verfügbar.

- 3 Zeigen Sie auf eine Vorlage und klicken Sie auf das Symbol **Exportieren**.

- 4 Wählen Sie einen Ausgabeformattyp aus, wenn Sie dazu aufgefordert werden:

- **YAML-Blueprint**

Dieses Format hält sich an das Blueprint-YAML-Format, das in der vRealize Automation Composition-Service-API verwendet wird.

- **Docker Compose**

Dieses Format hält sich an das in der Docker Compose-Anwendung verwendete YAML-Format.

- 5 Klicken Sie auf **Exportieren**.

- 6 Speichern Sie die Datei oder öffnen Sie sie in einer entsprechenden Anwendung, wenn Sie dazu aufgefordert werden.

Verwenden von Containerregistrierungen

Eine Docker-Registrierung ist eine statusfreie, serverseitige Anwendung. Sie können Registrierungen in Container für vRealize Automation verwenden, um Docker-Images zu speichern und zu verteilen.

Um eine Registrierung zu konfigurieren, müssen Sie deren Adresse, einen benutzerdefinierten Registrierungsnamen und optional die Anmeldedaten angeben. Die Adresse muss mit HTTP oder HTTPS beginnen, um anzugeben, ob die Registrierung geschützt oder ungeschützt ist. Falls der Verbindungstyp nicht angegeben ist, wird standardmäßig HTTPS verwendet.

Hinweis Für HTTP müssen Sie Port 80 und für HTTPS Port 443 angeben. Wenn kein Port angegeben ist, erwartet die Docker-Engine Port 5000, was zu Verbindungstrennungen führen kann.

Hinweis Es wird empfohlen, keine HTTP-Registrierungen zu verwenden, da HTTP als ungeschützt betrachtet wird. Wenn Sie HTTP verwenden möchten, müssen Sie die `DOCKER_OPTS`-Eigenschaft wie folgt auf jedem Host ändern:

```
DOCKER_OPTS="--insecure-registry myregistrydomain.com:5000".
```

Weitere Informationen finden Sie in der Docker-Dokumentation unter <https://docs.docker.com/registry/insecure/>.

Container kann mit den Docker-Registrierungen HTTP API V1 und V2 in der folgenden Weise interagieren:

V1 über HTTP (ungeschützt, einfache HTTP-Registrierung)

Sie können diese Art von Registrierung frei durchsuchen, aber Sie müssen jeden Docker-Host manuell mit dem `--insecure-registry`-Flag konfigurieren, um Container auf Basis von Images aus ungeschützten Registrierungen bereitzustellen. Sie müssen nach Einstellen der Eigenschaft den Docker-Daemon neu starten.

V1 über HTTPS

Kann hinter einem Reverse Proxy wie z. B. NGINX, verwendet werden. Die Standardimplementierung steht als Open Source unter <https://github.com/docker/docker-registry> zur Verfügung.

V2 über HTTPS

Die Standardimplementierung steht als Open Source unter <https://github.com/docker/distribution> zur Verfügung.

V2 über HTTPS mit Standardauthentifizierung

Die Standardimplementierung steht als Open Source unter <https://github.com/docker/distribution> zur Verfügung.

V2 über HTTPS mit Authentifizierung über einen zentralen Dienst

Sie können eine Docker-Registrierung im eigenständigen Modus ausführen, bei dem keine Autorisierungsprüfungen durchgeführt werden. Unterstützte Drittanbieterregistrierungen sind JFrog Artifactory und Harbor. Docker Hub wird standardmäßig für alle Mandanten aktiviert und ist nicht in der Registrierungsliste vorhanden, kann aber mit einer Systemeigenschaft deaktiviert werden.

Hinweis Docker interagiert normalerweise nicht mit sicheren Registrierungen, die mit Zertifikaten konfiguriert wurden, die von einer unbekannten Zertifizierungsstelle signiert wurden. Der Containerdienst behandelt diesen Fall so, dass er automatisch nicht vertrauenswürdige Zertifikate auf alle Docker-Hosts hochlädt und den Hosts ermöglicht, zu diesen Registrierungen eine Verbindung herzustellen. Wenn ein Zertifikat nicht auf einen angegebenen Host hochgeladen werden kann, wird der Host automatisch deaktiviert.

Erstellen und Verwalten von Containerregistrierungen

Sie können mehrere Registrierungen konfigurieren, um Zugriff auf öffentliche und private Images zu erhalten.

Registrierungen sind öffentliche oder private Speicher, zu denen bzw. von denen Sie Images hoch- bzw. herunterladen können. Sie können die von Ihnen erstellten Registrierungen deaktivieren, bearbeiten oder deaktivieren. Die auf der Registerkarte **Vorlagen** angezeigten Images basieren auf den von Ihnen definierten Registrierungen.

Wenn Sie auf der Seite „Vorhandene Registrierungen“ Registrierungen erstellen oder verwalten, können Sie auf die Schaltflächen **Anmeldedaten** oder **Zertifikat** klicken, um Anmeldedaten und Zertifikate hinzuzufügen oder zu verwalten.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Containeradministrator** an.
- Stellen Sie sicher, dass mindestens ein Host konfiguriert und für die Container-Netzwerkconfiguration verfügbar ist.

Verfahren

- 1 Klicken Sie auf die Registerkarte **Container**.
- 2 Klicken Sie auf **Registrierungen**.
Die Seite mit den vorhandenen Registrierungen wird angezeigt.
- 3 Klicken Sie auf **+Registrierung**.
- 4 Geben Sie die Registrierungsadresse ein.
- 5 Geben Sie einen Namen für die Registrierung ein.
- 6 Wählen Sie Ihre Anmeldedaten aus der Dropdown-Liste aus.
- 7 (Optional) Klicken Sie auf **Überprüfen**, um die Gültigkeit der konfigurierten Parameter zu bestätigen.

8 Klicken Sie auf **Speichern**, um die Registrierung hinzuzufügen.

Konfigurieren von Netzwerkressourcen für Container

Sie können in der Container für vRealize Automation-Anwendung Netzwerkkonfigurationen erstellen, ändern und an Container und Containervorlagen anhängen.

Wenn Sie einen Container bereitstellen, ist die Netzwerkkonfiguration eingebettet und verfügbar. Sie können die Netzwerkeinstellungen für Containerkomponenten anpassen, die Sie einem vRealize Automation-Blueprint hinzugefügt haben.

Erstellen eines neuen Netzwerks für Container

Wenn eine geeignete Netzwerkkonfiguration nicht verfügbar ist, können Sie in vRealize Automation eine neue Konfiguration erstellen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Berechtigungen für die Rolle **Containeradministrator**, **Containerarchitekt** oder **IaaS-Administrator** verfügen.
- Stellen Sie sicher, dass mindestens ein Host konfiguriert und für die Container-Netzwerkkonfiguration verfügbar ist.

Verfahren

- 1** Melden Sie sich bei vRealize Automation an.
- 2** Klicken Sie auf die Registerkarte **Container**.
- 3** Wählen Sie im linken Bereich **Bereitstellungen > Netzwerke** aus.

Im Hauptbereich werden die vorhandenen Netzwerkkonfigurationen angezeigt, die als Teil der Containerbereitstellung bereitgestellt werden können. Die Netzwerkkonfigurationen enthalten beide Konfigurationen: diejenigen, die von den Docker-Hosts hinzugefügt wurden, und diejenigen, die in vRealize Automation erstellt wurden. Die Symbole, die die Netzwerkkonfigurationen abbilden, zeigen das Netzwerk und IPAM-Treiber, das Subnetz, das Gateway und IP-Bereichsinformationen, die Anzahl der Container, die die Netzwerkkonfiguration verwenden sowie die Anzahl der Hosts an.

- 4** Klicken Sie auf **+Netzwerk**.
- 5** Geben Sie einen Namen für das Netzwerk ein.

Sobald Sie die neue Konfiguration erstellt haben, wird am Namen eine eindeutige Kennung angehängt.

- 6** (Optional) Um detaillierte Konfigurationseinstellungen hinzuzufügen, aktivieren Sie das Kontrollkästchen **Erweitert**.

Im Bereich „Netzwerk hinzufügen“ werden weitere Einstellungen für die Netzwerkkonfiguration angezeigt.

7 Konfigurieren Sie die erweiterten Netzwerkkonfigurationseinstellungen.

Option	Beschreibung
IPAM-Konfiguration	<p>Subnetz</p> <p>Geben Sie Subnetz- und Gateway-Adressen ein, die für diese Netzwerkkonfiguration eindeutig sind. Diese Werte dürfen sich nicht mit anderen Netzwerken auf demselben Containerhost überschneiden.</p>
Benutzerdefinierte Eigenschaften	<p>Geben Sie wahlweise benutzerdefinierte Eigenschaften für die neue Netzwerkkonfiguration an.</p> <p>containers.ipam.driver</p> <p>Nur für die Verwendung mit Containern. Gibt den IPAM-Treiber an, der zu verwenden ist, wenn eine Container-Netzwerkkomponente zu einem Blueprint hinzugefügt wird. Welche Werte unterstützt werden, hängt von den Treibern ab, die in der Container-Hostumgebung installiert sind, in der sie verwendet werden. Ein unterstützter Wert wäre z. B. <code>infoblox</code> oder <code>calico</code>, je nachdem, welche IPAM-Plug-Ins auf dem Container-Host installiert sind.</p> <p>Bei diesem Eigenschaftsnamen und dem Wert wird die Groß-/Kleinschreibung beachtet. Beim Hinzufügen des Eigenschaftswerts wird dieser nicht überprüft. Wenn zur Bereitstellungszeit der angegebene Treiber nicht auf dem Container-Host vorhanden ist, wird eine Fehlermeldung ausgegeben und die Bereitstellung schlägt fehl.</p> <p>containers.network.driver</p> <p>Nur für die Verwendung mit Containern. Gibt den Netzwerktreiber an, der zu verwenden ist, wenn eine Container-Netzwerkkomponente zu einem Blueprint hinzugefügt wird. Welche Werte unterstützt werden, hängt von den Treibern ab, die in der Container-Hostumgebung installiert sind, in der sie verwendet werden. Standardmäßig gehören zu den von Docker bereitgestellten Netzwerktreibern Bridge-, Overlay- und Macvlan-Treiber, wobei bei den von Virtual Container Host (VCH) bereitgestellten Netzwerktreibern der Bridge-Treiber enthalten ist. Netzwerktreiber von Drittanbietern, wie z. B. <code>weave</code> und <code>calico</code>, stehen möglicherweise ebenfalls zur Verfügung, je nachdem, welche Netzwerk-Plug-Ins auf dem Container-Host installiert sind.</p> <p>Bei diesem Eigenschaftsnamen und dem Wert wird die Groß-/Kleinschreibung beachtet. Beim Hinzufügen des Eigenschaftswerts wird dieser nicht überprüft. Wenn zur Bereitstellungszeit der angegebene Treiber nicht auf dem Container-Host vorhanden ist, wird eine Fehlermeldung ausgegeben und die Bereitstellung schlägt fehl.</p>

Hinweis Wenn Sie das Netzwerk ohne erweiterte Einstellungen erstellen, stellt vRealize Automation die Einstellungen automatisch bereit.

- 8 Wählen Sie aus der Dropdown-Menü den Host aus, mit dem das Netzwerk verbunden werden soll.
- 9 Klicken Sie auf **Erstellen**.

Hinzufügen eines Netzwerks zu einer Containervorlage

Sie können einer Containervorlage eine Netzwerkkonfiguration hinzufügen, um die Container miteinander zu verbinden. Diese Netzwerkkonfiguration wird automatisch für alle Anwendungen implementiert, die die Vorlage verwenden. Sie können entweder ein vorhandenes Netzwerk hinzufügen oder ein neues Netzwerk konfigurieren und hinzufügen.

Voraussetzungen

- Stellen Sie sicher, dass eine Vorlage vorhanden ist. Ist dies nicht der Fall, müssen Sie eine Vorlage erstellen.
- Stellen Sie sicher, dass Sie über die Berechtigungen für die Rolle **Containeradministrator**, **Containerarchitekt** oder **IaaS-Administrator** verfügen.
- Stellen Sie sicher, dass mindestens ein Host konfiguriert und für die Container-Netzwerkkonfiguration verfügbar ist.

Verfahren

- 1 Melden Sie sich bei vRealize Automation an.
- 2 Klicken Sie auf die Registerkarte **Container**.
- 3 Klicken Sie im linken Bereich auf **Vorlagen**.

Mit einer Reihe von Symbolen werden die zur Bereitstellung verfügbaren Vorlagen und Images angezeigt.

- 4 (Optional) Ändern Sie die Ansicht, indem Sie in der oberen rechten Überschrift über den Symbolen auf **Ansicht: Vorlagen** klicken, um ausschließlich Vorlagen anzuzeigen.
- 5 Klicken Sie im oberen rechten Bereich der anzupassenden Vorlage auf **Bearbeiten**.

Die Seite „Vorlagen bearbeiten“ wird mit den Containersymbolen angezeigt (einschließlich eines leeren Symbols mit einem Pluszeichen).

- 6 Zeigen Sie auf das leere Symbol.
- 7 Klicken Sie auf das Symbol **Netzwerk hinzufügen**.

Der Bereich „Netzwerk hinzufügen“ wird angezeigt.

- 8 Fügen Sie ein vorhandenes Netzwerk hinzu oder erstellen Sie ein neues Netzwerk und fügen es hinzu.

Option	Beschreibung
Hinzufügen eines vorhandenen Netzwerks.	<ul style="list-style-type: none"> a Aktivieren Sie das Kontrollkästchen Vorhanden. b Klicken Sie in das Feld Name, um eine Liste mit den vorhandenen Netzwerken anzuzeigen. c Wählen Sie das Netzwerk aus, das Sie verwenden möchten, und klicken Sie auf Speichern.
Konfigurieren und Hinzufügen eines Netzwerks.	<ul style="list-style-type: none"> a Geben Sie einen Namen für das Netzwerk ein. b Um detaillierte Konfigurationseinstellungen hinzuzufügen, aktivieren Sie das Kontrollkästchen Erweitert. c Klicken Sie auf Speichern.

Der Bereich „Netzwerkconfiguration hinzufügen“ wird geschlossen, und das hinzugefügte Netzwerk wird als ein horizontales Symbol unterhalb der Containersymbole auf der Seite „Vorlage bearbeiten“ angezeigt. Zudem wird auch am unteren Rand der Containersymbole ein Netzwerksymbol angezeigt.

- 9 Verbinden Sie das Netzwerk mit einem Container, indem Sie das Netzwerkverbindungssymbol vom Container zu einer beliebigen Stelle des horizontalen Symbols ziehen, das das Netzwerk darstellt.

Konfigurieren von Volumes für Container

Sie können in der Container für vRealize Automation-Anwendung Volumes erstellen, ändern und an Container und Containervorlagen anhängen.

Container für vRealize Automation verwendet Docker-Volumes für die dauerhafte Datenverwaltung. Mit Volumes können Sie die folgenden Aufgaben durchführen:

- Volumes zwischen unterschiedlichen Containern innerhalb desselben Hosts freigeben.
- Daten sofort aktualisieren.
- Volumedaten nach dem Löschen des Containers speichern.

Erstellen eines neuen Volumes für Container

Wenn Sie Ihren Containerspeicher erweitern möchten, müssen Sie zunächst ein Datenvolume erstellen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Berechtigungen für die Rolle **Containeradministrator**, **Containerarchitekt** oder **IaaS-Administrator** verfügen.
- Stellen Sie sicher, dass mindestens ein Host konfiguriert und für die Container-Volume-Konfiguration verfügbar ist.

Verfahren

- 1 Melden Sie sich bei vRealize Automation an.
- 2 Klicken Sie auf die Registerkarte **Container**.
- 3 Wählen Sie im linken Bereich **Bereitstellungen > Volumes** aus.

Im Hauptfenster werden die vorhandenen Volume-Konfigurationen angezeigt, die mit den bereitgestellten Containern verknüpft werden können. Die Volume-Konfigurationen enthalten beide Konfigurationen: diejenigen, die von den Docker-Hosts hinzugefügt wurden, und diejenigen, die in vRealize Automation erstellt wurden. Die Volume-Instanzen zeigen den Treiber, den Umfang und die Treiberoptionen an.

- 4 Klicken Sie auf **+Volume**.
- 5 Geben Sie einen Namen für das Volume ein.

Sobald Sie die Konfiguration erstellt haben, wird an den Namen eine eindeutige Kennung angehängt.

- 6 Geben Sie in das Feld **Treiber** den Treiber des Volume-Plug-Ins ein, das Sie verwenden möchten. Wenn Sie keine Eingabe vornehmen, wird „local“ als Standardwert verwendet.
- 7 (Optional) Um detaillierte Konfigurationseinstellungen hinzuzufügen, aktivieren Sie das Kontrollkästchen **Erweitert**.

Zusätzliche Konfigurationseinstellungen werden angezeigt.

- 8 (Optional) Konfigurieren Sie die erweiterten Volumeeinstellungen.

Option	Beschreibung
Treiberoptionen	Geben Sie die Treiberoptionen an, die Sie verwenden möchten. Die Optionen hängen von dem von Ihnen verwendeten Volume-Plug-In ab.
Benutzerdefinierte Eigenschaften	Geben Sie benutzerdefinierte Eigenschaften für die neue Konfiguration an.

- 9 Wählen Sie im Dropdown-Menü den Host aus, mit dem das Volume verbunden werden soll.
- 10 Klicken Sie auf **Erstellen**.
Der Bereich „Volume erstellen“ wird geschlossen, und das hinzugefügte Volume wird auf der Registerkarte „Volumes“ angezeigt.

Nächste Schritte

[Hinzufügen eines Volumes zu einer Containervorlage](#)

Hinzufügen eines Volumes zu einer Containervorlage

Verbinden Sie ein Volume mit einem Container, indem Sie es zu einer Vorlage hinzufügen.

Voraussetzungen

- Stellen Sie sicher, dass eine Vorlage vorhanden ist. Ist dies nicht der Fall, müssen Sie eine Vorlage erstellen.

- Stellen Sie sicher, dass Sie über die Berechtigungen für die Rolle **Containeradministrator**, **Containerarchitekt** oder **IaaS-Administrator** verfügen.
- Stellen Sie sicher, dass mindestens ein Host konfiguriert und für die Container-Volume-Konfiguration verfügbar ist.

Verfahren

- 1 Melden Sie sich bei vRealize Automation an.
- 2 Klicken Sie auf die Registerkarte **Container**.
- 3 Klicken Sie im linken Bereich auf **Vorlagen**.

Mit einer Reihe von Symbolen werden die zur Bereitstellung verfügbaren Vorlagen und Images angezeigt.

- 4 (Optional) Ändern Sie die Ansicht, indem Sie in der oberen rechten Überschrift über den Symbolen auf **Ansicht: Vorlagen** klicken, um ausschließlich Vorlagen anzuzeigen.
- 5 Klicken Sie im oberen rechten Bereich der anzupassenden Vorlage auf **Bearbeiten**.
Die Seite „Vorlagen bearbeiten“ wird mit den Containersymbolen angezeigt (einschließlich eines leeren Symbols mit einem Pluszeichen).
- 6 Bewegen Sie den Mauszeiger so lange über das leere Symbol mit dem Pluszeichen, bis das Symbol **Volume hinzufügen** angezeigt wird.
- 7 Klicken Sie auf das Symbol **Volume hinzufügen**.
- 8 Fügen Sie ein vorhandenes Volume hinzu oder erstellen Sie ein neues Volume und fügen es hinzu.

Option	Beschreibung
Hinzufügen eines vorhandenen Volumes.	<ol style="list-style-type: none"> a Aktivieren Sie das Kontrollkästchen Vorhanden. b Klicken Sie in das Feld Name, um eine Liste mit vorhandenen Volumens anzuzeigen. c Wählen Sie das gewünschte Volume aus und klicken Sie auf Speichern.
Konfigurieren und Hinzufügen eines neuen Volumes.	<ol style="list-style-type: none"> a Geben Sie einen Namen für das Volume ein. b Geben Sie in das Feld Treiber den Treiber des Volume-Plug-Ins ein, das Sie verwenden möchten. Wenn Sie kein externes Speichersystem verwenden, geben Sie local ein. c Um detaillierte Konfigurationseinstellungen hinzuzufügen, aktivieren Sie das Kontrollkästchen Erweitert. d Klicken Sie auf Speichern.

Der Bereich „Volume hinzufügen“ wird geschlossen und das hinzugefügte Volume wird als ein horizontales Symbol unterhalb der Containersymbole auf der Seite „Vorlage bearbeiten“ angezeigt. Ein Volumesymbol wird auch am unteren Rand der Containersymbole angezeigt.

- 9 Verbinden Sie das Volume mit einem Container, indem Sie das Volume-Connector-Symbol aus dem Container an einen beliebigen Punkt auf dem horizontalen Symbol ziehen, das das Volume darstellt.

- 10** (Optional) Klicken Sie auf den Containerpfad, um den Speicherort zu ändern, an dem das Volume gemountet wird.

Nächste Schritte

[Bereitstellen eines Containers von einer Vorlage oder einem Image aus](#)

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 für die 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 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.

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.

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.

Verfahren

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 bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 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
ID	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.
Beschreibung	Die Beschreibung der Richtlinie.
Active Directory-Endpoint	Wählen Sie den Active Directory-Endpoint aus, für den diese Richtlinie erstellt wird.
Domäne	Geben Sie die Root-Domäne ein. Format: <i>meinunternehmen.com</i> .
Organisationseinheit	Geben Sie den definierten Namen der Organisationseinheit für diese Richtlinie ein. Die Hierarchie muss in Form einer kommasetrennten Liste eingegeben werden. Beispiel: <i>ou=development,dc=corp,dc=domain,dc=com</i> .

- 4 Klicken Sie auf **OK**.

Ergebnisse

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.

Nächste Schritte

- 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.

Verfahren

- 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**.

Ergebnisse

Der Test-Blueprint enthält die benutzerdefinierte Eigenschaft. Die benutzerdefinierte Eigenschaft wird den Benutzern im Anforderungsformular jedoch nicht angezeigt.

Nächste Schritte

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.

Benutzereinstellungen für Benachrichtigungen und Stellvertretungen

Sie verwenden die Benutzereinstellung, um die Standardkonfiguration für Ihre Systemgenehmigerbenachrichtigungen sowie die Spracheinstellungen für Ihre Benachrichtigungen einzeln zu überschreiben.

Klicken Sie in der Symbolleiste neben Ihrem Namen auf **Einstellungen**, um auf die Benutzereinstellungen zuzugreifen.

Die folgenden Optionen sind spezifisch für Sie als angemeldeter Benutzer.

Tabelle 2-21. Optionen für Benutzereinstellungen

Option	Beschreibung
Stellvertretungen zuweisen	Ermöglicht Ihnen, Ihre Genehmigungsanforderungen an andere Benutzer neu zuzuweisen. Angenommen, Sie sind ein Genehmiger von Kataloganforderungen und Ihr Urlaub steht kurz bevor. Sie delegieren Ihre gesamten Genehmigungsbenachrichtigungen an mindestens einen Genehmiger. Diese Zuweisung leitet die Anforderungen sofort an Ihre Stellvertretung weiter. Die Stellvertretungen sind so lange aktiv, bis Sie sie aus der Liste entfernen.
Benachrichtigungen	Ermöglicht Ihnen, Ihre Benachrichtigungssprache so zu ändern, dass Ihnen die E-Mail-Nachrichten nicht in der Standardsprache, sondern in der Sprache Ihrer Wahl gesendet werden. Wählen Sie eine Sprache aus und fügen Sie das Benachrichtigungsabonnement hinzu, das Ihre bevorzugte Sprache unterstützt.

Bereitstellen von Dienst-Blueprints für Benutzer

3

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 enthält die folgenden Themen:

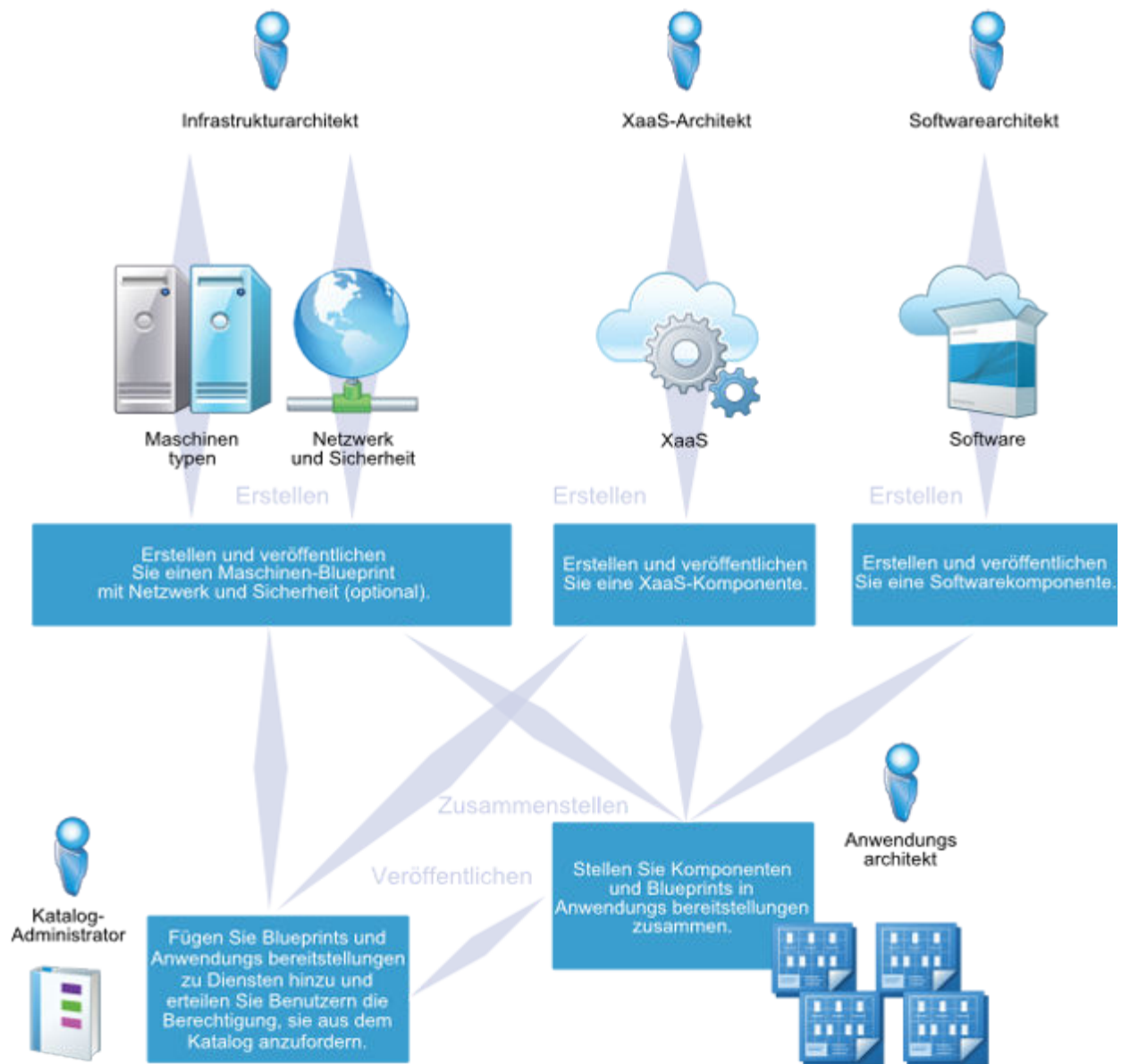
- [Entwerfen von Blueprints](#)
- [Erstellen Ihrer Design-Bibliothek](#)
- [Arbeiten mit von Entwicklern gesteuerten Blueprints](#)
- [Erstellen zusammengesetzter Blueprints](#)
- [Anpassen von Blueprint-Anforderungsformularen](#)
- [Verwalten des Servicekatalogs](#)
- [Verwalten von bereitgestellten Katalogelementen](#)

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. Der Katalog kann ein Standard-Anforderungsformular anzeigen, oder Sie können ein benutzerdefiniertes Formular für jeden veröffentlichten Blueprint erstellen.

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. Siehe [Entwerfen von Software-Komponenten](#).

Maschinen-Blueprints

Sie können einfache Blueprints erstellen und veröffentlichen, um einzelne Maschinen bereitzustellen, oder Sie können komplexere Blueprints erstellen, die zusätzliche Maschinenkomponenten und ggf. eine beliebige Kombination der folgenden Komponententypen enthalten:

- Software-Komponenten
- Vorhandene Blueprints
- NSX-Netzwerk und Sicherheitskomponenten
- XaaS-Komponenten
- Container-Komponenten
- Benutzerdefinierte oder andere Komponenten

Siehe [Entwerfen von Maschinen-Blueprints](#).

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. Siehe [Entwerfen von XaaS-Blueprints und Ressourcenaktionen](#).

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.

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.

Hinweis: Sie finden Beispiel-Blueprints auf VMware Solution Exchange unter <https://solutionexchange.vmware.com> und <https://code.vmware.com>.

Tabelle 3-1. Erstellen Ihrer Design-Bibliothek

Katalogelement	Rolle	Komponenten	Beschreibung	Details
Maschinen	Infrastrukturarchitekt	Erstellen Sie Maschinen-Blueprints auf der Registerkarte Blueprints .	<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>	Konfigurieren eines Maschinen-Blueprints
NSX-Netzwerk und Sicherheit auf Maschinen	Infrastrukturarchitekt	Fügen Sie NSX-Netzwerk- und Sicherheitskomponenten zu vSphere-Maschinen-Blueprints auf der Registerkarte Blueprints 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>	Entwerfen von Blueprints mit NSX-Einstellungen

Tabelle 3-1. Erstellen Ihrer Design-Bibliothek (Fortsetzung)

Katalogelement	Rolle	Komponenten	Beschreibung	Details
Software auf Maschinen	Softwarearchitekt Um Softwarekomponenten erfolgreich zur Design-Arbeitsfläche hinzuzufügen, müssen Sie Zugriff als Business-Gruppenmitglied, Business-Gruppenmanager oder Mandantenadministrator auf den Zielkatalog haben.	Erstellen und veröffentlichen Sie Software-Komponenten auf der Registerkarte Software . Kombinieren Sie diese anschließend mit Maschinen-Blueprints auf der Registerkarte Blueprints .	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. 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.	Erstellen einer Software-Komponente

Tabelle 3-1. Erstellen Ihrer Design-Bibliothek (Fortsetzung)

Katalogelement	Rolle	Komponenten	Beschreibung	Details
Benutzerdefinierte IT-Dienste	XaaS-Architekten	Erstellen und veröffentlichen Sie XaaS-Blueprints auf der Registerkarte XaaS .	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 Blueprints kombinieren, um ausgefeiltere Katalogelemente zu erstellen.	Entwerfen von XaaS-Blueprints und Ressourcenaktionen
Zusammenfügen von veröffentlichten Blueprint-Bausteinen in neuen Katalogelementen	<ul style="list-style-type: none"> ■ Anwendungsarchitekt ■ Infrastrukturarchitekt ■ Softwarearchitekt 	Kombinieren Sie auf der Registerkarte Blueprints 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.	Erstellen zusammengesetzter Blueprints

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.

Nachfolgend finden Sie einen allgemeinen Überblick über die erforderlichen Schritte für die Bereitstellung von Maschinen, die die FlexClone-Technologie verwenden:

- 1 Ein IaaS-Administrator erstellt einen NetApp ONTAP-Endpoint. Siehe [Endpoint-Einstellungen – Referenz](#).
- 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. Siehe [Erstellen einer Reservierung für Hyper-V, KVM, SCVMM, vSphere oder XenServer](#).
- 4 Ein Infrastrukturarchitekt oder ein anderer autorisierter Benutzer erstellt einen Blueprint für die FlexClone-Bereitstellung.

Verstehen und Verwenden der Blueprint-Parametrisierung

Sie können Komponentenprofile verwenden, um Blueprints zu parametrisieren. Statt einen separaten kleinen, mittleren und großen Blueprint für einen bestimmten Bereitstellungstyp zu erstellen, können Sie einen einzelnen Blueprint mit einer kleinen, mittleren oder großen virtuellen Maschine erstellen. Benutzer können eine dieser Größen auswählen, wenn sie das Katalogelement bereitstellen.

Komponentenprofile minimieren die Blueprint-Ausbreitung und vereinfachen Ihre Katalogangebote. Sie können Komponentenprofile verwenden, um vSphere-Maschinenkomponenten in einem Blueprint zu definieren. Die verfügbaren Komponentenprofiltypen sind *Size* und *Image*. Wenn Sie einer Maschinenkomponente Komponentenprofile hinzufügen, setzen die Komponentenprofileinstellungen die übrigen Einstellungen für die Maschinenkomponente, beispielsweise die Anzahl der CPUs oder die Speichermenge, außer Kraft.

Komponentenprofile sind nur für vSphere-Maschinenkomponenten verfügbar.

Informationen zum Definieren von Wertsätzen für die Komponentenprofile *Size* und *Image* finden Sie unter *Referenz für benutzerdefinierte Eigenschaften*

Informationen zum Hinzufügen von Komponentenprofilen und ausgewählten Wertsätzen für eine vSphere-Maschinenkomponente in einem Blueprint finden Sie unter [vSphere-Maschinenkomponenteneinstellungen](#).

Weitere Informationen zum Hinzufügen von Komponentenprofilinformationen mithilfe von Einstellungen, die aus einer OVF-Datei importiert wurden, finden Sie unter [Konfigurieren eines bereitzustellenden Blueprints in einer OVF-Datei](#).

Informationen zum Verwenden von Komponentenprofilen beim Anfordern der Maschinenbereitstellung finden Sie unter [Anfordern der Maschinenbereitstellung mit einem parametrisierten Blueprint](#).

Hinweis Sie können Genehmigungsrichtlinien erstellen, sodass eine Vorabgenehmigung erforderlich ist, wenn die Maschinenbereitstellung von Blueprints bezüglich Wertsatzbedingungen für die Komponentenprofile *Size* und *Image* angefordert wird. Weitere Informationen finden Sie unter [Beispiele für Genehmigungsrichtlinien basierend auf dem VM-Richtlinientyp](#).

Informationen zur Verwendung der Blueprint-Parametrisierung beim Anfordern der Maschinenbereitstellung aus dem Katalog finden Sie unter [Anfordern der Maschinenbereitstellung mit einem parametrisierten Blueprint](#).

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.

Diese Vorgehensweise bietet eine einfache Übersicht über das Erstellen eines Blueprints. Zusätzliche Details finden Sie hier:

- [Entwerfen von Blueprints mit NSX-Einstellungen](#)
- [Verstehen und Verwenden der Blueprint-Parametrisierung](#)
- [Konfigurieren eines bereitzustellenden Blueprints in einer OVF-Datei](#)
- [Exportieren und Importieren von Blueprints und Inhalten](#)
- [Erstellen von Microsoft Azure-Blueprints und Integrieren von Ressourcenaktionen](#)
- [Erstellen von Puppet-fähigen vSphere-Blueprints](#)

Voraussetzungen

- Melden Sie sich bei vRealize Automation 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 den Mandanten. Siehe [Konfigurieren der Mandanteneinstellungen](#).

- Konfigurieren Sie Ihre IaaS-Ressourcen. Siehe [Checkliste für die Konfiguration von IaaS-Ressourcen](#).
- Siehe *Konfigurieren von vRealize Automation*.

Verfahren

- 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**.

Ergebnisse

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.

Nächste Schritte

Sie können einen Maschinen-Blueprint mit Softwarekomponenten, XaaS-Blueprints oder zusätzlichen Maschinen-Blueprints kombinieren, um ausgefeiltere Anwendungs-Blueprints zu erstellen. Siehe [Erstellen zusammengesetzter Blueprints](#) und [Grundlegendes zum Verhalten von verschachtelten Blueprints](#).

Einstellungen für Maschinen-Blueprints

Sie können die Konfigurationseinstellungen und benutzerdefinierten Eigenschaften für den gesamten Blueprint definieren.

Blueprint-Eigenschaftseinstellungen

Beim Erstellen des Blueprints können Sie über die Seite **Blueprint-Eigenschaften** Einstellungen festlegen, die für den gesamten Blueprint gelten. Nach dem Erstellen des Blueprints können Sie diese Eigenschaften auf der Seite „Blueprint-Eigenschaften“ bearbeiten.

Registerkarte **Allgemein**

Wenden Sie Einstellungen auf den gesamten Blueprint an, einschließlich aller Komponenten, die Sie jetzt oder später hinzufügen möchten.

Tabelle 3-2. Einstellungen auf der Registerkarte **Allgemein**

Einstellung	Beschreibung
Name	Geben Sie einen Namen für Ihren Blueprint ein.
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.
Beschreibung	Eine Zusammenfassung Ihres Blueprints für andere Architekten. Diese Beschreibung wird Benutzern auch im Anforderungsformular angezeigt.
Bereitstellungsgrenzwert	Geben Sie die maximale Anzahl an Bereitstellungen an, die erstellt werden können, wenn dieser Blueprint zur Bereitstellung von Maschinen verwendet wird.
Leasetage: Mindestwert und Maximalwert	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. Wenn Sie keinen Mindestwert bzw. Maximalwert eingeben, ist die Leasedauer unbegrenzt.
Archivierung (Tage)	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.
Updates an vorhandene Bereitstellungen weitergeben	<p>Wenn diese Option aktiviert ist, wird festgelegt, dass jede Erweiterung der Grenzwerte, die Sie für Mindest- oder Maximaleinstellungen für CPU, Arbeitsspeicher und Speicher im Blueprint vornehmen, auf alle aktiven Bereitstellungen übertragen wird, die über den Blueprint bereitgestellt wurden. Wenn Sie beispielsweise ein Minimum von 2 und ein Maximum von 4 (2,4) angeben, würde eine Änderung wie (1,4) oder (2,5) bei einer Neukonfiguration wirksam werden, eine Änderung von (3,4) oder (2,3) jedoch nicht.</p> <p>Die Änderungen werden bei der nächsten Neukonfigurationsaktion wirksam. Weitere Informationen zu Neukonfigurationsaktionen finden Sie unter Befehle im Menü „Aktion“ für bereitgestellte Ressourcen.</p>

Registerkarte NSX-Einstellungen

Wenn Sie NSX konfiguriert haben, können Sie beim Erstellen oder Bearbeiten eines Blueprints Einstellungen für NSX-Transportzonen, Reservierungsrichtlinien für Edge und das geroutete Gateway sowie Anwendungsisolierungen angeben. Diese Einstellungen sind auf der Registerkarte **NSX-Einstellungen** auf den Seiten **Blueprint** und **Blueprint-Eigenschaften** verfügbar.

Informationen zu NSX-Einstellungen finden Sie unter [Neue Blueprint- und Blueprint-Eigenschaftsseiteneinstellungen 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 3-3. Einstellungen auf der Registerkarte Eigenschaften

Registerkarte	Einstellung	Beschreibung
Eigenschaftsgruppen		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.
	Hinzufügen	Fügen Sie eine oder mehrere vorhandene Eigenschaftsgruppen hinzu und weisen Sie diese dem gesamten Blueprint zu. Die folgenden Eigenschaftsgruppen im Zusammenhang mit Containern werden angegeben: <ul style="list-style-type: none"> ■ Container-Hosteigenschaften mit Zertifikatsauthentifizierung ■ Container-Hosteigenschaften mit Benutzer-/Kennwortauthentifizierung
	Nach oben verschieben/Nach unten verschieben	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.
	Eigenschaften anzeigen	Zeigen Sie die benutzerdefinierten Eigenschaften in der ausgewählten Eigenschaftsgruppe an.

Tabelle 3-3. Einstellungen auf der Registerkarte **Eigenschaften** (Fortsetzung)

Registerkarte	Einstellung	Beschreibung
	Zusammengeführte Eigenschaften anzeigen	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.
Benutzerdefinierte Eigenschaften	Anstelle von Eigenschaftsgruppen können Sie auch einzelne benutzerdefinierte Eigenschaften hinzufügen.	
	Neu	Fügen Sie eine einzelne benutzerdefinierte Eigenschaft hinzu und wenden Sie diese auf den gesamten Blueprint an.
	Name	Eingabe des Eigenschaftsnamens. Eine Liste der benutzerdefinierten Eigenschaften und deren Definitionen finden Sie unter <i>Referenz für benutzerdefinierte Eigenschaften</i> .
	Wert	Geben Sie den Wert für die benutzerdefinierte Eigenschaft ein.
	Verschlüsselt	Sie können den Eigenschaftswert verschlüsseln. Beispielsweise für den Fall, dass es sich bei dem Wert um ein Kennwort handelt.
	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.

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 3-4. Einstellungen auf der Registerkarte Allgemein

Einstellung	Beschreibung
ID	Geben Sie einen Namen für Ihre Maschinenkomponente ein oder übernehmen Sie den Standardwert.
Beschreibung	Eine Zusammenfassung Ihrer Maschinenkomponente für andere Architekten.
Speicherort auf Anforderung anzeigen	<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 Datencenter-Standorts, an dem eine angeforderte Maschine bereitgestellt werden soll, erlaubt wird. Für die vollständige Konfiguration dieser Option fügt ein Systemadministrator Informationen zum Datencenter-Standort zu einer Standortdatei hinzu und ein Fabric-Administrator bearbeitet eine Computing-Ressource, um sie einem Standort zuzuordnen.</p>
Reservierungsrichtlinie	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. Es sind nur die für den aktuellen Mandanten geltenden Reservierungsrichtlinien verfügbar.

Tabelle 3-4. Einstellungen auf der Registerkarte **Allgemein** (Fortsetzung)

Einstellung	Beschreibung
Maschinenpräfix	<p>Maschinenpräfixe werden von Fabric-Administratoren erstellt und zum Erstellen der Namen von bereitgestellten Maschinen verwendet. Wenn Sie Gruppenstandardwert verwenden 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. Es sind nur die für den aktuellen Mandanten geltenden Maschinenpräfixe verfügbar.</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>
Instanzen: Mindestwert und Maximalwert	<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 Minimalwert und Maximalwert 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 3-5. Registerkarte **Build-Informationen**

Einstellung	Beschreibung
Blueprint-Typ	Wählen Sie zu Statistik- und Lizenzierungszwecken aus, ob über diesen Blueprint bereitgestellte Maschinen als „Desktop“ oder „Server“ klassifiziert werden.
Aktion	<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"> ■ Erstellen <p>Erstellt die Spezifikation der Maschinenkomponente ohne die Verwendung einer Klon-Option.</p> ■ Klonen <p>Erstellt Kopien einer virtuellen Maschine anhand einer Vorlage und eines Anpassungsobjekts.</p> ■ Verknüpfter Klon <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> <p>Der im Blueprint angegebene VM-Snapshot sollte vor der Bereitstellung der verknüpften Klon-VMs ausgeschaltet werden.</p> ■ NetApp FlexClone <p>Wenn Ihre Fabric-Administratoren für Ihre Reservierungen die Verwendung von NetApp FlexClone-Speicher konfiguriert haben, können Sie mithilfe dieser Technologie speicherplatzeffiziente Kopien von Maschinen klonen.</p>

Tabelle 3-5. Registerkarte **Build-Informationen** (Fortsetzung)

Einstellung	Beschreibung
Bereitstellungsworkflow	<p data-bbox="810 268 1326 352">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="810 369 1043 390">■ BasicVmWorkflow <p data-bbox="847 415 1394 436">Stellt eine Maschine ohne Gastbetriebssystem bereit.</p> <li data-bbox="810 453 1171 474">■ ExternalProvisioningWorkflow <p data-bbox="847 499 1369 552">Erstellt eine Maschine durch Starten über eine VM-Instanz oder ein Cloud-basiertes Image.</p> <li data-bbox="810 569 1062 590">■ ImportOvfWorkflow <p data-bbox="847 615 1422 863">Ermöglicht Ihnen das Bereitstellen einer virtuellen vSphere-Maschine unter Verwendung einer OVF-Vorlage in derselben Weise wie ein CloneWorkflow Ihnen das Bereitstellen einer virtuellen vSphere-Maschine über eine VM-Vorlage ermöglicht. Sie können eine vSphere-Komponente in einen Maschinen-Blueprint oder in ein Image-Komponentenprofil für einen parametrisierten Blueprint importieren.</p> <li data-bbox="810 879 1102 900">■ LinuxKickstartWorkflow <p data-bbox="847 926 1422 1073">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 data-bbox="810 1089 1211 1110">■ VirtualSccmProvisioningWorkflow <p data-bbox="847 1136 1422 1283">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 data-bbox="810 1299 1066 1320">■ WIMImageWorkflow <p data-bbox="847 1346 1417 1493">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 1514 1422 1755">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>

Tabelle 3-5. Registerkarte **Build-Informationen** (Fortsetzung)

Einstellung	Beschreibung
Klonen von	<p>Wählen Sie eine zu klonende Maschinenvorlage aus. Die Liste der verfügbaren Vorlagen können Sie mithilfe der Option Filter im Dropdown-Menü jeder Spalte verfeinern, beispielsweise mit der Option Filter in der Spalte Namen.</p> <p>Für verknüpfte Klone 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>
Von Snapshot klonen	<p>Wählen Sie für verknüpfte Klone einen vorhandenen zu klonenden Snapshot basierend auf der ausgewählten Maschinenvorlage aus. 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 Aktuellen Snapshot verwenden 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>Hinweis Die Verwendung des Begriffs „Snapshot“ kann verwirrend sein. Wenn Sie einen vorhandenen Snapshot auswählen, wird mit der Option eine neue Festplatte erstellt, die dem Snapshot untergeordnet ist. Für die Option Aktuellen Snapshot verwenden ist keine als übergeordnete Festplatte verwendbare Basisfestplatte verfügbar, sodass im Hintergrund eine vollständige Klonaktion durchgeführt wird. Sie können dieses Problem umgehen, indem Sie Snapshots auf der Basisfestplatte erstellen oder einen vRealize Orchestrator-Workflow zum Erstellen eines Snapshots verwenden und den die Klonaktion sofort über den Snapshot durchführen.</p> <p>Diese Option ist nur 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 3-6. Registerkarte **Maschinenressourcen**

Einstellung	Beschreibung
CPUs: Mindestwert und Maximalwert	Geben Sie eine Mindest- und eine Maximalanzahl an CPUs ein, die durch diese Maschinenkomponente bereitgestellt werden können.
Arbeitsspeicher (MB): Mindestwert und Maximalwert	Geben Sie eine Mindest- und eine Maximalmenge für Arbeitsspeicher ein, die von dieser Maschinenkomponente bereitgestellte Maschinen verbrauchen können.
Speicher (GB): Mindestwert und Maximalwert	<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 3-7. Einstellungen auf der Registerkarte **Speicher**

Einstellung	Beschreibung
ID	Geben Sie eine ID oder einen Namen für das Speichervolume ein.
Kapazität (GB)	Geben Sie die Speicherkapazität für das Speichervolume ein.
Laufwerkbuchstabe / Bereitstellungspfad	Geben Sie einen Laufwerkbuchstaben oder einen Bereitstellungspfad für das Speichervolume ein.
Bezeichnung	Geben Sie eine Bezeichnung für den Laufwerkbuchstaben und den Bereitstellungspfad für das Speichervolume ein.
Speicherreservierungsrichtlinie	Geben Sie die vorhandene Speicherreservierungsrichtlinie ein, die mit diesem Speichervolume verwendet werden soll. Es sind nur die für den aktuellen Mandanten geltenden Speicherreservierungsrichtlinien verfügbar.

Tabelle 3-7. Einstellungen auf der Registerkarte **Speicher** (Fortsetzung)

Einstellung	Beschreibung
Benutzerdefinierte Eigenschaften	Geben Sie alle benutzerdefinierten Eigenschaften ein, die mit diesem Speichervolume verwendet werden sollen.
Maximale Anzahl von Volumes	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.
Anzeigen und Ändern von Speicherreservierungsrichtlinien durch Benutzer zulassen	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 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-Eigenschaftsseiteneinstellungen mit NSX](#).

Tabelle 3-8. Einstellungen auf der Registerkarte **Netzwerk**

Einstellung	Beschreibung
Netzwerk	Wählen Sie aus dem Dropdown-Menü eine Netzwerkkomponente aus. Es werden nur Netzwerkkomponenten aufgelistet, die auf der Design-Arbeitsfläche vorhanden sind. Es sind nur die für den aktuellen Mandanten geltenden Netzwerkprofile verfügbar.
Zuweisungstyp	Akzeptieren Sie die der Netzwerkkomponente entnommene Standardzuweisung oder wählen Sie aus dem Dropdown-Menü einen Zuweisungstyp aus. Die Optionswerte DHCP und Statisch werden den Einstellungen in der Netzwerkkomponente entnommen.
Adresse	Geben Sie die IP-Adresse für das Netzwerk an. Die Option ist nur für den statischen IP-Adresstyp verfügbar.
Lastausgleich	Geben Sie den für den Lastausgleich zu verwendenden Dienst ein.

Tabelle 3-8. Einstellungen auf der Registerkarte **Netzwerk** (Fortsetzung)

Einstellung	Beschreibung
Benutzerdefinierte Eigenschaften	Zeigt benutzerdefinierte Eigenschaften an, die für die ausgewählte Netzwerkkomponente bzw. das Netzwerkprofil konfiguriert werden.
Maximale Anzahl von Netzwerkadaptern	Geben Sie die maximale Anzahl von Netzwerkadaptern 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 verwenden.

Die Sicherheitseinstellungen von vorhandenen und bedarfsgesteuerten Sicherheitsgruppen und Sicherheits-Tag-Komponenten auf der Design-Arbeitsfläche 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-Eigenschaftsseiteneinstellungen mit NSX](#).

Tabelle 3-9. Einstellungen auf der Registerkarte **Sicherheit**

Einstellung	Beschreibung
Name	Zeigt den Namen einer NSX-Sicherheitsgruppe bzw. eines Sicherheits-Tags an. Die Namen werden den Sicherheitskomponenten auf der Design-Arbeitsfläche entnommen. Aktivieren Sie das Kontrollkästchen neben einer aufgelisteten Sicherheitsgruppe bzw. einem Sicherheits-Tag, um die Bereitstellung über diese Maschinenkomponente durchzuführen.
Typ	Gibt an, ob es sich bei dem Sicherheitselement um eine bedarfsgesteuerte Sicherheitsgruppe, eine vorhandene Sicherheitsgruppe oder ein Sicherheits-Tag handelt.
Beschreibung	Zeigt die für die Sicherheitsgruppe bzw. den Sicherheits-Tag definierte Beschreibung an.
Endpoint	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 **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 3-10. Einstellungen auf der Registerkarte **Eigenschaften > Benutzerdefinierte Eigenschaften**

Einstellung	Beschreibung
Name	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.
Wert	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.
Verschlüsselt	Sie können den Eigenschaftswert verschlüsseln. Beispielsweise für den Fall, dass es sich bei dem Wert um ein Kennwort handelt.

Tabelle 3-10. Einstellungen auf der Registerkarte **Eigenschaften > Benutzerdefinierte Eigenschaften** (Fortsetzung)

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.

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 3-11. Einstellungen auf der Registerkarte **Eigenschaften > Eigenschaftsgruppen**

Einstellung	Beschreibung
Name	Wählen Sie aus dem Dropdown-Menü eine verfügbare Sicherheitsgruppe aus.
Nach oben und Nach unten	Steuern Sie die Rangfolge der aufgelisteten Eigenschaftsgruppen in absteigender Reihenfolge. Die zuerst aufgelistete Eigenschaftsgruppe hat Vorrang vor der als nächstes aufgelisteten Eigenschaftsgruppe etc.
Eigenschaften anzeigen	Zeigen Sie die benutzerdefinierten Eigenschaften in der ausgewählten Eigenschaftsgruppe an.
Zusammengeführte Eigenschaften anzeigen	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.

Registerkarte „Profile“

Komponentenprofile stellen eine Möglichkeit zum Parametrisieren von Blueprints dar. Statt beispielsweise einen eigenen kleinen, mittleren und großen Blueprint zu erstellen, können Sie einen einzelnen Blueprint mit einer kleinen, mittleren und großen Kapazität erstellen und es Ihren Benutzern ermöglichen, beim Bereitstellen des Katalogelements eine der drei Größen auszuwählen. Komponentenprofile sind speziell dafür konzipiert, die Anzahl an Blueprints zu begrenzen und Ihren Katalog zu vereinfachen.

Wenn Sie Wertsätze für die angegebenen vRealize Automation-Komponentenprofile **Size** und **Image** erstellt haben, können Sie diese Einstellungen für die Maschinenkomponente im Blueprint hinzufügen und konfigurieren. Sie können auch einen anderen Wertsatz auswählen, wenn Sie das Katalogelement bereitstellen.

Komponentenprofile sind nur für vSphere-Maschinenkomponenten verfügbar.

Wenn Sie der vSphere-Maschinenkomponente in einem Blueprint ein Komponentenprofil hinzufügen, setzen die in dem ausgewählten Wertsatz bzw. den ausgewählten Wertsätzen des Profils definierten Einstellungen die übrigen Einstellungen der Maschinenkomponente, beispielsweise für die Anzahl der CPUs und den Speicher, außer Kraft.

Der festgelegte Wert des Komponentenprofils wird auf alle vSphere-Maschinen in einem Cluster angewendet.

Sie können Maschinen nicht mithilfe der Komponentenprofile **Size** oder **Image** neu konfigurieren. Der CPU-Bereich, der Arbeitsspeicher und der Speicher, die basierend auf dem Profil berechnet werden, bleiben jedoch für Neukonfigurationsaktionen verfügbar. Wenn Sie beispielsweise einen kleinen (1 CPU, 1024 MB Arbeitsspeicher und 10 GB Speicher), einen mittleren (3 CPUs, 2048 MB Arbeitsspeicher, 12 GB Speicher) und einen großen (5 CPUs, 3072 MB Arbeitsspeicher, 15 GB Speicher) **Size**-Wertsatz verwendet haben, sind die folgenden Bereiche während der Neukonfiguration der Maschine verfügbar: 1–5 CPUs, 1024–3072 MB Arbeitsspeicher und 1–15 GB Speicher.

Weitere Informationen zum Definieren von Wertsätzen für Komponentenprofile finden Sie in der *Referenz für benutzerdefinierte Eigenschaften*.

Tabelle 3-12. Registerkarte **Profile – Einstellungen**

Einstellung	Beschreibung
Hinzufügen	Hiermit fügen Sie das Komponentenprofil Size oder Image hinzu.
Wertsätze bearbeiten	Weisen Sie einen oder mehrere Wertsätze für das ausgewählte Komponentenprofil zu, indem Sie diese aus einer Liste der definierten Wertsätze auswählen. Sie können einen der Wertsätze als Standard festlegen.
Entfernen	Entfernen Sie das Komponentenprofil Size oder Image .

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 3-13. Einstellungen auf der Registerkarte **Allgemein**

Einstellung	Beschreibung
ID	Geben Sie einen Namen für Ihre Maschinenkomponente ein oder übernehmen Sie den Standardwert.
Beschreibung	Eine Zusammenfassung Ihrer Maschinenkomponente für andere Architekten.
Speicherort auf Anforderung anzeigen	<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>
Reservierungsrichtlinie	<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. Es sind nur die für den aktuellen Mandanten geltenden Reservierungsrichtlinien verfügbar.</p>

Tabelle 3-13. Einstellungen auf der Registerkarte **Allgemein** (Fortsetzung)

Einstellung	Beschreibung
Maschinenpräfix	<p>Maschinenpräfixe werden von Fabric-Administratoren erstellt und zum Erstellen der Namen von bereitgestellten Maschinen verwendet. Wenn Sie Gruppenstandardwert verwenden 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. Es sind nur die für den aktuellen Mandanten geltenden Maschinenpräfixe verfügbar.</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>
Instanzen: Mindestwert und Maximalwert	<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 Minimalwert und Maximalwert 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 3-14. Registerkarte **Build-Informationen**

Einstellung	Beschreibung
Blueprint-Typ	Wählen Sie zu Statistik- und Lizenzierungszwecken aus, ob über diesen Blueprint bereitgestellte Maschinen als „Desktop“ oder „Server“ klassifiziert werden.
Aktion	<p>Die im Dropdown-Menü „Aktion“ angezeigten Optionen hängen vom ausgewählten Maschinentyp ab.</p> <p>Die einzige verfügbare Aktion für eine vCloud Air-Maschinenkomponente ist das Klonen.</p> <ul style="list-style-type: none"> ■ Klonen <p>Erstellt Kopien einer virtuellen Maschine anhand einer Vorlage und eines Anpassungsobjekts.</p>

Tabelle 3-14. Registerkarte **Build-Informationen** (Fortsetzung)

Einstellung	Beschreibung
Bereitstellungsworkflow	<p>Die im Dropdown-Menü „Bereitstellungsworkflow“ angezeigten Optionen hängen vom ausgewählten Maschinentyp und der ausgewählten Aktion ab.</p> <p>Die einzige verfügbare Aktion für eine vCloud Air-Maschinenkomponente ist das Klonen eines Workflows.</p> <p>■ CloneWorkflow</p> <p>Erstellen Sie Kopien einer virtuellen Maschine durch Klonen, durch einen verknüpften Klon oder durch NetApp FlexClone.</p>
Klonen von	<p>Wählen Sie eine zu klonende Maschinenvorlage aus. Die Liste der verfügbaren Vorlagen können Sie mithilfe der Option Filter im Dropdown-Menü jeder Spalte verfeinern, beispielsweise mit der Option Filter in der Spalte Namen.</p> <p>Für verknüpfte Klone 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 3-15. Registerkarte **Maschinenressourcen**

Einstellung	Beschreibung
CPUs: Mindestwert und Maximalwert	Geben Sie eine Mindest- und eine Maximalanzahl an CPUs ein, die durch diese Maschinenkomponente bereitgestellt werden können.
Arbeitsspeicher (MB): Mindestwert und Maximalwert	Geben Sie eine Mindest- und eine Maximalmenge für Arbeitsspeicher ein, die von dieser Maschinenkomponente bereitgestellte Maschinen verbrauchen können.
Speicher (GB): Mindestwert und Maximalwert	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 3-16. Einstellungen auf der Registerkarte **Speicher**

Einstellung	Beschreibung
ID	Geben Sie eine ID oder einen Namen für das Speichervolume ein.
Kapazität (GB)	Geben Sie die Speicherkapazität für das Speichervolume ein.
Laufwerkbuchstabe / Bereitstellungspfad	Geben Sie einen Laufwerkbuchstaben oder einen Bereitstellungspfad für das Speichervolume ein.
Bezeichnung	Geben Sie eine Bezeichnung für den Laufwerkbuchstaben und den Bereitstellungspfad für das Speichervolume ein.
Speicherreservierungsrichtlinie	Geben Sie die vorhandene Speicherreservierungsrichtlinie ein, die mit diesem Speichervolume verwendet werden soll. Es sind nur die für den aktuellen Mandanten geltenden Speicherreservierungsrichtlinien verfügbar.
Benutzerdefinierte Eigenschaften	Geben Sie alle benutzerdefinierten Eigenschaften ein, die mit diesem Speichervolume verwendet werden sollen.
Maximale Anzahl von Volumes	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.
Anzeigen und Ändern von Speicherreservierungsrichtlinien durch Benutzer zulassen	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 **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 3-17. Einstellungen auf der Registerkarte **Eigenschaften > Benutzerdefinierte Eigenschaften**

Einstellung	Beschreibung
Name	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.
Wert	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.
Verschlüsselt	Sie können den Eigenschaftswert verschlüsseln. Beispielsweise für den Fall, dass es sich bei dem Wert um ein Kennwort handelt.
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.

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 3-18. Einstellungen auf der Registerkarte **Eigenschaften > Eigenschaftsgruppen**

Einstellung	Beschreibung
Name	Wählen Sie aus dem Dropdown-Menü eine verfügbare Sicherheitsgruppe aus.
Nach oben und Nach unten	Steuern Sie die Rangfolge der aufgelisteten Eigenschaftsgruppen in absteigender Reihenfolge. Die zuerst aufgelistete Eigenschaftsgruppe hat Vorrang vor der als nächstes aufgelisteten Eigenschaftsgruppe etc.
Eigenschaften anzeigen	Zeigen Sie die benutzerdefinierten Eigenschaften in der ausgewählten Eigenschaftsgruppe an.
Zusammengeführte Eigenschaften anzeigen	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 3-19. Einstellungen auf der Registerkarte **Allgemein**

Einstellung	Beschreibung
ID	Geben Sie einen Namen für Ihre Maschinenkomponente ein oder übernehmen Sie den Standardwert.
Beschreibung	Eine Zusammenfassung Ihrer Maschinenkomponente für andere Architekten.
Speicherort auf Anforderung anzeigen	<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>

Tabelle 3-19. Einstellungen auf der Registerkarte **Allgemein** (Fortsetzung)

Einstellung	Beschreibung
Reservierungsrichtlinie	<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. Es sind nur die für den aktuellen Mandanten geltenden Reservierungsrichtlinien verfügbar.</p>
Maschinenpräfix	<p>Maschinenpräfixe werden von Fabric-Administratoren erstellt und zum Erstellen der Namen von bereitgestellten Maschinen verwendet. Wenn Sie Gruppenstandardwert verwenden 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. Es sind nur die für den aktuellen Mandanten geltenden Maschinenpräfixe verfügbar.</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>
Instanzen: Mindestwert und Maximalwert	<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 Minimalwert und Maximalwert 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 3-20. Registerkarte „Build-Informationen“

Einstellung	Beschreibung
Blueprint-Typ	Wählen Sie zu Statistik- und Lizenzierungszwecken aus, ob über diesen Blueprint bereitgestellte Maschinen als „Desktop“ oder „Server“ klassifiziert werden.
Bereitstellungsworkflow	<p>Der einzige, für eine Amazon-Maschinenkomponente verfügbare Bereitstellungsworkflow ist CloudProvisioningWorkflow.</p> <ul style="list-style-type: none"> ■ CloudProvisioningWorkflow <p>Erstellt eine Maschine durch Starten über eine VM-Instanz oder ein Cloud-basiertes Image.</p>
Amazon-System-Image	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. Die Liste der angezeigten Amazon-Maschinen-Images können Sie mithilfe der Option Filter im Dropdown-Menü der Spalte AMI-ID verfeinern.
Schlüsselpaar	<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"> ■ Nicht angegeben <p>Das Verhalten von Schlüsselpaaren wird auf der Blueprint-Ebene anstatt auf der Reservierungsebene gesteuert.</p> ■ 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> ■ 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>

Tabelle 3-20. Registerkarte „Build-Informationen“ (Fortsetzung)

Einstellung	Beschreibung
Amazon-Netzwerkoptionen auf der Maschine aktivieren	Wählen Sie aus, ob Benutzer eine Maschine am Speicherort einer Virtual Private Cloud (VPC) oder Nicht-VPC bereitstellen dürfen, wenn Sie die Maschinenanforderung übermitteln.
Instanztypen	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. Informationen zur Verwendung von Amazon-Instanztypen in vRealize Automation finden Sie unter Grundlegendes zu Amazon-Instanztypen und Hinzufügen eines Amazon-Instanztyps .

Registerkarte **Maschinenressourcen**

Geben Sie Einstellungen für CPU, Arbeitsspeicher, Speicher und EBS-Datenträger für Ihre Amazon-Maschinenkomponente an.

Sie können auch alle Speichervolumes der Amazon-Maschine in der Bereitstellung außer dem Root-Volume neu konfigurieren.

Tabelle 3-21. Registerkarte **Maschinenressourcen**

Einstellung	Beschreibung
CPUs: Mindestwert und Maximalwert	Geben Sie eine Mindest- und eine Maximalanzahl an CPUs ein, die durch diese Maschinenkomponente bereitgestellt werden können.
Arbeitsspeicher (MB): Mindestwert und Maximalwert	Geben Sie eine Mindest- und eine Maximalmenge für Arbeitsspeicher ein, die von dieser Maschinenkomponente bereitgestellte Maschinen verbrauchen können.
Speicher (GB): Mindestwert und Maximalwert	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.
EBS-Speicher (GB): Mindestwert und Maximalwert	Geben Sie eine Mindest- und Maximalmenge für Speichervolumes 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 **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 3-22. Einstellungen auf der Registerkarte **Eigenschaften > Benutzerdefinierte Eigenschaften**

Einstellung	Beschreibung
Name	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.
Wert	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.
Verschlüsselt	Sie können den Eigenschaftswert verschlüsseln. Beispielsweise für den Fall, dass es sich bei dem Wert um ein Kennwort handelt.

Tabelle 3-22. Einstellungen auf der Registerkarte **Eigenschaften > Benutzerdefinierte Eigenschaften** (Fortsetzung)

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.

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 3-23. Einstellungen auf der Registerkarte **Eigenschaften > Eigenschaftsgruppen**

Einstellung	Beschreibung
Name	Wählen Sie aus dem Dropdown-Menü eine verfügbare Sicherheitsgruppe aus.
Nach oben und Nach unten	Steuern Sie die Rangfolge der aufgelisteten Eigenschaftsgruppen in absteigender Reihenfolge. Die zuerst aufgelistete Eigenschaftsgruppe hat Vorrang vor der als nächstes aufgelisteten Eigenschaftsgruppe etc.
Eigenschaften anzeigen	Zeigen Sie die benutzerdefinierten Eigenschaften in der ausgewählten Eigenschaftsgruppe an.
Zusammengeführte Eigenschaften anzeigen	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 3-24. Einstellungen auf der Registerkarte **Allgemein**

Einstellung	Beschreibung
ID	Geben Sie einen Namen für Ihre Maschinenkomponente ein oder übernehmen Sie den Standardwert.
Beschreibung	Eine Zusammenfassung Ihrer Maschinenkomponente für andere Architekten.
Speicherort auf Anforderung anzeigen	<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>
Reservierungsrichtlinie	<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. Es sind nur die für den aktuellen Mandanten geltenden Reservierungsrichtlinien verfügbar.</p>

Tabelle 3-24. Einstellungen auf der Registerkarte **Allgemein** (Fortsetzung)

Einstellung	Beschreibung
Maschinenpräfix	<p>Maschinenpräfixe werden von Fabric-Administratoren erstellt und zum Erstellen der Namen von bereitgestellten Maschinen verwendet. Wenn Sie Gruppenstandardwert verwenden 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. Es sind nur die für den aktuellen Mandanten geltenden Maschinenpräfixe verfügbar.</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>
Instanzen: Mindestwert und Maximalwert	<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 Minimalwert und Maximalwert 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 3-25. Registerkarte **Build-Informationen**

Einstellung	Beschreibung
Blueprint-Typ	Wählen Sie zu Statistik- und Lizenzierungszwecken aus, ob über diesen Blueprint bereitgestellte Maschinen als „Desktop“ oder „Server“ klassifiziert werden.
Bereitstellungsworkflow	<p>Die folgenden Bereitstellungsworkflows sind für eine OpenStack-Maschinenkomponente verfügbar:</p> <ul style="list-style-type: none"> ■ CloudLinuxKickstartWorkflow <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> ■ CloudProvisioningWorkflow <p>Erstellt eine Maschine durch Starten über eine VM-Instanz oder ein Cloud-basiertes Image.</p> ■ CloudWIMImageWorkflow <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>
OpenStack-Image	Wählen Sie ein verfügbares OpenStack-Image aus. Ein OpenStack-Image ist eine Vorlage, die eine Softwarekonfiguration einschließlich eines Betriebssystems enthält. Die Images werden über OpenStack-Konten verwaltet. Die Liste der angezeigten OpenStack-Images können Sie mithilfe der Option Filter im Dropdown-Menü der Spalte Namen verfeinern.

Tabelle 3-25. Registerkarte **Build-Informationen** (Fortsetzung)

Einstellung	Beschreibung
Schlüsselpaar	<p data-bbox="810 268 1390 321">Schlüsselpaare sind für die Bereitstellung mit OpenStack optional.</p> <p data-bbox="810 338 1406 453">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 data-bbox="810 470 1414 491">Die folgenden Optionen sind für Schlüsselpaare verfügbar:</p> <ul style="list-style-type: none"> <li data-bbox="810 508 1023 529">■ Nicht angegeben <p data-bbox="847 554 1390 638">Das Verhalten von Schlüsselpaaren wird auf der Blueprint-Ebene anstatt auf der Reservierungsebene gesteuert.</p> <li data-bbox="810 655 1302 676">■ Automatisch generiert pro Business-Gruppe <p data-bbox="847 701 1414 984">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 data-bbox="810 1001 1222 1022">■ Automatisch generiert pro Maschine <p data-bbox="847 1047 1386 1194">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>
Typen	<p data-bbox="810 1220 1414 1398">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 3-26. Registerkarte **Maschinenressourcen**

Einstellung	Beschreibung
CPUs: Mindestwert und Maximalwert	Geben Sie eine Mindest- und eine Maximalanzahl an CPUs ein, die durch diese Maschinenkomponente bereitgestellt werden können.
Arbeitsspeicher (MB): Mindestwert und Maximalwert	Geben Sie eine Mindest- und eine Maximalmenge für Arbeitsspeicher ein, die von dieser Maschinenkomponente bereitgestellte Maschinen verbrauchen können.
Speicher (GB): Mindestwert und Maximalwert	<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 **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 3-27. Einstellungen auf der Registerkarte **Eigenschaften > Benutzerdefinierte Eigenschaften**

Einstellung	Beschreibung
Name	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.
Wert	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.
Verschlüsselt	Sie können den Eigenschaftswert verschlüsseln. Beispielsweise für den Fall, dass es sich bei dem Wert um ein Kennwort handelt.
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.

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 3-28. Einstellungen auf der Registerkarte **Eigenschaften > Eigenschaftsgruppen**

Einstellung	Beschreibung
Name	Wählen Sie aus dem Dropdown-Menü eine verfügbare Sicherheitsgruppe aus.
Nach oben und Nach unten	Steuern Sie die Rangfolge der aufgelisteten Eigenschaftsgruppen in absteigender Reihenfolge. Die zuerst aufgelistete Eigenschaftsgruppe hat Vorrang vor der als nächstes aufgelisteten Eigenschaftsgruppe etc.
Eigenschaften anzeigen	Zeigen Sie die benutzerdefinierten Eigenschaften in der ausgewählten Eigenschaftsgruppe an.
Zusammengeführte Eigenschaften anzeigen	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.

Verwenden benutzerdefinierter Netzwerkeigenschaften

Mit benutzerdefinierten Netzwerkeigenschaften auf der Ebene von Blueprints oder Maschinenkomponenten können Sie Netzwerk- und Sicherheitsinformationen für Maschinenkomponenten, bei denen es sich nicht um vSphere handelt, und für Blueprints angeben, die NSX nicht enthalten.

Die **Netzwerk- und Sicherheitskomponenten** sind ausschließlich für die Verwendung mit vSphere-Maschinenkomponenten verfügbar. Nicht-vSphere-Maschinenkomponenten verfügen nicht über die Registerkarte **Netzwerk** oder **Sicherheit**.

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` zur entsprechenden Registerkarte **Eigenschaften** in der Design-Arbeitsfläche hinzufügen. Die Eigenschaften von NSX-Netzwerk-, -Sicherheits- und -Lastausgleichsdiensten gelten nur für 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*.

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.

Weitere Informationen über **Klonen von** und **Von Snapshot klonen** mit den Optionen **Aktuellen Snapshot verwenden**, die bei der Erstellung von Blueprints verfügbar sind, finden Sie unter [vSphere-Maschinenkomponenteneinstellungen](#).

Tabelle 3-29. 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"> ■ 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. ■ Stellen Sie bei neuen Vorlagen sicher, dass die IT-Abteilung die Vorlagen auf demselben Cluster platziert hat, der in Ihrer Fabric-Gruppe enthalten ist.
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 3-29. 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.

Entwerfen von Blueprints mit NSX-Einstellungen

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.

Weitere Informationen zur Integration von vRealize Automation und NSX und zur Verwendung der NSX-Netzwerk- und -Sicherheitskomponenten im vRealize Automation-Blueprint finden Sie in diesem Blogartikel: [vRA and NSX - Intro to Network and Security Automation](#) (vRA und NSX – Einführung in die Netzwerk- und Sicherheitsautomatisierung).

NSX-Einstellungen betreffen nur Typen der vSphere-Maschinenkomponenten.

Neue Blueprint- und Blueprint-Eigenschaftsseiteneinstellungen mit NSX

Beim Erstellen des Blueprints können Sie über die Seite **Neuer Blueprint** Einstellungen festlegen, die für den gesamten Blueprint gelten (darunter auch einige NSX-Einstellungen). Nach dem Erstellen des Blueprints können Sie diese Eigenschaften auf der Seite „Blueprint-Eigenschaften“ bearbeiten.

Registerkarte **Allgemein**

Wenden Sie Einstellungen auf den gesamten Blueprint an, einschließlich aller Komponenten, die Sie jetzt oder später hinzufügen möchten.

Tabelle 3-30. Einstellungen auf der Registerkarte **Allgemein**

Einstellung	Beschreibung
Name	Geben Sie einen Namen für Ihren Blueprint ein.
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.
Beschreibung	Eine Zusammenfassung Ihres Blueprints für andere Architekten. Diese Beschreibung wird Benutzern auch im Anforderungsformular angezeigt.
Bereitstellungsgrenzwert	Geben Sie die maximale Anzahl an Bereitstellungen an, die erstellt werden können, wenn dieser Blueprint zur Bereitstellung von Maschinen verwendet wird.
Leasetage: Mindestwert und Maximalwert	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. Wenn Sie keinen Mindestwert bzw. Maximalwert eingeben, ist die Leasedauer unbegrenzt.
Archivierung (Tage)	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.
Updates an vorhandene Bereitstellungen weitergeben	<p>Wenn diese Option aktiviert ist, wird festgelegt, dass jede Erweiterung der Grenzwerte, die Sie für Mindest- oder Maximaleinstellungen für CPU, Arbeitsspeicher und Speicher im Blueprint vornehmen, auf alle aktiven Bereitstellungen übertragen wird, die über den Blueprint bereitgestellt wurden. Wenn Sie beispielsweise ein Minimum von 2 und ein Maximum von 4 (2,4) angeben, würde eine Änderung wie (1,4) oder (2,5) bei einer Neukonfiguration wirksam werden, eine Änderung von (3,4) oder (2,3) jedoch nicht.</p> <p>Die Änderungen werden bei der nächsten Neukonfigurationsaktion wirksam. Weitere Informationen zu Neukonfigurationsaktionen finden Sie unter Befehle im Menü „Aktion“ für bereitgestellte Ressourcen.</p>

Registerkarte **NSX-Einstellungen**

Wenn Sie NSX konfiguriert haben, können Sie beim Erstellen oder Bearbeiten eines Blueprints Einstellungen für NSX-Transportzonen, Reservierungsrichtlinien für Edge und das geroutete Gateway sowie Anwendungsisolierungen angeben. Diese Einstellungen sind auf der Registerkarte **NSX-Einstellungen** auf den Seiten **Blueprint** und **Blueprint-Eigenschaften** verfügbar.

Informationen über das Konfigurieren von NSX finden Sie im *NSXAdministratorhandbuch*.

Tabelle 3-31. Einstellungen auf der Registerkarte **NSX-Einstellungen**

Einstellung	Beschreibung
Transportzone	<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. Es sind nur die für den aktuellen Mandanten geltenden Transportzonen verfügbar.</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>
Reservierungsrichtlinie für die Edge und das geroutete Gateway	<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>
Anwendungsisolierung	<p>Aktivieren Sie das Kontrollkästchen Anwendungsisolierung, 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 3-32. Einstellungen auf der Registerkarte **Eigenschaften**

Registerkarte	Einstellung	Beschreibung
Eigenschaftsgruppen		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.
	Hinzufügen	Fügen Sie eine oder mehrere vorhandene Eigenschaftsgruppen hinzu und weisen Sie diese dem gesamten Blueprint zu. Die folgenden Eigenschaftsgruppen im Zusammenhang mit Containern werden angegeben: <ul style="list-style-type: none"> ■ Container-Hosteigenschaften mit Zertifikatsauthentifizierung ■ Container-Hosteigenschaften mit Benutzer-/Kennwortauthentifizierung
	Nach oben verschieben/Nach unten verschieben	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.
	Eigenschaften anzeigen	Zeigen Sie die benutzerdefinierten Eigenschaften in der ausgewählten Eigenschaftsgruppe an.
	Zusammengeführte Eigenschaften anzeigen	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.
Benutzerdefinierte Eigenschaften		Anstelle von Eigenschaftsgruppen können Sie auch einzelne benutzerdefinierte Eigenschaften hinzufügen.
	Neu	Fügen Sie eine einzelne benutzerdefinierte Eigenschaft hinzu und wenden Sie diese auf den gesamten Blueprint an.

Tabelle 3-32. Einstellungen auf der Registerkarte **Eigenschaften** (Fortsetzung)

Registerkarte	Einstellung	Beschreibung
	Name	Eingabe des Eigenschaftsnamens. Eine Liste der benutzerdefinierten Eigenschaften und deren Definitionen finden Sie unter <i>Referenz für benutzerdefinierte Eigenschaften</i> .
	Wert	Geben Sie den Wert für die benutzerdefinierte Eigenschaft ein.
	Verschlüsselt	Sie können den Eigenschaftswert verschlüsseln. Beispielsweise für den Fall, dass es sich bei dem Wert um ein Kennwort handelt.
	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.

Beim Erstellen eines Blueprints werden nur die für den aktuellen Mandanten geltenden Transportzonen angezeigt. Insbesondere werden Transportzonen zur Verfügung gestellt, wenn sie von einer Reservierung im aktuellen Mandanten verwendet 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 die Seite **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 NSX-Endpoints und Zuordnen zu einem vSphere-Endpoint](#).

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 zum Zweck 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.

Hinweis Wenn ein Blueprint einen oder mehrere Lastausgleichsdienste enthält und die Anwendungsisolierung für den Blueprint aktiviert ist, werden die Lastausgleichs-VIPs als IPSet zur Sicherheitsgruppe der Anwendungsisolation hinzugefügt. Wenn ein Blueprint eine On-Demand-Sicherheitsgruppe enthält, die einer Maschinenebene zugewiesen ist, welche auch einem Lastausgleichsdienst zugewiesen ist, enthält die On-Demand-Sicherheitsgruppe die Maschinenebene und das IPSet mit der Lastausgleichs-VIP.

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 Design-Arbeitsfläche](#).

Konfigurieren der Einstellungen für Netzwerk- und Sicherheitskomponenten

vRealize Automation unterstützt virtualisierte Netzwerke basierend auf der NSX-Plattform. Integrierte Container für vRealize Automation-Netzwerke werden ebenfalls unterstützt.

Zur Integration von Netzwerk- und Sicherheitskomponenten in vRealize Automation muss ein IaaS-Administrator vSphere- und NSX-Endpoints konfigurieren.

Informationen zur externen Vorbereitung finden Sie unter *Konfigurieren von vRealize Automation*.

Sie können Netzwerkprofile erstellen, mit denen Netzwerkeinstellungen in Reservierungen und in der Design-Arbeitsfläche angegeben werden. Externe Netzwerkprofile definieren vorhandene physische Netzwerke. NAT und geroutete Profile sind Vorlagen, mit denen logische NSX-Switches und entsprechende Routing Einstellungen 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 Design-Arbeitsfläche hinzufügen, werden von der NSX-Konfiguration abgeleitet. Dafür muss die Datenerfassung für den NSX-Bestand für vSphere-Cluster 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*.

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` zur entsprechenden Registerkarte **Eigenschaften** in der Design-Arbeitsfläche hinzufügen. Die Eigenschaften von NSX-Netzwerk-, -Sicherheits- und -Lastausgleichsdiensten gelten nur für 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*.

Sie können Sicherheitseinstellungen für die bereitzustellenden virtuellen Maschinen konfigurieren, indem Sie Informationen in einem Reservierungs-, Blueprint- oder Gast-Agent-Skript angeben. Wenn die bereitzustellenden Maschinen einen Gast-Agent benötigen, müssen Sie eine Sicherheitsregel, die diese Anforderung enthält, zur Reservierung oder zum Blueprint hinzufügen. Wenn Sie z. B. eine Standardsicherheitsrichtlinie verwenden, die die Kommunikation zwischen allen Maschinen nicht zulässt, und Sie sich auf eine separate Sicherheitsrichtlinie verlassen, die die Kommunikation zwischen bestimmten Maschinen, kann der Gast-Agent während der Anpassungsphase möglicherweise mit vRealize Automation kommunizieren. Um dieses Problem während der Bereitstellung von Maschinen zu vermeiden, verwenden Sie eine Standardsicherheitsrichtlinie, die während der Anpassungsphase die Kommunikation ermöglicht.

Sie können auch eine Container-Netzwerkkomponente zu einem Blueprint hinzufügen.

Verwenden von Netzwerkkomponenten auf der Design-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 einer oder mehreren Maschinen-Komponenten im Blueprint zur Verfügung zu stellen.

Die Netzwerk- und Sicherheitskomponenteneinstellungen, die Sie zur Design-Arbeitsfläche hinzufügen, werden von der NSX-Konfiguration abgeleitet. Dafür muss die Datenerfassung für den NSX-Bestand für vSphere-Cluster 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*.

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 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` zur entsprechenden Registerkarte **Eigenschaften** in der Design-Arbeitsfläche hinzufügen. Die Eigenschaften von NSX-Netzwerk-, -Sicherheits- und -Lastausgleichsdiensten gelten nur für vSphere-Maschinen.

Nur die Netzwerkprofile, die für den aktuellen Mandanten gelten, werden beim Erstellen eines Blueprints angezeigt. Insbesondere werden Netzwerkprofile dann zur Verfügung gestellt, wenn mindestens eine Reservierung in dem aktuellen Mandanten vorhanden ist, der mindestens ein dem Profil zugewiesenes Netzwerk aufweist.

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 die NSX-Bestandsliste für Ihren Cluster erfolgreich ausgeführt wurde.
Um NSX-Konfigurationen in vRealize Automation verwenden zu können, müssen Sie die Datenerfassung ausführen.
- Erstellen Sie ein Netzwerkprofil.
- Melden Sie sich bei vRealize Automation als **Infrastrukturarchitekt** an.
- Öffnen Sie mithilfe der Registerkarte **Design** einen neuen oder vorhandenen Blueprint in der Design-Arbeitsfläche.

Verfahren

- 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.

Nächste Schritte

Sie können weitere Netzwerkeinstellungen konfigurieren, indem Sie zusätzliche Netzwerkkomponenten hinzufügen und Einstellungen auf der Registerkarte **Netzwerk** einer vSphere-Maschinenkomponente auf der Design-Arbeitsfläche auswählen.

Erstellen und Verwenden von NAT-Regeln

Sie können NAT-Regeln zu einer 1:n-NAT-Netzwerkkomponente in einem Blueprint hinzufügen, wenn die NAT-Netzwerkkomponente einer nicht gruppierten vSphere-Maschinenkomponente oder einer bedarfsorientierten Komponente für den NSX-Lastausgleichsdienst zugewiesen ist.

Sie können NAT-Regeln für alle von NSX unterstützten Protokolle definieren. Sie können einen Port oder einen Bereich aus der externen IP-Adresse eines Edge zu einer privaten IP-Adresse in der NAT-Netzwerkkomponente zuordnen.

- vSphere-Maschinenkomponente

Sie können NAT-Regeln für eine 1:n-NAT-Netzwerkkomponente erstellen, die einer nicht gruppierten vSphere-Maschinenkomponente zugewiesen ist.

Beispiel: Wenn zwei Maschinen einer 1:n-NAT-Netzwerkkomponente im Blueprint zugewiesen sind, können Sie eine NAT-Regel definieren, die ermöglicht, dass Port 443 in der externen IP-Adresse mit dem TCP-Protokoll eine Verbindung zu den Maschinen über Port 80 im NAT-Netzwerk herstellen kann.

- NSX-Lastausgleichsdienstkomponente

Sie können NAT-Regeln für eine 1:n-NAT-Netzwerkkomponente erstellen, die dem VIP-Netzwerk einer NSX-Lastausgleichsdienstkomponente zugewiesen ist.

Beispiel: Wenn die NAT-Netzwerkkomponente einer Lastausgleichsdienstkomponente zugewiesen ist, die den Lastausgleich von drei Maschinen durchführt, können Sie eine NAT-Regel definieren, die ermöglicht, dass Port 90 in der externen IP-Adresse mit dem UDP-Protokoll eine Verbindung zur Lastausgleichsdienst-VIP über Port 80 im NAT-Netzwerk herstellen kann.

Sie können eine beliebige Anzahl von NAT-Regeln erstellen und die Reihenfolge steuern, in der die Regeln verarbeitet werden.

Die folgenden Elemente werden für NAT-Regeln nicht unterstützt:

- Netzwerkkarten, die sich nicht im aktuellen Netzwerk befinden

- Netzwerkkarten, die zum Abrufen von IP-Adressen unter Verwendung von DHCP konfiguriert sind
- Maschinencluster

Weitere Informationen zum Hinzufügen von NAT-Regeln zu einer NAT-Netzwerkkomponente in einem Blueprint finden Sie unter [Hinzufügen einer bedarfsgesteuerten NAT- oder bedarfsgesteuerten gerouteten Netzwerkkomponente](#).

Weitere Informationen zur Verwendung von NAT-Regeln finden Sie in öffentlichen Artikel wie z. B. diesem [VMwareLab-Blog-Beitrag](#).

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 Design-Arbeitsfläche hinzufügen.

Ein einzelner Blueprint kann mehr als eine bedarfsgesteuerte Netzwerkkomponente enthalten. Alle im Blueprint enthaltenen bedarfsgesteuerten Netzwerkprofile müssen jedoch auf dasselbe externe Netzwerkprofil verweisen.

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` zur entsprechenden Registerkarte **Eigenschaften** in der Design-Arbeitsfläche hinzufügen. Die Eigenschaften von NSX-Netzwerk-, -Sicherheits- und -Lastausgleichsdiensten gelten nur für vSphere-Maschinen.

Nur die Netzwerkprofile, die für den aktuellen Mandanten gelten, werden beim Erstellen eines Blueprints angezeigt. Insbesondere werden Netzwerkprofile dann zur Verfügung gestellt, wenn mindestens eine Reservierung in dem aktuellen Mandanten vorhanden ist, der mindestens ein dem Profil zugewiesenes Netzwerk aufweist.

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 die NSX-Bestandsliste für Ihren Cluster erfolgreich ausgeführt wurde.

Um NSX-Konfigurationen in vRealize Automation verwenden zu können, müssen Sie die Datenerfassung ausführen.

- Erstellen Sie ein bedarfsgesteuertes Netzwerkprofil. Siehe [Erstellen eines Netzwerkprofils](#).
Wenn Sie beispielsweise eine bedarfsgesteuerte NAT-Netzwerkkomponente hinzufügen, finden Sie weitere Informationen unter [Erstellen eines NAT-Netzwerkprofils für ein bedarfsgesteuertes Netzwerk](#).
- Melden Sie sich bei vRealize Automation als **Infrastrukturarchitekt** an.
- Öffnen Sie mithilfe der Registerkarte **Design** einen neuen oder vorhandenen Blueprint in der Design-Arbeitsfläche.
- Wenn Sie NAT-Regeln für eine NAT-Netzwerkkomponente angeben möchten, müssen Sie ein 1:1-NAT-Netzwerkprofil verwenden. Siehe [Erstellen eines NAT-Netzwerkprofils unter Verwendung des bereitgestellten IPAM-Endpoints](#) oder [Erstellen eines NAT-Netzwerkprofils unter Verwendung eines IPAM-Endpoints eines Drittanbieters](#). Informationen über NAT-Regeln finden Sie unter [Erstellen und Verwenden von NAT-Regeln](#).

Verfahren

- 1 Klicken Sie im Abschnitt „Kategorien“ auf **Netzwerk und Sicherheit**, um die Liste der verfügbaren Netzwerk- und Sicherheitskomponenten anzuzeigen.
- 2 Ziehen Sie eine bedarfsgesteuerte NAT oder eine bedarfsgesteuerte geroutete Netzwerkkomponente auf die Design-Arbeitsfläche.
- 3 Geben Sie im Textfeld **ID** einen Komponentennamen ein, der die Komponente auf der Design-Arbeitsfläche eindeutig kennzeichnet.
- 4 Wählen Sie aus dem Dropdown-Menü **Übergeordnetes Netzwerkprofil** ein entsprechendes Netzwerkprofil aus. Wenn Sie beispielsweise eine NAT-Netzwerkkomponente hinzufügen möchten, wählen Sie ein NAT-Netzwerkprofil aus, das für die Unterstützung Ihrer beabsichtigten Netzwerkeinstellungen konfiguriert ist.

Wenn Sie NAT-Regeln in einer NAT-Netzwerkkomponente angeben möchten, müssen Sie ein übergeordnetes Netzwerkprofil verwenden, das für 1:n-NAT konfiguriert ist.

Je nach ausgewähltem Profiltyp werden die folgenden Netzwerkeinstellungen basierend auf Ihrem ausgewählten Netzwerkprofil ausgefüllt. 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) Geben Sie im Textfeld **Beschreibung** eine Beschreibung für die Komponente ein.
 - 6 (Optional) Klicken Sie auf die Registerkarte **DNS/WINS**.

- 7 (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.

- 8 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.

- a Geben Sie im Textfeld **Beginn des IP-Bereichs** den Wert für eine IP-Startadresse ein.
- b Geben Sie im Textfeld **Beginn des IP-Bereichs** den Wert für eine IP-Startadresse ein.

- 9 Wenn Sie ein NAT-Netzwerk verwenden, das auf einem 1:n-NAT-Netzwerkprofil basiert, das statische IP-Adressbereiche verwendet, können Sie die Registerkarte **NAT-Regeln** verwenden, um Regeln hinzuzufügen, die eine externe IP-Adresse für den Zugriff auf Komponenten im internen NAT-Netzwerk aktivieren.

Für ein NAT-Netzwerk vom Typ 1:n können Sie NAT-Regeln definieren, die konfiguriert werden können, wenn Sie eine NAT-Netzwerkkomponente dem Blueprint hinzufügen, und die geändert werden können, wenn Sie das NAT-Netzwerk in einer Bereitstellung bearbeiten.

Die Optionen, die zur Auswahl stehen, basieren auf der vSphere-Maschine oder den NSX-Lastausgleichskomponenten, die Sie der NAT-Netzwerkkomponente zugeordnet haben.

- **Name:** Geben Sie einen eindeutigen Regelnamen ein.
- **Komponente:** Wählen Sie aus der Liste der zugeordneten vSphere-Maschinen- oder -Lastausgleichskomponenten aus, denen das NAT-Netzwerk zugeordnet ist.

NAT-Regeln werden nur für nicht geclusterte Maschinen unterstützt. Wenn Sie eine Clustergröße von mehr als 1 angegeben haben, werden keine Komponenten aufgeführt, da die Konfiguration nicht unterstützt wird.

- **Quellport:** Wählen Sie die Option „Beliebige“ aus, geben Sie einen gültigen Port oder Portbereich ein oder geben Sie eine gültige Eigenschaftsbindung ein.
- **Zielpport:** Wählen Sie die Option „Beliebige“ aus, geben Sie einen gültigen Port oder Portbereich ein oder geben Sie eine gültige Eigenschaftsbindung an.
- **Protokoll:** Geben Sie gültiges von NSX unterstütztes Protokoll ein oder wählen Sie die Option „TCP“, „UDP“ oder „Beliebige“ aus.

- **Beschreibung:** Geben Sie eine kurze Beschreibung dessen ein, wofür die NAT-Regel konzipiert wurde.

10 Klicken Sie auf **Fertig stellen**, um den Blueprint als Entwurf zu speichern, oder setzen Sie die Konfiguration des Blueprints fort.

Nächste Schritte

Sie können weitere Netzwerkeinstellungen konfigurieren, indem Sie zusätzliche Netzwerkkomponenten hinzufügen und Einstellungen auf der Registerkarte **Netzwerk** einer vSphere-Maschinenkomponente auf der Design-Arbeitsfläche auswählen.

Verwenden von Lastausgleichsdienst-Komponenten auf der Design-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 Design-Arbeitsfläche hinzufügen, werden von der NSX-Konfiguration abgeleitet. Dafür muss die Datenerfassung für den NSX-Bestand für vSphere-Cluster 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*.

Die folgenden Regeln gelten für Lastausgleichsdienst-Pools und VIP-Netzwerkeinstellungen im Blueprint.

- Ist NAT das Poolnetzwerkprofil, kann das VIP-Netzwerkprofil nur dasselbe externe 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.

Jede Komponente des Lastausgleichsdiensts kann mehrere virtuelle Server aufweisen, die auch als Lastausgleichsdienste bezeichnet werden. Jeder virtuelle Server in der Komponente für den Lastausgleichsdienst hat einen Port und ein Protokoll. Beispielsweise können Sie den Lastausgleich für einen HTTP- oder HTTPS-Dienst anwenden. Ein Lastausgleichsdienst kann auf mehrere Dienste angewendet werden.

Der NSX Edge ist das Netzwerkgerät, das die virtuellen Server der Lastausgleichsdienste enthält. Auch wenn ein Blueprint mehrere Lastausgleichsdienstkomponenten aufweisen kann, sind die in jeder Lastausgleichsdienstkomponente definierten virtuellen Server bei der Bereitstellung der Maschinen in einem einzelnen NSX Edge enthalten.

Wenn ein Blueprint einen oder mehrere Lastausgleichsdienste enthält und die Anwendungsisolierung für den Blueprint aktiviert ist, werden die Lastausgleichs-VIPs als IPSet zur Sicherheitsgruppe der Anwendungsisolierung hinzugefügt. Wenn ein Blueprint eine On-Demand-Sicherheitsgruppe enthält, die einer Maschinenebene zugewiesen ist, welche auch einem Lastausgleichsdienst zugewiesen ist, enthält die On-Demand-Sicherheitsgruppe die Maschinenebene und das IPSet mit der Lastausgleichs-VIP.

Sie können die Lastausgleichsdienst-Einstellungen in einer vorhandenen Bereitstellung neu konfigurieren, um virtuelle Server hinzuzufügen, zu bearbeiten oder zu löschen. Weitere Informationen hierzu finden Sie unter [Erneutes Konfigurieren eines Lastausgleichsdiensts in einer Bereitstellung](#).

Informationen zum Arbeiten mit Lastausgleichsdienstkomponenten nach dem Upgrade oder der Migration finden Sie unter [Überlegungen bei der Arbeit mit aktualisierten oder migrierten Lastausgleichsdienst-Komponenten](#).

Überlegungen bei der Arbeit mit aktualisierten oder migrierten Lastausgleichsdienst-Komponenten

Es ist wichtig, dass Sie die folgenden Überlegungen verstehen und in Bezug auf die Komponenten des NSX-Lastausgleichsdiensts in der zielseitigen vRealize Automation-Version entsprechend handeln.

Diese Informationen beziehen sich auf Komponenten des NSX-Lastausgleichsdiensts, die auf diese Version von vRealize Automation aktualisiert oder migriert wurden.

- Sie müssen die Erfassung von Bestandslistendaten für die NSX-Netzwerk- und -Sicherheitsplattform vor und nach dem Upgrade oder der Migration auf diese Version ausführen, um Probleme bei der Ausführung der Aktion „Lastausgleichsdienst neu konfigurieren“ zu vermeiden. Die Aktion „Lastausgleichsdienst neu konfigurieren“ für neue Bereitstellungen wird nicht beeinträchtigt.

Weitere Informationen dazu finden Sie unter *Upgrade von vRealize Automation 7.1, 7.2 oder 7.3* und *Migrieren von vRealize Automation*.

- Ab vRealize Automation 7.3 können Sie einen Lastausgleichsdienst neu konfigurieren. Die erforderliche Katalogberechtigung ist „Neu konfigurieren (Lastausgleichsdienst)“. Informationen hierzu finden Sie unter [Erneutes Konfigurieren eines Lastausgleichsdiensts in einer Bereitstellung](#).
- Bei Bereitstellungen, die von vRealize Automation 7.x auf diese Version von vRealize Automation aktualisiert bzw. migriert wurden, ist die Neukonfiguration auf Bereitstellungen beschränkt, die einen einzelnen Lastausgleichsdienst enthalten.
- Der Vorgang „Lastausgleichsdienst neu konfigurieren“ wird für Bereitstellungen, die von vRealize Automation 6.2.x auf diese Version von vRealize Automation aktualisiert oder migriert wurden, nicht unterstützt.

Hinzufügen einer Komponente für den Lastausgleichsdienst nach Bedarf

Sie können eine bedarfsgesteuerte NSX-Komponente für den Lastausgleichsdienst auf die Design-Arbeitsfläche ziehen und ihre Einstellungen für den Einsatz von vSphere-Maschinenkomponenten und Container-Komponenten im Blueprint konfigurieren.

Weitere Informationen zum Erstellen von NSX-Anwendungsprofilen zum Definieren des Verhaltens einer bestimmten Art von Netzwerkverkehr finden Sie im *Administratorhandbuch für NSX* für Ihre Version unter https://www.vmware.com/support/pubs/nsx_pubs.html.

Verfahren

1 Definieren der Einstellungen für Mitglieder des Lastausgleichsdiensts

Sie können eine Komponente des bedarfsgesteuerten NSX-Lastausgleichsdiensts definieren, um die Verarbeitung von Aufgaben auf bereitgestellte vSphere-Mitgliedsmaschinen oder Container-Maschinen in einem Netzwerk zu verteilen.

2 Definieren von allgemeinen Einstellungen für den virtuellen Server

Sie können ein einzelnes Protokoll für den virtuellen Server und einen einzelnen Port für Ihren Lastausgleichsdienst definieren oder weitere virtuelle Server hinzufügen, um zusätzliche NSX-Lastausgleichsdienstoptionen anzupassen.

3 Definieren der Einstellungen für die Verteilung von virtuellen Servern

Durch Auswahl der Option **Anpassen** auf der Registerkarte **Allgemein** können Sie Informationen zu den Poolmitgliedern angeben, wie z. B. den Port, an dem die Mitglieder Datenverkehr erhalten, den Protokolltyp, den der NSX-Lastausgleichsdienst für den Zugriff auf diesen Port verwenden kann, den Algorithmus, der für den Lastausgleichsdienst verwendet wird, oder Persistenzeinstellungen.

4 Definieren der Einstellungen für Integritätsprüfungen im virtuellen Server

Durch Auswahl der Option **Anpassen** auf der Registerkarte **Allgemein** können Sie festlegen, wie bzw. ob der NSX-Lastausgleichsdienst Integritätsprüfungen für Pool-Mitglieder innerhalb des virtuellen Servers durchführt.

5 Definieren der erweiterten Einstellungen für den virtuellen Server

Indem Sie die Option **Anpassen** auf der Registerkarte **Allgemein** auswählen, können Sie die NSX-Komponente für den Lastausgleichsdienst anpassen, um Einstellungen wie die Anzahl gleichzeitiger Verbindungen, die ein einzelnes Poolmitglied erkennen kann, und die maximale Anzahl gleichzeitiger Verbindungen, die der virtuelle Server verarbeiten kann, anzugeben.

6 Definieren von Protokollierungsoptionen für den Lastausgleichsdienst

Sie können die Typen der Protokollierungsaktionen für den Lastausgleichsdienst festlegen, die in den Protokollen des Lastausgleichsdiensts erfasst und aufgezeichnet werden.

Definieren der Einstellungen für Mitglieder des Lastausgleichsdiensts

Sie können eine Komponente des bedarfsgesteuerten NSX-Lastausgleichsdiensts definieren, um die Verarbeitung von Aufgaben auf bereitgestellte vSphere-Mitgliedsmaschinen oder Container-Maschinen in einem Netzwerk zu verteilen.

Wenn Sie eine Komponente für den Lastausgleichsdienst zur Design-Arbeitsfläche hinzufügen, können Sie beim Erstellen oder Bearbeiten der Definitionen Ihres virtuellen Servers in der Komponente für den Lastausgleichsdienst entweder eine Standardoption oder eine benutzerdefinierte Option auswählen. Die Standardoption ermöglicht Ihnen die Angabe des Protokolls, des Ports und der Beschreibung für den virtuellen Server sowie der Standardwerte für alle anderen Einstellungen. Mit der benutzerdefinierten Option können Sie zusätzliche Detailebenen definieren.

Wenn der Lastausgleich mit einem externen Netzwerk bereitgestellt wird, müssen sich die VIP-Adresse (mit **VIP-Netzwerk**) und der Mitgliederpool (mit **Mitgliedernetzwerk** angegeben) im selben vorhandenen Netzwerk befinden. Wenn sich die VIP und der Pool nicht im selben externen Netzwerk befinden, tritt ein Fehler während der Bereitstellung auf.

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 die NSX-Bestandsliste für Ihren Cluster erfolgreich ausgeführt wurde.
Um NSX-Konfigurationen in vRealize Automation verwenden zu können, müssen Sie die Datenerfassung ausführen.
- Erstellen Sie ein Netzwerkprofil.
- Melden Sie sich bei vRealize Automation als **Infrastrukturarchitekt** an.
- Öffnen Sie mithilfe der Registerkarte **Design** einen neuen oder vorhandenen Blueprint in der Design-Arbeitsfläche.
- Stellen Sie sicher, dass mindestens eine vSphere-Maschinenkomponente oder -Containerkomponente im Blueprint vorhanden ist.

Verfahren

- 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 **ID** einen Komponentennamen ein, der die Komponente auf der Design-Arbeitsfläche eindeutig kennzeichnet.
- 4 Wählen Sie einen Namen für die vSphere-Maschinenkomponenten oder -Containerkomponenten aus dem Dropdown-Menü **Mitglied** aus.

Die Liste enthält nur die vSphere-Maschinenkomponenten und -Containerkomponenten im aktiven Blueprint.

- 5 Wählen Sie die Netzwerkkarte für den Lastenausgleich über das Dropdown-Menü **Mitgliedernetzwerk** aus.

Die Liste enthält Netzwerkkarten, die für das ausgewählte vSphere-Maschinenmitglied definiert wurden.

- 6 Wählen Sie ein verfügbares Netzwerk für die virtuellen IP-Adressen aus dem Dropdown-Menü **VIP-Netzwerk** aus. Wählen Sie beispielsweise ein verfügbares externes oder NAT-Netzwerk aus.

Da Ihr Blueprint mehrere NSX-Lastenausgleichs- und bedarfsgesteuerte NSX-Netzwerkkomponenten enthalten kann, müssen all diese Komponenten mit demselben VIP-Netzwerk verbunden sein.

- 7 (Optional) Geben Sie in das Textfeld für die **IP-Adresse** eine gültige IP-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 die nächste verfügbare IP-Adresse aus dem zugehörigen VIP-Netzwerk zugewiesen.

Lassen Sie das Feld für die IP-Adresse leer, damit die IP-Adresse während der Bereitstellung vom zugehörigen VIP-Netzwerk zugeteilt wird.

Um eine IP-Adresse angeben zu können, muss die VIP in einem NAT-Netzwerk erstellt werden.

- 8 Um die Definition eines virtuellen Servers zu erstellen, klicken Sie auf **Neu**. Weitere Informationen finden Sie unter [Definieren von allgemeinen Einstellungen für den virtuellen Server](#).

Jede Komponente des Lastenausgleichsdiensts benötigt mindestens einen virtuellen Server.

Informationen zur Angabe von Protokollierungsoptionen finden Sie unter [Definieren von Protokollierungsoptionen für den Lastenausgleichsdienst](#).

Definieren von allgemeinen Einstellungen für den virtuellen Server

Sie können ein einzelnes Protokoll für den virtuellen Server und einen einzelnen Port für Ihren Lastenausgleichsdienst definieren oder weitere virtuelle Server hinzufügen, um zusätzliche NSX-Lastenausgleichsdienstoptionen anzupassen.

Beispiel: Sie können die Komponente für den Lastenausgleichsdienst anpassen, um Einstellungen wie Protokoll und Port, Algorithmus, Persistenz und Transparenz für die Integritätsprüfung zu definieren.

Voraussetzungen

[Definieren der Einstellungen für Mitglieder des Lastenausgleichsdiensts](#).

Verfahren

- 1 Klicken Sie auf die Registerkarte **Allgemein** auf der Seite **Neuer virtueller Server**.

- 2 Wählen Sie das Protokoll für den Netzwerkdatenverkehr im Dropdown-Menü **Protokoll** aus, das Sie für den Lastausgleich des virtuellen Servers verwenden möchten.

Die Protokolloptionen sind HTTP, HTTPS, TCP und UDP.

- 3 Geben Sie einen Portwert in das Textfeld **Port** ein.

Das ausgewählte Protokoll legt die Standardeinstellung für den Port fest.

Protokoll	Standardport
HTTP	80
HTTPS	443
TCP	8080
UDP	Kein Standardport

Die Protokolle HTTP, HTTPS und TCP können einen Port mit UDP gemeinsam verwenden. Beispiel: Wenn Dienst 1 TCP, HTTP oder HTTPS an Port 80 verwendet, kann Dienst 2 UDP an Port 80 verwenden. Wenn Dienst 1 UDP an Port 80 verwendet, kann Dienst 2 UDP nicht an Port 80 verwenden.

- 4 (Optional) Geben Sie eine Beschreibung für die virtuelle Serverkomponente ein.
- 5 Wählen Sie eine der Optionen unter **Einstellungen** aus.

■ **Standardwert für alle anderen Einstellungen verwenden**

Akzeptieren Sie alle anderen Standardeinstellungen. Klicken Sie auf **OK**, um die Definition der Komponente für den Lastausgleichsdienst abzuschließen, und fahren Sie mit dem Arbeiten im Blueprint fort.

Sie können die Standardwerte anzeigen, indem Sie auf **Anpassen** klicken und die weiteren Registerkartenoptionen prüfen. Falls die Standardeinstellungen annehmbar sind, klicken Sie auf der Registerkarte **Allgemein** auf **Standardwert für alle anderen Einstellungen verwenden**.

■ **Anpassen**

Konfigurieren Sie die Komponente für den Lastausgleichsdienst mit zusätzlichen Einstellungen, zum Beispiel zum Definieren eines anderen Protokolls für die Überwachung des Systemzustands oder zum Definieren eines anderen Ports für die Überwachung des von den Mitgliedern verursachten Datenverkehrs.

Weitere Registerkarten werden angezeigt, mit deren Hilfe Sie Einstellungen anpassen können.

Wenn Sie **Standardwert für alle anderen Einstellungen verwenden** ausgewählt und auf **OK** geklickt haben, ist der Vorgang abgeschlossen und Sie können mit dem Definieren und Bearbeiten Ihres Blueprints auf der Design-Arbeitsfläche fortfahren. Wenn Sie **Anpassen** ausgewählt haben, fahren Sie mit dem Schritt fort.

- 6 Klicken Sie auf die Registerkarte **Verteilung** und fahren Sie mit dem Thema [Definieren der Einstellungen für die Verteilung von virtuellen Servern](#) fort, um das Definieren des virtuellen Servers für den NSX-Lastausgleichsdienst fortzusetzen.

Definieren der Einstellungen für die Verteilung von virtuellen Servern

Durch Auswahl der Option **Anpassen** auf der Registerkarte **Allgemein** können Sie Informationen zu den Poolmitgliedern angeben, wie z. B. den Port, an dem die Mitglieder Datenverkehr erhalten, den Protokolltyp, den der NSX-Lastausgleichsdienst für den Zugriff auf diesen Port verwenden kann, den Algorithmus, der für den Lastausgleichsdienst verwendet wird, oder Persistenzeinstellungen.

Ein Pool stellt einen Cluster aus Maschinen mit Lastausgleich dar. Ein Poolmitglied steht für eine Maschine in diesem Cluster.

Das Standardmitgliedsprotokoll und die Mitgliedsporteinstellungen stimmen mit den Protokoll- und Porteeinstellungen auf der Seite **Allgemein** überein.

Der Pool der Mitgliedsmaschinen wird im Optionswert **Mitglied** auf der Benutzeroberfläche der Blueprint-Komponente für den Lastausgleichsdienst angezeigt. Der Eintrag **Mitglied** ist auf den Pool oder Cluster von Maschinen festgelegt.

Voraussetzungen

[Definieren von allgemeinen Einstellungen für den virtuellen Server.](#)

Verfahren

- 1 (Optional) Die Einstellung **Mitgliedsprotokoll** entspricht dem Protokoll, das Sie auf der Registerkarte **Allgemein** angegeben haben. Diese Einstellung definiert, wie das Poolmitglied Netzwerkdatenverkehr empfängt.
- 2 (Optional) Geben Sie eine Portnummer in das Textfeld **Mitgliedsport** ein, um den Port anzugeben, auf dem das Poolmitglied Netzwerkdatenverkehr empfangen soll.

Wenn die eingehende Anforderung für die virtuelle IP-Adresse (VIP) des Lastausgleichsdiensts an Port 80 ankommt, möchten Sie die Anforderung möglicherweise an einen anderen Port innerhalb der Poolmitglieder weiterleiten, zum Beispiel an Port 8080.

3 (Optional) Wählen Sie die algorithmische Ausgleichsmethode für diesen Pool aus.

Die Algorithmusoptionen und die Algorithmusparameter für die Optionen, die diese benötigen, werden in der folgenden Tabelle beschrieben.

Option	Beschreibung und Algorithmusparameter
ROUND_ROBIN	<p>Dabei wird die jedem Server zugeordnete Gewichtung berücksichtigt. Wenn der Lastausgleichsdienst in vRealize Automation erstellt wurde, ist die Gewichtung für alle Mitglieder identisch.</p> <p>Dies ist der geeignetste Algorithmus bei gleichmäßig verteilter Prozessorzeit auf dem Server.</p> <p>Algorithmusparameter sind für diese Option deaktiviert.</p>
IP-HASH	<p>Wählt einen Server auf der Basis eines Hash der Quell-IP-Adresse und der gesamten Gewichtung aller ausgeführten Server aus.</p> <p>Algorithmusparameter sind für diese Option deaktiviert.</p>
LEASTCONN	<p>Verteilt basierend auf der Anzahl der bereits auf den Servern aktiven Verbindungen die Client-Anforderungen an mehrere Server.</p> <p>Neue Verbindungen werden an den Server mit den wenigsten Verbindungen gesendet.</p> <p>Algorithmusparameter sind für diese Option deaktiviert.</p>
URI	<p>Der linke Teil des URI (vor dem Fragezeichen) wird zerlegt und durch die Gesamtgewichtung der ausgeführten Server geteilt.</p> <p>Aus dem Ergebnis wird ersichtlich, welcher Server die Anforderung erhält. Dies gewährleistet, dass ein URI immer auf denselben Server gerichtet ist, solange kein Server heruntergefahren oder gestartet wird.</p> <p>Der URI-Algorithmusparameter verfügt über zwei Optionen: <code>uriLength=<len></code> und <code>uriDepth=<dep></code>. Geben Sie die Parameter für Länge und Tiefe in separate Zeilen in das Textfeld Algorithmus-Parameter ein.</p> <p>Den Parametern für Länge und Tiefe folgt eine positive Ganzzahl. Mit diesen Optionen können Server nur auf der Basis des Anfangs des URI ausgeglichen werden.</p> <p>Der Längenparameter gibt an, dass der Algorithmus nur die definierten Zeichen am Anfang des URI zur Berechnung des Hash verwenden soll. Der Bereich für den Längenparameter lautet <code>1<=len<256</code>.</p> <p>Der Tiefenparameter legt die maximale Verzeichnistiefe zur Berechnung des Hash fest. Jeder Schrägstrich in der Anforderung wird als ein Level behandelt. Der Bereich für den Tiefenparameter lautet <code>1<=dep<10</code>.</p> <p>Bei Angabe beider Parameter wird die Evaluierung beendet, wenn der Wert eines der beiden Parameter erreicht ist.</p>

Option	Beschreibung und Algorithmusparameter
HTTPHEADER	<p>Der Name des HTTP-Headers, der in jeder HTTP-Anforderung gesucht wird. Für den Header-Namen in Klammern wird wie bei der Funktion ACL 'hdr()' nicht zwischen Groß- und Kleinschreibung unterschieden.</p> <p>Der HTTPHEADER-Algorithmusparameter verfügt über eine Option: headerName=<name>. Beispielsweise können Sie als HTTPHEADER-Algorithmusparameter host verwenden.</p> <p>Wenn der Header nicht vorhanden ist oder keinen Wert enthält, wird der Round-Robin-Algorithmus angewendet.</p>
URL	<p>Der im Argument angegebene URL-Parameter wird in der Abfragezeichenfolge jeder HTTP GET-Anforderung gesucht.</p> <p>Der URL-Algorithmusparameter verfügt über eine Option: urlParam=<url>. Stehen nach dem Parameter ein Gleichheitszeichen (=) und ein Wert, erhält der Wert einen Hash und wird durch die gesamte Gewichtung der ausgeführten Server geteilt. Aus dem Ergebnis wird ersichtlich, welcher Server die Anforderung erhält. Mit diesem Vorgang werden Benutzerbezeichner in Anforderungen ermittelt und es wird damit sichergestellt, dass eine bestimmte Benutzer-ID immer zum selben Server gesendet wird, solange kein Server aktiviert oder deaktiviert wird.</p> <p>Wenn kein Wert oder kein Parameter gefunden wurde, wird ein Round-Robin-Algorithmus angewendet.</p>

4 (Optional) Wählen Sie die Persistenzmethode für diesen Pool aus.

Die Persistenz verfolgt und speichert Sitzungsdaten wie das spezifische Poolmitglied, das eine Client-Anforderung verarbeitet hat. Mit Persistenz werden die Client-Anforderungen in einer gesamten Sitzung oder während nachfolgender Sitzungen demselben Poolmitglied zugeordnet.

Protokoll	Unterstützte Persistenzmethode
HTTP	Keine, Cookie, Quell-IP
HTTPS	Keine, Quell-IP und SSL-Sitzungs-ID
TCP	Keine, Quell-IP, MSRDP
UDP	Keine, Quell-IP

- Wählen Sie **Cookie** aus, um ein eindeutiges Cookie zur Identifizierung der Sitzung beim ersten Zugriff eines Clients auf die Site einzufügen. Auf das Cookie wird in den folgenden Anforderungen zur Aufrechterhaltung der Verbindung mit dem jeweiligen Server Bezug genommen.
- Wählen Sie **Quell-IP** aus, um Sitzungen auf der Basis der Quell-IP-Adresse nachzuverfolgen. Wenn ein Client eine Verbindung zu einem virtuellen Server anfordert, der die Affinitätspersistenz der Quelladresse unterstützt, überprüft der Lastausgleichsdienst, ob der Client sich zuvor verbunden hat, und wenn dies der Fall ist, gibt er den Client an dasselbe Poolmitglied zurück.

- Wählen Sie **SSL-Sitzungs-ID** aus und wählen Sie das HTTPS-Datenverkehrsmuster für SSL-Passthrough aus.
 - SSL-Passthrough – Client -> HTTPS-> LB (mit SSL-Passthrough) -> HTTPS -> Server
 - Client -> HTTP-> LB -> HTTP -> Server

Hinweis vRealize Automation unterstützt derzeit nur SSL-Passthrough. Die Methode SSL-Passthrough wird unabhängig davon, welche Option Sie ausgewählt haben, verwendet.

- Wählen Sie **MSRDP** aus, um dauerhafte Sitzungen zwischen Windows-Clients und -Servern beizubehalten, auf denen der Remotedesktopprotokoll-Dienst von Microsoft (RDP) ausgeführt wird. Das empfohlene Szenario für die Aktivierung der MSRDP-Persistenz ist das Erstellen eines Lastausgleichspools, der aus Mitgliedern besteht, die die unterstützte Windows Server-Version ausführen, wobei alle Mitglieder zu einem Windows-Cluster gehören und an einem Windows-Sitzungsverzeichnis teilnehmen.
 - Wählen Sie **Keine** aus, um anzugeben, dass die Sitzungsaktionen nicht für nachfolgende Rückrufe gespeichert werden.
- 5** Wenn Sie eine Cookiepersistenzeinstellung verwenden, geben Sie den Cookienamen ein.
- 6** (Optional) Wählen Sie den Modus aus, in dem das Cookie über das Dropdown-Menü **Modus** eingefügt wird.

Option	Beschreibung
Einfügen	<p>NSX Edge sendet ein Cookie.</p> <p>Sendet der Server eines oder mehrere Cookies, dann erhält der Client ein zusätzliches Cookie (Server-Cookie(s) + NSX Edge-Cookie). Sendet der Server keine Cookies, dann erhält der Client nur das NSX Edge-Cookie.</p>
Präfix	<p>Der Server sendet ein Cookie. Verwenden Sie diese Option, wenn Ihr Client nur ein Cookie unterstützt.</p> <p>Wenn Sie über eine proprietäre Anwendung verfügen, die einen proprietären Client verwendet, der nur ein Cookie unterstützt, sendet der Webserver ein Cookie, aber der NSX Edge fügt seine Cookieinformationen im Servercookiewert (als Präfix) ein.</p>
App-Sitzung	<p>Der Server sendet kein Cookie. Stattdessen sendet er die Informationen zur Benutzersitzung als URL.</p> <p>Beispiel: <code>http://mysite.com/admin/UpdateUserServlet;jsessionid=X000X0XXX0XXXX</code>, wobei <code>jsessionid</code> die Informationen zur Benutzersitzung darstellen und für die Persistenz verwendet werden.</p>

- 7** (Optional) Geben Sie das Persistenz-Ablaufdatum für das Cookie in Sekunden ein.

Beispiel: Der Persistenzeintrag für den L7-Lastausgleich mit einer TCP-Quell-IP läuft ab, wenn keine neuen TCP-Verbindungen für das angegebene Ablaufdatum hergestellt werden, auch wenn die vorhandenen Verbindungen immer noch aktiv sind.

- 8** (Optional) Klicken Sie auf die Registerkarte **Integritätsprüfung** und fahren Sie mit dem Thema [Definieren der Einstellungen für Integritätsprüfungen im virtuellen Server](#) fort, um das Definieren des virtuellen Servers für den NSX-Lastausgleichsdienst fortzusetzen.

Definieren der Einstellungen für Integritätsprüfungen im virtuellen Server

Durch Auswahl der Option **Anpassen** auf der Registerkarte **Allgemein** können Sie festlegen, wie bzw. ob der NSX-Lastausgleichsdienst Integritätsprüfungen für Pool-Mitglieder innerhalb des virtuellen Servers durchführt.

Die Standardeinstellungen für Integritätsprüfungsprotokolle und -ports stimmen mit den Protokoll- und Porteeinstellungen auf der Registerkarte **Allgemein** überein.

Weitere Informationen finden Sie unter *Create a Service Monitor* in der NSX-Produktdokumentation unter https://www.vmware.com/support/pubs/nsx_pubs.html. Beachten Sie, dass in der NSX-Dokumentation das Mitglied des virtuellen Servers als Poolmitglied bezeichnet wird.

Voraussetzungen

[Definieren von allgemeinen Einstellungen für den virtuellen Server.](#)

Verfahren

- 1** (Optional) Wählen Sie im Dropdown-Menü **Integritätsprüfungsprotokoll** ein Integritätsprüfungsprotokoll aus, um anzugeben, wie der Zugriff auf das Poolmitglied erfolgt, wenn der Lastausgleichsdienst das Poolmitglied überwacht, um dessen Integrität zu bestimmen.

Die Protokolloptionen sind **HTTP, HTTPS, TCP, ICMP, UDP** und **Keine**.

Sie können auch das Standardprotokoll wie angegeben auf der Registerkarte „Allgemein“ akzeptieren.

- 2** (Optional) Geben Sie einen Wert in das Feld **Integritätsprüfungsport** ein, um anzugeben, welcher Port vom Lastausgleichsdienst abgehört wird, um die Integrität des virtuellen Servermitglieds bzw. des Poolmitglieds zu überwachen.

Beachten Sie, dass in der NSX-Dokumentation das Mitglied des virtuellen Servers als Poolmitglied bezeichnet wird.

Die Protokolle HTTP, HTTPS und TCP können einen Port mit UDP gemeinsam verwenden. Beispiel: Wenn Dienst 1 TCP, HTTP oder HTTPS an Port 80 verwendet, kann Dienst 2 UDP an Port 80 verwenden. Wenn Dienst 1 UDP an Port 80 verwendet, kann Dienst 2 UDP nicht an Port 80 verwenden.

- 3** Geben Sie das **Intervall**, in dem ein Server gepingt werden soll, in Sekunden ein.
- 4** Geben Sie den maximalen Wert für die **Zeitüberschreitung** in Sekunden ein, in der eine Antwort vom Server empfangen werden muss.
- 5** Geben Sie einen Wert für **Max. Wiederholungen** ein, um anzugeben, wie oft der Server gepingt werden muss, bevor er als inaktiv erklärt wird.

- 6** Geben Sie zusätzliche Einstellungen für die Integritätsprüfung entsprechend dem ausgewählten **Integritätsprüfungsprotokoll** an.
- a Geben Sie die **Methode** ein, die für das Erkennen des Serverstatus verwendet wird. Die Optionen sind GET, OPTIONS und POST.
 - b Geben Sie die **URL** ein, die in der Anforderung für das Erkennen des Serverstatus verwendet wird. Dies ist die URL, die für die Optionen der GET- und POST-Methode (standardmäßig „/“) verwendet wird.
 - c Geben Sie in das Textfeld **Senden** die Zeichenfolge ein, an den Server gesendet werden soll, nachdem eine Verbindung hergestellt wurde.

Geben Sie in das Textfeld **Senden** die Zeichenfolge ein, an den Server gesendet werden soll, nachdem eine Verbindung hergestellt wurde.
 - d Geben Sie im Textfeld **Empfangen** die Zeichenfolge ein, die vom Server erwartet wird.

Der Server wird erst dann als aktiv eingestuft, wenn die empfangene Zeichenfolge mit dieser Definition übereinstimmt.

Die Zeichenfolge kann sich in der Kopfzeile oder im Text der Antwort befinden.
- 7** Klicken Sie auf die Registerkarte **Erweitert** und fahren Sie mit dem Thema [Definieren der erweiterten Einstellungen für den virtuellen Server](#) fort, um das Definieren des virtuellen Servers für die NSX-Lastausgleichskomponente fortzusetzen.

Informationen zur Angabe von Protokollierungsoptionen finden Sie unter [Definieren von Protokollierungsoptionen für den Lastausgleichsdienst](#).

Definieren der erweiterten Einstellungen für den virtuellen Server

Indem Sie die Option **Anpassen** auf der Registerkarte **Allgemein** auswählen, können Sie die NSX-Komponente für den Lastausgleichsdienst anpassen, um Einstellungen wie die Anzahl gleichzeitiger Verbindungen, die ein einzelnes Poolmitglied erkennen kann, und die maximale Anzahl gleichzeitiger Verbindungen, die der virtuelle Server verarbeiten kann, anzugeben.

Voraussetzungen

[Definieren von allgemeinen Einstellungen für den virtuellen Server.](#)

Verfahren

- 1** Geben Sie einen Wert in das Textfeld **Verbindungsgrenzwert** ein, um die maximale Anzahl gleichzeitiger Verbindungen in NSX anzugeben, die der virtuelle Server verarbeiten kann.

Diese Einstellung berücksichtigt die Anzahl aller Mitgliedsverbindungen.

Geben Sie einen Wert von 0 ein, um keinen Grenzwert anzugeben.
- 2** Geben Sie einen Wert in das Textfeld **Grenzwert für Verbindungsrate** ein, um die maximale Anzahl der Anforderungen für eingehende Verbindungen in NSX anzugeben, die pro Sekunde akzeptiert werden können.

Diese Einstellung berücksichtigt die Anzahl aller Mitgliedsverbindungen.

Geben Sie einen Wert von 0 ein, um keinen Grenzwert anzugeben.

- 3 (Optional) Aktivieren Sie das Kontrollkästchen **Beschleunigung aktivieren**, um anzugeben, dass jede virtuelle IP (VIP) den schnelleren L4-Lastausgleichsdienst anstelle des L7-Lastausgleichsdiensts verwendet.
- 4 (Optional) Aktivieren Sie das Kontrollkästchen **Transparent**, damit die Poolmitglieder des Lastausgleichsdiensts die IP-Adresse der Maschinen anzeigen können, die den Lastausgleichsdienst aufrufen.

Wenn Sie das Kontrollkästchen nicht aktivieren, betrachten die Poolmitglieder des Lastausgleichsdiensts die Quell-IP-Adresse des Datenverkehrs als eine interne IP-Adresse des Lastausgleichsdiensts.

- 5 Geben Sie einen Wert in das Textfeld **Maximale Anzahl an Verbindungen** ein, um die maximale Anzahl gleichzeitiger Verbindungen anzugeben, die ein einzelnes Poolmitglied erkennen kann.

Wenn die Anzahl der eingehenden Anforderungen höher als dieser Wert ist, werden die Anforderungen in die Warteschlange gestellt und anschließend in der Reihenfolge verarbeitet, in der sie beim Freigeben der Verbindungen empfangen wurden.

Geben Sie einen Wert von 0 ein, um keinen Maximalwert anzugeben.

- 6 Geben Sie einen Wert in das Textfeld **Mindestanzahl an Verbindungen** ein, um die Mindestanzahl gleichzeitiger Verbindungen anzugeben, die ein einzelnes Poolmitglied immer akzeptieren muss.

Geben Sie einen Wert von 0 ein, um keinen Mindestwert anzugeben.

- 7 Klicken Sie auf **OK**, um die Definition des virtuellen Servers abzuschließen.
- 8 Informationen zur Angabe von Protokollierungsoptionen finden Sie unter [Definieren von Protokollierungsoptionen für den Lastausgleichsdienst](#). Klicken Sie andernfalls auf **Speichern** oder **Fertig stellen**.

Definieren von Protokollierungsoptionen für den Lastausgleichsdienst

Sie können die Typen der Protokollierungsaktionen für den Lastausgleichsdienst festlegen, die in den Protokollen des Lastausgleichsdiensts erfasst und aufgezeichnet werden.

Nachdem Sie eine Komponente für den Lastausgleichsdienst definiert haben oder während dieses Verfahrens können Sie die Protokollierungsebene für das Erfassen von Datenverkehrsprotokollen für den Lastausgleichsdienst angeben. Die Protokollierungsebenen, die Sie für Lastausgleichsdienstkomponenten im Blueprint definieren, gelten für alle im Blueprint definierten Lastausgleichsdienste.

Zu den Protokollierungsebenen zählen die Ebenen „Debuggen“, „Info“, „Warnung“, „Fehler“ und „Kritisch“. Mit den Optionen „Debuggen“ und „Info“ werden Benutzeranforderungen protokolliert, während mit den Optionen „Warnung“, „Fehler“ und „Kritisch“ keine Benutzeranforderungen protokolliert werden.

Weitere Informationen zur Protokollierung für den NSX-Lastausgleichsdienst finden Sie im *Administratorhandbuch für NSX*.

Voraussetzungen

[Definieren der Einstellungen für Mitglieder des Lastausgleichsdiensts.](#)

Verfahren

- 1 Wählen Sie die Registerkarte **Global** in der Lastausgleichsdienstkomponente auf der Design-Arbeitsfläche aus.
- 2 Wählen Sie eine oder mehrere Protokollierungsoptionen aus dem Dropdown-Menü **Protokollierungsebene** aus.

Wählen Sie eine Protokollierungsebene für die Erfassung von Protokollen für den Datenverkehr des Lastausgleichsdiensts aus. Die Einstellung gilt für alle Komponenten des NSX-Lastausgleichsdiensts im Blueprint.

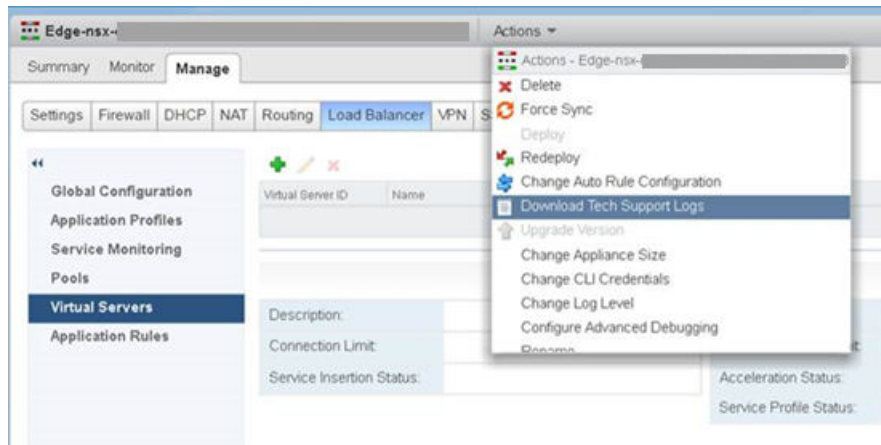
Die Protokollierungseinstellungen werden im vSphere Web Client definiert.

- Keine
- Info
- Notfall
- Alarm
- Kritisch
- Fehler
- Warnung
- Hinweis
- Debuggen

- 3 Klicken Sie auf **Speichern**.

Ergebnisse

Sie können die Protokolle im vSphere Web Client anzeigen und herunterladen. Verwenden Sie hierzu das Menü **Aktionen** für NSX Edge, wie in *Download Tech Support Logs for NSX Edge* in der NSX-Produktdokumentation unter https://www.vmware.com/support/pubs/nsx_pubs.html beschrieben.



Verwenden von Sicherheitskomponenten auf der Design-Arbeitsfläche

Sie können NSX-Sicherheitskomponenten zur Arbeitsfläche hinzufügen, um deren konfigurierte Einstellungen einer oder mehreren vSphere-Maschinen-Komponenten im Blueprint zur Verfügung zu stellen.

Sicherheitsgruppen, -Tags und -Richtlinien werden außerhalb von vRealize Automation in der NSX-Anwendung konfiguriert.

Die Netzwerk- und Sicherheitskomponenteneinstellungen, die Sie zur Design-Arbeitsfläche hinzufügen, werden von der NSX-Konfiguration abgeleitet. Dafür muss die Datenerfassung für den NSX-Bestand für vSphere-Cluster 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 Netzwerkadapter 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 vorhandene oder bedarfsgesteuerte NSX-Sicherheitsgruppen zu einem Blueprint hinzufügen.

Sie können eine oder mehrere bedarfsgesteuerte Sicherheitsgruppen erstellen. Sie können eine oder mehrere Sicherheitsrichtlinien auswählen, um eine Sicherheitsgruppe zu konfigurieren.

Sicherheitsgruppen werden in der Quellressource verwaltet. Informationen zum Verwalten von Sicherheitsgruppen für verschiedene Ressourcentypen finden Sie in der NSX-Dokumentation.

Wenn ein Blueprint einen oder mehrere Lastausgleichsdienste enthält und die Anwendungsisolierung für den Blueprint aktiviert ist, werden die Lastausgleichs-VIPs als IPSet zur Sicherheitsgruppe der Anwendungsisolierung hinzugefügt. Wenn ein Blueprint eine On-Demand-Sicherheitsgruppe enthält, die einer Maschinenebene zugewiesen ist, welche auch einem Lastausgleichsdienst zugewiesen ist, enthält die On-Demand-Sicherheitsgruppe die Maschinenebene und das IPSet mit der Lastausgleichs-VIP.

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 Design-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.

Steuern des Mandantenzugriffs für Sicherheitsobjekte

Sie können die mandantenübergreifende Verfügbarkeit von NSX-Sicherheitsobjekten in vRealize Automation steuern.

Wenn Sie ein NSX-Sicherheitsobjekt in vRealize Automation erstellen, kann seine Standardverfügbarkeit entweder auf „Global“, d. h. verfügbar in allen Mandanten, für die der zugehörige Endpoint eine Reservierung aufweist, oder auf „Verborgen“ für alle Benutzer mit Ausnahme des Administrators gesetzt sein.

Die mandantenübergreifende Verfügbarkeit von Sicherheitsobjekten richtet sich auch danach, ob der zugehörige Endpoint eine Reservierung oder Reservierungsrichtlinie im Mandanten aufweist.

NSX fungiert nicht als Mandant für Sicherheitsgruppen. Sie können die Verfügbarkeit von Sicherheitsgruppen in vRealize Automation jedoch mithilfe der benutzerdefinierten Eigenschaft `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` steuern.

Standardmäßig stehen neue Sicherheitsobjekte allen Mandanten für die zugeordneten NSX-Endpoints zur Verfügung, in denen Sie über eine Reservierung verfügen. Wenn der Endpoint keine Reservierung im aktiven Mandanten aufweist, stehen die Sicherheitsobjekte im aktiven Mandanten nicht zur Verfügung.

Wenn Sie die benutzerdefinierte Eigenschaft `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` nicht auf NSX-Endpoints festgelegt haben, werden neue Sicherheitsobjekte standardmäßig auf „Global“ gesetzt. Sicherheitsobjekte, die vor dem Upgrade auf diese Version von vRealize Automation vorhanden waren, werden unabhängig von der benutzerdefinierten Eigenschaft auf „Global“ gesetzt.

Hinweis Wenn Sie ein Upgrade auf diese vRealize Automation-Version durchführen, werden Sicherheitsgruppen aus der vorherigen Version standardmäßig auf „Global“ gesetzt. Vorhandene Sicherheitsgruppen und Sicherheits-Tags sind in allen Mandanten verfügbar, in denen der zugeordnete Endpoint eine Reservierung aufweist.

Sie können neue Sicherheitsgruppen standardmäßig ausblenden, indem Sie die benutzerdefinierte Eigenschaft `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` zum zugeordneten NSX-Endpoint hinzufügen. Diese Einstellung wird wirksam, wenn das nächste Mal Daten für den NSX-Endpoint erfasst werden, und gilt nur für neue Sicherheitsobjekte.

Sie können die Mandanteneinstellung eines vorhandenen Sicherheitsobjekts auch programmgesteuert ändern. Wenn eine Sicherheitsgruppe beispielsweise auf „Global“ gesetzt ist, können Sie die Mandantenverfügbarkeit eines Sicherheitsobjekts ändern, indem Sie die Einstellung „Mandanten-ID“ des zugeordneten NSX-Endpoints in der REST-API von vRealize Automation oder in vRealize CloudClient verwenden. Die verfügbaren Einstellungen unter „Mandanten-ID“ für den NSX-Endpoint lauten wie folgt:

- "`<global>`" – das Sicherheitsobjekt steht allen Mandanten zur Verfügung. Dies ist die Standardeinstellung für vorhandene Sicherheitsobjekte nach dem Upgrade auf diese Version und für alle neuen Sicherheitsobjekte, die Sie erstellen.
- "`<unscoped>`" – das Sicherheitsobjekt steht keinem Mandanten zur Verfügung. Nur der Systemadministrator kann auf das Sicherheitsobjekt zugreifen. Diese Einstellung eignet sich für die Definition von Sicherheitsobjekten, die irgendwann einem bestimmten Mandanten zugewiesen werden sollen.
- "`Tenant_id_name`" – das Sicherheitsobjekt steht nur einem einzelnen benannten Mandanten zur Verfügung.

Sie können die REST-API von vRealize Automation oder die vRealize CloudClient-Tools verwenden, um einem benannten Mandanten den Parameter „Mandanten-ID“ (*tenantid*) von Sicherheitsobjekten zuzuweisen, die mit einem bestimmten Endpoint verbunden sind. Weitere Informationen finden Sie unter <https://code.vmware.com/apis/vrealize-automation> und <https://code.vmware.com/web/dp/explorer-apis>. Informationen zu vRealize CloudClient finden Sie unter <https://code.vmware.com/web/dp/tool/cloudclient>. Weitere Informationen finden Sie im vRealize Automation *Programmierhandbuch* unter <https://docs.vmware.com/de/vRealize-Automation>.

Hinzufügen einer vorhandenen Sicherheitsgruppenkomponente

Sie können eine vorhandene NSX-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.

Standardmäßig werden nur die Sicherheitsgruppen, die für den aktuellen Mandanten gelten, beim Erstellen eines Blueprints angezeigt. Insbesondere werden Sicherheitsgruppen zur Verfügung gestellt, wenn der zugeordnete Endpoint eine Reservierung im aktuellen Mandanten aufweist.

Weitere Informationen zur Steuerung des Mandantenzugriffs finden Sie unter [Steuern des Mandantenzugriffs für Sicherheitsobjekte](#).

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 die NSX-Bestandsliste für Ihren Cluster erfolgreich ausgeführt wurde.
Um NSX-Konfigurationen in vRealize Automation verwenden zu können, müssen Sie die Datenerfassung ausführen.
- Lesen Sie sich noch einmal die Konzepte der Sicherheitskomponenten durch. Siehe [Verwenden von Sicherheitskomponenten auf der Design-Arbeitsfläche](#).
- Melden Sie sich bei vRealize Automation als **Infrastrukturarchitekt** an.
- Öffnen Sie mithilfe der Registerkarte **Design** einen neuen oder vorhandenen Blueprint in der Design-Arbeitsfläche.

Verfahren

- 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.

Ergebnisse

Sie können weitere Sicherheitseinstellungen konfigurieren, indem Sie zusätzliche Sicherheitskomponenten hinzufügen und Einstellungen auf der Registerkarte **Sicherheit** einer vSphere-Maschinenkomponente auf der Design-Arbeitsfläche auswählen.

Hinzufügen einer bedarfsgesteuerten Sicherheitsgruppenkomponente

Sie können eine bedarfsgesteuerte NSX-Sicherheitsgruppenkomponente zur Design-Arbeitsfläche hinzufügen, um die Zuordnung ihrer Einstellungen zu einer oder mehreren vSphere-Maschinenkomponenten oder zu anderen verfügbaren Komponententypen im Blueprint vorzubereiten.

Beim Erstellen einer bedarfsgesteuerten Sicherheitsgruppe fügen Sie Sicherheitsrichtlinien zum Erstellen der Gruppe hinzu. Die Sicherheitsrichtlinien können global angezeigt oder standardmäßig ausgeblendet werden. Richtlinien werden nur in Mandanten angezeigt, für die der zugeordnete NSX-Endpoint eine Reservierung in diesem Mandanten aufweist.

Standardmäßig werden nur die Sicherheitsgruppen, die für den aktuellen Mandanten gelten, beim Erstellen eines Blueprints angezeigt. Insbesondere werden Sicherheitsgruppen zur Verfügung gestellt, wenn der zugeordnete Endpoint eine Reservierung im aktuellen Mandanten aufweist. Weitere Informationen zur Steuerung des Mandantenzugriffs finden Sie unter [Steuern des Mandantenzugriffs für Sicherheitsobjekte](#).

Voraussetzungen

- Erstellen und konfigurieren Sie eine Sicherheitsrichtlinie in NSX. Informationen dazu finden Sie im *NSX-Administratorhandbuch*.
- Stellen Sie sicher, dass die NSX-Bestandsliste für Ihren Cluster erfolgreich ausgeführt wurde.
Um NSX-Konfigurationen in vRealize Automation verwenden zu können, müssen Sie die Datenerfassung ausführen.
- Melden Sie sich bei vRealize Automation als **Infrastrukturarchitekt** an.
- Lesen Sie sich noch einmal die Konzepte der Sicherheitskomponenten durch. Siehe [Verwenden von Sicherheitskomponenten auf der Design-Arbeitsfläche](#).
- Öffnen Sie mithilfe der Registerkarte **Design** einen neuen oder vorhandenen Blueprint in der Design-Arbeitsfläche.

Verfahren

- 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.

Ergebnisse

Sie können weitere Sicherheitseinstellungen konfigurieren, indem Sie zusätzliche Sicherheitskomponenten hinzufügen und Einstellungen auf der Registerkarte **Sicherheit** einer vSphere-Maschinenkomponente auf der Design-Arbeitsfläche auswählen.

Hinzufügen einer vorhandenen Sicherheits-Tag-Komponente

Sie können eine NSX-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.

Standardmäßig werden Sicherheits-Tags, die für den aktuellen Mandanten gelten, beim Erstellen eines Blueprints angezeigt. Insbesondere werden Sicherheits-Tags zur Verfügung gestellt, wenn der zugehörige Endpoint eine Reservierung im aktuellen Mandanten aufweist. Weitere Informationen zur Steuerung des Mandantenzugriffs finden Sie unter [Steuern des Mandantenzugriffs für Sicherheitsobjekte](#).

Sie können mehrere Netzwerk- und Sicherheitskomponenten zur 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 die NSX-Bestandsliste für Ihren Cluster erfolgreich ausgeführt wurde. Um NSX-Konfigurationen in vRealize Automation verwenden zu können, müssen Sie die Datenerfassung ausführen.
- Melden Sie sich bei vRealize Automation als **Infrastrukturarchitekt** an.
- Öffnen Sie mithilfe der Registerkarte **Design** einen neuen oder vorhandenen Blueprint in der Design-Arbeitsfläche.

Verfahren

- 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.

Ergebnisse

Sie können weitere Sicherheitseinstellungen konfigurieren, indem Sie zusätzliche Sicherheitskomponenten hinzufügen und Einstellungen auf der Registerkarte **Sicherheit** einer vSphere-Maschinenkomponente auf der Design-Arbeitsfläche auswählen.

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 Design-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.

Sie können eine bedarfsgesteuerte NAT-Netzwerkkomponente auf die Design-Arbeitsfläche ziehen und mit einer Komponente einer vSphere-Maschine oder einer Komponente eines NSX-Lastausgleichsdiensts im Blueprint verknüpfen.

Die Netzwerk- und Sicherheitskomponenteneinstellungen, die Sie zur Design-Arbeitsfläche hinzufügen, werden von der NSX-Konfiguration abgeleitet. Dafür muss die Datenerfassung für den NSX-Bestand für vSphere-Cluster 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*.

Hinweis Wenn ein Blueprint einen oder mehrere Lastausgleichsdienste enthält und die Anwendungsisolierung für den Blueprint aktiviert ist, werden die Lastausgleichs-VIPs als IPSet zur Sicherheitsgruppe der Anwendungsisolierung hinzugefügt. Wenn ein Blueprint eine On-Demand-Sicherheitsgruppe enthält, die einer Maschinenebene zugewiesen ist, welche auch einem Lastausgleichsdienst zugewiesen ist, enthält die On-Demand-Sicherheitsgruppe die Maschinenebene und das IPSet mit der Lastausgleichs-VIP.

Informationen dazu, wie Sie NAT-Regeln verwenden, um die Zuordnung eines TCP- oder UDP-Ports von der externen IP-Adresse einer Edge (Quellport) zu einer privaten IP-Adresse in der NAT-Netzwerkkomponente (Zielpport) zu ermöglichen, finden Sie unter [Erstellen und Verwenden von NAT-Regeln](#).

Konfigurieren eines bereitzustellenden Blueprints in einer OVF-Datei

Sie können eine OVF-Datei verwenden, um vSphere-Maschineneigenschaften und -Hardwareeinstellungen zu definieren, die normalerweise auf Blueprint-Konfigurationsseiten in vRealize Automation oder programmatisch durch Verwendung von vRealize Automation-REST-APIs oder vRealize CloudClient definiert werden.

Sie können zum Definieren eines Wertsatzes für ein Image-Komponentenprofil auch Einstellungen von einer OVF-Datei importieren. Parametrisierte Blueprints verwenden die Komponentenprofiltypen Image und Größe.

OVF ist ein Open-Source-Standard für die Verpackung und Verteilung von Softwareanwendungen für virtuelle Maschinen.

Eine OVF-Bereitstellung ähnelt dem Klonen, die Quellmaschine ist jedoch eine auf einem Server oder einer Website gehostete OVF-Vorlage statt einer in vCenter gehosteten VM-Vorlage.

Eine OVF-Datei wird normalerweise zum Beschreiben einer einzelnen virtuellen Maschine oder virtuellen Appliance verwendet. Sie kann Informationen zum Format der virtuellen Festplatten-Image-Datei und eine Beschreibung der virtuellen Hardware, die zum Ausführen des Betriebssystems oder der auf dem Festplatten-Image enthaltenen Anwendung emuliert werden muss, enthalten. Eine OVA-Datei ist ein virtuelles Appliance-Paket, das Dateien zum Beschreiben einer virtuellen Maschine enthält. Dazu gehören eine OVF-Deskriptordatei, optionale Manifest- und Zertifikatsdateien und andere zugehörige Dateien.

Die Bereitstellungsoption `ImportOvfWorkflow` ist auf einer vSphere-Maschinenkomponente verfügbar, wenn Sie einen Blueprint definieren. Sie ist auch dann verfügbar, wenn Sie im Eigenschaftenwörterbuch einen Wertsatz für ein Image-Komponentenprofil erstellen.

Sie können einer OVF-Datei Blueprint-Konfigurationseinstellungen hinzufügen, um folgende Informationstypen zu beschreiben:

- Zuweisung von CPU-Minimum, Arbeitsspeicher und Speicher.
- Vom Benutzer konfigurierbare benutzerdefinierte Eigenschaften.
- Komponentenprofileinstellungen für Blueprint-Parametrisierung.

OVF und OVA in Verbindung mit mehreren Maschinen wird nicht unterstützt.

Wichtige Aspekte enthalten die folgenden Anweisungen:

- OVF-Dateien und OVA-Pakete werden unterstützt.
- Standardauthentifizierung des Benutzernamens und des Kennworts für den HTTP-Server, auf dem sich die gehostete OVF- oder OVA-Datei befindet, wird unterstützt. Die angegebene URL wird im Blueprint überprüft.
- OVFs und OVAs werden bei der Erfassung von Daten von vCenter Server nicht erfasst.
- EBS-Abonnements werden unterstützt.
- Sie können beim Importieren benutzerkonfigurierbarer OVF-Einstellungen in den Blueprint benutzerdefinierte Eigenschaften definieren.

- Sie können beim Anfordern einer vSphere-Maschinenbereitstellung aus einem OVF-Import abgerufene Einstellungen hinzufügen, ändern oder entfernen.
- Bei der Neukonfiguration der Maschine können Sie Einstellungen hinzufügen, ändern oder entfernen.

Definieren von Blueprint-Einstellungen für eine vSphere-Komponente unter Verwendung einer OVF-Datei

Sie können Einstellungen aus einer OVF-Datei importieren, um die Konfiguration der Einstellungen für vSphere-Maschinenkomponenten in einem vRealize Automation-Blueprint zu vereinfachen.

Bei diesem Verfahren wird davon ausgegangen, dass Sie über grundlegende Kenntnisse bezüglich der Erstellung eines vRealize Automation-Blueprints verfügen.

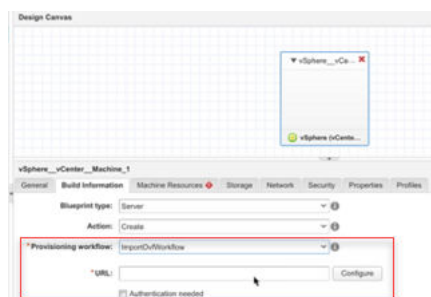
Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Infrastrukturarchitekt** an.
- Erfüllen Sie die verbleibenden Voraussetzungen unter [Konfigurieren eines Maschinen-Blueprints](#).

Verfahren

- 1 Wählen Sie **Design > Blueprints** aus.
- 2 Klicken Sie auf das Symbol **Neu (+)**.
- 3 Geben Sie einen Namen und eine Beschreibung für den Blueprint ein und klicken Sie auf **OK**.
- 4 Klicken Sie im Bereich „Kategorien“ auf **Maschinentypen** und ziehen Sie eine **vSphere (vCenter)-Maschinenkomponente** auf die Design-Arbeitsfläche.
- 5 Klicken Sie auf die Registerkarte **Build-Informationen** und geben Sie die folgenden Optionen ein:
 - **Blueprint-Typ:** Server
 - **Aktion:** Erstellen
 - **Bereitstellungsworkflow:** ImportOvfWorkflow

Mit dieser ImportOvfWorkflow-Einstellung ist die Option **URL** verfügbar.



6 Geben Sie den Speicherort der OVF-Datei an.

- Geben Sie den Pfad zur OVF-URL unter Verwendung des Formats `https://server/folder/name.ovf` oder `name.ova` ein.

Wenn Sie die Authentifizierung beim Server, der die OVF-Datei hostet, aktivieren, geben Sie die Anmeldedaten für den zu authentifizierenden Benutzer ein.

- Wenn die OVF-Datei auf einer Website gehostet wird und Sie einen Proxy-Endpoint erstellt haben, der für den Zugriff auf die Website verwendet werden soll, wählen Sie **Proxy verwenden** und den verfügbaren Proxy-Endpoint aus.

7 Klicken Sie auf **Konfigurieren**.

Hinweis Wenn Sie eine Authentifizierungsfehlermeldung erhalten, sind für den Server, auf dem die OVF-Datei gehostet ist, Anmeldedaten für die Authentifizierung erforderlich. Aktivieren Sie in diesem Fall das Kontrollkästchen **Authentifizierung erforderlich**, geben Sie unter **Benutzername** und **Kennwort** die Anmeldedaten für die Authentifizierung beim HTTP-Server ein, auf dem sich die OVF-Datei befindet, und klicken Sie erneut auf **Konfigurieren**.

Mit der Option „Konfigurieren“ wird ein Assistent geöffnet, der alle benutzerkonfigurierbaren Eigenschaften und Werte anzeigt, die aus der OVF-Datei als benutzerdefinierte Eigenschaften importiert werden sollen. Der Bereich ist leer, wenn es keine zu importierenden konfigurierbaren Eigenschaften gibt.

- akzeptieren Sie mithilfe des Assistenten entweder die zu importierenden Standardwerte oder ändern Sie die Werte für den Blueprint vor dem Import.
- Klicken Sie auf **OK**, um die Eigenschaften und Werte zu importieren.

Einige benutzerkonfigurierbare Eigenschaften in der OVF-Vorlage werden als editierbare benutzerdefinierte Eigenschaften von vRealize Automation in den Blueprint importiert, und VMware.Ovf wird vorangestellt. Andere Eigenschaften hingegen werden als ausgeblendete Eigenschaften importiert, die nach dem Import nicht zur Bearbeitung vorgesehen sind.

8 Klicken Sie auf die Registerkarte **Maschinenressourcen**, um die Ergebnisse des OVF-Imports anzuzeigen, die sich aus den Mindestwerteinträgen für die Optionen **CPUs**, **Arbeitsspeicher (MB)** und **Speicher (GB)** zusammensetzen.

Sie können jeden dieser Werte nach dem Importieren ändern.

9 Klicken Sie auf die Registerkarte **Speicher**, um die Ergebnisse des OVF-Imports anzuzeigen.**10** Klicken Sie auf die Registerkartenabfolge **Eigenschaften > Benutzerdefinierte Eigenschaften**, um die Ergebnisse des OVF-Imports anzuzeigen.**11** Klicken Sie auf **Speichern**.**Nächste Schritte**

Fahren Sie mit dem Definieren der Blueprint-Einstellungen fort oder klicken Sie auf **Fertig stellen**.

Definieren eines Image-Wertsatzes für ein Komponentenprofil unter Verwendung einer OVF-Datei

Sie können Einstellungen von einer OVF-Datei importieren, um einen oder mehrere Wertsätze für ein Image-Komponentenprofil zur Verwendung in einem parametrisierten vRealize Automation-Blueprint zu erstellen.

Nachdem Sie Wertsatzdefinitionen für das Komponentenprofil **Image** importiert haben, können Sie dem Komponentenprofil für eine vSphere-Maschinenkomponente in einem Blueprint einen oder mehrere Wertsätze hinzufügen. Wenn ein Benutzer ein Katalogelement anfordert, kann er ein verfügbares Image auswählen und unter Verwendung von Parametern, die im Wertsatz des Images definiert sind, bereitstellen.

Wenn Sie die OVF-Datei importieren, werden benutzerkonfigurierbare Eigenschaften und Werte in der OVF-Datei nicht als benutzerdefinierte Eigenschaften in den Wertsatz importiert. Wenn Sie neue benutzerdefinierte Eigenschaften aus der importierten OVF-Datei in Bezug auf den Image-Wertsatz verwenden möchten, müssen Sie die neuen benutzerdefinierten Eigenschaften in der vSphere-Maschinenkomponente oder im gesamten Blueprint manuell definieren. Die im parametrisierten Blueprint erstellten benutzerdefinierten Eigenschaften sollten auf den Wertsatz für jedes Komponentenprofil-Image anwendbar sein.

Hinweis Die benutzerdefinierten OVF-Eigenschaften für vRealize Automation sind nicht anwendbar auf die benutzerdefinierten OVF-Eigenschaften für vSphere. Ziehen Sie in Betracht, einen Image-Wertsatz für vRealize Automation und einen Image-Wertsatz für vSphere zu erstellen.

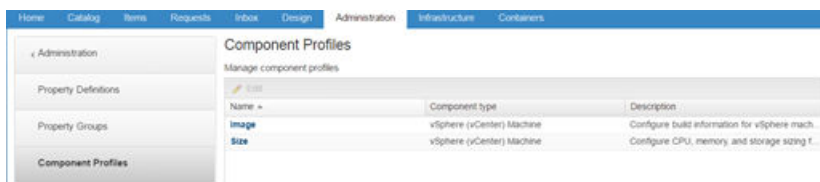
Weitere Informationen zur Verwendung von Komponentenprofilen für die Blueprint-Parametrisierung finden Sie unter [Verstehen und Verwenden der Blueprint-Parametrisierung](#).

Voraussetzungen

- Melden Sie sich bei vRealize Automation als Administrator mit **Mandantenadministrator-** und **IaaS-Administrator-**Zugriffsrechten an.

Verfahren

- 1 Wählen Sie **Administration > Eigenschaftenwörterbuch > Komponentenprofile** aus.



- 2 Klicken Sie in der Spalte „Name“ auf **Image**.

Es werden Informationen über die angegebene Image-Komponenteneigenschaft angezeigt.

- 3 Klicken Sie auf die Registerkarte **Wertsätze**.

- 4 Klicken Sie zum Definieren eines neuen Wertsatzes auf **Neu** und konfigurieren Sie dann die **Image-Einstellungen**.
 - a Geben Sie in das Feld **Anzeigename** einen Wert ein, um das ValueSet-Trennzeichen hinzuzufügen (z. B. **ProdOVF**).
 - b Akzeptieren Sie den im Textfeld **Name** angezeigten Standardwert oder geben Sie einen benutzerdefinierten Namen ein.
 - c Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein. Beispiel:
Build-Einstellungen für Klon-Szenario A.
 - d Wählen Sie im Dropdown-Menü **Status** die Option **Aktiv** oder **Inaktiv** aus.

Wählen Sie **Aktiv** aus, damit der Wertsatz im Anforderungsformular für die Katalogbereitstellung sichtbar ist.
 - e Wählen Sie die Build-Aktion **Erstellen** aus.
 - f Wählen Sie **Server** oder **Desktop** als Blueprint-Typ aus.
 - g Wählen Sie den Bereitstellungsworkflow **ImportOvfWorkflow** aus.
 - h Geben Sie den Pfad zur OVF-URL unter Verwendung des Formats `https://server/folder/name.ovf` oder `name.ova` ein.
 - i Wenn Sie die Authentifizierung beim Server, der die OVF-Datei hostet, aktivieren, geben Sie die Anmeldedaten für den zu authentifizierenden Benutzer ein.
 - j Wenn die OVF-Datei auf einer Website gehostet wird und Sie einen Proxy-Endpoint erstellt haben, der für den Zugriff auf die Website verwendet werden soll, wählen Sie **Proxy verwenden** und den verfügbaren Proxy-Endpoint aus.
- 5 Klicken Sie auf **Speichern**.
- 6 Wenn Sie mit Ihren Einstellungen zufrieden sind, klicken Sie auf **Fertig stellen**.

Nächste Schritte

Nachdem Sie das Image erstellt und die OVF-Datei zum Definieren des Image-Wertsatzes erstellt haben, können Sie das Image einer vSphere-Maschinenkomponente in einem Blueprint hinzufügen.

Verwenden von Containerkomponenten in Blueprints

Sie können Containerkomponenten im Blueprint konfigurieren und verwenden.

Nachdem ein Containeradministrator Containerdefinitionen in Container für vRealize Automation erstellt hat, kann ein Containerarchitekt Containerkomponenten für vRealize Automation-Blueprints auf der Design-Arbeitsfläche hinzufügen und konfigurieren.

Containerkomponenteneinstellungen

Sie können Blueprint-Optionen und -Einstellungen für eine Container für vRealize Automation-Containerkomponente im vRealize Automation-Design-Arbeitsbereich festlegen.

Registerkarte **Allgemein**

Konfigurieren Sie allgemeine Einstellungen für die Blueprint-Containerkomponente auf der Design-Arbeitsfläche.

Tabelle 3-33. Einstellungen auf der Registerkarte **Allgemein**

Einstellung	Beschreibung
Name	Geben Sie im Blueprint einen Namen für Ihre Containerkomponente ein.
Beschreibung	Fassen Sie Ihre Containerkomponente zum Wohle weiterer Architekten zusammen.
Image	Geben Sie den vollständigen Namen eines Images in einer verwalteten Registrierung ein, beispielsweise in einer privaten Registrierung oder einer Docker Hub-Registrierung, z. B. registry.hub.docker.com/library/python.
Befehle	Geben Sie einen Befehl ein, der für das angegebene Image gilt, z. B. python app.py. Der Befehl wird ausgeführt, wenn der Prozess für das Bereitstellen des Containers gestartet wird.
Links	Links bieten eine weitere Möglichkeit, um Container auf einem einzelnen Host oder über Hosts hinweg zu verbinden. Geben Sie einen oder mehrere Dienste ein, mit denen dieser Container verlinkt werden soll, z. B. redis oder datadog.

Registerkarte **Netzwerk**

Konfigurieren Sie Netzwerkeinstellungen für die Blueprint-Containerkomponente auf der Design-Arbeitsfläche.

Sie können einen Container an ein Netzwerk anhängen. Das Netzwerk wird auf der Design-Arbeitsfläche als Container-Netzkomponente dargestellt. Informationen über verfügbare Netzwerke werden auf der Seite „Netzwerk“ des Containerkomponentenformulars angegeben.

Tabelle 3-34. Einstellungen auf der Registerkarte **Netzwerk**

Einstellung	Beschreibung
Netzwerke	Geben Sie die vorhandenen Netzwerke an, die für das ausgewählte Image definiert sind. Sie können auch ein neues Netzwerk erstellen. Wenn Sie ein Netzwerk-Containerkomponente zum Design-Formular hinzufügen, werden die von Ihnen angegebenen Netzwerke als Optionen zur Auswahl angeboten.
Port-Bindungen	Geben Sie die Port-Bindungen für das ausgewählte Netzwerk an. Port-Bindungen bestehen aus Protokoll-Host, Hostport und Container-Port.
Alle Ports veröffentlichen	Aktivieren Sie das Kontrollkästchen, um die im Container-Image verwendeten Ports für alle Benutzer freizulegen.

Tabelle 3-34. Einstellungen auf der Registerkarte **Netzwerk** (Fortsetzung)

Einstellung	Beschreibung
Hostname	Geben Sie den Hostnamen des Containers an. Wird kein Name angegeben, wird standardmäßig der Name der Containerkomponente im Blueprint verwendet.
Netzwerkmodus	Geben Sie den Netzwerk-Stack des Containers an. Wenn kein Wert angegeben wird, wird der Container im Bridge-Netzwerkmodus konfiguriert.

Registerkarte **Speicher**

Konfigurieren Sie Speichereinstellungen für die Blueprint-Containerkomponente auf der Design-Arbeitsfläche.

Tabelle 3-35. Einstellungen auf der Registerkarte **Speicher**

Einstellungen	Beschreibung
Volumes	Geben Sie die Speichervolumes an, die vom Host für die Verwendung durch den Container zugeordnet werden.
Volumes von	Geben Sie die Speichervolumes an, die von einem anderen Container geerbt werden sollen.
Arbeitsverzeichnis	Geben Sie das Verzeichnis an, von wo aus Befehle ausgeführt werden sollen.

Registerkarte **Richtlinie**

Konfigurieren Sie die Richtlinieneinstellungen, z. B. Bereitstellungsrichtlinie und Affinitätsoptionen für die Blueprint-Containerkomponente auf der Design-Arbeitsfläche.

Tabelle 3-36. Einstellungen der Registerkarte **Richtlinie**

Einstellungen	Beschreibung
Bereitstellungsrichtlinie	Geben Sie eine Bereitstellungsrichtlinie an, um die Voreinstellungen für die Gruppe von Hosts festzulegen, die für die Bereitstellung dieses Containers zu verwenden ist. Sie können Bereitstellungsrichtlinien mit Hosts, Richtlinien und Containerdefinitionen verknüpfen, um für die Bereitstellung eines Containers eine Präferenz für Hosts, Richtlinien und Kontingente festzulegen. Sie können auf der Registerkarte Container in vRealize Automation eine Bereitstellungsrichtlinie hinzufügen.
Clustergröße	Geben Sie die Anzahl der Instanzen an, die von diesem Container als Cluster generiert werden sollen.
Neustartrichtlinie	Geben Sie eine Neustartrichtlinie dafür ein, wie ein Container beim Beenden neu gestartet wird.
Max. Neustart	Wenn Sie „Bei Fehler“ als Neustartrichtlinie ausgewählt haben, können Sie die maximale Anzahl der Neustarts angeben.
CPU-Anteile	Geben Sie die Anzahl der zugeteilten CPU-Anteile für die bereitgestellte Ressource an.

Tabelle 3-36. Einstellungen der Registerkarte **Richtlinie** (Fortsetzung)

Einstellungen	Beschreibung
Arbeitsspeichergrenzwert	Geben Sie eine Zahl zwischen 0 und dem verfügbaren Arbeitsspeicher in der Platzierungszone an. Dies ist der gesamte verfügbare Speicher für Ressourcen in dieser Platzierung. 0 bedeutet keine Begrenzung.
Auslagerungsspeicher	Gesamt-Arbeitsspeichergrenzwert.
Affinitätseinschränkungen	<p>Definiert Regeln für die Bereitstellung von Containern auf demselben oder auf verschiedenen Hosts.</p> <ul style="list-style-type: none"> ■ Affinitätstyp <p>Im Fall von Anti-Affinität werden die Container auf unterschiedlichen Hosts platziert, anderenfalls werden sie auf demselben Host platziert.</p> ■ Dienst <p>Der Dienstname im Drop-Down-Menü entspricht dem Namen der Containerkomponente, der im Feld Name auf der Registerkarte Allgemein angegeben ist.</p> ■ Option <p>Eine harte Option gibt an, dass die Bereitstellung fehlschlagen soll, wenn der Option nicht entsprochen werden kann. Eine weiche Option gibt an, dass die Bereitstellung weiter durchgeführt werden soll, wenn der Option nicht entsprochen werden kann.</p>

Registerkarte **Umgebung**

Konfigurieren Sie Umgebungseinstellungen, wie z. B. Eigenschaftsbindungen für die Blueprint-Containerkomponente, auf der Design-Arbeitsfläche.

Tabelle 3-37. Einstellungen auf der Registerkarte **Umgebung**

Einstellung	Beschreibung
Name	Name der Variable.
Bindung	<p>Binden Sie die Variable an eine andere Eigenschaft, die Teil der Vorlage ist. Wenn Sie die Bindung auswählen, müssen Sie einen Wert in der <code>_resource~TemplateComponent~TemplateComponentProperty-</code> Syntax eingeben.</p>
Wert	Der Wert der Umgebungsvariable oder, wenn Sie die Bindung ausgewählt haben, der Wert der Eigenschaft, die Sie binden möchten.

Registerkarte „Eigenschaften“

Konfigurieren Sie einzelne sowie Gruppen von benutzerdefinierten Eigenschaften für die Blueprint-Containerkomponente auf der Design-Arbeitsfläche.

Wenn Sie die Registerkarte **Eigenschaftsgruppen** wählen und auf **Hinzufügen** klicken, stehen die folgenden Optionen zur Verfügung:

- Container-Hosteigenschaften mit Zertifikatsauthentifizierung
- Container-Hosteigenschaften mit Benutzer-/Kennwortauthentifizierung

Wenn zusätzliche Eigenschaftsgruppen definiert wurden, werden sie ebenfalls aufgeführt.

Wenn Sie die Registerkarte **Benutzerdefinierte Eigenschaften** wählen und auf **Hinzufügen** klicken, können Sie einzelne benutzerdefinierte Eigenschaften zur Container-Komponente hinzufügen.

Tabelle 3-38. Einstellungen der Registerkarte **Eigenschaften für benutzerdefinierte Eigenschaften**

Einstellung	Beschreibung
Name	Geben Sie den Namen einer benutzerdefinierten Eigenschaft ein oder wählen Sie aus dem Dropdown-Menü eine verfügbare benutzerdefinierte Eigenschaft aus.
Wert	Geben Sie einen Wert ein bzw. bearbeiten Sie einen Wert, der mit der benutzerdefinierten Eigenschaft verknüpft werden soll.
Verschlüsselt	Sie können den Eigenschaftswert verschlüsseln. Beispielsweise für den Fall, dass es sich bei dem Wert um ein Kennwort handelt.
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 auch Überschreibbar wählen, wenn Sie möchten, dass Benutzer einen Wert eingeben.

Registerkarte **Systemzustandskonfiguration**

Geben Sie auf der Design-Arbeitsfläche einen Modus für die Systemzustandskonfiguration für die Blueprint-Containerkomponente an.

Tabelle 3-39. Einstellungen der Registerkarte **Systemzustandskonfiguration**

Modus-Einstellung	Beschreibung
Keine	Standard. Keine Integritätsprüfungen sind konfiguriert.
HTTP	<p>Wenn Sie HTTP auswählen, müssen Sie eine API für den Zugriff sowie eine zu verwendende HTTP-Methode und -Version angeben. Die API ist relativ und Sie müssen nicht die Adresse des Containers eingeben. Sie können auch einen Wert für eine Zeitüberschreitung des Vorgangs und Integritätsschwellenwerte festlegen.</p> <p>Beispiel: Ein Fehlerfrei-Schwellenwert von 2 bedeutet, dass zwei hintereinander durchgeführte Aufrufe erfolgreich sein müssen, damit der Container als fehlerfrei und als ausgeführt betrachtet wird (Status: WIRD AUSGEFÜHRT).</p> <p>Beispiel: Ein Fehlerhaft-Schwellenwert von 2 bedeutet, dass zwei hintereinander durchgeführte Aufrufe nicht erfolgreich sein müssen, damit der Container als fehlerhaft (Status: FEHLER) betrachtet wird. Für alle Zustände zwischen diesen Schwellenwerten ist der Containerstatus „HERABGESTUFT“.</p>
TCP-Verbindung	Wenn Sie TCP-Verbindung auswählen, müssen Sie nur einen Port für den Container eingeben. Die Integritätsprüfung versucht, eine TCP-Verbindung mit dem Container über den bereitgestellten Port herzustellen. Sie können auch einen Zeitüberschreitungswert für den Vorgang angeben und ähnlich wie bei HTTP Fehlerfrei- bzw. Fehlerhaft-Schwellenwerte festlegen.
Befehl	Wenn Sie Befehl auswählen, müssen Sie einen Befehl eingeben, der für den Container ausgeführt wird. Der Erfolg der Integritätsprüfung wird durch den Exitcode des Befehls angegeben.
Integritätsprüfung bei Bereitstellung ignorieren	Deaktivieren Sie diese Option, um eine Integritätsprüfung bei der Bereitstellung zu erzwingen. Dadurch wird erreicht, dass ein Container erst nach einer erfolgreichen Integritätsprüfung als bereitgestellt gilt.
Autodeploy	Ermöglicht automatische erneute Bereitstellung von Containern, wenn sie den Status FEHLER aufweisen.

Registerkarte **Protokollkonfiguration**

Geben Sie auf der Design-Arbeitsfläche einen Protokollierungsmodus sowie optionale Protokollierungsoptionen für die Blueprint-Containerkomponenten ein.

Tabelle 3-40. Einstellungen der Registerkarte **Protokollkonfiguration**

Einstellung	Beschreibung
Treiber	Wählen Sie ein Protokollierungsformat aus dem Dropdown-Menü aus.
Optionen	Geben Sie Treiberoptionen mithilfe eines Name-/Wertformats an, das dem Protokollierungsformat entspricht.

Verwenden von Container-Eigenschaften und Eigenschaftsgruppen in einem Blueprint

Sie können einer Containerkomponente in einem vRealize Automation-Blueprint vordefinierte Eigenschaftsgruppen hinzufügen. Wenn Maschinen, die diese Eigenschaften enthalten, mithilfe eines Blueprints bereitgestellt werden, wird die bereitgestellte Maschine als Docker Container-Hostmaschine registriert.

Container für vRealize Automation stellt die folgenden beiden Eigenschaftsgruppen von containerspezifischen benutzerdefinierten Eigenschaften bereit. Wenn Sie einem Blueprint eine Containerkomponente hinzufügen, können Sie diese Eigenschaftsgruppen zum Container hinzufügen, um bereitgestellte Maschinen als Container-Hosts zu registrieren.

- Container-Hosteigenschaften mit Zertifikatsauthentifizierung
- Container-Hosteigenschaften mit Benutzer-/Kennwortauthentifizierung

Diese Eigenschaftsgruppen sind in vRealize Automation sichtbar, wenn Sie **Verwaltung > Eigenschaftsdiktionär > Eigenschaftsgruppen** wählen.

Da Eigenschaftsgruppen von allen Mandanten gemeinsam genutzt werden, ziehen Sie das Klonen und Anpassen Ihrer Eigenschaften in Betracht, wenn Sie in einer Umgebung mit mehreren Mandanten arbeiten. Wenn Sie die Eigenschaftsgruppen und Eigenschaften in den Gruppen eindeutig benennen, können Sie sie bearbeiten, um benutzerdefinierte Werte zur Verwendung in einem bestimmten Mandanten zu definieren.

Die am häufigsten verwendeten Eigenschaften sind `Container.Auth.PublicKey` und `Container.Auth.PrivateKey`. Mit diesen stellt der Container-Administrator das Clientzertifikat zum Authentifizieren mit dem Container-Host bereit.

Tabelle 3-41. ContainerBenutzerdefinierte Eigenschaften

Eigenschaft	Beschreibung
<code>containers.ipam.driver</code>	Nur für die Verwendung mit Containern. Gibt den IPAM-Treiber an, der zu verwenden ist, wenn eine Container-Netzwerkkomponente zu einem Blueprint hinzugefügt wird. Welche Werte unterstützt werden, hängt von den Treibern ab, die in der Container-Hostumgebung installiert sind, in der sie verwendet werden. Ein unterstützter Wert wäre z. B. <code>infoblox</code> oder <code>calico</code> , je nachdem, welche IPAM-Plug-Ins auf dem Container-Host installiert sind.
<code>containers.network.driver</code>	Nur für die Verwendung mit Containern. Gibt den Netzwerktreiber an, der zu verwenden ist, wenn eine Container-Netzwerkkomponente zu einem Blueprint hinzugefügt wird. Welche Werte unterstützt werden, hängt von den Treibern ab, die in der Container-Hostumgebung installiert sind, in der sie verwendet werden. Standardmäßig gehören zu den von Docker bereitgestellten Netzwerktreibern Bridge-, Overlay- und Macvlan-Treiber, wobei bei den von Virtual Container Host (VCH) bereitgestellten Netzwerktreibern der Bridge-Treiber enthalten ist. Netzwerktreiber von Drittanbietern, wie z. B. <code>weave</code> und <code>calico</code> , stehen möglicherweise ebenfalls zur Verfügung, je nachdem, welche Netzwerk-Plug-Ins auf dem Container-Host installiert sind.
<code>Container</code>	Nur für die Verwendung mit Containern. Der Standardwert ist <code>App.Docker</code> und erforderlich. Ändern Sie diese Eigenschaft nicht.
<code>Container.Auth.User</code>	Nur für die Verwendung mit Containern. Gibt den Benutzernamen für das Herstellen einer Verbindung zum Container-Host an.
<code>Container.Auth.Password</code>	Nur für die Verwendung mit Containern. Gibt entweder das Kennwort für den Benutzernamen oder für den zu verwendenden öffentlichen bzw. privaten Schlüssel an. Verschlüsselter Eigenschaftswert wird unterstützt.
<code>Container.Auth.PublicKey</code>	Nur für die Verwendung mit Containern. Gibt den öffentlichen Schlüssel für das Herstellen einer Verbindung zum Container-Host an.
<code>Container.Auth.PrivateKey</code>	Nur für die Verwendung mit Containern. Gibt den privaten Schlüssel für das Herstellen einer Verbindung zum Container-Host an. Verschlüsselter Eigenschaftswert wird unterstützt.
<code>Container.Connection.Protocol</code>	Nur für die Verwendung mit Containern. Gibt das Kommunikationsprotokoll an. Der Standardwert ist <code>API</code> und erforderlich. Ändern Sie diese Eigenschaft nicht.
<code>Container.Connection.Scheme</code>	Nur für die Verwendung mit Containern. Gibt das Kommunikationsschema an. Die Standardeinstellung ist <code>https</code> .

Tabelle 3-41. ContainerBenutzerdefinierte Eigenschaften (Fortsetzung)

Eigenschaft	Beschreibung
Container.Connection.Port	Nur für die Verwendung mit Containern. Gibt den Container-Verbindungs-Port an. Die Standardeinstellung ist 2376.
Extensibility.Lifecycle.Properties.VMPSMasterWorkflow32.MachineActivated	Nur für die Verwendung mit Containern. Gibt die Event-Broker-Eigenschaft an, um alle Container-Eigenschaften freizulegen, und wird für das Registrieren eines bereitgestellten Hosts verwendet. Der Standardwert ist Container* und erforderlich. Ändern Sie diese Eigenschaft nicht.
Extensibility.Lifecycle.Properties.VMPSMasterWorkflow32.Disposing	Nur für die Verwendung mit Containern. Gibt die Event-Broker-Eigenschaft an, um alle der oben genannten Container-Eigenschaften freizulegen, und wird für das Aufheben der Registrierung eines bereitgestellten Hosts verwendet. Der Standardwert ist Container* und erforderlich. Ändern Sie diese Eigenschaft nicht.

Verwenden von Container-Netzwerkkomponenten auf der Design-Arbeitsfläche

Sie können mindestens eine Container-Netzwerkkomponente zur Design-Arbeitsfläche hinzufügen und im Blueprint deren Einstellungen für vSphere-Maschinenkomponenten konfigurieren.

Sie können `containers.ipam.driver` und `containers.network.driver` zur Komponente hinzufügen, wenn Sie diese zum Blueprint hinzufügen.

Hinzufügen einer vorhandenen Container-Netzwerkkomponente

Sie können Container-Netzwerkinformationen zu einem vRealize Automation-Blueprint hinzufügen, der Containerkomponenten enthält.

Sie können Container in Container für vRealize Automation unter Verwendung der Registerkarte vRealize Automation **Container** konfigurieren. Sie können diese Container und deren Netzwerkeinstellungen als Komponenten in einem Blueprint hinzufügen, indem Sie die Optionen auf der Registerkarte vRealize Automation **Design** verwenden.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Containerarchitekt** an.
- Öffnen Sie mithilfe der Registerkarte **Design** einen neuen oder vorhandenen Blueprint in der Design-Arbeitsfläche.

Verfahren

- 1 Klicken Sie im Abschnitt „Kategorien“ auf **Netzwerk und Sicherheit**, um die Liste der verfügbaren Netzwerk- und Sicherheitskomponenten anzuzeigen.
- 2 Ziehen Sie eine **Container-Netzwerkkomponente** auf die Design-Arbeitsfläche.
- 3 Geben Sie im Textfeld **Name** einen Namen ein, der die Komponente auf der Design-Arbeitsfläche eindeutig kennzeichnet.

- 4 (Optional) Geben Sie im Textfeld **Beschreibung** eine Beschreibung für die Komponente ein.
- 5 (Optional) Aktivieren Sie das Kontrollkästchen **Extern**, wenn Sie externe IPAM-Einstellungen angeben möchten.

Wenn Sie das Kontrollkästchen **Extern** aktivieren, wird die Registerkarte **IPAM-Konfiguration** entfernt.

- 6 Klicken Sie auf die Registerkarte **IPAM-Konfiguration**, um ein vorhandenes bzw. neues Subnetz, einen IP-Bereich und ein Gateway für das Netzwerk anzugeben bzw. zu bearbeiten, das in einer Containerkomponente im Blueprint angegeben ist.

Im Gegensatz zu Netzwerken, die vormals in Docker oder einer anderen unterstützten Containeranwendung erstellt wurden, wird die IPAM-Konfiguration auf neue Netzwerke angewendet, die von vRealize Automation erstellt wurden. Diese Einstellungen wurden nicht überprüft und die Bereitstellung schlägt fehl, wenn sich die Einstellungen mit anderen Netzwerken überschneiden. Beispielsweise müssen das Subnetz und das Gateway innerhalb des Containerhosts eindeutig sein.

- 7 Klicken Sie auf die Registerkarte **Eigenschaften**, um benutzerdefinierte Eigenschaften für die Komponente anzugeben.

Wenn Sie die Registerkarte **Eigenschaftsgruppen** wählen und auf **Hinzufügen** klicken, stehen die folgenden Optionen zur Verfügung:

- Container-Hosteigenschaften mit Zertifikatsauthentifizierung
- Container-Hosteigenschaften mit Benutzer-/Kennwortauthentifizierung

Wenn zusätzliche Eigenschaftsgruppen definiert wurden, werden sie ebenfalls aufgeführt.

Wenn Sie die Registerkarte **Benutzerdefinierte Eigenschaften** wählen und auf **Hinzufügen** klicken, können Sie einzelne benutzerdefinierte Eigenschaften zur Container-Komponente hinzufügen.

Tabelle 3-42. Einstellungen der Registerkarte **Eigenschaften für benutzerdefinierte Eigenschaften**

Einstellung	Beschreibung
Name	Geben Sie den Namen einer benutzerdefinierten Eigenschaft ein oder wählen Sie aus dem Dropdown-Menü eine verfügbare benutzerdefinierte Eigenschaft aus.
Wert	Geben Sie einen Wert ein bzw. bearbeiten Sie einen Wert, der mit der benutzerdefinierten Eigenschaft verknüpft werden soll.
Verschlüsselt	Sie können den Eigenschaftswert verschlüsseln. Beispielsweise für den Fall, dass es sich bei dem Wert um ein Kennwort handelt.

Tabelle 3-42. Einstellungen der Registerkarte **Eigenschaften** für benutzerdefinierte Eigenschaften (Fortsetzung)

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 auch Überschreibbar wählen, wenn Sie möchten, dass Benutzer einen Wert eingeben.

- 8 Klicken Sie auf **Fertig stellen**, um den Blueprint als Entwurf zu speichern, oder setzen Sie die Konfiguration des Blueprints fort.

Nächste Schritte

Auf der Registerkarte **Netzwerk** der Containerkomponente auf der Design-Arbeitsfläche können Sie die Konfiguration der Container-Netzwerkeinstellungen fortsetzen.

Weitergeben von Containervorlagen für die Verwendung in Blueprints

Sie können eine Containervorlage für die Verwendung in einem vRealize Automation-Blueprint zur Verfügung stellen.

Ein Containervorlage kann mehrere Container umfassen. Wenn Sie eine Multi-Container-Vorlage an vRealize Automation weitergeben, wird die Vorlage als Multi-Komponenten-Blueprint in vRealize Automation erstellt.

Die containerspezifischen Eigenschaften, die Sie der Containervorlage hinzufügen, werden im vRealize Automation-Blueprint erkannt. Siehe [Verwenden von Container-Eigenschaften und Eigenschaftsgruppen in einem Blueprint](#).

Wenn Sie die Bereitstellung eines Blueprints anfordern, der im vRealize Automation-Katalog veröffentlicht wurde, stellen Sie die Quellcontaineranwendung für diesen Blueprint bereit.

Sie können weitere Komponenten zum vRealize Automation-Blueprint hinzufügen, einschließlich der folgenden Komponententypen:

- Maschinentypen
- Softwarekomponenten
- Anderen Blueprints
- NSX-Netzwerk und Sicherheitskomponenten

- XaaS-Komponenten
- Benutzerdefinierte Komponenten

Sie können eine Vorlage von Container nach vRealize Automation weitergeben. Änderungen, die Sie am vRealize Automation-Blueprint vornehmen, haben keine Auswirkung auf die Container-Vorlage.

Sie können nachträglich Änderungen an der Container-Vorlage vornehmen und sie erneut weitergeben, um den Blueprint in vRealize Automation zu überschreiben. Wenn Sie die Vorlage an vRealize Automation weitergeben, wird der Blueprint überschrieben und alle in vRealize Automation am Blueprint vorgenommenen Änderungen gehen verloren. Um zu verhindern, dass Sie Blueprint-Änderungen verlieren, verwenden Sie vRealize CloudClient zum Klonen eines neuen Blueprints oder zum Exportieren des Blueprints.

Bereitstellen eines Docker-Containers oder Hosts von einem Blueprint aus

Sie können vRealize Automation-Blueprints erstellen und verwenden, um Maschinen als registrierte Docker-Container-Hosts bereitzustellen.

Damit eine bereitgestellte Maschine als Container-Host registriert werden kann, müssen die folgenden Anforderungen erfüllt werden:

- Die Maschine wird von einem Blueprint bereitgestellt, der Container-spezifische benutzerdefinierte Eigenschaften enthält.

Die erforderlichen containerspezifischen benutzerdefinierten Eigenschaften werden in zwei Eigenschaftsgruppen angeboten. Siehe [Verwenden von Container-Eigenschaften und Eigenschaftsgruppen in einem Blueprint](#).

Informationen zum Verwenden von benutzerdefinierten Eigenschaften und Eigenschaftsgruppen in vRealize Automation finden Sie unter *Referenz für benutzerdefinierte Eigenschaften*.

- Auf die Maschine kann über das Netzwerk zugegriffen werden.

Beispielsweise muss die Maschine über eine gültige IP-Adresse verfügen und eingeschaltet sein.

Sie können einen vRealize Automation-Blueprint so definieren, dass er bestimmte benutzerdefinierte Eigenschaften enthält, die eine Maschine als Container-Host designieren, wenn sie mithilfe des Blueprints bereitgestellt wird.

Wenn eine Maschine mit den erforderlichen Blueprint-Eigenschaften erfolgreich bereitgestellt wurde, wird sie in den Container registriert und empfängt Ereignisse und Aktionen von vRealize Automation.

Erstellen von Microsoft Azure-Blueprints und Integrieren von Ressourcenaktionen

Als Cloud- oder Fabric-Administrator können Sie Microsoft Azure-VM-Blueprints erstellen, die Administratoren von Business-Gruppen als Bausteine zum Erstellen von benutzerdefinierten

bereitgestellten Maschinen für Verbraucher einsetzen. Auch DevOps-Administratoren können Azure-Maschinen-Blueprints erstellen oder sie können beim Erstellen von zusammengesetzten Blueprints vorhandene Azure-Maschinen-Blueprints verwenden.

- **Erstellen eines Blueprints für Microsoft Azure**

Sie können Blueprints virtueller Microsoft Azure-Maschinen erstellen, die Zugriff auf die Ressourcen virtueller Azure-Maschinen bieten.

- **Erstellen von benutzerdefinierten Ressourcenaktionen für Azure**

Sie können benutzerdefinierte Ressourcenaktionen zum Steuern von virtuellen Azure-Maschinen erstellen und verwenden.

Erstellen eines Blueprints für Microsoft Azure

Sie können Blueprints virtueller Microsoft Azure-Maschinen erstellen, die Zugriff auf die Ressourcen virtueller Azure-Maschinen bieten.

In der Kategorie **Maschinentypen** auf der vRealize Automation-Seite „Blueprint bearbeiten“ wird eine standardmäßige Azure-Maschinenvorlage angezeigt. Sie können diese VM-Vorlage als Basis eines Azure-Blueprints verwenden, wie im folgenden Verfahren beschrieben. Nachdem Sie einen Azure-Blueprint erstellt haben, können Sie ihn wie gewünscht veröffentlichen und bereitstellen oder Sie können ihn in Verbindung mit benutzerdefinierten Azure-Ressourcen oder mit anderen Blueprints verwenden, um einen zusammengesetzten Blueprint zu erstellen.

Nach der Erstellung und Veröffentlichung des Blueprints können Benutzer mit den entsprechenden Berechtigungen eine Azure-Instanz über den vRealize Automation-Servicekatalog anfordern und bereitstellen.

Hinweis: Azure-Blueprints definieren Anforderungen für virtuelle Maschinen. vRealize Automation verwendet diese Anforderungen, um die geeignetste Reservierung für die Bereitstellung auszuwählen.

Informationen über die Registerkarte für NSX-Einstellungen und Eigenschaften im Dialogfeld „Neuer Blueprint“ finden Sie unter *Konfigurieren von vRealize Automation*.

Wenn Sie zwei virtuelle Maschinen von einer einzelnen Bereitstellung aus gleichzeitig erstellen möchten, müssen Sie zwei Namen für Netzwerkschnittstellen und zwei Namen für virtuelle Maschinen erstellen.

Hinweis Vermeiden Sie die Implementierung einer Bereitstellung auf Azure und vSphere mit dem gleichen Namenspräfix, da dies zu einer doppelten Namensgebung in Azure und vSphere führen kann, die für einige Benutzer Probleme verursachen könnte.

Voraussetzungen

- Besorgen Sie sich eine gültige Azure-Abonnement-ID sowie zugehörige Informationen wie Ressourcengruppe, Speicherkonto und virtuellen Netzwerke, die Sie möglicherweise zum Erstellen eines Blueprints benötigen.

- Konfigurieren Sie einen Azure-Endpoint, um eine Verbindung zu Azure für die Verwendung mit Ihrer vRealize Automation-Bereitstellung zu erstellen.
- Konfigurieren Sie Azure-Reservierungen passend für Ihre Business-Gruppen.

Verfahren

- 1 Wählen Sie **Design > Blueprints** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Geben Sie in das Textfeld **Name** einen Blueprint-Namen ein.

Der eingegebene Name füllt auch das Textfeld **ID** aus. In den meisten Fällen können Sie die Registerkarten **NSX-Einstellungen** und **Eigenschaften** ignorieren.

- 4 Klicken Sie auf **OK**.
- 5 Klicken Sie im Menü „Kategorien“ auf **Maschinentypen**.
- 6 Ziehen Sie die Vorlage für die virtuelle **Azure-Maschine** auf die Design-Arbeitsfläche.

Falls Sie eine benutzerdefinierte Azure-Ressource als Basis eines Blueprints erstellt haben, können Sie diese Ressource aus der zugewiesenen Kategorie in der Liste „Kategorien“ auswählen.

- 7 Geben Sie die erforderlichen Informationen für die virtuelle Azure-Maschine in die Textfelder auf den Seiten im Registerkartenformat ein. Diese befinden sich auf der unteren Hälfte der Design-Arbeitsfläche, die angezeigt wird, wenn Sie die Azure-Maschinenvorlage auf die Design-Arbeitsfläche ziehen.

Die verfügbare Auswahl für Textfelder und andere Parameter auf all diesen Registerkarten ist meist durch den Azure-Endpoint festgelegt, der als Basis für Blueprints konfiguriert wurde.

Für die meisten Parameter gilt, dass wenn Sie in das Textfeld neben dem Parameternamen klicken können, ein neuer Fensterbereich auf der rechten Seite geöffnet wird. In diesem Bereich können Sie Parameterwerte in das Textfeld **Wert** eingeben und angeben, ob der Wert **erforderlich** ist oder nicht. Beachten Sie, dass Sie in einigen Fällen einen **Minimalwert** und einen **Maximalwert** eingeben können. Klicken Sie im rechten Bereich auf **Übernehmen**, um das anfängliche Textfeld aufzufüllen.

Abbildung 3-1. Azure-Blueprint, Menü auf der rechten Seite

The screenshot displays the configuration page for an Azure Machine blueprint. The 'Storage' tab is selected. The 'Resource Group' section has 'Use Existing' selected, with the name 'RG1-vAficionado' entered. The 'Availability Set' section has 'None' selected. On the right, the 'Value' field is populated with 'RG1-vAficionado', and the 'Required' status is set to 'No'. A red arrow highlights the link between the 'Use Existing' option and the 'Value' field.

Die meisten Parameter verfügen auch über die Schaltfläche **Erweiterte Optionen**. Mit diesen Optionen können Sie die Länge von Parametern angeben und sogar Parameter für Endbenutzer ausblenden.

Hinweis Sie müssen die erforderlichen Parameter auf den einzelnen Registerkarten auffüllen, damit die Blueprint-Konfiguration fortgesetzt werden kann. Wenn Sie ein Feld leer lassen möchten, können Sie vor dem Speichern zurückgehen und den Eintrag löschen.

Registerkarte	Beschreibung	Wichtige Parameter
Allgemein	Wählen Sie grundlegende Verbindungsinformationen für die virtuelle Azure-Maschine wie beispielsweise den zu verwendenden Endpoint aus.	<p>ID: Identifiziert die virtuelle Azure-Maschine, die Sie erstellen. Wenn Sie diesen Namen ändern, wird das Image der virtuellen Azure-Maschine auf der Design-Arbeitsfläche auch automatisch aktualisiert.</p> <p>Beschreibung: Identifiziert die virtuelle Maschine, die Sie erstellen, und ob sie erforderlich ist.</p> <p>Instanzen - Mit dieser Auswahl können Sie eine skalierbare virtuelle Maschine erstellen. Verwenden Sie die Felder Mindestwert und Maximalwert, um die Anzahl der Azure-Instanzen zu identifizieren, die von dieser Maschine erzeugt werden kann.</p> <p>Kennwortauthentifizierung verwenden: Wählen Sie „Ja“, um die Kennwortauthentifizierung zu verwenden, oder „Nein“, um SSH zu verwenden.</p> <p>Administratorbenutzername: Lassen Sie dies leer, damit er durch den Benutzer, der die Maschine bereitstellt, zugewiesen werden kann.</p> <p>Administratorkennwort: Lassen Sie dies leer, damit der Benutzer, der die Maschine bereitstellt, das entsprechende Kennwort zuweisen kann.</p>
Build-Informationen	Hiermit können Sie Informationen über die zu erstellende virtuelle Maschine konfigurieren.	<p>Standort: Wählen Sie den geografischen Ort aus, an dem diese virtuelle Maschine bereitgestellt wird.</p> <p>Maschinenpräfix: Aktivieren Sie das entsprechende Optionsfeld, um anzugeben, ob Sie das Maschinenpräfix aus der zugehörigen Business-Gruppe verwenden oder ein benutzerdefiniertes Präfix erstellen möchten. Wenn Sie ein benutzerdefiniertes Präfix verwenden möchten, geben Sie es im Textfeld Benutzerdefiniertes Maschinenpräfix ein.</p> <p>Image-Typ der virtuellen Maschine: Aktivieren Sie das entsprechende Optionsfeld, um ein benutzerdefiniertes bzw. ein standardmäßiges VM-Image auszuwählen. Eine benutzerdefinierte virtuelle Maschine wird aus der klassischen Azure-Bereitstellung erstellt und bietet mehr Konfigurationsoptionen bezüglich Cloud-Diensten, Speicherkonten und Verfügbarkeitssätzen an.</p> <p>VM-Image: Identifizieren Sie das Azure-VM-Image, das als Grundlage für den Blueprint dienen soll.</p> <ul style="list-style-type: none"> ■ Im Falle eines standardmäßigen VM-Images muss der URN des Maschine-Images dem folgenden Format entsprechen: (Veröffentlicher):(Angebot):(SKU): (Version). ■ Bei einem benutzerdefinierten VM-Image muss der URN des Maschine-Images dem folgenden Format entsprechen: <code>https://storageaccount.blob.core.windows.net/container/image.vhd</code> <p>Zudem müssen Sie für benutzerdefinierte Images das Textfeld „Betriebssystem-Image-Typ (Windows oder Linux)“ ausfüllen.</p> <p>Admin-Benutzer: Geben Sie den Namen des designierten Administrators für auf diesem Blueprint basierende virtuelle Maschinen ein. Alternativ können Sie dieses Feld leer lassen und die Informationen auf dem Anfrageformular eintragen.</p>

Registerkarte	Beschreibung	Wichtige Parameter
		<p>Authentifizierung: Aktivieren Sie das entsprechende Optionsfeld, um anzugeben, ob auf diesem Blueprint basierende virtuelle Maschinen eine Authentifizierung mittels Kennworts oder eine SSH-Authentifizierung benötigen.</p> <p>Administratorkennwort: Das Administratorkennwort für die Instanz der virtuellen Maschine.</p> <p>Serie: Gibt die allgemeine Größe einer VM-Instanz an. Informationen zu Serien finden Sie in der Azure-Dokumentation unter https://azure.microsoft.com/de-de/documentation/articles/virtual-machines-windows-sizes/.</p> <p>Größe: Gibt die spezifische Größe für VM-Instanzen innerhalb einer Serie an. Die Größe ist abhängig von den ausgewählten Serien. Wenn Sie über eine gültige Verbindung zu einer Azure-Instanz verfügen, werden die verfügbaren Größen dynamisch basierend auf dem Abonnement und der Auswahl des Standorts und der Serien aufgefüllt. Größeninformationen finden Sie in der Azure-Dokumentation.</p> <p>Details zur Instanzgröße: Optionale Informationen über die VM-Instanzserie und die Größe.</p>

Registerkarte	Beschreibung	Wichtige Parameter
Maschinenressourcen	<p>Organisieren Sie virtuelle Maschinenressourcen in Buckets. Eine Ressourcengruppe ist ein Organisationskonstrukt, mit dem virtuelle Maschinenressourcen wie Websites, Konten, Datenbanken und Netzwerke gruppiert werden.</p> <p>Eine Verfügbarkeitsgruppe ist ein Mechanismus für die Verwaltung von mindestens zwei virtuellen Maschinen, um Redundanz zu unterstützen. Weitere Informationen zu Azure-Verfügbarkeitsgruppen finden Sie unter https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-manage-availability/.</p> <hr/> <p>Hinweis Wenn Sie eine Vorlage so konfigurieren, dass die maximale Anzahl von Azure-Instanzen größer als 1 ist, sollten Sie die vorhandene Ressourcen- und Verfügbarkeitsgruppe verwenden, anstatt neue zu erstellen. Wenn Sie neue Ressourcen- oder Verfügbarkeitsgruppen auf mehr als eine Instanz in der gleichen Bereitstellung verwenden, treten Fehler und weitere Probleme im Zusammenhang mit Lastausgleichsmodulen auf.</p>	<p>Ressourcengruppe erstellen oder wiederverwenden: Aktivieren Sie das entsprechende Optionsfeld, um anzugeben, ob Sie die vorhandene Azure-Ressourcengruppe verwenden oder eine neue Gruppe erstellen möchten. Sie finden diesen Namen der vorhandenen Ressourcengruppe auf der Seite für Ressourcengruppen im Azure-Portal. Wenn Sie eine neue Ressourcengruppe erstellen möchten, enthält das Textfeld Ressourcengruppe automatisch einen geeigneten Namen für die neue Gruppe.</p> <p>Verfügbarkeitsgruppe erstellen oder wiederverwenden: Aktivieren Sie das entsprechende Optionsfeld für die Aktion, die Sie durchführen möchten. Wenn Sie „Neu erstellen“ wählen, enthält das Textfeld die entsprechenden Informationen für die neue Verfügbarkeitsgruppe.</p>

Registerkarte	Beschreibung	Wichtige Parameter
Speicher	Hiermit können Sie Azure-Speicherkonten organisieren. Mit einem Speicherkonto verfügen Sie über Zugriff auf verschiedene Arten des Azure Storage wie beispielsweise Azure-Blob, Warteschlangentabelle und Dateispeicher. Für die meisten Blueprints können Sie die Standardwerte übernehmen.	<p>Speicherkonto: Geben Sie ggf. den Namen des Speicherkontos für die virtuelle Maschine ein. Die Betriebssystemfestplatte der virtuellen Azure-Maschine wurde für dieses Speicherkonto bereitgestellt. Im Azure-Portal sind Informationen zu Speichergruppen angegeben. Sie können über ein oder mehrere Speicherkonten verfügen.</p> <hr/> <p>Hinweis Speicherkontonamen mit Unterstrichen oder anderen Sonderzeichen können zu Fehlern führen.</p> <hr/> <p>Diagnosespeicher hinzufügen: Aktivieren Sie dieses Kontrollkästchen, wenn Sie Diagnosedaten mit Ihrer Azure-Instanz verwenden.</p> <p>Anzahl der Speicherfestplatten: Geben Sie die geeignete Anzahl der von der virtuellen Maschine verwendeten Datenspeicherplatten an. Sie können bis zu vier Festplatten angeben. Diese Festplatten gelten zusätzlich zur im Textfeld Speicherkonto angegebenen Betriebssystemfestplatte.</p> <p>Speicherfestplatten-Nr.</p> <ul style="list-style-type: none"> ■ Festplattenname: Gibt den der Festplatte zugewiesenen Namen an. ■ Festplattentyp: Typ des Speichergeräts. ■ Festplattengröße: Speichergröße. ■ Replizierung: Die Redundanzmethode, die für das Sichern von Festplatten verwendet wird. ■ Host-Caching: Gibt an, ob Lese-/Schreibvorgänge zwischengespeichert werden, um die Leistung zu erhöhen.

Registerkarte	Beschreibung	Wichtige Parameter
Netzwerk	<p>Ermöglicht Ihnen die Auswahl des Netzwerks für den Blueprint virtueller Maschinen. Für die meisten Blueprints können Sie die Standardwerte übernehmen. Der Verbraucher gibt dann während der Bereitstellung die entsprechenden Netzwerkinformationen ein.</p> <hr/> <p>Hinweis Sie können nur eine virtuelle Maschine pro Schnittstelle erstellen, aber jede virtuelle Maschine kann bis zu vier Schnittstellen aufweisen.</p> <hr/>	<p>Klicken Sie auf die Tabelle, um ein Dialogfeld auf der rechten Seite zu öffnen. In diesem ist eine weitere bearbeitbare Tabelle mit den folgenden Feldern enthalten.</p> <ul style="list-style-type: none"> ■ Name des Lastausgleichsdiensts: Der mit der Azure-Instanz verwendete Lastausgleichsdienst. ■ Anzahl der Netzwerkschnittstellen: Wählen Sie die Anzahl der Netzwerkschnittstellen aus, die mit der Azure-Instanz verwendet werden. Die Anzahl der Netzwerkschnittstellen muss von der Größe der virtuellen Maschine, wie dies auf der Registerkarte „Speicher“ angegeben wurde, unterstützt werden. ■ Netzwerkschnittstelle: Wählen Sie die entsprechende Netzwerkschnittstelle für den virtuellen Maschinen-Blueprint aus. Wenn Sie ein vorhandenes Netzwerk eingeben, können Sie alle anderen Registerkarten für Netzwerke ignorieren. Wenn Sie einen Namen für die Netzwerkschnittstelle eingeben, der nicht vorhanden ist, wird eine neue Schnittstelle mit diesem Namen erstellt. Sie können dann die anderen Registerkarten für Netzwerke verwenden, um die Schnittstelle zu konfigurieren. ■ NIC-Namenspräfix: Das Präfix für die Netzwerkkarte (NIC). ■ IP-Adresstyp: Geben Sie an, ob die virtuelle Maschine eine statische oder eine dynamische IP-Adresse verwendet. ■ Netzwerkconfiguration: Geben Sie die entsprechende Netzwerkconfiguration ein. Netzwerkprofile werden unterstützt. Es gibt die beiden Optionen Azure-Netzwerke angeben und Netzwerkprofil verwenden und die nachfolgenden Felder ändern sich abhängig davon, welche Option Sie auswählen. <ul style="list-style-type: none"> ■ Die folgenden Optionen sind verfügbar, wenn Sie Azure-Netzwerke angeben auswählen. Wenn Sie diese Textfelder leer lassen, werden auf der Grundlage der in der entsprechenden Reservierung angegebenen Informationen Standard-Netzwerkstrukture verwendet. <ul style="list-style-type: none"> ■ vNet-Name: Der Name des virtuellen Netzwerks ■ subNet-Name: Der Domänenname des Azure-Subnetzes. <hr/> <p>Hinweis Die öffentliche IP-Adresse für Azure kann während der 2-Tage-Vorgänge festgelegt werden.</p> <ul style="list-style-type: none"> ■ Wenn Sie Netzwerkprofil verwenden auswählen, wird die Netzwerkconfiguration von den zugrunde liegenden Azure-Konstrukten getrennt und stattdessen mit dem vRealize Automation-Netzwerkprofil gekoppelt. <ul style="list-style-type: none"> ■ Wenn Sie das Textfeld Netzwerkprofil leer lassen, wird das standardmäßige Azure-vNet/Subnetzpaar basierend auf entsprechenden Reservierungen, bei denen ein Netzwerkprofil angegeben wurde, aufgelöst.

Registerkarte	Beschreibung	Wichtige Parameter
		<ul style="list-style-type: none"> ■ Wenn Sie ein Netzwerkprofil eingeben, werden das Azure vNet und das Subnetz anhand der übereinstimmenden Reservierung aufgelöst.
Eigenschaften	<p>Hiermit können Sie Ihrem Blueprint benutzerdefinierte Eigenschaften hinzufügen.</p> <p>Hier angewendete benutzerdefinierte Eigenschaften können durch 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 <i>Referenz für benutzerdefinierte Eigenschaften</i>.</p>	<p>Wie auf zwei Registerkarten im Dialogfeld „Eigenschaften“ ersichtlich, gibt zwei Optionen zum Hinzufügen von benutzerdefinierten Eigenschaften.</p> <ul style="list-style-type: none"> ■ Eigenschaftsgruppen: Dies sind wiederverwendbare Gruppen, die das Hinzufügen benutzerdefinierter Eigenschaften vereinfachen. Es gibt vier Optionen für die Auswahl von Eigenschaftsgruppen: <ul style="list-style-type: none"> ■ Hinzufügen: Hiermit können Sie eine verfügbare Eigenschaftsgruppe zum Blueprint hinzufügen. ■ Nach oben verschieben/Nach unten verschieben: Hiermit können Sie die Rangfolge von Eigenschaftsgruppen zu steuern. Die erste Gruppe hat die höchste Priorität und deren benutzerdefinierte Eigenschaften haben absoluten Vorrang. ■ Eigenschaften anzeigen: Hiermit können Sie die benutzerdefinierten Eigenschaften in der ausgewählten Gruppe anzeigen. ■ Zusammengeführte Eigenschaften anzeigen: 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. ■ Benutzerdefinierte Eigenschaften: Verwenden Sie diese Registerkarte, um einzelne benutzerdefinierte Eigenschaften hinzuzufügen. <ul style="list-style-type: none"> ■ Neu: Hiermit können Sie eine einzelne benutzerdefinierte Eigenschaft zum Blueprint hinzufügen. ■ Name: Geben Sie einen Namen für die Eigenschaft ein. Eine Liste der benutzerdefinierten Eigenschaften und deren Definitionen finden Sie unter <i>Referenz für benutzerdefinierte Eigenschaften</i>. ■ Wert: Geben Sie einen Wert für die benutzerdefinierte Eigenschaft ein. ■ Verschlüsselt: Sie können die Eigenschaft verschlüsseln. ■ Überschreibbar: Sie können festlegen, dass der Eigenschaftswert von dem nächsten oder nachfolgenden Benutzer überschrieben werden kann. 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

Registerkarte	Beschreibung	Wichtige Parameter
		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.

- 8 Klicken Sie auf **Beenden**, um die Blueprint-Konfiguration zu speichern und zur Blueprints-Hauptseite zurückzukehren.

Nächste Schritte

Wenn Sie benutzerdefinierte Eigenschaften in Ihrer Azure-Reservierung zur Unterstützung eines VPN-Tunnels konfiguriert haben, können Sie Software-Komponenten zu Azure-Blueprints hinzufügen.

- 1 Wählen Sie im Menü „Kategorien“ die Option **Softwarekomponenten** aus.
Softwarekomponenten, die Sie für Azure-Blueprints konfiguriert haben, werden im unteren Bereich angezeigt.
- 2 Wählen Sie die virtuelle Azure-Maschine in den Container-Dropdown-Werten aus.
- 3 Wählen Sie die gewünschte Softwarekomponente aus und ziehen Sie sie in die virtuelle Azure-Maschine auf der Design-Arbeitsfläche.
- 4 Wenn für die Softwarekomponente erforderliche Eigenschaften vorhanden sind, geben Sie sie in die entsprechenden Textfelder der Parameter unterhalb der Design-Arbeitsfläche ein.
- 5 Klicken Sie auf **Speichern**.

Wenn Sie den Blueprint veröffentlichen möchten, wählen Sie ihn auf der Blueprints-Hauptseite aus und klicken Sie auf **Veröffentlichen**. Ein veröffentlichter Blueprint steht auf der Katalogelementseite zur Verfügung. Zudem kann ein Manager einer Business-Gruppe oder eine gleichwertige Person diesen veröffentlichten Blueprint als Grundlage für einen zusammengesetzten Blueprint verwenden.

Erstellen von benutzerdefinierten Ressourcenaktionen für Azure

Sie können benutzerdefinierte Ressourcenaktionen zum Steuern von virtuellen Azure-Maschinen erstellen und verwenden.

Die Azure-Implementierung von vRealize Automation wird mit zwei sofort einsatzbereiten benutzerdefinierten Ressourcenaktionen zur Verfügung gestellt:

- Starten von virtuellen Maschinen
- Beenden von virtuellen Maschinen

Darüber hinaus können Sie benutzerdefinierte Ressourcenaktionen mithilfe von Workflows erstellen, auf die über die vRealize Orchestrator-Bibliothek zugegriffen werden kann, die über die vRealize Automation-Schnittstelle verfügbar ist.

Mit Azure-Ressourcenaktionen können Sie genauso wie mit allen übrigen XaaS-Ressourcenaktionen in vRealize Automation arbeiten. Weitere Informationen zu XaaS-Ressourcenaktionen finden Sie unter *Erstellen von XaaS-Blueprints und -Ressourcenaktionen* und *vRealize Orchestrator-Integration in vRealize Automation* in *Konfigurieren von vRealize Automation*.

Voraussetzungen

Konfigurieren Sie einen gültigen Azure-Endpoint für Ihre vRealize Automation-Bereitstellung.

Verfahren

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Klicken Sie auf **Neu**.
- 3 Navigieren Sie zu **Orchestrator > Bibliothek > Azure** in der vRealize Orchestrator-Workflow-Bibliothek.
- 4 Wählen Sie den gewünschten Ordner und Workflow aus.
- 5 Konfigurieren Sie die Aktion Ihren Anforderungen entsprechend wie jede andere XaaS-Ressourcenaktion.

Erstellen von Puppet-fähigen vSphere-Blueprints

Sie können Puppet-fähige vSphere-Blueprints erstellen, die die Puppet-basierte Konfigurationsverwaltung von virtuellen vSphere-Maschinen unterstützen.

In der Puppet-basierten Konfigurationsverwaltung werden in der Regel Rollen und Umgebungen verwendet, um die Softwarekonfiguration zu definieren und zu verwalten. Beachten Sie, dass die Bedeutung der Begriffe Rolle und Umgebung für Puppet von den allgemeineren Bedeutungen in der IT abweichen.

Ein Endpoint stellt eine Verbindung mit einer vorhandenen Puppet Enterprise-Bereitstellung her. Nachdem der Endpoint erstellt ist, ruft vRealize Automation die Liste der Umgebungen und Rollen ab, die den angegebenen Bereitstellungen zugeordnet sind. Sie können diese Umgebungen und Rollen in Szenarien mit früher Bindung oder mit später Bindung verwenden, wenn Sie einen Puppet-fähigen Blueprint für virtuelle Maschinen konfigurieren.

Hinweis Puppet-Komponenten werden derzeit nur auf vSphere-Blueprints und virtuellen Maschinen unterstützt.

Hinzufügen einer Puppet-Komponente zu einem vSphere-Blueprint

Sie können eine Puppet-Komponente für die Konfigurationsverwaltung zu einem vSphere-Blueprint hinzufügen, um das Erzwingen der Verwaltung von virtuellen vSphere-Maschinen anhand eines Puppet-Masters zu ermöglichen.

Durch das Hinzufügen einer Puppet-Komponente zu einem vSphere-Blueprint wird den über diesen Blueprint erstellten virtuellen Maschinen ein Puppet-Agent hinzugefügt.

Wenn Sie Puppet-fähige vSphere-Blueprints erstellen, müssen Sie wählen, ob Sie eine Konfiguration mit früher oder später Bindung erstellen.

Mit früher Bindung definieren Benutzer die Puppet-Rolle und Umgebungseinstellungen für alle virtuellen Maschinen basierend auf einem bestimmten Blueprint, wenn die Puppet-Komponente dem Blueprint hinzugefügt wird. Diese Einstellungen bleiben während der Lebensdauer des Blueprints statisch. Für späte Bindung haben Sie verschiedene Möglichkeiten.

- Lassen Sie die Textfelder **Puppet-Umgebung** und **Puppet-Rolle** im Blueprint leer. Diese Einstellungen werden von den Benutzern bei Anforderung vorgenommen.
- Geben Sie eine **Puppet-Umgebung** an und lassen Sie das Feld **Puppet-Rolle** leer. Benutzer müssen die Rolle bei Anforderung angeben.

Voraussetzungen

Erstellen Sie einen geeigneten vSphere-Blueprint. Weitere Informationen hierzu finden Sie unter [vSphere-Maschinenkomponenteneinstellungen](#).

Verfahren

- 1 Wählen Sie **Design > Blueprints** aus.
- 2 Wählen Sie im Menü „Kategorien“ auf der Seite „Design“ für Blueprints die Option **Konfigurationsverwaltung** aus.
- 3 Wählen Sie die Puppet-Komponente aus, und ziehen Sie sie in die vSphere-Komponente auf der Design-Arbeitsfläche.
- 4 Geben Sie auf der Registerkarte „Allgemein“ im unteren Bereich der Seite eine **ID** und eine **Beschreibung** für die Puppet-Komponente ein.
Die ID und die Beschreibung können frei gewählt werden.
- 5 Klicken Sie auf die Registerkarte „Server“.
- 6 Klicken Sie auf den Dropdown-Pfeil, und wählen Sie den entsprechenden Puppet-Master für den Blueprint aus.
- 7 Wählen Sie die entsprechende **Puppet-Umgebung** und die **Puppet-Rolle** aus, wenn Sie für diese Komponente frühe Bindung verwenden möchten.

Wählen Sie zum Konfigurieren der frühen Bindung eine Puppet-Umgebung und -Rolle aus. Wenn Sie eine Komponente mit später Bindung erstellen möchten, wählen Sie eine **Puppet-Umgebung** aus oder lassen Sie die Textfelder **Puppet-Umgebung** und **Puppet-Rolle** leer und aktivieren Sie die Kontrollkästchen **In Anforderungsformular festlegen**.

Hinweis Die Kontrollkästchen **In Anforderungsformular festlegen** sind miteinander verbunden. Wenn Sie eines aktivieren, wird das andere automatisch ebenfalls aktiviert.

- 8 Klicken Sie auf **Fertig stellen**, um die Konfiguration der Puppet-Komponente zu speichern und zur Design-Hauptseite für Blueprints zurückzukehren.

Hinzufügen der Unterstützung von RDP-Verbindungen zu Ihren Windows-Maschinen-Blueprints

Um zuzulassen, dass Katalogadministratoren Benutzern die Berechtigung „Verbindungsherstellung mithilfe von RDP“ für Windows-Blueprints erteilen, fügen Sie dem Blueprint benutzerdefinierte RDP-Eigenschaften hinzu und referenzieren Sie die RDP-Datei, die der Systemadministrator vorbereitet hat.

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 bei vRealize Automation 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.

Verfahren

- 1 Wählen Sie **Design > 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
VirtualMachine.Rdp.File	Gibt eine RDP-Datei an, aus der Einstellungen bezogen werden sollen, wie beispielsweise <code>My_RDP_Settings.rdp</code> . Diese Datei muss im Unterverzeichnis <code>Website\Rdp</code> des Installationsverzeichnisses von vRealize Automation gespeichert sein.
VirtualMachine.Rdp.SettingN	Gibt die RDP-Einstellungen ein, die beim Öffnen eines RDP-Links zu einer Maschine verwendet werden sollen. <i>N</i> ist eine eindeutige Zahl zur Unterscheidung der RDP-Einstellungen. Beispiel: Um die RDP-Authentifizierungsebene so festzulegen, dass keine Authentifizierungsanforderung festgelegt wird, definieren Sie die benutzerdefinierte Eigenschaft <code>VirtualMachine.Rdp.Setting1</code> und legen den Wert für die Authentifizierungsebene auf „i:3“ fest. Weitere Informationen zu RDP-Einstellungen und ihrer korrekten Syntax finden Sie in der Dokumentation zu Microsoft Windows RDP wie beispielsweise unter RDP Settings for Remote Desktop Services in Windows Server .
VirtualMachine.Admin.NameCompletion	Gibt den Domännennamen an, der in den vollqualifizierten Domännennamen der Maschine einbezogen werden soll, den die RDP- oder SSH-Dateien für die Benutzeroberflächenoptionen Verbindungsherstellung mithilfe von RDP oder Verbindungsherstellung mithilfe von SSH generieren. Legen Sie beispielsweise „myCompany.com“ als Wert fest, um den vollqualifizierten Domännennamen <code>my-machine-name.myCompany.com</code> in der RDP- oder SSH-Datei zu generieren.

- c Klicken Sie auf **Speichern**.

7 Wählen Sie die Blueprint-Zeile aus und klicken Sie auf **Veröffentlichen**.

Ergebnisse

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.

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 Ihren 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 bei vRealize Automation 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 [Konfigurieren eines Maschinen-Blueprints](#).

Verfahren

- 1 Wählen Sie **Design > Blueprints** aus.
- 2 Zeigen Sie auf Ihren 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
Plugin.AdMachineCleanup.UserName	Geben Sie im Textfeld Wert 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.
Plugin.AdMachineCleanup.Password	Geben Sie im Textfeld Wert das Kennwort für den Benutzernamen des Active Directory-Kontos ein.
Plugin.AdMachineCleanup.Delete	Legen Sie diese Eigenschaft auf „True“ fest, um die Konten gelöschter Maschinen zu entfernen, anstatt sie zu deaktivieren.
Plugin.AdMachineCleanup.MoveToOu	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 <i>ou=OU, dc=dc</i> erforderlich, wie beispielsweise „ou=trash,cn=computers,dc=lab,dc=local“.
Plugin.AdMachineCleanup.RenamePrefix	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**.

Ergebnisse

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 bei vRealize Automation als **Infrastrukturarchitekt** an.
- Erstellen Sie einen Maschinen-Blueprint. Siehe *Installieren und Konfigurieren von vRealize Automation für das Rainpole-Szenario*.

Verfahren

- 1 Wählen Sie **Design > 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**.

Ergebnisse

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 Datencenter-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 Datencenter 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 bei vRealize Automation als **Infrastrukturarchitekt** an.
- Als Systemadministrator definieren Sie die Datacenter-Standorte. Siehe [Szenario: Hinzufügen von Datacenter-Standorten für regionsübergreifende Bereitstellungen](#).
- Als Fabric-Administrator wenden Sie die entsprechenden Standorte auf Ihre Computing-Ressourcen an. Siehe [Szenario: Anwenden eines Standorts auf eine Computing-Ressource für regionsübergreifende Bereitstellungen](#).
- Erstellen Sie einen Maschinen-Blueprint. Siehe *Installieren und Konfigurieren von vRealize Automation für das Rainpole-Szenario*.

Verfahren

- 1 Wählen Sie **Design > 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**.

Ergebnisse

Benutzer in Business-Gruppen werden jetzt zur Auswahl eines Datacenter-Standorts aufgefordert, wenn sie die Bereitstellung einer Maschine aus dem Blueprint anfordern.

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-Adresseigenschaft 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 3-43. 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.
- Informationen zur REST-API von vRealize Automation finden Sie unter *Programmierhandbuch* und *vRealize Automation-Inhaltsdienst-API* auf der Website <https://code.vmware.com>.
- 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
Verschlüsselt	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.
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.
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.

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 3-44. 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 Aktionskripte 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.

Beim Erstellen einer Softwareeigenschaft vom Typ Array und dem Datentyp „Ganzzahl“ oder „Dezimal“ müssen Sie unabhängig von dem Gebietsschema ein Semikolon als Trennzeichen für Array-Elemente verwenden. Verwenden Sie ein Komma (,) oder einen Punkt (.). Bei einigen Gebietsschemata können Sie als Dezimaltrennzeichen ein Komma (,) verwenden. Beispiel:

- Ein gültiges Array für Französisch ähnelt Folgendem: [1,11;2,22;3,33]
- Ein gültiges Array für Englisch ähnelt Folgendem: [1.11,2.22,3.33]

Wenn Sie große Zahlen in einem Array übergeben, verwenden Sie nicht das Gruppierungsformat. Beispiel: Verwenden Sie nicht **4444 444.000** (Französisch), **4.444.444,000** (Italienisch) oder **4,444,444.000** (Englisch), da Datendateien, die Gebietsschema-spezifische Formate enthalten, fehlinterpretiert werden könnten, wenn sie auf eine Maschine mit einem anderen Gebietsschema übertragen werden. Das Gruppierungsformat ist nicht zulässig, da eine Zahl wie **4,444,444.000** als drei separate Zahlen betrachtet wird. Geben Sie stattdessen nur **4444444.000** ein.

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 Design-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	<pre>for ((i = 0 ; i < \$ {#operating_systems[@]; i++)); do echo \${operating_systems[\$i]} done</pre>
	Windows CMD - %operating_systems_% wo N die Position des Elements im Array darstellt	<pre>for /F "delims== tokens=2" %A in ('set operating_systems_') do (echo %A)</pre>

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 „Dukes 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
cheetah_tgz_url = "http:// app_content_server_ip:port/artifacts/ software/jboss/cheetah-2.4.4.tar.gz"	Bash - \$cheetah_tgz_url	<pre>tar -zxvf \$cheetah_tgz_url</pre>
	Windows CMD - %cheetah_tgz_url%	<pre>start /wait c:\unzip.exe %cheetah_tgz_url%</pre>
	Windows PowerShell - \$cheetah_tgz_url	<pre>& c:\unzip.exe \$cheetah_tgz_url</pre>

Boolesche Eigenschaft

Verwenden Sie den booleschen Eigenschaftstyp, um eine Wahl zwischen „Wahr“ und „Falsch“ im Dropdown-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 3-45. 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 3-45. 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 3-46. 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"

Eine ausführliche Erklärung der unterstützten Eigenschaftstypen finden Sie unter [Eigenschaftstypen und Einstellungsoptionen](#).

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 vRealize Automation als **Softwarearchitekt** an.

Verfahren

- 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 Eigenschaftsbindungen 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
Maschinen	Ihre Software-Komponente muss direkt auf einer Maschine abgelegt werden.
Eine Ihrer veröffentlichten Software-Komponenten	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.
Software-Komponenten	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"> ■ Geben Sie einen Wert ein. ■ Deaktivieren Sie Überschreibbar. ■ Wählen Sie Erforderlich aus.
Architekten zur Angabe eines Wert auffordern	<ul style="list-style-type: none"> ■ Geben Sie einen Wert als Standardwert ein. ■ Wählen Sie Überschreibbar aus. ■ Wählen Sie Erforderlich aus.
Architekten, falls von diesen erwünscht, die Angabe eines Wert erlauben	<ul style="list-style-type: none"> ■ Geben Sie einen Wert als Standardwert ein. ■ Wählen Sie Überschreibbar aus. ■ Deaktivieren Sie Erforderlich.

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 3-47. 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. Deinstallationssskripts 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"> ■ return 0 ■ exit 0 	<ul style="list-style-type: none"> ■ return non-zero ■ exit non-zero 	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**.

Ergebnisse

Sie haben eine Software-Komponente konfiguriert und veröffentlicht. Andere Software-, IaaS- und Anwendungsarchitekten können diese Software-Komponente verwenden, um Software zu Anwendungs-Blueprints hinzuzufügen.

Nächste Schritte

Fügen Sie Ihre veröffentlichte Software-Komponente einem Anwendungs-Blueprint hinzu. Siehe [Erstellen zusammengesetzter Blueprints](#).

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**, um eine neue Software-Komponente zu erstellen.

Neue allgemeine Software-Einstellungen

Wenden Sie allgemeine Einstellungen auf die Software-Komponente an.

Tabelle 3-48. Neue allgemeine Software-Einstellungen

Einstellung	Beschreibung
Name	Geben Sie einen Namen für die Software-Komponente ein.
ID	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.
Beschreibung	Fassen Sie die Software-Komponente zugunsten anderer Architekten zusammen.
Container	<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"> ■ Wählen Sie Maschinen aus, damit Architekten Ihre Softwarekomponente direkt auf einer Maschinenkomponente in der Design-Arbeitsfläche platzieren müssen. ■ Wählen Sie Softwarekomponenten 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. ■ Wählen Sie eine bestimmte veröffentlichte Softwarekomponente aus, wenn Sie eine Softwarekomponente speziell zum Verschachteln in einer anderen von Ihnen erstellten Softwarekomponente entwerfen. ■ Wählen Sie Virtueller Azure-Computer aus, wenn Sie eine Software-Komponente speziell für einen Azure-Blueprint entwerfen.

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 3-49. Neue Software-Eigenschaften

Einstellung	Beschreibung
Name	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.
Beschreibung	Fassen Sie zugunsten anderer Benutzer die Eigenschaft und alle Anforderungen für den Wert zusammen.
Typ	Software unterstützt Zeichenfolgen-, Array-, Inhalts-, Ganzzahl- und boolesche Typen. Eine ausführliche Erklärung der unterstützten Eigenschaftstypen finden Sie unter Eigenschaftstypen und Einstellungsoptionen . Informationen zu Eigenschaftsbindungen finden Sie unter Wann Ihre Softwarekomponente Informationen einer anderen Komponente benötigt und Erstellen von Eigenschaftsbindungen zwischen Blueprint-Komponenten .
Wert	<ul style="list-style-type: none"> ■ So verwenden Sie den von Ihnen angegebenen Wert: <ul style="list-style-type: none"> ■ Geben Sie einen Wert ein. ■ Wählen Sie Erforderlich aus. ■ Deaktivieren Sie Überschreibbar. ■ So fordern Sie Architekten zur Angabe eines Werts auf: <ul style="list-style-type: none"> ■ (Optional) Geben Sie einen Wert ein, um einen Standardwert festzulegen. ■ Wählen Sie Überschreibbar aus. ■ Wählen Sie Erforderlich aus. ■ So erlauben Sie Architekten, einen Wert anzugeben oder den Wert leer zu lassen: <ul style="list-style-type: none"> ■ (Optional) Geben Sie einen Wert ein, um einen Standardwert festzulegen. ■ Wählen Sie Überschreibbar aus. ■ Deaktivieren Sie Erforderlich.
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>Wichtig 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 3-49. 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 3-50. 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"> ■ return 0 ■ exit 0 	<ul style="list-style-type: none"> ■ return non-zero ■ exit non-zero 	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.

Entwerfen 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 und Active Directory-Benutzern in Gruppen oder zum Ausführen von 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.

Sie können einen XaaS-Blueprint als eine Komponente in einem Blueprint verwenden, den Sie auf der Design-Arbeitsfläche erstellen, oder Sie können ihn direkt im Servicekatalog veröffentlichen.

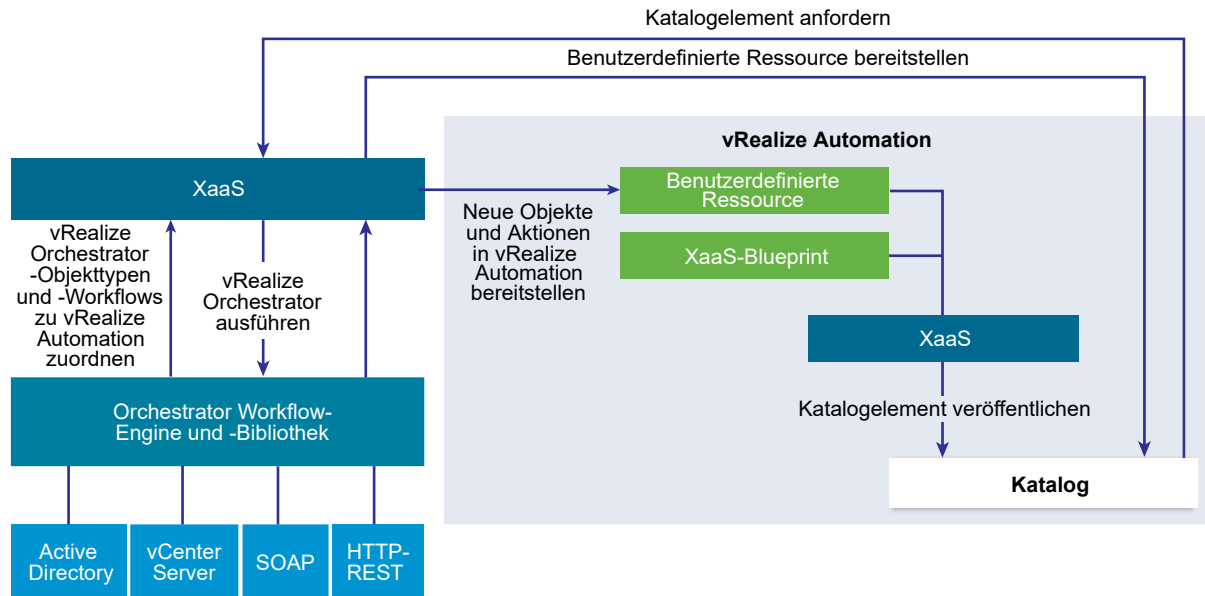
Wenn Sie einen Blueprint als eine Komponente in einem andern Blueprint verwenden, können Sie ihn so konfigurieren, dass er skaliert wird, wenn der bereitgestellte Blueprint skaliert wird.

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.

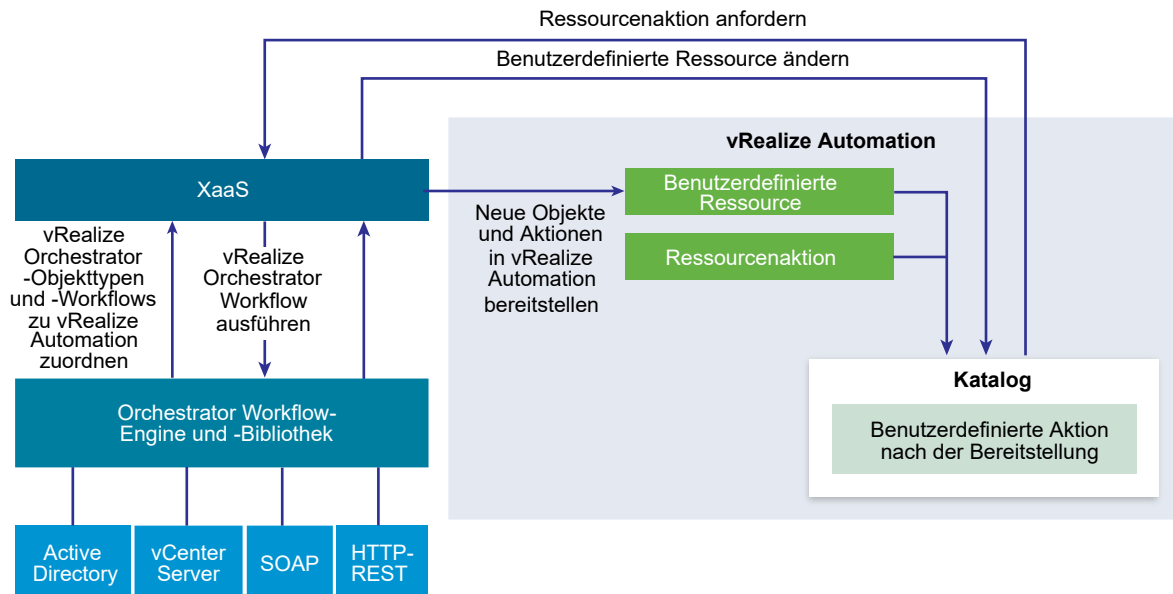
Abbildung 3-2. Erstellen und Anfordern von Katalogelementen in XaaS zur Bereitstellung einer benutzerdefinierten Ressource



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 3-3. 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 3-51. 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 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 3-52. 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.

Tabelle 3-52. Standardmäßig in vRealize Orchestrator enthaltene Plug-Ins (Fortsetzung)

Plug-In	Zweck
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.
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	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™.

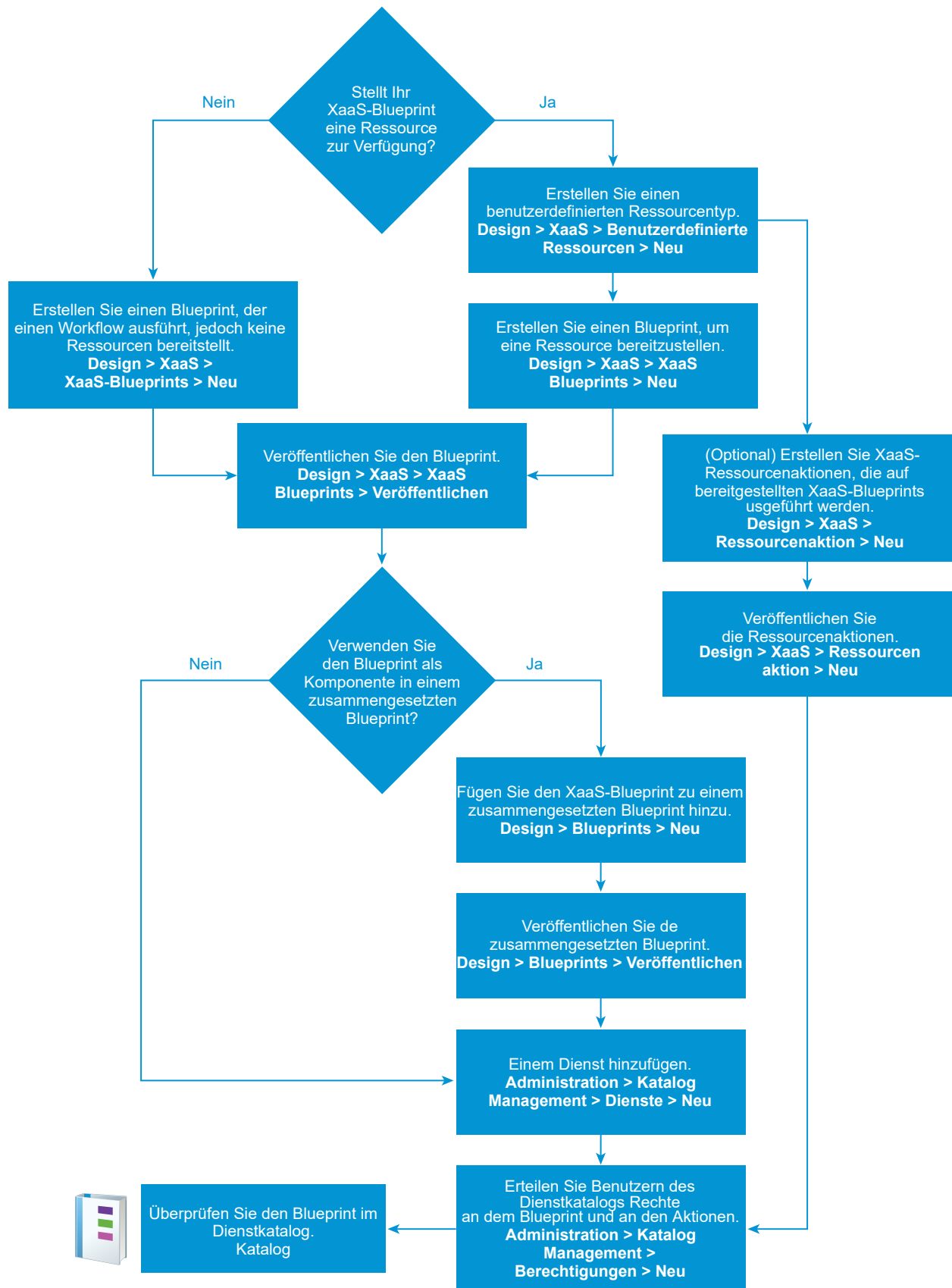
Erstellen von XaaS-Blueprints und -Ressourcenaktionen

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. Sie können eine Ressourcenaktion verwenden, um festzulegen, dass der Benutzer das Kennwort ändern muss.

XaaS Blueprint-Workflow

Der Workflow, den Sie durchführen, um einen XaaS-Blueprint und alle optionalen Ressourcenaktionen zu erstellen, variiert je nachdem, wie Sie den Entwurf verwenden möchten. Der folgende Workflow stellt den grundlegenden Vorgang dar.



Terminologie von XaaS-Blueprints

XaaS-Blueprints sind vRealize Orchestrator-Workflows, die Ressourcen bereitstellen, Änderungen an bereitgestellten Ressourcen vornehmen oder sich als Dienste verhalten können, die Aufgaben in Ihrer Umgebung durchführen. Die Blueprints und die Ressourcenaktionen weisen mehrere Nuancen auf, die Sie verstehen müssen, wenn Sie Blueprints für Ihren Servicekatalog-Benutzer entwerfen.

Die folgenden Definitionen helfen Ihnen, die verwendeten Begriffe beim Arbeiten mit XaaS-Blueprints zu verstehen.

Benutzerdefinierte Ressource

Ein vRealize Orchestrator-Objektyp, der als Ressource über die API eines vRealize Orchestrator-Plug-In freigelegt wird. Sie erstellen eine benutzerdefinierte Ressource, um den Ausgabeparameter eines XaaS-Blueprints für die Bereitstellung und einen Eingabeparameter einer Ressourcenaktion zu definieren.

XaaS-Blueprint-Komponente

Ein Blueprint für die Bereitstellung oder ein Blueprint, der nicht für eine Bereitstellung verwendet wird, den Sie auf der Design-Arbeitsfläche von Blueprint verwenden. Bei diesem Blueprint kann es sich auch um einen eigenständigen XaaS-Blueprint handeln.

Eigenständiger XaaS-Blueprint

Ein Blueprint für die Bereitstellung oder ein Blueprint, der nicht für eine Bereitstellung verwendet wird, der veröffentlicht wurde und direkt für den Servicekatalog vorgesehen ist.

Blueprint für die Bereitstellung

Ein Blueprint für die Bereitstellung, der einen vRealize Orchestrator-Workflow für das Bereitstellen von Ressourcen auf dem Ziel-Endpoint unter Verwendung der vRealize Orchestrator-Plug-In-API für den Endpoint ausführt. Fügen Sie z. B. virtuelle Netzwerkkarten zu einem Netzwerkgerät in vSphere hinzu. Um einen Blueprint für die Bereitstellung zu erstellen, benötigen Sie eine benutzerdefinierte Ressource, die den vRealize Orchestrator-Ressourcentyp definiert.

Wenn ein Servicekatalog-Benutzer diesen Typ von Katalogelement anfordert, stellt der Workflow das Element bereit und das bereitgestellte Element wird auf der Registerkarte **Elemente** gespeichert. Sie können Vorgänge für die Zeit nach der Bereitstellung für diese Art der bereitgestellten Ressourcen definieren. Zudem können Sie Blueprints skalierbar machen, indem Sie eine Instanz hinzufügen bzw. entfernen.

Blueprint, der nicht für eine Bereitstellung verwendet wird

Ein Blueprint, der nicht für eine Bereitstellung verwendet wird, führt einen vRealize Orchestrator-Workflow aus, um eine Aufgabe durchzuführen, für die die API nicht benötigt wird, um Änderungen an einem Endpoint vorzunehmen. Beispiel: Der ausgeführte Workflow generiert einen Bericht und sendet ihn anschließend per E-Mail oder postet ihn in einem Zielkommunikationssystem.

Wenn ein Servicekatalog-Benutzer diesen Typ von Katalogelement anfordert, führt der Workflow die Skript-Aufgabe durch, aber das Element wird nicht zur Registerkarte **Elemente** hinzugefügt. Sie können für diesen Typ von Blueprint keine Vorgänge nach der Bereitstellung durchführen. Sie können Blueprints, die nicht für eine Bereitstellung verwendet werden, als unterstützende Workflows in skalierbaren Blueprints verwenden. Beispiel: Sie können einen Blueprint erstellen, um einen Lastausgleichsdienst mit hoher Verfügbarkeit zu aktualisieren.

Zusammengesetzter Blueprint

Ein Blueprint, der mithilfe der Design-Arbeitsfläche erstellt wurde. Der zusammengesetzte Blueprint verwendet eine oder mehrere Komponenten. Zum Beispiel eine Maschinenkomponente, eine Softwarekomponente oder eine XaaS-Komponente. Wenn Sie ihn zu einem Dienst hinzufügen, wird er als Bereitstellung aufgelistet. Wenn Sie ihn zu einer Berechtigung hinzufügen, um ihn den Servicekatalog-Benutzern zur Verfügung zu stellen, wird er als ein zusammengesetzter Blueprint aufgelistet. Ein zusammengesetzter Blueprint kann über eine Blueprint-Komponente verfügen oder er kann eine ganze Anwendung mit mehreren Maschinen, Software und Netzwerken umfassen.

Ressourcenaktion

Ein Workflow, den Sie auf einem bereitgestellten Blueprint für die Bereitstellung ausführen können. Bei dem bereitgestellten Blueprint kann es sich um einen XaaS-Blueprint oder eine -Blueprintkomponente handeln, oder es kann ein Maschinentyp sein, den Sie einem vRealize Orchestrator-Ressourcentyp zugeordnet haben.

Überlegungen zum Entwerfen eines XaaS-Blueprints

Bevor Sie einen XaaS-Blueprint erstellen, müssen Sie die beabsichtigte Verwendung des Blueprints verstehen, sodass Sie einen Blueprint erstellen, der Ihre Ressourcen ordnungsgemäß bereitstellt.

Sie können XaaS-Blueprints als eine Blueprint-Komponente auf der Design-Arbeitsfläche oder als einen eigenständigen Blueprint erstellen und verwenden. Bei dem Blueprint kann es sich um einen Blueprint für die Bereitstellung oder einen Blueprint, der nicht für eine Bereitstellung verwendet wird, handeln.

Tabelle 3-53. XaaS Blueprinttypen und -ergebnisse

XaaS Blueprinttyp	Wird eine benutzerdefinierte Ressource benötigt?	Ist der Blueprint in einer Bereitstellung skalierbar?	Kann ich eine Ressourcenaktion für einen bereitgestellten Blueprint ausführen?
Blueprint-Komponente, die Ressourcen bereitstellt	Ja	Ja. Wenn er maßstäblich konfiguriert ist, wird er skaliert, wenn die Bereitstellung skaliert wird.	Ja. Er wird skaliert, wenn die Bereitstellung skaliert wird, und Sie können andere Ressourcenaktionen für die bereitgestellte Komponente ausführen. Die Blueprint-Komponente wird auf der Registerkarte „Elemente“ angezeigt.
Blueprint-Komponente, die einen Workflow ausführt, aber keine Ressourcen bereitstellt	Nein. Der Blueprint verwendet die vRealize Orchestrator-Serverkonfiguration, benötigt jedoch keine benutzerdefinierte XaaS-Ressource.	Nein. Er stellt keine Ressourcen bereit, kann jedoch als Teil eines Skalierungsvorgangs ausgeführt werden. Aktualisieren Sie z. B. auf Basis des Skalierungsvorgangs einen Lastausgleichsdienst mit der neuen Konfiguration.	Nein. Sie können keine Ressourcenaktion für eine Komponente ausführen, die nicht für eine Bereitstellung verwendet wird.
Eigenständiger Blueprint, der Ressourcen bereitstellt	Ja	Nein. Sie müssen Ressourcenaktionen erstellen, um Instanzen hinzuzufügen oder zu löschen.	Ja. Sie können für die bereitgestellte Ressource Ressourcenaktionen ausführen, einschließlich Aktionen, die Sie zum Unterstützen der Skalierung erstellt haben. Der Blueprint wird auf der Registerkarte „Elemente“ angezeigt.
Eigenständiger Blueprint, der einen Workflow ausführt, aber keine Ressourcen bereitstellt	Nein. Der Blueprint verwendet die vRealize Orchestrator-Serverkonfiguration, benötigt jedoch keine benutzerdefinierte XaaS-Ressource.	Nein. Er stellt keine Ressourcen bereit, kann jedoch als Teil einer Ressourcenaktion ausgeführt werden.	Nein. Sie können keine Ressourcenaktion für eine Komponente ausführen, die nicht für eine Bereitstellung verwendet wird.

Hinzufügen einer benutzerdefinierten XaaS-Ressource

Sie erstellen eine benutzerdefinierte Ressource zum Definieren des XaaS-Elements für die Bereitstellung. Um einen XaaS-Blueprint oder eine Aktion erstellen zu können, benötigen Sie eine benutzerdefinierte Ressource, die mit dem Objekttyp des Blueprint- bzw. Aktionsworkflows kompatibel ist.

Durch Erstellen einer benutzerdefinierten Ressource ordnen Sie einen Objekttyp, der durch die API eines vRealize Orchestrator-Plug-Ins verfügbar gemacht wird, als Ressource zu. Die benutzerdefinierte Ressource definiert den Ausgabeparameter eines XaaS-Blueprints für eine Bereitstellung und für das Definieren eines Eingabeparameters einer Ressourcenaktion.

Wenn ein Blueprint- oder Ressourcenaktionsworkflow eine Ressource nicht bereitstellt oder auf einem bereitgestellten Blueprint ausgeführt wird, brauchen Sie keine benutzerdefinierte Ressource zu erstellen. Sie benötigen beispielsweise keine benutzerdefinierte Ressource, wenn nach einem Bereitstellungsvorgang Ihr Workflow einen Datenbankwert aktualisiert oder eine E-Mail sendet.

Wenn Sie eine benutzerdefinierte Ressource erstellen, können Sie in den Details eines bereitgestellten Elements die Felder des schreibgeschützten Formulars angeben. Siehe [Entwerfen eines benutzerdefinierten Ressourcenformulars](#).

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **XaaS-Architekt** an.
- Verwenden Sie die detaillierten Informationen zu den Optionen, um die benutzerdefinierte Ressource zu konfigurieren. Siehe [Assistentenoptionen für benutzerdefinierte XaaS-Ressourcen](#).

Verfahren

- 1 Wählen Sie **Design > XaaS > Benutzerdefinierte Ressourcen** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Konfigurieren Sie die Werte auf der Registerkarte **Ressourcentyp**.
 - a Geben Sie den vRealize Orchestrator-Objekttyp im Textfeld **Orchestrator-Typ** ein bzw. wählen Sie ihn aus.

Geben Sie z. B. **v** ein, um die Typen mit dem Buchstaben „v“ anzuzeigen. Geben Sie ein Leerzeichen ein, um alle Typen anzuzeigen.
 - b Geben Sie einen Namen und optional eine Beschreibung ein.
 - c Geben Sie eine Version ein.

Das unterstützte Format erstreckt sich auch auf major.minor.micro-revision.
 - d Klicken Sie auf **Weiter**.
- 4 Bearbeiten Sie ggf. das **Detailformular**.

Sie können das benutzerdefinierte Ressourcenformular bearbeiten, indem Sie Elemente löschen, bearbeiten und neu anordnen. Darüber hinaus können Sie ein Formular und Formularseiten hinzufügen und die Elemente auf das neue Formular und die Formularseite ziehen.
- 5 Klicken Sie auf **Beenden**.

Ergebnisse

Sie haben eine benutzerdefinierte Ressource erstellt, die auf der Seite „Benutzerdefinierte Ressourcen“ aufgeführt wird. Basierend auf dieser benutzerdefinierten Ressource können Sie XaaS-Blueprints oder -Aktionen erstellen.

Nächste Schritte

- Erstellen Sie einen XaaS-Blueprint. Siehe [Hinzufügen eines XaaS-Blueprints](#).
- Erstellen Sie eine XaaS-Ressourcenaktion. Siehe [Erstellen einer XaaS Ressourcenaktion](#).

Assistentenoptionen für benutzerdefinierte XaaS-Ressourcen

Sie verwenden diese benutzerdefinierten Ressourcenoptionen zum Erstellen oder Ändern einer benutzerdefinierten Ressource, damit Sie den XaaS-Blueprint und Ressourcenaktionsworkflows ausführen können, die Ressourcen bereitstellen oder bereitgestellte Ressourcen ändern.

Sie können nur eine benutzerdefinierte Ressource für einen Objekttyp erstellen. Sie können die benutzerdefinierte Ressource für mehrere Blueprints und Ressourcenaktionen verwenden.

Um eine benutzerdefinierte Ressource zu erstellen, wählen Sie **Design > XaaS >**

Benutzerdefinierte Ressourcen

Ressourcentyp

Die Liste der möglichen Objekttypen, die auf der Registerkarte **Ressourcentyp** auf Basis der installierten Plug-Ins in der konfigurierten vRealize Orchestrator-Instanz angezeigt wird. vRealize Automation sammelt die Werte aus der konfigurierten vRealize Orchestrator-Instanz.

Tabelle 3-54. Optionen für Ressourcentypen

Option	Beschreibung
Orchestrator-Typ	Geben Sie den Typ ein oder wählen Sie ihn aus, der den Workflow unterstützt, den Sie zum Bereitstellen verwenden. Der Typ besteht aus dem Plug-In-Namen, wie er in der Skript-API erscheint, beispielsweise VC für vCenter, und dem Objekttyp, beispielsweise VirtualMachine. In diesem Beispiel verwendet die API den Wert VC:VirtualMachine. Dieser Typ kann der Ausgabeparameter des Blueprint-Workflows oder der Eingabeparameter des Ressourcenaktionsworkflows sein.
Name	Geben Sie einen sinnvollen Namen für die benutzerdefinierte Ressource ein, damit Sie sie identifizieren können, wenn Sie XaaS-Blueprints oder Ressourcenaktionen erstellen.
Beschreibung	Geben Sie eine ausführliche Beschreibung ein.
Version	Das unterstützte Formular erweitert sich zu major.minor.micro-revision.

Detailformular

Diese Formularfelder erscheinen als schreibgeschützte Werte, wenn Ihre Servicekatalog-Benutzer ein Element bereitstellen, das diese benutzerdefinierte Ressource verwendet. Sie können die vorhandenen Felder ändern und neue, extern definierte Felder hinzufügen.

Weitere Informationen über das Konfigurieren der Formulare finden Sie unter [Entwerfen eines benutzerdefinierten Ressourcenformulars](#).

Wo verwendet

Da Sie nur eine benutzerdefinierte Ressource pro Objekttyp erstellen können, können Sie anhand dieser Seite des Assistenten verstehen, wie die benutzerdefinierte Ressource verwendet wird.

Diese Registerkarte steht für gespeicherte benutzerdefinierte Ressourcen zur Verfügung und nicht beim Erstellen der Ressource.

Tabelle 3-55. Wo werden Optionen verwendet

Option	Beschreibung
XaaS-Blueprints	<p>Eine Liste der Blueprints, die zur Verwendung dieser benutzerdefinierten Ressource konfiguriert sind.</p> <p>Von dieser Seite aus können Sie die folgenden Aktionen durchführen:</p> <ul style="list-style-type: none"> ■ Bearbeiten. Öffnet den Blueprint, damit Sie sehen können, wie er konfiguriert ist, oder um ihn zu ändern. ■ Veröffentlichen/Veröffentlichung rückgängig machen. Sie ändern den Zustand des Blueprints, indem Sie ihn zur Verwendung in einem zusammengesetzten Blueprint oder zum Hinzufügen zu einem Dienst verfügbar machen. Wenn Sie die Veröffentlichung eines Blueprints rückgängig machen, steht er potenziell nicht zur Verwendung in zusammengesetzten Blueprints, zum Hinzufügen zu einem Dienst oder im Servicekatalog zur Verfügung. ■ Löschen. Entfernt diesen Blueprint vom System.
Ressourcenaktionen	<p>Eine Liste der Ressourcenaktionen, die zur Verwendung dieser benutzerdefinierten Ressource konfiguriert sind.</p> <p>Von dieser Seite aus können Sie die folgenden Aktionen durchführen:</p> <ul style="list-style-type: none"> ■ Bearbeiten. Öffnet die Ressourcenaktion, damit Sie sehen können, wie sie konfiguriert ist, oder um sie zu ändern. ■ Veröffentlichen/Veröffentlichung rückgängig machen. Sie ändern den Zustand der Ressourcenaktion, indem Sie sie in einer Berechtigung verfügbar machen. Wenn Sie die Veröffentlichung einer Ressourcenaktion rückgängig machen, können Sie sie ggf. für das Hinzufügen zu einem Dienst oder für das Ausführen auf bereitgestellten Blueprints unverfügbar machen. ■ Löschen. Entfernt diese Ressourcenaktion vom System.

Erstellen Sie einen XaaS-Blueprint

Ein XaaS-Blueprint ist ein Bereitstellungs- oder Nicht-Bereitstellungs-Blueprint. Zu den verfügbaren vRealize Orchestrator-Bereitstellungsworkflows gehören unter anderem das Erstellen von virtuellen Maschinen, das Hinzufügen von Benutzern zu Active Directory oder das Erstellen von Snapshots einer virtuellen Maschine. Einige der Nicht-Bereitstellungsworkflows, die Sie möglicherweise erstellen, beinhalten das Update Ihres Lastausgleichsdiensts oder das Erstellen eines Berichts und das Senden dieses Berichts an Empfänger.

Sie können XaaS-Blueprints basierend auf den in vRealize Orchestrator bereitgestellten Workflows erstellen oder Sie können Workflows verwenden, die Sie erstellen, um die für Ihre Umgebung spezifischen Ziele zu erreichen.

Verfahren

1 Hinzufügen eines XaaS-Blueprints

Ein XaaS-Blueprint ist eine Spezifizierung für die Ausführung eines vRealize Orchestrator-Workflows, der eine Änderung am Zielsystem in Ihrer Umgebung vornimmt. Der Blueprint enthält den Workflow und kann Eingabeparameter, Übermittlungs- und schreibgeschützte Formulare, Aktionsfolgen und den Bereitstellungs- bzw. Nicht-Bereitstellungsvorgang enthalten.

2 Hinzufügen eines XaaS-Blueprints zu einem zusammengesetzten Blueprint

Sie fügen einen XaaS-Blueprint als eine Komponente eines zusammengesetzten Blueprints auf ähnliche Weise hinzu, wie Sie andere Blueprint-Komponenten auf der Design-Arbeitsfläche hinzufügen.

Hinzufügen eines XaaS-Blueprints

Ein XaaS-Blueprint ist eine Spezifizierung für die Ausführung eines vRealize Orchestrator-Workflows, der eine Änderung am Zielsystem in Ihrer Umgebung vornimmt. Der Blueprint enthält den Workflow und kann Eingabeparameter, Übermittlungs- und schreibgeschützte Formulare, Aktionsfolgen und den Bereitstellungs- bzw. Nicht-Bereitstellungsvorgang enthalten.

Sie können XaaS-Blueprints erstellen, die Sie auf mindestens eine der folgenden Arten verwenden:

- Erstellen einer XaaS-Blueprint-Komponente. Ein Komponenten-Blueprint ist ein Bereitstellungs- bzw. Nicht-Bereitstellungs-Blueprint, den Sie auf der Design-Arbeitsfläche als Teil eines zusammengesetzten Blueprints verwenden können. Wenn Sie ihn als Komponente verwenden, müssen Sie die Optionen für den Lebenszyklus der Komponente konfigurieren, die vertikale oder horizontale Skalierungen auf dem bereitgestellten zusammengesetzten Blueprint unterstützen.

Dieser Blueprint-Typ kann auch als eigenständiger Blueprint veröffentlicht werden.
- Erstellen eines eigenständigen XaaS-Blueprints. Ein eigenständiger Blueprint ist ein Bereitstellungs- bzw. Nicht-Bereitstellungs-Blueprint, der veröffentlicht wird und für den Dienstkatalog direkt berechtigt ist.

Ein Beispiel zum Erstellen von Active Directory-Benutzern unter Verwendung eines XaaS-Blueprints finden Sie unter [Erstellen eines XaaS-Blueprints und einer Aktion zum Erstellen und Ändern eines Benutzers](#).

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **XaaS-Architekt** an.
- Wenn der Blueprint Ressourcen bereitstellen muss, erstellen Sie eine benutzerdefinierte Ressource entsprechend dem Ausgabeparameter des Dienst-Blueprints. Siehe [Hinzufügen einer benutzerdefinierten XaaS-Ressource](#). Wenn er keine vRealize Orchestrator-Plug-In-API verwendet, müssen Sie keine benutzerdefinierte Ressource konfigurieren.
- Beim Erstellen eines XaaS-Blueprints veröffentlichen Sie einen vRealize Orchestrator-Workflow als einen potenziellen Komponenten-Blueprint oder als Katalogelement. Der Blueprint enthält ein Formular, das Sie bearbeiten können. Siehe [Entwerfen eines XaaS-Blueprint-Formulars](#).
- Verwenden Sie die detaillierten Optionsinformationen, um den Blueprint zu konfigurieren. Siehe [XaaS-Blueprint – Assistentenoptionen „Neu“ oder „Bearbeiten“](#).

Verfahren

- 1 Wählen Sie **Design > XaaS > XaaS-Blueprints** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Wählen Sie auf der Registerkarte **Workflow** den Workflow aus, der ausgeführt wird, wenn der Blueprint die Ressource bereitstellt.
Diese Registerkarte ist nicht verfügbar, wenn Sie einen Blueprint bearbeiten.
 - a Navigieren Sie in der vRealize Orchestrator-Workflowbibliothek und wählen Sie einen entsprechenden Workflow für Ihre benutzerdefinierte Ressource aus.
 - b Überprüfen Sie die Eingabe- und Ausgabeparameter, um sicherzustellen, dass Sie die richtigen Werte zu einem späteren Zeitpunkt eingeben können.
 - c Klicken Sie auf **Weiter**.
- 4 Konfigurieren Sie auf der Registerkarte **Allgemein** die Optionen und klicken Sie auf **Weiter**.
 - a Geben Sie im Textfeld **Name** den Namen ein, der diesen Blueprint von ähnlichen Blueprints unterscheidet.
 - b Wenn Sie diesen Blueprint nicht als eine Komponente in einem zusammengesetzten Blueprint verwenden möchten, deaktivieren Sie das Kontrollkästchen **Als Komponente auf der Design-Arbeitsfläche verfügbar machen**.
- 5 Bearbeiten Sie auf der Registerkarte **Blueprint-Formular** das Formular nach Bedarf und klicken Sie auf **Weiter**.

- 6 Wählen Sie auf der Seite **Bereitgestellte Ressource** einen Wert aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Keine Bereitstellung	Wenn der Workflow keine Ressourcen bereitstellt, können Sie diese Option auswählen oder das Feld leer lassen.
<Eine zuvor erstellte benutzerdefinierte Ressource>	Wählen Sie eine benutzerdefinierte Ressource aus, die diesen Bereitstellungsworkflow unterstützt.

- 7 Legen Sie auf der Registerkarte **Lebenszyklus der Komponente** fest, wie sich dieser Blueprint während vertikalen oder horizontalen Skalierungen und Löschvorgängen verhält.

Diese Workflows werden auf einem bereitgestellten zusammengesetzten Blueprint ausgeführt, wobei es sich bei diesem Blueprint um eine Komponente handelt. Die Verfügbarkeit der verschiedenen Optionen hängt vom jeweiligen Blueprint ab. Nicht alle Blueprint-Workflows unterstützen oder erfordern alle Optionen.

- 8 Klicken Sie auf **Beenden**.
- 9 Wählen Sie die Zeile für Ihren Blueprint aus und klicken Sie auf **Veröffentlichen**.

Ergebnisse

Sie haben einen XaaS-Blueprint erstellt und veröffentlicht.

Nächste Schritte

- Um diesen Blueprint als einen eigenständigen Blueprint direkt zum Dienstkatalog hinzuzufügen, fügen Sie einen Dienst hinzu und fügen Sie den Blueprint einem Dienst hinzu. Siehe [Hinzufügen eines Diensts](#).
- Informationen zur Verwendung dieses Blueprints als eine Komponente in einem zusammengesetzten Blueprint finden Sie unter [Hinzufügen eines XaaS-Blueprints zu einem zusammengesetzten Blueprint](#).

XaaS-Blueprint – Assistentenoptionen „Neu“ oder „Bearbeiten“

Sie verwenden diese Optionen, um einen XaaS-Blueprint zu erstellen, der einen vRealize Orchestrator-Workflow ausführt, wenn der Blueprint bereitgestellt wird. Der Workflow ändert ein Zielsystem in Ihrer Umgebung.

Weitere Informationen über die auszuführenden Schritte zum Erstellen des Blueprints finden Sie unter [Hinzufügen eines XaaS-Blueprints](#).

Um diesen Assistenten zu verwenden, wählen Sie **Design > XaaS > XaaS-Blueprints**.

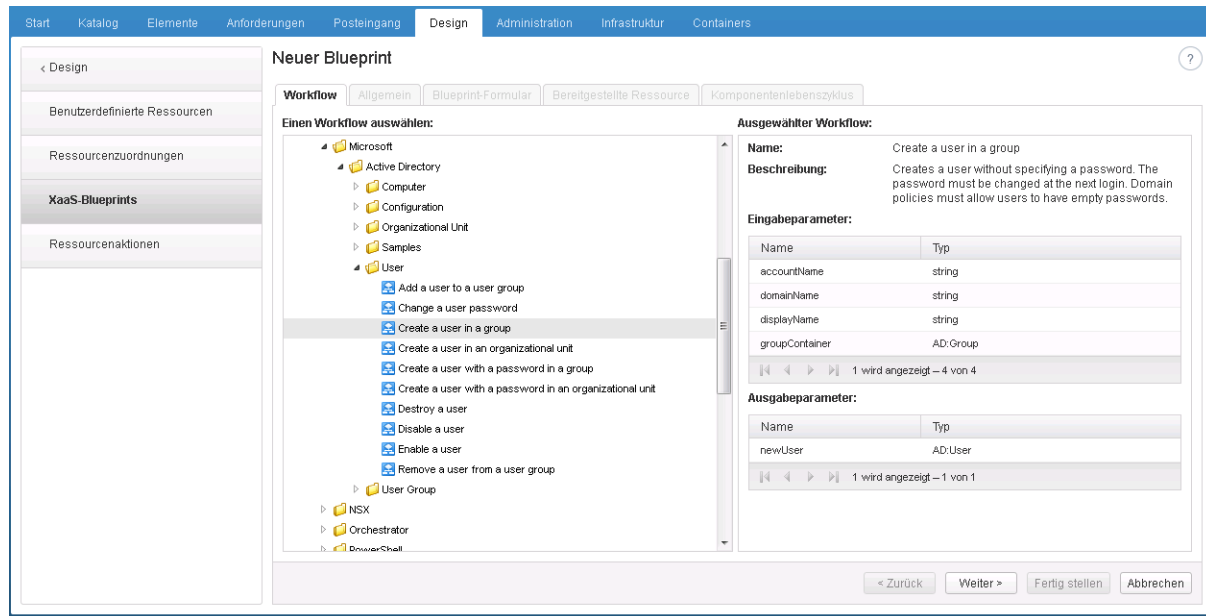
Registerkarte „Workflow“

Wählen Sie den Workflow aus, der ausgeführt wird, wenn der Blueprint die Ressource bereitstellt.

Diese Registerkarte ist nicht verfügbar, wenn Sie einen Blueprint bearbeiten.

In der folgenden Abbildung befindet sich der Workflow-Baum links und die Parameter werden rechts angezeigt.

Abbildung 3-4. Registerkarte „Workflow“ im Assistenten „XaaS-Blueprint“



Überprüfen Sie die Eingabe- und Ausgabeparameter, um sicherzugehen, dass Sie bzw. Ihre Service-Katalog-Benutzer unter den folgenden Bedingungen die korrekten Werte angeben können:

- Wenn Sie das Blueprint-Formular in diesem Assistenten oder auf der Design-Arbeitsfläche anpassen.
- Wenn Sie alle Eingabeparameter leer lassen, können die Servicekatalog-Benutzer die Werte festlegen.

Registerkarte „Allgemein“

Konfigurieren Sie die Metadaten bezüglich des Blueprints und dessen Verhalten.

Tabelle 3-56. Optionen der Registerkarte „Allgemein“

Option	Beschreibung
Name	<p>Der Name des Blueprints, wie er an den folgenden Stellen angezeigt werden soll:</p> <ul style="list-style-type: none"> ■ Design-Arbeitsfläche. Wenn Sie „Als Komponente auf der Design-Arbeitsfläche verfügbar machen“ auswählen, wird dieser Wert als der Name verwendet, der in der Kategorieliste erscheint. ■ Dienste. Wenn Sie diesen Blueprint als eigenständigen Blueprint verwenden, ist dieser Wert der Name, den Sie sehen, wenn Sie Katalogelemente zum Dienst hinzufügen. ■ Berechtigungen. Wenn Sie den Blueprint als Einzelelement berechtigen, ist dieser Wert der Name, den Sie in der Liste „Elemente hinzufügen“ sehen.
Beschreibung	Geben Sie eine ausführliche Beschreibung an, die Ihnen dabei hilft, ähnliche Elemente auseinanderzuhalten.
Informationsseite zur Kataloganforderung ausblenden	Aktivieren Sie das Kontrollkästchen, wenn Sie nicht möchten, dass die Servicekatalogverbraucher eine Beschreibung und einen Grund angeben müssen, wenn sie das Element anfordern. Das Kontrollkästchen ist standardmäßig aktiviert.
Version	Das unterstützte Format erstreckt sich auch auf major.minor.micro-revision.
Als Komponente auf der Design-Arbeitsfläche verfügbar machen	<p>Wenn Sie vorhaben, den Blueprint als eine Komponente in einem Design-Arbeitsflächen-Blueprint zu verwenden, wählen Sie diese Option.</p> <p>Wenn er veröffentlicht wird, steht der Blueprint in der Kategorie zur Verfügung, die Sie auswählten, als Sie die benutzerdefinierte Ressource konfigurierten.</p> <p>Wenn Sie diese Option nicht auswählen, erscheint der Blueprint nicht auf der Design-Arbeitsfläche. Sie können ihn dennoch zu einem Dienst hinzufügen und Benutzern die Berechtigung erteilen, ihn als eigenständigen Blueprint bereitzustellen.</p>

Registerkarte „Blueprint-Formular“

Bei den Feldern, die auf dieser Seite des Assistenten angezeigt werden, handelt es sich um die Workflow-Eingabeparameter. Sie können eine oder mehrere der folgenden Änderungen vornehmen:

- Hinzufügen von Feldern zum Formular.
- Ändern der vorhandenen Felder durch Löschen oder Neuordnen der Felder.
- Angeben von Standardwerte als Eingabeparameter.

Alle Änderungen wirken sich auf das Formular aus, das den folgenden Benutzern vorgelegt wird:

- Der Anwendungsarchitekt, der auf der Design-Arbeitsfläche arbeitet, wenn dieser XaaS-Blueprint als eine Blueprintkomponente verwendet wird.
- Der Servicekatalog-Benutzer, wenn dieser Blueprint als eigenständiger Blueprint veröffentlicht wird.

Weitere Informationen über das Konfigurieren der Formulare finden Sie unter [Entwerfen eines XaaS-Blueprint-Formulars](#).

Bereitgestellte Ressource

Die bereitgestellte Ressource verknüpft den Blueprint mit einer entsprechenden benutzerdefinierten XaaS-Ressource, die Sie auf der Seite „Benutzerdefinierte Ressource“ unter **Design > XaaS > Benutzerdefinierte Ressource** konfiguriert haben.

Tabelle 3-57. Optionen für bereitgestellte Ressourcen

Option	Beschreibung
Eine benutzerdefinierte Ressource, die Sie bereits erstellt haben	<p>Wählen Sie die benutzerdefinierte Ressource aus, die den vRealize Orchestrator-Ressourcentyp definiert, der zum Ausführen des Blueprints für die Bereitstellung erforderlich ist.</p> <p>Ein Blueprint für die Bereitstellung führt einen vRealize Orchestrator-Workflow aus, der unter Verwendung der vRealize Orchestrator-Plug-In-API für den Endpoint Ressourcen auf dem Ziel-Endpoint bereitstellt. Fügen Sie z. B. virtuelle Netzwerkkarten zu einem Netzwerkgerät in vSphere hinzu.</p> <p>Sie können Vorgänge für die Zeit nach der Bereitstellung für diese Art der bereitgestellten Ressourcen definieren. Zudem können Sie den Blueprint skalierbar machen, indem Sie Instanzen hinzufügen bzw. entfernen.</p> <p>Ergebnisse</p> <ul style="list-style-type: none"> ■ Der Blueprint kann skaliert werden. ■ Der Blueprint erscheint auf der Design-Arbeitsfläche in der Kategorie, die für die ausgewählte benutzerdefinierte Ressource angegeben wurde. ■ Der Blueprint wird auf der Registerkarte Elemente angezeigt, wenn Sie einen Blueprint bereitstellen, der ihn enthält, und nach der Bereitstellung können Sie für das Element alle Aktionen ausführen.
Keine Bereitstellung	<p>Ein Blueprint, der nicht für eine Bereitstellung verwendet wird, führt einen vRealize Orchestrator-Workflow aus, um eine Aufgabe durchzuführen, für die die API nicht benötigt wird, um Änderungen an einem Endpoint vorzunehmen. Erstellen Sie beispielsweise einen Bericht und senden Sie ihn per E-Mail an ein Zielkommunikationssystem bzw. veröffentlichen Sie ihn auf einem solchen.</p> <p>Ergebnisse</p> <ul style="list-style-type: none"> ■ Der Blueprint kann nicht skaliert werden. Sie können Blueprints, die nicht für eine Bereitstellung verwendet werden, als unterstützende Workflows in skalierbaren Blueprints verwenden. Beispiel: Sie können einen Blueprint erstellen, um einen Lastausgleichsdienst mit hoher Verfügbarkeit zu aktualisieren. ■ Der Blueprint wird auf der Design-Arbeitsfläche in der Kategorie „XaaS“ angezeigt. ■ Der Blueprint wird nicht auf der Registerkarte Elemente angezeigt, wenn Sie einen Blueprint bereitstellen, der es enthält. Und nach der Bereitstellung können Sie für das Element keine Aktionen ausführen.

Registerkarte „Komponentenlebenszyklus“

Die Registerkarte „Komponentenlebenszyklus“ steht zur Verfügung, wenn Sie **Als Komponente auf der Design-Arbeitsfläche verfügbar machen** auf der Registerkarte **Allgemein** ausgewählt haben.

Sie verwenden diese Optionen, um festzulegen, wie sich dieser Blueprint nach der Bereitstellung bei Skalierungsvorgängen verhält, wenn er als Komponente in einem zusammengesetzten Blueprint verwendet wird.

Die Verfügbarkeit der verschiedenen Optionen hängt vom Blueprint ab. Nicht alle Blueprint-Workflows unterstützen oder erfordern alle Optionen. Da Ihr XaaS in einem zusammengesetzten Blueprint verwendet werden könnte, sollten Sie die Optionen für das Aktualisieren und das Löschen sowie für das Zuteilen und Freigeben konfigurieren, sofern sie dem Blueprint zur Verfügung stehen, sodass der Blueprint ordnungsgemäß skaliert wird.

Tabelle 3-58. Komponentenlebenszyklus-Optionen

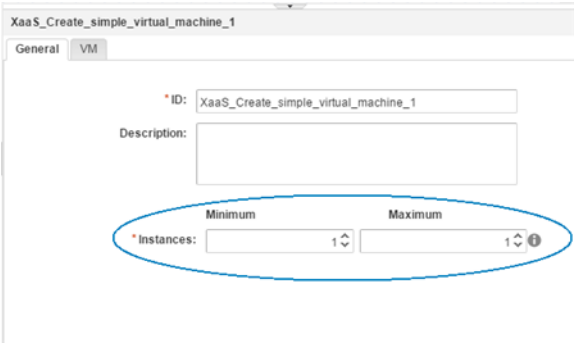
Option	Beschreibung
Skalierbar	<p>Wählen Sie diese Option, um dem Servicekatalogbenutzer zu ermöglichen, nach der Bereitstellung die Anzahl der Instanzen dieser Blueprint-Komponente als Teil des Vorgangs für die vertikale oder horizontale Skalierung zu ändern.</p> <p>Diese Option steht zur Verfügung, wenn Sie auf der Registerkarte „Ressourcen“ eine benutzerdefinierte Ressource ausgewählt haben. Sie ist nicht verfügbar, wenn Sie die Option „Keine Bereitstellung“ ausgewählt haben.</p> <p>Wenn Sie diesen Blueprint skalierbar machen, wird die Option „Instanzen“ zur Registerkarte „Allgemein“ auf der Design-Arbeitsfläche hinzugefügt. Betrachten Sie das nachfolgende Beispiel. Wenn Sie „Skalierbar“ nicht auswählen, steht die Option „Instanzen“ nicht auf der Design-Arbeitsfläche zur Verfügung.</p> 
Bereitstellungsworkflow	<p>Der Workflow, der während einer Bereitstellung oder eines horizontalen Skalierungsvorgangs läuft. Dieser Workflow wurde ausgewählt, als Sie diesen Blueprint erstellten, und Sie können den Wert nicht bearbeiten.</p>

Tabelle 3-58. Komponentenlebenszyklus-Optionen (Fortsetzung)

Option	Beschreibung
Zuteilungsworkflow	<p>Wählen Sie den Workflow, der vor jedem Erstbereitstellungsvorgang oder jedem Vorgang für die horizontale Skalierung ausgeführt wird.</p> <p>Dieser Lebenszyklus-Workflowtyp steht für Azure-Zuteilungen zur Verfügung. Wenn Sie einen Zuteilungsworkflow für einen Skalierungsvorgang erstellen, muss er die folgenden Werte enthalten:</p> <ul style="list-style-type: none"> ■ Eingabeparameter <ul style="list-style-type: none"> ■ Der Parametername ist <code>requestData</code> und der Parametertyp ist <code>Properties</code>. ■ Der Parametername ist <code>subtenant</code> und der Parametertyp ist <code>Properties</code>. ■ <code>reservations</code> und der Parametertyp ist <code>Arrays/Properties</code>. ■ Ausgabeparameter <ul style="list-style-type: none"> ■ Muss einen Parameter enthalten und der Parametertyp muss <code>Properties</code> sein
Aktualisierungsworkflow	<p>Wählen Sie den Workflow aus, der während der Aktualisierungsvorgänge ausgeführt wird, einschließlich horizontaler und vertikaler Skalierungsvorgänge, wenn eine Komponente nicht skalierbar ist, aber aktualisiert werden kann.</p> <p>Ein Lastausgleichsdienst wird beispielsweise mit der neuen Konfiguration aktualisiert, die mit dem horizontalen bzw. vertikalen Skalierungsvorgang für eine Komponente im zusammengesetzten Blueprint erstellt wurde.</p> <p>Der Aktualisierungsworkflow gilt möglicherweise für eine Komponente, die an die skalierte Komponente gebunden, aber selbst nicht skalierbar ist. Dieser Aktualisierungsworkflow kann die nicht skalierbare Komponente basierend auf einem Aktualisierungsvorgang ändern.</p> <p>Wenn Sie einen Aktualisierungsworkflow für einen Skalierungsvorgang erstellen, muss er die folgenden Werte enthalten:</p> <ul style="list-style-type: none"> ■ Eingabeparameter <ul style="list-style-type: none"> ■ Muss einen Parameter enthalten – dabei ist der Parametername unerheblich –, der dem Ausgabeparametertyp des Bereitstellungsworkflows entspricht. ■ Der Parametername ist <code>data</code> und der Parametertyp ist <code>Properties</code>.

Tabelle 3-58. Komponentenlebenszyklus-Optionen (Fortsetzung)

Option	Beschreibung
Löschworkflow:	<p>Wählen Sie den Workflow aus, der während eines vertikalen Skalierungs- oder Löschvorgangs ausgeführt wird.</p> <p>Wenn Sie einen Löschworkflow für einen Skalierungsvorgang erstellen, muss er den folgenden Wert enthalten:</p> <ul style="list-style-type: none"> ■ Eingabeparameter <ul style="list-style-type: none"> ■ Muss einen Parameter enthalten – dabei ist der Parametername unerheblich –, der dem Ausgabeparametertyp des Bereitstellungsworkflows entspricht. <p>Wenn z. B. der Bereitstellungsworkflow „Einfache virtuelle Maschine erstellen“ den Ausgabeparameter „VC:VirtualMachine“ enthält, muss der Löschworkflow einen Eingabeparameter des Typs „VC:VirtualMachine“ enthalten.</p>
Workflow zur Aufhebung der Zuteilung	<p>Wählen Sie den Workflow aus, der nach einem vertikalen Skalierungs- oder Löschvorgang ausgeführt wird. Wenn während des Vorgangs die Zuteilung nicht aufgehoben werden kann, wird der Löschworkflow weiterhin erwartungsgemäß ausgeführt.</p> <p>Das Aufheben der Zuteilung ist der letzte Prozess, wenn Sie einen zusammengesetzten Blueprint vertikal skalieren oder löschen. Dies wird nach dem Löschvorgang ausgeführt und gibt Ressourcen frei.</p> <p>Dieser Lebenszyklus-Workflowtyp steht für Azure-Zuteilungen zur Verfügung. Wenn Sie einen Workflow zur Aufhebung der Zuteilung für einen Skalierungsvorgang erstellen, muss er den folgenden Wert enthalten:</p> <ul style="list-style-type: none"> ■ Eingabeparameter <ul style="list-style-type: none"> ■ Der Parametername ist <code>data</code> und der Parametertyp ist <code>Properties</code>.
Kategorie	<p>Um die Position des XaaS-Blueprints auf der Design-Arbeitsfläche anzugeben, wählen Sie im Dropdown-Menü Kategorie der Design-Arbeitsfläche einen Wert aus.</p> <p>Wenn Sie keine Kategorie auswählen, wird der Blueprint zur XaaS-Kategorie hinzugefügt, wenn er veröffentlicht wird.</p>

Hinzufügen eines XaaS-Blueprints zu einem zusammengesetzten Blueprint

Sie fügen einen XaaS-Blueprint als eine Komponente eines zusammengesetzten Blueprints auf ähnliche Weise hinzu, wie Sie andere Blueprint-Komponenten auf der Design-Arbeitsfläche hinzufügen.

Verwenden Sie diese Methode zum Hinzufügen eines XaaS zu einem zusammengesetzten Blueprint. Dieser Blueprint kann die einzige Blueprint-Komponente oder eine von mehreren Komponenten sein, aus der bzw. denen ein Anwendungs-Blueprint besteht.

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 zusammengesetzten Blueprint hinzuzufügen.

Wenn Sie für einen Anwendungs-Blueprint eine vertikale oder horizontale Skalierung vornehmen, richtet sich die Skalierung des XaaS-Blueprints nach der Konfiguration der Lebenszyklusoptionen des Blueprints.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Infrastrukturarchitekt** an.
- Erstellen und veröffentlichen Sie einen XaaS-Blueprint. Siehe [Erstellen Sie einen XaaS-Blueprint](#). Nach dem Erstellen des Blueprints geben Sie die Kategorie an, in der sich der Blueprint auf der Design-Arbeitsfläche befindet.
- Informieren Sie sich darüber, wie die XaaS-Blueprint-Formulare im zusammengesetzten Blueprint angepasst werden. Siehe [Entwerfen von Formularen für XaaS-Blueprints und Aktionen](#).

Verfahren

- 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 Suchen Sie den Blueprint in der Liste „Kategorien“.
- 4 Ziehen Sie Ihren Blueprint auf die Arbeitsfläche.
- 5 Konfigurieren Sie die Standardwerte auf den Registerkarten „Allgemein“ und „Erstellen“.

Dies sind die Standardwerte, die im Servicekatalogformular angezeigt werden, wenn ein Benutzer das Element anfordert.
- 6 Klicken Sie auf **Fertig stellen**.
- 7 Wählen Sie den Blueprint aus und klicken Sie auf **Veröffentlichen**.

Ergebnisse

Der XaaS-Blueprint ist nun Teil des zusammengesetzten Blueprints.

Nächste Schritte

Fügen Sie den zusammengesetzten Blueprint einem Dienst hinzu. Siehe [Verwalten des Servicekatalogs](#).

Erstellen einer XaaS Ressourcenaktion

Sie erstellen eine Ressourcenaktion, um bereitgestellte Elemente mithilfe von vRealize Orchestrator-Workflows verwalten zu können.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **XaaS-Architekt** an.
- Überprüfen Sie, ob eine benutzerdefinierte Ressource vorhanden ist, die die Aktion unterstützt. Siehe [Hinzufügen einer benutzerdefinierten XaaS-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](#).

Verfahren

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 Entwurfszustand, und Sie müssen die Ressourcenaktion veröffentlichen.

3 Zuweisen eines Symbols zu einer XaaS-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 vRealize Automation als **XaaS-Architekt** an.
- Erstellen Sie eine benutzerdefinierte Ressource, die dem Eingabeparameter der Ressourcenaktion entspricht.

Verfahren

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Navigieren Sie in der vRealize Orchestrator-Workflowbibliothek und wählen Sie einen entsprechenden Workflow für Ihre benutzerdefinierte Ressource 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.

Das unterstützte Format erstreckt sich auch auf major.minor.micro-revision.
- 11 (Optional) Wählen Sie den Aktionstyp aus.

Option	Beschreibung
Löschung	Der Eingabeparameter des Ressourcenaktionsworkflows wird gelöscht und das Element wird auf der Registerkarte Elemente entfernt. Beispielsweise dient die Ressourcenaktion zum Löschen einer bereitgestellten Maschine.
Bereitstellung	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 Elemente hinzugefügt. Wenn nur die Option Keine Bereitstellung 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
Formular hinzufügen	Klicken Sie neben dem Formularnamen auf das Symbol Neues Formular (+), geben Sie die erforderlichen Informationen ein und klicken Sie auf Übernehmen .
Formular bearbeiten	Klicken Sie neben dem Formularnamen auf das Symbol Bearbeiten (✎), nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf Übernehmen .
Workflow-Präsentation neu generieren	Klicken Sie neben dem Formularnamen auf das Symbol Neu erstellen (↺) und klicken Sie auf OK .
Formular löschen	Klicken Sie neben dem Formularnamen auf das Symbol Löschen (✖) und klicken Sie im Bestätigungsdialogfeld auf OK .
Formularseite hinzufügen	Klicken Sie neben dem Formularnamen auf das Symbol Neue Seite (+), geben Sie die erforderlichen Informationen ein und klicken Sie auf Übernehmen .
Formularseite bearbeiten	Klicken Sie neben dem Namen der Formularseite auf das Symbol Bearbeiten (✎), nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf Übernehmen .
Formularseite löschen	Klicken Sie neben dem Formularnamen auf das Symbol Löschen (✖) und klicken Sie im Bestätigungsdialogfeld auf OK .
Element zur Formularseite hinzufügen	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 Übernehmen klicken.
Element bearbeiten	Klicken Sie neben dem zu bearbeitenden Element auf das Symbol Bearbeiten (✎), nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf Übernehmen .
Element löschen	Klicken Sie neben dem zu löschenden Element auf das Symbol Löschen (✖) und klicken Sie im Bestätigungsdialogfeld auf OK .

14 Klicken Sie auf **Beenden**.

Ergebnisse

Sie haben eine Ressourcenaktion erstellt, und die Ressourcenaktion wird auf der Seite „Ressourcenaktionen“ aufgeführt.

Nächste Schritte

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 vRealize Automation als **XaaS-Architekt** an.

Verfahren

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Wählen Sie die Zeile der zu veröffentlichenden Ressourcenaktion aus und klicken Sie auf die Schaltfläche **Veröffentlichen**.

Ergebnisse

Der Status der Ressourcenaktion ändert sich zu „Veröffentlicht“.

Nächste Schritte

Weisen Sie der Ressourcenaktion ein Symbol zu. Siehe [Zuweisen eines Symbols zu einer XaaS-Ressourcenaktion](#). Mandantenadministratoren und Business-Gruppenmanager können dann die Aktion beim Erstellen einer Berechtigung verwenden.

Zuweisen eines Symbols zu einer XaaS-Ressourcenaktion

Nachdem Sie eine Ressourcenaktion erstellt und veröffentlicht haben, können Sie sie bearbeiten und der Aktion ein Symbol zuweisen.

Voraussetzungen

Melden Sie sich bei vRealize Automation als **XaaS-Architekt** an.

Verfahren

- 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**.

Ergebnisse

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 vRealize Automation als **XaaS-Architekt** an.
- Stellen Sie sicher, dass das Zuordnungs-Skript oder Zuordnungs-Workflow in vRealize Orchestrator ist. Siehe [Skriptaktionen und Workflows für Ressourcenzuordnungen](#).

Verfahren

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.

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-Objektyp 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
Alle folgenden Optionen	Wenn alle der definierten Klauseln erfüllt werden, stehen dem Benutzer die durch diese Ressourcenzuordnung erstellten Ressourcenaktionen zur Verfügung.
Eine der folgenden Optionen	Wenn eine der definierten Klauseln erfüllt wird, stehen dem Benutzer die durch diese Ressourcenzuordnung erstellten Ressourcenaktionen zur Verfügung.
Nicht die folgende	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 3-59. 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 Firewallinstellungen 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 3-60. Neue Felder im Ressourcenaktions- oder XaaS-Blueprint-Formular

Feld	Beschreibung
Textfeld	Einzeiliges Textfeld
Textbereich	Mehrzeiliges Textfeld
Link	Feld zur Eingabe einer URL durch Verbraucher. Sie können http, https, ftp, Mailto, oder / verwenden. Verwenden Sie nicht file://.
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

Tabelle 3-60. Neue Felder im Ressourcenaktions- oder XaaS-Blueprint-Formular (Fortsetzung)

Feld	Beschreibung
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 Ja oder Nein
Dropdown	Dropdown-Menü
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 enthaltenen Optionen außer Kraft.

Nach der Berechnung für ein Feld werden die Mindest- und Maximalbindungen nur neu berechnet, wenn ein Blueprint angefordert wird.

Für jede Option, die Sie auf ein Element anwenden, können Sie eines der folgenden Attribute zum Definieren der Option auswählen:

Nicht eingestellt

Ruft die Eigenschaft aus der vRealize Orchestrator-Workflow-Präsentation ab.

Konstante

Legt das Element, das Sie bearbeiten, auf „Erforderlich“ oder „Optional“ fest.

Feld

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.

Bedingt

Wendet eine Bedingung an. Verwenden Sie die Bedingungen, um verschiedene Klauseln und Ausdrücke zu erstellen und auf den Status oder die Optionen des Elements anzuwenden.

Extern

Wählen Sie eine vRealize Orchestrator-Skriptaktion aus, die den Wert definiert.

Tabelle 3-61. Optionen im Formulardesigner

Option	Beschreibung
Erforderlich	Gibt an, ob das Element erforderlich ist.
Nur Lesen	Gibt an, ob das Feld schreibgeschützt ist.
Wert	Legt einen Wert für das Element fest.
Sichtbar	<p>Gibt an, ob das Element für den Verbraucher sichtbar ist.</p> <p>Wenn Sie eine Sichtbarkeitsoption auf eine Anzeigegruppe im vRealize Orchestrator-Workflow anwenden, wird die Option im XaaS-Formular „Übermittelte Anforderungsdetails“ ignoriert, und die Felder, die Sie ausblenden möchten, werden im Formular angezeigt.</p> <p>Um Felder, die nicht im Formular „Übermittelte Anforderungsdetails“ angezeigt werden sollen, auszublenden, und wenn diese für den die Anforderung stellenden Benutzer nicht erforderlich sind, entfernen Sie die Felder aus dem Formular „Übermittelte Anforderungsdetails“ auf der Registerkarte „Blueprints-Formular“ im XaaS-Blueprint-Designer. Informationen dazu, wo sich diese Registerkarte befindet, finden Sie unter Hinzufügen eines neuen XaaS-Blueprint-Formulars.</p>
Mindestlänge	Legt eine Mindestanzahl an Zeichen für das Eingabeelement Zeichenfolge fest.
Maximallänge	Legt eine maximal zulässige Anzahl an Zeichen für das Eingabeelement Zeichenfolge fest.
Minimalwert	Legt einen Minimalwert für das Eingabeelement Zeichenfolge fest.
Maximalwert	Legt einen Maximalwert für das Eingabeelement Zahl fest.
Inkrement	Legt ein Inkrement für ein Element wie beispielsweise ein Feld vom Typ Dezimal oder Integer fest. Wenn beispielsweise ein Feld vom Typ Integer als Schieberegler dargestellt werden soll, können Sie den Wert dieses Schritts verwenden.

Tabelle 3-61. Optionen im Formulardesigner (Fortsetzung)

Option	Beschreibung
Mindestanzahl	Legt eine Mindestanzahl für die Auswahl von Elementen fest. Wenn Sie beispielsweise eine Kontrollkästchen-Liste hinzufügen oder bearbeiten, können Sie die Mindestanzahl von Kontrollkästchen festlegen, die der Verbraucher auswählen muss, um den Vorgang fortsetzen zu können.
Höchstanzahl	Legt eine Höchstanzahl für die Auswahl von Elementen fest. Wenn Sie beispielsweise eine Kontrollkästchen-Liste 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 3-62. 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.
Wert	Definiert einen statischen benutzerdefinierten Wert mit Bezeichnungen.
Externe Werte	Wählen Sie eine vRealize Orchestrator-Skriptaktion aus, die für den Wert Informationen definiert, 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.

Wenn Sie einen Blueprint mit einem Workflow erstellen, der ein obligatorisches Feld enthält, ist dieses im Anforderungsformular obligatorisch, selbst wenn Sie es auf nicht obligatorisch festlegen.

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.

Start Workflow : Create cluster

1 Common parameters

2 vCloud Distributed Storage

* Parent host folder
Not set

* Name of the new cluster

* Enable VMware HA
☐ Yes ☒ No

* Enable VMware DRS
☐ Yes ☒ No

Cancel Back Next Submit

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 vRealize Automation als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Hinzufügen einer benutzerdefinierten XaaS-Ressource.](#)

Verfahren

- 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 vRealize Automation als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Hinzufügen einer benutzerdefinierten XaaS-Ressource](#).

Verfahren

- 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**.

Ergebnisse

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 vRealize Automation als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Hinzufügen einer benutzerdefinierten XaaS-Ressource](#).

Verfahren

- 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 vRealize Automation als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Hinzufügen einer benutzerdefinierten XaaS-Ressource](#).

Verfahren

- 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 vRealize Automation als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Hinzufügen einer benutzerdefinierten XaaS-Ressource](#).
- Entwickeln oder importieren Sie eine vRealize Orchestrator-Skriptaktion zum Abrufen der Informationen, die Sie Verbrauchern bereitstellen möchten.

Verfahren

- 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**.

Ergebnisse

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 vRealize Automation als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Hinzufügen eines XaaS-Blueprints](#).

Verfahren

- 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
Details zu Katalogelementen	Die Seite „Details zu Katalogelementen“ wird Verbrauchern angezeigt, wenn sie auf ein Katalogelement klicken.
Anforderungsformular	Das standardmäßige XaaS-Blueprint-Formular. Die Verbraucher sehen das Anforderungsformular, wenn sie das Katalogelement anfordern.
Übermittelte Anforderungsdetails	Eine Anforderungsdetailsseite, die Verbrauchern angezeigt wird, wenn sie das Element anfordern und die Anforderungsdetails auf der Registerkarte Anforderung anzeigen möchten.

7 Klicken Sie auf **Übernehmen**.

Nächste Schritte

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 vRealize Automation als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Hinzufügen eines XaaS-Blueprints](#).

Verfahren

- 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
Nicht eingestellt	Ruft den Wert des Elements ab, das Sie in der vRealize Orchestrator-Workflow-Präsentation bearbeiten.
Konstante	Legt den Standardwert des Elements, das Sie bearbeiten, auf einen von Ihnen angegebenen Konstantenwert fest.

Option	Beschreibung
Feld	Bindet den Standardwert des Elements an einen Parameter eines anderen Elements aus der Repräsentation.
Bedingt	Wendet eine Bedingung an. Mithilfe von Bedingungen können Sie verschiedene Klauseln und Ausdrücke erstellen und auf ein Element anwenden.
Extern	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
Nicht eingestellt	Ruft den Wert des Elements ab, das Sie in der vRealize Orchestrator-Workflow-Präsentation bearbeiten.
Konstante	Legt den Standardwert des Elements, das Sie bearbeiten, auf einen von Ihnen angegebenen Konstantenwert fest.
Feld	Bindet den Standardwert des Elements an einen Parameter eines anderen Elements aus der Repräsentation.
Bedingt	Wendet eine Bedingung an. Mithilfe von Bedingungen können Sie verschiedene Klauseln und Ausdrücke erstellen und auf ein Element anwenden.
Extern	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
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. <ul style="list-style-type: none"> a Geben Sie in das Suchfeld Vordefinierte Werte einen Wert ein, um die vRealize Orchestrator-Bestandsliste zu durchsuchen. b Wählen Sie in den Suchergebnissen einen Wert aus und drücken Sie die Eingabetaste.

Option	Beschreibung
Wert	<p>Definieren Sie benutzerdefinierte Werte mit Bezeichnungen.</p> <ol style="list-style-type: none"> Geben Sie in das Textfeld Wert einen Wert ein. Geben Sie in das Textfeld Bezeichnung eine Bezeichnung für den Wert ein. Klicken Sie auf das Symbol Hinzufügen (+).
Externe Werte	<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"> ■ Wählen Sie Externen Wert hinzufügen aus. ■ Wählen Sie Ihre vRealize Orchestrator-Skriptaktion aus. ■ Klicken Sie auf Übernehmen.

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 vRealize Automation als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Hinzufügen eines XaaS-Blueprints](#).

Verfahren

- 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
Ergebnistyp	Wenn Sie ein Skript zum Definieren eines externen Werts für das Feld verwenden, geben Sie den Ergebnistyp Ihrer vRealize Orchestrator-Skriptaktion ein.
Eingabeparameter	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.
Ausgabeparameter	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**.

Nächste Schritte

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 vRealize Automation als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Hinzufügen eines XaaS-Blueprints](#).

Verfahren

- 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 vRealize Automation als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Hinzufügen eines XaaS-Blueprints](#).

Verfahren

- 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 vRealize Automation als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Erstellen einer Ressourcenaktion](#).

Verfahren

- 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
Aktionsformular	Das standardmäßige Ressourcenaktionsformular, das Verbrauchern angezeigt wird, wenn sie die Aktion nach der Bereitstellung ausführen möchten.
Übermittelte Aktionsdetails	Eine Anforderungsdetailsseite, die Verbrauchern angezeigt wird, wenn sie die Aktion anfordern und die Anforderungsdetails auf der Registerkarte Anforderung anzeigen möchten.

- 7 Klicken Sie auf **Übernehmen**.

Nächste Schritte

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 vRealize Automation als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Erstellen einer Ressourcenaktion](#).

Verfahren

- 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
Ergebnistyp	Wenn Sie ein Skript zum Definieren eines externen Werts für das Feld verwenden, geben Sie den Ergebnistyp Ihrer vRealize Orchestrator-Skriptaktion ein.
Eingabeparameter	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.
Ausgabeparameter	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**.

Nächste Schritte

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 vRealize Automation als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Erstellen einer Ressourcenaktion](#).

Verfahren

- 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
Nicht eingestellt	Ruft den Wert des Elements ab, das Sie in der vRealize Orchestrator-Workflow-Präsentation bearbeiten.
Konstante	Legt den Standardwert des Elements, das Sie bearbeiten, auf einen von Ihnen angegebenen Konstantenwert fest.
Feld	Bindet den Standardwert des Elements an einen Parameter eines anderen Elements aus der Repräsentation.
Bedingt	Wendet eine Bedingung an. Mithilfe von Bedingungen können Sie verschiedene Klauseln und Ausdrücke erstellen und auf ein Element anwenden.
Extern	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
Nicht eingestellt	Ruft den Wert des Elements ab, das Sie in der vRealize Orchestrator-Workflow-Präsentation bearbeiten.
Konstante	Legt den Standardwert des Elements, das Sie bearbeiten, auf einen von Ihnen angegebenen Konstantenwert fest.
Feld	Bindet den Standardwert des Elements an einen Parameter eines anderen Elements aus der Repräsentation.
Bedingt	Wendet eine Bedingung an. Mithilfe von Bedingungen können Sie verschiedene Klauseln und Ausdrücke erstellen und auf ein Element anwenden.
Extern	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
Nicht eingestellt	Ruft den Wert des Elements ab, das Sie in der vRealize Orchestrator-Workflow-Präsentation bearbeiten.
Vordefinierte Werte	<p>Wählen Sie in der vRealize Orchestrator-Bestandsliste Werte aus einer Liste mit verwandten Objekten aus.</p> <ol style="list-style-type: none"> Geben Sie in das Suchfeld Vordefinierte Werte einen Wert ein, um die vRealize Orchestrator-Bestandsliste zu durchsuchen. Wählen Sie in den Suchergebnissen einen Wert aus und drücken Sie die Eingabetaste.
Wert	<p>Definieren Sie benutzerdefinierte Werte mit Bezeichnungen.</p> <ol style="list-style-type: none"> Geben Sie in das Textfeld Wert einen Wert ein. Geben Sie in das Textfeld Bezeichnung eine Bezeichnung für den Wert ein. Klicken Sie auf das Symbol Hinzufügen (+).
Externe Werte	<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"> ■ Wählen Sie Externen Wert hinzufügen aus. ■ Wählen Sie Ihre vRealize Orchestrator-Skriptaktion aus. ■ Klicken Sie auf Übernehmen.

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 vRealize Automation als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Erstellen einer Ressourcenaktion](#).

Verfahren

- 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 **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**.

Hinzufügen eines Textelements zu einem Ressourcenaktionsformular

Sie können ein Textfeld einfügen, um dem Formular beschreibenden Text hinzuzufügen.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Mandantenadministrator** oder **XaaS-Architekt** an.
- [Erstellen einer Ressourcenaktion](#).

Verfahren

- 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 zudem einen neuen Vorgang nach der Bereitstellung zuordnen. Beispielsweise einen Vorgang, damit die Servicekatalog-Benutzer ihre Kennwörter ändern können.

Als XaaS-Architekt erstellen Sie eine 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.

Verfahren

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

Sie erstellen den XaaS-Blueprint „Benutzer in einer Gruppe erstellen“, sodass Sie den Workflow ausführen können, der einen Active Directory-Benutzer hinzufügt und diesen Benutzer einer Active Directory-Gruppe zuweist. Sie können den Blueprint als eigenständigen XaaS-Blueprint oder als eine Blueprintkomponente erstellen. In diesem Szenario erstellen Sie einen eigenständigen Blueprint.

3 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.

4 Erstellen eines Diensts und Hinzufügen eines Blueprints „Erstellen eines Testbenutzers“ zum Dienst

Sie können einen Dienst erstellen, um im Servicekatalog ein Katalogelement des Typs „Erstellen eines Benutzers“ anzuzeigen.

5 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. Nach Erhalt der Berechtigung können sie den Dienst in ihrem Katalog sehen und das im Dienst enthaltene Katalogelement „Erstellen eines Testbenutzers“ anfordern. 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 vRealize Automation als **XaaS-Architekt** an.

Verfahren

1 Wählen Sie **Design > XaaS > Benutzerdefinierte Ressourcen** aus.

2 Klicken Sie auf das Symbol **Neu** (+).

- 3 Geben Sie im Textfeld **Orchestrator-TypAD:Benutzer** ein und drücken Sie 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 Übernehmen Sie die Standardwerte.
- 9 Klicken Sie auf **Fertig stellen**.

Ergebnisse

Sie haben die benutzerdefinierte Testressource erstellt, die auf der Seite „Benutzerdefinierte Ressourcen“ aufgeführt wird.

Nächste Schritte

Erstellen Sie einen XaaS-Blueprint.

Erstellen eines XaaS-Blueprints zum Erstellen eines Benutzers

Sie erstellen den XaaS-Blueprint „Benutzer in einer Gruppe erstellen“, sodass Sie den Workflow ausführen können, der einen Active Directory-Benutzer hinzufügt und diesen Benutzer einer Active Directory-Gruppe zuweist. Sie können den Blueprint als eigenständigen XaaS-Blueprint oder als eine Blueprintkomponente erstellen. In diesem Szenario erstellen Sie einen eigenständigen Blueprint.

Voraussetzungen

- Stellen Sie sicher, dass Sie eine benutzerdefinierte Ressourcenaktion erstellen, die das Bereitstellen von Active Directory-Benutzern unterstützt. Siehe [Erstellen eines Testbenutzers als benutzerdefinierte Ressource](#).
- Melden Sie sich bei vRealize Automation als **XaaS-Architekt** an.

Verfahren

- 1 Wählen Sie **Design > XaaS > XaaS-Blueprints** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Navigieren Sie im Fenster „Einen Workflow auswählen“ zu **Orchestrator > Bibliothek > Microsoft > Active Directory > Benutzer** und wählen Sie den Workflow **Benutzer in einer Gruppe erstellen** aus.
- 4 Klicken Sie auf **Weiter**.

5 Konfigurieren Sie die Optionen der Registerkarte Allgemein.

- a Ändern Sie den Namen des Blueprints in **Testbenutzer erstellen** und übernehmen Sie die Beschreibung.
- b Heben Sie die Auswahl des Kontrollkästchens **Als Komponente auf der Design-Arbeitsfläche verfügbar machen** auf.

Sie veröffentlichen diesen Blueprint direkt im Servicekatalog, anstatt ihn als eine Blueprintkomponente auf der Design-Arbeitsfläche zu verwenden. Sie müssen keine Workflows für das vertikale oder horizontale Skalierung konfigurieren.

Die Registerkarte **Komponentenlebenszyklus** wird aus der Benutzeroberfläche entfernt.

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.
- d Klicken Sie auf den Dropdown-Pfeil **Sichtbar**, wählen Sie im Dropdown-Menü **Konstante** aus und wählen Sie 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 Weiter.****11 Klicken Sie auf Fertig stellen.****12 Wählen Sie auf der Seite XaaS-Blueprints die Zeile Testbenutzer erstellen aus und klicken Sie auf Veröffentlichen.****Ergebnisse**

Sie haben einen Blueprint zum Erstellen eines Testbenutzers erstellt und Sie haben den Blueprint verfügbar gemacht, damit er zu einem Dienst hinzugefügt werden kann.

Nächste Schritte

Erstellen Sie eine Aktion, die für das bereitgestellte Benutzerkonto ausgeführt wird. Siehe [Erstellen einer Ressourcenaktion zum Ändern eines Benutzerkennworts](#).

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 vRealize Automation als **XaaS-Architekt** an.
- Stellen Sie sicher, dass Sie eine benutzerdefinierte Ressourcenaktion erstellen, die das Bereitstellen von Active Directory-Benutzern unterstützt. Siehe [Erstellen eines Testbenutzers als benutzerdefinierte Ressource](#).

Verfahren

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 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.
Diese Auswahl ist die benutzerdefinierte Ressource, die Sie vorher 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 **Fertig stellen**.
- 12 Wählen Sie auf der Seite „Ressourcenaktionen“ die Zeile **Kennwort des Testbenutzers ändern** aus und klicken Sie auf **Veröffentlichen**.

Ergebnisse

Sie haben eine Ressourcenaktion erstellt, um das Kennwort eines Benutzers zu ändern, und Sie haben sie für das Hinzufügen zu einer Berechtigung bereitgestellt.

Nächste Schritte

Fügen Sie den Blueprint „Erstellen eines Testbenutzers“ zu einem Dienst hinzu. Siehe [Erstellen eines Diensts und Hinzufügen eines Blueprints „Erstellen eines Testbenutzers“ zum Dienst](#).

Erstellen eines Diensts und Hinzufügen eines Blueprints „Erstellen eines Testbenutzers“ zum Dienst

Sie können einen Dienst erstellen, um im Servicekatalog ein Katalogelement des Typs „Erstellen eines Benutzers“ anzuzeigen.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Mandantenadministrator** oder **Katalogadministrator** an.
- Stellen Sie sicher, dass Sie einen XaaS-Blueprint erstellt haben. Siehe [Erstellen eines XaaS-Blueprints zum Erstellen eines Benutzers](#).

Melden Sie sich bei vRealize Automation als **Mandantenadministrator** oder **Katalogadministrator** an.

Verfahren

- 1 Wählen Sie **Administration > Katalogmanagement > Services** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Geben Sie **Active Directory-Testbenutzer** als Namen des Diensts an.
- 4 Wählen Sie aus dem Dropdown-Menü **Status** den Eintrag **Aktiv** aus.
- 5 Lassen Sie die anderen Textfelder leer.
- 6 Klicken Sie auf **OK**.
- 7 Wählen Sie in der Liste „Dienste“ die Zeile **Active Directory-Testbenutzer** aus und klicken Sie auf **Katalogelemente verwalten**.
- 8 Klicken Sie auf das Symbol **Neu** (+).
- 9 Wählen Sie **Erstellen eines Testbenutzers** aus und klicken Sie auf **OK**.
Der XaaS-Blueprint „Erstellen eines Testbenutzers“ wird in die Liste der Katalogelemente aufgenommen.
- 10 Klicken Sie auf **Schließen**.

Ergebnisse

Der Dienst „Active Directory-Testbenutzer“ enthält jetzt den Blueprint „Erstellen eines Testbenutzers“. Sie brauchen keine Aktionen zu diesen Diensten hinzuzufügen.

Nächste Schritte

Sie können Benutzern die Berechtigung erteilen, den Blueprint anzufordern und anschließend die Aktion auszuführen. Siehe [Erteilen der Berechtigung für den Dienst und die Ressourcenaktion an einen Verbraucher](#).

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. Nach Erhalt der Berechtigung können sie den Dienst in ihrem Katalog sehen und das im Dienst enthaltene Katalogelement „Erstellen eines Testbenutzers“ anfordern. Nachdem die Verbraucher das Element bereitgestellt haben, können sie die Änderung des Benutzerkennworts anfordern.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Mandantenadministrator** oder **Business-Gruppenmanager** an.
- Stellen Sie sicher, dass der Blueprint „Erstellen eines Testbenutzers“ zum Dienst hinzugefügt wurde. Siehe [Erstellen eines Diensts und Hinzufügen eines Blueprints „Erstellen eines Testbenutzers“ zum Dienst](#).
- Stellen Sie sicher, dass die Ressourcenaktion „Benutzerkennwort ändern“ vorhanden ist. Siehe [Erstellen einer Ressourcenaktion zum Ändern eines Benutzerkennworts](#).

Verfahren

- 1 Wählen Sie **Administration > Katalogmanagement > Berechtigungen** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Geben Sie **Erstellen eines Active Directory–Benutzers** im 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.
Z. B. IT-Kundenberater.
- 7 Wählen Sie **Benutzer und Gruppen** aus, um allen Mitgliedern der Business-Gruppe, z. B. Kundenberatern, zu erlauben, ein Benutzerkonto zu erstellen.

Die Benutzer, die Sie auswählen, können im Katalog den Dienst und die im Dienst enthaltenen Katalogelemente ansehen. Sie können nach dessen Erstellung die Kennwortänderungsaktion für das Benutzerkonto ausführen.
- 8 Klicken Sie auf **Weiter**.
- 9 Geben Sie im Textfeld **Berechtigte Services** **Active Directory–Testbenutzer** ein und drücken Sie die Eingabetaste.
- 10 Geben Sie im Textfeld **Berechtigte Aktionen** **Ändern des Kennworts des Test–Benutzers** ein und drücken Sie die Eingabetaste.
- 11 Klicken Sie auf **Fertig stellen**.

Ergebnisse

Sie haben eine aktive Berechtigung erstellt, damit Benutzer, die Mitglieder der Business-Gruppe „IT-Kundenberater“ sind, Benutzer erstellen können. Sobald der Benutzer bereitgestellt wurde, kann er für das bereitgestellte Benutzerkonto die Ressourcenaktion „Benutzerkennwort ändern“ ausführen.

Nächste Schritte

Melden Sie sich als Benutzer an, der berechtigt ist, einen Active Directory-Benutzer zu erstellen. Stellen Sie auf der Registerkarte **Katalog** sicher, dass der XaaS-Blueprint den Benutzer wie erwartet erstellt. Sobald der Benutzer erstellt wurde, führen Sie von der Registerkarte **Elemente** aus die Aktion „Benutzerkennwort ändern“ aus.

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 vRealize Automation als **XaaS-Architekt** an.

Verfahren

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.

Verfahren

- 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**.

Ergebnisse

Sie haben eine Ressourcenaktion erstellt, um eine virtuelle Maschine zu migrieren, und die Ressourcenaktion wird auf der Seite „Ressourcenaktionen“ aufgeführt.

Nächste Schritte

[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.

Verfahren

- 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**.

Ergebnisse

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 XaaS-Ressourcenaktion](#).

Nächste Schritte

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 vRealize Automation als **XaaS-Architekt** an.

Verfahren

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 erfolgreicher 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 erfolgreicher 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 erfolgreicher 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.

Verfahren

- 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**.

Nächste Schritte

[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 erfolgreicher Bereitstellung ausführen.

Verfahren


- 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**.

Ergebnisse

Sie haben die Workflow-Präsentation des Workflows „Virtuelle Maschine mit vMotion migrieren“ bearbeitet.


Nächste Schritte


[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.

Verfahren

- 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**.

Ergebnisse

Sie haben eine Ressourcenaktion erstellt, um eine virtuelle Maschine mit vMotion zu migrieren, und die Ressourcenaktion wird auf der Seite „Ressourcenaktionen“ aufgeführt.

Nächste Schritte

[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.

Verfahren

- 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**.

Ergebnisse

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 XaaS-Ressourcenaktion](#).

Darüber hinaus haben Sie die Präsentation des Workflows bearbeitet und das Erscheinungsbild der Aktion definiert.

Nächste Schritte

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 vRealize Automation als **XaaS-Architekt** an.

Verfahren

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 erfolgreicher 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.

Verfahren

- 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**.

Ergebnisse

Sie haben eine Ressourcenaktion erstellt, um einen Snapshot einer virtuellen Maschine zu erstellen, und die Ressourcenaktion wird auf der Seite „Ressourcenaktionen“ aufgeführt.

Nächste Schritte

[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.

Verfahren

- 1 Wählen Sie **Design > XaaS > Ressourcenaktionen** aus.
- 2 Wählen Sie die Zeile der Aktion „Snapshot erstellen“ aus und klicken Sie auf die Schaltfläche **Veröffentlichen**.

Ergebnisse

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 XaaS-Ressourcenaktion](#).

Nächste Schritte

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.

Verfahren

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 vRealize Automation als **XaaS-Architekt** an.
- Erstellen oder importieren Sie einen Workflow oder eine Skriptaktion für die vRealize Orchestrator-Ressourcenzuordnung.

Verfahren

- 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**.

Ergebnisse

Mithilfe Ihrer Amazon-Ressourcenzuordnung können Sie Ressourcenaktionen für mithilfe von IaaS bereitgestellte Amazon-Maschinen erstellen.

Nächste Schritte

[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 vRealize Automation als **XaaS-Architekt** an.

Verfahren

- 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**.

Ergebnisse

Sie haben eine Ressourcenaktion erstellt, um virtuelle Amazon-Maschinen zu starten, und die Ressourcenaktion wird auf der Seite „Ressourcenaktionen“ aufgeführt.

Nächste Schritte

[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 vRealize Automation als **XaaS-Architekt** an.

Verfahren

- 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**.

Ergebnisse

Der Status der Ressourcenaktion zum Starten von Instanzen ändert sich zu „Veröffentlicht“.

Nächste Schritte

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 Stellen Sie sicher, 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 bei vRealize Automation als **Infrastrukturarchitekt** an.
- Erstellen Sie einen Blueprint. Siehe *Checkliste für das Erstellen von vRealize Automation-Blueprints*.

Verfahren

- 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**.

Ergebnisse

Der Blueprint wird als Katalogelement veröffentlicht. Sie müssen ihm jedoch zuerst eine Berechtigung erteilen, damit er Benutzern im Servicekatalog zur Verfügung steht.

Nächste Schritte

Fügen Sie den Blueprint dem Katalogdienst hinzu und erteilen Sie Benutzern die Berechtigung, das Katalogelement für die Maschinenbereitstellung anzufordern, wie im Blueprint definiert.

Arbeiten mit von Entwicklern gesteuerten Blueprints

Zusätzlich zur Methode zum Erstellen von vRealize Automation-Blueprints über die Benutzeroberfläche können Sie auch programmgesteuert mithilfe von Tools wie vRealize CloudClient, mit eigenständigen bereitgestellten oder auf andere Weise bezogenen Blueprints und in Abstimmung mit anderen Entwicklern anhand von vRealize Suite-Anwendungen und -Workflows und Drittanbieter-Tools arbeiten.

Informationen zu diesen Methoden finden Sie in den folgenden Themen:

- [Exportieren und Importieren von Blueprints und Inhalten](#)
- [Herunterladen und Konfigurieren des bereitgestellten eigenständigen Blueprints](#)
- [Erstellen von Blueprints und anderem IaaS-Inhalt in einer Umgebung mit mehreren Entwicklern](#)

Exportieren und Importieren von Blueprints und Inhalten

Mithilfe der vRealize Automation-REST-API oder dem vRealize CloudClient können Sie Blueprints und 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-Inhaltselemente können Sie programmgesteuert importieren und exportieren:

- Anwendungs-Blueprints und alle zugehörigen Komponenten
- IaaS-Maschinen-Blueprints
- Software-Komponenten
- XaaS-Blueprints
- Komponentenprofile
- 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 3-63. Auswählen Ihres Import- und Exporttools

Tool	Weitere Informationen
vRealize CloudClient	Auf der vRealize CloudClient-Seite der VMware-Site code.vmware.com unter https://developercenter.vmware.com/tool/cloudclient .
vRealize Automation-REST-API	In der API-Dokumentation im VMware-API-Explorer für vRealize Automation unter https://code.vmware.com/apis/vrealize-automation .

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 IPAM-Drittanbieters](#).

- 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

Verfahren

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.

Ergebnisse

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.

Verfahren

- 1 Melden Sie sich bei der vRealize Automation-Appliance als Root-Benutzer 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 vRealize CloudClient von <http://developercenter.vmware.com/tool/cloudclient> in das Verzeichnis /tmp herunter.
- 4 Dekomprimieren Sie das Paket cloudclient-4x-dist.zip.
- 5 Führen Sie vRealize CloudClient unter dem Verzeichnis /bin aus.

```
$>./bin/cloudclient.sh
```

- 6 Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung.
- 7 Verwenden Sie vRealize CloudClient, um sich bei der vRealize Automation-Appliance als Benutzer mit den Berechtigungen **Softwarearchitekt** und **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
```

Beachten Sie, dass für den Eintrag ÜBERSCHREIBEN die Groß-/Kleinschreibung beachtet und der Eintrag in Großbuchstaben geschrieben werden muss.

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
```

Beachten Sie, dass für den Eintrag ÜBERSCHREIBEN die Groß-/Kleinschreibung beachtet und der Eintrag in Großbuchstaben geschrieben werden muss.

Ergebnisse

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.

Verfahren

- 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**.

Ergebnisse

Sie haben den Dukes Bank-Beispielanwendungs-Blueprint für Ihre Umgebung konfiguriert und den fertiggestellten Blueprint veröffentlicht.

Nächste Schritte

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.

Verfahren

- 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 Lastausgleichsdienstservers, 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-Lastausgleichsdienstserver 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.

Ergebnisse

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.

Herunterladen und Konfigurieren des bereitgestellten eigenständigen Blueprints

Sie können einen bereitgestellten eigenständigen Blueprint und dessen zugehörige Softwarekomponenten von der vRealize Automation-Appliance herunterladen.

Das Dokument [Herunterladen und Konfigurieren des eigenständigen vRealize Automation-Blueprints](#) führt Sie durch den Prozess zum Herunterladen eines eigenständigen vRealize Automation-Blueprints von der vRealize Automation-Appliance. Außerdem wird beschrieben, wie Sie diesen Blueprint anschließend in vRealize Automation importieren, konfigurieren und zusammen mit verschiedenen vRealize Orchestrator-Workflows verwenden.

Erstellen von Blueprints und anderem IaaS-Inhalt in einer Umgebung mit mehreren Entwicklern

Mehrere Entwickler können vRealize Orchestrator-Workflows in Verbindung mit vRealize Automation und Entwicklertools von Drittanbietern verwenden, um gleichzeitig an verschiedenen

vRealize Automation-Blueprint-Artefakten für dieselben oder unterschiedliche vRealize Suite-Blueprints zu arbeiten.

Sie können Tools wie vRealize Suite Lifecycle Manager verwenden, um eine Umgebung mit mehreren Entwicklern für vRealize Automation und andere vRealize Suite-Tools und -OVAs zu vereinfachen. Zu diesen Tools zählen auch Drittanbietertools wie GitLab/GitHub, Houdini und andere Anwendungs-Artefakte von [VMware Solutions Exchange](#).

Mithilfe der folgenden Ressourcen erfahren Sie mehr über das Erstellen von vRealize Automation-Blueprints und weiteren IaaS-Inhalten, wie z. B. Eigenschaften, Ereignisbroker-Abonnements, Softwarekomponenten und vRealize Orchestrator-Workflows in einer Umgebung mit mehreren Entwicklern:

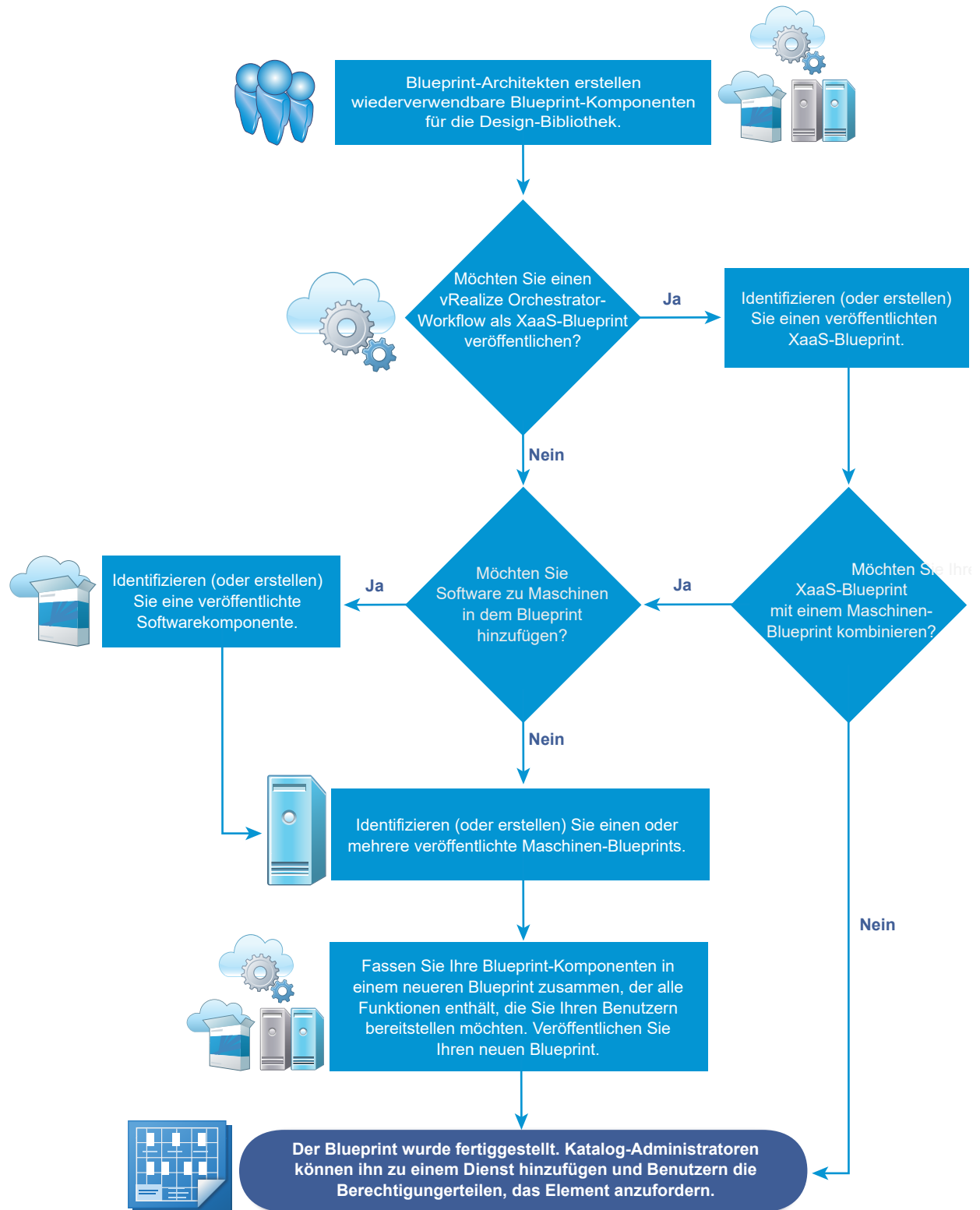
- [Video – Neuheiten in Lifecycle Manager](#)
- [Blogbeitrag – vRealize Automation mit Infrastruktur-Blueprint – Konfigurieren einer Umgebung für mehrere Entwickler](#)
- Dokumentation – [Herunterladen und Konfigurieren des bereitgestellten eigenständigen Blueprints](#)
- [Blogbeitrag – Lifecycle Manager mit GitLab-Integration](#)
- [Blogbeitrag – Übersicht über LifeCycle Manager](#)

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.

Wenn die Komponenten-Blueprints benutzerdefinierte Formulare haben, werden die benutzerdefinierte Anforderungsformulare nicht auf den neuen Blueprint angewendet. Sie müssen neue Formulare für den neuen Blueprint erstellen. Weitere Informationen zu benutzerdefinierten Anforderungsformularen finden Sie unter [Anpassen von Blueprint-Anforderungsformularen](#).

Abbildung 3-5. 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.

- **Verwenden von Maschinenkomponenten und Software-Komponenten beim Zusammenfügen von Blueprints**

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 von 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 abhängige Aktualisierungen aus. Softwarekomponenten müssen in einem Blueprint sortiert werden.

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 über die Berechtigung verfügt, auf den äußeren Blueprint zuzugreifen, ist er auch berechtigt, auf dessen verschachtelte Blueprints zuzugreifen.
- 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 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 den äußeren Blueprints angezeigt, außer Sie haben diese Einstellungen im äußeren Blueprint überschrieben.
- Beschränken Sie die maximale Leasedauer des äußeren Blueprints auf die niedrigste maximale Leasedauer eines Komponenten-Blueprints.

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.
- Wenn Sie einen Blueprint öffnen, in dem eine Maschinenkomponente oder ein verschachtelter Blueprint entfernt oder seine ID geändert wurde und die Maschinenkomponente mit Komponenten im aktuellen Blueprint verknüpft war, werden die verknüpften Komponenten entfernt und die folgende bzw. eine ähnliche Meldung wird angezeigt:

Eine Maschinenkomponente in einem verschachtelten Blueprint, auf die von Komponenten im aktuellen Blueprint verwiesen wird, wurde entfernt oder seine Maschinenkomponenten-ID wurde geändert. Alle Komponenten im aktuellen Blueprint, die mit der fehlenden bzw. geänderten Maschinenkomponenten-ID verknüpft waren, wurden entfernt. Klicken Sie auf „Abbrechen“, um die Verknüpfungshistorie zwischen der fehlenden bzw. geänderten Maschinenkomponente-ID im verschachtelten Blueprint und Komponenten im aktuellen Blueprint beizubehalten und das Problem im verschachtelten Blueprint zu beheben. Öffnen Sie den verschachtelten Blueprint und fügen Sie die fehlende Maschinenkomponente mit der ursprünglichen ID neu hinzu, oder stellen Sie die ursprüngliche Maschinenkomponenten-ID wieder her. Klicken Sie auf „Speichern“, um die Verknüpfungshistorie zwischen der fehlenden bzw. geänderten Maschinenkomponenten-ID im verschachtelten Blueprint und den Komponenten im aktuellen Blueprint vollständig zu entfernen.

- Wenn Sie einen Blueprint veröffentlichen, werden die Daten der Softwarekomponenten wie ein Snapshot behandelt. Wenn Sie später Änderungen an den Eigenschaften der Softwarekomponente vornehmen, werden nur neue Eigenschaften durch den Blueprint erkannt, in dem die Softwarekomponente enthalten ist. Updates an den Eigenschaften, die zum Zeitpunkt der Veröffentlichung des Blueprints in der Softwarekomponente vorhanden waren, werden im Blueprint nicht aktualisiert. Nur Eigenschaften, die nach der Veröffentlichung des Blueprints hinzugefügt wurden, werden vom Blueprint geerbt. Allerdings können Sie Änderungen an Instanzen der Softwarekomponente in Blueprints vornehmen, in denen die Softwarekomponente gespeichert ist, um diesen bestimmten Blueprint zu ändern.

Regeln und Überlegungen für das Verschachteln von Blueprints im Zusammenhang mit Netzwerken und der Sicherheit

- Netzwerk- und Sicherheitskomponenten in äußeren Blueprints können Maschinen zugeordnet werden, die in verschachtelten Blueprints definiert sind.
- Netzwerk-, Sicherheits- und Lastausgleichsdienst-Komponenten von NSX und deren Einstellungen werden in verschachtelten Blueprints nicht unterstützt.
- 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 Transportzoneneinstellungen, 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.
- Die Komponenteneinstellungen können sich abhängig davon ändern, in welchem Blueprint sich die Komponente befindet. Wenn Sie z. B. Sicherheitsgruppen, Sicherheits-Tags oder On-Demand-Netzwerke sowohl auf der Ebene des inneren als auch auf der Ebene des äußeren Blueprints einschließen, setzen die Einstellungen des äußeren Blueprints diejenigen des inneren Blueprints außer Kraft. Netzwerk- und Sicherheitskomponenten werden nur auf der Ebene des äußeren Blueprints unterstützt, außer im Fall von vorhandenen Netzwerken, die auf Ebene des inneren Blueprints funktionieren. Um Fehler zu vermeiden, fügen Sie alle Sicherheitsgruppen, Sicherheits-Tags und bedarfsgesteuerten Netzwerke nur zum äußeren Blueprint hinzu.

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 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.

Verwenden von Maschinenkomponenten und Software-Komponenten beim Zusammenfügen von Blueprints

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 IPv6 (Internet Protocol Version 6) nicht unterstützen, verwenden Sie IPv4-Einstellungen.

Hinweis Softwarekomponenten müssen eine geordnete Abhängigkeit im Blueprint aufweisen. Ungeordnete Softwarekomponenten können dazu führen, dass dieas Blueprint-ProvisioningBereitstellung fehlschlägt. Besteht keine tatsächliche Reihenfolgeabhängigkeit für die Softwarekomponenten, können Sie die Anforderung der Blueprint-Anordnung durch Hinzufügen einer Pseudoabhängigkeit zwischen den Softwarekomponenten erfüllen.

Wenn Sie Blueprints als skalierbar konfigurieren, empfiehlt es sich, Einzel-Layer-Blueprints zu erstellen, die andere Blueprints nicht wiederverwenden. In der Regel werden die während der Skalierung verwendeten Update-Vorgänge durch implizite Abhängigkeiten ausgelöst, zum Beispiel durch Eigenschaftsbindungen. 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.

Um Softwarekomponenten erfolgreich zur Design-Arbeitsfläche hinzuzufügen, müssen Sie Zugriff als Business-Gruppenmitglied, Business-Gruppenmanager oder Mandantenadministrator auf den Zielkatalog haben.

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.

Hinweis Wenn Sie einen Blueprint veröffentlichen, werden die Daten der Softwarekomponenten wie ein Snapshot behandelt. Wenn Sie später Änderungen an den Eigenschaften der Softwarekomponente vornehmen, werden nur neue Eigenschaften durch den Blueprint erkannt, in dem die Softwarekomponente enthalten ist. Updates an den Eigenschaften, die zum Zeitpunkt der Veröffentlichung des Blueprints in der Softwarekomponente vorhanden waren, werden im Blueprint nicht aktualisiert. Nur Eigenschaften, die nach der Veröffentlichung des Blueprints hinzugefügt wurden, werden vom Blueprint geerbt. Allerdings können Sie Änderungen an Instanzen der Softwarekomponente in Blueprints vornehmen, in denen die Softwarekomponente gespeichert ist, um diesen bestimmten Blueprint zu ändern.

Tabelle 3-64. 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

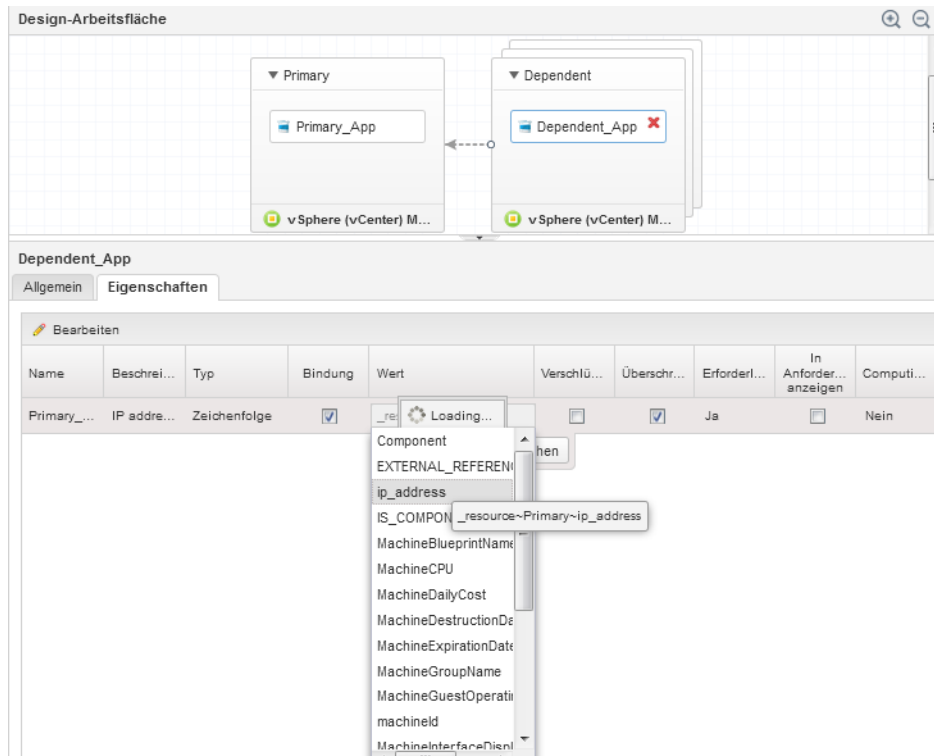
Bei verschiedenen Bereitstellungsszenarien ist für eine Komponente der Eigenschaftswert einer anderen Komponente erforderlich, damit sie selbst angepasst werden kann. Sie können Eigenschaften von XaaS, Maschinen und Software sowie benutzerdefinierte Eigenschaften in einem Blueprint an andere Eigenschaften 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-Schriftzeichen (~) 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 3-6. Binden einer Softwareeigenschaft an die IP-Adresse einer Maschine



Erstellen von Abhängigkeiten und Steuern der Bereitstellungsreihenfolge

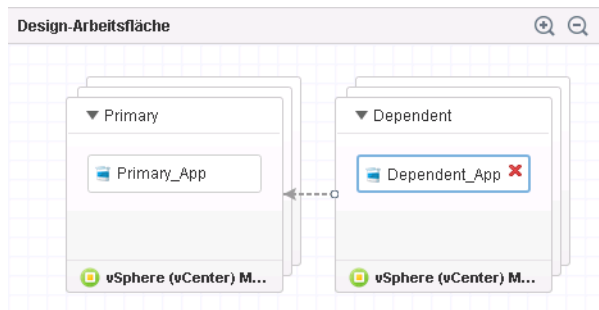
Wenn Sie Informationen für eine Ihrer Blueprint-Komponenten benötigen, um die Bereitstellung einer anderen Komponente abzuschließen, können Sie auf der Design-Arbeitsfläche eine explizite Abhängigkeit erstellen. Auf diese Weise können Sie die Bereitstellung staffeln, damit die abhängige Komponente nicht vorzeitig bereitgestellt wird. Explizite Abhängigkeiten steuern die Bereitstellungsreihenfolge und lösen während eines vertikalen oder horizontalen Skalierungsvorgangs abhängige Aktualisierungen aus. Softwarekomponenten müssen in einem Blueprint sortiert werden.

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.

Hinweis Softwarekomponenten müssen eine geordnete Abhängigkeit im Blueprint aufweisen. Ungeordnete Softwarekomponenten können dazu führen, dass die Blueprint-Bereitstellung fehlschlägt. Besteht keine tatsächliche Reihenfolgeabhängigkeit für die Softwarekomponenten, können Sie die Anforderung der Blueprint-Anordnung durch Hinzufügen einer Pseudoabhängigkeit zwischen den Softwarekomponenten erfüllen.

Um eine Abhängigkeit auf der Design-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 3-7. 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.

Anpassen von Blueprint-Anforderungsformularen

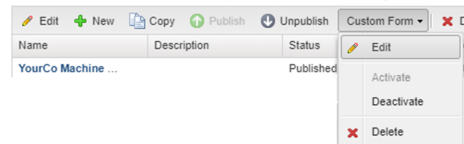
Jeder Blueprint, den Sie erstellen und veröffentlichen, zeigt ein Formular an, wenn Benutzer den Blueprint im Katalog anfordern. Sie können das Standardformular verwenden oder Blueprint-Anforderungsformulare anpassen, wenn Sie einen Blueprint erstellen oder bearbeiten. Sie passen ein Formular an, wenn die auf dem Standardformular angegebenen oder erforderlichen Informationen nicht diejenigen sind, die Sie Benutzern anzeigen möchten.

Anpassen von Anforderungsformularen

Sie greifen aus dem Blueprint-Datenraster oder der Blueprint-Arbeitsfläche auf den Designer für benutzerdefinierte Anforderungsformulare zu.

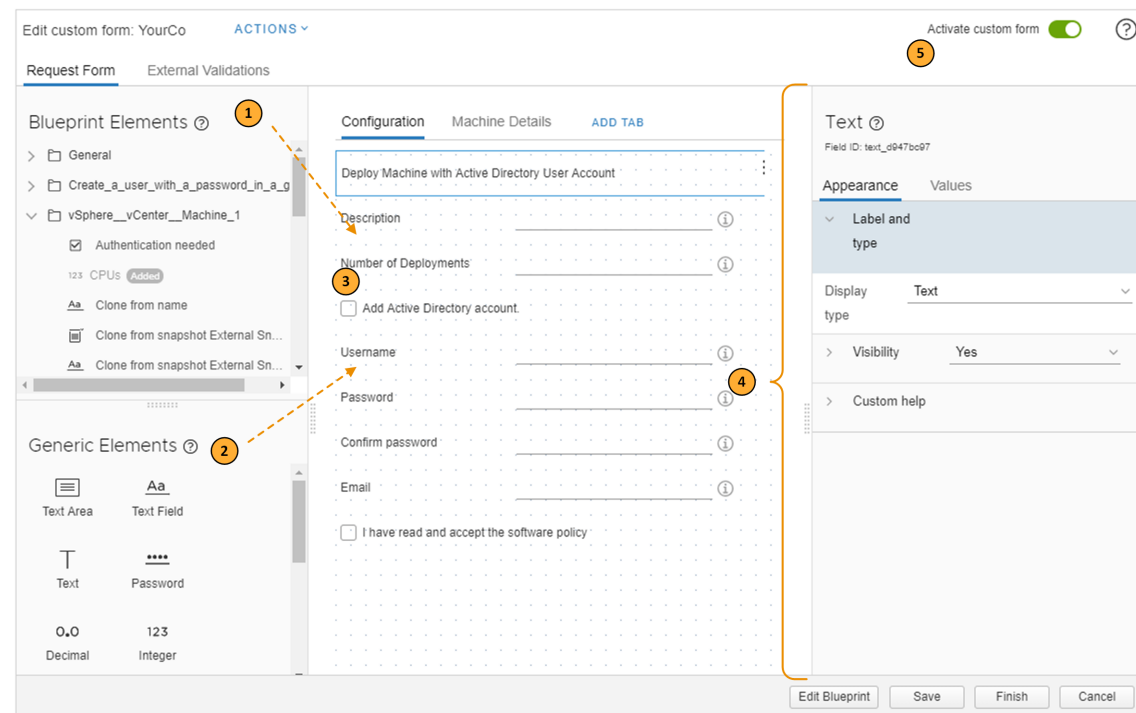
Blueprints

Create and manage blueprints. Publish a blueprint to allow architects to reuse your blue administrators to entitle users to request your blueprint from the catalog.



Designer für benutzerdefinierte Anforderungsformulare

Sie verwenden den Formulardesigner, um Ihr eigenes benutzerdefiniertes Formular zu erstellen.



So erstellen Sie ein benutzerdefiniertes Formular:

- 1 Ziehen Sie Elemente (1 und 2) auf die Design-Arbeitsfläche (3).
- 2 Konfigurieren Sie jedes Element über den Bereich „Eigenschaften“ (4).

3 Aktivieren Sie das Formular (5).

Der Formulardesigner für benutzerdefinierte Formulare unterstützt die Datenvalidierung durch Hinzufügen von Einschränkungen zu einem Feld oder mithilfe einer externen Validierungsquelle. Informationen zu Einschränkungsoptionen, die bei der Erstellung ein Formulars angewendet werden, finden Sie unter [Benutzerdefinierte Formulardesigner-Feldeigenschaften](#). Ein Beispiel für eine Einschränkung finden Sie unter [Erstellen eines benutzerdefinierten Anforderungsformulars mit Active Directory-Optionen](#). Informationen zur externen Validierung finden Sie unter [Verwenden der externen Validierung im Designer für benutzerdefinierte Formulare](#).

Die Liste der Blueprint-Elemente enthält benutzerdefinierte Eigenschaften, es sei denn, eine Eigenschaft ist so konfiguriert, dass sie nicht überschrieben werden kann. Wenn die Option „Überschreibbar“ für die Eigenschaft auf „Nein“ gesetzt ist, kann das Feld nicht angepasst werden.

Aktionen mit benutzerdefinierten Anforderungsformularen

Sie verwenden die Elemente im Aktionsmenü zum Auffüllen von Formularen und zur gemeinsamen Nutzung mit anderen Systemen.

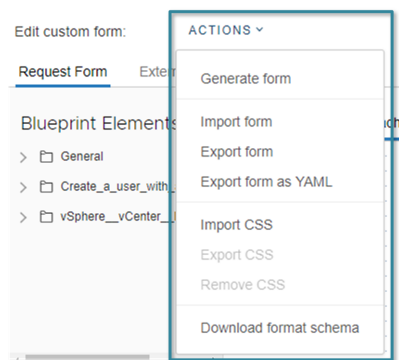


Tabelle 3-65. Elemente im Aktionsmenü für benutzerdefinierte Anforderungsformulare

Aktionsmenüelement	Beschreibung
Formular generieren	Fügt alle Felder, die mit den einzelnen Blueprint-Komponenten verknüpft sind, zum Formulardesigner hinzu. Jede Komponente wird einer Registerkarte hinzugefügt. Wenn Sie dieses Menüelement verwenden, nachdem Sie ein Formular erstellt oder geändert haben, überschreibt das generierte Formular Ihr aktuelles Formular. Wenn Sie dieses Menüelement verwenden, können Sie Felder, die Sie den Benutzern im Katalog nicht anzeigen möchten, ausblenden oder entfernen. Wenn Sie das Formular nicht generieren, können Sie dennoch Textfelder hinzufügen und konfigurieren, die den Benutzern angezeigt werden sollen.
Formular importieren.	Importiert eine JSON- oder YAML-Datei für ein benutzerdefiniertes Formular.

Tabelle 3-65. Elemente im Aktionsmenü für benutzerdefinierte Anforderungsformulare (Fortsetzung)

Aktionsmenüelement	Beschreibung
Formular exportieren	<p>Exportiert das aktuelle benutzerdefinierte Formular als JSON-Datei.</p> <p>Exportieren Sie die Datei, wenn Sie einen Teil davon verwenden möchten, der einer Komponente entspricht, die Sie in einem anderen Blueprint verwenden.</p>
Formular als YAML exportieren	<p>Exportiert das aktuelle benutzerdefinierte Formular als YAML.</p> <p>Exportieren Sie die Datei als YAML, wenn Sie ein benutzerdefiniertes Formular aus einer vRealize Automation-Instanz in eine andere verschieben möchten. Beispiel: Von Ihrer Testumgebung in Ihre Produktionsumgebung. Wenn Sie das Formular als YAML bearbeiten möchten, können Sie es exportieren, bearbeiten und dann wieder in den Blueprint importieren.</p>
CSS importieren	<p>Importiert eine CSS-Datei, die das Kataloganforderungsformular erweitert.</p> <p>Die Datei ähnlich möglicherweise dem folgenden Beispiel. In diesem Beispiel wird die Schriftgröße geändert und der Text fett formatiert. Das referenzierte Feld ist das Textfeld „Deploy Machine with Active Directory User Account“ (Maschine mit Active Directory-Benutzerkonto bereitstellen), das im Abschnitt oben zum Designer für benutzerdefinierte Anforderungsformulare in der Abbildung angezeigt wird.</p> <pre>#<field-ID> .grid-item { font-size: 16px; font-weight: bold; width: 600px; }</pre> <p>In diesem Beispiel ist <field-ID> die ID für das Feld auf der Arbeitsfläche. Um den Wert zu suchen, wählen Sie das Feld auf der Arbeitsfläche aus. Der Wert befindet sich im rechten Fensterbereich unterhalb des Namens. In der Abbildung oben lautet der Wert text_d947bc97.</p> <p>Um die Datei zu importieren, speichern Sie sie als <Dateiname>.css.</p>
CSS exportieren	Exportiert das importierte CSS.

Tabelle 3-65. Elemente im Aktionsmenü für benutzerdefinierte Anforderungsformulare (Fortsetzung)

Aktionsmenüelement	Beschreibung
CSS entfernen	Verwirft das benutzerdefinierte CSS. Das verworfene CSS kann nicht wiederhergestellt werden.
Formatschema herunterladen	Lädt eine JSON-Datei herunter, die die Struktur und Beschreibung der verwendeten Steuerelemente und Zustände in einem benutzerdefinierten Formular enthält. Sie können dieses Schema verwenden, um ein Formular zu erstellen oder ein vorhandenes Formular zu ändern. Sie können die geänderte JSON-Datei als das benutzerdefinierte Formular importieren.

Erstellen eines benutzerdefinierten Anforderungsformulars mit Active Directory-Optionen

Sie erstellen ein benutzerdefiniertes Formular, wenn das Standardformular dem anfordernden Benutzer zu viele oder zu wenige Informationen bereitstellt. Sie können weitere Felder zum Formular hinzufügen, Felder in einem Formular ausblenden oder Felder im Vorhinein ausfüllen und diese entweder ein- oder ausblenden.

Dieser Anwendungsfall basiert auf einem Blueprint, der einen virtuellen vSphere-Maschinentyp und einen XaaS-Blueprint beinhaltet, der ein Active Directory-Administratorkonto auf der virtuellen Maschine konfiguriert. Der XaaS-Blueprint basiert auf dem Workflow zum Erstellen eines Benutzers mit einem Kennwort in einer Gruppe.

Ihre Aufgaben in diesem Anwendungsfall:

- Ermöglichen Sie dem Benutzer, das Administratorkennwort zu konfigurieren.
- Konfigurieren Sie die Details der Maschine so, dass die CPU- und Arbeitsspeicherwerte beide auf GB basieren.

Wie profitieren Sie von diesem Anwendungsfall? Der Anwendungsfall enthält Beispiele für die folgenden Formularanpassungen:

- Fügen Sie bestimmte Felder zu einem leeren Formular hinzu.
- Konfigurieren Sie ein Kontrollkästchen zum Anzeigen bzw. Ausblenden.
- Blenden Sie Felder aus, bis der anfordernde Benutzer das Kontrollkästchen aktiviert.
- Fügen Sie eine Validierung zu Feldern hinzu.
- Zeigen Sie ein Arbeitsspeicherfeld in GB an, auch wenn das Feld „Blueprint“ in MB berechnet wird.
- Verwenden Sie reguläre Ausdrücke.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Anwendungsarchitekt**, **Softwarearchitekt** oder **Infrastrukturarchitekt** an.
- Erstellen Sie einen YourCo-Maschine- und -Benutzer-Blueprint, der einen vSphere-Blueprint und einen XaaS-Blueprint zum Erstellen eines Active Directory-Benutzerkontos mit einem Kennwort in einer Gruppe beinhaltet. Ein Beispiel finden Sie unter [Erstellen eines XaaS-Blueprints zum Erstellen eines Benutzers](#).

Verfahren

- 1 Wählen Sie **Design > Blueprints** aus.
- 2 Markieren Sie die Zeile, die den YourCo-Maschine- und -Benutzer-Blueprint enthält, und klicken Sie auf **Benutzerdefiniertes Formular > Bearbeiten**.
- 3 Benennen Sie die Registerkarte „Allgemein“ um.
 - a Klicken Sie auf die Registerkarte.
 - b Geben Sie in der Eigenschaft **Titel** im rechten Eigenschaftenbereich **Konfiguration** ein.
- 4 Fügen Sie auf Ihrer neuen Registerkarte „Konfiguration“ die folgenden Felder hinzu und konfigurieren Sie sie mit den angegebenen Werten.

The screenshot displays the 'Edit custom form' window in vRealize Automation. At the top, there's a header with 'Edit custom form: ACTIONS' and a toggle for 'Activate custom form'. Below this, the 'Request Form' is shown with two tabs: 'Configuration' (selected) and 'Machine Details'. The 'Configuration' tab contains several form fields: 'Deploy Machine with Active Directory User Account', 'Description', 'Number of Deployments', 'Add Active Directory account' (checkbox), 'Username', 'Password', 'Confirm password', 'Email', and 'I have read and accept the software policy' (checkbox). To the left of the form, there are two panels: 'Blueprint Elements' and 'Generic Elements'. 'Blueprint Elements' shows a tree structure with 'General', 'Create_a_user_with_a_pas', and 'vSphere_vCenter_Machi'. 'Generic Elements' shows various form elements like 'Text Area', 'Text Field', 'Text', and 'Password'. At the bottom of the window, there are buttons for 'Edit Blueprint', 'Save', 'Finish', and 'Cancel'.

Verwenden Sie die bereitgestellten Werte für „Darstellung“, „Werte“ und „Einschränkungen“. Behebt alle Fehler während der Erstellung des Formulars.

Feld in Screenshot	Quelle des Blueprint-Elements	Darstellung	Werte	Optionen
Maschine mit dem Active Directory-Benutzerkonto bereitstellen	Generische Elemente > Text	Bezeichnung und Typ <ul style="list-style-type: none"> ■ Anzeigetyp = Text Sichtbarkeit <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Sichtbar = Ja 	Standardwert <ul style="list-style-type: none"> ■ Standardwert = Maschine mit Active Directory-Benutzerkonto bereitstellen ■ Wertquelle = Konstante 	
Grund für die Anforderung	Blueprint-Elemente > vSphere_vCenter_Machine > Beschreibung	Bezeichnung und Typ <ul style="list-style-type: none"> ■ Bezeichnung = Grund für die Anforderung ■ Anzeigetyp = Textfeld Sichtbarkeit <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Sichtbar = Ja Schreibgeschützt <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Schreibgeschützt = Nein Benutzerdefinierte Hilfe <ul style="list-style-type: none"> ■ Wegweiser-Hilfe = Grund für Ihre Anforderung angeben. 		Erforderlich <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Erforderlich = Ja
Anzahl Bereitstellungen	Blueprint-Elemente > Allgemein > Anzahl der Bereitstellungen	Bezeichnung und Typ <ul style="list-style-type: none"> ■ Bezeichnung = Anzahl der Bereitstellungen ■ Anzeigetyp = Integer Sichtbarkeit <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Sichtbar = Ja Schreibgeschützt <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Schreibgeschützt = Nein Benutzerdefinierte Hilfe <ul style="list-style-type: none"> ■ Wegweiser-Hilfe = Anzahl der bereitzustellenden Blueprint-Instanzen auswählen. 	Standardwert <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Standardwert = 1 	Erforderlich <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Erforderlich = Ja Minimalwert <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Min.-Wert = 1
Kontrollkästchen für Active Directory-Konto hinzufügen	Generische Elemente > Kontrollkästchen	Bezeichnung und Typ <ul style="list-style-type: none"> ■ Bezeichnung = Active Directory-Konto hinzufügen. ■ Anzeigetyp = Kontrollkästchen Sichtbarkeit <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Sichtbar = Ja 		

Feld in Screenshot	Quelle des Blueprint-Elements	Darstellung	Werte	Optionen
Benutzername	Blueprint-Elemente > Einen Benutzer mit einem Kennwort in einer Gruppe erstellen > Der Kontonamen für den Benutzer	<p>Bezeichnung und Typ</p> <ul style="list-style-type: none"> ■ Bezeichnung = Benutzername ■ Anzeigetyp = Textfeld <p>Sichtbarkeit</p> <p>Hinweis Diese Sichtbarkeitseigenschaft, die auch in den nachfolgenden Feldern identisch konfiguriert ist, blendet das Feld aus, es sei denn, das Kontrollkästchen „Active Directory-Konto“ ist aktiviert.</p> <ul style="list-style-type: none"> ■ Wertquelle = Bedingter Wert ■ Ausdruck = <p>Wert festlegen = Ja</p> <p>Wenn „Active Directory hinzufügen“ gleich „Ja“ ist</p> <p>Benutzerdefinierte Hilfe</p> <ul style="list-style-type: none"> ■ Wegweiser-Hilfe = Administratorbenutzernamen angeben. 	<p>Standardwert</p> <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Standardwert = Admin 	<p>Erforderlich</p> <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Erforderlich = Ja <p>Regulärer Ausdruck</p> <p>Hinweis Die regulären Ausdrücke müssen die JavaScript-Syntax einhalten.</p> <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Regulärer Ausdruck = "[a-zA-Z]*\$" ■ Validierungsfehlermeldung = Ihr Benutzername darf keine Sonderzeichen oder Zahlen enthalten.
Kennwort	Blueprint-Elemente > Benutzer mit einem Kennwort in einer Gruppe erstellen > Kennwort für das neu erstellte Konto festlegen	<p>Bezeichnung und Typ</p> <ul style="list-style-type: none"> ■ Bezeichnung = Kennwort ■ Anzeigetyp = Kennwort <p>Sichtbarkeit</p> <ul style="list-style-type: none"> ■ Wertquelle = Bedingter Wert ■ Ausdruck = <p>Wert festlegen = Ja</p> <p>Wenn „Active Directory hinzufügen“ gleich „Ja“ ist</p> <p>Benutzerdefinierte Hilfe</p> <ul style="list-style-type: none"> ■ Wegweiser-Hilfe = Kennwort für Ihr Administratorkonto angeben. 		<p>Erforderlich</p> <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Erforderlich = Ja <p>Regulärer Ausdruck</p> <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Regulärer Ausdruck = "[A-Z]{8,}[a-z]{8,}\$" ■ Meldung = Ihr Administratorkennwort muss mindestens acht Zeichen lang sein und kann alphanumerische Zeichen und Sonderzeichen enthalten.

Feld in Screenshot	Quelle des Blueprint-Elements	Darstellung	Werte	Optionen
Kennwort bestätigen	Blueprint-Elemente > Benutzer mit einem Kennwort in einer Gruppe erstellen > Bestätigung des Kennworts	Bezeichnung und Typ <ul style="list-style-type: none"> ■ Bezeichnung = Kennwort bestätigen Anzeigetyp = Kennwort Sichtbarkeit <ul style="list-style-type: none"> ■ Wertquelle = Bedingter Wert ■ Ausdruck = Wert auf „Ja“ festlegen Wenn „Active Directory hinzufügen“ gleich „Ja“ ist Benutzerdefinierte Hilfe <ul style="list-style-type: none"> ■ Wegweiser-Hilfe = Kennwort für Ihr Administratorkonto erneut eingeben. 		Erforderlich <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Erforderlich = Ja Übereinstimmendes Feld festlegen <ul style="list-style-type: none"> ■ Übereinstimmendes Feld = Kennwort
E-Mail	Generische Elemente > Textfeld	Bezeichnung und Typ <ul style="list-style-type: none"> ■ Bezeichnung = E-Mail ■ Anzeigetyp = Textfeld Sichtbarkeit <ul style="list-style-type: none"> ■ Wertquelle = Bedingter Wert ■ Ausdruck = Wert festlegen = Ja Wenn „Active Directory hinzufügen“ gleich „Ja“ ist Benutzerdefinierte Hilfe <ul style="list-style-type: none"> ■ Wegweiser-Hilfe = Administrator-E-Mail eingeben. 	Standardwert <ul style="list-style-type: none"> ■ Wertquelle = Berechneter Wert ■ Operator = Verketteten ■ Wert hinzufügen = Feld. Benutzernamen auswählen ■ Wert hinzufügen = Konstante. @yourco.com eingeben 	Regulärer Ausdruck <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Regulärer Ausdruck = "^[A-Za-z0-9-_%+~]+@[A-Za-z0-9-~]+\\.([A-Za-z]{2,})\$" ■ Validierungsfehlermeldung = Gültige E-Mail eingeben
Kontrollkästchen „Ich habe die Softwarerichtlinie gelesen und akzeptiert“	Generische Elemente > Kontrollkästchen	Bezeichnung und Typ <ul style="list-style-type: none"> ■ Elementbezeichnung = Ich habe die Softwarerichtlinie gelesen und akzeptiert ■ Anzeigetyp = Kontrollkästchen Sichtbarkeit <ul style="list-style-type: none"> ■ Wertquelle = Bedingter Wert ■ Ausdruck = Wert festlegen = Ja Wenn „Active Directory hinzufügen“ gleich „Ja“ ist		

- 5 Klicken Sie auf **Registerkarte hinzufügen** und geben Sie in der **Titel**-Eigenschaft rechts **Maschinendetails** ein.

6 Konfigurieren Sie die folgenden Felder auf der Registerkarte „Maschinendetails“.

The screenshot shows the 'Edit custom form' window in vRealize Automation. The 'Machine Details' tab is selected, displaying a form with the following fields:

- Storage (GB): A text input field.
- Number of CPUs: A text input field.
- Memory (GB): A text input field.
- Memory (MB): A text input field.

The left sidebar contains 'Blueprint Elements' and 'Generic Elements'. The right sidebar shows 'Machine Details' with a title 'Machine Details' and a visibility setting 'y'.

Verwenden Sie die bereitgestellten Werte für „Darstellung“, „Werte“ und „Einschränkungen“.

Feld in Screenshot	Blueprint-Elementquelle	Darstellung	Werte	Optionen
Speicher (GB)	Blueprint-Elemente > vSphere_vCenter_Machine > Speicher (GB)	Bezeichnung und Typ <ul style="list-style-type: none"> ■ Bezeichnung = Speicher (GB) ■ Anzeigetyp = Integer Sichtbarkeit <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Sichtbarkeit = Ja Schreibgeschützt <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Schreibgeschützt = Nein 	Standardwert <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Standardwert = 4 	Minimalwert <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Minimalwert = 2
Anzahl der CPUs	Blueprint-Elemente > vSphere_vCenter_Machine > CPUs	Bezeichnung und Typ <ul style="list-style-type: none"> ■ Bezeichnung = Anzahl der CPUs ■ Anzeigetyp = Integer Sichtbarkeit <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Sichtbarkeit = Ja 	Standardwert <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Standardwert = 1 	Minimalwert <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Min.-Wert = 1

Feld in Screenshot	Blueprint-Elementquelle	Darstellung	Werte	Optionen
Arbeitsspeicher (GB)	Generische Elemente > Ganzzahl	Bezeichnung und Typ <ul style="list-style-type: none"> ■ Bezeichnung = Arbeitsspeicher (GB) ■ Anzeigetyp = Integer Sichtbarkeit <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Sichtbarkeit = Ja 	Standardwert <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Standardwert = 1 	Minimalwert <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Minimalwert = 1
Arbeitsspeicher (MB)	Blueprint-Elemente > vSphere_vCenter_Machine > Arbeitsspeicher (MB)	Bezeichnung und Typ <ul style="list-style-type: none"> ■ Bezeichnung = Arbeitsspeicher (MB) ■ Anzeigetyp = Integer Sichtbarkeit <ul style="list-style-type: none"> ■ Wertquelle = Konstante ■ Sichtbarkeit = Nein 	Standardwert <ul style="list-style-type: none"> ■ Wertquelle = Berechneter Wert ■ Operator = Multiplizieren ■ Wert hinzufügen = Feld. Arbeitsspeicher auswählen (GB) ■ Wert hinzufügen = Konstante. 1024 eingeben 	

- 7 Mögliche Fehler beheben. Sie können das Formular speichern, aber es erst aktivieren, wenn es fehlerfrei ist.
- 8 Um das Formular zu speichern und den Formulardesigner zu schließen, klicken Sie auf **Fertig stellen**.
- 9 Wählen Sie den Blueprint aus und klicken Sie auf **Veröffentlichen**.
- 10 Damit das benutzerdefinierte Formular verfügbar ist, wenn Benutzer das Element im Servicekatalog anfordern, wählen Sie in der Symbolleiste der Blueprints-Seite **Benutzerdefiniertes Formular > Aktivieren** aus.

Nächste Schritte

- Stellen Sie den Blueprint im Servicekatalog zur Verfügung. Siehe [Verwalten des Servicekatalogs](#).
- Vergewissern Sie sich, dass das Anforderungsformular im Katalog dem folgenden Beispiel ähnlich ist:

The image displays two overlapping screenshots of the vRealize Automation 'New Request' form. The top screenshot shows the 'Machine Details' tab, which includes fields for 'Storage (GB)' (4), 'Number of CPUs' (1), and 'Memory (GB)' (1). The bottom screenshot shows the 'Configuration' tab, which includes a section for 'Deploy Machine with Active Directory User Account'. This section contains fields for 'Reason for Request', 'Number of Deployments' (1), 'Username' (admin), 'Password', 'Confirm password', and 'Email' (admin@yourco.com). There is also a checkbox for 'Add Active Directory account' and a checkbox for 'I have read and accept the software policy'. Both screenshots show a navigation bar at the top with tabs: Home, Catalog, Items, Requests, Inbox, Design, Administration, Infrastructure, and Containers.

Benutzerdefinierte Formulardesigner-Feldeigenschaften

Die Feldeigenschaften bestimmen, wie das ausgewählte Feld aussieht und welche Standardwerte dem Benutzer angezeigt werden. Sie legen außerdem fest, welche Regeln Sie auf das Feld anwenden möchten, um sicherzustellen, dass der Benutzer einen gültigen Eintrag im Kataloganforderungsformular in vRealize Automation angibt.

Sie konfigurieren jedes Feld einzeln. Wählen Sie das Feld aus und bearbeiten Sie die Feldeigenschaften.

Wertquelle

Für viele der Eigenschaften können Sie eine Auswahl aus verschiedenen Wertquellenoptionen treffen. Nicht alle Quellenoptionen sind für alle Feldtypen oder Eigenschaften verfügbar.

- **Konstante.** Der Wert wird nicht geändert. Je nach der Eigenschaft kann der Wert eine Zeichenfolge, eine Ganzzahl, ein regulärer Ausdruck oder ein aus einer begrenzten Liste ausgewählter Wert, wie beispielsweise „Ja“ oder „Nein“, sein. Sie können beispielsweise „1“ als ganzzahligen Standardwert angeben, „Nein“ für die Eigenschaft „Schreibgeschützt“ auswählen oder den regulären Ausdruck angeben, um einen Feldeintrag zu validieren.

- **Bedingter Wert.** Der Wert basiert auf einer oder mehreren Bedingungen. Die Bedingungen werden in der aufgeführten Reihenfolge verarbeitet. Wenn mehrere Bedingungen zutreffen, bestimmt die letzte Bedingung, die zutrifft, das Verhalten des Felds für diese Eigenschaft. Sie können beispielsweise eine Bedingung erstellen, die bestimmt, ob ein Feld basierend auf dem Wert in einem anderen Feld angezeigt wird.
- **Externe Quelle.** Der Wert basiert auf den Ergebnissen einer vRealize Orchestrator-Aktion. Berechnen Sie beispielsweise die Kosten basierend auf einer vRealize Orchestrator-Skriptaktion. Ein Beispiel finden Sie unter [Verwenden von vRealize Orchestrator-Aktionen im Designer für benutzerdefinierte Formulare](#).
- **Feld binden.** Der Wert ist mit dem Feld identisch, an das er gebunden ist. Die verfügbaren Felder sind auf denselben Feldtyp beschränkt. Sie können beispielsweise den Standardwert für ein Kontrollkästchenfeld „Authentifizierung erforderlich“ an ein anderes Kontrollkästchenfeld binden. Wenn ein Kontrollkästchen-Zielfeld im Anforderungsformular aktiviert ist, wird das Kontrollkästchen in dem aktuellen Feld aktiviert.
- **Berechneter Wert.** Der Wert wird basierend darauf bestimmt, wie der Operator die ausgewählten Felder und Werte verarbeitet. Textfelder verwenden den Operator „Verkettung“. Ganzzahlfelder verwenden die ausgewählten Vorgänge zum Addieren, Subtrahieren, Multiplizieren oder Dividieren. Sie können beispielsweise ein ganzzahliges Feld zum Umrechnen von Megabyte in Gigabyte über den Multiplizieren-Vorgang konfigurieren.

Felddarstellung

Sie verwenden die Darstellungseigenschaften, um zu bestimmen, ob das Feld im Formular angezeigt wird und welche Bezeichnung und benutzerdefinierte Hilfe Sie den Katalogbenutzern bereitstellen möchten.

Tabelle 3-66. Optionen auf der Registerkarte „Darstellung“

Option	Beschreibung
Bezeichnung und Typ	<p>Geben Sie eine Bezeichnung an und wählen Sie einen Anzeigetyp aus.</p> <p>Die verfügbaren Anzeigetypen sind vom Feld abhängig. Einige Felder unterstützen mehrere Texttypen und andere unterstützen nur Ganzzahlen. Mögliche Werte:</p> <ul style="list-style-type: none"> ■ Dezimal ■ Dropdown ■ Image ■ Integer ■ Mehrfach- auswahl ■ Kennwort ■ Optionsfeld- gruppe, ■ Text ■ Textbereich ■ Textfelder <p>Dropdown-und Datenraster-Felder enthalten eine Platzhalter-Einstellung. Der eingegebene Wert wird als eine interne Bezeichnung oder Anweisung im Dropdown-Menü oder als allgemeine Bezeichnung oder Anweisung im Datenraster angezeigt.</p>
Sichtbarkeit	<p>Blenden Sie ein Feld auf dem Anforderungsformular ein oder aus.</p> <ul style="list-style-type: none"> ■ Konstante. Wählen Sie „Ja“ aus, um das Feld im Formular anzuzeigen. Wählen Sie „Nein“ aus, um das Feld auszublenden. ■ Bedingter Wert. Die Sichtbarkeit wird durch den ersten Ausdruck bestimmt, der zutrifft. Ein Feld ist beispielsweise sichtbar, wenn ein Kontrollkästchen in einem Formular aktiviert ist. ■ Externe Quelle. Die Sichtbarkeit wird durch die Ergebnisse der ausgewählten vRealize Orchestrator-Aktion bestimmt.
Schreibgeschützt	<p>Verhindern Sie, dass Benutzer die Feldwerte ändern.</p> <ul style="list-style-type: none"> ■ Konstante. Wählen Sie „Ja“, um den Wert anzuzeigen, aber Änderungen zu verhindern. Wählen Sie „Nein“, um Änderungen zuzulassen. ■ Bedingter Wert. Der Status wird durch den ersten Ausdruck bestimmt, der zutrifft. Ein Feld ist beispielsweise schreibgeschützt, wenn der Wert in einem Speicherfeld größer als 2 GB ist. ■ Externe Quelle. Der Status wird durch die Ergebnisse der ausgewählten vRealize Orchestrator-Aktion bestimmt.

Tabelle 3-66. Optionen auf der Registerkarte „Darstellung“ (Fortsetzung)

Option	Beschreibung
Zeilen pro Seite	Nur für Datenrasterelemente. Geben Sie die Anzahl der Zeilen ein.
Benutzerdefinierte Hilfe	Geben Sie den Benutzern Informationen zum Feld an. Diese Informationen werden in der Wegweiser-Hilfe für das Feld angezeigt. Sie können einfachen Text oder HTML-Format verwenden, einschließlich Href-Links. Beispiel: <code>vRealize Automation documentation</code> .

Feldwerte

Sie verwenden die Werteigenschaften, um Standardwerte anzugeben.

Tabelle 3-67. Optionen auf der Registerkarte „Werte“

Option	Beschreibung
Spalten	Nur für das Datenrasterelement. Geben Sie die Bezeichnung, die ID und den Werttyp für jede Spalte in der Tabelle an. Der Standardwert für das Datenraster muss die Kopfzeilendaten enthalten, die den definierten Spalten entsprechen. Wenn Sie beispielsweise user_name-ID für eine Spalte und user_role-ID für eine andere verwenden, ist die erste Zeile user_name,user_role. Konfigurationsbeispiele finden Sie unter Verwenden des Datenrasterelements im Designer für benutzerdefinierte Formulare .
Standardwert	Füllt das Feld mit einem Standardwert basierend auf der Wertquelle. Mögliche Wertquellen sind vom Feld abhängig. <ul style="list-style-type: none"> ■ Konstante. Die eingegebene Zeichenfolge. ■ Bedingter Wert. Der Standardwert wird durch den ersten Ausdruck bestimmt, der zutrifft. Der Standardwert eines Speicherfelds beträgt beispielsweise 1 GB, wenn das Arbeitsspeicherfeld weniger als 512 MB beträgt. ■ Externe Quelle. Der Wert basiert auf den Ergebnissen der ausgewählten vRealize Orchestrator-Aktion. ■ Feld binden. Der Wert ist mit dem ausgewählten Feld identisch. ■ Berechneter Wert. Der Wert basiert auf den Ergebnissen der angegebenen Feldwerte und des ausgewählten Operators. Der Standardwert des Arbeitsspeichers in MB basiert beispielsweise auf dem Arbeitsspeicher in GB multipliziert mit 1024.

Tabelle 3-67. Optionen auf der Registerkarte „Werte“ (Fortsetzung)

Option	Beschreibung
Wertoption	<p>Füllt Felder des Typs Dropdown, Mehrfachauswahl, Optionsfeldgruppe oder Wertauswahl.</p> <ul style="list-style-type: none"> ■ Konstante. Das Format für die Liste ist Wert Bezeichnung,Wert Bezeichnung,Wert Bezeichnung. Beispiel: 2 Small,4 Medium,8 Large. ■ Externe Quelle. Der Wert basiert auf den Ergebnissen der ausgewählten vRealize Orchestrator-Aktion.
Schritt	<p>Definieren Sie für Ganzzahl- oder Dezimalzahlfelder die inkrementellen oder dekrementellen Werte.</p> <p>Wenn der Standardwert beispielsweise 1 lautet und Sie den Schrittwert auf 3 festlegen, sind die zulässigen Werte 4, 7, 10 usw.</p>

Feldeinschränkungen

Sie verwenden die Einschränkungseigenschaften, um sicherzustellen, dass der anfordernde Benutzer gültige Werte im Anforderungsformular angibt.

Sie können auch die externe Validierung als alternative Methode zur Gewährleistung gültiger Werte verwenden. Siehe [Verwenden der externen Validierung im Designer für benutzerdefinierte Formulare](#).

Tabelle 3-68. Optionen auf der Registerkarte „Einschränkungen“

Option	Beschreibung
Erforderlich	<p>Der anfordernde Benutzer muss einen Wert für dieses Feld angeben.</p> <ul style="list-style-type: none"> ■ Konstante. Wählen Sie „Ja“ aus, um festzulegen, dass der anfordernde Benutzer einen Wert angeben muss. Wählen Sie „Nein“ aus, wenn das Feld optional ist. ■ Bedingter Wert. Ob das Feld ein Pflichtfeld ist oder nicht, wird durch den ersten Ausdruck bestimmt, der zutrifft. Dieses Feld ist z. B. erforderlich, wenn die Betriebssystemfamilie in einem anderen Feld mit „Darwin“ beginnt. ■ Externe Quelle. Der Status basiert auf den Ergebnissen der ausgewählten vRealize Orchestrator-Aktion.
Regulärer Ausdruck	<p>Geben Sie einen regulären Ausdruck an, der den Wert validiert, und eine Meldung, die angezeigt wird, wenn die Validierung fehlschlägt.</p> <p>Die regulären Ausdrücke müssen die JavaScript-Syntax einhalten. Einen Überblick finden Sie unter Erstellen eines regulären Ausdrucks. Genaue Anweisungen finden Sie unter Syntax.</p> <ul style="list-style-type: none"> ■ Konstante. Geben Sie einen regulären Ausdruck an. Bei einer E-Mail-Adresse kann der reguläre Ausdruck beispielsweise <code>^[A-Za-z0-9._%+-]+@[A-Zaz0-9.-]+\.[A-Za-z]{2,}\$</code> sein und die Validierungsfehlermeldung <code>Das E-Mail-Adressformat ist nicht gültig. Bitte versuchen Sie es erneut.</code> ■ Bedingter Wert. Der verwendete reguläre Ausdruck wird durch den ersten Ausdruck bestimmt, der zutrifft.
Minimalwert	<p>Geben Sie einen numerischen Minimalwert ein. Beispiel: Ein Kennwort muss mindestens 8 Zeichen enthalten.</p> <p>Geben Sie eine Fehlermeldung an. Beispiel: <code>Das Kennwort muss mindestens 8 Zeichen enthalten.</code></p> <ul style="list-style-type: none"> ■ Konstante. Geben Sie die Ganzzahl ein. ■ Bedingter Wert. Der Minimalwert wird durch den ersten Ausdruck bestimmt, der zutrifft. Ein CPU-Minimalwert ist beispielsweise 4, wenn das Betriebssystem nicht Linux ist. ■ Externe Quelle. Der Wert basiert auf den Ergebnissen der ausgewählten vRealize Orchestrator-Aktion.

Tabelle 3-68. Optionen auf der Registerkarte „Einschränkungen“ (Fortsetzung)

Option	Beschreibung
Maximalwert	<p>Numerischer Maximalwert. Beispiel: Ein Feld ist auf 50 Zeichen begrenzt.</p> <p>Geben Sie eine Fehlermeldung an. Beispiel: Diese Beschreibung darf nicht mehr als 50 Zeichen enthalten.</p> <ul style="list-style-type: none"> ■ Konstante. Geben Sie die Ganzzahl ein. ■ Bedingter Wert. Der Maximalwert wird durch den ersten Ausdruck bestimmt, der zutrifft. Ein maximaler Speicherwert ist beispielsweise 2 GB, wenn der Bereitstellungsort AMEA entspricht. ■ Externe Quelle. Der Wert basiert auf den Ergebnissen der ausgewählten vRealize Orchestrator-Aktion.
Übereinstimmendes Feld festlegen	<p>Dieser Feldwert muss mit dem ausgewählten Feldwert übereinstimmen.</p> <p>Beispiel: Ein Kennwortbestätigungsfeld muss mit dem Kennwortfeld übereinstimmen.</p>

Verwenden von vRealize Orchestrator-Aktionen im Designer für benutzerdefinierte Formulare

Wenn Sie das Anforderungsformular für einen vRealize Automation-Blueprint anpassen, können Sie das Verhalten einiger Felder auf die Ergebnisse einer vRealize Orchestrator-Aktion gründen.

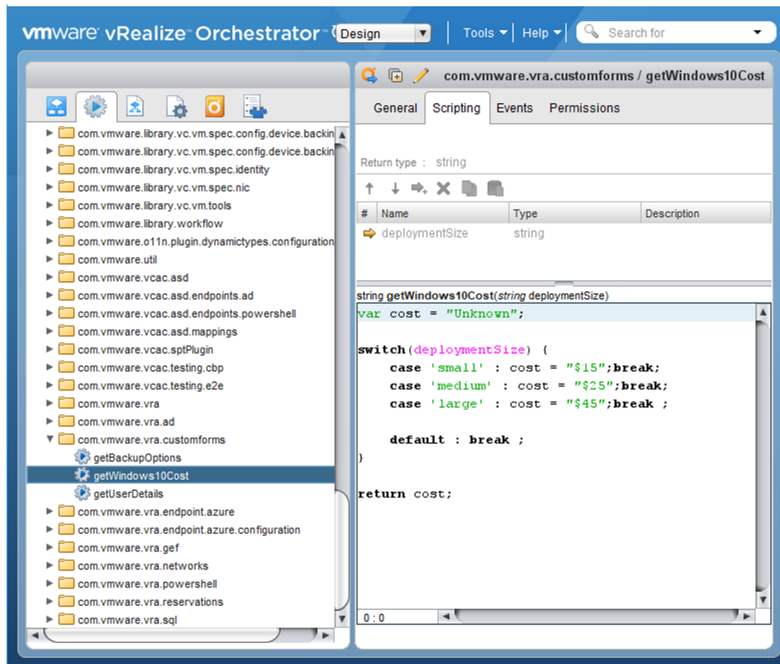
Es gibt mehrere Möglichkeiten der Verwendung von vRealize Orchestrator-Aktionen.

Möglicherweise führen Sie eine Aktion aus, bei der die Daten aus einer dritten Quelle bezogen werden, oder Sie verwenden ein Skript, das die Größe und Kosten definiert. In diesem Beispiel wird ein Skript verwendet.

Beispiel: Felder für Größe und Kosten - Beispiel

In diesem Anwendungsfall soll der Katalogbenutzer die Größe einer virtuellen Maschine auswählen und anschließend die Kosten dieser Maschine pro Tag anzeigen. Für dieses Beispiel verfügen Sie über eine vRealize Orchestrator-Instanz, die die Größe und Kosten korreliert, und Sie fügen dem benutzerdefinierten Blueprint-Formular ein Größenfeld und ein Kostenfeld hinzu. Das Größenfeld legt den Wert fest, der im Kostenfeld angezeigt wird.

- 1 Konfigurieren Sie in vRealize Orchestrator eine Aktion, `getWindows10Cost`, deren `deploymentSize`-Skript dem folgenden Beispiel gleicht.



Verwenden Sie das Folgende als Skriptbeispiel.

```
var cost = "Unknown";

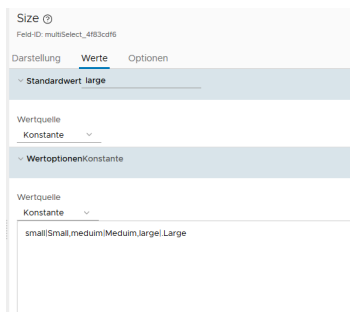
switch(deploymentSize) {
  case 'small' : cost = "$15";break;
  case 'medium' : cost = "$25";break;
  case 'large' : cost = "$45";break ;

  default : break ;
}

return cost;
```

- 2 Fügen Sie in vRealize Automation dem benutzerdefinierten Blueprint-Formular ein Größenfeld und ein Kostenfeld hinzu.

Konfigurieren Sie das Größenfeld als Mehrfachauswahlfeld mit den Werten „Klein“, „Mittel“ und „Groß“.



Fügen Sie in vRealize Automation dem benutzerdefinierten Blueprint-Formular ein Größenfeld und ein Kostenfeld hinzu.

Konfigurieren Sie die folgenden Eigenschaftswerte auf der Registerkarte „Werte“.

- Standardwert = **Groß**
- Wertoptionen
 - Wertquelle = **Konstante**
 - Wertdefinition = **small|Small,medium|Medium,large|Large**

- 3 Konfigurieren Sie das Kostenfeld, um die Kosten gemäß der Definition in der auf den im Größensfeld ausgewählten Werten basierten vRealize Orchestrator-Aktion anzuzeigen.

Cost ⓘ
Field ID: cost

Appearance **Values** Constraints

▼ Default value External source

Value source External source ▼

Select action com.vmware.vra.customforms/getWindows10Cost

Action inputs

deploymentSize Field ▼ Size ▼

Konfigurieren Sie die folgenden Eigenschaftswerte auf der Registerkarte „Werte“.

- Standardwert = Externe Quelle
- Aktion auswählen = <IhrvRealize Orchestrator-Aktionsordner>/getWindows10Cost
- Aktionseingabe
 - deploymentSize. Dieser Wert wurde in der Aktion konfiguriert.
 - Feld
 - Größe

Verwenden des Datenrasterelements im Designer für benutzerdefinierte Formulare

Wenn Sie das Anforderungsformular für einen Blueprint anpassen, fügen Sie Informationen in einem Tabellenformat hinzu. Die in der Tabelle enthaltenen Daten können manuell oder basierend auf einer externen Quelle bereitgestellt werden.

Beispiel: Bereitgestellte CSV-Daten - Beispiel

In diesem Anwendungsfall haben Sie eine Tabelle mit Werten, die Sie im benutzerdefinierten Anforderungsformular bereitstellen. Sie geben die Informationen in der Tabelle als eine konstante Wertquelle an. Die Quelle basiert auf einer CSV-Datenstruktur, wobei die erste Zeile die Kopfzeile ist. Die Kopfzeilen sind die durch ein Komma getrennten Spalten-IDs. Alle zusätzlichen Zeilen sind die Daten, die in jeder Zeile in der Tabelle angezeigt werden.

- 1 Fügen Sie das generische Datenrasterelement zur Design-Arbeitsfläche hinzu.
- 2 Wählen Sie das Datenraster aus und definieren Sie die Werte im Bereich „Eigenschaften“.

Data Grid ⓘ
Field ID: datagrid_0a3999da

Appearance **Values**

Columns

ADD COLUMN

Label	Username	
Id	username	
Type	String	▼

Label	Employee ID	
Id	employeeId	
Type	Integer	▼

Label	Manager	
Id	manager	
Type	String	▼

Default value Constant

Value source Constant ▼

CSV

```
username,employeeId,manager
leonardo,95621,Farah
vindhya,15496,Farah
martina,52648,Nikolai
```

Bezeichnung	ID	Typ
Benutzername	Benutzername	String
Mitarbeiter-ID	employeeId	Integer
Manger	manager	String

Definieren Sie die CSV-Werte.

```
username,employeeId,manager
leonardo,95621,Farah
vindhya,15496,Farah
martina,52648,Nikolai
```

- 3 Stellen Sie sicher, dass das Datenraster die erwarteten Daten im Blueprint-Anforderungsformular anzeigt.

+

-

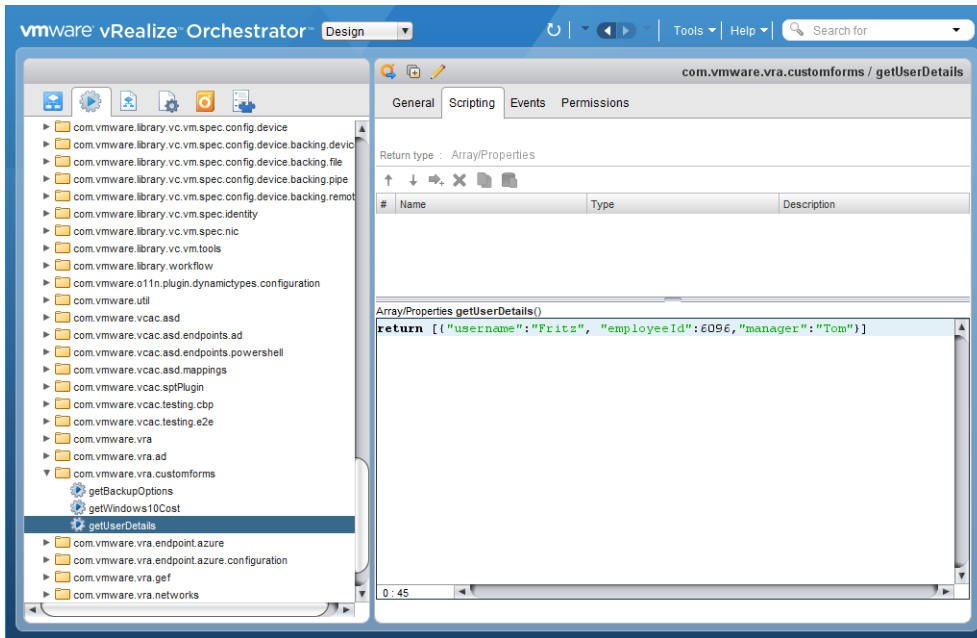
<input type="checkbox"/>	Username ▼	Employee ID ▼	Manager ▼
<input checked="" type="checkbox"/>	leonardo	95621	Farah
<input type="checkbox"/>	vindhya	15496	Farah
<input type="checkbox"/>	martina	52648	Nikolai
<input checked="" type="checkbox"/> 1 1 - 3 von 3			

Beispiel: Externe Quelle - Beispiel

In diesem Beispiel wird das vorherige Beispiel verwendet, die Werte basieren jedoch auf einer vRealize Orchestrator-Aktion. Dies ist ein Beispiel für eine einfache Aktion. Sie können aber auch eine komplexere Aktion verwenden, mit der Sie diese Informationen aus einer lokalen Datenbank oder einem lokalen System abrufen.

Die als Validierung verwendete Aktion, muss über einen Eingabeparameter vom Typ „Array/Eigenschaften“ verfügen.

- 1 Konfigurieren Sie in vRealize Orchestrator eine Aktion, `getUserDetails`, mit einem Datenfeld ähnlich wie im folgenden Beispiel.



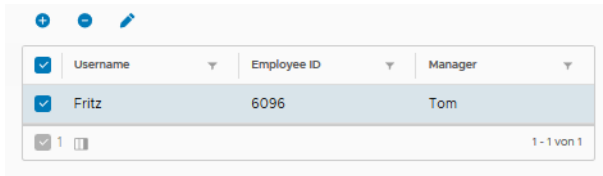
Verwenden Sie das folgende Skriptbeispiel.

```
return [{"username": "Fritz", "employeeId": 6096, "manager": "Tom"}]
```

- 2 Fügen Sie in vRealize Automation das Datenraster hinzu und konfigurieren Sie die Datenrasterspalten mit den folgenden Werten.

Bezeichnung	ID	Typ
Benutzername	Benutzername	String
Mitarbeiter-ID	employeeId	Integer
Manger	manger	String

- 3 Wählen Sie in der Liste „Wertquelle“ den Eintrag **Externe Quelle** aus.
- 4 Geben Sie unter „Aktion auswählen“ den Befehl „getUserDetails“ ein und wählen Sie die in vRealize Orchestrator erstellte Aktion aus.
- 5 Speichern und überprüfen Sie die Tabelle im Anforderungsformular.



<input checked="" type="checkbox"/>	Username	Employee ID	Manager
<input checked="" type="checkbox"/>	Fritz	6096	Tom

1 - 1 von 1

Verwenden der externen Validierung im Designer für benutzerdefinierte Formulare

Sie können ein Anforderungsformular anpassen, um sicherzustellen, dass Benutzer während der Anforderungszeit gültige Werte eingeben, indem Sie Einschränkungen zu Feldern hinzufügen oder eine externe Validierungsquelle verwenden.

Einige Feldeigenschaften, wie zum Beispiel „Mindestwert“, „Maximalwert“, „reguläre Ausdrücke“, „übereinstimmende Felder“ oder „nicht leer“ können mit Einschränkungen konfiguriert werden, um gültige Werte sicherzustellen. Siehe [Benutzerdefinierte Formulardesigner-Feldeigenschaften](#).

Bei der externen Validierung wird mithilfe von vRealize Orchestrator-Aktionen nach gültigen Werten aus einer externen Quelle gesucht.

Beim Überprüfen eines Datenrasterwerts muss die für die Validierung verwendete Aktion einen Eingabeparameter vom Typ „Array/Eigenschaften“ aufweisen.

Im Folgenden finden Sie eine Auflistung von Beispielen, in denen Sie möglicherweise eine externe Validierung verwenden möchten.

- Die gültigen Werte werden in einer externen Quelle definiert. Beispiel: vRealize Orchestrator.
- Die Validierung muss sich auf mehrere Felder auswirken. Beispiel: Eine vRealize Orchestrator-Aktion erfasst die Festplattengröße und Kapazität des Speicherpools und validiert die angegebenen Größenwerte basierend auf dem verfügbaren Speicherplatz.

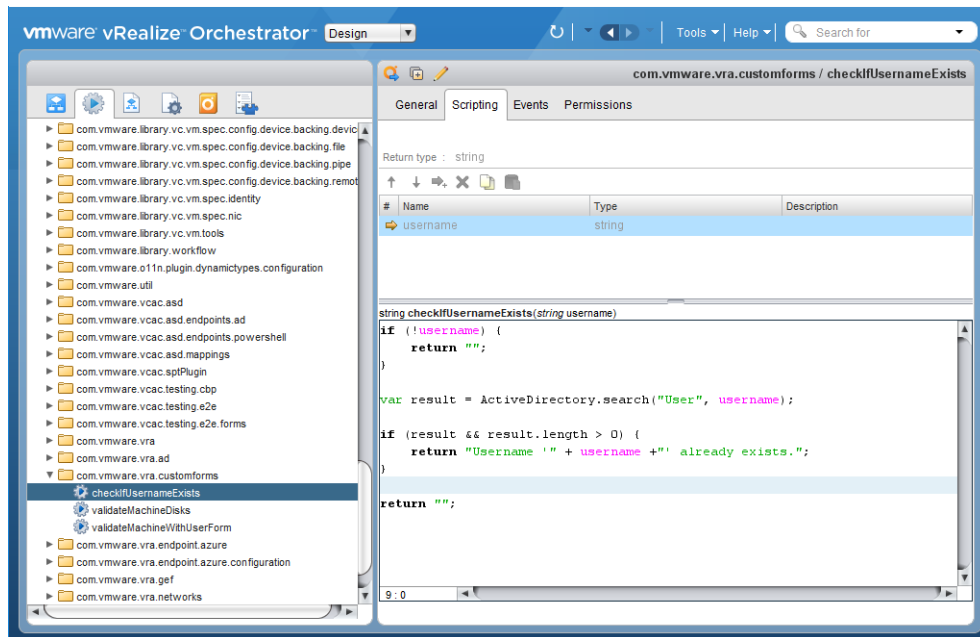
Wie ordnen Sie mehrere externe Validierungen in einem Blueprint an? Die Validierungen werden in der Reihenfolge verarbeitet, in der sie auf der Arbeitsfläche „Externe Validierungen“ angezeigt werden. Wenn Sie über zwei Validierungen verfügen, die dasselbe Feld validieren, überschreiben die Ergebnisse der zweiten Validierung die Ergebnisse der ersten. Um die Validierungen neu anzuordnen, können Sie auf die Karten auf der Arbeitsfläche klicken und diese ziehen.

Beispiel: vRealize Orchestrator-Benutzer - Beispiel

In diesem Anwendungsfall soll der Katalogbenutzer nur einen neuen Benutzernamen angeben. Für dieses Beispiel verfügen Sie über eine vRealize Orchestrator-Aktion, die überprüft, ob der im Formular angegebene Benutzername in Ihrer Active Directory-Datenbank vorhanden ist. Wenn der Name vorhanden ist, wird eine Fehlermeldung im Anforderungsformular angezeigt.

Dieser Anwendungsfall wird auf das [Erstellen eines benutzerdefinierten Anforderungsformulars mit Active Directory-Optionen](#)-Beispiel angewendet.

- 1 Konfigurieren Sie in vRealize Orchestrator eine Aktion, `checkIfUsernameExists`, mit einem Skript ähnlich dem folgenden Beispiel.



Verwenden Sie das Folgende als Skriptbeispiel. In diesem Beispiel ist return die Meldung, die angezeigt wird, wenn die Validierung fehlschlägt.

```

if (!username) {
    return "";
}

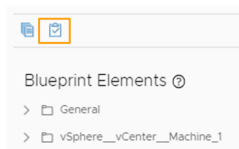
var result = ActiveDirectory.search("User", username);

if (result && result.length > 0) {
    return "Username '" + username + "' already exists.";
}

return "";

```

- Öffnen Sie in vRealize Automation den Designer für benutzerdefinierte Anforderungsformulare für Ihren Blueprint, klicken Sie auf **Externe Validierung** und ziehen Sie den Typ der **Orchestrator-Validierung** auf die Arbeitsfläche.



- Konfigurieren Sie die externen Validierungsoptionen.

- Validierungsbezeichnung = prüfen, ob der Benutzername vorhanden ist
- Aktion auswählen = <Ihr vRealize Orchestrator-Aktionsordner>/checkIfUsernameExists
- Aktionseingabe
 - Benutzername = Feld und Benutzername
- Hervorgehobene Felder
 - Klicken Sie auf **Feld hinzufügen** und wählen Sie „Benutzername“ aus.

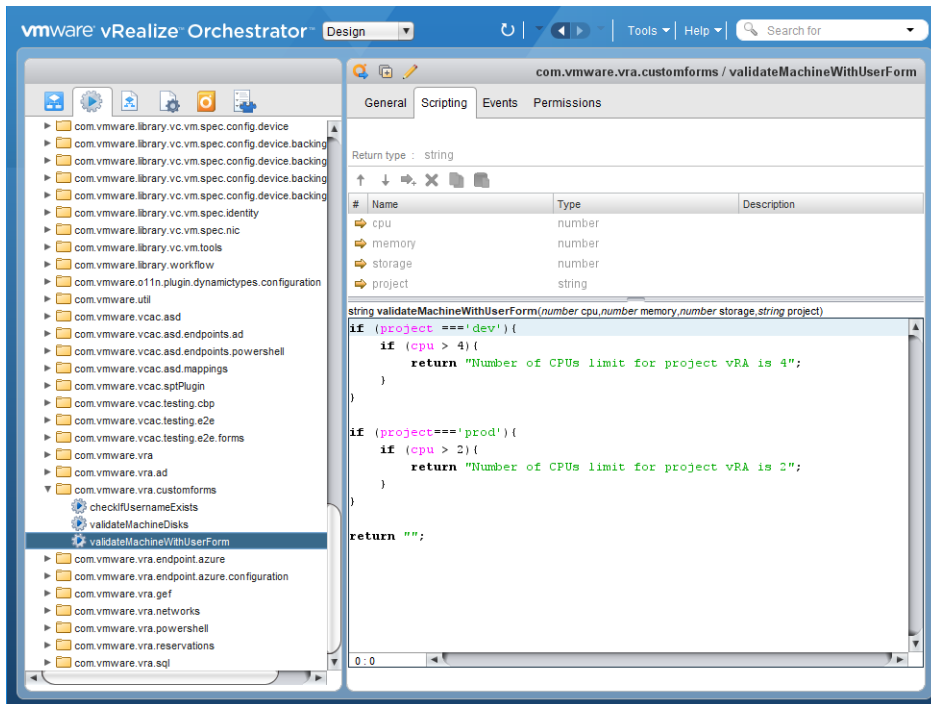
Ein Validierungsfehler auf Feldebene wird im Kataloganforderungsformular angezeigt, wenn die Validierung aufgrund eines eingegebenen Werts fehlschlägt. Wenn Sie einen globale Fehler erzeugen möchten, konfigurieren Sie das markierte Feld nicht.

Beispiel: Mehrere Felder in vRealize Orchestrator - Beispiel

In diesem Anwendungsfall soll die Validierung der CPU, des Arbeitsspeichers und der Speicherwerte auf dem Projektwert basieren. Wenn die Benutzer zum Beispiel das Entwicklungsprojekt (Dev) auswählen, ist 4 die maximale Anzahl der CPUs. Wenn sie das Produktionsprojekt (Prod) auswählen, ist 2 der Maximalwert.

Fügen Sie für diesen Anwendungsfall ein Projektfeld zum [Erstellen eines benutzerdefinierten Anforderungsformulars mit Active Directory-Optionen](#)-Beispiel hinzu. Konfigurieren Sie das Projekt als eine Dropdownliste mit „Dev“ und „Prod“.

- 1 Konfigurieren Sie in vRealize Orchestrator eine Aktion, `validateMachineWithUserForm`, mit einem Skript ähnlich dem folgenden Beispiel.



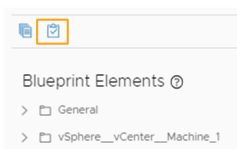
Verwenden Sie das Folgende als Skriptbeispiel für die CPU-Überprüfung. Fahren Sie mit dem Hinzufügen der Arbeitsspeicher- und Speicherwerte zum Skript nach Bedarf fort. In diesem Beispiel ist „zurückgeben“ die Meldung, die beim Fehlschlagen der Validierung angezeigt wird.

```
if (project === 'dev'){
    if (cpu > 4){
        return "Number of CPUs limit for project vRA is 4";
    }
}

if (project === 'prod'){
    if (cpu > 2){
        return "Number of CPUs limit for project vRA is 2";
    }
}

return "";
```

- Öffnen Sie in vRealize Automation den Designer für benutzerdefinierte Anforderungsformulare für Ihren Blueprint, klicken Sie auf **Externe Validierung** und ziehen Sie den Typ der **Orchestrator-Validierung** auf die Arbeitsfläche.



- Konfigurieren Sie die externen Validierungsoptionen.

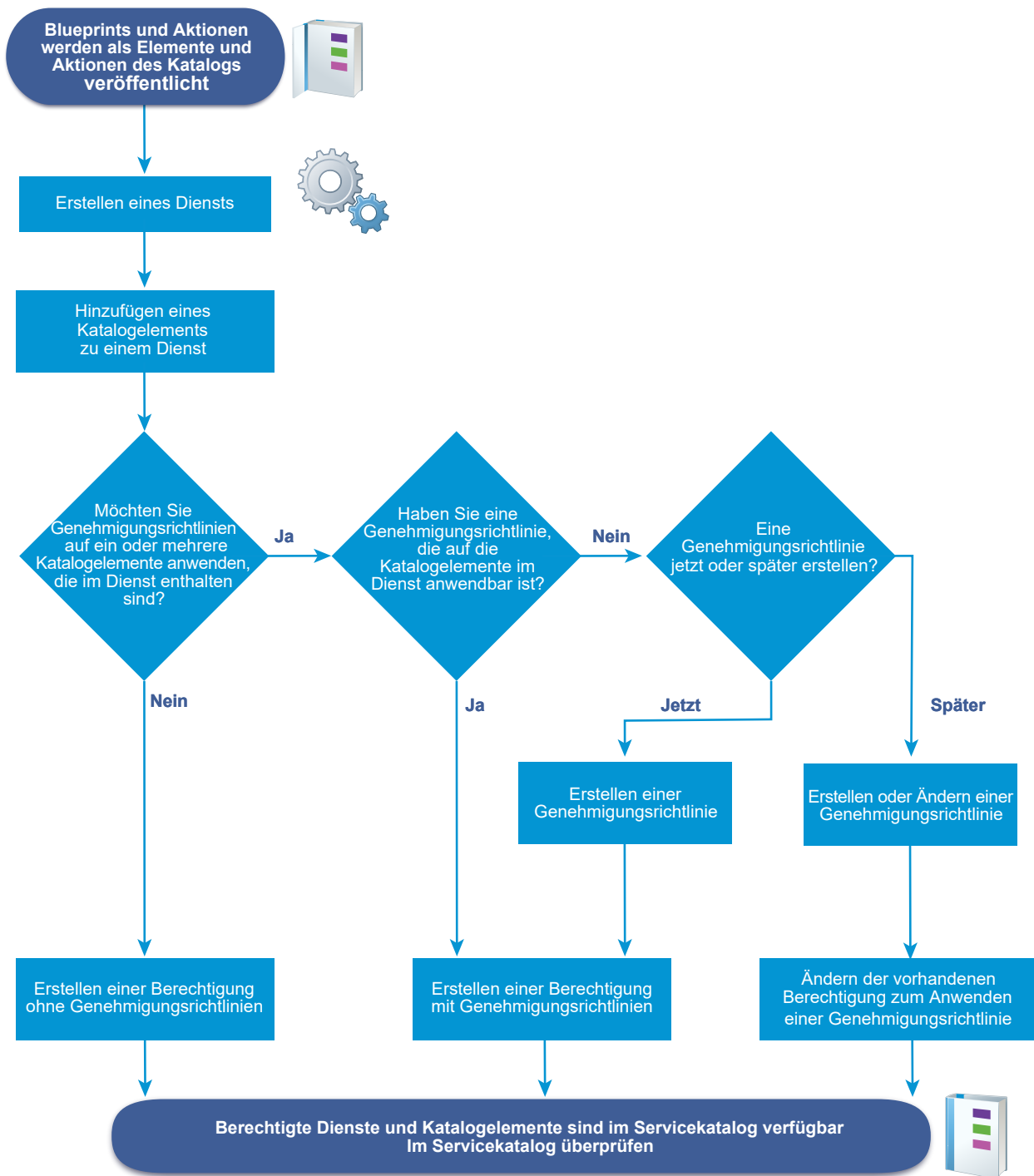
- Validierungsbezeichnung = Maschinendetails validieren
- Aktion auswählen = <Ihr vRealize Orchestrator-Aktionsordner>/validateMachineWithUserForm
- Aktionseingabe
 - CPU = Feld und Anzahl der CPUs
 - Speicher = Feld und Arbeitsspeicher (GB)
 - Speicher = Feld und Speicher (GB)
 - Projekt = Feld und Projekt
- Hervorgehobene Felder
 - Klicken Sie auf **Feld hinzufügen** und wählen Sie **Projekt** aus.

Im Katalog wird Ihrem Katalogbenutzer möglicherweise eine Fehlermeldung ähnlich dem folgenden Beispiel angezeigt.

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 3-69. Konfigurieren der Checkliste für den Servicekatalog

Aufgabe	Erforderliche Rolle	Details
<input type="checkbox"/> Hinzufügen eines Diensts.	Mandantenadministrator oder Katalogadministrator	Siehe Hinzufügen eines Diensts .
<input type="checkbox"/> Hinzufügen eines Katalogelements zu einem Dienst.	Mandantenadministrator oder Katalogadministrator	Siehe Hinzufügen von Katalogelementen zu einem Dienst .
<input type="checkbox"/> Konfigurieren des Katalogelements im Dienst.	Mandantenadministrator oder Katalogadministrator	Siehe Konfigurieren eines Katalogelements .
<input type="checkbox"/> Erstellen und Anwenden von Berechtigungen für das Katalogelement.	Mandantenadministrator oder Business-Gruppenmanager	Siehe Erteilen der Berechtigung für Dienste, Katalogelemente und Aktionen .
<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.	Weitere Informationen finden Sie unter Erstellen einer Genehmigungsrichtlinie .

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 vRealize Automation als **Mandantenadministrator** oder **Katalogadministrator** an.

Verfahren

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
Inaktiv	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 Inaktiv für einen Dienst auswählen, der aktiv und berechtigt ist, wird dieser aus dem Servicekatalog entfernt, bis Sie ihn erneut aktivieren.
Aktiv	(Standard) Für den Dienst und die zugehörigen Katalogelemente kann Benutzern die Berechtigung erteilt werden und sie sind dann im Servicekatalog für diese Benutzer verfügbar.
Gelöscht	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 Diensteinstellungen

Die folgenden Einstellungen liefern Informationen zu den Servicekatalogbenutzern. Diese Einstellungen haben keine Auswirkung auf die Dienstverfügbarkeit.

Option	Beschreibung
Stunden	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.
Besitzer	Geben Sie den Benutzer oder die Benutzergruppe an, der bzw. die der primäre Besitzer des Diensts und der zugehörigen Katalogelemente ist.
Support-Team	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.
Änderungsfenster	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**.

Nächste Schritte

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 vRealize Automation 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](#).

Verfahren

- 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**.

Nächste Schritte

- 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 deaktivieren, wenn Sie Sie vorübergehend aus dem Servicekatalog entfernen möchten, und 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 **Bereitstellungen** 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 **Bereitstellungen** 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 vRealize Automation als **Mandantenadministrator** oder **Katalogadministrator** an.
- Stellen Sie sicher, dass Sie mindestens ein als Katalogelement veröffentlichter Blueprint vorhanden ist. Siehe [Veröffentlichen eines Blueprints](#).

Verfahren

- 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
Symbol	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.
Status	<p>Mögliche Werte sind Aktiv, Inaktiv und Staging.</p> <ul style="list-style-type: none"> ■ Aktiv. 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. ■ Inaktiv. Das Katalogelement ist im Servicekatalog nicht verfügbar. Das Element wird in der Liste der Katalogelemente als zurückgezogen angezeigt. ■ Staging. 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.
Kontingent	<p>Legen Sie fest, wie viele Instanzen ein Benutzer von diesem Katalogelement bereitstellen darf.</p> <p>Wenn der Benutzer diese Zahl überschreitet, wird eine Benachrichtigung auf der Kataloganforderung angezeigt und die Anforderung wird nicht übermittelt.</p>
Dienst	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.

- 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**.

Nächste Schritte

- 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 vRealize Automation als **Mandantenadministrator** oder **Katalogadministrator** an.
- Stellen Sie sicher, dass Sie über mindestens eine veröffentlichte Aktion verfügen. Siehe [Veröffentlichen eines Blueprints](#) und [Veröffentlichen einer Ressourcenaktion](#).

Verfahren

- 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**.

Nächste Schritte

[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 Entwurfzustand 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 einen Dienst, ein Katalogelement oder eine Aktion hinzufügen, gestatten Sie den in der Berechtigung angegebenen Benutzern das Anfordern von bereitstellbaren Elementen im Servicekatalog. 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 Mitglieder in der Business-Gruppe für die Berechtigung angeben.

Informationen zum Erstellen einer Berechtigung, sodass Sie die Interaktionen von Diensten, Katalogelementen und Aktionen mit Genehmigungen verwenden können, finden Sie unter [Erstellen von Berechtigungen](#).

Voraussetzungen

- Melden Sie sich bei vRealize Automation 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 Berechtigungen auf die Elemente im Servicekatalog ohne Genehmigungen erteilen möchten, können Sie die Berechtigung später ändern, um Genehmigungen hinzuzufügen.

Verfahren

- 1 Wählen Sie **Administration > Katalogmanagement > Berechtigungen** aus.
- 2 Klicken Sie auf das Symbol **Neu** (+).
- 3 Konfigurieren Sie die Optionen **Details**.

Details bestimmen, wie die Berechtigung in der Berechtigungsliste angezeigt wird und welche Benutzer Zugriff auf die Elemente im Servicekatalog haben.

Option	Beschreibung
Name und Beschreibung	Informationen zur Berechtigung, die in der Berechtigungsliste angezeigt wird.
Ablaufdatum	Legen Sie das Datum und die Uhrzeit fest, wenn die Berechtigung an einem bestimmten Datum inaktiv werden soll.
Status	<p>Mögliche Werte sind „Aktiv“, „Inaktiv“ und „Gelöscht“.</p> <ul style="list-style-type: none"> ■ Aktiv. Elemente sind im Servicekatalog verfügbar. Diese Option ist verfügbar, wenn Sie Berechtigungen hinzufügen oder bearbeiten. ■ Inaktiv. Elemente sind im Servicekatalog nicht verfügbar. Die Berechtigung wurde aufgrund des Ablaufdatums oder durch einen Benutzer deaktiviert. ■ Gelöscht. Löscht die Berechtigung.
Business-Gruppe	<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 Sie allen Benutzern eine Berechtigung zur Verfügung stellen möchten, benötigen Sie eine Business-Gruppe „All Users“ oder Sie müssen für jede Business-Gruppe Berechtigungen erstellen.</p> <p>Wenn Sie als Business-Gruppenmanager angemeldet sind, können Sie nur Berechtigungen für Ihre Business-Gruppe erstellen.</p>
Benutzer und Gruppen	Wählen Sie Alle Benutzer und Gruppen , um allen Mitgliedern der Business-Gruppe Berechtigungen auf die Katalogelemente und Aktionen zu geben, oder Sie können einzelnen Benutzern oder Gruppen Berechtigungen erteilen. Um eine Berechtigung zu aktivieren, müssen Sie mindestens einen Benutzer einer Business-Gruppe oder eine Gruppe auswählen.

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
Berechtigte Services	<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 dem Dienst später ein Element hinzugefügt wird, wird es dem Servicekatalog für den berechtigten Benutzer hinzugefügt. Berechtigungen können sowohl Dienste als auch einzelne Katalogelemente enthalten.</p>
Berechtigte Katalogelemente und Komponenten	<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.</p> <p>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>

Option	Beschreibung
Berechtigte Aktionen	<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>
Aktionen gelten nur für die in dieser Berechtigung definierten Elemente	<p>Bestimmt, ob die berechtigten Aktionen für alle zutreffenden Dienstkatalogelemente berechtigt sind oder nur die Elemente in dieser Berechtigung.</p> <p>Falls ausgewählt, sind die Mitglieder der Business-Gruppe berechtigt, die Aktionen für die anwendbaren Elemente in dieser Berechtigung durchzuführen. Diese Methode zur Berechtigung der Durchführung von Aktionen ermöglicht Ihnen, die Aktionen für die spezifischen Elemente anzugeben.</p> <p>Ist diese 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**.

Ergebnisse

Wenn der Berechtigungsstatus „Aktiv“ lautet, werden der Dienst und die Elemente zum Servicekatalog hinzugefügt.

Nächste Schritte

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 Chris, ein Mitglied dieser Gruppe, anwenden können.

Tabelle 3-70. Beispielberechtigungen

Berechtigung 1	Berechtigung 2
Business-Gruppe: Finanzen	Business-Gruppe: Finanzen
Benutzer und Gruppen: Buchhaltungsgruppe	Benutzer und Gruppen: Chris
Katalogelement 1: Richtlinie A	Katalogelement 1: Richtlinie C

Chris 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 Chris angewendet.


Tabelle 3-71. 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. Chris ist ein Mitglied der Buchhaltungs-Benutzergruppe. Die Suche nach Chris als berechtigter Benutzer endet bei Berechtigung 1, und die Genehmigungsrichtlinie wird angewendet.	Die Richtlinie C wird angewendet. Die Suche nach Chris als berechtigter Benutzer endet bei Berechtigung 2, und die Genehmigungsrichtlinie wird angewendet.

Voraussetzungen

Melden Sie sich bei vRealize Automation als **Mandantenadministrator** oder **Katalogadministrator** an.

Verfahren

- 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
Aktualisieren	Speichert die Änderungen.
Aktualisieren und schließen	Speichert die Änderungen und schließt das Fenster Elemente priorisieren .

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 3-72. 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
Der Business-Gruppenmanager muss alle VM-Anforderungen genehmigen. Die Genehmigungsrichtlinie muss auf mehrere Business-Gruppen in mehreren Berechtigungen anwendbar sein.	Servicekatalog – Katalogelementanforderung – virtuelle Maschine	Zur Registerkarte „Vor der Genehmigung“ hinzufügen	Wählen Sie „Immer erforderlich“ aus.	Wählen Sie Genehmiger aus der Anforderung bestimmen aus. Wählen Sie die Bedingung Business-Gruppe > Manager > Benutzer > Manager aus. Wählen Sie Jeder kann genehmigen aus.	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.	Wählen Sie Bestimmte Benutzer und Gruppen aus. Wählen Sie die benutzerdefinierten Benutzergruppen des Virtual Infrastructure-Administrators aus. Wählen Sie Jeder kann genehmigen aus.	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 3-72. 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 virtuelle Infrastrukturen zu verwalten und die Preise zu kontrollieren, können Sie zwei Genehmigungsebenen „Vor der Bereitstellung“ hinzufügen, nämlich eine Genehmigung für Maschinenressourcen und eine zweite Genehmigung für den Preis der Maschine pro Tag.	Servicekatalog – Katalogelementanforderung – virtuelle Maschine	Zur Registerkarte „Vor der Genehmigung“ hinzufügen	Ebene 1 Wählen Sie Erforderlich basierend auf Bedingungen aus. Konfigurieren Sie die Bedingungen: CPUs > 6 oder Arbeitsspeicher > 8 oder Speicher > 100 GB.	Wählen Sie Genehmiger aus der Anforderung bestimmen aus. Wählen Sie die Bedingung „Angefordert von > Manager“ aus. Klicken Sie auf Systemeigenschaften und wählen Sie CPUs, Arbeitsspeicher und Speicher aus, damit der Genehmiger den Wert auf ein akzeptables Niveau ändern kann.	Diese Genehmigungsrichtlinie kann in einer Berechtigung verwendet werden, bei der der Manager des anfordernden Benutzers und ein Mitglied der Finanzabteilung die Anforderung genehmigen sollen.	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. Wenn dies nicht der Fall ist, wird die Bedingung für die Ebene 2 ausgewertet. Wenn die Anforderungen mindestens eine der Bedingungen der Ebene 1 überschreiten, muss der Manager die Anforderung genehmigen. Der Manager kann die angeforderten Konfigurationswerte reduzieren und die Anforderung genehmigen oder aber die

Tabelle 3-72. 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
			Ebene 2 Wählen Sie Erforderlich basierend auf Bedingungen aus. Konfigurieren Sie die Bedingung „Preis > 15,00 pro Tag“.	Wählen Sie Bestimmte Benutzer und Gruppen aus. Wählen Sie die benutzerdefinierte Benutzergruppe „Finanzen“ aus. Wählen Sie Jeder kann genehmigen aus.		Anforderung ablehnen.
Für parametrisierte Blueprint-Katalogelemente muss ein Cloud-Administrator Bereitstellungsanforderungen genehmigen, in denen ein vSphere-Maschinenkomponentenprofil von size auf large festgelegt ist.	Servicekatalog – Katalogelementanforderung – virtuelle Maschine	Zur Registerkarte „Vor der Genehmigung“ hinzufügen	Ebene 1 Wählen Sie Erforderlich basierend auf Bedingungen aus. Ebene 2 Wählen Sie Einzelne Bedingung aus. Wählen Sie Komponentenprofil > vSphere-Maschinengröße aus. Konfigurieren Sie die Bedingung „size = large“.	Wählen Sie Bestimmte Benutzer und Gruppen aus. Wählen Sie Benutzer und Gruppen aus, die berechtigt sind, die Anforderung genehmigen. Wählen Sie Jeder kann genehmigen aus.	Diese Genehmigungsrichtlinie kann in einer Berechtigung verwendet werden, in der ein Cloud-Administrator die Bereitstellungsanforderung genehmigen soll.	Wenn der Servicekatalogbenutzer eine virtuelle Maschine anfordert, auf die diese Genehmigung angewendet wurde, muss ein Cloud-Administrator die Anforderung genehmigen, bevor die Maschine bereitgestellt wird.

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
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
Berechtigung 3	Richtlinie A (Genehmigungsrichtlinie „Löschen – Bereitstellung“) für Aktion „Löschen – Bereitstellung“ und Richtlinie B (Richtlinie „Löschen – Virtuelle Maschine“) für Aktion „Löschen – Virtuelle Maschine“	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
		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 3-73. Berechtigungskonfigurationen

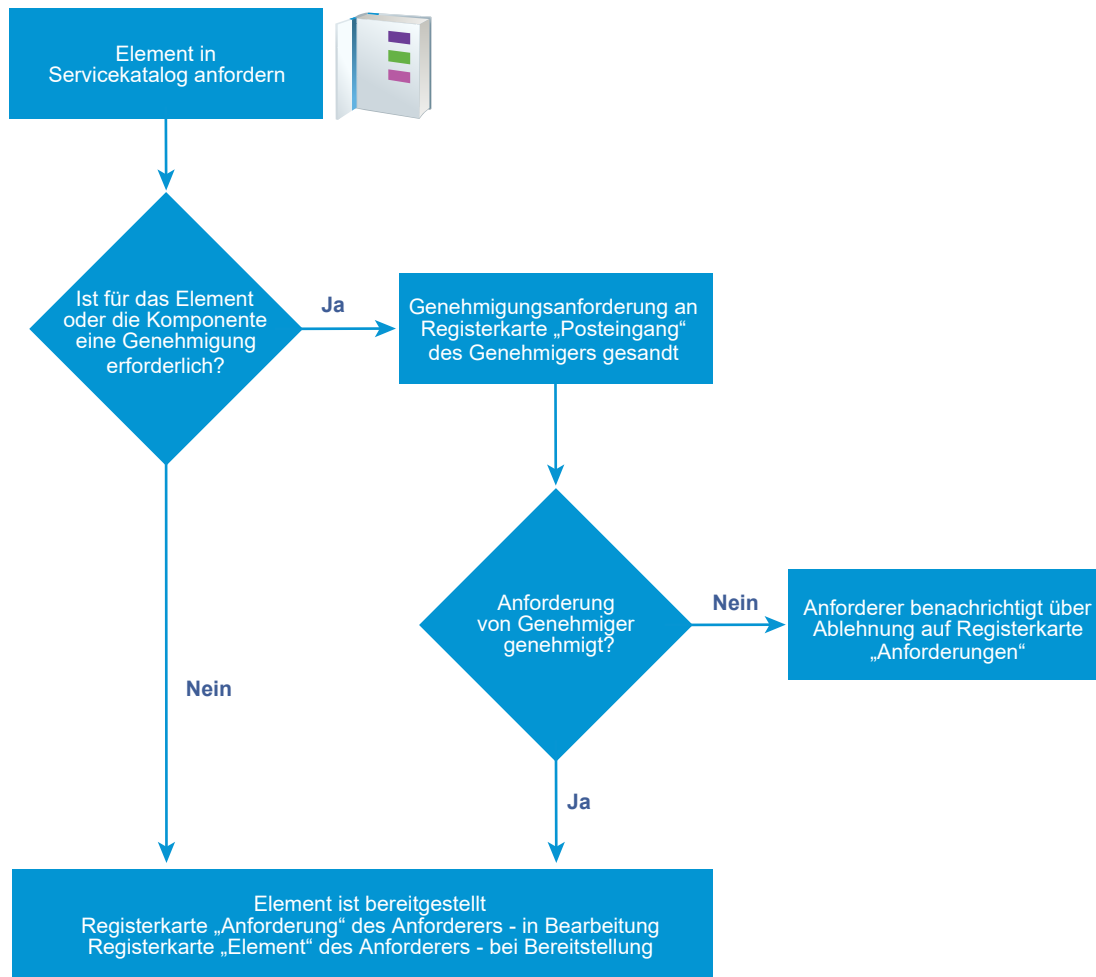
Berechtigungsname	Business-Gruppe	Berechtigter Service	Berechtigtes Element
Berechtigung 1	QE	Testen	Katalogelementanforderung – Virtuelle Maschine angewendet auf Komponente der virtuellen Maschine
Berechtigung 2	QE	Schulung	

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 vRealize Automation als **Mandantenadministrator** oder **Genehmigungsadministrator** an.

Verfahren

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 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 vRealize Automation als **Mandantenadministrator** oder **Genehmigungsadministrator** an.

Verfahren

1 Wählen Sie **Administration > Genehmigungsrichtlinien** aus.

2 Klicken Sie auf das Symbol **Neu** (+).

3 Wählen Sie einen Richtlinientyp oder eine Softwarekomponente aus.

Option	Beschreibung
Richtlinientyp auswählen	<p>Erstellen einer Genehmigungsrichtlinie auf Basis des Richtlinientyps.</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 Konfigurationsoptionen. 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>
Ein Element auswählen	<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 elementspezifisch und können detaillierter sein als die für ein Richtlinientypenelement angegebenen Kriterien.</p>
Liste	<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>

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
Entwurf	Speichert die Genehmigungsrichtlinie in einem bearbeitbaren Status.
Aktiv	Speichert die Genehmigungsrichtlinie in einem schreibgeschützten Status, den Sie in einer Berechtigung verwenden können.
Inaktiv	Speichert die Genehmigungsrichtlinie in einem schreibgeschützten Status, den Sie erst in einer Berechtigung verwenden können, nachdem Sie die Richtlinie aktiviert haben.

Nächste Schritte

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](#).

Wenn Sie eine Richtlinie konfigurieren, die durch eine Lease-Dauer-Anforderung ausgelöst wird, müssen Sie „Immer erforderlich“ als Genehmigungsanforderung auswählen.

Voraussetzungen

[Angabe von Informationen zu Genehmigungsrichtlinien](#).

Verfahren

- 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
Immer erforderlich	Die Genehmigungsrichtlinie wird bei jeder Anforderung ausgelöst.
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>

4 Wählen Sie die Genehmiger aus.

Option	Aktion
Bestimmte Benutzer und Gruppen	Sendet die Genehmigungsanforderung an die ausgewählten Benutzer.
Genehmiger aus der Anforderung bestimmen	Sendet die Genehmigungsanforderung an die Benutzer auf der Grundlage der definierten Bedingung.
Ereignisabonnement verwenden	Verarbeitet die Genehmigungsanforderung auf der Grundlage definierter Ereignisabonnements. Das Workflow-Abonnement muss unter Administration > Ereignisse > Abonnements definiert werden. Die entsprechenden Workflow-Abonnements gelten vor und nach Genehmigung.

5 Geben Sie an, wer die Anforderung oder die Aktion genehmigen muss.

Option	Beschreibung
Jeder kann genehmigen	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.
Alle müssen genehmigen	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**.

Nächste Schritte

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 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 vRealize Automation als **Mandantenadministrator** oder **Genehmigungsadministrator** an.
- [Erstellen einer Genehmigungsebene](#).

Verfahren

- 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
Name	Eingabe des Eigenschaftsnamens.
Bezeichnung	Eingabe der Bezeichnung, die dem Genehmiger im Genehmigungsformular angezeigt wird.
Beschreibung	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**.

Nächste Schritte

- 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 3-74. Optionen für Typen von Genehmigungsrichtlinien

Option	Beschreibung
Richtlinientyp auswählen	<p>Erstellen einer Genehmigungsrichtlinie auf Basis des Richtlinientyps.</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>
Ein Element auswählen	<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 Richtlinientypenelement angegebenen Kriterien.</p>
Liste	<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 Richtlinienotyp aus und klicken Sie auf **OK**.

Tabelle 3-75. 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.
Status	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> ■ Entwurf. Die Genehmigungsrichtlinie kann nicht in Berechtigungen angewendet werden. Nach der Aktivierung einer Richtlinie kann sie nicht mehr auf den Entwurfsstatus zurückgesetzt werden. ■ Aktiv. Die Genehmigungsrichtlinie kann in Berechtigungen angewendet werden. ■ 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.
Richtlinientyp	Zeigt den Anforderungstyp der Genehmigungsrichtlinie an. Wenn Sie ein Katalogelement als Basis für die Genehmigungsrichtlinie ausgewählt haben, wird der zugehörige Anforderungstyp angezeigt.
Element	Zeigt das ausgewählte Katalogelement an. Wenn Sie einen Anforderungstyp als Basis für die Genehmigungsrichtlinie ausgewählt haben, ist dieses Feld leer.
Zuletzt aktualisiert von	Der Name des Benutzers, der Änderungen an der Genehmigungsrichtlinie vorgenommen hat.
Zuletzt aktualisiert am	Das Datum der letzten Änderung an der Genehmigungsrichtlinie.
Vor Genehmigung – Ebene	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.

Tabelle 3-75. 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 3-76. 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 3-76. 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"> ■ Alle folgenden Optionen. Die Genehmigung wird ausgelöst, wenn alle Klauseln zutreffen. Hierbei gibt es einen Booleschen UND-Operator zwischen jeder Klausel. ■ Eine der folgenden Optionen. Die Genehmigungsebene wird ausgelöst, wenn mindestens eine der Klauseln zutrifft. Hierbei gibt es einen Booleschen ODER-Operator zwischen jeder Klausel. ■ Nicht die folgende. Die Genehmigungsebene wird ausgelöst, wenn keine der Klauseln zutrifft. Hierbei gibt es einen Booleschen NICHT-Operator zwischen jeder Klausel.
Genehmiger	Auswählen der Genehmigmethode.

Tabelle 3-76. Optionen für Ebeneninformationen (Fortsetzung)

Option	Beschreibung
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 Jeder kann genehmigen an die Administratorgruppe für die virtuelle Infrastruktur gesendet.</p>
Benutzer aus der Anforderung bestimmen	<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 Business-Gruppe > Verbraucher > Benutzer > Manager aus.</p>
Ereignisabonnement verwenden	<p>Verarbeitet die Genehmigungsanforderung auf der Grundlage definierter Ereignisabonnements.</p> <p>Das Workflow-Abonnement muss unter Administration > Ereignisse > Abonnements definiert werden. Die entsprechenden Workflow-Abonnements gelten vor und nach Genehmigung.</p>

Tabelle 3-76. Optionen für Ebeneninformationen (Fortsetzung)

Option	Beschreibung
Jeder kann genehmigen	<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 Bestimmte Benutzer und Gruppen oder Genehmiger aus der Anforderung bestimmen 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>
Alle müssen genehmigen	<p>Alle der angegebenen Genehmiger müssen genehmigen, bevor die Anforderung verarbeitet wird.</p> <p>Wenn Sie Bestimmte Benutzer und Gruppen oder Genehmiger aus der Anforderung bestimmen 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 Richtlinientyp 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 3-77. Systemeigenschaften-Optionen

Option	Beschreibung
Eigenschaften	<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 Richtlinientyp 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 3-78. Benutzerdefinierte Eigenschaften

Option	Beschreibung
Name	Eingabe des Eigenschaftsnamens.
Bezeichnung	Eingabe der Bezeichnung, die dem Genehmiger im Genehmigungsformular angezeigt wird.
Beschreibung	<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 vRealize Automation als **Mandantenadministrator** oder **Genehmigungsadministrator** an.

Verfahren

- 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
Entwurf	Speichert die Genehmigungsrichtlinie in einem bearbeitbaren Status.
Aktiv	Speichert die Genehmigungsrichtlinie in einem schreibgeschützten Status, den Sie in einer Berechtigung verwenden können.
Inaktiv	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**.

Ergebnisse

Sie haben eine neue Genehmigungsrichtlinie basierend auf einer vorhandenen Genehmigungsrichtlinie erstellt.

Nächste Schritte

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 vRealize Automation als **Mandantenadministrator** oder **Genehmigungsadministrator** an.

Verfahren

- 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**.

Ergebnisse

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.

Nächste Schritte

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 vRealize Automation als **Mandantenadministrator** oder **Genehmigungsadministrator** an.

Verfahren

- 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**.

Ergebnisse

Die Genehmigungsrichtlinie wird gelöscht.

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](#).

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.

Verfahren

- 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
Name	Geben Sie CentOS auf vSphere CPU oder Arbeitsspeicher VM ein.
Beschreibung	Geben Sie Erfordert VI-Admin-Genehmigung für CPU>2 oder Arbeitsspeicher>2048 ein.
Status	Wählen Sie Aktiv 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**.

Ergebnisse

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.

Verfahren

- 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 MySQL tracking approval ein.
Beschreibung	Geben Sie Approval request sent to software manager ein.
Status	Wählen Sie Aktiv 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**.

Ergebnisse

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 Genehmigungsrichtlinien 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.

Verfahren

- 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.

- Klicken Sie auf das Symbol **Aktionen hinzufügen** (+) neben der Überschrift „Berechtigte Aktionen“.
- Wählen Sie die folgenden Aktionen aus.

Name / Typ	Beschreibung
Snapshot erstellen / Virtuelle Maschine	Erstellt einen Snapshot der virtuellen Maschine, einschließlich der installierten Software. Ermöglicht den Entwicklern, Snapshots zu erstellen, auf die sie bei der Entwicklung wiederherstellen können.
Löschen / Bereitstellung	Löscht den gesamten bereitgestellten Blueprint, nicht nur die Maschine. Verwenden Sie diese Aktion, um verwaiste Komponenten zu vermeiden.
Ausschalten / Maschine	Schaltet die virtuelle Maschine aus.
Einschalten / Maschine	Schaltet die virtuelle Maschine ein.
Auf Snapshot wiederherstellen / Virtuelle Maschine	Stellt auf den zuvor erstellten Snapshot wieder her.

- Klicken Sie auf **OK**.

- 7 Klicken Sie auf **Beenden**.

Ergebnisse

Diese Berechtigung ermöglicht es Ihnen, verschiedene Genehmigungen auf unterschiedlichen Blueprint-Komponenten anzufordern.

Nächste Schritte

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.

Anfordern der Maschinenbereitstellung mit einem parametrisierten Blueprint

Beim Anfordern der Maschinenbereitstellung für einen vSphere-Maschinen-Blueprint, der zwecks Einbeziehung der Größen- oder Image-Komponentenprofile entwickelt wurde, geben Sie die Bereitstellungseinstellung anhand der Auswahl eines verfügbaren Wertsatzes an.

Wenn Sie die Bereitstellung aus dem Katalog anfordern, können Sie aus den verfügbaren Wertmengen für die Komponentendienstprofile **Size** und **Image** auswählen. Wenn Sie eine Wertmenge auswählen, werden die entsprechenden Eigenschaftswerte anschließend mit der Anforderung verknüpft.

Der festgelegte Wert des Komponentenprofils wird auf alle vSphere-Maschinen in einem Cluster angewendet.

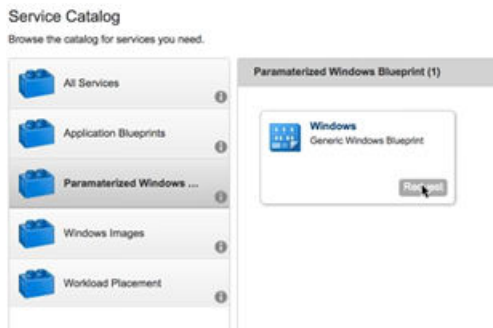
Weitere Informationen zur Konfiguration des Komponentenprofils finden Sie unter [Verstehen und Verwenden der Blueprint-Parametrisierung](#).

Voraussetzungen

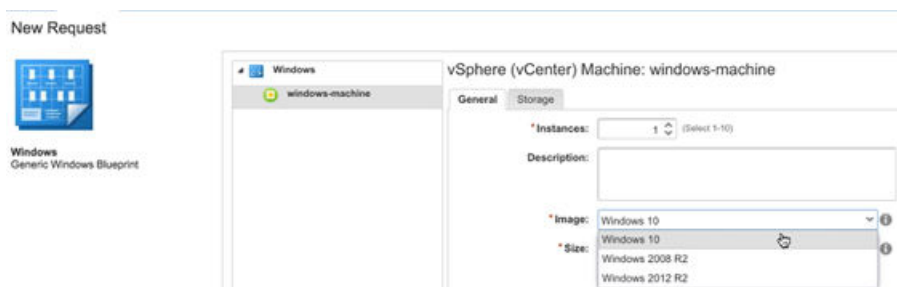
- Definieren Sie Wertsätze für Size- oder Image-Komponentenprofile. Weitere Informationen finden Sie unter und in *Referenz für benutzerdefinierte Eigenschaften*.
- Erstellen Sie einen Blueprint, der eine vSphere-Maschinenkomponente mit einem Image- oder Size-Komponentenprofil enthält. Siehe [Konfigurieren eines Maschinen-Blueprints](#) und [vSphere-Maschinenkomponenteneinstellungen](#).
- Veröffentlichen Sie den Blueprint im Katalog. Siehe [Veröffentlichen eines Blueprints](#).
- Konfigurieren Sie den Blueprint im Katalog. Siehe [Checkliste für die Konfiguration des Servicekatalogs](#) und [Beispiele für Genehmigungsrichtlinien basierend auf dem VM-Richtlinientyp](#).

Verfahren

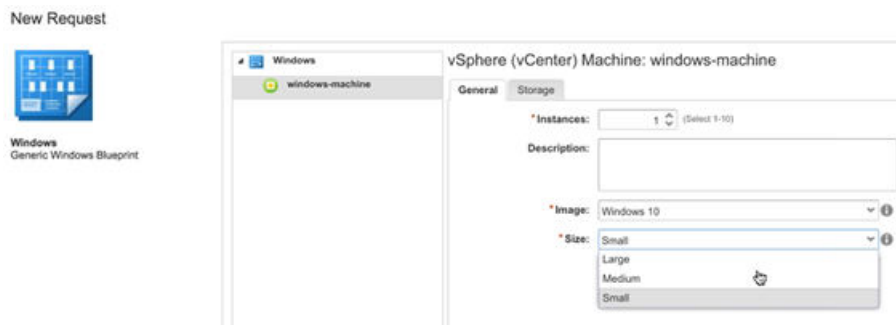
- 1 Klicken Sie auf **Katalog**.
- 2 Wählen Sie den Katalogdienst aus, den Sie anfordern möchten, und klicken Sie auf **Anfordern**.



- 3 Wählen Sie die bereitzustellende vSphere-Maschinenkomponente aus und geben Sie die Anzahl der bereitzustellenden Instanzen an.
- 4 Wählen Sie im Dropdown-Menü **Image** eine Option für den Wertsatz des Image aus.



- 5 Wählen Sie im Dropdown-Menü **Größe** eine Option für den Wertsatz der Größe aus.



- 6 Klicken Sie auf **Übernehmen**.

Nächste Schritte

Die Wertsätze, die Sie für die Size- und Image-Komponentenprofile ausgewählt haben, sind jetzt in den Dropdown-Menüs **Image** und **Größe** auf der Registerkarte **Catalog** im Anforderungsformular für die Katalogbereitstellung verfügbar.

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 vRealize Automation als **Mandantenadministrator** oder **Katalogadministrator** an.
- Veröffentlichen Sie einen Blueprint, um virtuelle „MySQL unter vSphere CentOS“-Maschinen bereitzustellen. Siehe *Installieren und Konfigurieren von vRealize Automation für das Rainpole-Szenario*.
- Wenn Sie Blueprints in einer Entwicklungsumgebung erstellen, importieren Sie Ihren Blueprint in Ihre Produktionsumgebung. Siehe [Exportieren und Importieren von Blueprints und Inhalten](#).

- 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](#).

Verfahren

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.

Verfahren

- 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**.

Ergebnisse

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.

Verfahren

- 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**.

Ergebnisse

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.

Verfahren

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**.

Ergebnisse

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.

Nächste Schritte

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](#).

Verwalten von bereitgestellten Katalogelementen

Sie können implementierte Bereitstellungen, einschließlich Maschinen, Lastausgleichsdienste, Netzwerke und weitere Bereitstellungsressourcen anzeigen und darauf reagieren.

Ausführen von Aktionen für bereitgestellte Ressourcen

Die für eine bereitgestellte Ressource verfügbaren Aktionen sind abhängig vom Ressourcentyp, wie die Aktion konfiguriert und für bereitgestellte Elemente verfügbar gemacht wurde sowie vom Betriebszustand des Elements.

Die konfigurierten Aktionen, die für eine bereitgestellte Maschine oder eine Bereitstellung verfügbar sind, werden im Menü **Aktionen** für die ausgewählte Ressource auf der Registerkarte **Elemente** angezeigt.

Wenn das Element mithilfe eines IaaS-Maschinen-Blueprints bereitgestellt wurde, ist die Liste der verfügbaren Aktionen abhängig von Ihrer Auswahl auf der Registerkarte **Aktionen** für die Maschinentypkomponente zum Zeitpunkt der Erstellung des Blueprints sowie anschließend von den entsprechenden Optionen für den Maschinentyp oder den Maschinenzustand.

Wenn das Element mithilfe eines XaaS-Blueprints bereitgestellt wurde, müssen die Ressourcenaktionen im selben Dienst erstellt, veröffentlicht und gewährt werden, der zur Bereitstellung des Elements verwendet wird. Die Liste der verfügbaren Aktionen ist abhängig vom Elementtyp und dem aktuellen Status des Elements.

Zu den verfügbaren Aktionen für ein Element, das als IaaS-Maschine bereitgestellt wurde, können auch XaaS-Ressourcenaktionen zählen, falls die Aktionen dem Element zugeordnet sind.

Befehle im Menü „Aktion“ für bereitgestellte Ressourcen

Aktionen sind Änderungen, die Sie an bereitgestellten Ressourcen vornehmen können. Mithilfe der vRealize Automation-Aktionen wird der Lebenszyklus der Ressourcen verwaltet.

Zu den Befehlen im Menü **Aktion** für eine bereitgestellte Ressource zählen die Aktionen, die im Blueprint angegeben wurden, und sie können benutzerdefinierte Menüvorgänge umfassen, die von Ihren Servicearchitekten eingerichtet wurden. Die verfügbaren Aktionen sind abhängig davon, wie Ihr Business-Gruppenmanager oder Mandantenadministrator die Berechtigung konfiguriert hat, die die Ressource beinhaltet, für die die Aktionen ausgeführt werden.

Die durch vRealize Automation verwalteten NSX-Objekte sollten nicht außerhalb von vRealize Automation verwaltet werden. Wenn Sie beispielsweise den Mitgliedsport eines bereitgestellten NSX-Lastausgleichsdiensts nicht in vRealize Automation, sondern in NSX ändern möchten, dann beschädigt die NSX-Datenerfassung die Zuordnung zwischen der bereitgestellten Maschine und ihrem ansonsten zugeordneten Mitgliedspool des Lastausgleichsdiensts. Vertikale und horizontale Skalierungsvorgänge führen ebenfalls zu unvorhersehbaren Ergebnissen, wenn der Mitgliedsport eines bereitgestellten Lastausgleichsdiensts außerhalb von vRealize Automation geändert wird.

Die in der folgenden Tabelle aufgeführten Aktionen gelten nicht für alle bereitgestellten Ressourcentypen. Beispielsweise unterstützen einige NSX-Integrationselemente keine der folgenden Aktionen.

Tabelle 3-79. Befehle des Menüs „Aktion“

Aktion	Ressourcentyp	Beschreibung
Pool-IP-Adresse zuweisen	Maschine (OpenStack)	Weist einer OpenStack-Maschine eine Pool-IP-Adresse zu.
Neukonfiguration abbrechen	Maschine	Bricht eine ausgeführte Neukonfigurationsaktion ab.
Lease ändern	Bereitstellung und Maschine	Ändert die Anzahl der Tage, die in der Lease für eine bestimmte Maschine oder für alle in einer Bereitstellung enthaltenen Ressourcen verbleiben. Wenn Sie keinen Wert eingeben, läuft die Lease nicht ab.
NAT-Regeln ändern	NAT-Netzwerk	Sie können neue NAT-Portweiterleitungsregeln hinzufügen, die Reihenfolge von Regeln ändern, vorhandene Regeln bearbeiten oder Regeln löschen. Weitere Informationen finden Sie unter Ändern von NAT-Regeln in einer Bereitstellung .
Besitzer ändern	Bereitstellung	Ändert den Besitzer der Bereitstellung und aller zugehörigen Ressourcen. Nur Business-Gruppenmanager und Supportbenutzer können den Besitzer einer Bereitstellung ändern. Die Maschine muss sich im Zustand „Eingeschaltet“, „Ausgeschaltet“ oder „Aktiv“ befinden, wenn Sie die Aktion „Besitzer ändern“ initiieren. Andernfalls schlägt die Aktion mit der folgenden Meldung fehl: Die Aktion ist für die Maschine ungültig.
Sicherheit ändern	Bereitstellung	Sie können vorhandene NSX-Sicherheitsgruppen und Sicherheits-Tags hinzufügen oder entfernen. Sie können auch bedarfsgesteuerte Sicherheitsgruppen entfernen. Weitere Informationen finden Sie unter Hinzufügen oder Entfernen von Sicherheitselementen in einer Bereitstellung .

Tabelle 3-79. Befehle des Menüs „Aktion“ (Fortsetzung)

Aktion	Ressourcentyp	Beschreibung
Verbinden via VMRC	Maschine	<p>Stellt eine Verbindung zur virtuellen Maschine über eine VMRC 8.x-Anwendung her.</p> <p>Um diese Aktion zu verwenden, muss die VMRC-Anwendung auf dem lokalen System des Servicekatalogbenutzers, der die Aktion ausführt, installiert sein.</p> <p>Anweisungen zur Installation und Verwendung finden Sie in der Dokumentation zu VMware Remote Console. Informationen zum Herunterladen finden Sie unter Herunterladen von VMware Remote Console.</p> <p>VMRC 8.x ersetzt die frühere VMware Remote Console.</p>
Mit Remote-Konsole verbinden	Maschine	<p>Stellt mithilfe von VMware Remote Console eine Verbindung zur ausgewählten Maschine her.</p> <p>Die Konsole für die virtuelle Maschine wird im Browser angezeigt. VMRC 8.x ersetzt die VMware Remote Console.</p>
Verbindungsherstellung mithilfe von Konsolenticket	Maschine (OpenStack und KVM)	<p>Stellt für eine VMware Remote Console-Verbindung mithilfe eines Konsolentickets eine Verbindung zur virtuellen OpenStack- oder KVM-Maschine her.</p>
Verbindungsherstellung mithilfe von ICA	Maschine (Citrix)	<p>Stellt mithilfe von ICA (Independent Computing Architecture) eine Verbindung zur Citrix-Maschine her.</p>
Verbindungsherstellung mithilfe von RDP	Maschine	<p>Stellt mithilfe von Microsoft Remote Desktop Protocol eine Verbindung zur Maschine her.</p>
Verbindungsherstellung mithilfe von SSH	Maschine	<p>Stellt mithilfe von SSH eine Verbindung zur ausgewählten Maschine her.</p> <p>Gemäß der Option Verbindungsherstellung mithilfe von SSH muss der Browser über ein Plug-In verfügen, das SSH unterstützt, z. B. der SSH-Terminalclient „FireSSH“ für Mozilla Firefox und Google Chrome. Wenn das Plug-In vorhanden ist, wird bei Auswahl von Verbindungsherstellung mithilfe von SSH eine SSH-Konsole mit der Aufforderung angezeigt, Administratoranmeldedaten einzugeben.</p> <p>Um diese Option zu verwenden, muss die benutzerdefinierte Eigenschaft <code>Machine.SSH</code> in der Maschinenkomponente des Blueprints in einer Eigenschaftsgruppe oder einer einzelnen benutzerdefinierten Eigenschaft vorhanden und auf „True“ festgelegt sein.</p>

Tabelle 3-79. Befehle des Menüs „Aktion“ (Fortsetzung)

Aktion	Ressourcentyp	Beschreibung
Verbindungsherstellung mithilfe von virtuellem Desktop	Maschine	Stellt mithilfe von Microsoft Virtual Desktop eine Verbindung zur ausgewählten Maschine her.
Snapshot erstellen	Virtuelle Maschine	Erstellt einen Snapshot der virtuellen Maschine. Wenn nur zwei Snapshots für Sie zulässig sind und Sie diese bereits erstellt haben, ist dieser Befehl erst wieder verfügbar, nachdem Sie einen Snapshot gelöscht haben. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer virtuellen Maschine .
Snapshot löschen	Virtuelle Maschine	Löscht einen Snapshot der virtuellen Maschine.

Tabelle 3-79. Befehle des Menüs „Aktion“ (Fortsetzung)

Aktion	Ressourcentyp	Beschreibung
Löschen	Bereitstellung, Maschine und bedarfsgesteuerte Sicherheitsgruppe	<p>Löscht eine bereitgestellte Ressource sofort.</p> <p>Mit Ausnahme von XaaS wird das Löschen von Komponenten einer Bereitstellung nicht empfohlen. Reduzieren Sie die Anzahl der Maschinen in der Bereitstellung mithilfe der vertikalen Skalierung oder löschen Sie die gesamte Bereitstellung.</p> <p>Sie müssen diese Aktion ausführen, um XaaS-Ressourcen zu löschen, selbst wenn sie Teil einer Bereitstellung sind, die von Ihnen gelöscht wird. Andere Ressourcen werden gelöscht, wenn ihre Lease oder ihr Archivierungszeitraum abgelaufen ist.</p> <p>Die Aktion „Löschen“ ist für die folgenden Bereitstellungssituationen nicht verfügbar:</p> <ul style="list-style-type: none"> ■ Bereitstellungen mit physischen Maschinen ■ Bereitstellungen mit einem vorhandenen NSX-Netzwerk oder einer vorhandenen NSX-Sicherheitsressource ■ Bereitstellungen mit einer bedarfsgesteuerten NSX-Lastausgleichsdienstressource <p>Da ein NSX-Lastausgleichsdienst zu einem NSX Edge gehört, wird beim Löschen eines NSX Edge auch die Lastausgleichsdienstressource gelöscht und die Ressourcen werden freigegeben. Wenn</p>

Tabelle 3-79. Befehle des Menüs „Aktion“ (Fortsetzung)

Aktion	Ressourcentyp	Beschreibung
		<p>eine Maschinenschicht mit Lastausgleich gelöscht wird, wird sie aus dem Lastausgleichsdienst-Pool auf dem entsprechenden NSX Edge entfernt.</p> <hr/> <p>Hinweis Die Aktion „Löschen“ gibt möglicherweise selbst dann eine Erfolgsmeldung zurück, wenn sie die Bereitstellung einer Maschine nicht von deren Endpoint entfernen kann, beispielsweise, wenn sich eine vSphere-Maschine auf einem Nicht-vSAN-Datenspeicher befindet und ihre .vmx-Datei beschädigte oder anderweitig ungültige Daten enthält. Sie sollten das Anforderungsprotokoll auf zusätzliche Informationen prüfen, selbst wenn die Meldung der Aktion „Löschen“ angibt, dass der Vorgang erfolgreich war. Das Erzwingen der Löschung einer Maschine in diesem Zustand kann dazu führen, dass sie weiterhin auf dem Endpoint ausgeführt wird, und dies kann zu IP-Konflikten führen. Wenn die Beschädigung auf dem Endpoint (außerhalb von vRealize Automation) behoben wird, können Sie die Aktion „Löschen“ erneut versuchen.</p> <hr/> <p>Business-Gruppen-Administratoren können sich entscheiden, das Löschen einer Bereitstellung zu erzwingen, nachdem eine Löschanforderung fehlgeschlagen ist. „Löschen erzwingen“ weist vRealize Automation an, Fehler beim Löschen einzelner Ressourcen beim Löschen der Bereitstellung zu ignorieren. Weitere Informationen zur Verwendung von „Löschen erzwingen“ finden Sie unter Erzwingen des Löschens einer Bereitstellung nach einer fehlgeschlagenen Löschanforderung.</p> <hr/> <p>Hinweis Speicher und Arbeitsspeicher, die mittels einer Reservierung einer bereitgestellten Maschine zugewiesen sind, werden freigegeben, wenn die Maschine, der der Speicher oder Arbeitsspeicher zugewiesen ist, in vRealize Automation mithilfe der Aktion „Löschen“ gelöscht wird. Der Speicher und der Arbeitsspeicher werden nicht freigegeben, wenn die Maschine auf dem vCenter Server gelöscht wird.</p>

Tabelle 3-79. Befehle des Menüs „Aktion“ (Fortsetzung)

Aktion	Ressourcentyp	Beschreibung
		<p>Wenn Sie eine Bereitstellung löschen, die eine Amazon-Maschinenkomponente enthält, können Sie mehrere EBS-Volumes gleichzeitig löschen, je nachdem, wie die Einstellung Volumes löschen im Blueprint konfiguriert wurde. Weitere Informationen finden Sie unter Einstellungen für Amazon-Maschinenkomponenten.</p> <p>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.</p>
Pool-IP-Adresse zurücknehmen	Maschine (OpenStack)	Entfernt die Pool-IP-Adresse von der OpenStack-Maschine.
Neukonfiguration ausführen	Maschine	Überschreibt eine geplante Neukonfiguration oder führt eine fehlgeschlagene Konfiguration erneut aus bzw. plant diese erneut.
Ablauf	Bereitstellung und Maschine	Beendet die Lease der Bereitstellung oder der Maschine für alle in der Bereitstellung enthaltenen Ressourcen.
Zertifikat exportieren	Maschine	Exportiert das Zertifikat von einer Cloud-Maschine.
Ablauferinnerung	Maschine	Lädt eine Kalenderereignisdatei für das aktuelle Leaseablaufdatum herunter.
VMware Tools installieren	Maschine	Installieren von VMware Tools auf einer virtuellen vSphere-Maschine
Zurücksetzen	Maschine	Schaltet die Maschine aus und wieder ein.
Ausschalten	Maschine	Schaltet die virtuelle Maschine aus, ohne das Gastbetriebssystem herunterzufahren.
Einschalten	Maschine	Schaltet die Maschine ein. Wenn die Maschine angehalten wurde, wird der normale Betrieb an dem Punkt fortgesetzt, an dem die Maschine angehalten wurde.
Neu starten	Maschine	Starten Sie das Gastbetriebssystem auf einer virtuellen vSphere-Maschine neu. VMware Tools muss auf der Maschine installiert sein, damit diese Aktion verwendet werden kann.

Tabelle 3-79. Befehle des Menüs „Aktion“ (Fortsetzung)

Aktion	Ressourcentyp	Beschreibung
Neu konfigurieren	Maschine	<p>Ein Business-Gruppenmanager, Supportbenutzer oder Maschinenbesitzer kann die folgenden Neukonfigurationsaktionen für die ausgewählte virtuelle vSphere-Maschine durchführen:</p> <ul style="list-style-type: none"> ■ Beschreibung ändern ■ Einstellungen für CPU, Arbeitsspeicher, Netzwerk und Festplatten ändern ■ Benutzerdefinierte Eigenschaften und Eigenschaftsgruppen hinzufügen, bearbeiten und löschen ■ Netzwerkadapter für NAT-Portweiterleitungsregeln hinzufügen, bearbeiten, löschen oder deren Reihenfolge ändern ■ Herunterfahren neu konfigurieren ■ Maschinenbesitzer ändern (nur für Business-Gruppenmanager und Supportbenutzer verfügbar) <p>Sie können keine Speicherreservierungsrichtlinie ändern, wenn hierdurch das Speicherprofil auf einer Festplatte geändert wird.</p> <p>Weitere Informationen finden Sie unter Angaben von Einstellungen für die Neukonfiguration von Maschinen und Überlegungen bei der Neukonfiguration.</p> <p>Wenn Sie die Option Updates für vorhandene Bereitstellungen weitergeben auf der Seite Blueprints-Einstellungen im Quell-Blueprint auswählen, wird jede Erhöhung oder Erweiterung in den Mindest- und Maximaleinstellungen für CPU, Arbeitsspeicher oder Speicher im Blueprint auf aktive Bereitstellungen verschoben, die von diesem Blueprint bereitgestellt wurden. Weitere Informationen finden Sie unter Blueprint-Eigenschaftseinstellungen.</p>

Tabelle 3-79. Befehle des Menüs „Aktion“ (Fortsetzung)

Aktion	Ressourcentyp	Beschreibung
Lastausgleichsdienst neu konfigurieren	Bereitstellung	<p>Ein berechtigter Maschinenbesitzer, Supportbenutzer, Mandantenadministrator oder Business-Gruppenmanager kann alle Einstellungen eines virtuellen Servers ändern und virtuelle Server im NSX-Lastausgleichsdienst hinzufügen oder daraus entfernen.</p> <p>Weitere Informationen finden Sie unter Erneutes Konfigurieren eines Lastausgleichsdiensts in einer Bereitstellung.</p> <p>Weitere Informationen zu den Einstellungen für virtuelle Server im Lastausgleichsdienst finden Sie unter Hinzufügen einer Komponente für den Lastausgleichsdienst nach Bedarf.</p>
VDI registrieren	Virtuelle Maschine (XenServer)	Registriert das virtuelle Festplatten-Image auf XenServer-Komponenten.
Erneut bereitstellen	Maschine	<p>Löscht die Maschine und startet dann den Bereitstellungsworkflow, um eine Maschine mit demselben Namen zu erstellen.</p> <p>Wenn Sie die erneute Bereitstellung einer Maschine anfordern, zeigt vRealize Automation aufgrund eines bekannten Problems möglicherweise den Status für die erneute Bereitstellung im Katalog als „Vollständig“ an, obwohl der Status eigentlich „In Bearbeitung“ lautet. Nachdem Sie die erneute Bereitstellung einer Maschine angefordert haben, können Sie mithilfe der folgenden Befehlsabfolgen den Status der erneut bereitgestellten Maschine überprüfen:</p> <ul style="list-style-type: none"> ■ Infrastruktur > Verwaltete Maschinen ■ Elemente > Elementdetails ■ Administration > Ereignisse > Ereignisprotokolle <p>Hinweis Sie können eine Amazon-Maschine nicht erneut bereitstellen.</p> <p>Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel „Reprovisioned machine tasks ... (2065873)“ unter http://kb.vmware.com/kb/2065873.</p>
Fortsetzen	Bereitstellung	Wenn eine Bereitstellung aufgrund von vorübergehenden Umgebungs- bzw. Infrastrukturproblemen, Zeitüberschreitungen oder anderen lokalen Problemen fehlschlägt, können Sie den Bereitstellungsprozess fortsetzen, anstatt eine neue Bereitstellungsanforderung zu erstellen.

Tabelle 3-79. Befehle des Menüs „Aktion“ (Fortsetzung)

Aktion	Ressourcentyp	Beschreibung
Snapshot wiederherstellen	Virtuelle Maschine	Stellt einen vorherigen Snapshot der Maschine wiederher. Es muss ein Snapshot vorhanden sein, damit Sie diese Aktion ausführen können.
Vertikal skalieren	Bereitstellung	<p>Löschen Sie nicht benötigte Instanzen von Maschinen in Ihrer Bereitstellung, um eine Anpassung an die verringerten Kapazitätsanforderungen vorzunehmen. Maschinenkomponenten und alle ggf. darauf installierten Softwarekomponenten werden gelöscht. Abhängige Softwarekomponenten sowie Netzwerk- und Sicherheitskomponenten werden für die neue Bereitstellungsconfiguration aktualisiert. XaaS-Komponenten sind nicht skalierbar und werden bei Skalierungsvorgängen nicht aktualisiert.</p> <p>Sie können versuchen, teilweise erfolgreiche Skalierungsvorgänge zu reparieren, indem Sie die Bereitstellung erneut skalieren. Es ist jedoch nicht möglich, eine Bereitstellung auf die aktuelle Größe zu skalieren, und bei der Reparatur einer teilweise erfolgreichen Skalierung auf diese Weise wird die Zuteilung der nicht zugeordneten Ressourcen nicht aufgehoben. Sie können den Bildschirm mit den Ausführungsdetails zu der Anforderung anzeigen und feststellen, welche Aufgaben für welche Knoten fehlgeschlagen sind. Dies erleichtert die Entscheidung, ob die teilweise erfolgreiche Skalierung durch einen erneuten Skalierungsvorgang repariert werden soll. Fehlgeschlagene und teilweise erfolgreiche Skalierungsvorgänge haben keine Auswirkungen auf die Funktionalität Ihrer ursprünglichen Bereitstellung und Sie können während der Fehlerbehebung Ihre Katalogelemente weiterverwenden.</p>

Tabelle 3-79. Befehle des Menüs „Aktion“ (Fortsetzung)

Aktion	Ressourcentyp	Beschreibung
Horizontal skalieren	Bereitstellung	<p>Stellen Sie weitere Maschineninstanzen in Ihrer Bereitstellung zur Verfügung, um eine Anpassung an die zunehmenden Kapazitätsanforderungen vorzunehmen. Maschinenkomponenten und alle ggf. darauf installierten Softwarekomponenten werden bereitgestellt. Abhängige Softwarekomponenten sowie Netzwerk- und Sicherheitskomponenten werden für die neue Bereitstellungskonfiguration aktualisiert. XaaS-Komponenten sind nicht skalierbar und werden bei Skalierungsvorgängen nicht aktualisiert.</p> <p>Sie können versuchen, teilweise erfolgreiche Skalierungsvorgänge zu reparieren, indem Sie die Bereitstellung erneut skalieren. Es ist jedoch nicht möglich, eine Bereitstellung auf die aktuelle Größe zu skalieren, und bei der Reparatur einer teilweise erfolgreichen Skalierung auf diese Weise wird die Zuteilung der nicht zugeordneten Ressourcen nicht aufgehoben. Sie können den Bildschirm mit den Ausführungsdetails zu der Anforderung anzeigen und feststellen, welche Aufgaben für welche Knoten fehlgeschlagen sind. Dies erleichtert die Entscheidung, ob die teilweise erfolgreiche Skalierung durch einen erneuten Skalierungsvorgang repariert werden soll. Fehlgeschlagene und teilweise erfolgreiche Skalierungsvorgänge haben keine Auswirkungen auf die Funktionalität Ihrer ursprünglichen Bereitstellung und Sie können während der Fehlerbehebung Ihre Katalogelemente weiterverwenden.</p>
Herunterfahren	Maschine	Führt das Gastbetriebssystem herunter und schaltet die Maschine aus. VMware Tools muss auf der Maschine installiert sein, damit diese Aktion verwendet werden kann.
Anhalten	Maschine	Hält die Maschine an, sodass sie nicht verwendet werden kann und keine Systemressourcen außer dem verwendeten Speicher verbraucht.
Registrierung aufheben	Maschine	Entfernt die Maschine aus der Bestandsliste, ohne sie zu löschen. Nicht registrierte Maschinen können nicht verwendet werden.

Tabelle 3-79. Befehle des Menüs „Aktion“ (Fortsetzung)

Aktion	Ressourcentyp	Beschreibung
Registrierung aufheben	Netzwerk	Entfernt das Netzwerk aus der Bestandsliste, ohne es zu löschen. Nicht registrierte Netzwerke können nicht verwendet werden.
Registrierung von VDI aufheben	Virtuelle Maschine (XenServer)	Hebt die Registrierung des virtuellen Festplatten-Images auf XenServer-Komponenten auf.

Konfigurieren eines Metrikanbieters

Sie können für vRealize Automation die Verwendung von Systemzustands- und Ressourcenmetriken von vRealize Operations Manager für virtuelle vSphere-Maschinen konfigurieren.

Weitere Informationen zu Systemzustand-Badges und Metriken von vRealize Operations Manager finden Sie in der Dokumentation zu vRealize Operations Manager.

Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator**, **Business-Gruppenmanager** oder **Maschinenbesitzer** an.
- Erstellen Sie ein vRealize Operations Manager-Benutzerkonto mit Abfragerechten für Ansichts- und Ressourcenmetriken für alle vSphere-Server, die Sie in vRealize Automation integrieren.
- Erstellen Sie vRealize Operations Manager-Adapterinstanzen für alle vSphere-Server, die Sie als Endpoints in vRealize Automation hinzufügen. Informationen zum Erstellen von Adapterinstanzen finden Sie in der Dokumentation zu vRealize Operations Manager.

Verfahren

- 1 Wählen Sie **Administration > Rückforderung > Metrikanbieter** aus.
- 2 Wählen Sie einen Metrikanbieter aus.

Option	Beschreibung
(Standard) vRealize Automation-Metrikanbieter	Wenn Sie nicht über eine vRealize Operations Manager-Instanz verfügen, stellt vRealize Automation grundlegende Maschinenmetriken bereit.
vRealize Operations Manager-Endpoint	Liefert Verbindungsinformationen für die vRealize Operations Manager-Instanz, die Sie als Metrikanbieter für virtuelle vSphere-Maschinen verwenden möchten.

- 3 Klicken Sie auf **Testverbindung**.
- 4 Klicken Sie auf **Speichern**.

Ergebnisse

Mandantenadministratoren, Maschinenbesitzer und Business-Gruppenmanager der Gruppe, in der sich die Maschine befindet, können Integritäts-Badges und -warnungen auf den Detailseiten des Elements für virtuelle vSphere-Maschinen anzeigen. Darüber hinaus können sie vRealize Operations Manager-Metriken und Integritäts-Badges anzeigen, wenn sie auf der Rückforderungsseite nach dem Plattformtyp vSphere filtern.

Nächste Schritte

[Senden von Rückforderungsanfragen.](#)

Senden von Rückforderungsanfragen

Sie können Bereitstellungen anzeigen und verwalten und Rückforderungsanfragen an Bereitstellungsbesitzer senden. Eine Rückforderungsanfrage gibt eine neue Leasedauer in Tagen, die festgelegte Zeitdauer für die Antwort des Bereitstellungsbesitzers sowie die als Ziel für die Rückforderung verwendeten Maschinen an.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Mandantenadministrator** an.
- (Optional) Informationen zum Anzeigen von Integritäts-Badges oder von durch vRealize Operations Manager bereitgestellte Metriken finden Sie unter [Konfigurieren eines Metrikanbieters](#).

Verfahren

- 1 Wählen Sie **Verwaltung > Rückforderung > Bereitstellungen**.

2 Suchen Sie nach VM-Bereitstellungen, die Ihren Suchkriterien entsprechen.

Sie müssen Plattformtyp vSphere auswählen, um durch vRealize Operations Manager angegebene Metriken anzuzeigen.

- a Klicken Sie auf den Pfeil nach unten **Erweiterte Suche**, um das Suchfeld zu öffnen.
- b Führen Sie die Eingabe oder Auswahl von mindestens einem Suchwert durch.

Option	Aktion
Der Name der virtuellen Maschine enthält	Geben Sie mindestens ein Zeichen im Textfeld ein, um übereinstimmende Namen von virtuellen Maschinen zu finden.
Der Besitzername enthält	Geben Sie im Textfeld einen Namen ein, um übereinstimmende Besitzernamen zu finden.
Der Business-Gruppenname enthält	Geben Sie im Textfeld einen Namen ein, um übereinstimmende Business-Gruppennamen zu finden.
Plattformtyp	Wählen Sie einen Plattformtyp aus dem Dropdown-Menü aus. Wählen Sie vSphere aus, um durch vRealize Operations Manager angegebene Metriken anzuzeigen. Erforderlich für vRealize Operations Manager.
Betriebszustand	Wählen Sie aus dem Dropdown-Menü einen Wert für den Betriebszustand aus, um virtuelle Maschinen mit einem übereinstimmenden Betriebszustand zu finden.
Ablaufdatum zwischen	Klicken Sie auf die Kalendersymbole und wählen Sie ein Start- und Enddatum aus, um Ablaufdaten innerhalb dieses Zeitraums zu finden.
CPU-Auslastung	Wählen Sie aus dem Dropdown-Menü einen Wert aus, um virtuelle Maschinen mit hoher CPU-Auslastung (über 80 %), niedriger CPU-Auslastung (unter 5 %) oder keiner CPU-Auslastung (kein Wert) zu finden. Wenn Sie vRealize Operations Manager-Metriken abfragen, können Sie diesen Filter für die Abfrage nicht verwenden, und Sie können Ergebnisse nicht nach der CPU-Auslastung anordnen.
Arbeitsspeichernutzung	Wählen Sie aus dem Dropdown-Menü einen Wert aus, um virtuelle Maschinen mit hoher Arbeitsspeicherauslastung (über 80 %), niedriger Arbeitsspeicherauslastung (unter 10 %) oder keiner Arbeitsspeicherauslastung (kein Wert) zu finden. Wenn Sie vRealize Operations Manager-Metriken abfragen, können Sie diesen Filter für die Abfrage nicht verwenden, und Sie können Ergebnisse nicht nach der Arbeitsspeicherauslastung anordnen.
Festplattennutzung	Wählen Sie aus dem Dropdown-Menü einen Wert aus, um virtuelle Maschinen mit geringer Festplattennutzung (weniger als 2 KB pro Sekunde) oder keiner Festplattennutzung (kein Wert) zu finden. Wenn Sie vRealize Operations Manager-Metriken abfragen, können Sie diesen Filter für die Abfrage nicht verwenden, und Sie können Ergebnisse nicht nach der Festplattennutzung anordnen.
Netzwerknutzung	Wählen Sie aus dem Dropdown-Menü einen Wert aus, um virtuelle Maschinen mit geringer Netzwerknutzung (weniger als 1 KB pro Sekunde) oder keiner Netzwerknutzung (kein Wert) zu finden.

Option	Aktion
	Wenn Sie vRealize Operations Manager-Metriken abfragen, können Sie diesen Filter für die Abfrage nicht verwenden, und Sie können Ergebnisse nicht nach der Netzwerknutzung anordnen.
Komplexe Metrik	<p>Wählen Sie aus dem Dropdown-Menü einen Wert aus, um virtuelle Maschinen basierend auf komplexen Metriken zu finden. Wählen Sie z. B. „Im Leerlauf“ aus, um Maschinen zu finden, deren Werte für CPU-Auslastung, Netzwerknutzung, Arbeitsspeicherauslastung und Festplattennutzung allesamt unter 20 % liegen.</p> <p>Sie können diesen Filter nicht verwenden, wenn Sie vRealize Operations Manager-Metriken abfragen.</p>

c Klicken Sie auf das Suchsymbol (.

- 3 Wählen Sie auf der Seite „Bereitstellungen“ eine oder mehrere Maschinen aus, deren übergeordnete Bereitstellung zurückgewonnen werden soll.

Nur auf der aktuellen Ergebnisseite sichtbare ausgewählte Maschinen werden zurückgewonnen.

- 4 Klicken Sie auf **Rückforderung**.

Die Bereitstellungen, die auf der aktuellen Seite ausgewählte virtuelle Maschinen enthalten, sind in der Anforderung enthalten.

Hinweis Auf der Seite „Rückforderungsbereitstellung“ können Maschinen aufgelistet werden, die für eine Rückforderung nicht verfügbar sind, wie z. B. Maschinen, deren Lease abgelaufen ist. Wenn Sie eine Maschine angeben, die für eine Rückforderung nicht verfügbar ist, erhalten Sie folgende Fehlermeldung:

```
Selection Error: Virtual machine name is not in valid state for reclamation.
```

- 5 Geben Sie die Dauer für die neue Lease im Textfeld **Neue Leasedauer (Tage)** ein.

Die minimale Dauer beträgt 1 Tag, die maximale Dauer 365 Tage und die Standarddauer 7 Tage.

- 6 Geben Sie im Textfeld **Warten vor Leaseerzwingung (Tage)** die Anzahl von Tagen ein, innerhalb derer der Bereitstellungsbesitzer auf die Rückforderungsanfrage antworten muss.

Nach Ablauf dieser Zeit erhält die Bereitstellung eine neue Lease mit der neuen Leasedauer. Die minimale Wartezeit beträgt 1 Tag, die maximale Wartezeit 365 Tage und die Standardwartezeit 3 Tage.

- 7 Geben Sie in das Textfeld **Grund für die Anforderung** einen Grund für die Anforderung ein.

- 8 Klicken Sie auf **Übernehmen**.

- 9 Klicken Sie auf **OK**.

Ergebnisse

Wenn Sie eine Rückforderungsanfrage senden, wird sie im Posteingang des Bereitstellungsbesitzers angezeigt. Wenn der Besitzer nicht innerhalb der erforderlichen Anzahl von Tagen auf die Anforderung reagiert, erhält die Bereitstellung eine neue Lease mit der angegebenen Dauer, es sei denn, die aktuelle Lease ist kürzer. Wenn der Besitzer bei der Rückforderungsanfrage auf **Verwendetes Objekt** klickt, bleibt die Lease der Bereitstellung unverändert. Wenn der Besitzer auf **Zur Rückforderung freigeben** klickt, läuft die Bereitstellungs-Lease sofort ab.

Nächste Schritte

[Verfolgen von Rückforderungsanfragen.](#)

Verfolgen von Rückforderungsanfragen

Sie können den aktuellen Status von Rückforderungsanfragen und andere Details verfolgen.

Folgende Alternativen stehen zur Verfügung, um eine neu eingereichte Rückforderungsanfrage zu überprüfen:

- Klicken Sie auf die Registerkarte **Posteingang** und wählen Sie **Rückforderungsanfragen** aus, um Informationen zu Rückforderungsanfragen anzuzeigen.
- Klicken Sie auf die Registerkarte **Rückforderungsanfragen** und sehen Sie sich die Liste der neu eingereichten Anfragen an.
- Klicken Sie auf die Registerkarte **Elemente** und wählen Sie **Bereitstellungen**, um die jüngsten Bereitstellungsänderungen anzuzeigen.

Voraussetzungen

Melden Sie sich bei vRealize Automation als **Mandantenadministrator** an.


Verfahren

- 1 Wählen Sie **Administration > Rückforderung > Rückforderungsanfragen** aus.

2 Finden Sie die virtuellen Maschinen, die Ihren Suchkriterien entsprechen.

- Klicken Sie auf den Pfeil nach unten **Erweiterte Suche**, um das Suchfeld zu öffnen.
- Führen Sie die Eingabe oder Auswahl von mindestens einem Suchwert durch.

Option	Aktion
Der Name der virtuellen Maschine enthält	Geben Sie mindestens ein Zeichen im Textfeld ein, um übereinstimmende Namen von virtuellen Maschinen zu finden.
Der Besitzername enthält	Geben Sie mindestens ein Zeichen im Textfeld ein, um übereinstimmende Besitzernamen zu finden.
Anforderungsgrund enthält:	Geben Sie mindestens ein Zeichen im Textfeld ein, um einen übereinstimmenden Anforderungsgrund zu finden.
Anforderungsstatus	Wählen Sie aus dem Dropdown-Menü einen Wert für den Anforderungsstatus aus, um virtuelle Maschinen mit einem übereinstimmenden Anforderungsstatus zu finden.

- Klicken Sie auf das Symbol **Suchen** () oder drücken Sie die Eingabetaste, um die Suche zu starten.
- Klicken Sie auf den Pfeil nach oben **Erweiterte Suche**, um das Suchfeld zu schließen.

3 (Optional) Klicken Sie auf **Daten aktualisieren**, um die Anzeige der Rückforderungsanfragen zu aktualisieren.

Ändern der Reservierung einer verwalteten Maschine

Sie können die Einstellung für Reservierung oder Speicher für eine verwaltete Maschine ändern. Dies ist hilfreich, wenn eine Maschine in einen neuen Speicherpfad verschoben wird, der in der aktuellen Reservierung nicht verfügbar ist. Für die Bereitstellung einer einzelnen Maschine können Sie auch die Business-Gruppe für diese Maschine ändern.

Sie können eine Maschine in einer einzelnen Maschinenbereitstellung in eine andere Business-Gruppe verschieben, wenn der Maschinenbesitzer ein Mitglied der Ziel-Business-Gruppe ist. Zum Ändern der Einstellung für die Business-Gruppe müssen Sie ein Business-Gruppenmanager der ursprünglichen Business-Gruppe und der Ziel-Business-Gruppe sein.

Hinweis Wenn der Maschine eine Reservierungsrichtlinie zugewiesen ist, können Sie deren Business-Gruppe nicht ändern.

Sie können zusätzliche Reservierungen für die verknüpfte Computing-Ressource mithilfe der Menüoptionen **Administration > Computing-Ressource** erstellen.

Speicher und Arbeitsspeicher, die mittels einer Reservierung einer bereitgestellten Maschine zugewiesen sind, werden freigegeben, wenn die Maschine, der der Speicher oder Arbeitsspeicher zugewiesen ist, in vRealize Automation mithilfe der Aktion „Löschen“ gelöscht wird. Der Speicher und der Arbeitsspeicher werden nicht freigegeben, wenn die Maschine auf dem vCenter Server gelöscht wird.

Sie können beispielsweise Reservierungen, die Maschinen in einer vorhandenen Bereitstellung zugeordnet sind, nicht löschen. Wenn Sie bereitgestellte Maschinen manuell im vCenter Server verschieben oder löschen, erkennt vRealize Automation die bereitgestellten Maschinen weiterhin als aktiv und verhindert das Löschen von zugeordneten Reservierungen.

Wenn durch Änderung der Reservierung eine Maschine in vCenter Server in einen neuen Speicherpfad verschoben wird, der nicht zur Reservierung dieser Maschine in vRealize Automation gehört, stellen Sie sicher, dass das Ziel oder der neue Speicherpfad in der Zielreservierung der Maschine ausgewählt ist, bevor Sie die Reservierung der Maschine ändern.

Voraussetzungen

Melden Sie sich bei vRealize Automation als **Fabric-Administrator** an.

Verfahren

- 1 Wählen Sie **Infrastruktur > Verwaltete Maschinen** aus.
- 2 Suchen Sie die Maschine mit der zu ändernden Reservierung.
- 3 Klicken Sie im Dropdown-Menü auf **Reservierung ändern**.
 Sie können Informationen zur verwalteten Maschine anzeigen, wie z. B. den zugeordneten Blueprint und die Computing-Ressource, indem Sie im Dropdown-Menü auf **Anzeigen** klicken.
- 4 (Optional) Wählen Sie aus dem Dropdown-Menü **Business-Gruppe** eine Business-Gruppe aus.
- 5 (Optional) Wählen Sie aus dem Dropdown-Menü **Reservierung** eine Reservierung aus.
- 6 (Optional) Wählen Sie aus dem Dropdown-Menü **Speicher** eine Speicherrichtlinie aus.
- 7 Klicken Sie auf **OK**.

Funktionsweise der Aktion „Fortsetzen“

Sie können die Aktion „Fortsetzen“ bei fehlgeschlagenen Bereitstellungen verwenden, um die Bereitstellung ab dem Zeitpunkt des Ausfalls und unter bestimmten Umständen neu zu starten. Wenn aktiviert, ist die Aktion „Fortsetzen“ für fehlgeschlagene Bereitstellungsanforderungen oder entsprechende Aktionen verfügbar.

Um Bereitstellungsanforderungen fortzusetzen, müssen Sie die Eigenschaft „_debug_deployment = true custom“ für den Blueprint hinzufügen. Standardmäßig werden fehlgeschlagene Bereitstellungen zurückgesetzt und bereinigt, sodass die Ressourcen zurückgewonnen werden. Eigenschaft „_debug_deployment = true custom“ behält die Bereitstellung zum Zeitpunkt des Ausfalls bei und ermöglicht, sofern unterstützt und basierend auf der Funktionsweise, eine Fortsetzungsaktion. Wenn Sie die Fortsetzungsaktion nur für die unterstützten Aktionen verwenden, müssen Sie die Eigenschaft „_debug_deployment“ nicht aktivieren.

Weitere Informationen zu „_debug_deployment“ finden Sie unter *Referenz für benutzerdefinierte Eigenschaften*.

Um „Fortsetzen“ für eine Bereitstellungsanforderung oder für die verfügbaren Aktionen zu verwenden, berechtigen Sie die Benutzer zur Aktion „Fortsetzen“. Siehe [Erteilen der Berechtigung für Dienste, Katalogelemente und Aktionen](#).

Sie können Benutzer für diese Bereitstellungsaktivitäten zur Aktion „Fortsetzen“ berechtigen.

- Bereitstellungsanforderungen
- Aktion „Fortsetzen“
- Aktion „Vertikal skalieren“
- Aktion „Horizontal skalieren“
- Aktion löschen

Einschränkungen für die Aktion „Fortsetzen“

Wenn Sie entscheiden, ob Sie „Fortsetzen“ verwenden können, anstatt eine neue Instanz eines Blueprints anzufordern, beachten Sie die Einschränkungen.

- Der Blueprint kann ab dem Zeitpunkt der Anforderung nicht mehr geändert werden.

Zum Zeitpunkt der Anforderung wird der Kataloganforderung eine unveränderbare Version des Blueprints zugeordnet. Diese statische Version enthält alle Spezifikationen, einschließlich Attribute, benutzerdefinierte Eigenschaften, Einstellungen usw., wie sie zu Beginn der Bereitstellung verwendet wurden. Wenn Sie einen ausfallerzeugenden Fehler in Ihrem Blueprint haben, funktioniert die Fehlerbehebung und dann die Verwendung der Aktion „Fortsetzen“ nicht, da sie sich auf die Version bezieht, die mit der Anforderung verknüpft ist. In diesem Szenario müssen Sie eine neue Instanz bereitstellen.

Beispiele

- Blueprint A verlangt 5 GB RAM, aber die Anforderung schlägt fehl, weil Sie nur für 3 GB reserviert haben. Wenn Sie den Blueprint auf nur 3 GB aktualisieren und dann „Fortsetzen“ ausführen, schlägt die Aktion „Fortsetzen“ fehl. Wenn „Fortsetzen“ ausgeführt wird, prüft es die ursprüngliche Anforderung und sucht immer noch nach 5 GB. Wenn Sie jedoch die Systemreservierung für die Business-Gruppe auf 5 GB erhöhen und „Fortsetzen“ ausführen, ist die Aktion „Fortsetzen“ erfolgreich.
- Wenn Sie Blueprint B anfordern, der eine benutzerdefinierte Gast-Spezifikation enthält, schlägt die Aktion fehl. Die Untersuchung ergab, dass die benutzerdefinierte Gast-Spezifikation auf Ihrer vCenter Server-Instanz umbenannt wurde. Wenn Sie den Blueprint mit dem neuen Namen aktualisieren und „Fortsetzen“ ausführen, schlägt die Aktion fehl. Sie haben den Blueprint aktualisiert, aber die ursprüngliche Version wird für die Aktion „Fortsetzen“ verwendet. Wenn der neue Name derjenige ist, den Sie in Zukunft verwenden möchten, stellen Sie eine neue Instanz des Blueprints bereit, anstatt „Fortsetzen“ zu verwenden. Andernfalls müssen Sie den Namen der benutzerdefinierten Gast-Spezifikation auf der vCenter Server-Instanz wieder in den Namen ändern, der von der ursprünglichen Version erwartet wird, und „Fortsetzen“ ausführen. Wenn Sie nicht möchten, dass die nächste Bereitstellungsanforderung fehlschlägt, vergessen Sie nicht, den Blueprint mit der korrekten benutzerdefinierten Gast-Spezifikation zu aktualisieren.

„Fortsetzen“ funktioniert, wenn Sie die Zielbereitstellungsumgebung aktualisieren können, um die Blueprint-Spezifikationen so zu unterstützen, wie sie zum Zeitpunkt der Anforderung vorhanden waren.

- Der Wiederholungsversuch ist erst ab dem Zeitpunkt des Ausfalls möglich.

Die Aktion „Fortsetzen“ versucht, die Komponentenaufgaben ab dem Zeitpunkt des Ausfalls erneut durchzuführen. Es wird nicht die gesamte Bereitstellungsanforderung erneut ausgeführt.

Beispiele

- Blueprint C erstellt eine virtuelle Maschine für Anwendungen und eine virtuelle Maschine für Datenbanken. Die Datenbank-VM ist erfolgreich installiert, aber die Bereitstellung schlägt auf der Anwendungs-VM fehl. Wenn Sie die Aktion „Fortsetzen“ ausführen, wird nur die VM-Bereitstellung der Anwendung erneut versucht.

Wenn eine Komponente als „Fehlgeschlagen“ markiert ist, wird sie so behandelt, als ob sie nie ausgeführt worden wäre. Wenn die Installation während der Konfigurationsphase auf der Datenbank-VM fehlschlägt, z. B. aufgrund eines Skriptfehlers, aber die Datenbank intakt ist, bleibt die Datenbank bestehen, wenn das Skript während einer Fortsetzungsaktion ausgeführt wird. Das Installationsskript, das das Konfigurationsskript enthält, wird nicht erneut ausgeführt. Ihre Aktion „Fortsetzen“ ist nicht erfolgreich. Sie müssen das Skript korrigieren und eine neue Instanz bereitstellen.

- Eine weitere zu berücksichtigende Variante ist, wo die Zuweisung des Schrittes gelungen ist, die Bereitstellung aber fehlgeschlagen ist. Wenn Sie in diesem Beispiel fortfahren, also die Aktion ab dem Zeitpunkt der fehlgeschlagenen Bereitstellung erneut durchführen, verarbeitet die Fortsetzungsanforderung veraltete Zuordnungsinformationen und der Fortsetzungsvorgang schlägt fehl.

Erstellen eines Snapshots Ihrer virtuellen Maschine

Je nachdem, wie Ihre Administratoren Ihre Umgebung konfiguriert haben, können Sie möglicherweise einen Snapshot Ihrer virtuellen Maschine erstellen. Ein Snapshot ist ein Image einer virtuellen Maschine zu einem bestimmten Zeitpunkt. Hierbei handelt es sich um eine platzsparende Kopie des ursprünglichen VM-Images. Snapshots stellen eine einfache Möglichkeit dar, um ein System bei Beschädigung, Datenverlust oder Sicherheitsbedrohungen wiederherzustellen. Nachdem Sie einen Snapshot Ihrer virtuellen Maschine erstellt haben, können Sie ihn anwenden und den Zustand Ihres Systems zum Zeitpunkt der Erstellung des Snapshots wiederherstellen.

Wenn Sie einen Arbeitsspeicher-Snapshot erstellen, erfasst der Snapshot den Status der Energieeinstellungen und optional den Arbeitsspeicherstatus der virtuellen Maschine. Wenn Sie den Arbeitsspeicherstatus der virtuellen Maschine erfassen, dauert der Snapshot-Vorgang länger. Die Antwort über das Netzwerk kann ebenfalls kurzzeitig verzögert sein.

Voraussetzungen

- Eine vorhandene virtuelle Maschine, die eingeschaltet, ausgeschaltet oder inaktiv ist.

- Wenn Ihre virtuelle Maschine für eine oder mehrere unabhängige Festplatten konfiguriert ist, schalten Sie die Maschine aus, bevor Sie einen Snapshot erstellen. Wenn die virtuelle Maschine eingeschaltet ist, können Sie keinen Snapshot erstellen. Informationen zur Festplattenkonfiguration finden Sie unter *Tabelle mit benutzerdefinierten Eigenschaften – V*.
- Ihr Mandantenadministrator oder Business-Gruppenmanager hat Ihnen die Berechtigung für die Snapshot-Aktion erteilt.

Verfahren

- 1 Wählen Sie **Elemente > Maschinen** aus.

Alternativ können Sie auch **Elemente > Bereitstellung** auswählen und zu der Maschine in der Bereitstellung wechseln.

- 2 Suchen Sie nach der Maschine, für die ein Snapshot erstellt werden soll.
- 3 Klicken Sie in der Spalte „Aktionen“ auf den nach unten weisenden Pfeil und dann auf **Details anzeigen**.
- 4 Klicken Sie im Menü „Aktionen“ auf **Snapshot erstellen**.
- 5 Geben Sie einen Namen und optional eine Beschreibung ein.
- 6 Wählen Sie **Arbeitsspeicher einbeziehen** aus, wenn Sie die Arbeitsspeicher- und Energieeinstellungen der Maschine erfassen möchten.
- 7 Klicken Sie auf **Übernehmen**.

Herstellen einer Remoteverbindung zu einer Maschine

Über die vRealize Automation-Konsole können Sie eine Remoteverbindung zu einer Maschine herstellen.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Maschinenbesitzer**, **Mandantenadministrator** oder **Business-Gruppenmanager** an.

- Stellen Sie sicher, dass VMware Tools installiert ist.

VMware Tools muss auf Ihrem vRealize Automation-Client installiert sein, um bei der Verbindungsherstellung mit VMware Remote Console den vollfunktionsfähigen Zugriff zu unterstützen. Wenn VMware Tools nicht installiert ist, treten Probleme auf, wie beispielsweise, dass der Mauszeiger und die Maustasten nach dem Herstellen einer Verbindung zur Zielmaschine nicht mehr funktionieren. Informationen zu unterstützten Versionen von VMware Tools finden Sie unter *Übersicht über die Unterstützung von vRealize Automation*.

- Stellen Sie sicher, dass die bereitgestellte Maschine eingeschaltet ist.

Verfahren

- 1 Wählen Sie **Elemente > Bereitstellung** aus.

- 2 Klicken Sie in der Zeile „Maschinenname“ auf **Aktionen** oder wählen Sie die Maschine aus und klicken Sie auf ihrer Maschinenseite auf **Aktionen**.
- 3 Wählen Sie die Remote-Verbindungsmethode aus.
 - Wählen Sie **Verbinden via RDP** aus, um mithilfe von RDP eine Verbindung herzustellen.
 - Wählen Sie **Mit Remote-Konsole verbinden** aus, um mithilfe von VMware Remote Console eine Verbindung herzustellen.Beantworten Sie Eingabeaufforderungen.
- 4 Klicken Sie auf **Verbinden** und melden Sie sich gemäß den Anweisungen an der Maschine an.
- 5 Melden Sie sich am Ende ab und schließen Sie das Browser-Fenster.

Konfigurieren von Remote-Konsolen für vSphere mit nicht vertrauenswürdigen SSL-Zertifikaten

Wenn Ihre vRealize Automation-Bereitstellung nicht vertrauenswürdige Zertifikate verwendet, müssen Sie Ihren Client-Browser vor der Verwendung der Remote-Konsolen mit VMware Remote Console so konfigurieren, dass dem Zertifikat vertraut wird. Die erforderlichen Schritte richten sich nach dem jeweiligen Browser.

Wenn vRealize Automation mit einem vertrauenswürdigen SSL-Zertifikat für Ihre Umgebung konfiguriert ist, erfordert VMware Remote Console keine zusätzliche Konfiguration in Client-Browsern. Wenn ein vRealize Automation-Appliance-Zertifikat durch ein vertrauenswürdiges Zertifikat ersetzt wird, müssen die Informationen des Zertifikats für den Webbrowser-Client nicht aktualisiert werden.

Informationen zum Ersetzen des Zertifikats finden Sie im Thema zum Ersetzen eines vRealize Automation-Appliance-Zertifikats im Handbuch *Systemverwaltung* für vRealize Automation.

Remoteverbindungen mithilfe von VMware Remote Console für in vSphere bereitgestellte Maschinen werden durch vRealize Automation-Appliance-Zertifikate über eine Proxy-Konsole geschützt. VMware Remote Console erfordert die Unterstützung von WebSockets im Browser, und die Browser müssen dem vRealize Automation-Appliance-Zertifikat vertrauen. Das Zertifikat ist auf der Root-Ebene der virtuellen Appliance unter einer Adresse im Format `https://vra-va.eng.mycompany.com/` abrufbar.

Informationen zu den Support-Anforderungen für Browser und vSphere finden Sie in der *Übersicht über die Unterstützung von vRealize Automation*.

Konfigurieren eines vertrauenswürdigen Zertifikats für vRealize Automation in Firefox

Nicht vertrauenswürdige vRealize Automation-Appliance-Zertifikate müssen manuell in Client-Browser importiert werden, um VMware Remote Console auf Clients zu unterstützen, die auf vSphere bereitgestellt wurden.

Informationen zu unterstützten Versionen von Firefox finden Sie in der *VMware vRealize-Support-Matrix* im vRealize Automation-[Informationscenter](#).

Hinweis Wenn vRealize Automation mit einem vertrauenswürdigen SSL-Zertifikat für Ihre Umgebung konfiguriert ist, erfordert VMware Remote Console keine zusätzliche Konfiguration in Client-Browsern.

Verfahren

- 1 Melden Sie sich in einem Firefox-Browser bei der vRealize Automation-Appliance an.
Es wird eine Meldung angezeigt, dass das Zertifikat nicht vertrauenswürdig ist.
- 2 Wählen Sie **Menü öffnen > Optionen** aus.
- 3 Klicken Sie auf **Datenschutz und Sicherheit** und dann auf **Zertifikate anzeigen**.
- 4 Klicken Sie im Dialogfeld „Zertifikatsmanager“ auf **Server** und dann auf **Ausnahme hinzufügen**.
- 5 Fügen Sie die URL für Ihre vRealize Automation-Appliance mit dem Port 8444 hinzu.
Beispiel: `https://your-vra-fqdn-domain:8444`.
- 6 Klicken Sie auf **Zertifikat abrufen** und dann auf **Sicherheitsausnahme bestätigen**.
- 7 Klicken Sie auf **OK**.

Ergebnisse

Sie können eine Verbindung mit der Remote-Konsole ohne Zertifikatsfehler herstellen.

Konfigurieren eines vertrauenswürdigen Zertifikats für die vRealize Automation-Appliance in Internet Explorer

Nicht vertrauenswürdige vRealize Automation-Appliance-Zertifikate müssen manuell in Client-Browsern importiert werden, um VMware Remote Console auf in vSphere bereitgestellten Clients zu unterstützen.

Hinweis Wenn vRealize Automation mit einem vertrauenswürdigen SSL-Zertifikat für Ihre Umgebung konfiguriert ist, erfordert VMware Remote Console keine zusätzliche Konfiguration in Client-Browsern.

Die Schritte in diesem Verfahren betreffen selbstsignierte Zertifikate und von einer Zertifizierungsstelle ausgestellte Zertifikate.

Informationen zu unterstützten Versionen von Internet Explorer finden Sie in der *Übersicht über die Unterstützung von VMware vRealize* auf der VMware-Website.

Verfahren

- 1 Melden Sie sich in einem Internet Explorer-Browser bei der vRealize Automation-Appliance an.

- 2 Klicken Sie in der Zertifikatfehlermeldung, die in der Adressleiste des Browsers angezeigt wird, auf **Zertifikat anzeigen**.
- 3 Klicken Sie im Fenster „Zertifikatinformationen“ auf die Registerkarte **Allgemein**.
- 4 Stellen Sie sicher, dass die Informationen zum Zertifikat stimmen, und klicken Sie auf **Zertifikat installieren**.
- 5 Wählen Sie im Dialogfeld „Zertifikatspeicher“ die Option **Alle Zertifikate in folgendem Speicher speichern** aus.
- 6 Klicken Sie auf **Durchsuchen**, um nach dem Zertifikatspeicher zu suchen.
- 7 Wählen Sie **Vertrauenswürdige Stammzertifizierungsstelle** aus und klicken Sie auf **OK**.
- 8 Klicken Sie im Dialogfeld „Zertifikatspeicher“ auf **Weiter**.
- 9 Klicken Sie im Dialogfeld „Sicherheitswarnung“ auf **Ja**, um das Zertifikat zu installieren.
- 10 Starten Sie den Browser neu.

Ergebnisse

Sie können eine Verbindung mit der Remote-Konsole ohne Zertifikatsfehler herstellen.

Konfigurieren eines vertrauenswürdigen Zertifikats für die vRealize Automation-Appliance in Chrome

Nicht vertrauenswürdige vRealize Automation-Appliance-Zertifikate müssen manuell in Client-Browsern importiert werden, um VMware Remote Console auf in vSphere bereitgestellten Clients zu unterstützen.

Informationen zu unterstützten Versionen von Chrome finden Sie in der *Übersicht über die Unterstützung von VMware vRealize* auf der VMware-Website.

Hinweis Wenn vRealize Automation mit einem vertrauenswürdigen SSL-Zertifikat für Ihre Umgebung konfiguriert ist, erfordert VMware Remote Console keine zusätzliche Konfiguration in Client-Browsern.

Unter Windows verwenden Chrome und Internet Explorer denselben Zertifikatspeicher. Dies bedeutet, dass Zertifikate, die für Internet Explorer vertrauenswürdige sind, auch für Chrome vertrauenswürdige sind. Um vertrauenswürdige Zertifikate für Chrome einzurichten, importieren Sie diese über Internet Explorer. Informationen zur Vorgehensweise finden Sie unter [Konfigurieren eines vertrauenswürdigen Zertifikats für die vRealize Automation-Appliance in Internet Explorer](#).

Starten Sie nach Abschluss dieses Verfahrens Chrome neu.

Um einem Zertifikat unter dem Macintosh-Betriebssystem dauerhaft zu vertrauen, laden Sie die Zertifikatsdatei herunter und installieren Sie das Zertifikat in Ihrem Zertifikatsverwaltungstool als vertrauenswürdige Zertifikat.

Verfahren

- 1 Melden Sie sich in einem Chrome-Browser bei der vRealize Automation-Appliance an.
- 2 Klicken Sie auf das Symbol in der Adressleiste.
- 3 Klicken Sie auf den Link für Zertifikatinformationen.
- 4 Speichern Sie das Zertifikat, indem Sie das Zertifikatsymbol auf den Desktop ziehen.
- 5 Starten Sie die Anwendung Schlüsselbund.
- 6 Wählen Sie **Datei > Elemente importieren** aus.
- 7 Wählen Sie im Schlüsselbund-Bildschirm die zuvor gespeicherte Zertifikatdatei aus.
Legen Sie für **Zielschlüssel** den Wert **System** fest.
- 8 Klicken Sie auf **Öffnen**, um das Zertifikat zu importieren.
- 9 Starten Sie den Browser neu.

Erzwingen des Löschens einer Bereitstellung nach einer fehlgeschlagenen Löschanforderung

Sie können das Löschen einer Bereitstellung erzwingen, die sich infolge einer fehlgeschlagenen Löschanforderung in einem inkonsistenten Zustand befindet.

Wenn vRealize Automation eine Bereitstellungsressource während eines Bereitstellungslöschvorgangs nicht löschen kann, wird der Löschvorgang sofort angehalten, ohne die verbleibenden Bereitstellungsressourcen zu löschen. Durch diesen Fehler bleibt die Bereitstellung in einem inkonsistenten Zustand zurück und verbraucht Ressourcen, ohne dass die Bereitstellung einfach gelöscht werden kann. Business-Gruppen-Administratoren können das Löschen von Bereitstellungen erzwingen, die sich in diesem inkonsistenten Zustand befinden.

Voraussetzungen

- Stellen Sie sicher, dass Sie bei vRealize Automation als **Business-Gruppen-Administrator** angemeldet sind.
- Bevor Sie die Aktion „Löschen erzwingen“ ausführen, lesen Sie die Beschreibung der Aktion „Löschen“ unter [Befehle im Menü „Aktion“ für bereitgestellte Ressourcen](#).

Verfahren

- 1 Klicken Sie auf der Registerkarte **Elemente** auf **Bereitstellungen**, und wählen Sie die zu löschende Bereitstellung aus.
- 2 Klicken Sie auf **Aktionen** und dann auf **Löschen**.
- 3 Geben Sie eine Beschreibung und einen Grund für die Anforderung ein.
- 4 Wählen Sie die **Löschen erzwingen** aus und klicken Sie auf **Absenden**.

Ergebnisse

vRealize Automation versucht, die Bereitstellung einschließlich aller Ressourcen in der Bereitstellung vollständig zu löschen. Wenn vRealize Automation eine Bereitstellungsressource nicht löschen kann, wird diese Ressource übersprungen, und das Löschen der verbleibenden Ressourcen in der Bereitstellung wird fortgesetzt.

Nächste Schritte

Klicken Sie auf die Registerkarte **Anforderungen** und stellen Sie sicher, dass alle Ressourcen in der Bereitstellung erfolgreich gelöscht wurden. Alle Ressourcen, die während eines erzwungenen Löschvorgangs nicht gelöscht wurden, müssen manuell gelöscht werden. Stellen Sie außerdem sicher, dass alle bereitgestellten virtuellen Maschinenobjekte gelöscht werden, da vRealize Automation versuchen kann, ihre Hostnamen, IP-Adressen und andere Konfigurationsdetails während der nachfolgenden Provisioning-Vorgänge wiederzuverwenden.

Fehlerbehebung bei fehlenden Aktionen im Menü „Ressourcenaktionen“

Als Maschinen- oder Ressourcenbesitzer werden Ihnen nicht alle berechtigten Aktionen für ein bereitgestelltes Element angezeigt.

Problem

In einer Umgebung, von der Sie wissen, dass Ihrer Benutzergruppe oder Business-Gruppe eine Aktion gewährt wurde, erwarten Sie, dass alle Aktionen angezeigt werden, wenn Sie ein Element in Ihrer Liste **Elemente** auswählen.

Ursache

Die Verfügbarkeit von Aktionen ist abhängig vom Typ der bereitgestellten Ressource, vom Betriebszustand der Ressource sowie von der Art und Weise, wie die Ressource konfiguriert und verfügbar gemacht wurde. Nachfolgend finden Sie einige Ursachen, weshalb nicht alle konfigurierten Aktionen angezeigt werden.

- Die Aktion ist aufgrund des aktuellen Status der bereitgestellten Ressource nicht anwendbar. Beispielsweise ist „Ausschalten“ nur verfügbar, wenn die Maschine eingeschaltet ist.
- Die Aktion ist für den ausgewählten Elementtyp nicht anwendbar. Wenn die Aktion von dem Element nicht unterstützt wird, wird sie nicht in der Liste angezeigt. Beispielsweise ist die Aktion „Snapshot erstellen“ für eine physische Maschine nicht verfügbar, und die Aktion „Verbinden via RDP“ ist nicht verfügbar, wenn es sich beim ausgewählten Element um eine Linux-Maschine handelt.
- Die Aktion ist für den bereitgestellten Ressourcentyp anwendbar, aber die Aktion ist im Infrastruktur-Blueprint deaktiviert. Wenn die Aktion deaktiviert ist, wird sie nie als verfügbare Aktion für Elemente angezeigt, die mithilfe des Blueprints bereitgestellt wurden.
- Die Aktion ist nicht in der Berechtigung enthalten, mit der das Element bereitgestellt wird, für das Sie die Aktion ausführen müssen. Nur berechtigte Aktionen können entweder im Rahmen eines IaaS-Blueprints oder als XaaS-Ressourcenaktion im Menü „Aktionen“ angezeigt werden.

- Die Aktion wird als XaaS-Ressourcenaktion erstellt, war aber nicht in der Berechtigung enthalten, mit der das Element bereitgestellt wird, für das Sie die Aktion ausführen müssen. Nur berechtigte Aktionen werden im Menü „Aktionen“ angezeigt.
- Die Aktion ist möglicherweise basierend auf den konfigurierten Zielkriterien für XaaS-Ressourcenaktionen oder -Ressourcenzuordnungen auf bereitgestellte IaaS-Maschine beschränkt.

Lösung

- ◆ Stellen Sie sicher, dass die Aktion für das bereitgestellte Element oder den Status des bereitgestellten Elements anwendbar ist.
- ◆ Stellen Sie sicher, dass die Aktion konfiguriert ist und in der Berechtigung enthalten ist, mit der das Element bereitgestellt wird.

Fehlerbehebung bei einer fehlgeschlagenen Bereitstellung mit einem vRealize Orchestrator-Workflow

Wenn die fehlgeschlagene Bereitstellung eines Blueprints einen vRealize Orchestrator-Workflow enthält, können Sie die Token-ID zur Fehlerbehebung bei Problemen mit dem Workflow verwenden. Sie verwenden die Token-ID, um die Protokolle in vRealize Orchestrator zu suchen.

Lösung

- 1 Suchen Sie nach der Token-ID für den fehlgeschlagenen Workflow.
 - a Klicken Sie in vRealize Automation auf die Registerkarte **Anforderung**.
 - b Klicken Sie auf die Zahl in der Spalte „Anforderung“.
die Anforderung kann eine Bereitstellung oder eine Aktion sein.
 - c Klicken Sie auf die Registerkarte **Allgemein**.
Wenn der Blueprint auf einem vRealize Orchestrator-Workflow basiert, lautet der Seitentitel „Ausführungsdetails für den vRealize Orchestrator-Workflow“.
 - d Suchen Sie die Token-ID und kopieren Sie sie in die Zwischenablage oder in eine Textdatei.
Beispiel: ff8080815a685352015a6c8d450801ee.
- 2 Suchen Sie im Control Center die Workflow-Protokolle in vRealize Orchestrator
 - a Geben Sie die Basis-URL für vRealize Automation in einem Browser-Suchfeld ein.
Die Seite „VMwarevRealize Automation-Appliance“ wird angezeigt.
 - b Klicken Sie auf **vRealize Orchestrator Control Center**.
 - c Melden Sie sich als Benutzer mit Root-Berechtigungen an.
 - d Klicken Sie auf **Workflows überprüfen**.
 - e Klicken Sie auf **Workflows abgeschlossen**.

- f Fügen Sie das Workflow-Token in das Textfeld „Token-ID“ ein.

Die Liste wird für den Workflow angezeigt, der mit der Token-ID übereinstimmt.

- g Klicken Sie auf die Zeile und überprüfen Sie die Fehlerursache in den Protokollen.

Angeben von Einstellungen für die Neukonfiguration von Maschinen und Überlegungen bei der Neukonfiguration

vSphere-, vCloud Air- und vCloud Director-Plattformen unterstützen die Neukonfiguration von vorhandenen Maschinen in einer Bereitstellung, um die Spezifikationen, wie z. B. CPU, Arbeitsspeicher und Speicher, zu ändern.

Neukonfigurationsanforderungen unterliegen der Genehmigung basierend auf Berechtigungen, Richtlinien und den für die Maschinenkomponente im Blueprint aktivierten Aktionen.

Die Neukonfiguration einer virtuellen Maschine, die einem bedarfsgesteuerten Netzwerk zugewiesen ist, wird nicht unterstützt. Sie können eine Netzwerkkarte, die mit einem bedarfsgesteuerten Netzwerk verbunden ist, nicht neu konfigurieren. Wenn Sie versuchen, ein bedarfsgesteuertes NAT-Netzwerk oder ein geroutetes Netzwerk neu zu konfigurieren, wird die Fehlermeldung 'Original network [<network>] is not selected in the machine's reservation.' angezeigt. Die Netzwerke der Maschine bleiben davon unberührt und die IP-Adressen der Maschine werden nicht geändert.

Wenn Sie über die Berechtigung für die Aktionen „Neukonfiguration abbrechen“ (Maschine) und „Neukonfiguration ausführen“ (Maschine) verfügen, können Sie eine Neukonfiguration abbrechen oder eine fehlgeschlagene Neukonfiguration erneut ausführen.

Das Erweitern einer Festplatte auf einer VM, die über einen Linked Clone-Blueprint bereitgestellt wurde, wird nicht unterstützt.

Sie können Maschinen nicht mithilfe der Komponentenprofile **Size** oder **Image** neu konfigurieren. Der CPU-Bereich, der Arbeitsspeicher und der Speicher, die basierend auf dem Profil berechnet werden, bleiben jedoch für Neukonfigurationsaktionen verfügbar. Wenn Sie beispielsweise einen kleinen (1 CPU, 1024 MB Arbeitsspeicher und 10 GB Speicher), einen mittleren (3 CPUs, 2048 MB Arbeitsspeicher, 12 GB Speicher) und einen großen (5 CPUs, 3072 MB Arbeitsspeicher, 15 GB Speicher) **Size**-Wertsatz verwendet haben, sind die folgenden Bereiche während der Neukonfiguration der Maschine verfügbar: 1–5 CPUs, 1024–3072 MB Arbeitsspeicher und 1–15 GB Speicher.

vRealize Automation erstellt bei der Bereitstellung einen Blueprint-Snapshot. Falls Sie bei einer Bereitstellung auf Neukonfigurationsprobleme bei der Aktualisierung von Maschineneigenschaften wie z. B. CPU und RAM stoßen, lesen Sie den Knowledgebase-Artikel [2150829 vRA 7.x Blueprint Snapshotting](#).

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Maschinenbesitzer**, **Supportbenutzer**, **Business-Gruppenbenutzer mit gemeinsam genutztem Zugriff** oder **Business-Gruppenmanager** an.

- Die Maschine, die Sie neu konfigurieren möchten, muss den Status „Ein“ oder „Aus“ ohne aktiven Neukonfigurierungsstatus aufweisen.
- Bei dem Maschinentyp muss es sich um vSphere, vCloud Air oder vCloud Director handeln, obwohl die NSX-Einstellungen nur für vSphere gelten.
- Stellen Sie sicher, dass Sie zur Neukonfiguration einer Maschine berechtigt sind.

Verfahren

- 1 Wählen Sie **Elemente > Maschinen** aus.

Alternativ können Sie auch **Elemente > Bereitstellung** auswählen und zu der Maschine in der Bereitstellung wechseln.

- 2 Wählen Sie die Maschine aus, die Sie neu konfigurieren möchten.



- 3 Wählen Sie im Menü **Aktionen** die Option **Neu konfigurieren** aus.
- 4 Wählen Sie die für die Einstellungen, die Sie neu konfigurieren möchten, die entsprechende Registerkarte aus.

Tabelle 3-80. Anfordern von Neukonfigurationsänderungen

Registerkarte	Thema
Allgemein	Neukonfigurieren der CPUs und des Arbeitsspeichers
Speicher	Bearbeiten der Speichereinstellungen
Netzwerk	Ändern von Netzwerkeinstellungen Informationen zum Ändern von NAT-Regeln finden Sie unter Ändern von NAT-Regeln in einer Bereitstellung .
Sicherheit	Informationen zum Neukonfigurieren der Sicherheitseinstellungen finden Sie unter Hinzufügen oder Entfernen von Sicherheitselementen in einer Bereitstellung .
Eigenschaften	Ändern der benutzerdefinierten Eigenschaft und der Eigenschaftsgruppeneinstellungen

Nächste Schritte

[Ausführen der angeforderten Neukonfiguration der Maschine](#) .

Neukonfigurieren der CPUs und des Arbeitsspeichers

Sie können die Anzahl der CPUs oder den Arbeitsspeicher und Speicherplatz ändern, die bzw. der von der bereitgestellten Maschine verwendet wird. Die Änderung muss innerhalb der von dem Bereitstellungs-Blueprint gesetzten Grenzwerte vorgenommen werden.

Für bereitgestellte Amazon-Bereitstellungen können Sie alle Speichervolumen in der Bereitstellung außer dem Root-Volume neu konfigurieren.

Das Erweitern einer Festplatte auf einer VM, die über einen Linked Clone-Blueprint bereitgestellt wurde, wird nicht unterstützt.

Voraussetzungen

[Angaben von Einstellungen für die Neukonfiguration von Maschinen und Überlegungen bei der Neukonfiguration.](#)

Verfahren

- 1 Klicken Sie auf die Registerkarte **Allgemein**.
- 2 Geben Sie die Anzahl der CPUs in das Textfeld **Nr. CPUs** ein.
- 3 Geben Sie den Arbeitsspeicher in das Textfeld **Arbeitsspeicher (MB)** ein.
- 4 Geben Sie den Speicherplatz in das Textfeld **Speicher (GB)** ein.

Nächste Schritte

Geben Sie weitere Einstellungen für die Neukonfiguration der Maschine an. Wenn Sie die Änderung der Maschineneinstellungen abgeschlossen haben, starten Sie die Neukonfigurationsanforderung der Maschine. Siehe [Ausführen der angeforderten Neukonfiguration der Maschine](#).

Bearbeiten der Speichereinstellungen

Sie können ein Speichervolume auf einer bereitgestellten virtuellen Maschine hinzufügen, löschen oder die Größe des Speichervolumens ändern.

Sie können den Speicher für den IDE-Datenträgertyp nicht neu konfigurieren.

Speicher und Arbeitsspeicher, die mittels einer Reservierung einer bereitgestellten Maschine zugewiesen sind, werden freigegeben, wenn die Maschine, der der Speicher oder Arbeitsspeicher zugewiesen ist, in vRealize Automation mithilfe der Aktion „Löschen“ gelöscht wird. Der Speicher und der Arbeitsspeicher werden nicht freigegeben, wenn die Maschine auf dem vCenter Server gelöscht wird.

Sie können beispielsweise Reservierungen, die Maschinen in einer vorhandenen Bereitstellung zugeordnet sind, nicht löschen. Wenn Sie bereitgestellte Maschinen manuell im vCenter Server verschieben oder löschen, erkennt vRealize Automation die bereitgestellten Maschinen weiterhin als aktiv und verhindert das Löschen von zugeordneten Reservierungen.

Voraussetzungen

[Angaben von Einstellungen für die Neukonfiguration von Maschinen und Überlegungen bei der Neukonfiguration.](#)


Für bereitgestellte Amazon-Bereitstellungen können Sie alle Speichervolumen in der Bereitstellung außer dem Root-Volume neu konfigurieren.

Verfahren


1 Klicken Sie auf die Registerkarte **Speicher**.

Der zulässige Bereich für den Speicher wird unter der Tabelle der Speichervolumen angezeigt.

2 Fügen Sie Einstellungen für Speichervolumen hinzu oder bearbeiten Sie sie.

- a Klicken Sie auf **Neues Volume**.
- b Geben Sie die Kapazität in das Textfeld **Kapazität (GB)** ein.
- c Wählen Sie eine Speicherreservierungsrichtlinie aus dem Dropdown-Menü **Speicherreservierungsrichtlinie** aus.
- d Klicken Sie auf das Symbol **Speichern** ()



3 Löschen Sie ein Volume.

- a Suchen Sie das Volume.
- b Klicken Sie auf das Symbol **Löschen** ()

Ein nicht auswählbares Symbol zeigt ein nicht lösches Volume wie beispielsweise eines von einem verknüpften Klon an.

4 Erhöhen Sie die Größe eines Volumes.

Sie können die Größe von vorhandenen Volumes nicht reduzieren. Die Größe des Volumes ist durch den Gesamtspeicherplatz begrenzt, der in dem Blueprint festgesetzt wurde, abzüglich des anderen Volumes zugewiesenen Speicherplatzes.

- a Suchen Sie das Volume.
- b Klicken Sie auf das Symbol **Bearbeiten** ()
- c Geben Sie die neue Größe in das Textfeld **Kapazität (GB)** ein.
- d Klicken Sie auf das Symbol **Speichern** ()

Nächste Schritte

Geben Sie weitere Einstellungen für die Neukonfiguration der Maschine an. Wenn Sie die Änderung der Maschineneinstellungen abgeschlossen haben, starten Sie die Neukonfigurationsanforderung der Maschine. Siehe [Ausführen der angeforderten Neukonfiguration der Maschine](#).

Ändern von Netzwerkeinstellungen

Sie können einen Netzwerkkarten hinzufügen, entfernen oder bearbeiten.

Während der Neukonfiguration einer Maschine können Sie die folgenden Netzwerkeinstellungen ändern:

- Hinzufügen oder Entfernen von Netzwerkkarten.

- Zuweisen oder Freigeben von IP-Adressen für vorhandene Netzwerkkarten.
- Zuweisen von neuen IP-Adressen zu Netzwerkkarten, vorausgesetzt, bei dem Netzwerk handelt es sich nicht um ein bedarfsgesteuertes NAT-Netzwerk oder bedarfsgesteuertes geroutetes Netzwerk.

Sie können ein bedarfsgesteuertes geroutetes Netzwerk oder ein bedarfsgesteuertes NAT-Netzwerk nicht erneut konfigurieren.

Für die Neukonfiguration eines Netzwerks ist es erforderlich, dass die Quell- und Zielnetzwerke in der Reservierung ausgewählt sind.

Wenn Sie Netzwerkkarten hinzufügen, werden IP-Adressen zugeteilt. Wenn Sie Netzwerkkarten entfernen, werden IP-Adressen freigegeben.

Wenn Sie ein Netzwerk auf Basis der Informationen zur Reservierung und zum Netzwerkprofil neu konfigurieren, wird die neue Netzwerk-IP-Adresse in vRealize Automation zugewiesen, aber die bereitgestellte Maschine wird nicht mit den neuen IP-Informationen aktualisiert. Nach Abschluss des Neukonfigurationsvorgangs müssen Sie die IP-Adresse der Maschine manuell zuweisen.

Die Neukonfiguration einer virtuellen Maschine, die einem bedarfsgesteuerten Netzwerk zugewiesen ist, wird nicht unterstützt. Sie können eine Netzwerkkarte, die mit einem bedarfsgesteuerten Netzwerk verbunden ist, nicht neu konfigurieren. Wenn Sie versuchen, ein bedarfsgesteuertes NAT-Netzwerk oder ein geroutetes Netzwerk neu zu konfigurieren, wird die Fehlermeldung 'Original network [<network>] is not selected in the machine's reservation.' angezeigt. Die Netzwerke der Maschine bleiben davon unberührt und die IP-Adressen der Maschine werden nicht geändert.

Das Ändern der NSX-Netzwerkeinstellungen wird für Bereitstellungen nicht unterstützt, die aktualisiert oder von vRealize Automation 6.2.x auf diese vRealize Automation Version migriert wurden.

Voraussetzungen

[Angaben von Einstellungen für die Neukonfiguration von Maschinen und Überlegungen bei der Neukonfiguration.](#)


Verfahren

- 1 Klicken Sie auf die Registerkarte **Netzwerk**.
- 2 (Optional) Fügen Sie einen Netzwerkadapter hinzu.
 - a Klicken Sie auf **Neuer Netzwerkadapter**.
 - b Wählen Sie ein Netzwerk im Dropdown-Menü **Netzwerkname** aus.

Alle auf der Reservierung der Maschine ausgewählten Netzwerke sind verfügbar.


- c Geben Sie eine statische IP-Adresse für das Netzwerk in das Textfeld **Adresse** ein.

Die IP-Adresse darf im Netzwerkprofil nicht zugewiesen sein, das in der Reservierung zugewiesen ist.

- d Klicken Sie auf das Symbol **Speichern** ()

3 (Optional) Entfernen Sie einen Netzwerkadapter.


- a Suchen Sie den Netzwerkadapter.

- b Klicken Sie auf das Symbol **Löschen** ()


Sie können Netzwerkadapter 0 nicht entfernen.

4 (Optional) Bearbeiten Sie einen Netzwerkadapter.

- a Suchen Sie den Netzwerkadapter.

- b Klicken Sie auf das Symbol **Bearbeiten** ()

- c Wählen Sie ein Netzwerk im Dropdown-Menü **Netzwerkname** aus.

- d Klicken Sie auf das Symbol **Speichern** ()

Nächste Schritte

Geben Sie weitere Einstellungen für die Neukonfiguration der Maschine an. Wenn Sie die Änderung der Maschineneinstellungen abgeschlossen haben, starten Sie die Neukonfigurationsanforderung der Maschine. Siehe [Ausführen der angeforderten Neukonfiguration der Maschine](#).

Ändern der benutzerdefinierten Eigenschaft und der Eigenschaftsgruppeneinstellungen

Sie können benutzerdefinierte Eigenschaften in der bereitgestellten Maschine bearbeiten, hinzufügen oder löschen.

Sie können benutzerdefinierte Eigenschaften nicht für die Eingabe von Werten für Volumedatenträgernummer, Kapazität, Bezeichnung oder Speicherreservierungsrichtlinie verwenden. Sie müssen diese Werte eingeben, indem Sie ein Volume in der Tabelle der Speichervolumen hinzufügen oder bearbeiten. Siehe [Bearbeiten der Speichereinstellungen](#).

Voraussetzungen

[Angaben von Einstellungen für die Neukonfiguration von Maschinen und Überlegungen bei der Neukonfiguration](#).

Verfahren

- 1 Klicken Sie auf die Registerkarte **Eigenschaften**.
- 2 Klicken Sie zum Hinzufügen einer Eigenschaft auf **Neue Eigenschaft**.
- 3 Geben Sie den Namen der Eigenschaft in das Textfeld **Name** ein.

- 4 Geben Sie den Wert der Eigenschaft in das Textfeld **Wert** ein.
- 5 Aktivieren Sie das Kontrollkästchen **Verschlüsselt** zum Verschlüsseln des Werts.
- 6 Aktivieren Sie das Kontrollkästchen **Eingabeaufforderung**, um Benutzer zur Eingabe des Werts aufzufordern, wenn sie die Maschine anfordern.
- 7 Fügen Sie eine weitere Eigenschaft hinzu, bearbeiten Sie eine vorhandene Eigenschaft oder löschen Sie eine Eigenschaft.

Nächste Schritte

Geben Sie weitere Einstellungen für die Neukonfiguration der Maschine an. Wenn Sie die Änderung der Maschineneinstellungen abgeschlossen haben, starten Sie die Neukonfigurationsanforderung der Maschine. Siehe [Ausführen der angeforderten Neukonfiguration der Maschine](#).

Ausführen der angeforderten Neukonfiguration der Maschine

Sie können die angeforderte Neukonfiguration der Maschine sofort starten oder den Start an einem bestimmten Tag und zu einer bestimmten Uhrzeit planen. Sie können auch vor dem Neukonfigurieren die Energieoption für die Maschine angeben.

Voraussetzungen

[Angaben von Einstellungen für die Neukonfiguration von Maschinen und Überlegungen bei der Neukonfiguration.](#)

Verfahren

- 1 Wenn die Registerkarte **Ausführung** angezeigt wird, können Sie sie auswählen, um weitere Einstellungen für die Neukonfiguration anzugeben. Wenn sie nicht angezeigt wird, klicken Sie auf **Übermitteln**, um die Neukonfiguration der Maschine zu starten.
- 2 Wenn die Registerkarte **Ausführung** angezeigt wird, klicken Sie auf **Ausführung**, um die Neukonfiguration zu planen.
- 3 (Optional) Wählen Sie eine Option aus dem Dropdown-Menü **Anforderung ausführen** aus.

Option	Beschreibung
Sofort	Startet die Neukonfiguration so schnell wie möglich nach der Genehmigung.
Geplant	Startet die Neukonfiguration zum angegebenen Datum und zur angegebenen Uhrzeit. Geben Sie das Datum und die Uhrzeit in die angezeigten Textfelder ein.

Die geplante Zeit ist die lokale Zeit des Landes, in dem sich der vRealize Automation-Webserver befindet. Wenn **Anforderung ausführen** nicht verfügbar ist, wird die Neukonfiguration sofort gestartet.

- 4 (Optional) Wählen Sie eine auszuführende Aktion im Dropdown-Menü **Auszuführende Aktion** aus.

Option	Beschreibung
Falls erforderlich, neu starten	(Standard) Startet die Maschine bei Bedarf vor der Neukonfiguration neu.
Neu starten	Startet die Maschine vor der Neukonfiguration neu, unabhängig davon, ob ein Neustart erforderlich ist.
Nicht neu starten	Startet die Maschine vor der Neukonfiguration nicht neu, selbst wenn ein Neustart erforderlich ist.

Die folgenden Zustände erfordern einen Neustart der Maschine vor der Neukonfiguration:

- CPU-Änderung, wenn Hot-Add nicht unterstützt wird oder deaktiviert ist
- Änderung des Arbeitsspeichers, wenn Hot-Memory nicht unterstützt wird oder deaktiviert ist
- Änderung des Speichers, wenn Hot-Storage deaktiviert ist

Beindet sich die Maschine im Status zum Herunterfahren, wird sie nicht neu gestartet.

Hinweis Sie können die vSphere-Hot-Add-Option unter Verwendung der benutzerdefinierten Eigenschaft `VirtualMachine.Reconfigure.DisableHotCpu` deaktivieren.

- 5 Klicken Sie auf **OK**.

Nächste Schritte

Sie können den Fortschritt der Neukonfiguration überwachen, indem Sie die in der Benutzerschnittstelle angezeigten Workflowstatus beobachten. Siehe [Workflowstatus von Neukonfigurierungsvorgängen](#).

Workflowstatus von Neukonfigurierungsvorgängen

Wenn die Neukonfiguration gestartet wird und diese den Workflow durchläuft, können Sie den Fortschritt über die Seite zum Bearbeiten überwachen.

Tabelle 3-81. Workflowstatus von Neukonfigurierungsvorgängen

Zustand	Beschreibung
Neukonfigurieren ausstehend	Der Statusvorgang wurde erstellt.
Geplant	Es wurde ein geplanter Workflow für den Distributed Execution Manager (DEM) erstellt.
Neukonfiguration	Ein schnittstellenspezifischer Workflow wird ausgeführt.
Fehler bei der Neukonfiguration, Warten auf Wiederholung	Es gab einen Fehler bei der Neukonfiguration, es wird gewartet, bis der Besitzer eine Wiederholung anfordert. Wenn der Maschinenbesitzer für die Aktionen „Neu konfigurieren“ oder „Neukonfiguration abbrechen“ berechtigt ist, kann der Besitzer eine Neukonfiguration erneut versuchen oder abbrechen.
ReconfigureFailed	Es gab einen Fehler bei der Neukonfiguration, es wird gewartet, bis der Workflow die nächste Aktion ausführt.

Tabelle 3-81. Workflowstatus von Neukonfigurierungsvorgängen (Fortsetzung)

Zustand	Beschreibung
ReconfigureSuccessful	Die Neukonfiguration war erfolgreich, es wird gewartet, bis der Workflow die nächste Aktion ausführt.
Abgebrochen	Der Benutzer hat die Neukonfiguration abgebrochen. Dazu berechnigte Maschinenbesitzer können eine Neukonfiguration abbrechen.
Vollständig	Der Fertigstellungs-Workflow legt diesen Status nach Fertigstellung der Bereinigung fest, sodass der Workflow die Statusvorgänge und Genehmigungen weiter bereinigen kann. Ein Vollständig-Status zeigt an, dass die Anforderung von vRealize Automation abgeschlossen wurde, aber er zeigt nicht an, dass die Maschinenneukonfiguration erfolgreich fertiggestellt wurde.

Erneutes Konfigurieren eines Lastausgleichsdiensts in einer Bereitstellung

Sie können einen virtuellen Server zu einem bereitgestellten NSX-Lastausgleichsdienst hinzufügen, ihn bearbeiten oder löschen.

Die folgenden Informationen gelten für Bereitstellungen, die für vRealize Automation 7.2 oder eine ältere Version generiert wurden:

- Die Neukonfiguration des Lastausgleichsdiensts ist auf Bereitstellungen beschränkt, die einen einzigen Lastausgleichsdienst einschließen.
- Auf der Seite „Elementdetails“ der Lastausgleichsdienste in einer Bereitstellung werden die virtuellen Server angezeigt, die von allen Lastausgleichsdiensten in der Bereitstellung verwendet werden. Weitere Informationen finden Sie im [Knowledge Base-Artikel 2150276](#).
- Der Vorgang „Lastausgleichsdienst neu konfigurieren“ wird für Bereitstellungen, die von vRealize Automation 6.2.x auf diese Version von vRealize Automation aktualisiert oder migriert wurden, nicht unterstützt.

Vermeiden Sie es, für aktualisierte Lastausgleichsdienste und in der aktuellen Version von vRealize Automation bereitgestellte Lastausgleichsdienste in derselben Anforderung zugleich das Bearbeiten und Hinzufügen eines virtuellen Servers anzufordern. Weitere Informationen finden Sie im [Knowledge Base-Artikel 2150240](#).

Wenn Sie die erneute Konfiguration eines Lastausgleichsdiensts anfordern, während eine andere Bereitstellungsaktion ausgeführt wird (zum Beispiel ein laufender Skalierungsvorgang während der Bereitstellung), schlägt die Neukonfiguration mit einer Hinweismeldung fehl. In diesem Fall können Sie warten, bis die Aktion abgeschlossen ist, und die Neukonfigurationsanforderung anschließend erneut übermitteln.

Hinweis Wenn der der Bereitstellung zugeordnete Blueprint aus einer YAML-Datei importiert wurde, die einen bedarfsgesteuerten Lastausgleichsdienst mit einem Wert im Namensfeld enthält, der sich von dem Wert im ID-Feld unterscheidet, schlägt die Aktion **Neukonfigurieren** fehl. Um die Option für die Neukonfiguration des Lastausgleichsdiensts für eine Bereitstellung zu ermöglichen, die auf einem importierten Blueprint basiert, führen Sie die folgenden Schritte im Blueprint aus, um Aktionen nach der Bereitstellung für Lastausgleichsdienst-Komponenten in zukünftigen Bereitstellungen zuzulassen.

- 1 Wählen Sie in der vRealize Automation-Konsole den Blueprint aus.
- 2 Klicken Sie auf **Bearbeiten** und ändern Sie den Blueprint-Namen. Dadurch wird der Namen und die eingebettete-ID auf denselben Wert festgelegt.
- 3 Wählen Sie die Lastausgleichsdienst-Komponente im Blueprint aus.
- 4 Klicken Sie auf **Bearbeiten** und geben Sie den Blueprint-Namen erneut ein. Dadurch wird der Namen und die eingebettete-ID auf denselben Wert festgelegt.
- 5 Wiederholen Sie diesen Vorgang für alle Lastausgleichsdienst-Komponenten im Blueprint.
- 6 Speichern Sie den Blueprint.

Wenn Sie eine neue Bereitstellung mithilfe des bearbeiteten Blueprints bereitstellen, funktioniert die Aktion „Lastausgleichsdienst neu konfigurieren“. Um dieses Problem zu vermeiden, stellen Sie sicher, dass alle YAML-Dateien vor deren Import über identische Namen und ID-Werte für alle Lastausgleichsdienste, Netzwerke und Sicherheitskomponenten verfügen.

Die durch vRealize Automation verwalteten NSX-Objekte sollten nicht außerhalb von vRealize Automation verwaltet werden. Wenn Sie beispielsweise den Mitgliedsport eines bereitgestellten NSX-Lastausgleichsdiensts nicht in vRealize Automation, sondern in NSX ändern möchten, dann beschädigt die NSX-Datenerfassung die Zuordnung zwischen der bereitgestellten Maschine und ihrem ansonsten zugeordneten Mitgliedspool des Lastausgleichsdiensts. Vertikale und horizontale Skalierungsvorgänge führen ebenfalls zu unvorhersehbaren Ergebnissen, wenn der Mitgliedsport eines bereitgestellten Lastausgleichsdiensts außerhalb von vRealize Automation geändert wird.

Weitere Informationen zu den Einstellungen, die beim Hinzufügen oder Bearbeiten eines virtuellen Servers verfügbar sind, finden Sie unter [Hinzufügen einer Komponente für den Lastausgleichsdienst nach Bedarf](#).

Wenn Sie einen Lastausgleichsdienst in vRealize Automation neu konfigurieren, werden einige der Einstellungen, die in NSX konfiguriert wurden und als Einstellungen in vRealize Automation nicht verfügbar sind, auf ihren jeweiligen Standardwert zurückgesetzt. Nachdem Sie die Neukonfiguration des Lastausgleichsdiensts in vRealize Automation ausgeführt haben, überprüfen Sie die Einstellungen in NSX:

- Insert-X-Forwarded for HTTP Header
- HTTP Redirect URL
- Service Monitor Extension

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Maschinenbesitzer, Supportbenutzer, Business-Gruppenbenutzer mit gemeinsam genutztem Zugriff** oder **Business-Gruppenmanager** an.
- Stellen Sie sicher, dass Sie über die Berechtigung zum erneuten Konfigurieren von Lastausgleichsdiensten in einer Bereitstellung verfügen. Die erforderliche Katalogberechtigung ist „Neu konfigurieren (Lastausgleichsdienst)“.

Verfahren

- 1 Wählen Sie **Elemente > Bereitstellung** aus.
- 2 Suchen Sie die Bereitstellung und zeigen Sie deren untergeordnete Komponenten an.



- 3 Wählen Sie den zu bearbeitenden NSX-Lastausgleichsdienst aus.



- 4 Wählen Sie im Menü **Aktionen** die Option **Neu konfigurieren** aus.
- 5 Fügen Sie virtuelle Server hinzu, bearbeiten oder löschen Sie sie.

Virtual servers:

Protocol	Port	Description	Member Protocol	Member Port	Health Check Protocol	Health Check Port
HTTP	80		HTTP	80	HTTP	80
HTTP	81		HTTP	81	HTTP	81

- 6 Klicken Sie nach dem Hinzufügen, Bearbeiten oder Löschen der virtuellen Server auf **Übernehmen**, um die Neukonfiguration anzufordern.

Ändern von NAT-Regeln in einer Bereitstellung

Sie können vorhandene NSX-NAT-Regeln in einem bereitgestellten NAT-Netzwerk vom Typ 1:n hinzufügen, bearbeiten und löschen.

Sie können auch die Reihenfolge ändern, in der die NAT-Regeln verarbeitet werden.

Hinweis Wenn der Quell-Blueprint der Bereitstellung aus einer YAML-Datei importiert wird, die eine NAT-Netzwerkkomponente enthält, und der Name und die ID-Werte der NAT-Netzwerkkomponente nicht übereinstimmen, schlägt die Aktion **NAT-Regeln ändern** fehl. Um die Aktion **NAT-Regeln ändern** für eine Bereitstellung zuzulassen, die auf einem importierten Blueprint basiert, führen Sie vor der Bereitstellung die folgenden Schritte im Blueprint durch.

- 1 Starten Sie vRealize Automation, klicken Sie auf die Registerkarte „Design“ und öffnen Sie den Blueprint.
- 2 Klicken Sie auf **Bearbeiten** und ändern Sie den Namen des Blueprints. Dadurch wird der Namen und die eingebettete-ID auf denselben Wert festgelegt.
- 3 Wählen Sie die NAT-Netzwerkkomponente im Blueprint aus.
- 4 Klicken Sie auf **Bearbeiten** und geben Sie den Blueprint-Namen erneut ein. Dadurch wird der Namen und die eingebettete-ID auf denselben Wert festgelegt.
- 5 Wiederholen Sie diesen Schritt für alle NAT-Netzwerkkomponenten im Blueprint.
- 6 Speichern Sie den Blueprint.

Stellen Sie zur Vermeidung dieses Problems sicher, dass alle YAML-Dateien vor deren Import über identische Namen und ID-Werte für alle Blueprints und Lastausgleichsdienst-, Netzwerk- und Sicherheitskomponenten verfügen.

Weitere Informationen dazu finden Sie unter [Erstellen und Verwenden von NAT-Regeln](#) und [Hinzufügen einer bedarfsgesteuerten NAT- oder bedarfsgesteuerten gerouteten Netzwerkkomponente](#).

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Maschinenbesitzer, Supportbenutzer, Business-Gruppenbenutzer mit gemeinsam genutztem Zugriff** oder **Business-Gruppenmanager** an.
- Stellen Sie sicher, dass Sie berechtigt sind, NAT-Regeln in einem Netzwerk zu ändern.
- Stellen Sie sicher, dass das NAT-Netzwerk als NAT-Netzwerk vom Typ 1:n konfiguriert ist. Die Aktion ist für 1:1-NAT-Netzwerke nicht verfügbar.

Verfahren

- 1 Wählen Sie **Elemente > Bereitstellung** aus.
- 2 Suchen Sie die Bereitstellung und zeigen Sie deren untergeordnete Komponenten an.



- 3 Wählen Sie die NAT-Netzwerkkomponente aus, die bearbeitet werden soll.



Bei einem mit einem IPAM-Drittanbieter verbundenen bedarfsgesteuerten NAT-Netzwerk können Sie die Komponente nicht bearbeiten. Sie können jedoch manuell eine neue IP-Zieladresse hinzufügen. Wenn Sie eine neue IP-Zieladresse hinzufügen, wird der Komponentenwert auf Null gesetzt. Die neue IP-Zieladresse und die auf Null gesetzte Maschinen-ID werden verarbeitet, wenn Sie die Anforderung zur Neukonfiguration übermitteln.

- 4 Klicken Sie im Menü **Aktionen** auf **NAT-Regeln ändern**.



- 5 Sie können neue NAT-Portweiterleitungsregeln hinzufügen, die Reihenfolge von Regeln ändern, vorhandene Regeln bearbeiten oder Regeln löschen.
- 6 Wenn Sie die Änderungen abgeschlossen haben, klicken Sie auf **Speichern** oder **Absenden**, um die Neukonfigurationsanforderung zu übermitteln.

Hinzufügen oder Entfernen von Sicherheitselementen in einer Bereitstellung

Sie können vorhandene NSX-Sicherheitsgruppen und -Sicherheits-Tags in einer Maschinenbereitstellung hinzufügen oder entfernen. Bedarfsgesteuerte Sicherheitsgruppen können nicht hinzugefügt werden, aber Sie können sie entfernen.

Die Aktion zum Ändern der Sicherheit basiert auf einer Maschinenkomponente oder einem Cluster. Wenn die Sicherheit beispielsweise einem Cluster mit dem Namen AppTier2 zugeordnet ist, der aus 2 Maschinen besteht, können Sie den Vorgang zum Ändern der Sicherheit auf dem Cluster AppTier2 und nicht auf den einzelnen Maschinen im Cluster durchführen.

Der Vorgang zum Ändern der Sicherheit wird nicht für Bereitstellungen unterstützt, die von vRealize Automation 6.2.x auf diese Version von vRealize Automation aktualisiert oder migriert wurden.

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Maschinenbesitzer**, **Supportbenutzer**, **Business-Gruppenbenutzer mit gemeinsam genutztem Zugriff** oder **Business-Gruppenmanager** an.
- Stellen Sie sicher, dass Sie zum Ändern der Sicherheit in einer Bereitstellung berechtigt sind. Die erforderliche Katalogberechtigung ist „Sicherheit ändern (Bereitstellung)“.

Verfahren

- 1 Wählen Sie **Elemente > Bereitstellung** aus.

- 2 Suchen Sie die Bereitstellung und zeigen Sie deren untergeordnete Komponenten an.



- 3 Klicken Sie im Menü **Aktionen** auf **Sicherheit ändern**.



- 4 Wählen Sie die bereitgestellte Maschinenkomponente oder den Cluster zum Hinzufügen oder Entfernen der Sicherheitselemente aus.



- 5 Sie können vorhandene Sicherheitsgruppen und Sicherheits-Tags für jede Maschinenkomponente oder jeden Cluster in der Bereitstellung nach Bedarf hinzufügen oder entfernen.
- 6 Entfernen Sie bedarfsgesteuerte Sicherheitsgruppen für jede Maschinenkomponente oder jeden Cluster in der Bereitstellung nach Bedarf.
- 7 (Optional) Klicken Sie auf die Registerkarte **Grund** und geben Sie einen Grund für die Anforderung ein.
- 8 Wenn Sie die Änderungen abgeschlossen haben, klicken Sie auf **Speichern**, oder klicken Sie auf **Absenden**, um die Änderungsanforderung zu übermitteln.

Anzeigen aller NAT-Regeln für einen vorhandenen NSX Edge

Sie können die Informationen zu NAT-Regel über die NSX Edges anzeigen, die in aktiven Bereitstellungen verwendet werden.

Die NAT-Regeln werden in der Edge-Ansicht als Zusammenfassung aller in der Bereitstellung verwendeten NAT-Regeln angezeigt. In der Edge-Ansicht werden die Regeln nicht notwendigerweise in der Reihenfolge angezeigt, in der sie verarbeitet werden.

Informationen dazu, wie Sie sehen und optional ändern können, in welcher Reihenfolge die NAT-Regeln in einem 1:n-NAT-Netzwerk verarbeitet werden, finden Sie unter [Ändern von NAT-Regeln in einer Bereitstellung](#).

Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Maschinenbesitzer**, **Supportbenutzer**, **Business-Gruppenbenutzer mit gemeinsam genutztem Zugriff** oder **Business-Gruppenmanager** an.

Verfahren

- 1 Wählen Sie **Elemente > Bereitstellung** aus.

- 2 Suchen Sie die Bereitstellung und zeigen Sie deren untergeordnete Komponenten an.



- 3 Wählen Sie den NSX-Edge, den Sie anzeigen möchten.



- 4 Klicken Sie abschließend auf **Schließen**.