

Verwenden und Verwalten von vRealize Automation Cloud Assembly

Oktober 2022

vRealize Automation 8.2

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 © 2022 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

1	Was ist vRealize Automation Cloud Assembly?	7
	Funktionsweise von vRealize Automation Cloud Assembly	8
2	Lernprogramme	11
	Einrichten und Testen der vSphere-Infrastruktur und -Bereitstellungen	13
	Konfigurieren und Bereitstellen einer Produktionsarbeitslast	31
	Multi-Cloud-Infrastruktur und Bereitstellungen	39
	Teil 1: Konfigurieren der Beispielinfrastruktur	39
	Teil 2: Erstellen des Beispielprojekts	46
	Teil 3: Entwerfen und Bereitstellen der Beispiel-Cloud-Vorlage	47
	Konfigurieren von VMware Cloud on AWS	64
	Konfigurieren eines grundlegenden VMware Cloud on AWS-Workflows	65
	Konfigurieren eines isolierten Netzwerks in VMware Cloud on AWS	80
	Konfigurieren einer externen IPAM-Integration für Infoblox	85
	Hinzufügen erforderlicher erweiterbarer Attribute in der Infoblox-Anwendung vor der Bereitstellung des Download-Pakets	86
	Herunterladen und Bereitstellen eines externen IPAM-Anbieterpakets	88
	Erstellen einer Ausführungsumgebung für einen IPAM-Integrationspunkt	89
	Hinzufügen einer externen IPAM-Integration für Infoblox	91
	Konfigurieren eines Netzwerks und Netzwerkprofils zur Verwendung von IPAM (extern) für ein vorhandenes Netzwerk	95
	Definieren und Bereitstellen einer Cloud-Vorlage, die die Bereichszuweisung eines externen IPAM-Anbieters verwendet	98
	Verwenden Infoblox-spezifischer Eigenschaften für IPAM-Integrationen	101
3	Einrichten von vRealize Automation Cloud Assembly für Ihre Organisation	105
	Definition der vRealize Automation-Benutzerrollen	105
	Organisations- und Dienstbenutzerrollen	108
	Benutzerdefinierte Benutzerrollen	121
	Anwendungsbeispiele: Wie können Benutzerrollen mich bei der Steuerung des Zugriffs unterstützen	126
	Hinzufügen von Cloud-Konten	148
	Zum Arbeiten mit Cloud-Konten sind Anmeldedaten erforderlich	149
	Erstellen eines Microsoft Azure-Cloud-Kontos	167
	Erstellen eines Amazon Web Services-Cloud-Kontos	169
	Erstellen eines Google Cloud Platform-Cloud-Kontos	170
	Erstellen eines vCenter-Cloud-Kontos	171
	Erstellen eines NSX-V-Cloud-Kontos	173
	Erstellen eines NSX-T-Cloud-Kontos	175

Erstellen eines VMware Cloud on AWS-Cloud-Kontos	178
Erstellen eines VMware Cloud Foundation-Cloud-Kontos	180
Integrieren in andere Anwendungen	181
Vorgehensweise zum Verwenden der GitLab- und GitHub-Integration	182
Vorgehensweise zum Konfigurieren einer externen IPAM-Integration	188
Vorgehensweise zum Upgrade auf ein neueres externes IPAM-Integrationspaket	190
Konfigurieren der MyVMware-Integration in vRealize Automation Cloud Assembly	192
Konfigurieren der vRealize Orchestrator-Integration in Cloud Assembly	192
Vorgehensweise zum Arbeiten mit Kubernetes in vRealize Automation Cloud Assembly	195
Definition der Konfigurationsverwaltung in vRealize Automation Cloud Assembly	214
Vorgehensweise zum Erstellen einer Active Directory-Integration in vRealize Automation Cloud Assembly	224
Konfigurieren einer VMware SDDC Manager-Integration	226
Integrieren in vRealize Operations Manager	227
Definition von Onboarding-Plänen	236
Integrieren ausgewählter Maschinen als Einzelbereitstellung	237
Integrieren von durch Regeln gefilterten Maschinen als separate Bereitstellungen	240
Erweiterte Konfiguration	245
Vorgehensweise zum Integrieren eines Internet-Proxyservers	246
Wozu dienen NSX-T-Zuordnungen zu mehreren vCentern	250
Was passiert, wenn die Verknüpfung eines NSX-Cloud-Kontos entfernt wird	250
Vorgehensweise zum Verwenden des IPAM-SDK zur Erstellung eines anbieterspezifischen, externen IPAM-Integrationspakets	251
4 Erstellen der Ressourceninfrastruktur	253
Vorgehensweise zum Hinzufügen von Cloud-Zonen	253
Weitere Informationen zu Cloud-Zonen	254
Vorgehensweise zum Hinzufügen von Konfigurationszuordnungen	257
Weitere Informationen zu Konfigurationszuordnungen	257
Vorgehensweise zum Hinzufügen von Image-Zuordnungen	258
Weitere Informationen zu Image-Zuordnungen	258
Vorgehensweise zum Hinzufügen von Netzwerkprofilen	262
Weitere Informationen zu Netzwerkprofilen	262
Verwenden von Netzwerkeinstellungen	270
Verwenden von Sicherheitsgruppeneinstellungen	275
Verwenden der Einstellungen des Lastausgleichsdiensts	277
Vorgehensweise zum Konfigurieren eines Netzwerkprofils zur Unterstützung eines bedarfsgesteuerten Netzwerks für eine externe IPAM-Integration	278
Vorgehensweise zum Konfigurieren eines Netzwerkprofils zur Unterstützung eines vorhandenen Netzwerks für eine externe IPAM-Integration	282
Vorgehensweise zum Hinzufügen von Speicherprofilen	282
Weitere Informationen zu Speicherprofilen	283
Vorgehensweise zum Verwenden von Tags	284

Erstellen einer Tagging-Strategie	286
Verwenden von Funktions-Tags in vRealize Automation Cloud Assembly	288
Verwenden von Einschränkungs-Tags in vRealize Automation Cloud Assembly	289
Standard-Tags	291
Tag-Verarbeitung in vRealize Automation Cloud Assembly	292
Vorgehensweise zum Einrichten einer einfachen Tagging-Struktur	293
Vorgehensweise zum Arbeiten mit Ressourcen	295
Computing-Ressourcen	295
Netzwerkressourcen	295
Sicherheitsressourcen	297
Speicherressourcen	299
Maschinenressourcen	300
Volume-Ressourcen	300
Weitere Informationen zu Ressourcen	300
Konfigurieren von Mehrmandantenressourcen mit vRealize Automation	315
Vorgehensweise zum Erstellen einer virtuellen privaten Zone für vRealize Automation	316
Verwalten der VPZ-Konfiguration für vRealize Automation-Mandanten	319

5 Hinzufügen und Verwalten von Projekten 321

Vorgehensweise zum Hinzufügen eines Projekts für mein Entwicklungsteam	321
Weitere Informationen zu Projekten	324
Verwenden von Projekt-Tags und benutzerdefinierten Eigenschaften	324
Funktionsweise von Projekten zur Bereitstellungszeit	326

6 Entwerfen Ihrer Bereitstellungen 328

Möglichkeiten zum Erstellen von Cloud-Vorlagen	329
Vorgehensweise zum Erstellen einer einfachen Vorlage von Grund auf	331
Vorgehensweise zum Auswählen und Hinzufügen von Ressourcen zu einer Cloud-Vorlage	332
Verbinden von Cloud-Vorlagenressourcen	332
Vorgehensweise zum Erstellen von gültigem Cloud-Vorlagencode	334
Vorgehensweise zum Speichern verschiedener Versionen	336
Vorgehensweise zum Verbessern einer einfachen Cloud-Vorlage	338
Anpassen einer Cloud-Vorlage mit Benutzereingaben	339
Anpassen einer Anforderung mithilfe von Ressourcen-Flags	344
Vorgehensweise zum Festlegen der Reihenfolge der Ressourcenbereitstellung	347
Vorgehensweise zum Verwenden von Ausdrücken zur flexibleren Gestaltung von Cloud-Vorlagencode	348
Vorgehensweise zum Aktivieren des Remotezugriffs in Cloud-Vorlagen	357
Vorgehensweise zum Hinzufügen von erweiterten Funktionen zu Designs	361
Vorgehensweise zum Anpassen der Namen bereitgestellter Ressourcen	361

Vorgehensweise zum automatischen Initialisieren einer Maschine in einer Cloud-Vorlage	364
Vorgehensweise zum Erstellen benutzerdefinierter Ressourcentypen zur Verwendung in Cloud-Vorlagen	379
So bereiten Sie die Tag-2-Änderungen vor	390
Vorgehensweise zum Erweitern und Automatisieren der Lebenszyklen von Anwendungen mit Erweiterbarkeit	397
Eigenschaften der Ressource	440
Codebeispiele	441
vSphere-Ressourcenbeispiele in Cloud-Vorlagen	441
Neueinstellbare Cloud-Vorlage	445
Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in Cloud-Vorlagen	452
Puppet-fähige Cloud-Vorlage mit Zugriff auf Benutzernamen und Kennwort	474
Vorgehensweise zum Integrieren von Terraform-Konfigurationen	485
Vorbereiten einer Terraform-Laufzeitumgebung	485
Vorbereiten auf Terraform-Konfigurationen	492
Entwerfen für Terraform-Konfigurationen	493
Weitere Informationen zu Terraform-Konfigurationen	497
Vorgehensweise zum Verwenden des Marketplace	501

7 Verwalten von Bereitstellungen 502

Vorgehensweise zum Überwachen von Bereitstellungen	503
Vorgehensweise beim Fehlschlagen einer vRealize Automation Cloud Assembly-Bereitstellung	504
Vorgehensweise zum Verwalten des Lebenszyklus einer abgeschlossenen Bereitstellung	508
Welche Aktionen kann ich auf Bereitstellungen ausführen?	510

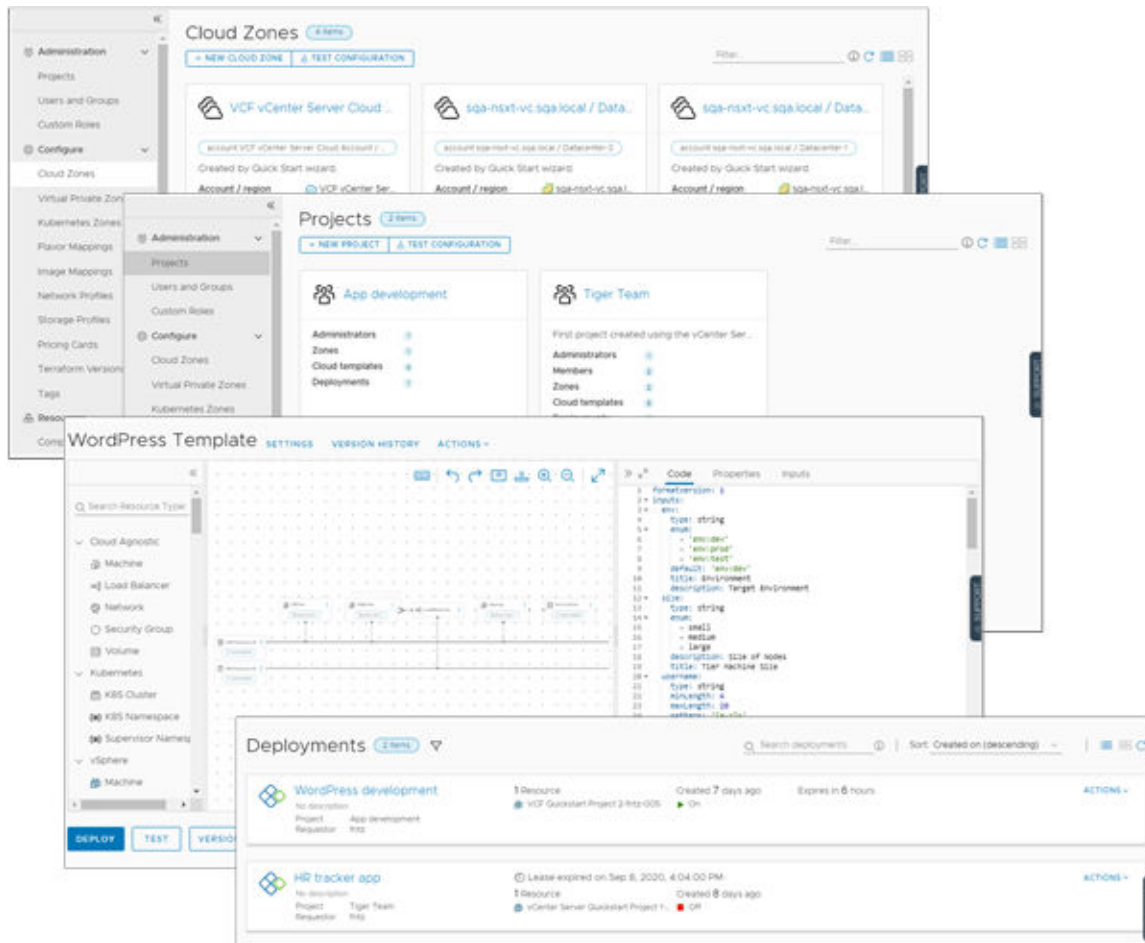
Was ist vRealize Automation Cloud Assembly?

1

Mit vRealize Automation Cloud Assembly stellen Sie eine Verbindung zu Ihren Public und Private Cloud-Anbietern her, damit Sie Maschinen, Anwendungen und Dienste bereitstellen können, die Sie für diese Ressourcen erstellen. Sie und ihre Teams entwickeln Cloud-Vorlagen-as-Code in einer Umgebung, die einen iterativen Workflow unterstützt, von der Entwicklung über die Tests bis zur Freigabe für die Produktionsumgebung. Bei der Bereitstellung können Sie eine Reihe von Cloud-Anbietern einsetzen. Der Dienst ist ein verwaltetes VMware-Framework auf SaaS- und NaaS-Basis.

Als Übersicht über vRealize Automation Cloud Assembly werden hier die folgenden allgemeinen Funktionen beschrieben.

- Auf der Registerkarte „Infrastruktur“ können Sie Ihre Cloud-Anbieter-Ressourcen und -Benutzer hinzufügen und organisieren. Diese Registerkarte enthält auch Informationen zu den bereitgestellten Cloud-Vorlagen.
- Die Registerkarte „Download-Center“ bietet VMware Solution Exchange-Cloud-Vorlagen und -Images, mit denen Sie Ihre Vorlagenbibliothek erstellen und auf unterstützende OVAs oder OVFes zugreifen können.
- Die Registerkarte „Design“ fungiert als Startseite für die Entwicklung. Die Arbeitsfläche und den YAML-Editor verwenden Sie zur Entwicklung und Bereitstellung von Maschinen und Anwendungen.
- Auf der Registerkarte „Entwicklung“ wird der aktuelle Status Ihrer bereitgestellten Ressourcen angezeigt. Sie können auf Details und Verlauf zugreifen, die Sie zum Verwalten Ihrer Bereitstellungen verwenden.



Dieses Kapitel enthält die folgenden Themen:

- Funktionsweise von vRealize Automation Cloud Assembly

Funktionsweise von vRealize Automation Cloud Assembly

Bei vRealize Automation Cloud Assembly handelt es sich um einen Entwicklungs- und Bereitstellungsdienst für Cloud-Vorlagen. Sie und ihre Teams verwenden den Dienst, um Ihren Cloud-Anbieterressourcen Maschinen, Anwendungen und Dienste bereitzustellen.

Als Cloud Assembly-Administrator, in der Regel als Cloud-Administrator bezeichnet, richten Sie die Bereitstellungsinfrastruktur ein und erstellen die Projekte, die Benutzer und Ressourcen gruppieren.

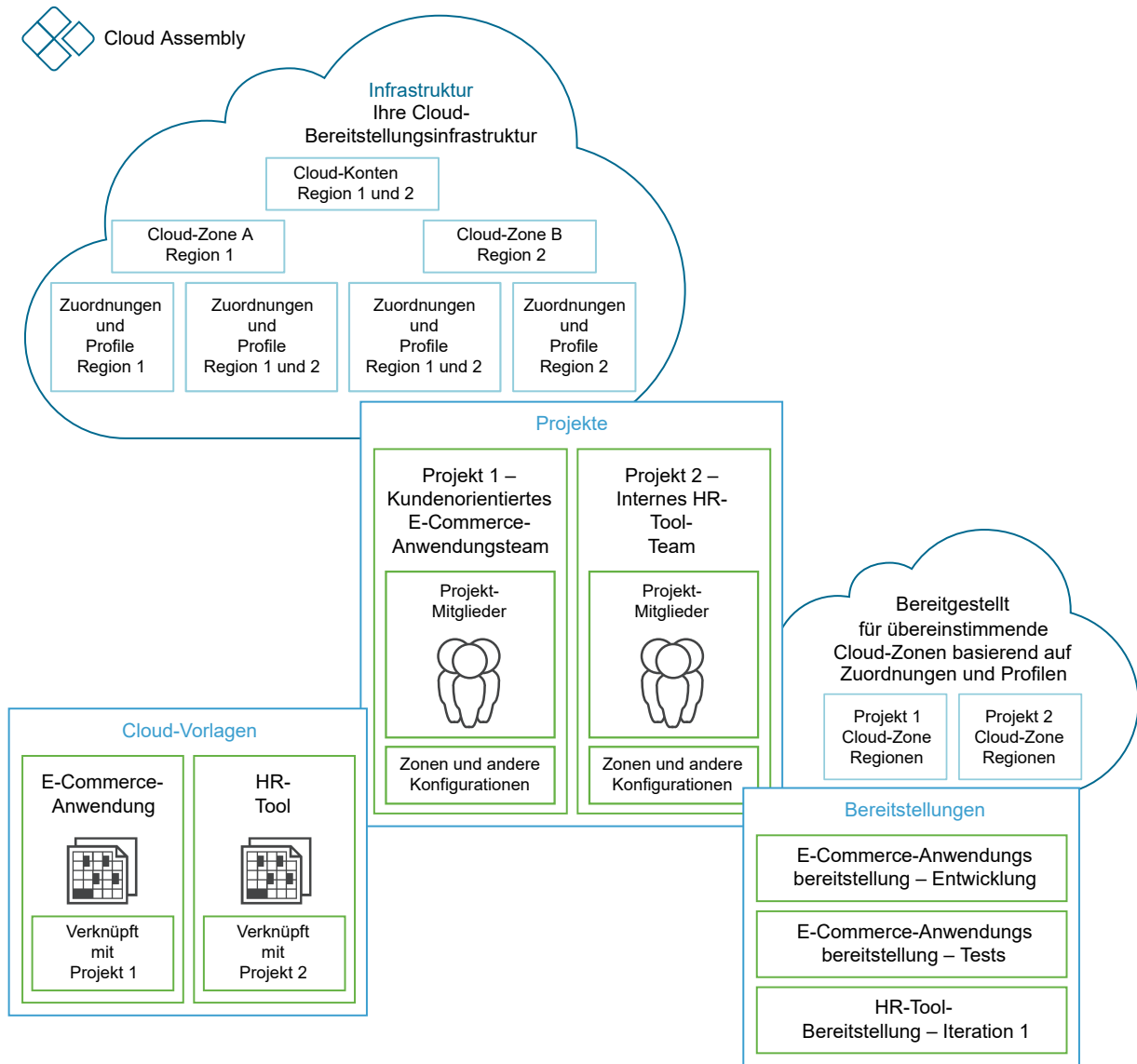
- Fügen Sie Ihre Cloud-Anbieterkonten hinzu. Weitere Informationen hierzu finden Sie unter [Hinzufügen von Cloud-Konten zu vRealize Automation Cloud Assembly](#).
- Legen Sie die Regionen und Datenspeicher fest, die als Cloud-Zonen für Bereitstellungen der Entwickler dienen sollen. Weitere Informationen hierzu finden Sie unter [Weitere Informationen zu vRealize Automation Cloud Assembly-Cloud-Zonen](#).

- Erstellen Sie Richtlinien, die die Cloud-Zonen definieren. Weitere Informationen hierzu finden Sie unter [Kapitel 4 Erstellen der vRealize Automation Cloud Assembly-Ressourceninfrastruktur](#).
- Erstellen Sie Projekte, die die Entwickler mit den Cloud-Zonen gruppieren. Weitere Informationen hierzu finden Sie unter [Verwenden von vRealize Automation Cloud Assembly-Projekt-Tags und benutzerdefinierten Eigenschaften](#).

Als Cloud-Vorlagenentwickler sind Sie Mitglied eines oder mehrerer Projekte. Sie erstellen Vorlagen und stellen sie in den Cloud-Zonen bereit, die mit einem Ihrer Projekte verknüpft sind.

- Entwickeln Sie Cloud-Vorlagen für Projekte mithilfe der Arbeitsfläche. Ihr Projektadministrator kann den Marketplace verwenden, um Vorlagen und unterstützende Images aus VMware Solution Exchange herunterzuladen. Weitere Informationen finden Sie unter [Kapitel 6 Entwerfen Ihrer vRealize Automation Cloud Assembly-Bereitstellungen und Vorgehensweise zum Verwenden des vRealize Automation Cloud Assembly-Marketplace](#).
- Stellen Sie Ihre Cloud-Vorlagen basierend auf Richtlinien und Einschränkungen in den Cloud-Zonen eines Projekts bereit.
- Verwalten Sie Ihre Bereitstellungen und löschen Sie nicht verwendete Anwendungen. Weitere Informationen hierzu finden Sie unter [Kapitel 7 Verwalten von vRealize Automation Cloud Assembly-Bereitstellungen](#).

Willkommen bei vRealize Automation Cloud Assembly. Wenn Sie ein Beispiel für die Definition der Infrastruktur benötigen und anschließend eine Cloud-Vorlage erstellen und bereitstellen möchten, finden Sie weitere Informationen unter [Lernprogramm: Einrichten und Testen einer Multi-Cloud-Infrastruktur und von Bereitstellungen in vRealize Automation Cloud Assembly](#).



Cloud Assembly-Lernprogramme

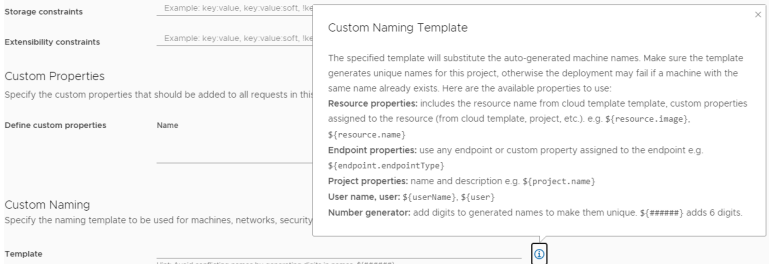
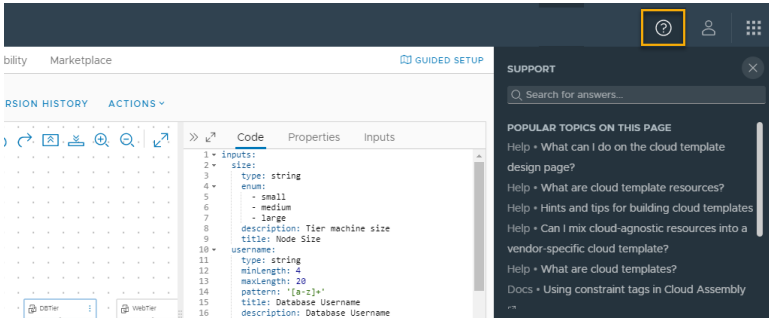
2

In diesen Lernprogrammen erhalten Sie Informationen zur Durchführung allgemeiner Aufgaben, die Sie dabei unterstützen, sich mit vRealize Automation Cloud Assembly vertraut zu machen.

Zunächst möchten wir Sie daran erinnern, dass zusätzlich zu den Schritten in diesen Lernprogrammen weitere Informationen in diesem Handbuch bereitstehen. Links zu relevanten Themen werden bereitgestellt.

Zugriff auf Benutzerunterstützung

Die ebenfalls wichtige Benutzerunterstützung wird in der gesamten Anwendung bereitgestellt. Die Benutzerunterstützung hilft Ihnen dabei, Funktionen zu verstehen, und stellt Informationen bereit, mit denen Sie Entscheidungen bezüglich des Ausfüllens von Textfeldern treffen können. Die externe Dokumentation enthält ausführliche Informationen, Codebeispiele und Anwendungsfälle.

Typ der Unterstützung	Vorgehensweise zum Zugreifen auf die Unterstützung	Beispiel
Wegweiser-Hilfe auf Feldebene	Klicken Sie auf das Symbol Info (i) neben einem Feld.	
Kontexthilfe im Support-Bereich	Klicken Sie auf das Hilfesymbol (?) neben Ihrem Namen und Ihrer Organisation.	
Zugriff auf die externe Dokumentation	Klicken Sie auf den Titel eines Artikels mit der Bezeichnung Docs oder klicken Sie auf Mehr anzeigen in VMware Docs .	

Dieses Kapitel enthält die folgenden Themen:

- Lernprogramm: Einrichten und Testen der vSphere-Infrastruktur und -Bereitstellungen in vRealize Automation Cloud Assembly
- Lernprogramm: Konfigurieren von vRealize Automation Cloud Assembly zur Bereitstellung einer Produktionsarbeitslast
- Lernprogramm: Einrichten und Testen einer Multi-Cloud-Infrastruktur und von Bereitstellungen in vRealize Automation Cloud Assembly
- Lernprogramm: Konfigurieren von VMware Cloud on AWS für vRealize Automation

- [Lernprogramm: Konfigurieren einer anbieterspezifischen externen IPAM-Integration für vRealize Automation](#)

Lernprogramm: Einrichten und Testen der vSphere-Infrastruktur und -Bereitstellungen in vRealize Automation Cloud Assembly

Wenn Sie noch nicht mit vRealize Automation vertraut sind oder lediglich einen Auffrischkurs benötigen, leitet Sie dieses Lernprogramm durch den Konfigurationsprozess für vRealize Automation Cloud Assembly. Sie durchlaufen den Prozess, indem Sie vSphere-Cloud-Konto-Endpoints hinzufügen, die Infrastruktur definieren, Benutzer zu Projekten hinzufügen und anschließend eine Arbeitslast mithilfe von VMware Cloud Templates basierend auf vSphere-Ressourcentypen entwerfen und bereitstellen.

Obwohl dieses Lernprogramm lediglich die Grundlagen liefert, sind Sie bereits jetzt in der Lage, Self-Service-Automatisierung und iterative Entwicklung bereitzustellen, die auf mehreren öffentlichen und privaten Clouds funktioniert. Dieses Handbuch konzentriert sich auf VMware vCenter Server und NSX-T. Nach Abschluss dieses Workflows können Sie das Gelernte anwenden, um weitere Typen von Cloud-Konten hinzuzufügen und ausgereifte Cloud-Vorlagen bereitzustellen.

Beim Durchführen der Schritte werden Datenbeispiele bereitgestellt. Ersetzen Sie die Beispiele durch Werte, die für Ihre Umgebung geeignet sind.

Sie führen alle Schritte in diesem Lernprogramm in vRealize Automation Cloud Assembly durch.

Dieses Lernprogramm dient als Leitfaden beim Konfigurieren der einzelnen erforderlichen Komponenten.

- [Schritt 1: Hinzufügen der vCenter Server- und NSX Cloud-Konten](#). Bei Cloud-Konten handelt es sich um die Anmeldedaten, über die vRealize Automation Cloud Assembly mit den Endpoints Ihres Cloud-Anbieters verbunden wird.
- [Schritt 2: Definieren der Computing-Ressourcen für die Cloud-Zone](#). Bei Cloud-Zonen handelt es sich um die ausgewählten Computing-Ressourcen in Konten/Regionen, die Sie anschließend basierend auf den Projektanforderungen und Ihren Zielen für die Verwaltung von Compliance und Kosten verschiedenen Projekten zuweisen.
- [Schritt 3: Konfigurieren der möglichen Ressourcen, die für das Konto/die Region verfügbar sind](#). Infrastrukturressourcen sind Definitionen von Computing-, Speicher-, Netzwerk- und anderen Ressourcen, die mit den in Cloud-Vorlagen verwendeten Konten/Regionen verknüpft sind.
- [Schritt 4: Erstellen eines Projekts](#). Projekte legen fest, wie Sie Ihren Benutzern basierend auf den Anwendungsentwicklungszielen des Projekts Zugriff auf die Cloud-Zonen erteilen.
- [Schritt 5: Entwerfen und Bereitstellen einer grundlegenden Cloud-Vorlage](#). Bei Cloud-Vorlagen handelt es sich um die Definitionen Ihrer Anwendungsarbeitslasten, die Sie iterativ entwickeln und bereitstellen.

Dieser Konfigurationsprozess stellt die Grundlage Ihrer Cloud Assembly-Entwicklungserfahrung dar. Während Sie die Infrastruktur erstellen und Ihre Kenntnisse im Bereich der Entwicklung von Cloud-Vorlagen festigen, wiederholen und erweitern Sie diesen Workflow.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie über die Cloud Assembly-Administratorrolle verfügen. Weitere Informationen hierzu finden Sie unter [Organisations- und Dienstbenutzerrollen in vRealize Automation](#).
- Wenn Sie die Schnellstart-Assistenten von VMware vCenter Server oder VMware Cloud Foundation nicht in der vRealize Automation-Konsole verwendet haben, können Sie dies jetzt tun.

Diese assistentengesteuerten Workflows enthalten die meisten, aber nicht alle Konfigurationen in diesem Lernprogramm.

Dieses Lernprogramm bietet praktische Übungen zur Erweiterung Ihrer Kenntnisse bezüglich des Aufbaus einer funktionierenden Infrastruktur und der Bereitstellung einer Arbeitslast.

Weitere Informationen finden Sie unter [Vorgehensweise zum Einrichten von Cloud Assembly](#) im Handbuch *Erste Schritte*.

- Wenn Sie das in vRealize Automation Cloud Assembly zur Verfügung stehende geführte Setup noch nicht verwendet haben, können Sie dies jetzt tun. Beim geführten Setup werden Sie durch die meisten, aber nicht durch alle Verfahren in diesem Lernprogramm geführt. Klicken Sie zum Öffnen des geführten Setups auf der rechten Seite der Registerkartenleiste auf **Geführtes Setup**.
- Stellen Sie sicher, dass Sie über vCenter Server- und NSX-Anmeldedaten verfügen. Weitere Informationen zu den Berechtigungen, die die Anmeldedaten aufweisen müssen, finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#). Wenn Sie weitere Benutzer zu Projekten hinzufügen möchten, stellen Sie sicher, dass diese Mitglieder des vRealize Automation Cloud Assembly-Diensts sind.

Schritt 1: Hinzufügen der vCenter Server- und NSX Cloud-Konten

Die Cloud-Konten stellen die Anmeldedaten bereit, mit denen vRealize Automation eine Verbindung mit vCenter Server und dem zugeordneten NSX-Server herstellt.

- 1 Fügen Sie das vCenter Server-Cloud-Konto hinzu.

Im vCenter Server-Cloud-Konto werden die vCenter-Anmeldedaten bereitgestellt, die von vRealize Automation Cloud Assembly zum Erkennen von Ressourcen und Bereitstellen von Cloud-Vorlagen verwendet werden.

Weitere Informationen zu vCenter Server-Cloud-Konten finden Sie unter [Erstellen Sie ein vCenter-Cloud-Konto in vRealize Automation](#).

- a Wählen Sie **Infrastruktur > Verbindungen > Cloud-Konten** aus.
- b Klicken Sie auf **Cloud-Konto hinzufügen** und wählen Sie **vCenter** aus.

- c Geben Sie die Werte ein.

New Cloud Account

Name * vCenter Server Account

Description

vCenter Server Credentials

vCenter IP address / FQDN * sc2vc05.cmbu.local ⓘ

Username * mgmt@cmbu.local

Password *

VALIDATE ✔ Credentials validated successfully. ✕

Configuration

Allow provisioning to these datacenters * ☒ wld01-DC

☒ Create a cloud zone for the selected datacenters

NSX cloud account

Capabilities

Capability tags ⓘ

ADD **CANCEL**

Beachten Sie, dass diese Werte nur Beispiele darstellen. Die Werte sind für Ihre Umgebung spezifisch.

Einstellung	Beispielwert
Name	vCenter Server-Konto
IP-Adresse/FQDN für vCenter	your-dev-vcenter.company.com
Benutzername und Kennwort	vCenterCredentials@yourCompany.com

- d Klicken Sie zum Überprüfen der Anmeldedaten auf **Überprüfen**.
- e Wenn Sie die **Bereitstellung für diese Datacenter zulassen** möchten, wählen Sie ein oder mehrere Datacenter aus.
- f Überspringen Sie das NSX Cloud-Konto. Die Konfiguration erfolgt zu einem späteren Zeitpunkt, indem das vCenter Server-Konto mit dem NSX Cloud-Konto verknüpft wird.
- g Klicken Sie auf **Hinzufügen**.
- 2 Fügen Sie ein zugeordnetes NSX Cloud-Konto hinzu.

Das NSX-T-Cloud-Konto stellt die NSX-T-Anmeldedaten bereit, die von vRealize Automation Cloud Assembly zum Erkennen von Netzwerkressourcen und Bereitstellen von Netzwerken mit Cloud-Vorlagen verwendet werden.

Weitere Informationen zu NSX-T-Cloud-Konten finden Sie unter [Erstellen Sie ein vCenter-Cloud-Konto in vRealize Automation..](#)

- Wählen Sie **Infrastruktur > Verbindungen > Cloud-Konten** aus.
- Klicken Sie auf **Cloud-Konto hinzufügen** und wählen Sie entweder „NSX-T“ oder „NSX-V“ aus. In diesem Lernprogramm wird **NSX-T** verwendet.
- Geben Sie die Werte ein.

New Cloud Account

Name * NSX-T Account

Description

NSX-T Credentials

NSX-T IP address / FQDN * sc2vc05-vip-nsx-mgmt.cmbu.local ⓘ

Username * mgmt@cmbu.local

Password *

NSX mode Policy ⓘ

VALIDATE ✔ Credentials validated successfully. ✕

Associations

vCenter cloud accounts + ADD ✕ REMOVE

<input type="checkbox"/>	Name	Status	Identifier	Type
<input type="checkbox"/>	vCenter Server Account	✔ OK	sc2vc05.cmbu.local	vCenter

1 - 1 of 1 cloud accounts

Capabilities

Capability tags Enter capability tags ⓘ

ADD CANCEL

Bei diesen Werten handelt es sich nur um Beispiele. Die Werte sind für Ihre Umgebung spezifisch.

Einstellung	Beispielwert
Name	NSX-T-Konto
IP-Adresse/FQDN für vCenter	your-dev-NSX-vcenter.company.com

Einstellung	Beispielwert
Benutzername und Kennwort	NSXCredentials@yourCompany.com
NSX-Modus	<p>Sie wissen nicht, was Sie auswählen sollen?</p> <p>Dies ist eine gute Gelegenheit, die in das Produkt integrierte Hilfe zu verwenden. Klicken Sie rechts neben dem betreffenden Feld auf das Informationssymbol. Beachten Sie, dass die Hilfe auf Feldebene Informationen enthält, die Sie bei der Konfiguration der Option unterstützen können.</p> <p>In diesem Beispiel wählen Sie Richtlinie aus.</p>

- d Klicken Sie zum Überprüfen der Anmeldedaten auf **Überprüfen**.
- e Um das im vorherigen Schritt erstellte vCenter Cloud-Konto zu verknüpfen, klicken Sie auf **Hinzufügen** und wählen Sie dann das **vCenter-Konto** aus.

Diese Verknüpfung des vCenter Cloud-Kontos gewährleistet Netzwerksicherheit.

- f Klicken Sie auf der Seite für das NSX Cloud-Konto auf **Hinzufügen**.

Schritt 2: Definieren der Computing-Ressourcen für die Cloud-Zone

Bei Cloud-Zonen handelt es sich um Gruppen von Computing-Ressourcen in einem Konto/ einer Region, die dann Projekten zur Verfügung gestellt werden. Die Projektmitglieder stellen Cloud-Vorlagen mithilfe der Ressourcen in den zugewiesenen Cloud-Zonen bereit. Um die Bereitstellungspunkte für die Cloud-Vorlagen des Projekts präziser zu steuern, können Sie mehrere Cloud-Zonen mit verschiedenen Computing-Ressourcen erstellen.

Über Konten/Regionen wird festgelegt, wie Cloud-Anbieter Ressourcen mit isolierten Regionen oder Datenspeichern verknüpfen. Das Konto gibt den Cloud-Kontotyp und die Region den Datenspeicher an. vCenter Server verwendet Datenspeicher, und die Bereitstellungsressourcen stellen die ausgewählten Cluster und Ressourcenpools dar.

Bei diesem Lernprogramm müssen Sie sicherstellen, dass die Cloud-Zonen die Ressourcen enthalten, die die Ziele des Projektentwicklungsteams und Ihre Budget- und Verwaltungsanforderungen unterstützen.

Weitere Informationen über Cloud-Zonen finden Sie unter [Weitere Informationen zu vRealize Automation Cloud Assembly-Cloud-Zonen](#).

- 1 Wählen Sie **Infrastruktur > Konfigurieren > Cloud-Zonen** aus.
- 2 Klicken Sie auf die für Ihre vCenter Server-Instanz hinzugefügte Cloud-Zone und geben Sie die Werte ein.

vCenter Account Cloud Zone DELETE

Summary Compute Projects

A cloud zone defines a set of compute resources that can be used for provisioning.

Account / region * vCenter Account / wild01-DC

Name * vCenter Account Cloud Zone

Description

Placement policy * DEFAULT ⓘ

Folder Select folder ⓘ

Capabilities

Capability tags are effectively applied to all compute resources in this cloud zone, but only in the context of this cloud zone.

Capability tags Enter capability tags ⓘ

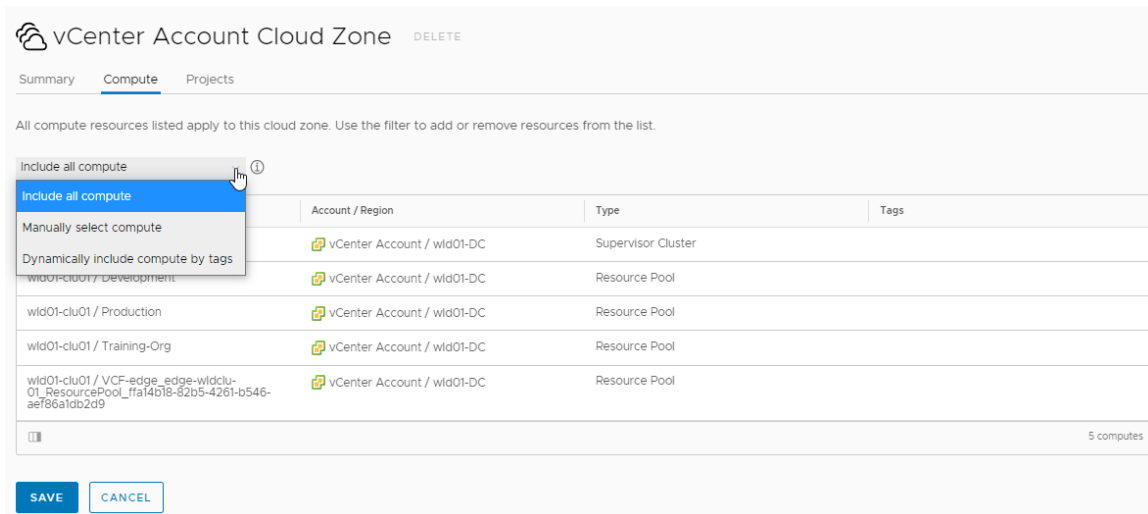
SAVE CANCEL

Einstellung	Beispielwert
Konto/Region	Name des vCenter-Kontos/-Datencenters
Name	vCenter Server-Cloud-Zone Dieser Wert kann nach seiner Erstellung nicht geändert werden. Wenn Sie ein anderes Datencenter für einen anderen vCenter Server konfigurieren möchten, müssen Sie eine neue Cloud-Zone erstellen, in der Sie das Konto bzw. die Region auswählen können.
Beschreibung	Alle vCenter Server-Computing-Ressourcen für die Entwicklung.
Richtlinie	Standard Bei Fragen zu einem Feldwert finden Sie weitere Informationen in der Hilfe.

Beachten Sie, dass alle Werte nur Beispiele sind. Ihre Zonenspezifikationen sind für Ihre Umgebung spezifisch.

- Klicken Sie auf die Registerkarte **Berechnen** und stellen Sie sicher, dass alle Computing-Ressourcen vorhanden sind.

Wenn Sie eine Ressource ausschließen müssen, wechseln Sie zu **Berechnung manuell auswählen** und fügen Sie nur diejenigen Ressourcen hinzu, die Sie in die Cloud-Zone aufnehmen möchten.



4 Klicken Sie auf **Speichern**.

5 Wiederholen Sie den Vorgang für alle zusätzlichen Cloud-Zonen. Stellen Sie dabei jedoch sicher, dass die Zonennamen eindeutig sind.

Schritt 3: Konfigurieren der möglichen Ressourcen, die für das Konto/die Region verfügbar sind

Sie haben das Konto/die Region zur Cloud-Zone hinzugefügt. Nun definieren Sie die möglichen Maschinengrößen (Typzuordnungen), Image-Zuordnungen, Netzwerkprofile und Speicherprofile für das Cloud-Konto. Die Zuordnungs- und Profildefinitionen werden bei der Bereitstellung einer Cloud-Vorlage auf Übereinstimmung geprüft, wobei sichergestellt wird, dass die Arbeitslast die entsprechende Maschinengröße (Typ), das Image, die Netzwerke und den Speicher enthält.

1 Konfigurieren Sie die Typzuordnungen für das Konto bzw. die Regionen.

Typen werden manchmal als „T-Shirt-Sizing“ bezeichnet. Je nach Konfiguration der Cloud-Vorlage bestimmt die angewendete Typzuordnung die Anzahl der CPUs und den Arbeitsspeicher.

Weitere Informationen zu Typzuordnungen finden Sie unter [Weitere Informationen zu Konfigurationszuordnungen in vRealize Automation](#).

a Wählen Sie **Infrastruktur > Konfigurieren > Typzuordnungen** aus.

b Klicken Sie auf **Neue Typzuordnung** und geben Sie Werte ein, die kleine, mittlere und große Maschinen definieren.

Beachten Sie, dass es sich hierbei um Beispielwerte handelt. Sie müssen die relevanten Konten/Regionen auswählen und die Größe definieren.

small DELETE

Allows you to define flavors by name in a cloud-agnostic way. ⓘ

Flavor name * small

Configuration *

Account / Region	Value
vCenter Account / wld01-DC	2
	1

GB ▾ + -

Einstellung	Beispielwert
Konfigurationsname	small
Konto/Region	vCenter-Konto/-Datencenter
CPU-Wert	2
Arbeitsspeicherwert	1 GB

- c Klicken Sie auf **Erstellen**.
- d Um zusätzliche Größen zu erstellen, konfigurieren Sie mittlere (medium) und große (large) Typzuordnungen für das Konto bzw. die Region.

Einstellung	Beispielwert
Konfigurationsname	medium
Konto/Region	vCenter-Konto/-Datencenter
CPU-Wert	4
Arbeitsspeicherwert	2 GB
Konfigurationsname	large
Konto/Region	vCenter-Konto/-Datencenter
CPU-Wert	8
Arbeitsspeicherwert	4 GB

- 2 Konfigurieren Sie die Image-Zuordnungen für das Konto bzw. die Regionen.

Bei den Images handelt es sich um das Betriebssystem für Maschinen in der Cloud-Vorlage. Wenn Sie mit vCenter Server-Images arbeiten, wählen Sie vCenter-Vorlagen aus.

Weitere Informationen zu Image-Zuordnungen finden Sie unter [Weitere Informationen zu Image-Zuordnungen in vRealize Automation](#).

- a Wählen Sie **Infrastruktur > Konfigurieren > Image-Zuordnungen** aus.
- b Klicken Sie auf **Neue Image-Zuordnung** und suchen Sie nach den Images für das Konto bzw. die Region.

Beachten Sie, dass es sich hierbei um Beispielwerte handelt. Sie müssen relevante Images auswählen, die in Ihrem Konto bzw. Ihrer Region ermittelt wurden.


Einstellung	Beispielwert
Image-Name	centos
Konto/Region	vCenter-Konto
Image	centos7

- c Klicken Sie auf **Erstellen**.
 - d Wiederholen Sie den Vorgang, um zusätzliche Image-Zuordnungen zu erstellen. Beispielsweise eine Ubuntu-Zuordnung für das Konto/die Region.
- 3 Konfigurieren Sie Netzwerkprofile.

Mit Netzwerkprofilen werden die Netzwerke und Netzwerkeinstellungen definiert, die für ein Konto/eine Region verfügbar sind. Die Profile müssen die Zielbereitstellungsumgebungen unterstützen.


In dieser Aufgabe wird die Mindestkonfiguration für eine erfolgreiche Durchführung bereitgestellt. Wenn Sie weitere Informationen zu Netzwerkprofilen benötigen, beginnen Sie mit [Weitere Informationen zu Netzwerkprofilen in vRealize Automation](#).

- a Wählen Sie **Infrastruktur > Konfigurieren > Netzwerkprofil** aus.
- b Klicken Sie auf **Neues Netzwerkprofil** und erstellen Sie ein Profil für das Konto bzw. die Region „vCenter Server/Datencenter“.

 **Network Profile** [DELETE](#)

[Summary](#) [Networks](#) [Network Policies](#) [Load Balancers](#) [Security Groups](#)


A network profile defines a group of networks and network settings used when machines are provisioned.

Account / region  vCenter Account / wld01-DC

Name *


Description

Capabilities
Capability tags listed here are matched to constraint tags in the cloud template.


Capability tags 

Einstellung	Beispielwert
Konto/Region	vCenter-Konto/-Datencenter
Name	Netzwerkprofil
Beschreibung	Netzwerke für Entwicklungsteams.







- c Klicken Sie auf die Registerkarte **Netzwerke** und dann auf **Netzwerk hinzufügen**.

 **Network Profile** [DELETE](#)

[Summary](#) [Networks](#) [Network Policies](#) [Load Balancers](#) [Security Groups](#)

Networks listed here are used when provisioning to existing, on-demand, or public networks. 

[+ ADD NETWORK](#) [TAGS](#) [MANAGE IP RANGES](#) [REMOVE](#)

<input type="checkbox"/>	Name	Account / Region	Zone	Network Domain	CIDR	Support Public IP	Default for Zone	Origin	Tags
<input type="checkbox"/>	DevProject-004	 NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	192.168.1.64/27	--	--	 Deployed	
<input type="checkbox"/>	External-mcm13/3520-150877845350	 NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	172.16.1.64/28	--	--	 Discovered	
<input type="checkbox"/>	seg-domain-c8e2a5389de-2772-43f5-9eaa-eddc05e35996-vmware-system-nsx-0	 NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	10.244.0.0/28	--	--	 Discovered	external_id.8... ncp/project_u... ncp/cluster.d... ncp/version.1... ncp/project.v...

1 - 3 of 3 networks

- d Wählen Sie die NSX-Netzwerke aus, die Sie für das Anwendungsentwicklungsteam verfügbar machen möchten.

In diesem Beispiel wurde ein NSX-T-Netzwerk mit dem Namen „DevProject-004“ verwendet.

- e Klicken Sie auf die Registerkarte **Netzwerkrichtlinien** und erstellen Sie eine Richtlinie.

Einstellung	Beispielwert
Isolierungsrichtlinie	Keine
Logischer Tier-0-Router	Tier-0-Router
Edge-Cluster	EdgeCluster

f Klicken Sie auf **Erstellen**.

4 Konfigurieren Sie Speicherprofile.

Speicherprofile definieren die Festplatten für ein Konto/eine Region. Die Profile müssen die Zielbereitstellungsumgebungen unterstützen.

Weitere Informationen zu Speicherprofilen finden Sie unter [Weitere Informationen zu Speicherprofilen in vRealize Automation](#).

- Wählen Sie **Infrastruktur > Konfigurieren > Speicherprofil** aus.
- Klicken Sie auf **Neues Speicherprofil** und erstellen Sie ein Profil für das Konto bzw. die Region „vCenter Server/Datencenter“.

Sofern die Tabelle keine anderen Angaben enthält, behalten Sie die Standardwerte bei.

Storage Profile

Account / region: vCenter Account / wld01-DC

Name: Storage Profile

Description:

Disk type: ☒ Standard disk ☐ First class disk (FCD) ⓘ

Storage policy: Datastore default ⓘ

Datastore / cluster: wld01-sc2vc05-wld01-clu01-vsan01 ⓘ

Provisioning type: Unspecified ⓘ

Shares: Unspecified ⓘ

Limit IOPS: ⓘ

Disk mode: Dependent ⓘ

☐ Supports encryption ⓘ

☒ Preferred storage for this region ⓘ

Capability tags: Enter capability tags ⓘ

SAVE **CANCEL**

Einstellung	Beispielwert
Konto/Region	vCenter-Konto/-Datencenter
Name	Speicherprofil
Datenspeicher/Cluster	Wählen Sie einen Datenspeicher mit ausreichender Kapazität aus, auf den alle Hosts zugreifen können.
Bevorzugter Speicher für diese Region	Aktivieren Sie das Kontrollkästchen.

c Klicken Sie auf **Erstellen**.

Schritt 4: Erstellen eines Projekts

An diesem Punkt beginnen Sie wirklich, über die Projektziele nachzudenken.

- Welche Benutzer benötigen Zugriff auf die Computing-Ressourcen, damit Sie eine Cloud-Vorlage für eine Anwendung erstellen und bereitstellen können? Weitere Informationen zu den Anzeige- und Ausführungsberechtigungen der verschiedenen Projektrollen finden Sie unter [Organisations- und Dienstbenutzerrollen in vRealize Automation](#).
- Werden die Projektmitglieder Anwendungen erstellen, die sich von der Entwicklung bis zur Produktion erstrecken? Welche Ressourcen werden benötigt?
- Welche Cloud-Zonen benötigen sie? Welche Priorität und welche Grenzwerte sollten für jede Zone des Projekts festgelegt werden?

In diesem Lernprogramm werden wir das Entwicklungsteam beim Erstellen und Weiterentwickeln einer internen Softwareanwendung unterstützen.

In dieser Aufgabe wird die Mindestkonfiguration für eine erfolgreiche Durchführung bereitgestellt. Wenn Sie weitere Informationen zu Projekten benötigen, beginnen Sie mit [Weitere Informationen zu vRealize Automation Cloud Assembly-Projekten](#).

- 1 Klicken Sie auf **Infrastruktur > Verwaltung > Projekte**.
- 2 Klicken Sie auf **Neues Projekt** und geben Sie den Namen **Entwicklungsprojekt** ein.
- 3 Klicken Sie auf die Registerkarte **Benutzer** und anschließend auf **Benutzer hinzufügen**.
Sie müssen zu diesem Zeitpunkt keine Benutzer hinzufügen. Wenn jedoch andere Benutzer mit Cloud-Vorlagen arbeiten sollen, müssen sie Mitglieder des Projekts sein.
- 4 Geben Sie E-Mail-Adressen ein, um Benutzer als Projektmitglieder oder Administratoren hinzuzufügen, je nachdem, welche Berechtigungen Sie für jeden einzelnen Benutzer erteilen möchten.

- 5 Klicken Sie auf **Bereitstellung** und dann auf **Zone hinzufügen > Cloud-Zone**.
- 6 Fügen Sie die Cloud-Zonen hinzu, in denen die Benutzer eine Bereitstellung durchführen können.

Sie können auch Ressourcengrenzwerte für die Cloud-Zone im Projekt festlegen. In Zukunft können Sie verschiedene Grenzwerte für andere Projekte festlegen.

Einstellung „Cloud-Projektzone“	Beispielwert
Cloud-Zone	Cloud-Zone des vCenter-Kontos
Bereitstellungspriorität	1
Instanzgrenzwert	5

- 7 Fügen Sie dem Projekt alle zusätzlichen Cloud-Zonen hinzu.

- 8 Klicken Sie auf **Erstellen**.
- 9 Um zu überprüfen, ob das Projekt zur Cloud-Zone hinzugefügt wurde, wählen Sie **Infrastruktur > Konfigurieren > Cloud-Zonen** aus. Öffnen Sie dann die Karte der Cloud-Zone „vCenter-Kontozone“, damit Sie sich die Registerkarte **Projekte** ansehen können. Das Entwicklungsprojekt sollte angezeigt werden.

Schritt 5: Entwerfen und Bereitstellen einer grundlegenden Cloud-Vorlage

Sie können die Cloud-Vorlage entwerfen und bereitstellen, um sicherzustellen, dass Ihre Infrastruktur ordnungsgemäß konfiguriert ist und die Vorlage unterstützt. Später können Sie die Vorlage beim Erstellen einer Anwendung zugrunde legen, die Ihren Projektanforderungen entspricht.

Eine Cloud-Vorlage wird am besten Komponente für Komponente erstellt, wobei überprüft wird, ob sie zwischen den einzelnen Änderungen bereitgestellt wird. Dieses Lernprogramm beginnt mit einer einfachen Maschine. Anschließend werden iterativ weitere Ressourcen hinzugefügt.

In den Beispielen in diesem Verfahren wird der YAML-Code-Editor verwendet. Damit werden Ihnen einfacher Codeausschnitte bereitgestellt. Falls Sie jedoch eine dialogfeldgesteuerte Benutzeroberfläche bevorzugen, klicken Sie auf **Eingaben**.

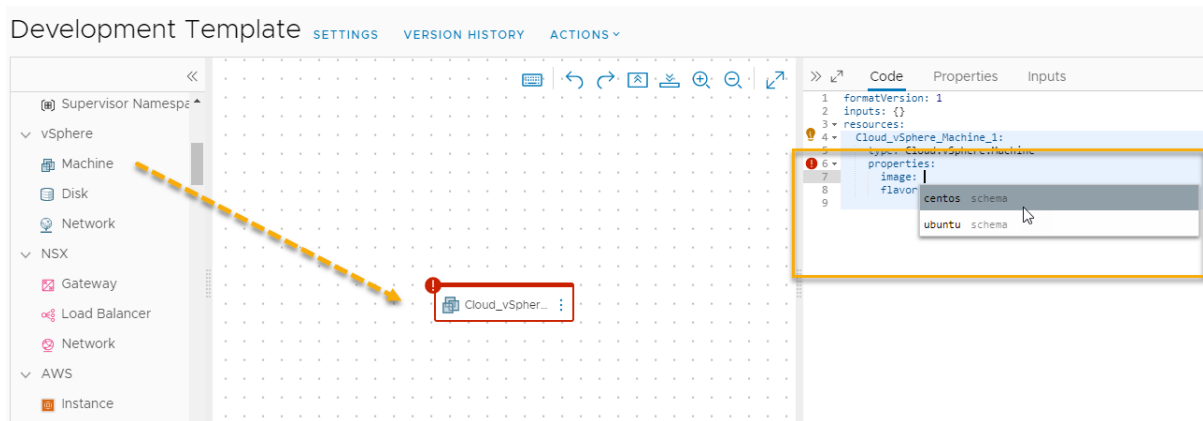
Außerhalb dieses Lernprogramms gibt es noch zahlreiche weitere Einsatzmöglichkeiten für Cloud-Vorlagen. Wenn Sie weitere Informationen benötigen, beginnen Sie mit [Kapitel 6 Entwerfen Ihrer vRealize Automation Cloud Assembly-Bereitstellungen](#).

In diesem Lernprogramm werden vSphere- und NSX-Ressourcentypen verwendet. Diese Ressourcentypen können nur auf vCenter Server-Cloud-Konto-Endpoints bereitgestellt werden. Sie können auch Cloud-unabhängige Ressourcentypen verwenden, um Cloud-Vorlagen zu erstellen, die auf einem beliebigen Endpoint bereitgestellt werden können. Ein Beispiel für die Konfiguration der Infrastruktur und des Designs der Vorlage für einen beliebigen Endpoint finden Sie unter [Lernprogramm: Einrichten und Testen einer Multi-Cloud-Infrastruktur und von Bereitstellungen in vRealize Automation Cloud Assembly](#).



Ein Video, in dem die grundlegenden Schritte in diesem Verfahren veranschaulicht werden, finden Sie unter [Vorgehensweise zum Entfernen und Bereitstellen einer einfachen Cloud-Vorlage](#).

- 1 Wählen Sie **Design > Cloud-Vorlagen** aus.
- 2 Wählen Sie **Neu von > Leere Arbeitsfläche** aus.
- 3 Geben Sie unter **Name Development Template** ein, wählen Sie unter **Projekt** die Option **Development Project** aus und klicken Sie auf **Erstellen**.
- 4 Fügen Sie der Design-Arbeitsfläche eine vSphere-Maschine hinzu, testen Sie sie und stellen Sie sie bereit.



- a Ziehen Sie eine **vSphere-Maschine** aus dem Fensterbereich „Ressourcentyp“ auf die Arbeitsfläche.

Beachten Sie, dass im Fensterbereich **Code** der YAML-Code für die Maschine mit einem leeren Wert für Image und vordefinierte CPU und Speichereigenschaften angezeigt wird. Sie gestalten diese Vorlage so, dass sie eine flexible Größenanpassung unterstützt.

- b Zur Auswahl eines Image-Werts platzieren Sie den Mauszeiger zwischen den einfachen Anführungszeichen für `image` und wählen **centos** in der Liste der konfigurierten Images aus.

Beachten Sie, dass es sich hierbei um Beispielwerte handelt. Wenn Sie kein centos-Image konfiguriert haben, wählen Sie ein von Ihnen konfiguriertes Image aus.

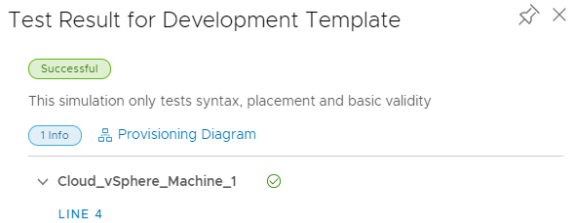
- c Erstellen Sie eine Zeile unter der Image-Eigenschaft und geben Sie `flavor` ein bzw. wählen Sie die Option aus und wählen Sie dann `small` in der Liste aus.
- d Löschen Sie `cpuCount` und `totalMemory`.

Ihr YAML-Code sollte ähnlich aussehen wie dieses Beispiel.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
```

- e Klicken Sie auf **Testen**.

Mit der Option „Testen“ können Sie die Syntax und die Platzierung Ihrer Cloud-Vorlage validieren. Ein erfolgreicher Test garantiert allerdings nicht, dass Sie die Vorlage ohne Fehler bereitstellen können.



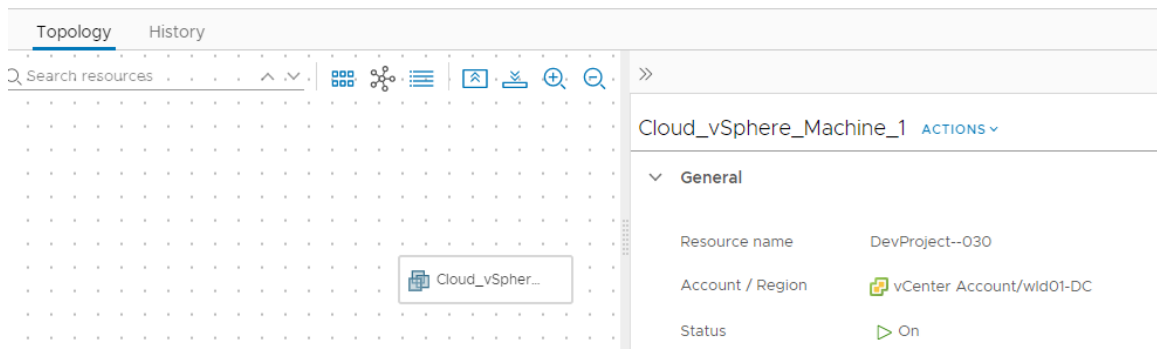
Falls der Test fehlschlägt, klicken Sie auf **Diagramm wird bereitgestellt** und suchen Sie nach den Fehlerpunkten. Weitere Informationen zur Verwendung des Diagramms für die Fehlerbehebung finden Sie unter [Testen einer einfachen Cloud-Vorlage](#).

- f Klicken Sie auf **Bereitstellen**.
- g Geben Sie unter **Name der Bereitstellung** den Namen **DevTemplate - machine** ein und klicken Sie auf **Bereitstellen**.

Sie können den Fortschritt der Bereitstellung auf der Seite „Bereitstellungsdetails“ der DevTemplate oder auf der Registerkarte „Bereitstellungen“ verfolgen.

Falls die Bereitstellung fehlschlägt, können Sie das Problem beheben und Ihre Vorlage überarbeiten. Weitere Informationen hierzu finden Sie unter [Vorgehensweise beim Fehlschlagen einer vRealize Automation Cloud Assembly-Bereitstellung](#).

Eine erfolgreiche Bereitstellung sieht ähnlich wie dieses Beispiel auf der Registerkarte „Bereitstellungen“ aus.

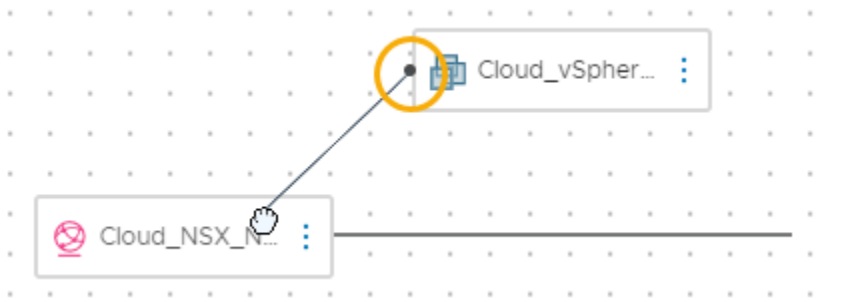


- 5 Versionieren Sie die Vorlage und fügen Sie ein Netzwerk hinzu.

Die Versionierung einer Cloud-Vorlage ist erforderlich, um sie im Service Broker-Katalog verfügbar zu machen. Sie ist jedoch auch sinnvoll, damit Sie während der Entwicklung eine einwandfrei funktionierende Version wiederherstellen können.

- a Öffnen Sie die Vorlage auf der Design-Arbeitsfläche.
- b Klicken Sie auf **Version**, geben Sie eine **Beschreibung** ein, beispielsweise **Simple deployable machine**, und klicken Sie auf **Erstellen**.
- c Ziehen Sie einen Ressourcentyp **NSX-Netzwerk** aus dem Fensterbereich „Ressourcentyp“ auf die Arbeitsfläche.
- d Verbinden Sie die Maschine mit dem Netzwerk.

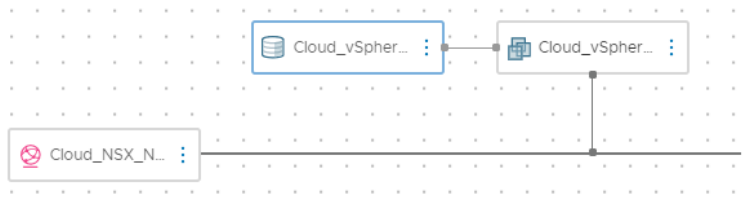
Klicken Sie auf den kleinen Kreis in der Maschinenkomponente und ziehen Sie die Verbindung auf das Netzwerk.



Der YAML-Code sieht nun ähnlich wie dieses Beispiel aus.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks: []
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
```

- e Klicken Sie auf **Testen**, um die Vorlage zu validieren.
 - f Klicken Sie auf **Bereitstellen**.
 - g Geben Sie den Namen **DevTemplate - machine - network** ein und klicken Sie auf **Bereitstellen**.
 - h Verfolgen Sie den Fortschritt und prüfen Sie, ob die Bereitstellung erfolgreich ist.
- 6 Versionieren Sie die Vorlage und fügen Sie eine Datenfestplatte hinzu.
- a Öffnen Sie die Vorlage auf der Design-Arbeitsfläche.
 - b Versionieren Sie die Vorlage.
- Geben Sie **Machine with existing network** als Beschreibung ein.
- c Ziehen Sie einen Ressourcentyp **vSphere-Festplatte** aus dem Fensterbereich „Ressourcentyp“ auf die Arbeitsfläche.
 - d Verbinden Sie die Festplatte mit der Maschine.



Der YAML-Code sieht nun ähnlich wie dieses Beispiel aus.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
```

- e Testen Sie die Vorlage.
- f Stellen Sie die Vorlage mit dem Namen **DevTemplate - machine - network - storage** bereit.
- g Verfolgen Sie den Fortschritt und prüfen Sie, ob die Bereitstellung erfolgreich ist.
- h Versionieren Sie die Vorlage.

Geben Sie **Machine with existing network and storage disk** als Beschreibung ein.

Durch diese endgültige Version wird sichergestellt, dass Sie dem Service Catalog eine funktionierende Vorlage hinzufügen können.

Lernprogramm – Ergebnisse

Sie haben den Workflow, durch den Sie Cloud Assembly als funktionierendes System konfiguriert haben, abgeschlossen. Sie sind jetzt mit den folgenden Konzepten vertraut.

- Bei Cloud-Konten handelt es sich um die Anmeldedaten, über die vRealize Automation Cloud Assembly mit den Endpoints Ihres Cloud-Anbieters verbunden wird.

- Bei Cloud-Zonen handelt es sich um die ausgewählten Computing-Ressourcen in Konten/Regionen, die Sie anschließend basierend auf den Projektanforderungen und Ihren Zielen für die Verwaltung von Kosten verschiedenen Projekten zuweisen.
- Infrastrukturressourcen sind Definitionen von Ressourcen, die mit dem Konto bzw. den Regionen verknüpft sind, die in Cloud-Vorlagen verwendet werden.
- Projekte legen fest, wie Sie Ihren Benutzern basierend auf den Anwendungsentwicklungszielen des Projekts Zugriff auf die Cloud-Zonen erteilen.
- Bei Cloud-Vorlagen handelt es sich um die Definitionen Ihrer Anwendungsarbeitslasten, die Sie iterativ entwickeln und bereitstellen.

Dieses Lernprogramm bildet die Grundlage für Ihre Kenntnisse bezüglich vRealize Automation Cloud Assembly-Bereitstellungen. Mithilfe dieses Vorgangs können Sie Ihre Infrastruktur erstellen und Ihre Kompetenz bei der Entwicklung von Cloud-Vorlagen verbessern.

Lernprogramm: Konfigurieren von vRealize Automation Cloud Assembly zur Bereitstellung einer Produktionsarbeitslast

Als Cloud-Administrator möchten Sie den Bereitstellungsprozess für ein Projekt automatisieren, damit beim Erstellen und Bereitstellen von Vorlagen durch die Cloud-Vorlagen-Designer vRealize Automation Cloud Assembly die Arbeit für Sie übernimmt. Beispiel: Die Arbeitslasten werden mit einem bestimmten benutzerdefinierten Maschinenbenennungsmuster bereitgestellt, die Maschinen werden einer bestimmten Active Directory-Organisationseinheit hinzugefügt und bestimmte DNS- und IP-Bereiche werden verwendet.

Indem Sie den Prozess für die Projektbereitstellungen automatisieren, können Sie mehrere Projekte für verschiedene Datacenter und Cloud-Umgebungen einfacher verwalten.

Sie müssen nicht alle Aufgaben abschließen. In Abhängigkeit von Ihren Verwaltungszielen können Sie diese Aufgaben frei miteinander kombinieren. Hier finden Sie eine Liste der möglichen Aufgaben.

- [Anpassen der Maschinennamen](#)
- [Erstellen von Active Directory-Maschinendatensätzen](#)
- [Festlegen von Netzwerk-DNS und internem IP-Bereich](#)

Bevor Sie beginnen

Dieses Lernprogramm setzt voraus, dass Sie die Infrastruktur konfiguriert und einer Maschine und einem Netzwerk erfolgreich eine Cloud-Vorlage bereitgestellt haben. Stellen Sie sicher, dass Folgendes bereits auf Ihrem System konfiguriert ist.

- Alle im Infrastrukturlernprogramm angegebenen Schritte wurden erfolgreich ausgeführt. Weitere Informationen hierzu finden Sie unter [Lernprogramm: Einrichten und Testen der vSphere-Infrastruktur und -Bereitstellungen in vRealize Automation Cloud Assembly](#).

- Sie verfügen über die Cloud Assembly-Administratorrolle. Weitere Informationen hierzu finden Sie unter [Organisations- und Dienstbenutzerrollen in vRealize Automation](#).

Anpassen der Maschinennamen

Ziel dieser Aufgabe ist es, sicherzustellen, dass die bereitgestellten Maschinen für das Entwicklungsprojekt basierend auf der Kostenstelle für das Projekt, dem zur Bereitstellungszeit ausgewählten Ressourcentyp und inkrementierter Zahlen benannt werden, um Eindeutigkeit zu gewährleisten. Beispiel: DevProject-centos-021.

Sie können dieses Beispiel an Ihre Benennungsanforderungen anpassen.

Weitere Informationen zu Projekten finden Sie unter [Kapitel 5 Hinzufügen und Verwalten von vRealize Automation Cloud Assembly-Projekten](#).



Ein Video, in dem dieses benutzerdefinierte Benennungsbeispiel veranschaulicht wird, finden Sie unter [Vorgehensweise zum Erstellen einer benutzerdefinierten Benennungsvorlage für Bereitstellungen](#).

- 1 Klicken Sie auf **Infrastruktur > Projekte**.
- 2 Wählen Sie ein vorhandenes Projekt aus oder erstellen Sie ein neues Projekt.
In diesem Lernprogramm lautet der Projektname „Entwicklungsprojekt“.
- 3 Klicken Sie auf **Erstellen**.
- 4 Klicken Sie auf der Seite „Projekte“ auf den Projektnamen auf der Kachel, damit Sie das Projekt konfigurieren können.
- 5 Klicken Sie auf die Registerkarte **Benutzer** und fügen Sie die Benutzer hinzu, die Mitglieder dieses Projekts sind.
- 6 Klicken Sie auf die Registerkarte **Bereitstellung**.
 - a Klicken Sie im Abschnitt „Zonen“ auf **Zone hinzufügen** und fügen Sie die möglichen Cloud-Zonen hinzu, in denen die Arbeitslasten für dieses Projekt bereitgestellt werden.
 - b Fügen Sie im Abschnitt „Benutzerdefinierte Eigenschaften“ eine benutzerdefinierte Eigenschaft mit dem Namen **costCenter** und dem Wert **DevProject** hinzu.

The screenshot displays the configuration interface for a project in vRealize Automation Cloud Assembly. It is divided into two main sections: 'Custom Properties' and 'Custom Naming'.

Custom Properties: This section allows defining properties for all requests in the project. It features a table with columns 'Name' and 'Value'. A single property is defined: 'costCenter' with the value 'DevProject'. The entire table is highlighted with an orange border.

Custom Naming: This section allows specifying a naming template for machines, networks, security groups, and disks. The template field contains the expression: `${resource.costCenter}-${resource.osType}-${###}`. This field is also highlighted with an orange border. Below the template field, a hint states: 'Hint: Avoid conflicting names by generating digits in names. \${#####}'.

- c Fügen Sie im Abschnitt „Benutzerdefinierte Benennung“ die folgende Benennungsvorlage hinzu.

```
${resource.costCenter}-${resource.osType}-${###}
```

`${resource.osType}` basiert auf dem Betriebssystem, das Sie bei der Bereitstellung der Cloud-Vorlage ausgewählt haben.

- 7 Klicken Sie auf **Speichern**.
- 8 Aktualisieren Sie die Cloud-Vorlage mit einem Eingabewert für den Betriebssystemtyp.

Mit Eingabewerten können Sie auf direktem Weg das Bereitstellungsanforderungsformular für Benutzer anpassen und den Entwicklungsprozess vereinfachen. Indem Sie Eingabewerte erstellen, können Sie eine einzelne Cloud-Vorlage zur Bereitstellung von Arbeitslasten mit verschiedenen Konfigurationen verwenden. Beispielsweise die Größe oder das Betriebssystem.

In diesem Beispiel wird die Entwicklungsvorlage aus einem früheren Lernprogramm verwendet. Weitere Informationen hierzu finden Sie unter [Schritt 5: Entwerfen und Bereitstellen einer grundlegenden Cloud-Vorlage](#).

- a Wählen Sie **Design** aus und öffnen Sie die Entwicklungsvorlage.
- b Ändern Sie die YAML im Bereich „Code“ wie folgt.

- Fügen Sie im Abschnitt `Inputs` den Eintrag **osType** hinzu.

Im nächsten Schritt können Sie sehen, dass die Eingabe `osType` auch zum Angeben des Image verwendet wird. Wenn Sie die Zeichenfolgen im Abschnitt `enum` hinzufügen, müssen die Werte – in diesem Beispiel `centos` und `ubuntu` – den Image-Namen entsprechen, die Sie unter **Infrastruktur > Konfigurieren > Image-Zuordnungen** definiert haben. Wenn der Name Ihrer Image-Zuordnung beispielsweise „CentOS“ statt „centos“ ist, müssen Sie im Eingabebereich „CentOS“ verwenden.

```
inputs:
  osType:
    type: string
    title: OS Type
    description: Select the operating system.
    enum:
      - centos
      - ubuntu
```

- Aktualisieren Sie im Abschnitt `Cloud_vSphere_Machine_1` das `image` auf einen `osType`-Eingabeparameter (`${input.osType}`) und fügen Sie eine benutzerdefinierte `osType`-Eigenschaft mit demselben Eingabeparameter hinzu.

```
resources:
  Cloud_vSphere_Disk_1:
```

```

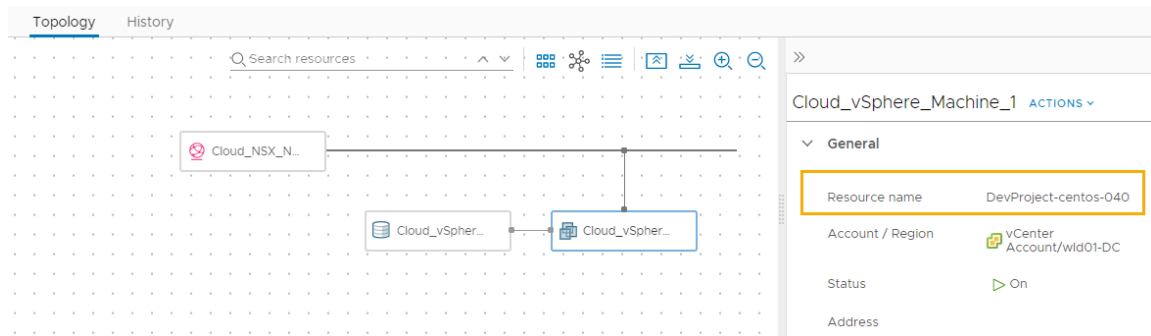
type: Cloud.vSphere.Disk
properties:
  capacityGb: 1
Cloud_vSphere_Machine_1:
  type: Cloud.vSphere.Machine
  properties:
    image: ${input.osType}
    osType: ${input.osType}
    flavor: small
    networks:
      - network: '${resource.Cloud_NSX_Network_1.id}'
    attachedDisks:
      - source: '${resource.Cloud_vSphere_Disk_1.id}'
Cloud_NSX_Network_1:
  type: Cloud.NSX.Network
  properties:
    networkType: existing

```

- c Klicken Sie auf **Bereitstellen** und geben Sie den Namen **Test zur Bereitstellung benutzerdefinierter Namen** ein.
- d Klicken Sie auf **Weiter**.
- e Wählen Sie im Dropdown-Menü das Betriebssystem **centos** aus.

The screenshot shows the 'Deployment Inputs' section of the vRealize Automation Cloud Assembly wizard. The 'OS Type' dropdown menu is open, showing 'centos' as the selected option. The 'Deploy Development Te...' section shows a list of deployment types. At the bottom are 'CANCEL', 'PREVIOUS', and 'DEPLOY' buttons.

- f Klicken Sie auf **Bereitstellen**.
- 9 Verfolgen Sie den Fortschritt und prüfen Sie, ob die Bereitstellung erfolgreich ist.
- Der Maschinenname in diesem Beispiel lautet „DevProject-centos-026“. Erinnerung: Dieses Beispiel basiert auf dem Lernprogramm, auf das am Anfang dieser Aufgabe verwiesen wird.



Erstellen von Active Directory-Maschinendatensätzen

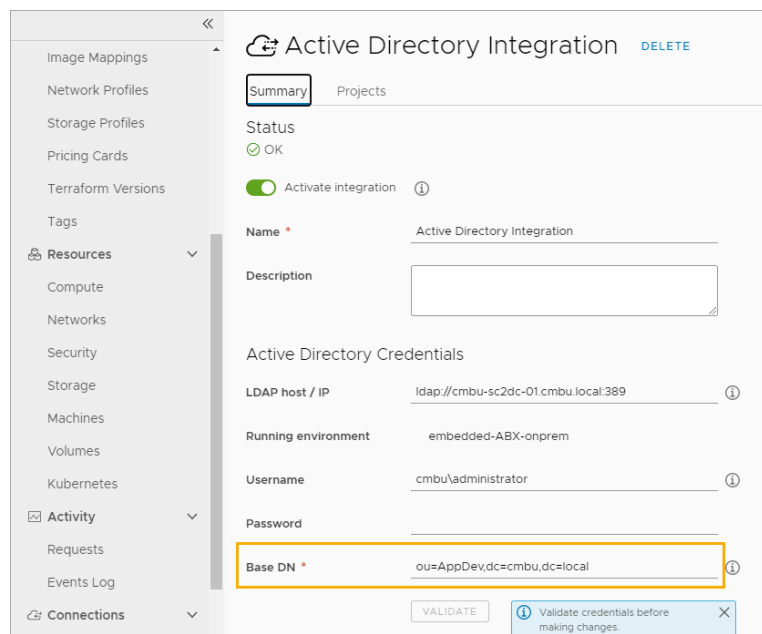
Wenn Sie eine Arbeitslast bereitstellen, können Sie Maschinendatensätze in Active Directory erstellen. Indem Sie vRealize Automation Cloud Assembly zur automatischen Durchführung dieser Aufgabe für die Bereitstellungen eines Projekts konfigurieren, verringern Sie Ihre eigene Arbeitsbelastung als Cloud-Administrator.

1 Fügen Sie die Active Directory-Integration hinzu.

a Wählen Sie **Infrastruktur > Verbindungen > Integrationen** aus.

Diese Schritte behandeln die grundlegende Active Directory-Konfiguration, die sich auf dieses Lernprogramm über AD-Maschinendatensätze bezieht. Weitere Informationen zur Integration von Active Directory finden Sie unter [Vorgehensweise zum Erstellen einer Active Directory-Integration in vRealize Automation Cloud Assembly](#).

b Klicken Sie auf **Integration hinzufügen** und dann auf **Active Directory**.



c Geben Sie den Namen ein, den Sie für diese Integration verwenden.

d Geben Sie **LDAP-Host/IP** und die zugehörigen Anmeldedaten ein.

e Geben Sie den **Basis-DN** ein.

In diesem Lernprogramm wird **ou=AppDev,dc=cmbu,dc=local** als Beispiel verwendet. „AppDev“ ist die übergeordnete Organisationseinheit (OE) für die Computer-OE, die Sie für das Projekt hinzufügen.

f Klicken Sie auf **Hinzufügen**.

2 Fügen Sie der Integration das Projekt hinzu.

3 Klicken Sie in der Active Directory-Integration auf die Registerkarte **Projekte** und dann auf **Projekt hinzufügen**.

Add Projects

Select a project and the OU it will be mapped to by adding its relative DN. The effective DN is created by appending the RDN to the integration base DN (**ou=AppDev,dc=cmbu,dc=local**).

Project *

Relative DN * ⓘ

Tags ⓘ

Matching zones

a Wählen Sie das Projekt „App Development“ aus.

b Geben Sie die relativen DNs ein. Beispiel: **OU=AppDev-Computers**.

c Klicken Sie auf **Hinzufügen**.

4 Um die Änderungen an der Integration zu speichern, klicken Sie auf **Speichern**.

5 Stellen Sie eine Cloud-Vorlage für das Projekt bereit und vergewissern Sie sich, dass die Maschine der korrekten Active Directory-Organisationseinheit hinzugefügt wurde.

Festlegen von Netzwerk-DNS und internem IP-Bereich

Aktualisieren Sie ein Netzwerkprofil, sodass es Ihre DNS-Server und internen IP-Bereiche enthält, oder fügen Sie eines hinzu.

Sie müssen bereits ein Cloud-Konto für vSphere, NSX-V oder NSX-T erstellt haben. Weitere Informationen finden Sie unter [Lernprogramm: Einrichten und Testen der vSphere-Infrastruktur und -Bereitstellungen in vRealize Automation Cloud Assembly](#) oder [Hinzufügen von Cloud-Konten zu vRealize Automation Cloud Assembly](#).

1 Wählen Sie **Infrastruktur > Konfigurieren > Netzwerkprofile** aus.

2 Wählen Sie ein vorhandenes Profil aus oder erstellen Sie ein Profil.

3 Wählen Sie auf der Registerkarte **Übersicht** unter **Konto/Region** ein Konto bzw. eine Region aus und geben Sie einen Namen ein.

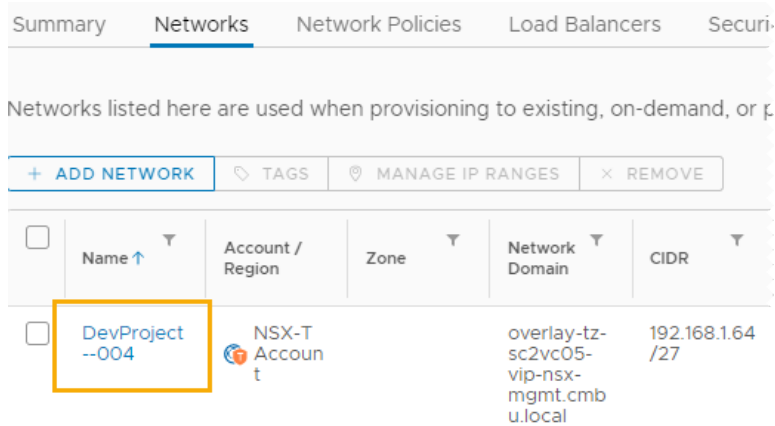
In diesem Lernprogramm wird „Netzwerkprofil“ als Name für das Netzwerkprofil verwendet.

4 Fügen Sie Netzwerke hinzu.

- a Klicken Sie auf die Registerkarte **Netzwerke**.
- b Klicken Sie auf **Netzwerk hinzufügen**.
- c Fügen Sie ein oder mehrere NSX- oder vSphere-Netzwerke hinzu.
- d Klicken Sie auf **Hinzufügen**.

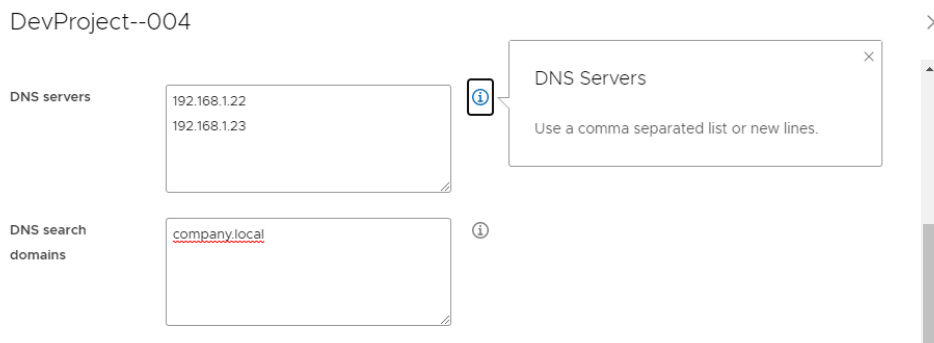
5 Konfigurieren Sie die DNS-Server.

- a Klicken Sie in der Liste „Netzwerke“ auf der Registerkarte **Netzwerke** auf den Namen des Netzwerks.



	Name ↑	Account / Region	Zone	Network Domain	CIDR
<input type="checkbox"/>	DevProject--004	NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	192.168.1.64 /27

- b Geben Sie die IP-Adressen des DNS-Servers ein, die in diesem Netzwerk verwendet werden sollen.



DevProject--004

DNS servers: 192.168.1.22, 192.168.1.23

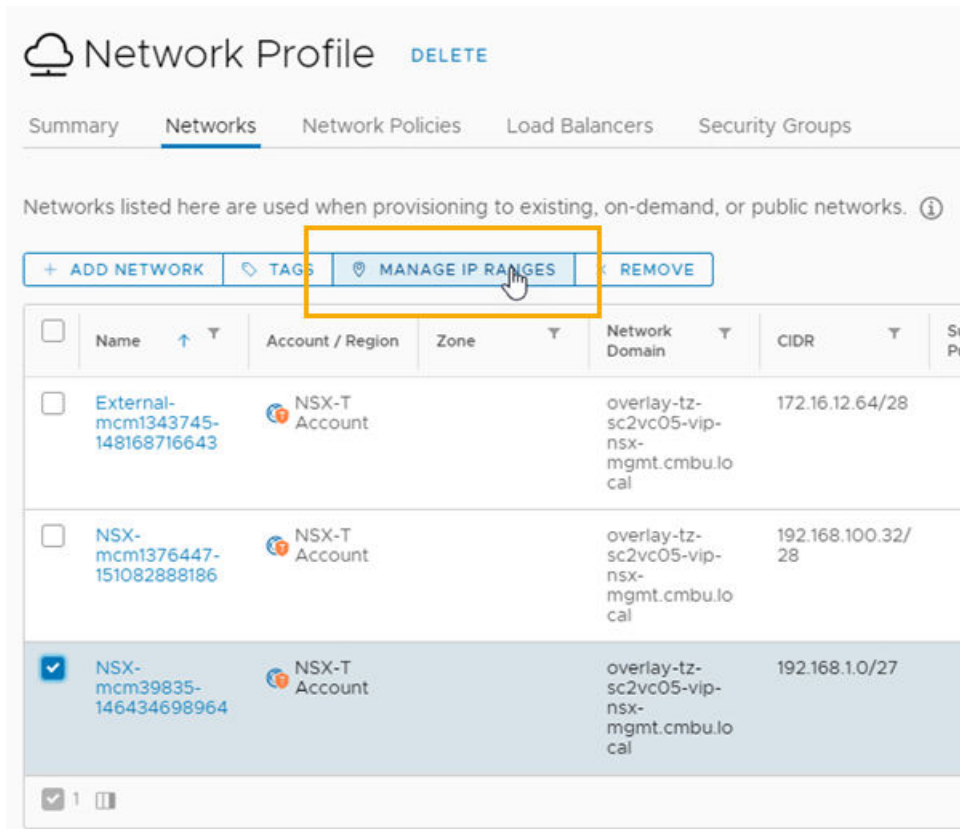
DNS search domains: company.local

DNS Servers tooltip: Use a comma separated list or new lines.

- c Klicken Sie auf **Speichern**.

6 Geben Sie den IP-Bereich für das Netzwerk an.

- a Aktivieren Sie in der Liste der Netzwerke das Kontrollkästchen neben dem betreffenden Netzwerknamen.



- b Klicken Sie auf **IP-Bereiche verwalten**.
- c Klicken Sie im Dialogfeld „IP-Bereiche verwalten“ auf **Neuer IP-Bereich**.

New IP Range

Network * NSX-mcm1376447-151082888186

Source ☒ Internal ☐ External

Name * DevProject Range

Description

CIDR 192.168.100.32/28

Start IP address * 192.168.100.34

End IP address * 192.168.100.46

- d Geben Sie einen Namen ein.

Beispiel: **DevProject-Bereich**.

- e Um den Bereich zu definieren, geben Sie die **Start-IP-Adresse** und die **End-IP-Adresse** ein.
 - f Klicken Sie auf **Hinzufügen**.
 - g Fügen Sie zusätzliche Bereiche hinzu oder klicken Sie auf **Schließen**.
- 7 Fügen Sie die Cloud-Zone mit dem verknüpften Netzwerkkonto bzw. der verknüpften Region hinzu, die Sie für das Entwicklungsprojekt konfiguriert haben.
 - 8 Stellen Sie eine Cloud-Vorlage für das Projekt bereit und vergewissern Sie sich, dass die Maschine innerhalb des angegebenen IP-Bereichs bereitgestellt wird.

Lernprogramm: Einrichten und Testen einer Multi-Cloud-Infrastruktur und von Bereitstellungen in vRealize Automation Cloud Assembly

In diesem vRealize Automation Cloud Assembly-Lernprogramm wird die Bereitstellung in einer Umgebung mit mehreren Clouds erläutert. Sie stellen mehreren Anbietern dieselbe Cloud-Vorlage bereit, in diesem Fall AWS und Microsoft Azure.

In diesem Beispiel handelt es sich bei der Anwendung um eine WordPress-Website. Sehen Sie sich die schrittweise Einrichtung an, um den Vorgang zu verstehen, der das ganze Design zum Abschluss bringt.

Beachten Sie, dass es sich bei den angezeigten Namen und Werten lediglich um Beispiele handelt. Sie können diese nicht eins zu eins auf Ihre eigene Umgebung übertragen.

Zur Anpassung an die Anforderungen Ihrer Cloud-Infrastruktur und -Bereitstellung überlegen Sie, an welchen Stellen Sie die Beispielwerte durch eigene Werte ersetzen möchten.

Teil 1: Konfigurieren der vRealize Automation Cloud Assembly-Beispielinfrastruktur

Konfigurieren Sie zunächst die Ressourcen, mit denen vRealize Automation Cloud Assembly-Engineering-Benutzer die Anwendung später entwickeln, testen und in Betrieb nehmen können.

Die Infrastruktur umfasst Cloud-Ziele und Definitionen rund um die verfügbaren Maschinen, Netzwerke und Speicher, die für die WordPress-Site erforderlich sind.

1 . Hinzufügen von Cloud-Konten

In diesem Schritt fügt der Cloud-Administrator zwei Cloud-Konten hinzu. Laut Beispielprojekt sollen Entwicklung und Test auf AWS durchgeführt werden, während die Produktion auf Azure stattfinden soll.

Verfahren

- 1 Navigieren Sie zu **Infrastruktur > Verbindungen > Cloud-Konten**.

- 2 Klicken Sie auf **Cloud-Konto hinzufügen**, wählen Sie Amazon Web Services aus und geben Sie Werte ein.

Einstellung	Beispielwert
Zugriffsschlüssel-ID	R5SDR3PXVV2ZW8B7YNSM
Geheimer Zugriffsschlüssel	SZXAINXU4UHNQAQ1E156S
Name	OurCo-AWS
Beschreibung	WordPress

Beachten Sie, dass alle Werte nur Beispiele sind. Die Kontospezifikationen sind unterschiedlich.

- 3 Klicken Sie zum Überprüfen der Anmeldedaten auf **Überprüfen**.
- 4 Klicken Sie auf **Hinzufügen**.
- 5 Bearbeiten Sie das neu hinzugefügte Konto **Konfiguration** und ermöglichen Sie die Bereitstellung für die Regionen „us-east-1“ und „us-west-2“.
- 6 Klicken Sie auf **Cloud-Konto hinzufügen**, wählen Sie Microsoft Azure aus und geben Sie Werte ein.

Einstellung	Beispielwert
Abonnement-ID	ef2avpf-dfdv-zxlugui1i-g4h0-i8ep2jwp4c9arbfe
Mandanten-ID	dso9wv3-4zgc-5nrcy5h3m-4skf-nnovp40wfxsro22r
Client-Anwendungs-ID	bg224oq-3ptp-mbhi6aa05-q511-uflyjr2sttyik6bs
Geheimer Schlüssel der Client-Anwendung	7uqxi57-0wtn-kymgf9wcj-t2l7-e52e4nu5fig4pmdd
Name	OurCo-Azure
Beschreibung	WordPress

- 7 Klicken Sie zum Überprüfen der Anmeldedaten auf **Überprüfen**.
- 8 Klicken Sie auf **Hinzufügen**.
- 9 Bearbeiten Sie das neu hinzugefügte Konto **Konfiguration** und ermöglichen Sie die Bereitstellung für die Region „East US“.

2 . Hinzufügen von Cloud-Zonen

In diesem Beispielschritt fügt der Cloud-Administrator drei Cloud-Zonen hinzu, jeweils eine für die Entwicklung, die Tests und die Produktion.

Cloud-Zonen sind die Ressourcen, auf denen das Projekt die Maschinen, Netzwerke und Speicher zur Unterstützung der WordPress-Site bereitstellt.

Verfahren

- 1 Wechseln Sie zu **Infrastruktur > Konfigurieren > Cloud-Zonen**.
- 2 Klicken Sie auf **Neue Cloud-Zone** und geben Sie Werte für die Entwicklungsumgebung ein.

Einstellungen für die Cloud-Zone	Beispielwert
Konto/Region	OurCo-AWS/us-east-1
Name	OurCo-AWS-US-East
Beschreibung	WordPress
Platzierungsrichtlinie	Standard
Funktions-Tags	env:dev

Beachten Sie, dass alle Werte nur Beispiele sind. Ihre Zonen-spezifischen Besonderheiten sind unterschiedlich.

- 3 Klicken Sie auf **Computing** und stellen Sie sicher, dass die erwarteten Zonen vorhanden sind.
- 4 Klicken Sie auf **Erstellen**.
- 5 Wiederholen Sie den Vorgang zweimal mit Werten für die Test- und die Produktionsumgebung.

Einstellungen für die Cloud-Zone	Beispielwert
Konto/Region	OurCo-AWS/us-west-2
Name	OurCo-AWS-US-West
Beschreibung	WordPress
Platzierungsrichtlinie	Standard
Funktions-Tags	env:test

Einstellungen für die Cloud-Zone	Beispielwert
Konto/Region	OurCo-Azure/East US
Name	OurCo-Azure-East-US
Beschreibung	WordPress
Platzierungsrichtlinie	Standard
Funktions-Tags	env:prod

3 . Hinzufügen von Typzuordnungen

In diesem Beispielschritt fügt der Cloud-Administrator Typzuordnungen hinzu, um die Kapazitätsanforderungen zu berücksichtigen, die je nach Bereitstellung variieren können.

Die Typzuordnung berücksichtigt Maschinenbereitstellungen unterschiedlicher Größe und wird informell als T-Shirt-Sizing bezeichnet.

Verfahren

- 1 Navigieren Sie zu **Infrastruktur > Konfigurieren > Typzuordnungen**. Jede Cloud-Zone muss für kleine, mittlere und große Konfigurationen geeignet sein.
- 2 Klicken Sie auf **Neue Konfigurationszuordnung** und geben Sie Werte für die Entwicklungs-Cloud-Zone ein.

Einstellung	Beispielwert
Konfigurationsname	small
Konto/Region Wert	OurCo-AWS/us-east-1 t2.micro
Konto/Region Wert	OurCo-AWS/us-west-2 t2.micro
Konto/Region Wert	OurCo-Azure/East US Standard_A0

Beachten Sie, dass alle Werte nur Beispiele sind. Ihre Konfigurationen werden variieren.

- 3 Klicken Sie auf **Erstellen**.
- 4 Wiederholen Sie den Vorgang zweimal mit Werten für mittlere und große Konfigurationen.

Einstellung	Beispielwert
Konfigurationsname	medium
Konto/Region Wert	OurCo-AWS/us-east-1 t2.medium
Konto/Region Wert	OurCo-AWS/us-west-2 t2.medium
Konto/Region Wert	OurCo-Azure/East US Standard_A3

Einstellung	Beispielwert
Konfigurationsname	large
Konto/Region Wert	OurCo-AWS/us-east-1 t2.large
Konto/Region Wert	OurCo-AWS/us-west-2 t2.large
Konto/Region Wert	OurCo-Azure/East US Standard_A7

4 . Hinzufügen von Image-Zuordnungen

In diesem Beispielschritt fügt der Cloud-Administrator eine Image-Zuordnung für Ubuntu hinzu, den Host für den WordPress-Server und den zugehörigen MySQL-Datenbankserver.

Planen Sie das Betriebssystem, indem Sie Image-Zuordnungen hinzufügen. Jede Cloud-Zone benötigt eine Ubuntu-Image-Zuordnung.

Verfahren

- 1 Navigieren Sie zu **Infrastruktur > Konfigurieren > Image-Zuordnungen**.
- 2 Klicken Sie auf **Neue Image-Zuordnung** und geben Sie Werte für Ubuntu-Server ein.

Einstellung	Beispielwert
Image-Name	ubuntu
Konto/Region	OurCo-AWS/us-east-1
Wert	ubuntu-16.04-server-cloudimg-amd64
Konto/Region	OurCo-AWS/us-west-2
Wert	ubuntu-16.04-server-cloudimg-amd64
Konto/Region	OurCo-Azure/East US
Wert	azul-zulu-ubuntu-1604-923eng

Beachten Sie, dass alle Werte nur Beispiele sind. Ihre Images sind unterschiedlich.

- 3 Klicken Sie auf **Erstellen**.

5 . Hinzufügen von Netzwerkprofilen

In diesem Beispielschritt fügt der Cloud-Administrator jeder Cloud-Zone ein Netzwerkprofil hinzu.

In jedem Profil fügt der Administrator ein Netzwerk für die WordPress-Maschinen sowie ein zweites Netzwerk hinzu, das sich auf der anderen Seite eines möglichen Lastausgleichsdiensts befindet. Bei dem zweiten Netzwerk handelt es sich um das Netzwerk, über das die Benutzer schließlich eine Verbindung herstellen.

Verfahren

- 1 Navigieren Sie zu **Infrastruktur > Konfigurieren > Netzwerkprofile**.
- 2 Klicken Sie auf **Neues Netzwerkprofil** und erstellen Sie ein Profil für die Cloud-Entwicklungszone.

Einstellung „Netzwerkprofiltyp“	Beispielwert
Konto/Region	OurCo-AWS/us-east-1
Name	devnets
Beschreibung	WordPress

- 3 Klicken Sie auf **Netzwerke** und dann auf **Netzwerk hinzufügen**.

- Wählen Sie „wpnet“, „appnet-public“ aus und klicken Sie auf **Hinzufügen**.

Beachten Sie, dass alle Werte nur Beispiele sind. Ihre Netzwerknamen sind unterschiedlich.

- Klicken Sie auf **Erstellen**.

In diesem WordPress-Beispiel ist es nicht notwendig, dass Sie Einstellungen für Netzwerkrichtlinien oder Netzwerksicherheit angeben.

- Wiederholen Sie den Vorgang zweimal, um ein Netzwerkprofil für die Cloud-Test- und Cloud-Produktionszonen des WordPress-Beispiels zu erstellen. Fügen Sie in jedem Fall die Netzwerke „wpnet“ und „appnet-puplic“ hinzu.

Einstellung „Netzwerkprofiltyp“	Beispielwert
Konto/Region	OurCo-AWS/us-west-2
Name	testnets
Beschreibung	WordPress
Einstellung „Netzwerkprofiltyp“	Wert
Konto/Region	OurCo-Azure/East US
Name	prodnets
Beschreibung	WordPress

6 . Hinzufügen von Speicherprofilen

In diesem Beispielschritt fügt der Cloud-Administrator jeder Cloud-Zone ein Speicherprofil hinzu.

Der Administrator platziert ein schnelles Speichergerät in der Produktionszone und ein allgemeines Speichergerät bei der Entwicklung und beim Test.

Verfahren

- Navigieren Sie zu **Infrastruktur > Konfigurieren > Speicherprofile**.
- Klicken Sie auf **Neues Speicherprofil** und erstellen Sie ein Profil für die Cloud-Entwicklungszone.

Nach der Auswahl des Kontos/der Region werden zusätzliche Felder angezeigt.

Einstellung für das Speicherprofil	Beispielwert
Konto/Region	OurCo-AWS/us-east-1
Name	OurCo-AWS-US-East-Disk
Beschreibung	WordPress
Gerätetyp	EBS

Einstellung für das Speicherprofil	Beispielwert
Volume-Typ	Universelle SSD
Funktions-Tags	Speicher:allgemein

Beachten Sie, dass alle Werte nur Beispiele sind.

- 3 Klicken Sie auf **Erstellen**.
- 4 Wiederholen Sie den Vorgang, um ein Profil für die Cloud-Testzone zu erstellen.

Einstellung für das Speicherprofil	Beispielwert
Konto/Region	OurCo-AWS/us-west-2
Name	OurCo-AWS-US-West-Disk
Beschreibung	WordPress
Gerätetyp	EBS
Volume-Typ	Universelle SSD
Funktions-Tags	Speicher:allgemein

- 5 Wiederholen Sie den Vorgang zum Erstellen eines Profils für die Cloud-Produktionszone, die andere Einstellungen aufweist, da es sich um eine Azure-Zone handelt.

Einstellung für das Speicherprofil	Beispielwert
Konto/Region	OurCo-Azure/East US
Name	OurCo-Azure-East-US-Disk
Beschreibung	WordPress
Speichertyp	Verwaltete Festplatten
Datenträgertyp	Premium-LRS
Caching der Betriebssystemfestplatte	Schreibgeschützt
Caching des Datenträgers	Schreibgeschützt
Funktions-Tags	Speicher:schnell

Nächste Schritte

Erstellen Sie ein Projekt zur Angabe von Benutzern und zur Definition von Bereitstellungseinstellungen. Weitere Informationen hierzu finden Sie unter [Teil 2: Erstellen des vRealize Automation Cloud Assembly-Beispielprojekts](#).

Teil 2: Erstellen des vRealize Automation Cloud Assembly-Beispielprojekts

Das vRealize Automation Cloud Assembly-Beispielprojekt aktiviert die Benutzer mit Bereitstellungsfunktion und konfiguriert die Bereitstellungsmöglichkeiten.

In Projekten werden die Einstellungen für den Benutzer und die Bereitstellung definiert.

- Benutzer und deren Berechtigungsrollenebene
- Priorität für Bereitstellungen, da sie in einer Cloud-Zone bereitgestellt werden
- Maximale Anzahl der Bereitstellungsinstanzen pro Cloud-Zone

Verfahren

- 1 Navigieren Sie zu **Infrastruktur > Verwaltung > Projekte**.
- 2 Klicken Sie auf **Neues Projekt** und geben Sie den Namen „WordPress“ ein.
- 3 Klicken Sie auf **Benutzer** und dann auf **Benutzer hinzufügen**.
- 4 Fügen Sie E-Mail-Adressen und Rollen für die Benutzer hinzu.

Zum erfolgreichen Hinzufügen eines Benutzers muss ein VMware Cloud Services-Administrator Zugriff auf vRealize Automation Cloud Assembly für den Benutzer aktiviert haben.

Beachten Sie, dass die hier gezeigten Adressen nur Beispiele sind.

- chris.ladd@ourco.com, Mitglied
 - kerry.mott@ourco.com, Mitglied
 - pat.tubb@ourco.com, Administrator
- 5 Klicken Sie auf **Bereitstellung** und dann auf **Cloud-Zone hinzufügen**.
 - 6 Fügen Sie die Cloud-Zonen hinzu, in denen die Benutzer eine Bereitstellung durchführen können.

Einstellung „Cloud-Projektzone“	Beispielwert
Cloud-Zone	OurCo-AWS-US-East
Bereitstellungspriorität	1
Grenzwert der Instanzen	5
Cloud-Zone	OurCo-AWS-US-West
Bereitstellungspriorität	1
Grenzwert der Instanzen	5
Cloud-Zone	OurCo-Azure-East-US
Bereitstellungspriorität	0
Grenzwert der Instanzen	1

- 7 Klicken Sie auf **Erstellen**.

- 8 Navigieren Sie zu **Infrastruktur > Konfigurieren > Cloud-Zonen** und öffnen Sie eine Zone, die zuvor erstellt wurde.
- 9 Klicken Sie auf **Projekte** und stellen Sie sicher, dass es sich bei WordPress um ein Projekt handelt, das zur Bereitstellung in der Zone berechtigt ist.
- 10 Überprüfen Sie die anderen Zonen, die Sie erstellt haben.

Nächste Schritte

Erstellen Sie eine einfache Cloud-Vorlage.

Teil 3: Entwerfen und Bereitstellen der vRealize Automation Cloud Assembly-Beispielvorlage

Als Nächstes definieren Sie die Beispielanwendung – die WordPress-Site – in Form einer generischen Cloud-Vorlage. Die Vorlage kann für verschiedene Cloud-Anbieter bereitgestellt werden, ohne dass ihr Design geändert werden muss.

Das Beispiel besteht aus einem WordPress-Anwendungsserver, einem MySQL-Datenbankserver und unterstützenden Ressourcen. Die Vorlage beginnt mit wenigen Ressourcen und vergrößert sich dann, wenn Sie die Ressourcen ändern und weitere hinzufügen.

Hier sind die Werte aus [Teil 1: Konfigurieren der vRealize Automation Cloud Assembly-Beispielinfrastruktur](#), der Infrastruktur, die von einem Cloud-Administrator festgelegt wurde:

- Zwei Cloud-Konten, AWS und Azure.
- Drei Cloud-Zonen-Umgebungen:
 - Entwicklung – OurCo-AWS-US-East
 - Test – OurCo-AWS-US-West
 - Produktion – OurCo-Azure-East-US
- Konfigurationszuordnungen mit kleinen, mittleren und großen Computing-Ressourcen für jede Zone.
- In jeder Zone konfigurierte Image-Zuordnungen für Ubuntu.
- Netzwerkprofile mit internen und externen Subnetzen für jede Zone.
- Speicher, auf dem die Bereitstellung erfolgen soll. Allgemeiner Speicher für die Entwicklungs- und Testzone und schneller Speicher für die Produktionszone.
- Das Beispielprojekt umfasst alle drei Cloud-Zonen-Umgebungen sowie die Benutzer, die Entwürfe erstellen können.

Voraussetzungen

Um fortfahren zu können, müssen Sie sich mit den eigenen Infrastrukturwerten vertraut machen. Dieses Beispiel verwendet AWS für die Entwicklung und für Tests und Azure für die Produktion. Wenn Sie eine eigene Cloud-Vorlage erstellen, ersetzen Sie Ihre eigenen Werte, die in der Regel von Ihrem Cloud-Administrator festgelegt werden.

Verfahren

1 Erstellen einer einfachen Cloud-Vorlage

In diesem vRealize Automation Cloud Assembly-Designbeispiel beginnen Sie mit einer Cloud-Vorlage, die nur ein Minimum an WordPress-Ressourcen enthält, zum Beispiel nur einen Anwendungsserver.

2 Testen einer einfachen Cloud-Vorlage

Während des Designs erstellen Sie häufig eine Cloud-Vorlage, indem Sie mit den Grundlagen beginnen, dann bereitstellen und testen, während die Vorlage sich weiterentwickelt. Dieses Beispiel zeigt einige der laufenden Tests, die in vRealize Automation Cloud Assembly integriert sind.

3 Erweitern einer Cloud-Vorlage

Nachdem Sie die einfache vRealize Automation Cloud Assembly-Vorlage für die Beispielanwendung erstellt und getestet haben, erweitern Sie sie in eine mehrschichtige Anwendung, die für die Entwicklung, den Test und schließlich die Produktion bereitgestellt werden kann.

Erstellen einer einfachen Cloud-Vorlage

In diesem vRealize Automation Cloud Assembly-Designbeispiel beginnen Sie mit einer Cloud-Vorlage, die nur ein Minimum an WordPress-Ressourcen enthält, zum Beispiel nur einen Anwendungsserver.

vRealize Automation Cloud Assembly ist ein „Infrastruktur-als-Code“-Tool. Sie können Ressourcen auf die Design-Arbeitsfläche ziehen, um den Vorgang zu starten. Anschließend vervollständigen Sie die Details mit dem Code-Editor rechts neben der Arbeitsfläche.

Mit dem Code-Editor können Sie Code direkt eingeben, ausschneiden und einfügen. Wenn Sie nicht gern Code bearbeiten, können Sie eine Ressource in der Arbeitsfläche auswählen, auf die Registerkarte **Eigenschaften** im Code-Editor klicken und die Werte dort eingeben. Die von Ihnen eingegebenen Werte werden im Code so angezeigt, als hätten Sie sie direkt eingegeben.

Verfahren

- 1 Gehen Sie zu **Design > Cloud-Vorlagen** und klicken Sie auf **Neu von > Leere Arbeitsfläche**.
- 2 Benennen Sie die Cloud-Vorlage **WordPress-BP**.
- 3 Wählen Sie das **WordPress**-Projekt aus und klicken Sie auf **Erstellen**.

- 4 Ziehen Sie aus den Ressourcen links auf der Cloud-Vorlagen-Designseite zwei Cloud-unabhängige Maschinen auf die Arbeitsfläche.

Die Maschinen dienen als WordPress-Anwendungsserver (WebTier) und MySQL-Datenbankserver (DBTier).

- 5 Bearbeiten Sie auf der rechten Seite den Maschinen-YAML-Code, um Namen, Images, Konfigurationen und Einschränkungs-Tags hinzuzufügen:

```
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      image: ubuntu
      flavor: small
      constraints:
        - tag: env:dev
  DBTier:
    type: Cloud.Machine
    properties:
      name: mysql
      image: ubuntu
      flavor: small
      constraints:
        - tag: env:dev
```

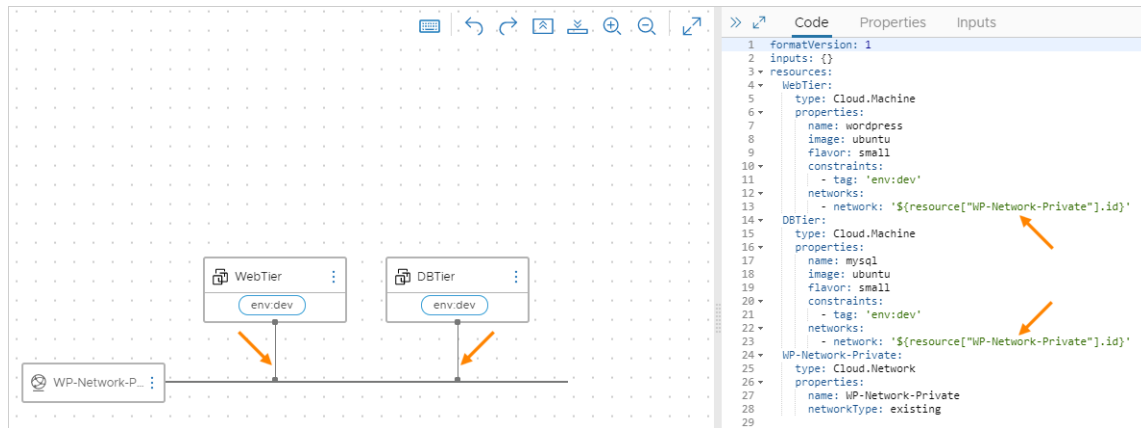
- 6 Ziehen Sie ein Cloud-unabhängiges Netzwerk auf die Arbeitsfläche und bearbeiten Sie den Code:

```
WP-Network-Private:
  type: Cloud.Network
  properties:
    name: WP-Network-Private
    networkType: existing
```

- 7 Verbinden Sie die Maschinen mit dem Netzwerk:

Bewegen Sie auf der Arbeitsfläche den Mauszeiger über den Netzwerkblock, klicken Sie an der Stelle auf die Blase, wo die Linie den Block berührt, halten Sie den Mauszeiger gedrückt, ziehen Sie die Blase auf einen Maschinenblock und lassen Sie die Maustaste los.

Beachten Sie beim Erstellen der Verbindungslinien, dass Netzwerkcode automatisch zu den Maschinen im Editor hinzugefügt wird.



8 Fügen Sie eine Benutzereingabeaufforderung hinzu.

An einigen Stellen wurde die Beispielinfrastruktur für mehrere Optionen eingerichtet. Beispiel:

- Cloud-Zonen-Umgebungen für Entwicklung, Tests und Produktion
- Konfigurationszuordnungen für kleine, mittlere und große Maschinen

Sie können eine bestimmte Option direkt in der Cloud-Vorlage festlegen. Ein besserer Ansatz ist jedoch, dass der Benutzer die Option zur Bereitstellungszeit der Cloud-Vorlage auswählen kann. Durch die Eingabeaufforderung für die Benutzereingabe können Sie eine Vorlage erstellen, die auf viele Arten bereitgestellt werden kann, anstatt mit vielen hartcodierten Vorlagen zu arbeiten.

- a Erstellen Sie einen `inputs`-Abschnitt im Code, damit Benutzer die Maschinengröße und die Zielumgebung zur Bereitstellungszeit auswählen können. Definieren Sie die auswählbaren Werte:

```
inputs:
  env:
    type: string
    enum:
      - env:dev
      - env:prod
      - env:test
    default: env:dev
    title: Environment
    description: Target Environment
  size:
    type: string
    enum:
      - small
      - medium
      - large
    description: Size of Nodes
    title: Tier Machine Size
```

- b Fügen Sie im `resources`-Abschnitt des Codes den Code `${input.input-name}` hinzu, um die Benutzerauswahl zu bestätigen:

```
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      image: ubuntu
      flavor: '${input.size}'
      constraints:
        - tag: '${input.env}'
      networks:
        - network: '${resource["WP-Network-Private"].id}'
  DBTier:
    type: Cloud.Machine
    properties:
      name: mysql
      image: ubuntu
      flavor: '${input.size}'
      constraints:
        - tag: '${input.env}'
```

```
networks:
  - network: '${resource["WP-Network-Private"].id}'
WP-Network-Private:
  type: Cloud.Network
  properties:
    name: WP-Network-Private
    networkType: existing
```

- 9 Erweitern Sie schließlich den `WebTier`- und den `DBTier`-Code anhand der folgenden Beispiele. Der `WP-Network-Private`-Code benötigt keine zusätzlichen Änderungen.

Beachten Sie, dass Anmeldezugriff auf die Datenbank und `cloudConfig`-Initialisierungsskripts zur Bereitstellungszeit zu den Verbesserungen gehören.

Komponente	Beispiel
Zusätzliche DBTier-Eingaben	<pre> username: type: string minLength: 4 maxLength: 20 pattern: '[a-z]+' title: Database Username description: Database Username userpassword: type: string pattern: '[a-z0-9A-Z@#]+\$' encrypted: true title: Database Password description: Database Password </pre>
DBTier-Ressource	<pre> DBTier: type: Cloud.Machine properties: name: mysql image: ubuntu flavor: '\${input.size}' constraints: - tag: '\${input.env}' networks: - network: '\${resource["WP-Network-Private"].id}' assignPublicIpAddress: true remoteAccess: authentication: usernamePassword username: '\${input.username}' password: '\${input.userpassword}' cloudConfig: #cloud-config repo_update: true repo_upgrade: all packages: - mysql-server runcmd: - sed -e '/bind-address/ s/^#/#/' -i /etc/mysql/mysql.conf.d/ mysqlld.cnf - service mysql restart - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'mysqlpassword';" - mysql -e "FLUSH PRIVILEGES;" attachedDisks: [] </pre>
WebTier-Ressource	<pre> WebTier: type: Cloud.Machine properties: name: wordpress image: ubuntu flavor: '\${input.size}' constraints: - tag: '\${input.env}' networks: - network: '\${resource["WP-Network-Private"].id}' assignPublicIpAddress: true cloudConfig: #cloud-config </pre>

Komponente	Beispiel
	<pre> repo_update: true repo_upgrade: all packages: - apache2 - php - php-mysql - libapache2-mod-php - php-mcrypt - mysql-client runcmd: - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/ latest.tar.gz -C /var/www/html/mywordpresssite --strip-components 1 - i=0; while [\$i -le 10]; do mysql --connect-timeout=3 -h \$ {DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break sleep 15; i=\$((i+1)); done - mysql -u root -pmysqlpassword -h \${DBTier.networks[0].address} -e "create database wordpress_blog;" - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/ html/mywordpresssite/wp-config.php - sed -i -e s/"define('DB_NAME', 'database_name_here');"/"define('DB_NAME', 'wordpress_blog');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i -e s/"define('DB_USER', 'username_here');"/"define('DB_USER', 'root');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i -e s/"define('DB_PASSWORD', 'password_here');"/"define('DB_PASSWORD', 'mysqlpassword');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i -e s/"define('DB_HOST', 'localhost');"/"define('DB_HOST', '\${DBTier.networks[0].address}');"/ /var/www/html/mywordpresssite/wp- config.php - service apache2 reload </pre>

Beispiel: Abgeschlossenes Codebeispiel für eine einfache Cloud-Vorlage

```

formatVersion: 1
inputs:
  env:
    type: string
    enum:
      - env:dev
      - env:prod
      - env:test
    default: env:dev
    title: Environment
    description: Target Environment
  size:
    type: string
    enum:
      - small
      - medium
      - large
    description: Size of Nodes
    title: Tier Machine Size
  username:
    type: string
    minLength: 4
    maxLength: 20

```

```

    pattern: '[a-z]+'
    title: Database Username
    description: Database Username
  userpassword:
    type: string
    pattern: '[a-z0-9A-Z@#&$]+'
    encrypted: true
    title: Database Password
    description: Database Password
  resources:
    WebTier:
      type: Cloud.Machine
      properties:
        name: wordpress
        image: ubuntu
        flavor: '${input.size}'
        constraints:
          - tag: '${input.env}'
      networks:
        - network: '${resource["WP-Network-Private"].id}'
          assignPublicIpAddress: true
      cloudConfig: |
        #cloud-config
        repo_update: true
        repo_upgrade: all
        packages:
          - apache2
          - php
          - php-mysql
          - libapache2-mod-php
          - php-mcrypt
          - mysql-client
        runcmd:
          - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
            https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
            mywordpresssite --strip-components 1
          - i=0; while [ $i -le 10 ]; do mysql --connect-timeout=3 -h $
            {DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;
            i=$((i+1)); done
          - mysql -u root -pmysqlpassword -h ${DBTier.networks[0].address} -e "create database
            wordpress_blog;"
          - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/
            mywordpresssite/wp-config.php
          - sed -i -e s/"define( 'DB_NAME', 'database_name_here' );"/"define( 'DB_NAME',
            'wordpress_blog' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
            -i -e s/"define( 'DB_USER', 'username_here' );"/"define( 'DB_USER',
            'root' );"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
            -e s/"define( 'DB_PASSWORD', 'password_here' );"/"define( 'DB_PASSWORD',
            'mysqlpassword' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
            -i -e s/"define( 'DB_HOST', 'localhost' );"/"define( 'DB_HOST', '$
            {DBTier.networks[0].address}' );"/ /var/www/html/mywordpresssite/wp-config.php
          - service apache2 reload
      DBTier:
        type: Cloud.Machine
        properties:

```

```

name: mysql
image: ubuntu
flavor: '${input.size}'
constraints:
  - tag: '${input.env}'
networks:
  - network: '${resource["WP-Network-Private"].id}'
    assignPublicIpAddress: true
remoteAccess:
  authentication: usernamePassword
  username: '${input.username}'
  password: '${input.userpassword}'
cloudConfig: |
  #cloud-config
  repo_update: true
  repo_upgrade: all
  packages:
    - mysql-server
  runcmd:
    - sed -e '/bind-address/ s/^#*\/#/' -i /etc/mysql/mysql.conf.d/mysqld.cnf
    - service mysql restart
    - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'mysqlpassword';"
    - mysql -e "FLUSH PRIVILEGES;"
  attachedDisks: []
WP-Network-Private:
  type: Cloud.Network
  properties:
    name: WP-Network-Private
    networkType: existing

```

Nächste Schritte

Testen Sie die Cloud-Vorlage, indem Sie die Syntax überprüfen und die Vorlage bereitstellen.

Testen einer einfachen Cloud-Vorlage

Während des Designs erstellen Sie häufig eine Cloud-Vorlage, indem Sie mit den Grundlagen beginnen, dann bereitstellen und testen, während die Vorlage sich weiterentwickelt. Dieses Beispiel zeigt einige der laufenden Tests, die in vRealize Automation Cloud Assembly integriert sind.

Wenn Sie sicherstellen möchten, dass eine Bereitstellung Ihren Anforderungen entsprechend funktioniert, können Sie die Cloud-Vorlage mehrmals testen und bereitstellen. Sie fügen schrittweise weitere Komponenten hinzu, testen den Blueprint erneut und stellen ihn erneut bereit.

Voraussetzungen

Erstellen Sie die einfache Cloud-Vorlage. Weitere Informationen hierzu finden Sie unter [Erstellen einer einfachen Cloud-Vorlage](#).

Verfahren

- 1 Klicken Sie auf **Cloud-Vorlagen** und öffnen Sie die WordPress-BP-Cloud-Vorlage.
Die einfache Cloud-Vorlage wird in der Design-Arbeitsfläche und im Code-Editor angezeigt.
- 2 Um die Vorlagensyntax, die Platzierung und die grundlegende Gültigkeit zu überprüfen, klicken Sie unten links auf **Test**.
- 3 Wählen Sie Eingabewerte aus und klicken Sie auf **Test**.

Testing Basic

Environment ⓘ

Tier Machine Size ⓘ

Database Username

Database Password

Der Test ist nur eine Simulation und virtuelle Maschinen oder sonstige Ressourcen werden dabei nicht wirklich bereitgestellt.

← Test Result for Basic ⓘ

Successful This simulation only tests syntax, placement and basic validity

3 Infos Provisioning Diagram

▼ WP-Network-Private

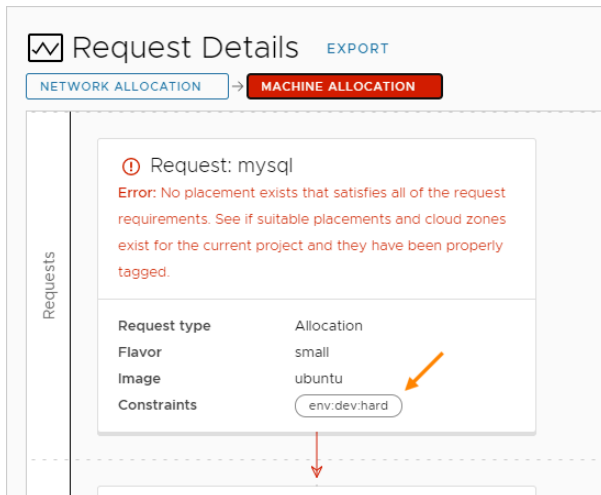
LINE 96

▼ DBTier

LINE 69

▼ WebTier

Der Test enthält einen Link zu einem **Bereitstellungsdiagramm**, in dem Sie den simulierten Bereitstellungsablauf überprüfen und die Ergebnisse anzeigen können. Die Simulation fördert potenzielle Probleme zutage, wie z. B. das Fehlen definierter Ressourcenkapazitäten, die mit den harten Einschränkungen in der Cloud-Vorlage übereinstimmen. Im folgenden Beispielfehler wurde eine Cloud-Zone des Funktions-Tags `env:dev` an keiner Stelle in der definierten Infrastruktur gefunden.



Eine erfolgreiche Simulation garantiert allerdings nicht, dass Sie die Vorlage ohne Fehler bereitstellen können.

- 4 Nachdem die Vorlage die Simulation erfolgreich durchlaufen hat, klicken Sie unten links auf **Bereitstellen**.
- 5 Wählen Sie **Neue Bereitstellung erstellen** aus.
- 6 Geben Sie der Bereitstellung den Namen **WordPress for OurCo** und klicken Sie auf **Weiter**.
- 7 Wählen Sie Eingabewerte aus und klicken Sie auf **Bereitstellen**.
- 8 Unter **Bereitstellungen > Bereitstellungen** können Sie überprüfen, ob die Vorlage erfolgreich bereitgestellt wurde.

Wenn eine Bereitstellung fehlschlägt, klicken Sie auf Ihren Namen und klicken Sie auf die Registerkarte **Verlauf**, um Nachrichten anzuzeigen, die Ihnen bei der Fehlerbehebung helfen können.

Timestamp	Status	Resource type	Resource name
Sep 8, 2020, 1...	CREATE_IN_PROGRESS	Cloud.Machine	WebTier
Sep 8, 2020, 1...	CREATE_FINISHED	Cloud.Machine	DBTier
Sep 8, 2020, 1...	CREATE_IN_PROGRESS	Cloud.Machine	DBTier
Sep 8, 2020, 1...	CREATE_FINISHED	Cloud.Network	WP-Network-Private
Sep 8, 2020, 1...	CREATE_IN_PROGRESS	Cloud.Network	WP-Network-Private

Einige Verlaufeinträge verfügen unter Umständen ganz rechts über einen Link **Bereitstellungsdiagramm**. Das Diagramm ähnelt dem simulierten, in dem Sie das Flussdiagramm von vRealize Automation Cloud Assembly-Entscheidungspunkten im Bereitstellungsprozess überprüfen.

Weitere Flussdiagramme sind unter **Infrastruktur > Aktivität > Anforderungen** verfügbar.

- 9 Um zu überprüfen, ob die Anwendung funktioniert, öffnen Sie die WordPress-Startseite in einem Browser.
 - a Warten Sie, bis die WordPress-Server vollständig erstellt und initialisiert wurden.
Die Initialisierung kann je nach Umgebung 30 Minuten oder länger dauern.
 - b Um den FQDN oder die IP-Adresse der Site zu finden, wechseln Sie zu **Bereitstellungen > Bereitstellungen > Topologie**.
 - c Klicken Sie auf der Arbeitsfläche auf die Webebene (WebTier) und suchen Sie die IP-Adresse im Bereich auf der rechten Seite.
 - d Geben Sie die IP-Adresse als Teil der vollständigen URL zur WordPress-Startseite ein.
In diesem Beispiel lautet die vollständige URL:
`http://{IP-address}/mywordpresssite`
oder
`http://{IP-address}/mywordpresssite/wp-admin/install.php`
- 10 Wenn Sie WordPress in einem Browser überprüft und festgestellt haben, dass die Anwendung noch nachbearbeitet werden muss, nehmen Sie Vorlagenänderungen vor und stellen Sie sie mit der Option **Vorhandene Bereitstellung aktualisieren** erneut bereit.
- 11 Überlegen Sie, ob Sie die Cloud-Vorlage versionieren möchten. Sie können eine funktionierende Version wiederherstellen, wenn eine Änderung dazu führt, dass die Bereitstellung fehlschlägt.
 - a Klicken Sie auf der Designseite der Cloud-Vorlage auf **Version**.
 - b Geben Sie auf der Seite „Version erstellen“ **WP-1.0** ein.
Geben Sie in Versionsnamen keine Leerzeichen ein.
 - c Klicken Sie auf **Erstellen**.
Um eine Version zu überprüfen oder wiederherzustellen, klicken Sie auf der Seite „Design“ auf die Registerkarte **Versionsverlauf**.
- 12 Wenn jetzt eine einfache Bereitstellung möglich ist, versuchen Sie, Ihre erste Bereitstellungszeit zu verbessern, indem Sie CPU und Arbeitsspeicher auf den Anwendungs- und Datenbankservern erhöhen.

Führen Sie eine Aktualisierung auf eine mittlere Knotengröße für beide Komponenten durch. Wählen Sie unter Verwendung derselben Vorlage **medium** zur Bereitstellungszeit aus, führen Sie die Bereitstellung erneut durch und überprüfen Sie die Anwendung erneut.

Nächste Schritte

Erweitern Sie die Cloud-Vorlage in eine produktionsfähige Anwendung, indem Sie noch weitere Ressourcen hinzufügen.

Erweitern einer Cloud-Vorlage

Nachdem Sie die einfache vRealize Automation Cloud Assembly-Vorlage für die Beispielanwendung erstellt und getestet haben, erweitern Sie sie in eine mehrschichtige Anwendung, die für die Entwicklung, den Test und schließlich die Produktion bereitgestellt werden kann.

Um die Cloud-Vorlage zu erweitern, fügen Sie die folgenden Verbesserungen hinzu.

- Eine Option zum Clustern von Anwendungsservern für eine größere Kapazität
- Ein öffentliches Netzwerk und ein Lastausgleichsdienst vor den Anwendungsservern
- Ein Sicherungsserver mit Archivspeicher

Voraussetzungen

Erstellen Sie die einfache Cloud-Vorlage und testen Sie sie. Weitere Informationen finden Sie unter [Erstellen einer einfachen Cloud-Vorlage](#) und [Testen einer einfachen Cloud-Vorlage](#).

Verfahren

- 1 Klicken Sie auf **Cloud-Vorlagen** und öffnen Sie die WordPress-BP-Cloud-Vorlage.

Die einfache Vorlage wird in der Design-Arbeitsfläche und im Code-Editor angezeigt.

- 2 Nehmen Sie Ergänzungen und Änderungen vor, indem Sie das Codebeispiel und die Abbildung für die Anleitung verwenden.

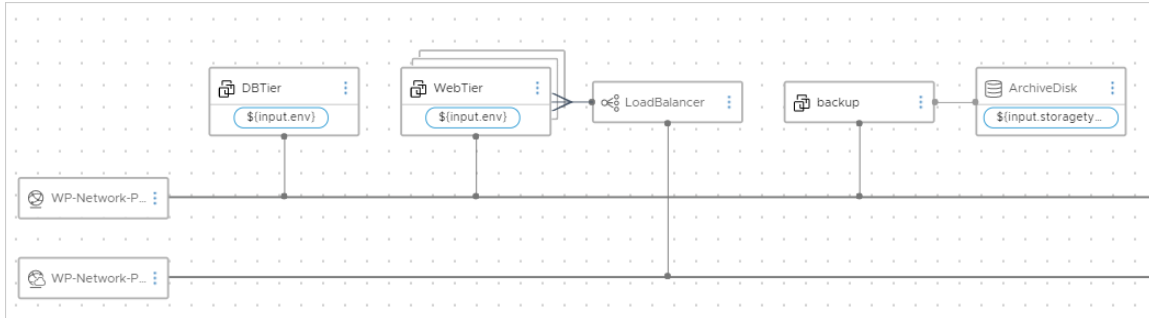
Sie verwenden die Benutzeroberfläche, um neue Ressourcen auf die Arbeitsfläche (zum Beispiel den Lastausgleichsdienst) zu ziehen, und schließen dann die Konfiguration im Code-Editor ab.

- a Fügen Sie eine Eingabeaufforderung vom Typ `count` hinzu, um den WordPress-Anwendungsserver in einen Cluster umzuwandeln.
- b Fügen Sie einen Cloud-unabhängigen Lastausgleichsdienst hinzu.
- c Verbinden Sie den Lastausgleichsdienst mit dem Cluster des WordPress-Anwendungsservers.
- d Fügen Sie eine Cloud-unabhängige Sicherungsmaschine hinzu.
- e Verbinden Sie die Sicherungsmaschine mit dem privaten/internen Netzwerk.
- f Fügen Sie ein Cloud-unabhängiges öffentliches/externes Netzwerk hinzu.
- g Verbinden Sie den Lastausgleichsdienst mit dem öffentlichen Netzwerk.
- h Fügen Sie einen Cloud-unabhängigen Speicherdatenträger zwecks Verwendung als Archivierungsdatenträger hinzu.
- i Verbinden Sie die Archivfestplatte mit der Sicherungsmaschine.
- j Fügen Sie eine Eingabeaufforderung für die Archivfestplattengeschwindigkeit hinzu.

- 3 Führen Sie die Bereitstellung, die Tests und Änderungen auf dieselbe Weise wie bei der einfachen Cloud-Vorlage durch.

Sie können vorhandene Bereitstellungen aktualisieren oder sogar neue Instanzen bereitstellen, damit Sie Bereitstellungen vergleichen können.

Ziel ist es, eine solide, wiederholbare Vorlage zu erhalten, die für Produktionsbereitstellungen verwendet werden kann.



Beispiel: Abgeschlossenes Codebeispiel für erweiterte Cloud-Vorlagen

```
formatVersion: 1
inputs:
  env:
    type: string
    enum:
      - env:dev
      - env:prod
      - env:test
    default: env:dev
    title: Environment
    description: Target Environment
  size:
    type: string
    enum:
      - small
      - medium
      - large
    description: Size of Nodes
    title: Tier Machine Size
  username:
    type: string
    minLength: 4
    maxLength: 20
    pattern: '[a-z]+'
    title: Database Username
    description: Database Username
  userpassword:
    type: string
    pattern: '[a-z0-9A-Z@#\$]+'
```

```

    encrypted: true
    title: Database Password
    description: Database Password
  count:
    type: integer
    default: 2
    maximum: 5
    minimum: 2
    title: WordPress Cluster Size
    description: WordPress Cluster Size (Number of Nodes)
  storagetype:
    type: string
    enum:
      - storage:general
      - storage:fast
    description: Archive Storage Disk Type
    title: Archive Disk Type
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      image: ubuntu
      flavor: '${input.size}'
      count: '${input.count}'
      constraints:
        - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
        assignPublicIpAddress: true
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
      packages:
        - apache2
        - php
        - php-mysql
        - libapache2-mod-php
        - php-mcrypt
        - mysql-client
      runcmd:
        - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
        https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
        mywordpresssite --strip-components 1
        - i=0; while [ $i -le 10 ]; do mysql --connect-timeout=3 -h $
        {DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;
        i=$((i+1)); done
        - mysql -u root -pmysqlpassword -h ${DBTier.networks[0].address} -e "create database
        wordpress_blog;"
        - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/
        mywordpresssite/wp-config.php
        - sed -i -e s/"define( 'DB_NAME', 'database_name_here' );"/"define( 'DB_NAME',
        'wordpress_blog' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
        -i -e s/"define( 'DB_USER', 'username_here' );"/"define( 'DB_USER',

```

```

'root' );"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
-e s/"define( 'DB_PASSWORD', 'password_here' );"/"define( 'DB_PASSWORD',
'mysqlpassword' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_HOST', 'localhost' );"/"define( 'DB_HOST', '$
{DBTier.networks[0].address}' );"/ /var/www/html/mywordpresssite/wp-config.php
    - service apache2 reload
DBTier:
  type: Cloud.Machine
  properties:
    name: mysql
    image: ubuntu
    flavor: '${input.size}'
    constraints:
      - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
        assignPublicIpAddress: true
    remoteAccess:
      authentication: usernamePassword
      username: '${input.username}'
      password: '${input.userpassword}'
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
      packages:
        - mysql-server
      runcmd:
        - sed -e '/bind-address/ s/^#*\/#/' -i /etc/mysql/mysql.conf.d/mysqld.cnf
        - service mysql restart
        - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'mysqlpassword';"
        - mysql -e "FLUSH PRIVILEGES;"
    attachedDisks: []
LoadBalancer:
  type: Cloud.LoadBalancer
  properties:
    name: myapp-lb
    network: '${resource["WP-Network-Public"].id}'
    instances:
      - '${WebTier.id}'
    routes:
      - protocol: HTTP
        port: '80'
        instanceProtocol: HTTP
        instancePort: '80'
        healthCheckConfiguration:
          protocol: HTTP
          port: '80'
          urlPath: /mywordpresssite/wp-admin/install.php
          intervalSeconds: 6
          timeoutSeconds: 5
          unhealthyThreshold: 2
          healthyThreshold: 2
        internetFacing: true
WP-Network-Private:

```

```

type: Cloud.Network
properties:
  name: WP-Network-Private
  networkType: existing
WP-Network-Public:
  type: Cloud.Network
  properties:
    name: WP-Network-Public
    networkType: public
backup:
  type: Cloud.Machine
  properties:
    name: backup
    flavor: '${input.size}'
    image: ubuntu
    networks:
      - network: '${resource["WP-Network-Private"].id}'
    attachedDisks:
      - source: '${resource.ArchiveDisk.id}'
ArchiveDisk:
  type: Cloud.Volume
  properties:
    name: ArchiveDisk
    capacityGb: 5
    constraints:
      - tag: '${input.storagetype}'

```

Nächste Schritte

Definieren Sie Ihre eigene Infrastruktur und erstellen Sie Ihre eigenen Cloud-Vorlagen.

Weitere Informationen finden Sie unter [Kapitel 4 Erstellen der vRealize Automation Cloud Assembly-Ressourceninfrastruktur](#) und [Kapitel 6 Entwerfen Ihrer vRealize Automation Cloud Assembly-Bereitstellungen](#).

Lernprogramm: Konfigurieren von VMware Cloud on AWS für vRealize Automation

In diesem vRealize Automation Cloud Assembly-Lernprogramm wird der Vorgang zum Definieren von Ressourceninfrastruktur- und Cloud-Vorlageneinstellungen für die Bereitstellung in einer VMware Cloud on AWS-Umgebung veranschaulicht.

Dieser Vorgang setzt voraus, dass ein Cloud-Administrator das VMware Cloud on AWS-SDDC Ihrer Organisation gemäß der Beschreibung unter *Bereitstellen und Verwalten eines SDDC (Software-Defined Data Center)* im Dokument [Erste Schritte mit VMware Cloud on AWS](#) bereits konfiguriert hat.

Schauen Sie sich die schrittweise Einrichtung genau an, um den Vorgang zum Konfigurieren Ihrer Umgebung für VMware Cloud on AWS zu verstehen. Beachten Sie, dass es sich bei den angezeigten Werten nur um Anwendungsfallbeispiele handelt. Überlegen Sie sich, wo Sie Ihre eigenen Ersetzungen vornehmen würden, oder übernehmen Sie eine Hochrechnung aus den Beispielwerten, um Ihre eigene Cloud-Infrastruktur einzurichten und Ihre Bereitstellungsanforderungen zu erfüllen.

Ein detailliertes Video eines ähnlichen Workflows hat *VMware Cloud Management Technical Marketing* unter dem Titel [How to Configure VMware Cloud on AWS for Cloud Assembly](#) (Konfigurieren von VMware Cloud on AWS für Cloud Assembly) bereitgestellt.

Verfahren

1 Konfigurieren eines grundlegenden VMware Cloud on AWS-Workflows in vRealize Automation

Dieser Anwendungsfall zeigt den Prozess, in dem die Ressourceninfrastruktur und eine entsprechende Cloud-Vorlage für die Bereitstellung in einer VMware Cloud on AWS-Umgebung definiert werden.

2 Konfigurieren eines isolierten Netzwerks im VMware Cloud on AWS-Workflow in vRealize Automation

In diesem Verfahren fügen Sie ein isoliertes Netzwerk für Ihre VMware Cloud on AWS-Bereitstellung in vRealize Automation hinzu.

Konfigurieren eines grundlegenden VMware Cloud on AWS-Workflows in vRealize Automation

Dieser Anwendungsfall zeigt den Prozess, in dem die Ressourceninfrastruktur und eine entsprechende Cloud-Vorlage für die Bereitstellung in einer VMware Cloud on AWS-Umgebung definiert werden.

In diesem Verfahren konfigurieren Sie Infrastruktur, die die Cloud-Vorlagenbereitstellung an Ressourcen in Ihrer vorhandenen VMware Cloud on AWS-Umgebung unterstützt.

Voraussetzungen

- Bevor Sie ein VMware Cloud on AWS-Cloud-Konto in vRealize Automation Cloud Assembly erstellen und konfigurieren können, müssen Sie Teil einer Organisation in einer vorhandenen VMware Cloud on AWS-SDDC-Umgebung sein. Informationen zum Konfigurieren des VMware Cloud on AWS-Diensts finden Sie in der [Dokumentation zu VMware Cloud on AWS](#).
- Um die erforderliche Verbindung zwischen Ihrem vorhandenen VMware Cloud on AWS-Host-SDDC in vCenter und einem VMware Cloud on AWS-Cloud-Konto in vRealize Automation

Cloud Assembly zu erleichtern, müssen Sie eine Netzwerkverbindung bereitstellen und Firewallregeln hinzufügen, indem Sie ein VPN oder ein ähnliches Netzwerk verwenden. Weitere Informationen finden Sie unter [Vorbereiten des VMware Cloud on AWS-SDDC für die Verbindung mit VMware Cloud on AWS-Cloud-Konten in vRealize Automation](#).

Verfahren

1 [Vorbereiten des VMware Cloud on AWS-SDDC für die Verbindung mit VMware Cloud on AWS-Cloud-Konten in vRealize Automation](#)

Bei Verwendung von VMware Cloud on AWS-Cloud-Konten in Ihrer lokalen vRealize Automation Cloud Assembly-Umgebung müssen Sie eine Netzwerkverbindung erstellen, um die Kommunikation zwischen Ihrem SDDC in vCenter und allen VMware Cloud on AWS-Cloud-Konten in vRealize Automation zu unterstützen.

2 [Erstellen eines VMware Cloud on AWS-Cloud-Kontos in vRealize Automation innerhalb eines Beispiel-Workflows](#)

In diesem Verfahren erstellen Sie ein VMware Cloud on AWS-Cloud-Konto in vRealize Automation.

3 [Erstellen einer Cloud-Zone für VMware Cloud on AWS-Bereitstellungen in vRealize Automation](#)

In diesem Schritt erstellen Sie eine Cloud-Zone zur Angabe einer Computing-Ressource, auf die der CloudAdmin-Benutzer beim Arbeiten mit VMware Cloud on AWS in vRealize Automation zugreifen kann.

4 [Konfigurieren von Netzwerk- und Speicherprofilen für VMware Cloud on AWS-Bereitstellungen in vRealize Automation](#)

In diesem Schritt konfigurieren Sie ein Netzwerk- und Speicherprofil zur Angabe von Ressourcen, die einem VMware Cloud on AWS-CloudAdmin-Benutzer in vRealize Automation zur Verfügung stehen.

5 [Erstellen eines Projekts zur Unterstützung von VMware Cloud on AWS-Bereitstellungen in vRealize Automation](#)

In diesem Schritt definieren Sie ein vRealize Automation-Projekt, das zum Steuern der Ressourcen verwendet werden kann, die für VMware Cloud on AWS-Bereitstellungen verfügbar sind.

6 [Definieren einer vCenter-Maschinenressource in einem Cloud-Vorlagendesign zur Unterstützung der VMware Cloud on AWS-Bereitstellung in vRealize Automation](#)

In diesem Schritt ziehen Sie eine vCenter-Maschinenressource auf die Design-Arbeitsfläche und fügen Einstellungen für eine VMware Cloud on AWS-Bereitstellung in vRealize Automation hinzu.

Vorbereiten des VMware Cloud on AWS-SDDC für die Verbindung mit VMware Cloud on AWS-Cloud-Konten in vRealize Automation

Bei Verwendung von VMware Cloud on AWS-Cloud-Konten in Ihrer lokalen vRealize Automation Cloud Assembly-Umgebung müssen Sie eine Netzwerkverbindung erstellen, um die Kommunikation zwischen Ihrem SDDC in vCenter und allen VMware Cloud on AWS-Cloud-Konten in vRealize Automation zu unterstützen.

Um die erforderliche Verbindung zwischen Ihrem vorhandenen VMware Cloud on AWS-Host-SDDC in vCenter und einem VMware Cloud on AWS-Cloud-Konto in vRealize Automation zu erleichtern, müssen Sie eine Netzwerkverbindung zwischen den beiden Elementen mithilfe eines VPN oder ähnlicher Netzwerkmittel bereitstellen.

Verfahren

- 1 Konfigurieren Sie eine VPN-Verbindung über das öffentliche Internet oder AWS Direct Connect.

Weitere Informationen finden Sie unter *VMware Cloud on AWS – Netzwerk und Sicherheit* in der [VMware Cloud on AWS-Dokumentation](#).

- 2 Stellen Sie sicher, dass der vCenter Server-FQDN unter einer privaten IP-Adresse im Verwaltungsnetzwerk aufgelöst werden kann.

Weitere Informationen finden Sie unter *VMware Cloud on AWS – Netzwerk und Sicherheit* in der [VMware Cloud on AWS-Dokumentation](#).

- 3 Konfigurieren Sie erforderliche Firewallregeln.

Sie müssen Firewallregeln für das Verwaltungs-Gateway in der VMware Cloud on AWS-Konsole des SDDC konfigurieren, um die Kommunikation zu unterstützen. Die Regeln müssen sich im Abschnitt mit Firewallregeln für das **Verwaltungs-Gateway** befinden. Erstellen Sie die Firewallregeln mithilfe der Optionen auf der Registerkarte **Netzwerke und Sicherheit** in der SDDC-Konsole.

- Begrenzen Sie den Netzwerkdatenverkehr zu ESXi für HTTPS (TCP 443)-Dienste auf die ermittelte IP-Adresse der/des vRealize Automation-Appliance/Servers oder die Lastausgleichsdienst-VIP für vRealize Automation.
- Begrenzen Sie den Netzwerkdatenverkehr zu vCenter für ICMP (Alle ICMP-), SSO (TCP 7444)- und HTTPS (TCP 443)-Dienste auf die ermittelte IP-Adresse der/des vRealize Automation-Appliance/Servers oder die Lastausgleichsdienst-VIP für vRealize Automation.
- Begrenzen Sie den Netzwerkdatenverkehr zu NSX-T Manager für HTTPS (TCP 443)-Dienste auf die ermittelte IP-Adresse der/des vRealize Automation-Appliances/Servers oder die Lastausgleichsdienst-VIP für vRealize Automation.

Die erforderlichen Firewallregeln werden in der folgenden Tabelle zusammengefasst.

Tabelle 2-1. Erforderliche Firewallregeln für das Verwaltungs-Gateway – Übersicht

Name	Quelle	Ziel	Dienst
vCenter	CIDR-Block des lokalen Datencenters	vCenter	Beliebig (Gesamter Datenverkehr)
vCenter-Ping	Alle	vCenter	ICMP (Gesamtes ICMP)
NSX Manager	CIDR-Block des lokalen Datencenters	NSX Manager	Beliebig (Gesamter Datenverkehr)
Lokal zu ESXi-Ping	CIDR-Block des lokalen Datencenters	Nur ESXi-Verwaltung	ICMP (Gesamtes ICMP)
Lokal zu ESXi Remote Console und Bereitstellung	CIDR-Block des lokalen Datencenters	Nur ESXi-Verwaltung	TCP 902
Lokal zu SDDC-VM	CIDR-Block des lokalen Datencenters	CIDR-Block des logischen SDDC-Netzwerks	Beliebig (Gesamter Datenverkehr)
SDDC-VM zu lokal	CIDR-Block des logischen SDDC-Netzwerks	CIDR-Block des lokalen Datencenters	Beliebig (Gesamter Datenverkehr)

Zugehörige Informationen finden Sie unter *Netzwerk und Sicherheit von VMware Cloud on AWS* und im *Betriebshandbuch für VMware Cloud on AWS* in der [VMware Cloud on AWS-Dokumentation](#).

Ergebnisse

Nachdem Sie den erforderlichen Zugriff auf Gateways und die Firewallregeln konfiguriert haben, können Sie mit dem Vorgang zum Erstellen eines VMware Cloud on AWS-Cloud-Kontos fortfahren.

Erstellen eines VMware Cloud on AWS-Cloud-Kontos in vRealize Automation innerhalb eines Beispiel-Workflows

In diesem Verfahren erstellen Sie ein VMware Cloud on AWS-Cloud-Konto in vRealize Automation.

Weitere Informationen finden Sie in der [Dokumentation zu VMware Cloud on AWS](#).

Sofern nicht anders angegeben, gelten die in diesem Verfahren eingegebenen Schrittwerte nur für diesen Beispiel-Workflow.

Voraussetzungen


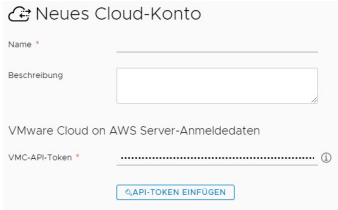
- Bei diesem Verfahren wird davon ausgegangen, dass Sie über die erforderlichen Administratoranmeldedaten verfügen, einschließlich VMware Cloud on AWS-CloudAdmin-Anmeldedaten für das Ziel-SDDC in vCenter, und dass der HTTPS-Zugriff auf Port 443 aktiviert wurde. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).

- Bei diesem Verfahren wird vorausgesetzt, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Um die erforderliche Verbindung zwischen Ihrem vorhandenen VMware Cloud on AWS-Host-SDDC in vCenter und einem VMware Cloud on AWS-Cloud-Konto in vRealize Automation zu erleichtern, müssen Sie eine Netzwerkverbindung und Firewallregeln bereitstellen, indem Sie ein VPN oder ein ähnliches Netzwerk verwenden. Weitere Informationen hierzu finden Sie unter [Vorbereiten des VMware Cloud on AWS-SDDC für die Verbindung mit VMware Cloud on AWS-Cloud-Konten in vRealize Automation](#). Wenn Sie einen externen HTTP-Internet-Proxy verwenden, muss dieser für IPv4 konfiguriert sein.
- Wenn Sie nicht über externen Internetzugriff verfügen, konfigurieren Sie einen Internet-Proxyserver. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Integrieren eines Internet-Proxyservers für vRealize Automation](#).

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Cloud-Konten** aus.
- 2 Klicken Sie auf **Cloud-Konto hinzufügen**, wählen Sie VMware Cloud on AWS aus und geben Sie Werte ein.

Beispielwerte und zusätzliche Informationen werden in der folgenden Tabelle bereitgestellt.

Einstellung	Beispielwert und Anweisung	Beschreibung
VMC-API-Token	<ol style="list-style-type: none"> Klicken Sie auf das <i>i</i>-Hilfesymbol am Ende der Zeile VMC-API-Token und klicken Sie auf die Seite API-Token im Hilfetextfeld, um die Registerkarte API-Token auf der Mein Konto-Seite Ihrer Organisation zu öffnen. Klicken Sie auf Token generieren, um die Optionen für Neues API-Token generieren anzuzeigen. Geben Sie einen Namen für das neue Token ein, z. B. myinitials_mytoken. Legen Sie die Token-TTL auf nie ablaufen fest. Wenn Sie ein Token erstellen, das auf „ablaufen“ festgelegt ist, funktionieren die VMware Cloud on AWS-Vorgänge von vRealize Automation nicht mehr, wenn das Token abläuft, und funktionieren erst wieder, nachdem Sie das Cloud-Konto mit einem neuen Token aktualisiert haben. Wählen Sie im Abschnitt Geltungsbereiche definieren die Option Alle Rollen.  Klicken Sie auf Generieren. Klicken Sie auf der Seite des generierten Tokens auf Kopieren und dann auf Weiter. Kehren Sie zur Seite Neues Cloud-Konto zurück, fügen Sie das kopierte Token in die Zeile VMC-API-Token ein und klicken Sie auf API-Token einfügen.  	<p>Sie können auf der verknüpften Seite API-Token für Ihre Organisation ein neues Token erstellen oder ein vorhandenes Token verwenden.</p> <p>Im Abschnitt Geltungsbereiche definieren müssen mindestens die folgenden Rollen für das API-Token festgelegt werden:</p> <ul style="list-style-type: none"> ■ Organisationsrollen <ul style="list-style-type: none"> ■ Organisationsmitglied ■ Organisationsbesitzer ■ Dienstrollen – VMware Cloud on AWS <ul style="list-style-type: none"> ■ Administrator ■ NSX Cloud-Administrator ■ NSX Cloud-Auditor <p>Hinweis Sie können das generierte Token kopieren, herunterladen oder drucken. Wenn Sie diese Seite verlassen, können Sie das generierte Token nicht mehr abrufen.</p> <p>Fügen Sie das generierte oder bereitgestellte Token ein, um eine Verbindung zur verfügbaren SDDC-Umgebung im VMware Cloud on AWS-Abonnement Ihrer Organisation herzustellen, und füllen Sie die Liste der SDDC-Namen auf.</p> <p>Wenn sich die vRealize Automation- und VMware Cloud on AWS-Dienste in unterschiedlichen Organisationen befinden, sollten Sie zur VMware Cloud on AWS-Organisation wechseln und dann das Token generieren.</p> <p>Weitere Informationen zu API-Token finden Sie unter Generieren von API-Token.</p>
SDDC-Name	Wählen Sie für dieses Beispiel „Datacenter:Datacenter-abz“ aus.	Treffen Sie eine Auswahl in der Liste der verfügbaren SDDCs in Ihrem VMware Cloud on AWS-Abonnement. Die Liste der SDDCs

Einstellung	Beispielwert und Anweisung	Beschreibung
	Die Einträge für den vCenter- und NSX-T-FQDN werden automatisch mit dem SDDC-Namen befüllt. Wenn bereits ein Cloud-Proxy für das SDDC bereitgestellt wurde, wird der Wert für den Cloud-Proxy ebenfalls automatisch befüllt.	<p>basiert auf dem VMware Cloud on AWS-API-Token.</p> <p>NSX-V-SDDCs werden nicht mit vRealize Automation unterstützt und in der Liste der verfügbaren SDDCs nicht angezeigt.</p>
vCenter-IP-Adresse/-FQDN	Die Adresse wird automatisch basierend auf der SDDC-Auswahl angegeben.	<p>Geben Sie die IP-Adresse oder den FQDN des vCenter Server im angegebenen SDDC ein.</p> <p>Als IP-Adresse wird standardmäßig die private IP-Adresse verwendet. Je nach Typ der Netzwerkverbindung, die für den Zugriff auf Ihr SDDC verwendet wird, kann sich die Standardadresse von der IP-Adresse des NSX Manager-Servers im angegebenen SDDC unterscheiden.</p>
IP-Adresse/FQDN in NSX Manager	Die Adresse wird automatisch basierend auf der SDDC-Auswahl angegeben.	<p>Gibt die IP-Adresse oder den FQDN des NSX Managers im angegebenen SDDC ein.</p> <p>Als IP-Adresse wird standardmäßig die private IP-Adresse verwendet. Je nach Typ der Netzwerkverbindung, die für den Zugriff auf Ihr SDDC verwendet wird, kann sich die Standardadresse von der IP-Adresse des NSX Manager-Servers im angegebenen SDDC unterscheiden.</p> <p>VMware Cloud on AWS-Cloud-Konten bieten Unterstützung für NSX-T.</p>
Benutzername und Kennwort in vCenter	Als Benutzername wird automatisch „cloudadmin@vmc.local“ angegeben.	<p>Geben Sie Ihren vCenter-Benutzernamen für das angegebene SDDC ein, wenn er sich von der Standardeinstellung unterscheidet.</p> <p>Der angegebene Benutzer benötigt CloudAdmin-Anmeldedaten. Der Benutzer benötigt keine CloudGlobalAdmin-Anmeldedaten.</p> <p>Geben Sie das Benutzerkennwort ein.</p>
Validieren	Klicken Sie auf Validieren .	Mit „Validieren“ werden Ihre Zugriffsrechte für das angegebene vCenter bestätigt und es wird überprüft, ob das vCenter ausgeführt wird.
Name und Beschreibung	<p>Geben Sie OurCo-VMC als Namen für das Cloud-Konto ein.</p> <p>Geben Sie Beispielbereitstellung für VMC als Beschreibung für das Cloud-Konto ein.</p>	
Bereitstellung für diese Datencenter zulassen	Diese Informationen sind schreibgeschützt.	Listet verfügbare Datencenter in der angegebenen VMware Cloud on AWS-SDDC-Umgebung auf.

Einstellung	Beispielwert und Anweisung	Beschreibung
Cloud-Zone erstellen	Deaktivieren Sie das Kontrollkästchen. In diesem Beispiel erstellen Sie später im Workflow eine Cloud-Zone.	Weitere Informationen hierzu finden Sie unter Weitere Informationen zu vRealize Automation Cloud Assembly-Cloud-Zonen .
Funktions-Tags	Lassen Sie dieses Feld leer. In diesem Workflow werden keine Funktions-Tags verwendet.	Verwenden Sie Tags gemäß der Tag-Strategie Ihrer Organisation. Weitere Informationen finden Sie unter Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen und Erstellen einer Tagging-Strategie .

3 Klicken Sie auf **Hinzufügen**.

Ergebnisse

Ressourcen, wie z. B. Maschinen und Volumes, werden vom VMware Cloud on AWS-SDDC-Datencenter erfasst und im Abschnitt **Ressourcen** der Registerkarte vRealize Automation **Infrastruktur** aufgelistet.

Nächste Schritte

[Erstellen einer Cloud-Zone für VMware Cloud on AWS-Bereitstellungen in vRealize Automation.](#)

Erstellen einer Cloud-Zone für VMware Cloud on AWS-Bereitstellungen in vRealize Automation

In diesem Schritt erstellen Sie eine Cloud-Zone zur Angabe einer Computing-Ressource, auf die der CloudAdmin-Benutzer beim Arbeiten mit VMware Cloud on AWS in vRealize Automation zugreifen kann.

In VMware Cloud on AWS lauten die beiden wichtigsten Administratoranmeldedaten „CloudGlobalAdmin“ und „CloudAdmin“. vRealize Automation Cloud Assembly wurde für die Unterstützung des CloudAdmin-Benutzers entwickelt. Stellen Sie die Ressourcen bereit, die für einen VMware Cloud on AWS CloudAdmin-Benutzer verfügbar sind. Führen Sie keine Bereitstellung für Ressourcen durch, die VMware Cloud on AWS CloudGlobalAdmin-Anmeldedaten benötigen.

Cloud-Zonen geben die Computing-Ressourcen an, auf denen eine Projekt-Cloud-Vorlage Maschinen, Netzwerke und Speicher bereitstellt. Weitere Informationen hierzu finden Sie unter [Weitere Informationen zu vRealize Automation Cloud Assembly-Cloud-Zonen](#).

Sofern nicht anders angegeben, gelten die in diesem Verfahren eingegebenen Schrittwerte nur für diesen Beispiel-Workflow.

Voraussetzungen

- Schließen Sie das Verfahren [Erstellen eines VMware Cloud on AWS-Cloud-Kontos in vRealize Automation innerhalb eines Beispiel-Workflows](#) ab.

- Bei diesem Verfahren wird vorausgesetzt, dass Sie über die erforderlichen Administratoranmeldedaten verfügen, einschließlich der VMware Cloud on AWS-CloudAdmin-Anmeldedaten für das Ziel-SDDC in vCenter. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Bei diesem Verfahren wird vorausgesetzt, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).

Verfahren

- 1 Wählen Sie **Infrastruktur > Konfigurieren > Cloud-Zonen** aus.
- 2 Klicken Sie auf **Neue Cloud-Zone** und geben Sie Werte für die VMware Cloud on AWS-Umgebung ein.

Einstellung	Beispielwert
Konto/Region	OurCo-VMC / Datacenter:Datacenter-abz Dies ist das Cloud-Konto und die zugehörige Region, die Sie im vorherigen Schritt, Erstellen eines VMware Cloud on AWS-Cloud-Kontos in vRealize Automation innerhalb eines Beispiel-Workflows , definiert haben.
Name	VMC_cloud_zone-1
Beschreibung	Nur VMware Cloud on AWS-Ressourcen
Platzierungsrichtlinie	Standard
Funktions-Tags	Lassen Sie dieses Feld leer. In diesem Workflow werden keine Funktions-Tags verwendet.

- 3 Klicken Sie auf die Registerkarte **Berechnen**.
- 4 Wie in Bereich 1 unten dargestellt, suchen und wählen Sie eine Computing-Ressource aus, die dem CloudAdmin-Benutzer zur Verfügung steht. Verwenden Sie für dieses Beispiel die Ressource mit dem Namen `Cluster 1/ Compute-ResourcePool`.

`Cluster 1/ Compute-ResourcePool` ist die standardmäßige Computing-Ressource für VMware Cloud on AWS.



- 5 Wie in Bereich 2 oben dargestellt, fügen Sie den Tag-Namen `vmc_placements_abz` hinzu.

Tags

1 Objekt(e) ausgewählt

Tags hinzufügen

vmc_placements_abz X

 Neues Tag eingeben

Tags entfernen

keine Tags ⓘ

- 6 Filtern Sie die Computing-Ressourcen, die in dieser Cloud-Zone verwendet werden, indem Sie `vmc_placements_abz` im Abschnitt **Filter-Tags** eingeben.
- 7 Klicken Sie auf **Speichern**.

<input type="checkbox"/>	Name	Konto/Region	Typ	Tags
<input type="checkbox"/>	ComputeClusterA	LK-TEST 测试资源池A中正在部署的Ubuntu / NSX62-Scale-DC	common.title cluster	Cluster ComputeClusterA
<input checked="" type="checkbox"/>	ComputeClusterA-New	nsx-vm 测试资源池A中正在部署的Ubuntu / NSX621-DataCenter	common.title cluster	ComputeClusterA
<input type="checkbox"/>	ComputeClusterA / Scale	270_VC_account 测试资源池A中正在部署的Ubuntu / NSX62-Scale-DC	ResourcePool	ComputeClusterA

In diesem Beispiel steht dem CloudAdmin-Benutzer nur die Computing-Ressource mit dem Namen Cluster 1/ Compute-ResourcePool zur Verfügung.

Nächste Schritte

[Konfigurieren von Netzwerk- und Speicherprofilen für VMware Cloud on AWS-Bereitstellungen in vRealize Automation.](#)

Konfigurieren von Netzwerk- und Speicherprofilen für VMware Cloud on AWS-Bereitstellungen in vRealize Automation

In diesem Schritt konfigurieren Sie ein Netzwerk- und Speicherprofil zur Angabe von Ressourcen, die einem VMware Cloud on AWS-CloudAdmin-Benutzer in vRealize Automation zur Verfügung stehen.

Obwohl auch ein Image- und Konfigurationswert benötigt werden, gibt es keine eindeutigen spezifischen Informationen zu den VMware Cloud on AWS-Benutzeranmeldedaten. In diesem Beispiel verwenden Sie einen Konfigurationswert vom Typ `small` und einen Image-Wert vom Typ `ubuntu-16`, wenn Sie die Cloud-Vorlage definieren.

Allgemeine Informationen zu Zuordnungen und Profilen finden Sie unter [Kapitel 4 Erstellen der vRealize Automation Cloud Assembly-Ressourceninfrastruktur](#).

Sofern nicht anders angegeben, gelten die in diesem Verfahren eingegebenen Schrittwerte nur für diesen Beispiel-Workflow.

Voraussetzungen

- Erstellen Sie eine Cloud-Zone. Weitere Informationen hierzu finden Sie unter [Erstellen einer Cloud-Zone für VMware Cloud on AWS-Bereitstellungen in vRealize Automation](#).
- Bei diesem Verfahren wird vorausgesetzt, dass Sie über die erforderlichen Administratoranmeldedaten verfügen, einschließlich der VMware Cloud on AWS-CloudAdmin-Anmeldedaten für das Ziel-SDDC in vCenter. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Bei diesem Verfahren wird vorausgesetzt, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).

Verfahren

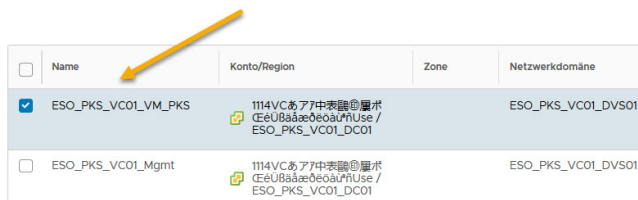
- 1 Definieren Sie ein Netzwerkprofil für VMware Cloud on AWS-Bereitstellungen.

- a Wählen Sie **Infrastruktur > Konfigurieren > Netzwerkprofile** aus und klicken Sie auf **Neues Netzwerkprofil**.

Einstellung	Beispielwert
Konto/Region	OurCo-VMC / Datacenter:Datacenter-abz Hinweis Wählen Sie das VMware Cloud on AWS-Cloud-Konto und das zugehörige SDDC aus, das Sie in Erstellen eines VMware Cloud on AWS-Cloud-Kontos in vRealize Automation innerhalb eines Beispiel-Workflows erstellt haben.
Name	vmc-network1
Beschreibung	Enthält Netzwerke, auf die Cloud-Vorlagenadministratoren mit VMware Cloud on AWS-CloudAdmin-Anmeldedaten zugreifen können.

- b Klicken Sie auf die Registerkarte **Netzwerk** und dann auf **Netzwerk hinzufügen**.
- c Wählen Sie ein Netzwerk aus, auf dem ein VMware Cloud on AWS-Benutzer mit CloudAdmin-Anmeldedaten eine Bereitstellung durchführen kann, wie z. B. `sddc-cgw-network-1`.

Netzwerk hinzufügen



<input type="checkbox"/>	Name	Konto/Region	Zone	Netzwerkdomäne
<input checked="" type="checkbox"/>	ESO_PKS_VC01_VM_PKS	114VCア7中表議@墨木 CEeUBaaæ0eoau7HUse / ESO_PKS_VC01_DC01		ESO_PKS_VC01_DVS01
<input type="checkbox"/>	ESO_PKS_VC01_Mgmt	114VCア7中表議@墨木 CEeUBaaæ0eoau7HUse / ESO_PKS_VC01_DC01		ESO_PKS_VC01_DVS01

- 2 Speichern Sie das Netzwerkprofil.

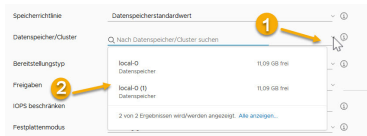
3 Definieren Sie ein Speicherprofil für VMware Cloud on AWS-Bereitstellungen.

Konfigurieren Sie ein Speicherprofil für einen Datenspeicher/Cluster, auf den der CloudAdmin-Benutzer zugreifen kann.

- a Wählen Sie **Infrastruktur > Konfigurieren > Speicherprofile** aus und klicken Sie auf **Neues Speicherprofil**.

Einstellung	Beispielwert
Konto/Region	OurCo-VMC / Datacenter:Datacenter-abz Wählen Sie das VMware Cloud on AWS-Cloud-Konto und das zugehörige SDDC aus, das Sie in Erstellen eines VMware Cloud on AWS-Cloud-Kontos in vRealize Automation innerhalb eines Beispiel-Workflows erstellt haben.
Name	vmc-storage1
Beschreibung	Enthält den Datenspeicher-Cluster, auf dem Cloud-Vorlagenadministratoren mit VMware Cloud on AWS-CloudAdmin-Anmeldedaten Bereitstellungen durchführen können.

- b Wählen Sie im Dropdown-Menü **Datenspeicher/Cluster** den Datenspeicher **WorkloadDatastore** aus.



Für VMware Cloud on AWS in vRealize Automation Cloud Assembly muss die Speicherrichtlinie den Datenspeicher **WorkloadDatastore** verwenden, um die VMware Cloud on AWS-Bereitstellung zu unterstützen.

4 Speichern Sie das Speicherprofil.

Nächste Schritte

[Erstellen eines Projekts zur Unterstützung von VMware Cloud on AWS-Bereitstellungen in vRealize Automation](#).

Erstellen eines Projekts zur Unterstützung von VMware Cloud on AWS-Bereitstellungen in vRealize Automation

In diesem Schritt definieren Sie ein vRealize Automation-Projekt, das zum Steuern der Ressourcen verwendet werden kann, die für VMware Cloud on AWS-Bereitstellungen verfügbar sind.

Weitere Informationen zu Projekten finden Sie unter [Funktionsweise von vRealize Automation Cloud Assembly-Projekten zur Bereitstellungszeit](#).

Sofern nicht anders angegeben, gelten die in diesem Verfahren eingegebenen Schrittwerte nur für diesen Beispiel-Workflow.

Voraussetzungen

- Schließen Sie das Verfahren [Konfigurieren von Netzwerk- und Speicherprofilen für VMware Cloud on AWS-Bereitstellungen in vRealize Automation](#) ab.
- Bei diesem Verfahren wird vorausgesetzt, dass Sie über die erforderlichen Administratoranmeldedaten verfügen, einschließlich der VMware Cloud on AWS-CloudAdmin-Anmeldedaten für das Ziel-SDDC in vCenter. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Bei diesem Verfahren wird vorausgesetzt, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).

Verfahren

- 1 Klicken Sie auf **Infrastruktur > Verwaltung > Projekte**.
- 2 Klicken Sie auf **Neues Projekt** und geben Sie den Projektnamen `VMC_proj-1_abz` ein.
- 3 Klicken Sie auf **Benutzer** und dann auf **Benutzer hinzufügen**.

Die Benutzer benötigen CloudAdmin-Anmeldedaten für das VMware Cloud on AWS-Abonnement ihrer Organisation.

- `chris.gray@ourco.com`, Administrator
- `kerry.white@ourco.com`, Mitglied

- 4 Klicken Sie auf **Bereitstellung** und dann auf **Cloud-Zone hinzufügen**.
- 5 Fügen Sie die Cloud-Zone hinzu, die Sie im vorherigen Schritt konfiguriert haben.

Einstellung	Beispielwert
Cloud-Zone	VMC_cloud_zone-1 Sie haben diese Cloud-Zone im vorherigen Schritt, Erstellen einer Cloud-Zone für VMware Cloud on AWS-Bereitstellungen in vRealize Automation , erstellt.
Bereitstellungspriorität	1
Grenzwert der Instanzen	3

- 6 Ignorieren Sie in diesem Beispiel die anderen Optionen.

Nächste Schritte

Erstellen Sie eine Cloud-Vorlage, die in Ihrer VMware Cloud on AWS-Umgebung bereitgestellt werden soll. Weitere Informationen hierzu finden Sie unter [Definieren einer vCenter-Maschinenressource in einem Cloud-Vorlagendesign zur Unterstützung der VMware Cloud on AWS-Bereitstellung in vRealize Automation](#).

Definieren einer vCenter-Maschinenressource in einem Cloud-Vorlagendesign zur Unterstützung der VMware Cloud on AWS-Bereitstellung in vRealize Automation

In diesem Schritt ziehen Sie eine vCenter-Maschinenressource auf die Design-Arbeitsfläche und fügen Einstellungen für eine VMware Cloud on AWS-Bereitstellung in vRealize Automation hinzu.

Erstellen Sie ein Cloud-Vorlagendesign, das Sie verfügbaren VMware Cloud on AWS-Ressourcen bereitstellen können.

Sofern nicht anders angegeben, gelten die in diesem Verfahren eingegebenen Schrittwerte nur für diesen Beispiel-Workflow.

Voraussetzungen

- Dieses Verfahren setzt voraus, dass Sie über Anmeldedaten als Cloud-Vorlagendesigner verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- In diesem Verfahren wird davon ausgegangen, dass Sie über VMware Cloud on AWS CloudAdmin-Anmeldedaten für das Ziel-SDDC in vCenter (Datacenter:Datacenter-abz) verfügen. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Konfigurieren Sie die Ressourceninfrastruktur und das Projekt gemäß der Beschreibung in den vorherigen Abschnitten.

Verfahren

- 1 Klicken Sie auf die Registerkarte **Design** und dann auf **Neu**.

Einstellung	Beispielwert
Name	vmc-bp_abz
Beschreibung	1
Projekt	VMC_proj-1_abz Dies ist das zuvor erstellte Projekt, das die ebenfalls bereits erstellte Cloud-Zone unterstützt. Das Projekt ist nun mit der Cloud-Zone verknüpft, die wiederum mit dem/der VMware Cloud on AWS-Cloud-Konto/-Region verknüpft ist, die Sie zuvor erstellt haben.

- 2 Ziehen Sie eine vSphere-Maschinenressource auf die Arbeitsfläche.
- 3 Bearbeiten Sie den folgenden (fett gedruckten) Cloud-Vorlagen-Ressourcencode in der Maschinenressource.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
```

```
properties:
  image: ubuntu-1604
  cpuCount: 1
  totalMemoryMB: 1024
  folderName: Workloads
```

Bei `image` kann es sich um einen beliebigen Wert handeln, der für Ihre Bereitstellungsanforderungen geeignet ist.

Sie müssen die `folderName: Workloads`-Anweisung zum Code des Cloud-Vorlagendesigns hinzufügen, um die VMware Cloud on AWS-Bereitstellung zu unterstützen. Die Einstellung `folderName: Workloads` unterstützt die CloudAdmin-Anmeldedaten in der VMware Cloud on AWS-SDDC-Umgebung und ist obligatorisch.

Hinweis: Obwohl die im obigen Codebeispiel angezeigte Einstellung `folderName: Workloads` notwendig ist, können Sie sie direkt in den Code der Cloud-Vorlage einfügen (wie oben gezeigt) oder zur verknüpften Cloud-Zone bzw. zum verknüpften Objekt hinzufügen. Wenn die Einstellung an mehr als einer dieser drei Positionen angegeben ist, lautet die Reihenfolge folgendermaßen:

- Die Projekteinstellung überschreibt die Cloud-Vorlagen- und die Cloud-Zoneneinstellung.
- Die Cloud-Vorlageneinstellung überschreibt die Cloud-Zoneneinstellung.

Hinweis: Sie können die Einstellungen für `cpuCount` und `totalMemoryMB` optional durch einen Eintrag vom Typ `flavor` (Größenänderung) ersetzen, wie nachfolgend dargestellt:

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: ubuntu-1604
      flavor: small
      folderName: Workloads
```

Wenn für die Cloud-Zone der Ordnerwert auf **Workloads** festgelegt ist, müssen Sie die Eigenschaft `folderName` in der Cloud-Vorlage nicht festlegen, es sei denn, Sie möchten den Wert für den Cloud-Zonenordner überschreiben.

Nächste Schritte

Erweitern Sie diesen grundlegenden VMware Cloud on AWS-Workflow, indem Sie Netzwerkisolation hinzufügen. Weitere Informationen hierzu finden Sie unter [Konfigurieren eines isolierten Netzwerks im VMware Cloud on AWS-Workflow in vRealize Automation](#).

Konfigurieren eines isolierten Netzwerks im VMware Cloud on AWS-Workflow in vRealize Automation

In diesem Verfahren fügen Sie ein isoliertes Netzwerk für Ihre VMware Cloud on AWS-Bereitstellung in vRealize Automation hinzu.

Beim Festlegen Ihres VMware Cloud on AWS-Cloud-Kontos stehen die NSX-T-Einstellungen zur Verfügung, die in Ihrem VMware Cloud on AWS-Dienst konfiguriert sind. Informationen zum Konfigurieren von NSX-T-Einstellungen in Ihrem VMware Cloud on AWS-Dienst finden Sie in der VMware Cloud on AWS-[Produktdokumentation](#).

vRealize Automation unterstützt VMware Cloud on AWS mit NSX-T. VMware Cloud on AWS wird mit NSX-V nicht unterstützt.

vRealize Automation unterstützt Netzwerkisolierung für VMware Cloud on AWS-Bereitstellungen. Für VMware Cloud on AWS werden keine anderen Netzwerkmethoden unterstützt.

Diese Erweiterung des grundlegenden VMware Cloud on AWS-Workflows beschreibt die folgenden Methoden zum Erstellen eines isolierten Netzwerks für die Verwendung in Ihrer Cloud-Vorlage:

- Konfigurieren Sie auf einem bedarfsgesteuerten Netzwerk basierende Isolierung.
- Konfigurieren Sie auf bedarfsgesteuerten Sicherheitsgruppen basierende Isolierung.

Voraussetzungen

Mit diesem Verfahren wird der grundlegende VMware Cloud on AWS-Workflow erweitert. Der Workflow verwendet dasselbe Cloud-Konto und dieselbe Region, dieselbe Cloud-Zone, dasselbe Projekt und Netzwerkprofil, die Sie im Workflow [Lernprogramm: Konfigurieren von VMware Cloud on AWS für vRealize Automation](#) konfiguriert haben.

Verfahren

1 [Definieren eines isolierten Netzwerks für eine VMware Cloud on AWS-Bereitstellung in vRealize Automation](#)

Sie können die Netzwerkisolierung für eine VMware Cloud on AWS-Bereitstellung mithilfe einer der folgenden Vorgehensweisen konfigurieren:

2 [Definieren einer Netzwerkkomponente in einer Cloud-Vorlage zur Unterstützung der Netzwerkisolierung für VMware Cloud on AWS in vRealize Automation](#)

In diesem Schritt ziehen Sie die Komponente einer Netzwerkmaschine auf die Arbeitsfläche einer vRealize Automation-Cloud-Vorlage und fügen Einstellungen für eine isolierte Netzwerkbereitstellung zu Ihrer VMware Cloud on AWS-Zielumgebung hinzu.

Definieren eines isolierten Netzwerks für eine VMware Cloud on AWS-Bereitstellung in vRealize Automation

Sie können die Netzwerkisolierung für eine VMware Cloud on AWS-Bereitstellung mithilfe einer der folgenden Vorgehensweisen konfigurieren:

- [Konfigurieren bedarfsgesteuerter netzwerkbasierter Isolierung in vRealize Automation](#)
- [Konfigurieren der auf bedarfsgesteuerten Sicherheitsgruppen basierenden Isolierung in vRealize Automation](#)

Konfigurieren bedarfsgesteuerter netzwerkbasierter Isolierung in vRealize Automation

Sie können Netzwerkisolierung für die Anforderungen Ihrer VMware Cloud on AWS-Bereitstellung konfigurieren, indem Sie bedarfsgesteuerte Netzwerkeinstellungen in einem Netzwerkprofil angeben und verwenden.

Sie können ein isoliertes Netzwerk mithilfe einer Sicherheitsgruppe oder mithilfe bedarfsgesteuerter Netzwerkeinstellungen angeben. In diesem Beispiel konfigurieren Sie Netzwerkisolierung durch Angabe bedarfsgesteuerter Netzwerkeinstellungen im Netzwerkprofil. Zu einem späteren Zeitpunkt greifen Sie auf das Netzwerk in einer Cloud-Vorlage zu und verwenden die Cloud-Vorlage in einer VMware Cloud on AWS-Bereitstellung.

Sofern nicht anders angegeben, gelten die in diesem Verfahren eingegebenen Schrittwerte nur für diesen Beispiel-Workflow.

Voraussetzungen

- Schließen Sie den unter [Konfigurieren eines grundlegenden VMware Cloud on AWS-Workflows in vRealize Automation](#) beschriebenen Workflow ab.
- Weitere Informationen finden Sie unter [Konfigurieren eines isolierten Netzwerks im VMware Cloud on AWS-Workflow in vRealize Automation](#).
- Bei diesem Verfahren wird vorausgesetzt, dass Sie über die erforderlichen Administratoranmeldedaten verfügen, einschließlich der VMware Cloud on AWS-CloudAdmin-Anmeldedaten für das Ziel-SDDC in vCenter. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Bei diesem Verfahren wird vorausgesetzt, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).

Verfahren

- 1 Öffnen Sie das Netzwerkprofil, das Sie im grundlegenden VMware Cloud on AWS-Workflow verwendet haben, z. B. `vmc-network1`. Weitere Informationen hierzu finden Sie unter [Konfigurieren von Netzwerk- und Speicherprofilen für VMware Cloud on AWS-Bereitstellungen in vRealize Automation](#).
- 2 Auf der Registerkarte **Netzwerke** muss keine Auswahl vorgenommen werden.
- 3 Klicken Sie auf die Registerkarte **Netzwerkrichtlinien**.

- 4 Wählen Sie die Option **Bedarfsgesteuertes Netzwerk erstellen** und die `cgw`-Standardnetzwerkdomäne aus. Geben Sie eine geeignete Größe für CIDR und Subnetz an.
- 5 Klicken Sie auf **Speichern**.

Bei Verwendung dieses Netzwerkprofils werden Maschinen in einem Netzwerk in der Standardnetzwerkdomäne bereitgestellt. Das Netzwerk wird von anderen Netzwerken isoliert, indem privater oder ausgehender Netzwerkzugriff verwendet wird.

Nächste Schritte

Konfigurieren Sie eine Netzwerkkomponente in Ihrer Cloud-Vorlage. Weitere Informationen finden Sie unter [Definieren einer Netzwerkkomponente in einer Cloud-Vorlage zur Unterstützung der Netzwerkisolierung für VMware Cloud on AWS in vRealize Automation](#)

Konfigurieren der auf bedarfsgesteuerten Sicherheitsgruppen basierenden Isolierung in vRealize Automation

Sie können die Netzwerkisolierung für Ihre VMware Cloud on AWS-Bereitstellungsanforderungen konfigurieren, indem Sie eine bedarfsgesteuerte Sicherheitsgruppe in einem Netzwerkprofil angeben und verwenden.

Sie können ein isoliertes Netzwerk mithilfe einer Sicherheitsgruppe oder mithilfe bedarfsgesteuerter Netzwerkeinstellungen angeben. In diesem Beispiel konfigurieren Sie Netzwerkisolierung durch Angabe einer bedarfsgesteuerten Sicherheitsgruppe im Netzwerkprofil. Zu einem späteren Zeitpunkt geben Sie das Netzwerk in einer Cloud-Vorlage an und verwenden die Cloud-Vorlage in einer VMware Cloud on AWS-Bereitstellung.

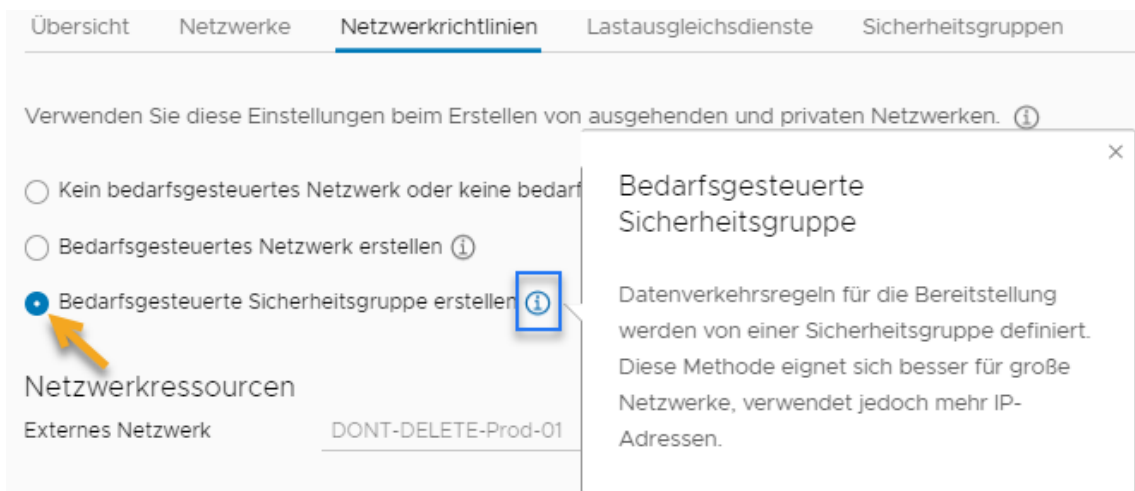
Sofern nicht anders angegeben, gelten die in diesem Verfahren eingegebenen Schrittwerte nur für diesen Beispiel-Workflow.

Voraussetzungen

- Schließen Sie den unter [Konfigurieren eines grundlegenden VMware Cloud on AWS-Workflows in vRealize Automation](#) beschriebenen Workflow ab.
- Weitere Informationen finden Sie unter [Konfigurieren eines isolierten Netzwerks im VMware Cloud on AWS-Workflow in vRealize Automation](#).
- Bei diesem Verfahren wird vorausgesetzt, dass Sie über die erforderlichen Administratoranmeldedaten verfügen, einschließlich der VMware Cloud on AWS-CloudAdmin-Anmeldedaten für das Ziel-SDDC in vCenter. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Bei diesem Verfahren wird vorausgesetzt, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).

Verfahren

- 1 Öffnen Sie das Netzwerkprofil, das Sie im grundlegenden VMware Cloud on AWS-Workflow verwendet haben, z. B. `vmc-network1`. Weitere Informationen finden Sie unter [Konfigurieren von Netzwerk- und Speicherprofilen für VMware Cloud on AWS-Bereitstellungen in vRealize Automation](#).
- 2 Wählen Sie das vorhandene Netzwerk aus, das Sie im grundlegenden VMware Cloud on AWS-Workflow verwendet haben, z. B. `sddc-cgw-network-1`. Weitere Informationen hierzu finden Sie unter [Konfigurieren von Netzwerk- und Speicherprofilen für VMware Cloud on AWS-Bereitstellungen in vRealize Automation](#).
- 3 Klicken Sie auf die Registerkarte **Netzwerkrichtlinien**.
- 4 Wählen Sie die Option **Bedarfsgesteuerte Sicherheitsgruppe erstellen** aus.



- 5 Klicken Sie auf **Speichern**.

Bei Verwendung dieses Netzwerkprofils werden Maschinen im ausgewählten Netzwerk bereitgestellt und durch eine neue Sicherheitsgruppenrichtlinie isoliert. Die neue Sicherheitsrichtlinie lässt privaten oder ausgehenden Netzwerkzugriff zu.

Nächste Schritte

Konfigurieren Sie eine Netzwerkkomponente in Ihrer Cloud-Vorlage. Weitere Informationen finden Sie unter [Definieren einer Netzwerkkomponente in einer Cloud-Vorlage zur Unterstützung der Netzwerkisolierung für VMware Cloud on AWS in vRealize Automation](#)

Definieren einer Netzwerkkomponente in einer Cloud-Vorlage zur Unterstützung der Netzwerkisolierung für VMware Cloud on AWS in vRealize Automation

In diesem Schritt ziehen Sie die Komponente einer Netzwerkmaschine auf die Arbeitsfläche einer vRealize Automation-Cloud-Vorlage und fügen Einstellungen für eine isolierte Netzwerkbereitstellung zu Ihrer VMware Cloud on AWS-Zielumgebung hinzu.

Fügen Sie der zuvor erstellten Cloud-Vorlage die Netzwerkisolierung hinzu. Die Cloud-Vorlage ist bereits mit einem Projekt und einer Cloud-Zone verknüpft, die die Bereitstellung in Ihrer VMware Cloud on AWS-Umgebung unterstützen, sowie mit dem Netzwerkprofil und dem Netzwerk, die Sie für die Isolierung konfiguriert haben.

Sofern nicht anders angegeben, gelten die in diesem Verfahren eingegebenen Schrittwerte nur für diesen Beispiel-Workflow.

Voraussetzungen

- Schließen Sie das Verfahren [Konfigurieren der auf bedarfsgesteuerten Sicherheitsgruppen basierenden Isolierung in vRealize Automation](#) oder [Konfigurieren bedarfsgesteuerter netzwerkbasierter Isolierung in vRealize Automation](#) ab.
- Dieses Verfahren setzt voraus, dass Sie über Anmeldedaten als Cloud-Vorlagendesigner verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Bei diesem Verfahren wird davon ausgegangen, dass Sie über VMware Cloud on AWS-CloudAdmin-Anmeldedaten für das Ziel-SDDC in vCenter verfügen. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).

Verfahren

- 1 Öffnen Sie die Cloud-Vorlage, die Sie im vorherigen Workflow erstellt haben. Weitere Informationen hierzu finden Sie unter [Definieren einer vCenter-Maschinenressource in einem Cloud-Vorlagendesign zur Unterstützung der VMware Cloud on AWS-Bereitstellung in vRealize Automation](#).
- 2 Ziehen Sie aus den Komponenten links auf der Entwurfsseite der Cloud-Vorlage eine Netzwerkkomponente auf die Arbeitsfläche.
- 3 Bearbeiten Sie den YAML-Code der Netzwerkkomponente, um den Netzwerktyp `private` oder `outbound` anzugeben (Fettformatierung).

```
resources: Cloud_Network_1:
  type: Cloud.Network
  properties:
    name: vmc_isolated
    networkType: private
```

ODER

```
resources: Cloud_Network_1:
  type: Cloud.Network
  properties:
    name: vmc_isolated
    networkType: outbound
```


Nächste Schritte

Sie können die Cloud-Vorlage nun bereitstellen oder schließen.

Lernprogramm: Konfigurieren einer anbieterspezifischen externen IPAM-Integration für vRealize Automation

Sie können einen externen IPAM-Anbieter zum Verwalten von IP-Adresszuweisungen für Ihre Cloud-Vorlagen-Bereitstellungen verwenden. In diesem Lernprogramm wird beschrieben, wie Sie eine externe IPAM-Integration mithilfe von Infoblox als externem IPAM-Anbieter in vRealize Automation konfigurieren.

In diesem Verfahren verwenden Sie ein vorhandenes IPAM-Anbieterpaket, in diesem Fall ein Infoblox-Paket, und eine vorhandene Ausführungsumgebung, um einen anbieterspezifischen IPAM-Integrationspunkt zu erstellen. Sie konfigurieren ein vorhandenes Netzwerk und erstellen ein Netzwerkprofil, um die IP-Adresszuteilung aus dem externen IPAM-Anbieter zu unterstützen. Schließlich erstellen Sie eine Cloud-Vorlage, die mit dem Netzwerk und Netzwerkprofil abgeglichen wird, und stellen vernetzte Maschinen mithilfe von IP-Werten bereit, die vom externen IPAM-Anbieter bezogen werden.

Informationen zum Erhalten und Konfigurieren des IPAM-Anbieterpakets sowie zum Konfigurieren einer Ausführungsumgebung, die zur Unterstützung der IPAM-Anbieterintegration auf einen Cloud-Erweiterbarkeits-Proxy zugreift, sind zu Referenzzwecken enthalten.

Beachten Sie, dass es sich bei den angezeigten Werten lediglich um Beispielwerte handelt. Sie können diese nicht eins zu eins auf Ihre Umgebung übertragen. Überlegen Sie, wo Sie Werte austauschen würden, oder führen Sie eine Extrapolation anhand der Beispielwerte durch, um die Anforderungen Ihres Unternehmens zu erfüllen.



Informationen zu einem ähnlichen vRealize Automation-Szenario, das einen Infoblox IPAM-Integrationsworkflow in einem Video veranschaulicht, finden Sie unter [Infoblox-IPAM-Plug-In 1.1-Integration mit vRealize Automation 8.1 / vRealize Automation Cloud](#).

Verfahren

1 [Hinzufügen erforderlicher erweiterbarer Attribute in der Infoblox-Anwendung für die Integration mit vRealize Automation](#)

Bevor Sie das Infoblox-Anbieterpaket (`infoblox.zip`) für die Integration mit vRealize Automation von der Infoblox-Website oder vom VMware Marketplace herunterladen und bereitstellen können, müssen Sie in Infoblox erforderliche Erweiterbarkeitsattribute hinzufügen.

2 [Herunterladen und Bereitstellen eines externen IPAM-Anbieterpakets zur Verwendung in vRealize Automation](#)

Bevor Sie einen externen IPAM-Integrationspunkt in vRealize Automation definieren können, benötigen Sie ein konfiguriertes IPAM-Anbieterpaket.

3 Erstellen einer Ausführungsumgebung für einen IPAM-Integrationspunkt in vRealize Automation

Bevor Sie einen externen IPAM-Integrationspunkt in vRealize Automation definieren können, müssen Sie eine Ausführungsumgebung erstellen bzw. auf eine vorhandene Ausführungsumgebung zugreifen, die als Vermittler zwischen dem IPAM-Anbieter und vRealize Automation fungiert. Die Ausführungsumgebung ist üblicherweise ein Amazon Web Services- oder Microsoft Azure-Cloud-Konto, das einem lokalen Integrationspunkt mit aktionsbasierter Erweiterbarkeit zugeordnet ist, der wiederum einem Cloud-Erweiterbarkeits-Proxy zugeordnet ist.

4 Hinzufügen einer externen IPAM-Integration für Infoblox in vRealize Automation

vRealize Automation unterstützt die Integration mit einem externen IPAM-Anbieter. In diesem Beispiel wird Infoblox als externer IPAM-Anbieter verwendet.

5 Konfigurieren eines Netzwerks und Netzwerkprofils zur Verwendung von IPAM (extern) für ein vorhandenes Netzwerk in vRealize Automation

Sie können ein vorhandenes Netzwerk so definieren, dass es IP-Adresswerte verwendet, die von einem externen IPAM-Anbieter anstatt intern von vRealize Automation abgerufen und verwaltet werden.

6 Definieren und Bereitstellen einer Cloud-Vorlage, die die Bereichszuweisung eines externen IPAM-Anbieters in vRealize Automation verwendet

Sie können eine Cloud-Vorlage definieren, um die IP-Adresszuweisungen des externen IPAM-Anbieters abzurufen und zu verwalten. In diesem Beispiel wird Infoblox als externer IPAM-Anbieter verwendet.

7 Verwenden Infoblox-spezifischer Eigenschaften und erweiterbarer Attribute für IPAM-Integrationen in vRealize Automation

Sie können für vRealize Automation-Projekte, die externe IPAM-Integrationen für Infoblox enthalten, Infoblox-spezifische Eigenschaften verwenden.

Hinzufügen erforderlicher erweiterbarer Attribute in der Infoblox-Anwendung für die Integration mit vRealize Automation

Bevor Sie das Infoblox-Anbieterpaket (`infoblox.zip`) für die Integration mit vRealize Automation von der Infoblox-Website oder vom VMware Marketplace herunterladen und bereitstellen können, müssen Sie in Infoblox erforderliche Erweiterbarkeitsattribute hinzufügen.

Dieses Verfahren ist anwendbar, wenn Sie für die Infoblox-Integration in vRealize Automation Cloud Assembly einen externen IPAM-Integrationspunkt erstellen.

Bevor Sie `infoblox.zip` herunterladen können, müssen Sie sich mit den Administratoranmeldedaten des Kontos Ihrer Organisation bei Ihrem Infoblox-Konto anmelden und die folgenden erweiterbaren Infoblox-Attribute vorab erstellen:

- `VMware NIC index`
- `VMware resource ID`

- Tenant ID
- CMP Type
- VM ID
- VM Name

Voraussetzungen

- Stellen Sie sicher, dass Sie über ein Konto bei [Infoblox](#) verfügen und dass Sie über die korrekten Zugriffsberechtigungen für das Infoblox-Konto Ihres Unternehmens verfügen.
- Bestätigen Sie, dass die WAPI-Version von Infoblox unterstützt wird. Die IPAM-Integration mit Infoblox beruht auf Infoblox WAPI v2.7. Alle Infoblox-Appliances mit Unterstützung für WAPI v2.7 werden unterstützt.
- Weitere Informationen finden Sie unter [Verwenden Infoblox-spezifischer Eigenschaften und erweiterbarer Attribute für IPAM-Integrationen in vRealize Automation](#).

Verfahren

- 1 Melden Sie sich mit Administratoranmeldedaten bei Ihrem Infoblox-Konto an.

Bei diesen Anmeldedaten handelt es sich um denselben Administratorbenutzernamen und das zugehörige Kennwort, die Sie beim Erstellen eines externen IPAM-Integrationspunkts in vRealize Automation Cloud Assembly über die Menüfolge **Infrastruktur > Verbindungen > Integrationen** > verwenden.

- 2 Verwenden Sie das in der Infoblox-Dokumentation beschriebene Verfahren, um die folgenden erforderlichen erweiterbaren Attribute in Ihrer Infoblox-Anwendung zu erstellen.

- VMware NIC index –Typ Ganzzahl
- VMware resource ID –Typ-Zeichenfolge
- Tenant ID –Typ-Zeichenfolge
- CMP Type –Typ-Zeichenfolge
- VM ID –Typ-Zeichenfolge
- VM Name –Typ-Zeichenfolge

Der Vorgang wird im Abschnitt *Hinzufügen von erweiterbaren Attributen* des Infoblox-Dokumentationsthemas [Informationen zu erweiterbaren Attributen](#) beschrieben. Weitere Informationen finden Sie unter [Verwalten von erweiterbaren Attributen](#).

Nächste Schritte

Nachdem Sie die erforderlichen Attribute hinzugefügt haben, können Sie den Vorgang zum Herunterladen und Bereitstellen des Infoblox-Pakets wie unter [Herunterladen und Bereitstellen eines externen IPAM-Anbieterpakets zur Verwendung in vRealize Automation](#) beschrieben fortsetzen.

Herunterladen und Bereitstellen eines externen IPAM-Anbieterpakets zur Verwendung in vRealize Automation

Bevor Sie einen externen IPAM-Integrationspunkt in vRealize Automation definieren können, benötigen Sie ein konfiguriertes IPAM-Anbieterpaket.

Sie können ein anbieterspezifisches Integrationspaket von der Website des IPAM-Anbieters, über den [VMware Solution Exchange Marketplace](#) oder, sofern verfügbar, über die vRealize Automation-Registerkarte **Marketplace** herunterladen.

Hinweis In diesem Beispiel wird das von VMware bereitgestellte Infoblox-Paket `Infoblox.zip` verwendet, das folgendermaßen über den [VMware Marketplace](#) heruntergeladen werden kann:

- [vRA Cloud Infoblox Plug-In Version 1.2](#) – kompatibel mit vRealize Automation 8.1.x und 8.2.x
- [vRA Cloud Infoblox Plug-In Version 1.1](#) – kompatibel mit vRealize Automation 8.1.x
- [vRA Cloud Infoblox Plug-In Version 1.0](#) – kompatibel mit vRealize Automation 8.0.1.x mit oder ohne Internetverbindung mit dem globalen Netzwerk
- [vRA Cloud Infoblox Plug-in Version 0.4](#) – kompatibel mit vRealize Automation 8.0.0.x und 8.0.1.x bei bestehender Internetverbindung mit dem globalen Netzwerk

Die IPAM-Integration mit Infoblox beruht auf Infoblox WAPI v2.7. Alle Infoblox-Appliances mit Unterstützung für WAPI v2.7 werden unterstützt.

Informationen zum Erstellen eines IPAM-Integrationspakets für andere IPAM-Anbieter finden Sie unter [Vorgehensweise zum Verwenden des IPAM-SDK zur Erstellung eines anbieterspezifischen, externen IPAM-Integrationspakets für vRealize Automation](#), wenn noch keins im Download-Center vorhanden ist.

Das IPAM-Anbieterpaket enthält Skripts in einem Paket mit Metadaten und anderen Konfigurationen. Die Skripts enthalten den Quellcode, der für die Vorgänge verwendet wird, die von vRealize Automation in Abstimmung mit dem externen IPAM-Anbieter ausgeführt werden. Zu den Beispielvorgängen gehören `Allocate an IP address for a virtual machine`, `Fetch a list of IP ranges from the provider` und `Update the MAC address of a host record in the provider`.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über Cloud-Administratoranmeldedaten verfügen. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Stellen Sie sicher, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Vergewissern Sie sich, dass Sie über ein Konto beim externen IPAM-Anbieter, z. B. [Infoblox](#) oder [BlueCat](#), und über die korrekten Zugriffsberechtigungen für das Konto Ihrer Organisation beim IPAM-Anbieter verfügen.

- Wenn Sie Infoblox als Ihren externen IPAM-Anbieter verwenden, vergewissern Sie sich, dass Sie Ihrem Infoblox-Konto die erforderlichen erweiterbaren Attribute hinzugefügt haben, bevor Sie fortfahren. Weitere Informationen hierzu finden Sie unter [Hinzufügen erforderlicher erweiterbarer Attribute in der Infoblox-Anwendung für die Integration mit vRealize Automation](#).

Hinweis Es ist ein Problem mit der Zertifikatskette aufgetreten, das davon abgeleitet wird, wie das Python-Element im Infoblox Plug-In SSL-Handshakes verarbeitet. Informationen zum Problem und den notwendigen Aktionen finden Sie im Knowledgebase-Artikel [vRA Cloud-Infoblox-Plug-In löst einen Zertifikatskettenfehler während des Authentifizierungsprozesses aus \(88057\)](#).

Verfahren

- 1 Navigieren Sie zur Seite des Pakets [vRA Cloud Infoblox Plug-In Version 1.1](#) im [VMware Marketplace](#).
- 2 Melden Sie sich an und laden Sie das Plug-In-Paket herunter.
- 3 Wenn Sie dies noch nicht getan haben, fügen Sie die erforderlichen erweiterbaren Eigenschaften in Infoblox hinzu. Weitere Informationen hierzu finden Sie unter [Hinzufügen erforderlicher erweiterbarer Attribute in der Infoblox-Anwendung für die Integration mit vRealize Automation](#).

Ergebnisse

Das Paket steht nun für die Bereitstellung über den Menüpfad **Integrationen > Integration hinzufügen > IPAM > Anbieter verwalten > Paket importieren** zur Verfügung. Siehe hierzu die Beschreibung in [Hinzufügen einer externen IPAM-Integration für Infoblox in vRealize Automation](#).

Erstellen einer Ausführungsumgebung für einen IPAM-Integrationspunkt in vRealize Automation

Bevor Sie einen externen IPAM-Integrationspunkt in vRealize Automation definieren können, müssen Sie eine Ausführungsumgebung erstellen bzw. auf eine vorhandene Ausführungsumgebung zugreifen, die als Vermittler zwischen dem IPAM-Anbieter und vRealize Automation fungiert. Die Ausführungsumgebung ist üblicherweise ein Amazon Web Services- oder Microsoft Azure-Cloud-Konto, das einem lokalen Integrationspunkt mit aktionsbasierter Erweiterbarkeit zugeordnet ist, der wiederum einem Cloud-Erweiterbarkeits-Proxy zugeordnet ist.

Für die externe IPAM-Integration ist eine Ausführungsumgebung erforderlich. Wenn Sie den IPAM-Integrationspunkt definieren, erstellen Sie eine Verbindung zwischen vRealize Automation Cloud Assembly und Ihrem IPAM-Anbieter, indem Sie eine verfügbare Ausführungsumgebung angeben.

Die IPAM-Integration verwendet eine Reihe von heruntergeladenen anbieterspezifischen Skripts oder Plug-Ins in einer Ausführungsumgebung, die von einem FaaS-Anbieter (Feature-as-a-Service) wie z. B. Amazon Web Services Lambda, Microsoft Azure-Funktionen oder einem lokalen eingebetteten Integrationspunkt mit aktionsbasierter Erweiterbarkeit (ABX) bereitgestellt wird. Die Ausführungsumgebung wird zum Herstellen einer Verbindung mit dem externen IPAM-Anbieter verwendet, z. B. Infoblox.

Hinweis Ein IPAM-Integrationspunkt von Infoblox erfordert einen lokalen eingebetteten Integrationspunkt mit aktionsbasierter Erweiterbarkeit.

Jeder Typ von Laufzeitumgebung hat Vor- und Nachteile:

- Integrationspunkt mit aktionsbasierter Erweiterbarkeit (ABX)
 - kostenlos, keine zusätzlichen Kosten für Anbieternutzung
 - kann eine Verbindung zu IPAM-Anbieter-Appliances herstellen, die sich in einem lokalen Datacenter hinter einer NAT/Firewall befinden, das nicht öffentlich zugänglich ist, z. B. Infoblox
 - langsamere und etwas weniger zuverlässige Leistung als kommerzielle Cloud-Anbieter
- Amazon Web Services
 - hat entsprechende Kosten für die Anbieter-FaaS-Verbindung/Nutzung
 - es kann keine Verbindung zu IPAM-Anbieter-Appliances hergestellt werden, die sich in einem lokalen Datacenter hinter einer NAT/Firewall befinden, das nicht öffentlich zugänglich ist
 - schnelle und äußerst zuverlässige Leistung
- Microsoft Azure
 - hat entsprechende Kosten für die Anbieter-FaaS-Verbindung/Nutzung
 - es kann keine Verbindung zu IPAM-Anbieter-Appliances hergestellt werden, die sich in einem lokalen Datacenter hinter einer NAT/Firewall befinden, das nicht öffentlich zugänglich ist
 - schnelle und äußerst zuverlässige Leistung

Voraussetzungen

- Vergewissern Sie sich, dass Sie über Cloud-Administratoranmeldedaten verfügen. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Stellen Sie sicher, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Vergewissern Sie sich, dass Sie über ein Konto beim externen IPAM-Anbieter, z. B. [Infoblox](#) oder [BlueCat](#), und über die korrekten Zugriffsberechtigungen für das Konto Ihrer Organisation beim IPAM-Anbieter verfügen.

- Vergewissern Sie sich, dass Sie auf ein bereitgestelltes Integrationspaket für Ihren IPAM-Anbieter zugreifen können, wie z. B. Infoblox oder BlueCat. Das bereitgestellte Paket wird zunächst als ZIP-Download von Ihrer IPAM-Anbieter-Website oder vom vRealize Automation Cloud Assembly-Marketplace abgerufen und anschließend in vRealize Automation Cloud Assembly bereitgestellt.

Informationen zum Bereitstellen der ZIP-Datei des Anbieterpakets und dessen Verfügbarmachung als Wert für **Anbieter** auf der Seite „IPAM-Integration“ finden Sie unter [Herunterladen und Bereitstellen eines externen IPAM-Anbieterpakets zur Verwendung in vRealize Automation](#).

Verfahren

- 1 Um eine lokale FaaS-basierte Erweiterbarkeitsaktion zu erstellen, die als Ausführungsumgebung der IPAM-Integration verwendet werden soll, wählen Sie **Erweiterbarkeit > Bibliothek > Aktionen** aus.
- 2 Klicken Sie auf **Neue Aktion**, geben Sie einen Aktionsnamen und eine Beschreibung ein und geben Sie ein Projekt an.
- 3 Wählen Sie im Dropdown-Menü **FaaS-Anbieter** die Option **Lokal** aus.
- 4 Füllen Sie das Formular aus, um die Erweiterbarkeitsaktion zu definieren.



Verwandte Informationen zur ausgeführten Umgebung finden Sie im Blog-Video [Infoblox IPAM Plug-in 1.1-Integration](#) ab Minute 24.

Hinzufügen einer externen IPAM-Integration für Infoblox in vRealize Automation

vRealize Automation unterstützt die Integration mit einem externen IPAM-Anbieter. In diesem Beispiel wird Infoblox als externer IPAM-Anbieter verwendet.

Sie können einen anbieterspezifischen IPAM-Integrationspunkt verwenden, um IP-Adressen und zugehörige Netzwerkeigenschaften für Cloud-Vorlagenbereitstellungen abzurufen und zu verwalten.

In diesem Beispiel erstellen Sie einen externen IPAM-Integrationspunkt, um den Zugriff auf das Konto Ihrer Organisation über einen externen IPAM-Anbieter zu unterstützen. In diesem Beispiel-Workflow ist der IPAM-Anbieter Infoblox, und das anbieterspezifische Integrationspaket ist bereits vorhanden. Obwohl diese Anweisungen für eine Infoblox-Integration spezifisch sind, können sie als Referenz verwendet werden, wenn Sie eine IPAM-Integration für einen anderen externen IPAM-Anbieter erstellen.

Sie können ein anbieterspezifisches Integrationspaket von der Website des IPAM-Anbieters, über den [VMware Solution Exchange Marketplace](#) oder, sofern verfügbar, über die vRealize Automation Cloud Assembly-Registerkarte **Marketplace** abrufen.

In diesem Beispiel wird das von VMware bereitgestellte Infoblox-Paket `Infoblox.zip` verwendet, das folgendermaßen über den VMware Solution Exchange Marketplace heruntergeladen werden kann.

- [vRA Cloud Infoblox Plug-In Version 1.1](#) – unterstützt vRealize Automation 8.1 und höher
- [vRA Cloud Infoblox Plug-In Version 1.0](#) – unterstützt vRealize Automation 8.0.1
- [vRA Cloud Infoblox Plug-In Version 0.1](#) – unterstützt vRealize Automation 8.0

Voraussetzungen

- Vergewissern Sie sich, dass Sie über Cloud-Administratoranmeldedaten verfügen. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Stellen Sie sicher, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Stellen Sie sicher, dass Sie über ein Konto beim externen IPAM-Anbieter sowie über die korrekten Zugriffsberechtigungen für das Konto Ihrer Organisation beim IPAM-Anbieter verfügen.

- Vergewissern Sie sich, dass Sie auf ein bereitgestelltes Integrationspaket für Ihren IPAM-Anbieter zugreifen können. Das bereitgestellte Paket wird zunächst als ZIP-Download von der Website Ihres IPAM-Anbieters oder aus dem VMware Solutions Exchange Marketplace abgerufen und anschließend in vRealize Automation bereitgestellt.

Informationen dazu, wie Sie die ZIP-Datei des Anbieterpakets herunterladen und bereitstellen und das Paket als Wert für **Anbieter** auf der Seite „IPAM-Integration“ zur Verfügung stellen, finden Sie unter [Herunterladen und Bereitstellen eines externen IPAM-Anbieterpakets zur Verwendung in vRealize Automation](#).

- Vergewissern Sie sich, dass Sie auf eine konfigurierte Ausführungsumgebung für den IPAM-Anbieter zugreifen können. Bei der Ausführungsumgebung handelt es sich in der Regel um einen lokalen eingebetteten Integrationspunkt mit aktionsbasierter Erweiterbarkeit.

Informationen zu den Merkmalen der Ausführungsumgebung finden Sie unter [Erstellen einer Ausführungsumgebung für einen IPAM-Integrationspunkt in vRealize Automation](#).

- Aktivieren Sie die erforderlichen erweiterbaren Attribute in Ihrer Infoblox-Anwendung. Weitere Informationen hierzu finden Sie unter [Hinzufügen erforderlicher erweiterbarer Attribute in der Infoblox-Anwendung für die Integration mit vRealize Automation](#).
- Wenn Sie nicht über externen Internetzugriff verfügen, können Sie einen Internet-Proxyserver konfigurieren. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Integrieren eines Internet-Proxyservers für vRealize Automation](#).
- Stellen Sie sicher, dass Sie über die erforderlichen Benutzeranmeldedaten für den Zugriff auf und die Nutzung Ihres Infoblox IPAM-Produkts verfügen. Öffnen Sie beispielsweise die Registerkarte „Administration“ in der Infoblox-Appliance und passen Sie die Einträge für Administrator, Gruppen und Rollen an. Sie müssen Mitglied einer Gruppe sein,

die über Administrator- oder Superuser-Berechtigungen verfügt, oder Mitglied einer benutzerdefinierter Gruppe mit DHCP-, DNS-, IPAM- und Rasterberechtigungen. Diese Einstellungen ermöglichen den Zugriff auf alle Funktionen, die im Infoblox-Plug-In verfügbar sind, und ermöglichen es Ihnen, eine Infoblox IPAM-Integration zu erstellen, die von Designern in Cloud-Vorlagen und Bereitstellungen verwendet werden kann. Weitere Informationen zu Benutzerberechtigungen finden Sie in der Produktdokumentation zu Infoblox.

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Integrationen** aus und klicken Sie auf **Integration hinzufügen**.
- 2 Klicken Sie auf **IPAM**.
- 3 Wählen Sie im Dropdown-Menü **Anbieter** ein konfiguriertes IPAM-Anbieterpaket in der Liste aus, z. B. *Infoblox_hrg*.

Wenn die Liste leer ist, klicken Sie auf **Anbieterpaket importieren**, navigieren Sie zur ZIP-Datei eines vorhandenen Anbieterpakets und wählen Sie sie aus. Wenn Sie nicht über die Anbieter-ZIP-Datei verfügen, können Sie sie von der Website Ihres IPAM-Anbieters oder über die Registerkarte **Marketplace** in vRealize Automation Cloud Assembly abrufen.

Informationen zum Bereitstellen der ZIP-Datei des Anbieterpakets in vCenter und als **Anbieter** auf der Seite „Integration“ finden Sie unter [Herunterladen und Bereitstellen eines externen IPAM-Anbieterpakets zur Verwendung in vRealize Automation](#).

Weitere Informationen zum Upgrade einer vorhandenen IPAM-Integration zur Verwendung einer aktuelleren Version des IPAM-Integrationspakets eines Anbieters finden Sie unter [Vorgehensweise zum Upgrade auf ein neueres externes IPAM-Integrationspaket in vRealize Automation](#).

- 4 Geben Sie Ihren Administratorbenutzernamen und das zugehörige Kennwort für Ihr Konto beim externen IPAM-Anbieter sowie die Informationen für alle anderen obligatorischen Felder (sofern vorhanden) ein, z. B. den Hostnamen Ihres Anbieters.

In diesem Beispiel erhalten Sie den Hostnamen Ihres Infoblox-IPAM-Anbieters mit den folgenden Schritten:

- a Melden Sie sich auf einer separaten Browser-Registerkarte mit Ihren Infoblox-Administratoranmeldedaten beim IPAM-Anbieterkonto an.
- b Kopieren Sie die URL des Hostnamens.
- c Fügen Sie die URL des Hostnamens im Feld **Hostname** auf der Seite „IPAM-Integration“ ein.

- 5 Wählen Sie in der Dropdown-Liste **Ausführungsumgebung** einen vorhandenen lokalen Integrationspunkt mit aktionsbasierter Erweiterbarkeit aus, z. B. *Infoblox_abx_intg*.

Die Ausführungsumgebung unterstützt die Kommunikation zwischen vRealize Automation und dem externen IPAM-Anbieter.

Hinweis Wenn Sie ein Amazon Web Services- oder ein Microsoft Azure-Cloud-Konto als Ausführungsumgebung der Integration verwenden, stellen Sie sicher, dass auf die IPAM-Anbieter-Appliance über das Internet zugegriffen werden kann, dass sie sich nicht hinter einer NAT oder Firewall befindet und dass sie einen öffentlich auflösbaren DNS-Namen aufweist. Wenn auf den IPAM-Anbieter nicht zugegriffen werden kann, können die Amazon Web Services-Lambda- oder Microsoft Azure-Funktionen keine Verbindung zu ihm herstellen und die Integration schlägt fehl. Informationen hierzu finden Sie unter [Erstellen einer Ausführungsumgebung für einen IPAM-Integrationspunkt in vRealize Automation](#).

Das IPAM-Framework unterstützt nur eine lokale eingebettete Ausführungsumgebung mit aktionsbasierter Erweiterbarkeit (ABX).

Hinweis Ein IPAM-Integrationspunkt von Infoblox erfordert einen lokalen eingebetteten Integrationspunkt mit aktionsbasierter Erweiterbarkeit.

Das konfigurierte Cloud-Konto bzw. der Integrationspunkt ermöglicht die Kommunikation zwischen vRealize Automation und dem IPAM-Anbieter, in diesem Beispiel Infoblox, über einen zugeordneten Cloud-Erweiterbarkeits-Proxy. Sie können einen bereits erstellten Anbieter auswählen oder einen Anbieter erstellen.

Informationen zum Erstellen einer Ausführungsumgebung finden Sie unter [Erstellen einer Ausführungsumgebung für einen IPAM-Integrationspunkt in vRealize Automation](#).

- 6 Klicken Sie auf **Validieren**.

Da in diesem Beispiel die lokale aktionsbasierte Erweiterbarkeitsintegration für die Ausführungsumgebung verwendet wird, können Sie die Validierungsaktion anzeigen.

- a Klicken Sie auf die Registerkarte **Erweiterbarkeit**.
- b Klicken Sie auf **Aktivität > Aktionsausführungen** und wählen Sie im Filter entweder **Alle Ausführungen** oder **Integrationsausführungen** aus. Sie sehen, dass eine Endpoint-Validierungsaktion initiiert ist und ausgeführt wird.

- 7 Wenn Sie dazu aufgefordert werden, dem selbstsignierten Zertifikat vom IPAM-Anbieter zu vertrauen, klicken Sie auf **Akzeptieren**.

Nachdem Sie das selbstsignierte Zertifikat akzeptiert haben, kann die Validierungsaktion bis zum Abschluss fortgesetzt werden.

- 8 Geben Sie einen **Namen** für diesen IPAM-Integrationspunkt (z. B. *Infoblox_Integration*) und eine **Beschreibung** (z. B. *Infoblox IPAM with ABX integration for team HRG*) ein.

- 9 Klicken Sie auf **Hinzufügen**, um den neuen externen IPAM-Integrationspunkt zu speichern.

Eine Datenerfassungsaktion wird initiiert. Die Daten zu Netzwerken und IP-Bereichen werden vom IPAM-Anbieter erfasst. Sie können die Datenerfassungsaktion folgendermaßen anzeigen:

- a Klicken Sie auf die Registerkarte **Erweiterbarkeit**.
- b Klicken Sie auf **Aktivität > Aktionsausführungen** und beachten Sie, dass eine Datenerfassungsaktion initiiert und ausgeführt wird. Sie können den Inhalt der Aktionsausführung öffnen und anzeigen.

Ergebnisse

Die anbieterspezifische externe IPAM-Integration steht nun zur Verwendung mit Netzwerken und Netzwerkprofilen zur Verfügung.

Konfigurieren eines Netzwerks und Netzwerkprofils zur Verwendung von IPAM (extern) für ein vorhandenes Netzwerk in vRealize Automation

Sie können ein vorhandenes Netzwerk so definieren, dass es IP-Adresswerte verwendet, die von einem externen IPAM-Anbieter anstatt intern von vRealize Automation abgerufen und verwaltet werden.

Sie können ein Netzwerk so definieren, dass es auf vorhandene IP-Einstellungen zugreift, die Sie im externen IPAM-Anbieterkonto Ihrer Organisation definiert haben. Dieser Schritt stellt eine Erweiterung der von Ihnen im vorherigen Schritt erstellten Infoblox-Anbieterintegration dar.

In diesem Beispiel konfigurieren Sie ein Netzwerkprofil mit vorhandenen Netzwerken, deren Daten von vCenter erfasst wurden. Anschließend konfigurieren Sie diese Netzwerke, um IP-Informationen von einem externen IPAM-Anbieter zu erhalten, in diesem Fall Infoblox. Virtuelle Maschinen, die Sie über vRealize Automation bereitstellen und die mit diesem Netzwerkprofil abgeglichen werden können, erhalten Ihre IP-Adresse und andere TCP/IP-bezogene Einstellungen vom externen IPAM-Anbieter.

Weitere Informationen zu Netzwerken finden Sie unter [Netzwerkressourcen in vRealize Automation](#). Weitere Informationen zu Netzwerkprofilen finden Sie unter [Vorgehensweise zum Hinzufügen von Netzwerkprofilen in vRealize Automation](#) und [Weitere Informationen zu Netzwerkprofilen in vRealize Automation](#).

Informationen hierzu finden Sie unter [Vorgehensweise zum Konfigurieren eines Netzwerkprofils zur Unterstützung eines bedarfsgesteuerten Netzwerks für eine externe IPAM-Integration in vRealize Automation](#).

Voraussetzungen

Diese Abfolge von Schritten wird im Kontext eines Workflows für die IPAM-Anbieterintegration angezeigt. Weitere Informationen hierzu finden Sie unter [Lernprogramm: Konfigurieren einer anbieterspezifischen externen IPAM-Integration für vRealize Automation](#).

- Vergewissern Sie sich, dass Sie über Cloud-Administratoranmeldedaten verfügen. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Stellen Sie sicher, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Vergewissern Sie sich, dass Sie über ein Konto beim externen IPAM-Anbieter, z. B. [Infoblox](#) oder [BlueCat](#), und über die korrekten Zugriffsberechtigungen für das Konto Ihrer Organisation beim IPAM-Anbieter verfügen. In diesem Beispiel-Workflow ist der IPAM-Anbieter Infoblox.
- Vergewissern Sie sich, dass Sie über einen IPAM-Integrationspunkt für den IPAM-Anbieter verfügen. Weitere Informationen hierzu finden Sie unter [Hinzufügen einer externen IPAM-Integration für Infoblox in vRealize Automation](#).

Verfahren

- 1 Um ein Netzwerk zu konfigurieren, klicken Sie auf **Infrastruktur > Ressourcen > Netzwerke**.
- 2 Wählen Sie auf der Registerkarte **Netzwerke** ein vorhandenes Netzwerk aus, das mit dem IPAM-Anbieter-Integrationspunkt verwendet werden soll. In diesem Beispiel lautet der Netzwerkname *net.23.117-only-IPAM*.

Die Daten der aufgelisteten Netzwerke wurden von vRealize Automation von einem vCenter in Ihrer Organisation erfasst.

- 3 Um Werte vom externen IPAM-Anbieter abzurufen, stellen Sie sicher, dass außer **Konto/Region**, **Name** und **Netzwerkdomäne** alle anderen Netzwerkeinstellungen leer sind, einschließlich der folgenden:
 - Domäne (siehe Hinweis in Schritt 8)
 - CIDR
 - Standard-Gateway
 - DNS-Server
 - DNS-Suchdomänen
- 4 Klicken Sie auf die Registerkarte **IP-Bereiche** und dann auf **IPAM-IP-Bereich hinzufügen**.
- 5 Wählen Sie im Menü **Netzwerk** das Netzwerk aus, das Sie gerade konfiguriert haben, z. B. *net.23.117-only-IPAM*.
- 6 Wählen Sie im Menü **Anbieter** den IPAM-Integrationspunkt *Infoblox_Integration* aus, den Sie zuvor im Workflow erstellt haben.

- 7 Wählen Sie im jetzt sichtbaren Dropdown-Menü **Adressraum** eine der aufgelisteten Netzwerkansichten aus.

Ein Adressraum in Infoblox wird als Netzwerkansicht bezeichnet.

Die Netzwerkansichten werden von Ihrem IPAM-Anbieterkonto abgerufen. In diesem Beispiel werden das Netzwerk-Subnetz, das Sie gerade konfiguriert haben, z. B. *net.23.117-only-IPAM*, der *Infoblox_Integration*-Integrationspunkt, den Sie zuvor im Workflow erstellt haben, und ein Adressraum mit dem Namen *default* verwendet.

Die aufgelisteten Adressraumwerte werden vom externen IPAM-Anbieter abgerufen.

- 8 Wählen Sie aus der Liste der angezeigten Netzwerke, die für den ausgewählten Adressraum verfügbar sind, ein oder mehrere Netzwerke aus. Wählen Sie beispielsweise 10.23.117.0/24 aus.

In diesem Beispiel enthalten die Spaltenwerte von **Domänen** und **DNS-Server** für das ausgewählte Netzwerk Werte aus Infoblox.

Hinweis Wenn Sie in Schritt 3 ein Netzwerk auswählen, für das eine Domäne für vRealize Automation angegeben wurde, und dann ein Netzwerk aus dem Adressraum des externen IPAM-Anbieters auswählen, der einen Domänenwert enthält, hat der Domänenwert im externen IPAM-Anbietwork Netzwerk Vorrang vor der in vRealize Automation angegebenen Domäne. Wenn die Einstellung für den IPAM-IP-Bereich keinen Domänenwert aufweist, der wie oben beschrieben entweder in Cloud Assembly oder im externen IPAM-Anbieter angegeben ist, schlägt die Bereitstellung fehl.

Für Infoblox können Sie die Blueprint-Eigenschaft `Infoblox.IPAM.Network.dnsSuffix` auf der Maschinenebene verwenden, um den Domänenwert zu überschreiben. Informationen hierzu finden Sie unter [Verwenden Infoblox-spezifischer Eigenschaften und erweiterbarer Attribute für IPAM-Integrationen in vRealize Automation](#).

- 9 Klicken Sie auf **Hinzufügen**, um den IPAM-IP-Bereich für das Netzwerk zu speichern.
Der Bereich wird in der Tabelle **IP-Bereiche** angezeigt.
- 10 Klicken Sie auf die Registerkarte **IP-Adressen**.
Nachdem Sie eine Maschine mithilfe des neuen Adressbereichs des externen IPAM-Anbieters bereitgestellt haben, wird ein neuer Datensatz in der Tabelle **IP-Adressen** angezeigt.
- 11 Um ein Netzwerkprofil für die Verwendung des Netzwerks zu konfigurieren, klicken Sie auf **Infrastruktur > Konfigurieren > Netzwerkprofile**.
- 12 Benennen Sie das Netzwerkprofil, z. B. als *Infoblox-NP*, und fügen Sie die folgenden Beispieleinstellungen hinzu.
 - Registerkarte „Übersicht“
 - Geben Sie ein/eine vSphere-Cloud-Konto/-Region an.
 - Fügen Sie ein Funktions-Tag für das Netzwerkprofil hinzu, z. B. mit dem Namen *infoblox_abx*.

Notieren Sie sich das Funktions-Tag, da Sie es auch als Einschränkungs-Tag der Cloud-Vorlage verwenden müssen, um die Bereitstellungszuordnung in der Cloud-Vorlage einzurichten.

- Registerkarte „Netzwerke“
 - Fügen Sie das zuvor erstellte Netzwerk hinzu, beispielsweise *net.23.117-only-IPAM*.

13 Klicken Sie auf **Speichern**, um das Netzwerkprofil mit diesen Einstellungen zu speichern.

Ergebnisse

Die Netzwerk- und Netzwerkprofileinstellungen werden nun für einen vorhandenen Netzwerktyp konfiguriert, der für die Infoblox IPAM-Integration in einem Cloud-Vorlagen-Design verwendet wird.

Definieren und Bereitstellen einer Cloud-Vorlage, die die Bereichszuweisung eines externen IPAM-Anbieters in vRealize Automation verwendet

Sie können eine Cloud-Vorlage definieren, um die IP-Adresszuweisungen des externen IPAM-Anbieters abzurufen und zu verwalten. In diesem Beispiel wird Infoblox als externer IPAM-Anbieter verwendet.

In diesem letzten Schritt im Workflow zur externen IPAM-Integration definieren Sie eine Cloud-Vorlage und stellen sie bereit, die Ihr zuvor definiertes Netzwerk und Netzwerkprofil mit dem Infoblox-Konto Ihrer Organisation verbindet, um IP-Adresszuweisungen für bereitgestellte VMs aus dem externen IPAM-Anbieter anstatt aus vRealize Automation Cloud Assembly abzurufen und zu verwalten.

Dieser Workflow verwendet Infoblox als externen IPAM-Anbieter, und in einigen Schritten gelten die Beispielwerte nur für Infoblox. Es besteht aber die Absicht, dass der Vorgang auf andere externe IPAM-Integrationen angewendet werden kann.



Im Infoblox-Blog [IPAM und DNS für VMs mithilfe von VMware vRealize Automation und Infoblox DDI automatisieren](#) werden verwandte Informationen bereitgestellt.

Nachdem Sie die Cloud-Vorlage bereitgestellt haben und die virtuelle Maschine gestartet wurde, wird die für jede VM in der Bereitstellung verwendete IP-Adresse als Netzwerkeintrag auf der Seite **Ressourcen > Netzwerke**, als neuer Hostdatensatz im IPAM-Anbieternetzwerk im Konto Ihres IPAM-Anbieters und im vSphere Web Client-Datensatz für jede bereitgestellte VM im Host-vCenter angezeigt.

Voraussetzungen

Diese Abfolge von Schritten wird im Kontext eines Workflows für die Integration eines externen IPAM-Anbieters gezeigt. Weitere Informationen hierzu finden Sie unter [Lernprogramm: Konfigurieren einer anbieterspezifischen externen IPAM-Integration für vRealize Automation](#).

- Vergewissern Sie sich, dass Sie über Cloud-Administratoranmeldedaten verfügen. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Stellen Sie sicher, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Vergewissern Sie sich, dass Sie über ein Konto beim externen IPAM-Anbieter, z. B. Infoblox oder BlueCat, und über die korrekten Zugriffsberechtigungen für das Konto Ihrer Organisation beim IPAM-Anbieter verfügen.
- Vergewissern Sie sich, dass Sie über Administratorzugriff auf das Hostkonto und alle Rollenanforderungen verfügen, die zum Anzeigen von Statusdatensätzen im vSphere Web Client-Datensatz für Ihre bereitgestellten VMs auf dem Host vCenter erforderlich sind.
- Stellen Sie sicher, dass Sie über einen IPAM-Integrationspunkt für den externen IPAM-Anbieter verfügen. Weitere Informationen hierzu finden Sie unter [Hinzufügen einer externen IPAM-Integration für Infoblox in vRealize Automation](#).
- Vergewissern Sie sich, dass Sie ein vRealize Automation Cloud Assembly-Netzwerk und -Netzwerkprofil konfiguriert haben, das die externe IPAM-Integration für Ihren geplanten IPAM-Integrationspunkt unterstützt. Weitere Informationen hierzu finden Sie unter [Konfigurieren eines Netzwerks und Netzwerkprofils zur Verwendung von IPAM \(extern\) für ein vorhandenes Netzwerk in vRealize Automation](#).
- Vergewissern Sie sich, dass das Projekt und die Cloud-Zone übereinstimmend mit den Tags im IPAM-Integrationspunkt und im Netzwerk oder Netzwerkprofil getaggt sind. Konfigurieren Sie optional das Projekt so, dass es die benutzerdefinierte Ressourcenbenennung unterstützt.

Weitere Informationen zur Rolle eines Projekts und einer Cloud-Zone sowie zur Rolle anderer Infrastrukturelemente in Ihrer Cloud-Vorlage finden Sie unter [Lernprogramm: Einrichten und Testen einer Multi-Cloud-Infrastruktur und von Bereitstellungen in vRealize Automation Cloud Assembly](#). Weitere Informationen zum Tagging finden Sie unter [Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen](#).

Informationen zur benutzerdefinierten Benennung von VMs mithilfe von Einstellungen in Ihrem Projekt finden Sie unter [Vorgehensweise zum Anpassen der Namen bereitgestellter Ressourcen mithilfe von vRealize Automation Cloud Assembly](#).

Verfahren

- 1 Klicken Sie auf **Cloud-Vorlagen > Neu**, geben Sie die folgenden Informationen auf der Seite **Neue Cloud-Vorlage** ein und klicken Sie auf **Erstellen**.
 - **Name** = ipam-bpa
 - **Beschreibung** = Cloud-Vorlage, die die Infoblox IPAM-Integration verwendet
 - **Projekt** = 123VC
- 2 Fügen Sie in diesem Beispiel eine Cloud-unabhängige Maschinenkomponente und eine Cloud-unabhängige Netzwerkkomponente zur Arbeitsfläche der Cloud-Vorlage hinzu und verbinden Sie die beiden Komponenten.
- 3 Bearbeiten Sie den Code der Cloud-Vorlage, um der Netzwerkkomponente ein Einschränkungs-Tag hinzuzufügen, das mit dem Funktions-Tag übereinstimmt, das Sie dem Netzwerkprofil hinzugefügt haben. In diesem Beispiel lautet der Tag-Wert *infoblox_abx*.
- 4 Bearbeiten Sie den Code der Cloud-Vorlage, um anzugeben, dass der Netzwerkzuweisungstyp *static* lautet.

Bei Verwendung eines externen IPAM-Anbieters ist die Einstellung `assignment: static` erforderlich.

In diesem Beispiel wird als bekannt vorausgesetzt, dass die angegebene IP-Adresse 10.23.117.4 derzeit im externen IPAM-Adressraum, den wir für das Netzwerk im zugeordneten Netzwerkprofil ausgewählt haben, verfügbar ist. Obwohl die Einstellung `assignment: static` erforderlich ist, ist die Einstellung `address: value` nicht erforderlich. Sie können wählen, ob die Auswahl externer IP-Adressen mit einem bestimmten Adresswert beginnen soll, aber dies ist nicht erforderlich. Wenn Sie keine Einstellung für `address: value` angeben, wählt der externe IPAM-Anbieter die nächste verfügbare Adresse im externen IPAM-Netzwerk aus.

- 5 Überprüfen Sie den Code der Cloud-Vorlage anhand des folgenden Beispiels.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: existing
      name: ipam
      constraints:
        - tag: infoblox_abx
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: ubuntu
      flavor: small
      networks:
```



```
- network: '${resource.Cloud_Network_1.id}'
  assignment: static
  address: 10.23.117.4
  name: '${resource.Cloud_Network_1.name}'
```

Beispiele für Infoblox-Eigenschaften, die zur Angabe von DNS- und DHCP-Einstellungen in Cloud-Vorlagen zur Verfügung stehen, finden Sie unter [Verwenden Infoblox-spezifischer Eigenschaften und erweiterbarer Attribute für IPAM-Integrationen in vRealize Automation](#).

- 6 Klicken Sie auf der Cloud-Vorlagenseite auf **Bereitstellen**, geben Sie der Bereitstellung den Namen *Infoblox-1* und klicken Sie auf **Bereitstellen** auf der Seite **Bereitstellungstyp**.
- 7 Klicken Sie bei der Bereitstellung der Cloud-Vorlage auf die Registerkarte **Erweiterbarkeit** und wählen Sie **Aktivität > Aktionsausführungen** aus, um die derzeit ausgeführte *Infoblox_AllocateIP_n*-Erweiterbarkeitsaktion anzuzeigen.

Nachdem die Erweiterbarkeitsaktion abgeschlossen ist und die Maschine bereitgestellt wurde, wird die MAC-Adresse von der Aktion *Infoblox_Update_n* an Infoblox weitergegeben.

- 8 Sie können sich bei Ihrem Infoblox-Konto anmelden und das Konto öffnen, um den neuen Hosteintrag für die IPAM-Adresse im zugehörigen Netzwerk 10.23.117.0/24 anzuzeigen. Sie können auch die Registerkarte „DNS“ in Infoblox öffnen, um den neuen DNS-Hostdatensatz anzuzeigen.
- 9 Um zu überprüfen, ob die VM bereitgestellt wird, melden Sie sich bei Ihrem Host-vCenter und vSphere Web Client an, um die bereitgestellte Maschine zu finden und den DNS-Namen und die IP-Adresse anzuzeigen.

Nach dem Starten der bereitgestellten virtuellen Maschine wird die MAC-Adresse durch eine *Infoblox_AllocateIP*-Erweiterbarkeitsaktion an Infoblox weitergegeben.

- 10 Um den neuen Netzwerkdatensatz in vRealize Automation Cloud Assembly anzuzeigen, wählen Sie **Infrastruktur > Ressourcen > Netzwerke** aus und klicken Sie, um die Registerkarte **IP-Adressen** zu öffnen.
- 11 Wenn Sie die Bereitstellung löschen, wird die IPAM-Adresse der VMs in der Bereitstellung freigegeben, und die IP-Adressen stehen dem externen IPAM-Anbieter für andere Zuteilungen erneut zur Verfügung. Die Erweiterbarkeitsaktion für dieses Ereignis in vRealize Automation Cloud Assembly lautet *Infoblox_Deallocate*.

Verwenden Infoblox-spezifischer Eigenschaften und erweiterbarer Attribute für IPAM-Integrationen in vRealize Automation

Sie können für vRealize Automation-Projekte, die externe IPAM-Integrationen für Infoblox enthalten, Infoblox-spezifische Eigenschaften verwenden.

Die folgenden Infoblox-Eigenschaften stehen zur Verwendung mit Infoblox IPAM-Integrationen in den Cloud-Vorlagen-Designs und Bereitstellungen zur Verfügung. Sie können sie in vRealize Automation verwenden, um die Zuteilung der IP-Adressen während der Cloud-Vorlagenbereitstellung weiter zu steuern. Die Verwendung dieser Eigenschaften ist optional.

- `Infoblox.IPAM.createFixedAddress`

Diese Eigenschaft ermöglicht es Ihnen, einen festen Adressdatensatz in Infoblox zu erstellen. Mögliche Werte sind „True“ und „False“. Standardmäßig wird ein Hostdatensatz erstellt. Der Standardwert lautet „False“.

- `Infoblox.IPAM.Network.dnsView`

Mit dieser Eigenschaft können Sie eine DNS-Ansicht beim Erstellen eines Hostdatensatzes in Infoblox verwenden.

- `Infoblox.IPAM.Network.enableDns`

Wenn Sie eine IP in Infoblox zuweisen, können Sie mit dieser Eigenschaft auch einen DNS-Datensatz erstellen. Mögliche Werte sind „True“ und „False“. Der Standardwert lautet „True“.

- `Infoblox.IPAM.Network.enableDhcp`

Sie können diese Option auf „True“ festlegen, um die DHCP-Konfiguration für die Hostadresse zu aktivieren.

- `Infoblox.IPAM.Network.dnsSuffix`

Mit dieser Eigenschaft können Sie die DHCP-Option *domain* eines Infoblox-Netzwerks mit einer neuen überschreiben. Diese Funktion ist nützlich, wenn für das Infoblox-Netzwerk die DHCP-Option *domain* nicht festgelegt ist oder wenn die DHCP-Option *domain* überschrieben werden muss. Der Standardwert lautet NULL (leere Zeichenfolge).

`Infoblox.IPAM.Network.dnsSuffix` ist nur anwendbar, wenn `Infoblox.IPAM.Network.enableDns` auf „True“ festgelegt ist.

Sie können eine Infoblox-Eigenschaft mithilfe einer der folgenden Methoden in vRealize Automation Cloud Assembly angeben:

- Sie können Eigenschaften in einem Projekt mithilfe des Abschnitts **Benutzerdefinierte Eigenschaften** auf der Seite **Infrastruktur > Verwaltung > Projekte** angeben. Mit dieser Methode werden die angegebenen Eigenschaften auf alle Maschinen angewendet, die im Rahmen dieses Projekts bereitgestellt werden.
- Sie können die Eigenschaften für jede Maschinenkomponente in einer Cloud-Vorlage angeben. Der folgende Beispielcode der Cloud-Vorlage veranschaulicht die Verwendung der `Infoblox.IPAM.Network.dnsView`-Eigenschaft:

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
```

```

properties:
  Infoblox.IPAM.Network.dnsView: default
  image: ubuntu
  cpuCount: 1
  totalMemoryMB: 1024
  networks:
    - network: '${resource.Cloud_Network_1.id}'
Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkType: existing
    constraints:
      - tag: mk-ipam-demo

```

- Sie können Eigenschaften mithilfe eines Erweiterbarkeitsabonnements angeben.

Verwandte Informationen zu den erweiterbaren Infoblox-Attributen in Bezug auf diesen Anwendungsfall finden Sie unter [Hinzufügen erforderlicher erweiterbarer Attribute in der Infoblox-Anwendung für die Integration mit vRealize Automation](#).

Verwenden von Infoblox-Eigenschaften auf verschiedenen Maschinennetzwerkkarten in einer Cloud-Vorlage

Die folgenden Infoblox-Eigenschaften können für jede Maschinennetzwerkkarte in der Cloud-Vorlage einen anderen Wert aufweisen:

- Infoblox.IPAM.Network.enableDhcp
- Infoblox.IPAM.Network.dnsView
- Infoblox.IPAM.Network.enableDns

Beispiel: Zur Verwendung eines anderen `Infoblox.IPAM.Network.dnsView`-Werts für jede Netzwerkkarte (NIC) verwenden Sie einen `Infoblox.IPAM.Network<nicIndex>.dnsView`-Eintrag für jede NIC. Das folgende Beispiel zeigt verschiedene `Infoblox.IPAM.Network.dnsView`-Werte für zwei Netzwerkkarten.

```

formatVersion: 1
inputs: {}
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      Infoblox.IPAM.Network0.dnsView: default
      Infoblox.IPAM.Network1.dnsView: my-net
      image: ubuntu
      flavor: small
      networks:
        - network: '${resource.Cloud_Network_1.id}'
          deviceIndex: 0
        - network: '${resource.Cloud_Network_2.id}'
          deviceIndex: 1
  Cloud_Network_1:
    type: Cloud.Network

```

```

properties:
  networkType: existing
Cloud_Network_2:
  type: Cloud.Network
  properties:
    networkType: existing

```

Standardmäßig erstellt die Infoblox-Integration einen DNS-Host-Datensatz in der *standardmäßigen* DNS-Ansicht in Infoblox. Wenn Ihr Infoblox-Administrator *benutzerdefinierte* DNS-Ansichten erstellt hat, können Sie das Standardintegrationsverhalten überschreiben und mithilfe der Eigenschaft `Infoblox.IPAM.Network.dnsView` in der Maschinenkomponente eine benannte Ansicht angeben. Sie können der Komponente `Cloud_Machine_1` beispielsweise die folgende Eigenschaft hinzufügen, um eine benannte DNS-Ansicht in Infoblox anzugeben.

```

Cloud_Machine_1:
  type: Cloud.Machine
  properties:
    image: ubuntu
    flavor: small
    Infoblox.IPAM.Network.dnsView:<dns-view-name>

```

Informationen zum Konfigurieren und Verwenden von DNS-Ansichten finden Sie unter [DNS-Ansichten](#) in der Infoblox-Produktdokumentation. Beispiele für den Workflow „Infoblox-Integration“ finden Sie unter [Definieren und Bereitstellen einer Cloud-Vorlage, die die Bereichszuweisung eines externen IPAM-Anbieters in vRealize Automation verwendet](#).

Einrichten von vRealize Automation Cloud Assembly für Ihre Organisation

3

Als Cloud Assembly-Administrator müssen Sie die Benutzerrollen verstehen und Verbindungen mit dem Cloud-Kontoanbieter und den Integrationsanwendungen einrichten.

Bei der Konfiguration der Cloud-Konten und -Integrationen richten Sie die Kommunikation zwischen Cloud Assembly und diesen Zielsystemen ein.

Dieses Kapitel enthält die folgenden Themen:

- [Definition der vRealize Automation-Benutzerrollen](#)
- [Hinzufügen von Cloud-Konten zu vRealize Automation Cloud Assembly](#)
- [Integrieren von vRealize Automation mit anderen Anwendungen](#)
- [Definition von Onboarding-Plänen in vRealize Automation Cloud Assembly](#)
- [Erweiterte Konfiguration für vRealize Automation Cloud Assembly-Umgebung](#)

Definition der vRealize Automation-Benutzerrollen

vRealize Automation hat mehrere Benutzerrollenebenen. Diese unterschiedlichen Ebenen steuern den Zugriff auf die Organisation, Dienste, Projekte, die die Cloud-Vorlagen erzeugen oder verbrauchen, Katalogelemente und Pipelines. Daneben steuern sie die Möglichkeit der Benutzer, bestimmte Teile der Benutzeroberfläche zu verwenden oder anzuzeigen. Mit diesen unterschiedlichen Ebenen verfügen Cloud-Administratoren über verschiedene Tools zum Anwenden der Granularitätsebene, die aufgrund der operativen Anforderungen benötigt wird.

Allgemeine Rollenbeschreibungen

Die Benutzerrollen werden auf verschiedenen Ebenen definiert. Die Rollen auf Dienstebene werden für jeden Dienst definiert.

Weitere Details zu den Dienstrollen sind unter der folgenden Tabelle aufgeführt.

Rolle	Allgemeine Berechtigungen	Ort, an dem die Rolle definiert wird
Organisationsbesitzer	<p>Kann auf die Konsole zugreifen und der Organisation Benutzer hinzufügen.</p> <p>Der Organisationsbesitzer kann nur dann auf einen Dienst zugreifen, wenn er über eine Dienstrolle verfügt.</p> <p>Weitere Informationen zu den Organisationsbenutzerrollen</p>	Organisationskonsole
Organisationsmitglied	<p>Kann auf die Konsole zugreifen.</p> <p>Das Organisationsmitglied kann nur dann auf einen Dienst zugreifen, wenn es über eine Dienstrolle verfügt.</p> <p>Weitere Informationen zu den Organisationsbenutzerrollen</p>	Organisationskonsole
Dienstadministrator	<p>Kann auf die Konsole zugreifen und verfügt im Dienst über umfassende Rechte zum Anzeigen, Aktualisieren und Löschen.</p> <ul style="list-style-type: none"> ■ Cloud Assembly-Dienstrollen ■ Service Broker-Dienstrollen ■ Code Stream-Dienstrollen 	Organisationskonsole
Dienstbenutzer	<p>Kann mit begrenzten Berechtigungen auf die Konsole und den Dienst zugreifen.</p> <p>Das Dienstmitglied verfügt über eine eingeschränkte Benutzeroberfläche. Was genau es anzeigen oder welche Aktionen es ausführen kann, hängt von seiner Projektmitgliedschaft ab.</p> <ul style="list-style-type: none"> ■ Cloud Assembly-Dienstrollen ■ Service Broker-Dienstrollen ■ Code Stream-Dienstrollen 	Organisationskonsole
Dienst-Viewer	<p>Kann auf die Konsole und den Dienst im schreibgeschützten Modus zugreifen.</p> <ul style="list-style-type: none"> ■ Cloud Assembly-Dienstrollen ■ Service Broker-Dienstrollen ■ Code Stream-Dienstrollen 	Organisationskonsole
Executor (nur vRealize Automation Code Stream)	<p>Kann auf die Konsole zugreifen und Pipeline-Ausführungen verwalten.</p> <p>Code Stream-Dienstrollen</p>	Organisationskonsole

Rolle	Allgemeine Berechtigungen	Ort, an dem die Rolle definiert wird
vRA Migration Assistant-Administrator	Kann auf die Konsole zugreifen und verfügt in vRA Migration Assistant und Cloud Assembly über umfassende Rechte zum Anzeigen, Aktualisieren und Löschen. Diese Rolle muss zusätzlich die Rolle „Cloud Assembly-Viewer“ aufweisen.	Organisationskonsole
vRA Migration Assistant-Viewer	Sie können im schreibgeschützten Modus auf die Konsole, vRA Migration Assistant und Cloud Assembly zugreifen. Diese Rolle muss zusätzlich die Rolle „Cloud Assembly-Viewer“ aufweisen.	Organisationskonsole
Orchestrator-Administrator	Kann auf alle vRealize Orchestrator Client-Funktionen und -Inhalte zugreifen, einschließlich der von bestimmten Gruppen erstellten Inhalte.	Organisationskonsole und vRealize Orchestrator Client
Orchestrator-Workflow-Designer	Kann eigene vRealize Orchestrator Client-Inhalte erstellen, ausführen, bearbeiten und löschen. Kann eigene Inhalte zur zugewiesenen Gruppe hinzufügen. Hat keinen Zugriff auf die Verwaltungs- und Fehlerbehebungsfunktionen des vRealize Orchestrator Client.	Organisationskonsole und vRealize Orchestrator Client
Projekttrollen	Kann abhängig von der Projekttrolle Projektressourcen anzeigen und verwalten. Zu den Projekttrollen gehören Administrator, Mitglied und Viewer. Organisations- und Dienstbenutzerrollen in vRealize Automation	vRealize Automation Cloud Assembly, vRealize Automation Service Broker und vRealize Automation Code Stream
Benutzerdefinierte Rollen	Die Berechtigungen werden von vRealize Automation Cloud Assembly für alle Dienste definiert. Der Benutzer muss mindestens über eine Dienst-Viewer-Rolle im jeweiligen Dienst verfügen, um auf den Dienst zugreifen zu können. Die benutzerdefinierten Rollen haben Vorrang vor den Dienstrollen. Benutzerdefinierte Benutzerrollen in vRealize Automation	vRealize Automation Cloud Assembly und vRealize Automation Service Broker

Organisations- und Dienstbenutzerrollen in vRealize Automation

Die Rollen für Organisations- und Dienstbenutzer, die für die Dienste vRealize Automation Cloud Assembly, vRealize Automation Service Broker und vRealize Automation Code Stream definiert sind, bestimmen, was dem Benutzer in den einzelnen Diensten angezeigt wird und welche Aktionen er jeweils ausführen kann.

Organisationsbenutzerrollen

Benutzerrollen werden von einem Organisationsbesitzer für die Organisation in der vRealize Automation-Konsole definiert. Es gibt zwei Arten von Rollen: Organisationsrollen und Dienstrollen.

Die Organisationsrollen sind global und gelten für alle Dienste in der Organisation. Die Rollen auf Organisationsebene sind die Rolle des Organisationsbesitzers oder des Organisationsmitglieds.

Weitere Informationen zu den Organisationsrollen finden Sie unter [Verwalten von vRealize Automation](#).

Die vRealize Automation Cloud Assembly-Dienstrollen, die dienstspezifische Berechtigungen sind, werden auch auf Organisationsebene in der Konsole zugewiesen.

Dienstrollen

Diese Rollen werden vom Organisationsbesitzer zugewiesen.

Dieser Artikel enthält Informationen zu allen drei Diensten.

- [Cloud Assembly-Dienstrollen](#)
- [Service Broker-Dienstrollen](#)
- [Code Stream-Dienstrollen](#)

Cloud Assembly-Dienstrollen

Über die vRealize Automation Cloud Assembly-Dienstrolle wird festgelegt, was Benutzern in vRealize Automation Cloud Assembly angezeigt wird und welche Aufgaben sie ausführen können. Diese Dienstrollen werden in der Konsole von einem Organisationsbesitzer definiert.

Tabelle 3-1. Beschreibungen der vRealize Automation Cloud Assembly-Dienstrollen

Rolle	Beschreibung
Cloud Assembly-Administrator	Ein Benutzer, der über Lese- und Schreibzugriff auf die gesamte Benutzeroberfläche und die API-Ressourcen verfügt. Dies ist die einzige Benutzerrolle, mit alles angezeigt und durchgeführt werden kann, einschließlich Cloud-Konten hinzufügen, neue Projekte erstellen und einen Projektadministrator zuweisen.
Cloud Assembly-Benutzer	Ein Benutzer, der nicht über die Rolle des Cloud Assembly-Administrators verfügt. In einem vRealize Automation Cloud Assembly-Projekt fügt der Administrator Projekten Benutzer als Projektmitglieder, -administratoren oder -Viewer hinzu. Der Administrator kann auch einen Projektadministrator hinzufügen.
Cloud Assembly-Viewer	Ein Benutzer, der Lesezugriff zum Anzeigen von Informationen hat, Werte jedoch nicht erstellen, aktualisieren oder löschen kann. Dies ist eine Rolle, die für alle Projekte nur über Leserechte verfügt. Benutzer mit der Rolle „Viewer“ können alle für den Administrator verfügbaren Informationen anzeigen. Er kann keine Aktionen ausführen, es sei denn, er wird zu einem Projektadministrator oder Projektmitglied gemacht. Wenn der Benutzer zu einem Projekt gehört, verfügt er über die Berechtigungen, die mit dieser Rolle verbunden sind. Der Projekt-Viewer erweitert seine Berechtigungen nicht in der Weise, wie dies bei den Rollen „Projektadministrator“ oder „Projektmitglied“ der Fall ist.

Zusätzlich zu den Dienstrollen verfügt vRealize Automation Cloud Assembly über Projektrollen. Jedes Projekt ist in allen Diensten verfügbar.

Die Projektrollen sind in vRealize Automation Cloud Assembly definiert und können zwischen Projekten variieren.

Beachten Sie in den folgenden Tabellen, in denen die Berechtigungen der verschiedenen Dienst- und Projektrollen beschrieben werden, dass die Dienstadministratoren über Vollzugriff auf alle Bereiche der Benutzeroberfläche verfügen.

Die Beschreibungen der Projektrollen helfen Ihnen bei der Entscheidung, welche Berechtigungen Sie Ihren Benutzern erteilen möchten.

- Projektadministratoren nutzen die vom Dienstadministrator erstellte Infrastruktur, um sicherzustellen, dass die Projektmitglieder über die Ressourcen verfügen, die sie für ihre Entwicklungsarbeit benötigen.
- Projektmitglieder arbeiten im Rahmen ihrer Projekte daran, Cloud-Vorlagen zu entwerfen und bereitzustellen.
- Projekt-Viewer weisen lediglich Lesezugriff auf, außer in einigen Fällen, in denen sie nicht zerstörerische Vorgänge wie das Herunterladen von Cloud-Vorlagen durchführen können.

Tabelle 3-2. vRealize Automation Cloud Assembly-Dienstrollen und -Projektrollen

UI-Kontext	Aufgabe	Cloud Assembly- Administrator	Cloud Assembly- Viewer	Cloud Assembly-Benutzer	
				Der Benutzer muss ein Projektadministrationsmitglied sein, um projektbezogene Aufgaben anzeigen und durchführen zu können.	
				Projektadministrator	Projektmitglied
Zugriff auf Cloud Assembly					
Konsole	In der vRA-Konsole können Sie Cloud Assembly anzeigen und öffnen	Ja	Ja	Ja	Ja
Infrastruktur					
	Die Registerkarte „Infrastruktur“ anzeigen und öffnen	Ja	Ja	Ja	Ja
Konfigurieren – Projekte	Projekte erstellen	Ja			
	Werte aus der Projektübersicht, aus Bereitstellungen, Kubernetes und Integrationen aktualisieren oder löschen und Projektkonfigurationen testen.	Ja			
	Benutzer und Gruppen hinzufügen und Rollen in Projekten zuweisen.	Ja		Ja. Ihre Projekte.	
	Projekte anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Konfigurieren – Cloud-Zonen	Cloud-Zonen erstellen, aktualisieren oder löschen	Ja			
	Cloud-Zonen anzeigen	Ja	Ja		
Konfigurieren – Kubernetes-Zonen	Kubernetes-Zonen erstellen, aktualisieren oder löschen	Ja			
	Kubernetes-Zonen anzeigen	Ja	Ja		
Konfigurieren – Konfigurationen	Konfigurationen erstellen, aktualisieren oder löschen	Ja			
	Konfigurationen anzeigen	Ja	Ja		
Konfigurieren – Image-Zuordnungen	Image-Zuordnungen erstellen, aktualisieren oder löschen	Ja			
	Image-Zuordnungen anzeigen	Ja	Ja		
Konfigurieren – Netzwerkprofile	Netzwerkprofile erstellen, aktualisieren oder löschen	Ja			
	Image-Netzwerkprofile anzeigen	Ja	Ja		
Konfigurieren – Speicherprofile	Speicherprofile erstellen, aktualisieren oder löschen	Ja			

Tabelle 3-2. vRealize Automation Cloud Assembly-Dienstrollen und -Projektrollen (Fortsetzung)

UI-Kontext	Aufgabe	Cloud Assembly-Administrator	Cloud Assembly-Viewer	Cloud Assembly-Benutzer Der Benutzer muss ein Projektadministrationsmitglied sein, um projektbezogene Aufgaben anzeigen und durchführen zu können.	
				Projektadministrator	Projektmitglied
	Image-Speicherprofile anzeigen	Ja	Ja		
Konfigurieren – Preisgestaltungskarten	Preisgestaltungskarten erstellen, aktualisieren oder löschen	Ja			
	Preisgestaltungskarten anzeigen	Ja	Ja		
Konfigurieren – Tags	Tags erstellen, aktualisieren oder löschen	Ja			
	Tags anzeigen	Ja	Ja		
Ressourcen – Computing	Erkannten Computing-Ressourcen Tags hinzufügen	Ja			
	Erkannte Computing-Ressourcen anzeigen	Ja	Ja		
Ressourcen – Netzwerke	Netzwerktag, IP-Bereiche, IP-Adresse ändern	Ja			
	Erkannte Netzwerkressourcen anzeigen	Ja	Ja		
Ressourcen – Sicherheit	Tags zu erkannten Sicherheitsgruppen hinzufügen	Ja			
	Erkannte Sicherheitsgruppen anzeigen	Ja	Ja		
Ressourcen – Speicher	Tags zu erfasstem Speicher	Ja			
	Speicher anzeigen	Ja	Ja		
Ressourcen – Maschinen	Maschinen hinzufügen und löschen	Ja			
	Maschinen anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Ressourcen – Volumes	Erkannte Speicher-Volumes löschen	Ja			
	Erkannte Speicher-Volumes anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Ressourcen – Kubernetes	Kubernetes-Cluster bereitstellen oder hinzufügen und Namespace erstellen oder hinzufügen	Ja			
	Kubernetes-Cluster und Namespaces anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte

Tabelle 3-2. vRealize Automation Cloud Assembly-Dienstrollen und -Projektrollen (Fortsetzung)

UI-Kontext	Aufgabe	Cloud Assembly-Administrator	Cloud Assembly-Viewer	Cloud Assembly-Benutzer Der Benutzer muss ein Projektadministrationsmitglied sein, um projektbezogene Aufgaben anzeigen und durchführen zu können.	
				Projektadministrator	Projektmitglied
Aktivität – Anforderungen	Datensätze der Bereitstellungsanforderung löschen	Ja			
	Datensätze der Bereitstellungsanforderung anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Aktivität – Ereignisprotokolle	Ereignisprotokolle anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Verbindungen – Cloud-Konten	Cloud-Konten erstellen, aktualisieren oder löschen	Ja			
	Cloud-Konten anzeigen	Ja	Ja		
Verbindungen – Integrationen	Integrationen erstellen, aktualisieren oder löschen	Ja			
	Integrationen anzeigen	Ja	Ja		
Onboarding	Onboarding-Pläne erstellen, aktualisieren oder löschen	Ja			
	Onboarding-Pläne anzeigen	Ja	Ja		
Marketplace					
	Die Registerkarte „Download-Center“ anzeigen und öffnen	Ja	Ja		
	Die heruntergeladenen Cloud-Vorlagen auf der Registerkarte „Design“ verwenden	Ja		Ja. Wenn sie mit Ihren Projekten verknüpft sind.	Ja. Wenn sie mit Ihren Projekten verknüpft sind.
Marketplace – Cloud-Vorlagen	Cloud-Vorlage herunterladen	Ja			
	Cloud-Vorlagen anzeigen	Ja	Ja		
Download-Center – Images	Images herunterladen	Ja			
	Images anzeigen	Ja	Ja		
Download-Center – Downloads	Protokoll aller heruntergeladenen Elemente anzeigen	Ja	Ja		
Erweiterbarkeit					
	Die Registerkarte „Erweiterbarkeit“ anzeigen und öffnen	Ja	Ja		

Tabelle 3-2. vRealize Automation Cloud Assembly-Dienstrollen und -Projektrollen (Fortsetzung)

UI-Kontext	Aufgabe	Cloud Assembly-Administrator	Cloud Assembly-Viewer	Cloud Assembly-Benutzer Der Benutzer muss ein Projektadministrationsmitglied sein, um projektbezogene Aufgaben anzeigen und durchführen zu können.	
				Projektadministrator	Projektmitglied
Ereignisse	Erweiterbarkeitsereignisse anzeigen	Ja	Ja		
Abonnements	Erweiterbarkeitsabonnements erstellen, aktualisieren oder löschen	Ja			
	Abonnements deaktivieren	Ja			
	Abonnements anzeigen	Ja	Ja		
Bibliothek – Ereignisthemen	Ereignisthemen anzeigen	Ja	Ja		
Bibliothek – Aktionen	Erweiterbarkeitsaktionen erstellen, aktualisieren oder löschen	Ja			
	Erweiterbarkeitsaktionen anzeigen	Ja	Ja		
Bibliothek – Workflows	Erweiterbarkeits-Workflows anzeigen	Ja	Ja		
Aktivität – Aktionsausführungen	Erweiterbarkeitsaktionsausführungen abbrechen oder löschen	Ja			
	Erweiterbarkeitsaktionsausführungen anzeigen	Ja	Ja		
Aktivität – Workflow-Ausführungen	Erweiterbarkeits-Workflow-Ausführungen anzeigen	Ja	Ja		
Design					
Design	Registerkarte „Design“ öffnen und eine Liste der Cloud-Vorlagen anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Cloud-Vorlagen	Cloud-Vorlagen erstellen, aktualisieren und löschen	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte
	Cloud-Vorlagen anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
	Cloud-Vorlagen herunterladen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
	Cloud-Vorlagen hochladen	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte
	Cloud-Vorlagen bereitstellen	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte
	Cloud-Vorlagen versionieren und wiederherstellen	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte

Tabelle 3-2. vRealize Automation Cloud Assembly-Dienstrollen und -Projektrollen (Fortsetzung)

UI-Kontext	Aufgabe	Cloud Assembly- Administrator	Cloud Assembly- Viewer	Cloud Assembly-Benutzer Der Benutzer muss ein Projektadministra- -mitglied sein, um projektbezogene Aufg- anzeigen und durchführen zu können.	
				Projektadministrator	Projektmitglied
	Cloud-Vorlagen für Katalog freigeben	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte
Benutzerdefinierte Ressourcen	Benutzerdefinierte Ressourcen erstellen, aktualisieren oder löschen	Ja			
	Benutzerdefinierte Ressourcen anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Benutzerdefinierte Aktionen	Benutzerdefinierte Aktionen erstellen, aktualisieren oder löschen	Ja			
	Benutzerdefinierte Aktionen anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
Bereitstellungen					
	Die Registerkarte „Bereitstellungen“ anzeigen und öffnen	Ja	Ja	Ja	Ja
	Bereitstellungen anzeigen, einschließlich Bereitstellungsdetails, Bereitstellungsverlauf und Informationen zur Fehlerbehebung.	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte
	Tag-2-Aktionen für Bereitstellungen basierend auf Richtlinien ausführen.	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte

Service Broker-Dienstrollen

Über die vRealize Automation Service Broker-Dienstrolle wird festgelegt, was Benutzern in vRealize Automation Service Broker angezeigt wird und welche Aufgaben sie ausführen können. Diese Dienstrollen werden in der Konsole von einem Organisationsbesitzer definiert.

Tabelle 3-3. Beschreibungen der Service Broker-Dienstrollen

Rolle	Beschreibung
Service Broker-Administrator	Muss über Lese- und Schreibzugriff auf die gesamte Benutzeroberfläche und die API-Ressourcen verfügen. Dies ist die einzige Benutzerrolle, mit der alle Aufgaben ausgeführt werden können, zum Beispiel das Erstellen eines neuen Projekts und die Zuweisung eines Projektadministrators.
Service Broker-Benutzer	Jeder Benutzer, der nicht über die vRealize Automation Service Broker-Administratorrolle verfügt. In einem vRealize Automation Service Broker-Projekt fügt der Administrator Projekten Benutzer als Projektmitglieder, -administratoren oder -Viewer hinzu. Der Administrator kann auch einen Projektadministrator hinzufügen.
Service Broker-Viewer	Ein Benutzer, der Lesezugriff zum Anzeigen von Informationen hat, Werte jedoch nicht erstellen, aktualisieren oder löschen kann. Benutzer mit der Rolle „Viewer“ können alle für den Administrator verfügbaren Informationen anzeigen. Er kann keine Aktionen ausführen, es sei denn, er wird zu einem Projektadministrator oder Projektmitglied gemacht. Wenn der Benutzer zu einem Projekt gehört, verfügt er über die Berechtigungen, die mit dieser Rolle verbunden sind. Der Projekt-Viewer erweitert seine Berechtigungen nicht in der Weise, wie dies bei den Rollen „Projektadministrator“ oder „Projektmitglied“ der Fall ist.

Zusätzlich zu den Dienstrollen verfügt vRealize Automation Service Broker über Projektrollen. Jedes Projekt ist in allen Diensten verfügbar.

Die Projektrollen sind in vRealize Automation Service Broker definiert und können zwischen Projekten variieren.

Beachten Sie in den folgenden Tabellen, in denen die Berechtigungen der verschiedenen Dienst- und Projektrollen beschrieben werden, dass die Dienstadministratoren über Vollzugriff auf alle Bereiche der Benutzeroberfläche verfügen.

Die folgenden Beschreibungen von Projektrollen helfen Ihnen bei der Entscheidung, welche Berechtigungen Sie Ihren Benutzern erteilen möchten.

- Projektadministratoren nutzen die vom Dienstadministrator erstellte Infrastruktur, um sicherzustellen, dass die Projektmitglieder über die Ressourcen verfügen, die sie für ihre Entwicklungsarbeit benötigen.
- Projektmitglieder arbeiten im Rahmen ihrer Projekte daran, Cloud-Vorlagen zu entwerfen und bereitzustellen.
- Projekt-Viewer sind auf Lesezugriff beschränkt.

Tabelle 3-4. Service Broker-Dienstrollen und -Projektrollen

UI-Kontext	Aufgabe	Service Broker-Administrator	Service Broker-Viewer	Service Broker-Benutzer		
				Der Benutzer muss ein Projektadministrator sein, um projektbezogene Aufgaben anzeigen und durchführen zu können.		
				Projektadministrator	Projektmitglied	Projekt-Viewer
Zugriff auf Service Broker						
Konsole	In der Konsole können Sie Service Broker anzeigen und öffnen	Ja	Ja	Ja	Ja	Ja
Infrastruktur						
	Die Registerkarte „Infrastruktur“ anzeigen und öffnen	Ja	Ja			
Konfigurieren – Projekte	Projekte erstellen	Ja				
	Werte aus der Projektübersicht, Bereitstellungen, Kubernetes und Integrationen aktualisieren oder löschen	Ja				
	Benutzer und Gruppen hinzufügen und Rollen in Projekten zuweisen.	Ja		Ja. Ihre Projekte.		
	Projekte anzeigen	Ja	Ja			
Konfigurieren – Cloud-Zonen	Cloud-Zonen erstellen, aktualisieren oder löschen	Ja				
	Cloud-Zonen anzeigen	Ja	Ja			
Konfigurieren – Kubernetes-Zonen	Kubernetes-Zonen erstellen, aktualisieren oder löschen	Ja				
	Kubernetes-Zonen anzeigen	Ja	Ja			
Verbindungen – Cloud-Konten	Cloud-Konten erstellen, aktualisieren oder löschen	Ja				
	Cloud-Konten anzeigen	Ja	Ja			
Verbindungen – Integrationen	Integrationen erstellen, aktualisieren oder löschen	Ja				
	Integrationen anzeigen	Ja	Ja			
Aktivität – Anforderungen	Datensätze der Bereitstellungsanforderung löschen	Ja				

Tabelle 3-4. Service Broker-Dienstrollen und -Projektrollen (Fortsetzung)

UI-Kontext	Aufgabe	Service Broker-Administrator	Service Broker-Viewer	Service Broker-Benutzer Der Benutzer muss ein Projektadministrator sein, um projektbezogene Aufgaben anzeigen und durchführen zu können.		
				Projektadministrator	Projektmitglied	Projekt-Viewer
	Datensätze der Bereitstellungsanforderung anzeigen	Ja				
Aktivität – Ereignisprotokolle	Ereignisprotokolle anzeigen	Ja				
Inhalt und Richtlinien						
	Die Registerkarte „Inhalt und Richtlinien“ anzeigen und öffnen	Ja	Ja			
Inhaltsquellen	Inhaltsquellen erstellen, aktualisieren oder löschen	Ja				
	Inhaltsquellen anzeigen	Ja	Ja			
Inhaltsfreigabe	Freigegebene Inhalte hinzufügen oder entfernen	Ja				
	Freigegebene Inhalte anzeigen	Ja	Ja			
Inhalt	Format anpassen und Element konfigurieren	Ja				
	Inhalt anzeigen	Ja	Ja			
Richtlinien – Definitionen	Richtliniendefinitionen erstellen, aktualisieren oder löschen	Ja				
	Richtliniendefinitionen anzeigen	Ja	Ja			
Richtlinien – Durchsetzung	Durchsetzungsprotokoll anzeigen	Ja	Ja			
Benachrichtigungen – E-Mail-Server	E-Mail-Server konfigurieren	Ja				
Katalog						
	Die Registerkarte „Katalog“ anzeigen und öffnen	Ja	Ja	Ja	Ja	Ja
	Verfügbare Katalogelemente anzeigen	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte	Ja. Ihre Projekte
	Ein Katalogelement anfordern	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte	

Tabelle 3-4. Service Broker-Dienstrollen und -Projektrollen (Fortsetzung)

UI-Kontext	Aufgabe	Service Broker-Administrator	Service Broker-Viewer	Service Broker-Benutzer		
				Der Benutzer muss ein Projektadministrator sein, um projektbezogene Aufgaben anzeigen und durchführen zu können.		
				Projektadministrator	Projektmitglied	Projekt-Viewer
Bereitstellungen						
	Die Registerkarte „Bereitstellungen“ anzeigen und öffnen	Ja	Ja	Ja.	Ja	Ja
	Bereitstellungen anzeigen, einschließlich Bereitstellungsdetails, Bereitstellungsverlauf und Informationen zur Fehlerbehebung.	Ja	Ja	Ja. Ihre Projekte	Ja. Ihre Projekte	Ja. Ihre Projekte
	Tag-2-Aktionen für Bereitstellungen basierend auf Richtlinien ausführen	Ja		Ja. Ihre Projekte	Ja. Ihre Projekte	
Genehmigungen						
	Die Registerkarte „Genehmigungen“ anzeigen und öffnen	Ja	Ja	Ja	Ja	Ja
	Auf Genehmigungsanforderungen antworten	Ja		Nur Service Broker-Benutzerrolle	Nur Service Broker-Benutzerrolle	Nur Service Broker-Benutzerrolle

Code Stream-Dienstrollen

Über die vRealize Automation Code Stream-Dienstrolle wird festgelegt, was Benutzern in vRealize Automation Code Stream angezeigt wird und welche Aufgaben sie ausführen können. Diese Rollen werden in der Konsole vom Organisationsbesitzer definiert. Jedes Projekt ist in allen Diensten verfügbar.

Tabelle 3-5. Beschreibungen der Code Stream Dienstrollen

Rolle	Beschreibung
Code Stream-Administrator	Ein Benutzer, der über Lese- und Schreibzugriff auf die gesamte Benutzeroberfläche und die API-Ressourcen verfügt. Dies ist die einzige Benutzerrolle, der alles angezeigt wird und die alle Aktionen ausführen kann, einschließlich dem Erstellen von Projekten, Integrieren von Endpoints, Hinzufügen von Auslösern, Erstellen von Pipelines und benutzerdefinierten Dashboards, Markieren von Endpoints und Variablen als eingeschränkte Ressourcen, Ausführen von Pipelines, die eingeschränkte Ressourcen verwenden, und Anfordern der Veröffentlichung von Pipelines in vRealize Automation Service Broker.
Code Stream-Entwickler	Ein Benutzer, der mit Pipelines, aber nicht mit eingeschränkten Endpoints oder Variablen arbeiten kann. Wenn eine Pipeline einen eingeschränkten Endpoint oder eine eingeschränkte Variable enthält, muss dieser Benutzer eine Genehmigung für die Pipeline-Aufgabe erhalten, die den eingeschränkten Endpoint oder die eingeschränkte Variable verwendet.
Code Stream-Executor	Ein Benutzer, der Pipelines ausführen und Benutzervorgangsaufgaben genehmigen oder ablehnen kann. Dieser Benutzer kann Ausführungen von Pipelines fortsetzen, anhalten und abbrechen, er kann jedoch Pipelines nicht ändern.
Code Stream-Benutzer	Ein Benutzer, der auf vRealize Automation Code Stream zugreifen kann, jedoch über keine anderen Rechte in vRealize Automation Code Stream verfügt.
Code Stream-Betrachter	Ein Benutzer, der über Lesezugriff zum Anzeigen von Pipelines, Endpoints, Pipeline-Ausführungen und Dashboards verfügt, diese jedoch nicht erstellen, aktualisieren oder löschen kann. Ein Benutzer, der auch über die Rolle „Dienst-Viewer“ verfügt, kann alle für den Administrator verfügbaren Informationen anzeigen. Er kann keine Aktionen ausführen, es sei denn, er wird zu einem Projektadministrator oder Projektmitglied gemacht. Wenn der Benutzer zu einem Projekt gehört, verfügt er über die Berechtigungen, die mit dieser Rolle verbunden sind. Der Projekt-Viewer erweitert seine Berechtigungen nicht in der Weise, wie dies bei den Rollen „Projektadministrator“ oder „Projektmitglied“ der Fall ist.

Zusätzlich zu den Dienstrollen verfügt vRealize Automation Code Stream über Projektrollen. Jedes Projekt ist in allen Diensten verfügbar.

Die Projektrollen sind in vRealize Automation Code Stream definiert und können zwischen Projekten variieren.

Beachten Sie in den folgenden Tabellen, in denen die Berechtigungen der verschiedenen Dienst- und Projektrollen beschrieben werden, dass die Dienstadministratoren über Vollzugriff auf alle Bereiche der Benutzeroberfläche verfügen.

Die folgenden Beschreibungen von Projektrollen helfen Ihnen bei der Entscheidung, welche Berechtigungen Sie Ihren Benutzern erteilen möchten.

- Projektadministratoren nutzen die vom Dienstadministrator erstellte Infrastruktur, um sicherzustellen, dass die Projektmitglieder über die Ressourcen verfügen, die sie für ihre Entwicklungsarbeit benötigen. Der Projektadministrator kann Mitglieder hinzufügen.
- Projektmitglieder mit einer Dienstrolle können Dienste verwenden.
- Projekt-Viewer können Projekte anzeigen, sie aber weder erstellen, aktualisieren noch löschen.

Alle Aktionen außer eingeschränkten bedeutet, dass dieser Rolle die Berechtigung zum Durchführen, Erstellen, Lesen, Aktualisieren und Löschen von Aktionen in Entitäten, ausgenommen eingeschränkter Variablen und Endpoints, erteilt wurde.

Tabelle 3-6. Funktionen der vRealize Automation Code Stream-Dienstrolle

UI-Kontext	Funktionen	Code Stream-Administratorrolle	Code Stream-Entwicklerrolle	Code Stream-Executor-Rolle	Code Stream-Viewer-Rolle	Code Stream-Benutzerrolle
Pipelines						
	Pipelines anzeigen	Ja	Ja	Ja	Ja	
	Pipelines erstellen	Ja	Ja			
	Pipelines ausführen	Ja	Ja	Ja		
	Pipelines ausführen, die eingeschränkte Endpoints oder Variablen enthalten	Ja				
	Pipelines aktualisieren	Ja	Ja			
	Pipelines löschen	Ja	Ja			
Pipelineausführungen						
	Pipeline-Ausführungen anzeigen	Ja	Ja	Ja	Ja	
	Pipeline-Ausführungen fortsetzen, anhalten und abbrechen	Ja	Ja	Ja		
	Pipelines fortsetzen, die für die Genehmigung auf eingeschränkten Ressourcen angehalten werden	Ja				
Benutzerdefinierte Integrationen						
	Benutzerdefinierte Integrationen erstellen	Ja	Ja			
	Benutzerdefinierte Integrationen lesen	Ja	Ja			
	Benutzerdefinierte Integration aktualisieren	Ja	Ja			
Endpoints						

Tabelle 3-6. Funktionen der vRealize Automation Code Stream-Dienstrolle (Fortsetzung)

UI-Kontext	Funktionen	Code Stream-Administratorrolle	Code Stream-Entwicklerrolle	Code Stream-Executor-Rolle	Code Stream-Viewer-Rolle	Code Stream-Benutzerrolle
	Ausführungen anzeigen	Ja	Ja	Ja	Ja	
	Ausführungen erstellen	Ja	Ja			
	Ausführungen aktualisieren	Ja	Ja			
	Ausführungen löschen	Ja	Ja			
Ressourcen als eingeschränkt markieren						
	Einen Endpoint oder eine Variable als eingeschränkt markieren	Ja				
Dashboards						
	Dashboards anzeigen	Ja	Ja	Ja	Ja	
	Dashboards erstellen	Ja	Ja			
	Dashboards aktualisieren	Ja	Ja			
	Dashboards löschen	Ja	Ja			

Benutzerdefinierte Benutzerrollen in vRealize Automation

Als vRealize Automation Cloud Assembly-Administrator können Sie benutzerdefinierte Rollen erstellen, die definieren, was Benutzer in vRealize Automation anzeigen und welche Aktionen sie ausführen können. Anschließend können Sie diesen Rollen Benutzer zuweisen.

Berechtigungen für benutzerdefinierte Benutzerrollen

Mithilfe von vRealize Automation Cloud Assembly können Sie präzisere Benutzerrollen definieren und diesen Rollen dann Benutzern zuweisen. Die benutzerdefinierten Rollen weisen die Kategorien „Anzeigen“ und „Verwalten“ auf.

- **Anzeigen.** Ein Benutzer, dem eine Rolle mit dieser Berechtigung zugewiesen ist, kann alle Elemente für alle Projekte in den ausgewählten Abschnitten der Benutzeroberfläche anzeigen. Diese Rolle eignet sich für Benutzer, die Konten, Konfigurationen oder zugewiesene Werte anzeigen müssen.

- **Verwalten.** Ein Benutzer, dem eine Rolle mit dieser Berechtigung zugewiesen ist, kann alle Elemente anzeigen und verfügt über uneingeschränkte Berechtigungen zum Hinzufügen, Bearbeiten und Löschen für alle Projekte in den ausgewählten Abschnitten der Benutzeroberfläche.

Diese Berechtigungen stellen eine Erweiterung der Berechtigungen dar, die von den anderen Rollen gewährt werden, und sind nicht durch die Projektmitgliedschaft eingeschränkt. Sie können beispielsweise die Berechtigungen eines Projektadministrators auf die Verwaltung von Teilen der Infrastruktur ausweiten oder einem Dienst-Viewer die Möglichkeit geben, Genehmigungen zu überprüfen und darauf zu antworten.

Um die Benutzerrollen zu definieren und Benutzer zuzuweisen, öffnen Sie vRealize Automation Cloud Assembly oder vRealize Automation Service Broker als Dienstadministrator und wählen Sie **Infrastruktur > Verwaltung > Benutzerdefinierte Rollen** aus. Sie können die benutzerdefinierten Rollen in vRealize Automation Code Stream nicht konfigurieren. Die Rollen gelten jedoch für alle Dienste.

Tabelle 3-7. Benutzerdefinierte Rollen

Benutzeroberfläche	Berechtigung	Beschreibung
Infrastruktur		
	Cloud-Konten anzeigen.	Cloud-Konten anzeigen.
	Cloud-Konten verwalten	Cloud-Konten erstellen, aktualisieren oder löschen.
	Image-Zuordnungen anzeigen	Image-Zuordnungen anzeigen.
	Image-Zuordnungen verwalten	Image-Zuordnungen erstellen, aktualisieren oder löschen.
	Typzuordnungen anzeigen	Typzuordnungen anzeigen.
	Typzuordnungen verwalten	Typzuordnungen erstellen, aktualisieren oder löschen.
	Cloud-Zonen anzeigen	Cloud-Zonen anzeigen.
	Cloud-Zonen verwalten	Cloud-Zonen erstellen, aktualisieren oder löschen.
	Maschinen anzeigen	Maschinen anzeigen.
	Anforderungen anzeigen	Aktivitätsanforderungen anzeigen.
	Anforderungen verwalten	Anforderungen aus der Liste löschen.
	Integrationen anzeigen	Integrationen anzeigen.
	Integrationen verwalten	Integrationen erstellen, aktualisieren oder löschen.
	Projekte anzeigen	Projekte anzeigen.

Tabelle 3-7. Benutzerdefinierte Rollen (Fortsetzung)

Benutzeroberfläche	Berechtigung	Beschreibung
	Projekte verwalten	Projekte erstellen. Benutzer hinzufügen und Rollen in einem Projekt zuweisen. Werte aus der Projektübersicht, Benutzern, Bereitstellungen, Kubernetes und Integrationen aktualisieren oder löschen und Projektkonfigurationen testen.
	Onboarding-Pläne anzeigen	Onboarding-Pläne anzeigen
	Onboarding-Pläne verwalten	Onboarding-Pläne erstellen, aktualisieren, ausführen oder löschen
Katalog		
	Inhalt anzeigen	
	Inhalt verwalten	Inhaltsquellen hinzufügen, aktualisieren, löschen. Inhalt freigeben. Den Inhalt anpassen, einschließlich der Katalogsymbole und Anfrageformulare.
Richtlinien		
	Richtlinien anzeigen	Richtliniendefinitionen anzeigen.
	Richtlinien verwalten	Richtliniendefinitionen erstellen, aktualisieren oder löschen.
Bereitstellungen		
	Bereitstellungen anzeigen	Alle Bereitstellungen anzeigen, einschließlich Bereitstellungsdetails, Bereitstellungsverlauf und Informationen zur Fehlerbehebung.
	Bereitstellungen verwalten	Alle Bereitstellungen anzeigen und alle Tag-2-Aktionen ausführen, die ein Administrator gemäß den Tag-2-Richtlinien für Bereitstellungen und Bereitstellungskomponenten ausführen darf.
Cloud-Vorlagen		
	Cloud-Vorlagen anzeigen	Cloud-Vorlagen anzeigen.

Tabelle 3-7. Benutzerdefinierte Rollen (Fortsetzung)

Benutzeroberfläche	Berechtigung	Beschreibung
	Cloud-Vorlagen verwalten	Cloud-Vorlagen erstellen, aktualisieren, testen, löschen, versionieren, freigeben und die Version einer Cloud-Vorlage freigeben bzw. deren Freigabe aufheben.
	Cloud-Vorlagen bearbeiten	Cloud-Vorlagen erstellen, aktualisieren, testen, versionieren, freigeben und die Version einer Cloud-Vorlage freigeben bzw. deren Freigabe aufheben. Die Rolle verfügt nicht über die Berechtigung zum Löschen von Cloud-Vorlagen.
	Cloud-Vorlagen bereitstellen	Alle Cloud-Vorlagen in einem beliebigen Projekt testen und bereitstellen.
	In Cloud-Vorlage integrierten Inhalt bereitstellen	Alle Cloud-Vorlagen in den Projekten bereitstellen, die mit den entsprechenden Personen verknüpft sind. Die Projektrollen können „Administrator“, „Mitglied“ oder „Viewer“ lauten.
XaaS		
	Benutzerdefinierte Ressourcen anzeigen	Benutzerdefinierte Ressourcen anzeigen.
	Benutzerdefinierte Ressourcen verwalten	Benutzerdefinierte Ressourcen erstellen, aktualisieren oder löschen
	Ressourcenaktionen anzeigen	Benutzerdefinierte Aktionen anzeigen.
	Ressourcenaktionen verwalten	Benutzerdefinierte Aktionen erstellen, aktualisieren oder löschen
Erweiterbarkeit		
	Erweiterbarkeitsressourcen anzeigen	Ereignisse, Abonnements, Ereignisthemen, Aktionen, Workflows, Aktions- und Workflowausführungen anzeigen.
	Erweiterbarkeitsressourcen verwalten	Erweiterbarkeitsabonnements erstellen, aktualisieren, löschen und deaktivieren. Erweiterbarkeitsaktionen erstellen, aktualisieren oder löschen. Erweiterbarkeitsaktionsausführungen abbrechen oder löschen.
Pipeline		

Tabelle 3-7. Benutzerdefinierte Rollen (Fortsetzung)

Benutzeroberfläche	Berechtigung	Beschreibung
	Pipelines verwalten	Pipeline-, Endpoint-, Variablen- und Auslöserkonfigurationen erstellen, bearbeiten und löschen. Eingeschränkte Modelle sind ausgeschlossen.
	Eingeschränkte Pipelines verwalten	Pipeline-, Endpoint-, Variablen- und Auslöserkonfigurationen erstellen, bearbeiten und löschen. Eingeschränkte Modelle sind eingeschlossen.
	Benutzerdefinierte Integrationen verwalten	Benutzerdefinierte Integrationen hinzufügen, bearbeiten und löschen.
	Pipelines ausführen	Ausführungen und Auslöser des Pipelinemodells ausführen und die Ausführungen und Auslöser anhalten, abbrechen, wiederaufnehmen oder erneut ausführen.
	Eingeschränkte Pipelines ausführen	Ausführungen und Auslöser des Pipelinemodells ausführen und die Ausführungen und Auslöser anhalten, abbrechen, wiederaufnehmen oder erneut ausführen. Eingeschränkte Endpoints und Variablen auflösen.
	Ausführungen verwalten	Ausführungen und Auslöser des Pipelinemodells ausführen und die Ausführungen und Auslöser anhalten, abbrechen, wiederaufnehmen oder erneut ausführen. Eingeschränkte Endpoints und Variablen auflösen. Ausführungen löschen.
Genehmigung		
	Genehmigungen verwalten	Zeigen Sie die Registerkarte „Genehmigungen“ an, auf der Genehmigungsanfragen genehmigt oder abgelehnt werden können. Der Genehmiger mit dieser Rolle erhält keine E-Mail-Benachrichtigung über eine Genehmigungsanforderung, es sei denn, er ist ein Genehmiger in der Richtlinie.

Anwendungsbeispiele: Wie können Benutzerrollen mich bei der Steuerung des Zugriffs in vRealize Automation unterstützen

Als Cloud-Administrator möchten Sie steuern, welche Aufgaben Ihre Benutzer in vRealize Automation ausführen können. Abhängig von Ihren Verwaltungszielen und den Zuständigkeiten des Anwendungsentwicklungsteams können Sie die Benutzerrollen für die Unterstützung dieser Ziele auf verschiedene Arten konfigurieren.

Die folgenden vRealize Automation Cloud Assembly- und vRealize Automation Service Broker-Beispiele basieren auf drei Anwendungsbeispielen. Diese Beispiele bieten nur genügend Anweisungen, um die Anwendung von Benutzerrollen zu veranschaulichen.

Die Zielgruppe für diese Anwendungsbeispiele sind der Cloud-Administrator, der auch solcher betrachtet wird, und die Dienstadministratoren.

Die Anwendungsbeispiele bauen aufeinander auf. Auch wenn Sie bereit sind, direkt zu Anwendungsbeispiel 3 zu gehen, müssen Sie möglicherweise die Anwendungsbeispiele 1 und 2 durchgehen, um besser zu verstehen, warum Sie die Rollen in der angegebenen Weise konfigurieren.

Der Zweck der Anwendungsbeispiele besteht darin, Benutzerrollen zu demonstrieren. Es geht nicht um detaillierte Informationen zum Konfigurieren Ihrer Infrastruktur, Verwalten von Projekten, Erstellen von Cloud-Vorlagen und Arbeiten mit Bereitstellungen.

Bevor Sie beginnen, müssen Sie die Ebenen der Benutzerrollen verstehen, die von einem Cloud-Administrator in der vRealize Automation-Konsole konfiguriert werden.

■ Organisationsrollen

Die Organisationsrollen steuern, wer auf die Konsole zugreifen kann.

Als Organisationsbesitzer müssen Sie sicherstellen, dass allen Benutzern von Diensten mindestens eine Organisationsmitglieds-Rolle zugewiesen wird.

Rolle	Beschreibung
Organisationsbesitzer	Ein Administrator kann Benutzer hinzufügen, die Rolle der Benutzer ändern und Benutzer aus der Organisation entfernen. Der Besitzer verwaltet, auf welche Dienste Benutzer Zugriff haben.
Organisationsmitglied	Ein allgemeiner Benutzer kann sich bei der Organisationskonsole anmelden. Für den Zugriff auf die Dienste muss ein Organisationsbesitzer den Benutzern Dienstrollen zuweisen.

■ Dienstrollen

Die Dienstrollen steuern, wer auf ihre zugewiesenen Dienste zugreifen kann.

Als Organisationsbesitzer müssen Sie sicherstellen, dass den Benutzern, die Zugriff auf die Dienste benötigen, die entsprechende Rolle zugewiesen wird. Sie verwenden die Rollen, um zu steuern, wie viel der Benutzer in jedem Dienst tun kann.

Tabelle 3-8. Beschreibungen der vRealize Automation Cloud Assembly-Dienstrollen

Rolle	Beschreibung
Cloud Assembly-Administrator	Ein Benutzer, der über Lese- und Schreibzugriff auf die gesamte Benutzeroberfläche und die API-Ressourcen verfügt. Dies ist die einzige Benutzerrolle, mit der alles angezeigt und durchgeführt werden kann, einschließlich Cloud-Konten hinzufügen, neue Projekte erstellen und einen Projektadministrator zuweisen.
Cloud Assembly-Benutzer	Ein Benutzer, der nicht über die Rolle des Cloud Assembly-Administrators verfügt. In einem vRealize Automation Cloud Assembly-Projekt fügt der Administrator Projekten Benutzer als Projektmitglieder, -administratoren oder -Viewer hinzu. Der Administrator kann auch einen Projektadministrator hinzufügen.
Cloud Assembly-Viewer	Ein Benutzer, der Lesezugriff zum Anzeigen von Informationen hat, Werte jedoch nicht erstellen, aktualisieren oder löschen kann. Dies ist eine Rolle, die für alle Projekte nur über Leserechte verfügt. Benutzer mit der Rolle „Viewer“ können alle für den Administrator verfügbaren Informationen anzeigen. Er kann keine Aktionen ausführen, es sei denn, er wird zu einem Projektadministrator oder Projektmitglied gemacht. Wenn der Benutzer zu einem Projekt gehört, verfügt er über die Berechtigungen, die mit dieser Rolle verbunden sind. Der Projekt-Viewer erweitert seine Berechtigungen nicht in der Weise, wie dies bei den Rollen „Projektadministrator“ oder „Projektmitglied“ der Fall ist.

Tabelle 3-9. Beschreibungen der Service Broker-Dienstrollen

Rolle	Beschreibung
Service Broker-Administrator	Muss über Lese- und Schreibzugriff auf die gesamte Benutzeroberfläche und die API-Ressourcen verfügen. Dies ist die einzige Benutzerrolle, mit der alle Aufgaben ausgeführt werden können, zum Beispiel das Erstellen eines neuen Projekts und die Zuweisung eines Projektadministrators.
Service Broker-Benutzer	Jeder Benutzer, der nicht über die vRealize Automation Service Broker-Administratorrolle verfügt.

Tabelle 3-9. Beschreibungen der Service Broker-Dienstrollen (Fortsetzung)

Rolle	Beschreibung
	In einem vRealize Automation Service Broker-Projekt fügt der Administrator Projekten Benutzer als Projektmitglieder, -administratoren oder -Viewer hinzu. Der Administrator kann auch einen Projektadministrator hinzufügen.
Service Broker-Viewer	<p>Ein Benutzer, der Lesezugriff zum Anzeigen von Informationen hat, Werte jedoch nicht erstellen, aktualisieren oder löschen kann.</p> <p>Benutzer mit der Rolle „Viewer“ können alle für den Administrator verfügbaren Informationen anzeigen. Er kann keine Aktionen ausführen, es sei denn, er wird zu einem Projektadministrator oder Projektmitglied gemacht. Wenn der Benutzer zu einem Projekt gehört, verfügt er über die Berechtigungen, die mit dieser Rolle verbunden sind. Der Projekt-Viewer erweitert seine Berechtigungen nicht in der Weise, wie dies bei den Rollen „Projektadministrator“ oder „Projektmitglied“ der Fall ist.</p>

Tabelle 3-10. Beschreibungen der Code Stream Dienstrollen

Rolle	Beschreibung
Code Stream-Administrator	Ein Benutzer, der über Lese- und Schreibzugriff auf die gesamte Benutzeroberfläche und die API-Ressourcen verfügt. Dies ist die einzige Benutzerrolle, der alles angezeigt wird und die alle Aktionen ausführen kann, einschließlich dem Erstellen von Projekten, Integrieren von Endpoints, Hinzufügen von Auslösern, Erstellen von Pipelines und benutzerdefinierten Dashboards, Markieren von Endpoints und Variablen als eingeschränkte Ressourcen, Ausführen von Pipelines, die eingeschränkte Ressourcen verwenden, und Anfordern der Veröffentlichung von Pipelines in vRealize Automation Service Broker.
Code Stream-Entwickler	Ein Benutzer, der mit Pipelines, aber nicht mit eingeschränkten Endpoints oder Variablen arbeiten kann. Wenn eine Pipeline einen eingeschränkten Endpoint oder eine eingeschränkte Variable enthält, muss dieser Benutzer eine Genehmigung für die Pipeline-Aufgabe erhalten, die den eingeschränkten Endpoint oder die eingeschränkte Variable verwendet.
Code Stream-Executor	Ein Benutzer, der Pipelines ausführen und Benutzervorgangsaufgaben genehmigen oder ablehnen kann. Dieser Benutzer kann Ausführungen von Pipelines fortsetzen, anhalten und abbrechen, er kann jedoch Pipelines nicht ändern.

Tabelle 3-10. Beschreibungen der Code Stream Dienstrollen (Fortsetzung)

Rolle	Beschreibung
Code Stream-Benutzer	Ein Benutzer, der auf vRealize Automation Code Stream zugreifen kann, jedoch über keine anderen Rechte in vRealize Automation Code Stream verfügt.
Code Stream-Betrachter	Ein Benutzer, der über Lesezugriff zum Anzeigen von Pipelines, Endpoints, Pipeline-Ausführungen und Dashboards verfügt, diese jedoch nicht erstellen, aktualisieren oder löschen kann. Ein Benutzer, der auch über die Rolle „Dienst-Viewer“ verfügt, kann alle für den Administrator verfügbaren Informationen anzeigen. Er kann keine Aktionen ausführen, es sei denn, er wird zu einem Projektadministrator oder Projektmitglied gemacht. Wenn der Benutzer zu einem Projekt gehört, verfügt er über die Berechtigungen, die mit dieser Rolle verbunden sind. Der Projekt-Viewer erweitert seine Berechtigungen nicht in der Weise, wie dies bei den Rollen „Projektadministrator“ oder „Projektmitglied“ der Fall ist.

■ Projektmitgliedschaftsrollen

Die Projektmitgliedschaft legt fest, welche Infrastrukturressourcen und Cloud-Vorlagen verfügbar sind.

Die Projektmitgliedschaft wird im Dienst von einem Benutzer mit einer Dienstadministrator-Rolle definiert. Der Dienstadministrator muss sicherstellen, dass den Benutzern, die Zugriff auf ein oder mehrere Projekte benötigen, die entsprechende Projekt-Rolle in jedem Projekt zugewiesen wird.

Tabelle 3-11. Projektrollen

Rolle	Beschreibung
Projektadministrator	Ein Projektadministrator kann seine eigenen Projekte verwalten, Cloud-Vorlagen erstellen und bereitstellen, die mit seinen Projekten verknüpft sind, und Projektbereitstellungen für alle Projektmitglieder verwalten.
Projektmitglied	Ein Projektmitglied kann Cloud-Vorlagen erstellen und bereitstellen, die mit seinen Projekten verknüpft sind, und seine eigenen sowie alle freigegebenen Bereitstellungen verwalten.
Projekt-Viewer	Ein Projekt-Viewer ist ein Mitglied des Projekts mit schreibgeschütztem Zugriff auf seine Projektressourcen, Cloud-Vorlagen und Bereitstellungen.

■ Benutzerdefinierte Rollen

Die benutzerdefinierten Rollen werden von vRealize Automation Cloud Assembly zur Optimierung der Mitglieds- und Viewer-Rollen erstellt.

Die in diesen Anwendungsbeispielen gezeigten Verfahren sind dazu gedacht, die Benutzerrollen zu erläutern. Es handelt sich nicht um detaillierte oder definitive Verfahren zum Einrichten von vRealize Automation.

Bedenken Sie bei der Konfiguration von Rollen, dass Benutzer, die API-Vorgänge ausführen, den Rollen unterliegen, die Sie hier zuweisen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Organisationsbesitzer-Rolle verfügen. Sie müssen die Registerkarte **Identitäts- und Zugriffsverwaltung** anzeigen können, um sich bei der Konsole anzumelden. Wenn dies nicht der Fall ist, wenden Sie sich an den Organisationsbesitzer.

■

- Stellen Sie sicher, dass Ihre Benutzer zu vRealize Automation hinzugefügt wurden.

Wenn Sie vRealize Automation installieren, werden Ihre Active Directory-Benutzer als Teil des Prozesses hinzugefügt.

- Eine ausführlichere Aufgaben- und Rollenliste für verschiedene Rollen finden Sie unter [Organisations- und Dienstbenutzerrollen in vRealize Automation](#).

Verfahren

1 [Benutzerrollen-Anwendungsbeispiel 1: Einrichten von vRealize Automation-Benutzerrollen zur Unterstützung eines kleinen Anwendungsentwicklungsteams](#)

Als vRealize Automation-Cloud-Administrator sind Sie für die Verwaltung des Zugriffs und des Budgets für Ihre Infrastrukturressourcen verantwortlich. Sie fügen sich und zwei andere Benutzer als Administratoren hinzu. Dieses kleine Team kann die Infrastruktur erstellen und die Cloud-Vorlagen entwickeln, die den Geschäftszielen der Teams entsprechen, die die Cloud-Vorlagen verbrauchen. Anschließend stellen Sie und Ihr kleines Administratorenteam die Cloud-Vorlagen für Ihre Verbraucher bereit, die keine Administratoren sind. Sie lassen nicht zu, dass Nicht-Administratoren auf vRealize Automation zugreifen.

2 [Anwendungsbeispiel für Benutzerrollen 2: Einrichten von vRealize Automation-Benutzerrollen zur Unterstützung größerer Entwicklungsteams und des Katalogs](#)

Als vRealize Automation-Organisationsbesitzer sind Sie für die Verwaltung des Zugriffs und das Budget für Ihre Infrastrukturressourcen verantwortlich. Sie verfügen über ein Team von Cloud-Vorlagenentwicklern, die Vorlagen iterativ für verschiedene Projekte erstellen und bereitstellen, bis sie zur Bereitstellung an die Verbraucher bereit sind. Anschließend stellen Sie den Verbrauchern in einem Katalog die einsatzfähigen Ressourcen bereit.

3 [Anwendungsbeispiel für Benutzerrolle 3: Einrichten benutzerdefinierter vRealize Automation-Benutzerrollen zur Optimierung von Systemrollen](#)

Als vRealize Automation-Organisationsbesitzer oder -Dienstadministrator verwalten Sie den Benutzerzugriff mithilfe der Organisations- und Dienstsysteemrollen. Sie möchten jedoch auch benutzerdefinierte Rollen für diese ausgewählten Benutzer erstellen und Aufgaben ausführen oder Inhalte anzeigen, die sich außerhalb der Systemrollen befinden.

Benutzerrollen-Anwendungsbeispiel 1: Einrichten von vRealize Automation-Benutzerrollen zur Unterstützung eines kleinen Anwendungsentwicklungsteams

Als vRealize Automation-Cloud-Administrator sind Sie für die Verwaltung des Zugriffs und des Budgets für Ihre Infrastrukturressourcen verantwortlich. Sie fügen sich und zwei andere Benutzer als Administratoren hinzu. Dieses kleine Team kann die Infrastruktur erstellen und die Cloud-Vorlagen entwickeln, die den Geschäftszielen der Teams entsprechen, die die Cloud-Vorlagen verbrauchen. Anschließend stellen Sie und Ihr kleines Administratorenteam die Cloud-Vorlagen für Ihre Verbraucher bereit, die keine Administratoren sind. Sie lassen nicht zu, dass Nicht-Administratoren auf vRealize Automation zugreifen.

In diesem Anwendungsbeispiel sind Sie der Organisationsbesitzer, und Sie haben ein kleines Team, in dem alle über die Dienstadministrator-Rolle verfügen.

Das folgende Verfahren verfolgt einen Benutzer durch den ganzen Vorgang. Sie können jeden Schritt für mehrere Benutzer durchführen.

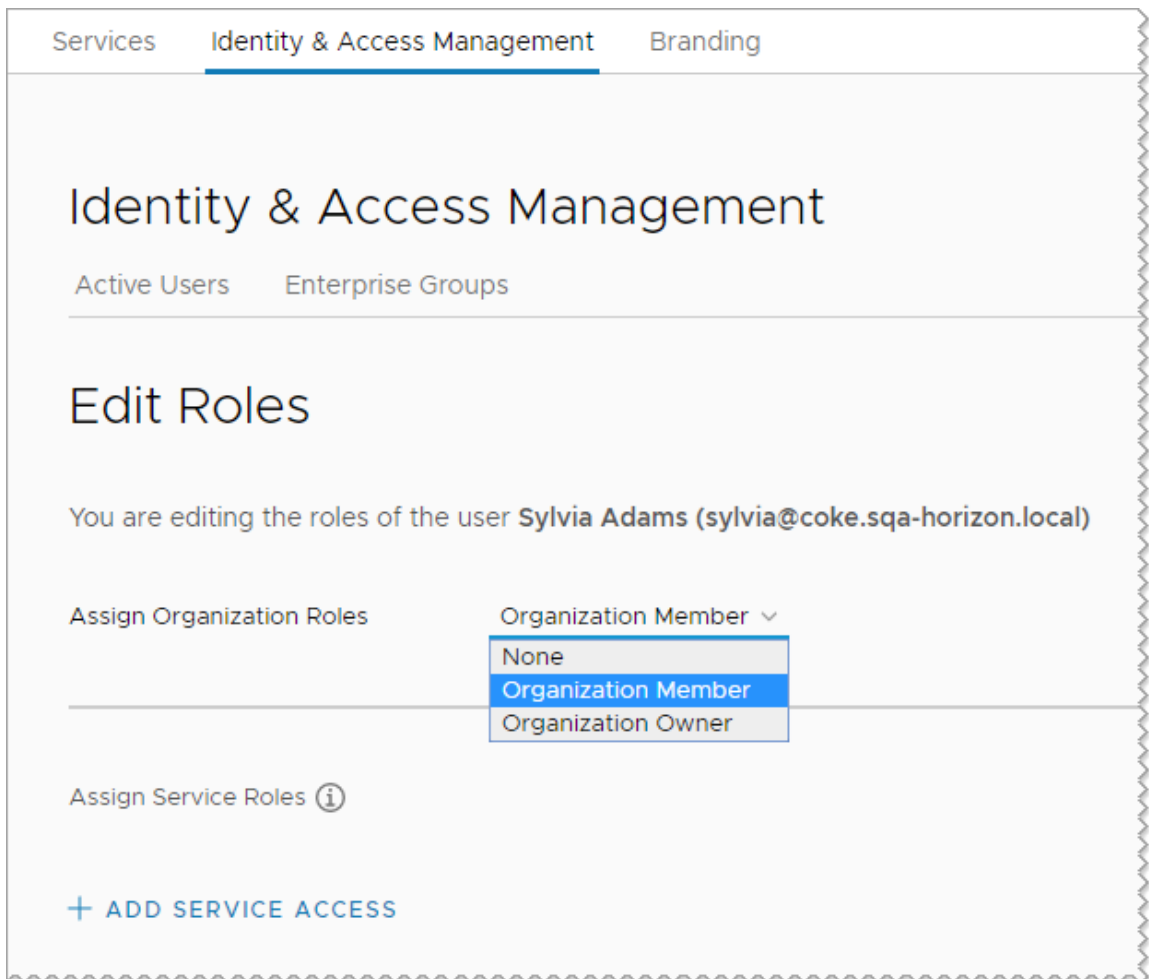
Voraussetzungen

- Stellen Sie sicher, dass Sie alle in der Einführung in das Anwendungsbeispiel festgelegten Voraussetzungen erfüllen. Weitere Informationen hierzu finden Sie unter [Anwendungsbeispiele: Wie können Benutzerrollen mich bei der Steuerung des Zugriffs in vRealize Automation unterstützen](#).

Verfahren

- 1 Weisen Sie Organisationsrollen zu. Klicken Sie auf **Identitäts- und Zugriffsverwaltung**.
 - a Melden Sie sich bei der vRealize Automation-Konsole an.
 - b Klicken Sie auf **Identitäts- und Zugriffsverwaltung**.

- c Wählen Sie den Benutzernamen aus und klicken Sie auf **Rollen bearbeiten**.
- d Wählen Sie im Dropdown-Menü **Organisationsrollen zuweisen** die Option **Organisationsmitglied** aus.



Die Organisationsmitglied-Rolle gewährleistet, dass der Benutzer auf die Konsolen und alle Dienste zugreifen kann, zu denen Sie ihn hinzufügen. Er kann keine Organisationsbenutzer verwalten.

Lassen Sie die Seite „Rolle bearbeiten“ für diesen Benutzer geöffnet und fahren Sie mit dem nächsten Schritt fort.

- 2 Weisen Sie die Cloud Assembly Administrator-Rolle sich selbst und mindestens einem oder zwei anderen Administratoren in diesem Szenario zu.

Die Dienstadministrator-Rolle verfügt über umfassende Berechtigungen zum Hinzufügen, Bearbeiten und Löschen von Infrastruktur, Projekten, Cloud-Vorlagen und Bereitstellungen. Das Definieren einer Administratorrolle für eine Person und der Benutzerrolle für eine andere Person wird in Szenario 2 erläutert. In diesem Beispiel wird Sylvia verwendet.

- Klicken Sie auf **Dienstzugriff hinzufügen**.
- Konfigurieren Sie den Benutzer mit dem folgenden Wert.

Dienst	Rolle
vRealize Automation Cloud Assembly	vRealize Automation Cloud Assembly-Administrator

[Services](#)
[Identity & Access Management](#)
[Branding](#)

Identity & Access Management

[Active Users](#) [Enterprise Groups](#)

Edit Roles

You are editing the roles of the user **Sylvia Adams** (sylvia@coke.sqa-horizon.local)

Assign Organization Roles Organization Member ▾

Assign Service Roles ⓘ

Cloud Assembly ▾ with roles Cloud Assembly Administrator ▾ ×

[+ ADD SERVICE ACCESS](#)

[SAVE](#) [CANCEL](#)

- 3 Erstellen Sie ein Projekt in Cloud Assembly, das Sie zum Gruppieren von Ressourcen und zum Verwalten der Ressourcenabrechnungen für verschiedene Business-Gruppen verwenden.

- Klicken Sie in der Konsole auf die Registerkarte **Dienste** und klicken Sie dann auf **Cloud Assembly**.
- Wählen Sie **Infrastruktur > Projekte > Neues Projekt**.

Dieses Benutzerrollen-Anwendungsbeispiel gibt schwerpunktmäßig Beispiele, wie Sie Benutzerrollen implementieren können, und erläutert nicht das Erstellen des vollständig definierten Systems.

Informationen zum Konfigurieren der Infrastruktur finden Sie unter [Erstellen der Ressourceninfrastruktur](#). Weitere Informationen zu Projekten finden Sie unter [Hinzufügen und Verwalten von Projekten](#).

- c Geben Sie **WebAppTeam** als Projektnamen ein.
- d Klicken Sie auf **Benutzer** und dann auf **Benutzer hinzufügen**.
- e Geben Sie die E-Mail-Adressen der Personen ein, die Sie beim Erstellen und Verwalten der Infrastruktur und der Cloud-Vorlagen unterstützen können.

Beispiel: tony@mycompany.com,sylvia@mycompany.com.

- f Wählen Sie im Dropdown-Menü **Rolle zuweisen** die Option **Administrator**.

Als vRealize Automation Cloud Assembly-Administratoren verfügen diese beiden Benutzer bereits über Administratorzugriff auf die Cloud-Konten, die Infrastruktur und alle Projekte. In diesem Schritt werden die in späteren Szenarios verwendeten Rollen erläutert. In den späteren Szenarien definieren Sie die Projektadministrator- und die Projektmitglied-Rolle, die über unterschiedliche Berechtigungen verfügen.

- g Klicken Sie auf die Registerkarte **Bereitstellung** und fügen Sie eine oder mehrere Cloud-Zonen hinzu.

Bitte beachten Sie: Bei diesem Anwendungsbeispiel geht es um Benutzerrollen.

- 4 Entwickeln Sie eine einfache Cloud-Vorlage, damit Sie das Projekt „WebAppTeam“ testen können.

Dieser Cloud-Vorlagen-Abschnitt ist verkürzt. Im Mittelpunkt stehen Benutzer und Benutzerrollen, die durch Projekte definiert sind, und nicht die Erstellung einer Cloud-Vorlage.

- a Wählen Sie **Cloud-Vorlagen > Neu**.
- b Geben Sie als neuen Namen für die Cloud-Vorlage **WebApp** ein.
- c Wählen Sie als **Projekt** „WebAppTeam“ aus.

New Cloud Template

Name * WebApp

Description

Project * WebAppTeam

Cloud template sharing in Service Broker

☒ Share only with this project

☐ Allow an administrator to share with any project in this organization

CANCEL CREATE

- d Wählen Sie die Option **Nur mit diesem Projekt gemeinsam nutzen**.

Diese Einstellung stellt sicher, dass die Cloud-Vorlage nur für Projektmitglieder verfügbar ist. Wenn Sie zum Bereitstellen der Cloud-Vorlagen für andere Teams bereit sind, können Sie die Option „Dem Administrator die Freigabe an jedes Projekt in dieser Organisation erlauben“ wählen. Die Freigabe der Cloud-Vorlage für andere Projekte bedeutet, dass Sie keine doppelten Instanzen derselben Basisvorlagen pflegen müssen. Sie können Cloud-Vorlagen von Entwicklungsprojekten in Produktionsprojekte verschieben, sodass Katalogverbraucher sie in Produktionsinfrastrukturressourcen bereitstellen können.

- e Klicken Sie auf **Erstellen**.

- f Ziehen Sie im Cloud-Vorlagen-Designer die Komponente **Cloud-unabhängige > Maschine** auf die Arbeitsfläche.

Weitere Informationen zum Konfigurieren von Cloud-Vorlagen finden Sie unter [Entwerfen Ihrer Bereitstellungen](#).

- g Klicken Sie auf **Bereitstellen**.

- h Fahren Sie mit den Durchgängen der Cloud-Vorlage fort, bis Sie sie für Ihre Verbraucher bereitstellen können.

- i Klicken Sie auf **Version** und veröffentlichen Sie eine Version der Cloud-Vorlage.

5 Senden Sie den Benutzern die Anmeldeinformationen mit der gängigsten Methode.

Ergebnisse

In diesem Anwendungsbeispiel haben Sie Ihre beiden Kollegen zu Organisationsmitgliedern gemacht. Sie haben dann Sylvia zu einem vRealize Automation Cloud Assembly-Administrator gemacht. Sie haben Tony zu einem WebApp-Projektadministrator gemacht. Diese Benutzerrollenkonfiguration funktioniert nur für kleine Teams, in denen Sie Ihren Verbrauchern bereitgestellte Anwendungen bereitstellen, anstatt ihnen Self-Service-Zugriff oder einen Katalog bereitzustellen.

Anwendungsbeispiel für Benutzerrollen 2: Einrichten von vRealize Automation-Benutzerrollen zur Unterstützung größerer Entwicklungsteams und des Katalogs

Als vRealize Automation-Organisationsbesitzer sind Sie für die Verwaltung des Zugriffs und das Budget für Ihre Infrastrukturressourcen verantwortlich. Sie verfügen über ein Team von Cloud-Vorlagenentwicklern, die Vorlagen iterativ für verschiedene Projekte erstellen und bereitstellen, bis sie zur Bereitstellung an die Verbraucher bereit sind. Anschließend stellen Sie den Verbrauchern in einem Katalog die einsatzfähigen Ressourcen bereit.

Bei diesem Anwendungsbeispiel wird davon ausgegangen, dass Sie sich bewusst sind, dass sich Anwendungsbeispiel 1 ausschließlich an Administratoren richtet. Sie möchten Ihr System jetzt erweitern, um eine größere Anzahl an Teams und größere Ziele zu unterstützen.

- Entwickler können eigene Anwendungs-Cloud-Vorlagen während der Entwicklung erstellen und bereitstellen. Sie fügen sich selbst als Administrator hinzu und fügen dann zusätzliche Benutzer sowohl mit der Dienstbenutzer- als auch mit der Dienst-Viewer-Rolle hinzu. Als Nächstes fügen Sie die Benutzer als Projektmitglieder hinzu. Die Projektmitglieder können ihre eigenen Cloud-Vorlagen entwickeln und bereitstellen.
- Veröffentlichen Sie Cloud-Vorlagen in einem Katalog, in dem sie für Nichtentwickler zur Bereitstellung verfügbar sind. Sie weisen jetzt Benutzerrollen für Service Broker zu. Service Broker stellt einen Katalog für die Cloud-Vorlagenverbraucher bereit. Sie können damit auch Richtlinien erstellen, einschließlich Leases und Berechtigungen, aber diese Funktionalität gehört nicht zu diesem Anwendungsbeispiel für Benutzerrollen.

Voraussetzungen

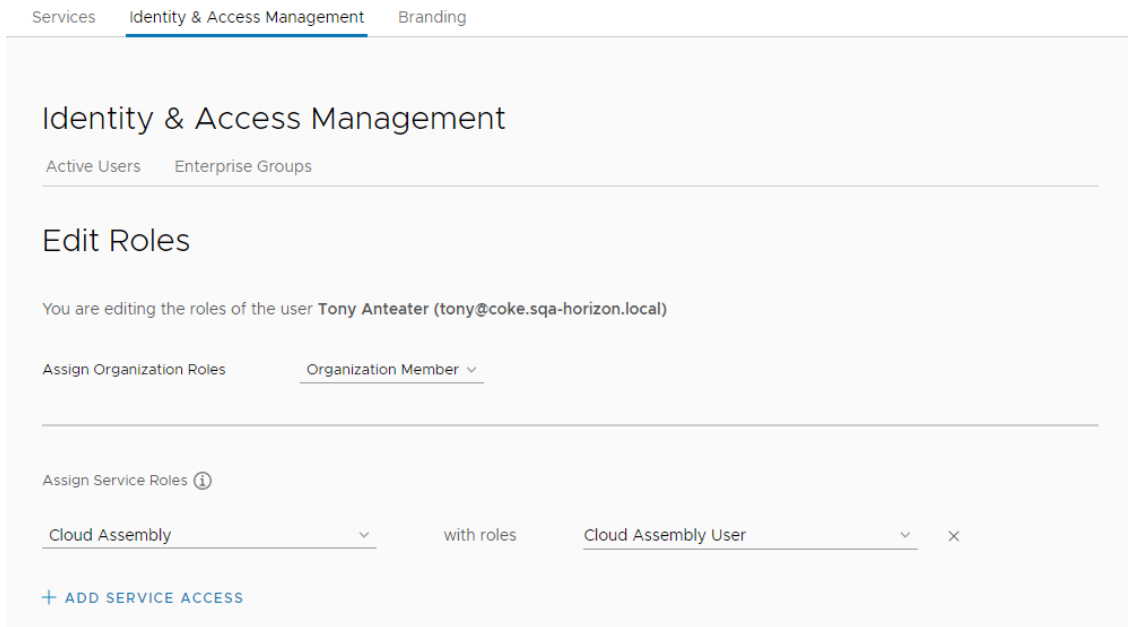
- Gehen Sie das erste Anwendungsbeispiel durch. Weitere Informationen hierzu finden Sie unter [Benutzerrollen-Anwendungsbeispiel 1: Einrichten von vRealize Automation-Benutzerrollen zur Unterstützung eines kleinen Anwendungsentwicklungsteams](#).
- Geben Sie die folgenden Benutzer basierend auf den Berechtigungen an, die ihnen erteilt werden sollen:
 - Cloud-Vorlagenentwickler, die als vRealize Automation Cloud Assembly-Benutzer und -Viewer fungieren
 - Ein vRealize Automation Service Broker-Administrator
 - Nichtentwickler, die als Katalogverbraucher fungieren, als vRealize Automation Service Broker-Benutzer.

Verfahren

- 1 Weisen Sie Ihren Cloud-Vorlagen-Entwicklerbenutzern Organisationsmitglied-Rollen zu.
Wenn Sie Anweisungen benötigen, finden Sie weitere Informationen im [Benutzerrollen-Anwendungsbeispiel 1: Einrichten von vRealize Automation-Benutzerrollen zur Unterstützung eines kleinen Anwendungsentwicklungsteams](#).

2 Weisen Sie den Cloud-Vorlagenentwicklern die vRealize Automation Cloud Assembly-Dienstmitglied-Rolle zu.

- a Klicken Sie auf **Dienstzugriff hinzufügen**.



- b Konfigurieren Sie den Benutzer mit dem folgenden Wert.

Dienst	Rolle
vRealize Automation Cloud Assembly	vRealize Automation Cloud Assembly-Benutzer
vRealize Automation Cloud Assembly	vRealize Automation Cloud Assembly-Viewer

In diesem Anwendungsbeispiel müssen Ihre Entwickler die Infrastruktur sehen können, um sicherzustellen, dass sie bereitstellbare Cloud-Vorlagen erstellen. Als Benutzer, die Sie im nächsten Schritt als Projektadministratoren und Projektmitglieder zuweisen werden, können sie die Infrastruktur nicht sehen. Als Dienst-Viewer können sie sehen, wie die Infrastruktur konfiguriert ist, aber keine Änderungen vornehmen. Als Cloud-Administrator behalten Sie die Kontrolle, geben ihnen aber Zugriff auf die Informationen, die sie zum Entwickeln von Cloud-Vorlagen benötigen.

3 Erstellen Sie Projekte in vRealize Automation Cloud Assembly, die Sie zum Gruppieren von Ressourcenbenutzern verwenden.

In diesem Anwendungsbeispiel erstellen Sie zwei Projekte. Das erste Projekt ist **PersonnelAppDev** und das zweite ist **PayrollAppDev**.

- Klicken Sie in der Konsole auf die Registerkarte **Dienste** und klicken Sie dann auf **Cloud Assembly**.
- Wählen Sie **Infrastruktur > Projekte > Neues Projekt**.
- Geben Sie **PersonnelAppDev** als den Namen ein.
- Klicken Sie auf **Benutzer** und dann auf **Benutzer hinzufügen**.

- e Fügen Sie Projektmitglieder hinzu und weisen Sie einen Projektadministrator zu.

Projektrolle	Beschreibung
Projektbenutzer	Ein Projektmitglied ist die primäre Entwickler-Benutzerrolle in einem Projekt. Projekte bestimmen, welche Cloudressourcen verfügbar sind, wenn Sie bereit sind, Ihre Entwicklungsarbeit zu testen, indem Sie eine Cloud-Vorlage bereitstellen.
Projektadministrator	Ein Projektadministrator unterstützt seine Entwickler durch Hinzufügen und Entfernen von Benutzern für Ihre Projekte. Sie können Ihre Projekte auch löschen. Um ein Projekt zu erstellen, müssen Sie über Dienstadministratorrechte verfügen.

- f Geben Sie für die Benutzer, die Sie als Projektmitglieder hinzufügen, die E-Mail-Adresse der einzelnen Benutzer durch Kommas getrennt ein und wählen Sie **Benutzer** im Dropdown-Menü **Rolle zuweisen** aus.

Beispiel: tony@mycompany.com,sylvia@mycompany.com.

PersonnelAppDev DELETE

Summary **Users** Provisioning Kubernetes Provisioning Integrations

Deployment sharing ☒ Deployments are shared between all users in the project

User roles Specify the users and groups related to this project.

+ ADD USERS + ADD GROUPS X REMOVE

Q Search users or groups

<input type="checkbox"/>	Name	Account	Role
<input type="checkbox"/>	Sylvia Adams	sylvia	Administrator
<input type="checkbox"/>	Gloria Martinez	gloria	Member
<input type="checkbox"/>	Tony Anteater	tony	Member

1 - 3 of 3 users

SAVE CANCEL

- g Wählen Sie für die designierten Administratoren **Administrator** im Dropdown-Menü **Rolle zuweisen** aus und geben Sie die erforderliche E-Mail-Adresse an.
- h Klicken Sie auf die Registerkarte **Bereitstellung** und fügen Sie eine oder mehrere Cloud-Zonen hinzu.

Wenn die Cloud-Vorlagenentwickler, die Teil dieses Projekts sind, eine Vorlage bereitstellen, wird sie an die in den Cloud-Zonen verfügbaren Ressourcen bereitgestellt. Sie müssen sicherstellen, dass die Ressourcen der Cloud-Zonen den Anforderungen der Vorlagen des Projektentwicklungsteams entsprechen.

- i Wiederholen Sie den Vorgang, um das Projekt „PayrollAppDev“ mit den erforderlichen Benutzern und einem Administrator hinzuzufügen.

- 4 Stellen Sie dem Dienstbenutzer die erforderlichen Anmeldeinformationen zur Verfügung und vergewissern Sie sich, dass die Mitglieder jedes Projekts die folgenden Aufgaben ausführen können.
 - a Öffnen Sie vRealize Automation Cloud Assembly.
 - b Zeigen Sie die Infrastruktur über alle Projekte hinweg an.
 - c Erstellen Sie eine Cloud-Vorlage für das Projekt, bei dem sie Mitglied sind.
 - d Stellen Sie die Cloud-Vorlage für die im Projekt definierten Cloud-Zonen-Ressourcen bereit.
 - e Verwalten Sie ihre Bereitstellungen.
- 5 Weisen Sie Ihren Cloud-Vorlagen-Entwicklerbenutzern Organisationsmitglied-Rollen zu.

Wenn Sie Anweisungen benötigen, finden Sie weitere Informationen im [Benutzerrollen-Anwendungsbeispiel 1: Einrichten von vRealize Automation-Benutzerrollen zur Unterstützung eines kleinen Anwendungsentwicklungsteams](#).
- 6 Weisen Sie einem Katalogadministrator, Katalogverbrauchern und Cloud-Vorlagenentwicklern ihrer Tätigkeit entsprechende Rollen zu.
 - a Klicken Sie auf **Dienstzugriff hinzufügen**.
 - b Konfigurieren Sie den Katalogadministrator mit folgendem Wert.

Diese Rolle können Sie, der Cloud-Administrator selbst oder jemand anders aus dem Anwendungsentwicklungsteam sein.

Dienst	Rolle
vRealize Automation Service Broker	vRealize Automation Service Broker-Administrator

- c Konfigurieren Sie die Cloud-Vorlagenverbraucher mit dem folgenden Wert.

Dienst	Rolle
vRealize Automation Service Broker	vRealize Automation Service Broker-Benutzer

Identity & Access Management

Active Users Enterprise Groups

Edit Roles

You are editing the roles of the user **Gloria Martinez** (gloria@coke.sqa-horizon.local)

Assign Organization Roles Organization Member ▾

Assign Service Roles ⓘ

Service Broker ▾
with roles
Service Broker User ▾
X

[+ ADD SERVICE ACCESS](#)

- d Konfigurieren Sie die Cloud-Vorlagenentwickler mit dem folgenden Wert.

Dienst	Rolle
Cloud AssemblyvRealize Automation Cloud Assembly	vRealize Automation Cloud Assembly-Benutzer

- 7 Erstellen Sie Projekte in vRealize Automation Cloud Assembly, die Sie zum Gruppieren von Ressourcen und Benutzern verwenden.

In diesem Anwendungsbeispiel erstellen Sie zwei Projekte. Das erste Projekt ist PersonnelAppDev und das zweite ist PayrollAppDev.

Wenn Sie Anweisungen benötigen, finden Sie weitere Informationen im [Anwendungsbeispiel für Benutzerrollen 2: Einrichten von vRealize Automation-Benutzerrollen zur Unterstützung größerer Entwicklungsteams und des Katalogs](#).

- 8 Erstellen Sie Cloud-Vorlagen und geben Sie sie für jedes Projektteam frei.

Wenn Sie Anweisungen benötigen, finden Sie weitere Informationen im [Benutzerrollen-Anwendungsbeispiel 1: Einrichten von vRealize Automation-Benutzerrollen zur Unterstützung eines kleinen Anwendungsentwicklungsteams](#).

9 Importieren Sie eine vRealize Automation Cloud Assembly Cloud-Vorlage in vRealize Automation Service Broker.

Sie müssen sich als Benutzer mit der vRealize Automation Service Broker-Administratorrolle anmelden.

- a Melden Sie sich als Benutzer mit der vRealize Automation Service Broker-Administratorrolle an.
- b Klicken Sie in der Konsole auf vRealize Automation Service Broker.
- c Wählen Sie **Inhalt und Richtlinien > Inhaltsquellen** aus und klicken Sie auf **Neu**.

- d Wählen Sie **Cloud Assembly-Cloud-Vorlage**.
 - e Geben Sie **PersonnelAppImport** als den Namen ein.
 - f Wählen Sie im Dropdown-Menü **Quellprojekt** die Option „PersonnelAppDev“ aus und klicken Sie auf **Validieren**.
 - g Wenn die Quelle validiert wird, klicken Sie auf **Erstellen und importieren**.
 - h Wiederholen Sie den Vorgang für PayrollAppDev unter Verwendung von PayrollAppImport als Namen der Inhaltsquelle.
- 10 Geben Sie eine importierte Cloud-Vorlage für ein Projekt frei.
- Obwohl die Cloud-Vorlage bereits mit einem Projekt verknüpft ist, müssen Sie sie in vRealize Automation Service Broker freigeben, um sie im Katalog verfügbar zu machen.
- a Fahren Sie als Benutzer mit der vRealize Automation Service Broker-Administratorrolle fort.
 - b Wählen Sie in vRealize Automation Service Broker **Inhalt und Richtlinien > Inhaltsfreigabe** aus.
 - c Wählen Sie das Projekt **PersonnelAppDev** aus, das die Benutzer enthält, die in der Lage sein müssen, die Cloud-Vorlage aus dem Katalog bereitzustellen.

- d Klicken Sie auf **Elemente hinzufügen** und wählen Sie dann die Cloud-Vorlage **PersonnelApp** aus, die für die Projektmitglieder freigegeben werden soll.

Share Items with PersonnelAppDev ×

Select the templates to share with the project members. ⓘ

CONTENT SOURCES Filter... ↻

<input checked="" type="checkbox"/>	Items Shared with this Project	Description
<input checked="" type="checkbox"/>	PersonnelAppImport	
	WebApp for Personnel	


☒ 1 1 item(s)

CANCEL SAVE

- e Klicken Sie auf **Speichern**.
- 11 Stellen Sie sicher, dass die Cloud-Vorlage im vRealize Automation Service Broker-Katalog für die Projektmitglieder verfügbar ist.
- a Fordern Sie ein Projektmitglied auf, sich anzumelden und auf die Registerkarte **Katalog** zu klicken.

Catalog Items 1 item ⌵

Search



WebApp for Perso...
VMware Cloud Templates

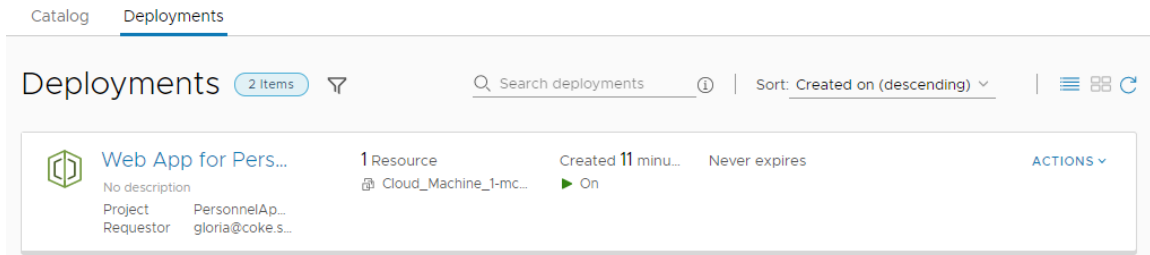
Projects: PersonnelAppDev

[REQUEST](#)

- b Klicken Sie auf der Karte für die Cloud-Vorlage **PersonnelApp** auf „Anfordern“.
- c Füllen Sie das Formular aus und klicken Sie auf **Senden**.

12 Stellen Sie sicher, dass das Projektmitglied den Bereitstellungsvorgang überwachen kann.

- a Fordern Sie das Projektmitglied auf, auf die Registerkarte **Bereitstellungen** zu klicken und nach seiner Bereitstellungsanforderung zu suchen.



- b Nachdem die Cloud-Vorlage bereitgestellt ist, überprüfen Sie, dass der anfordernde Benutzer auf die Anwendung zugreifen kann.

13 Wiederholen Sie den Vorgang für die zusätzlichen Projekte.

Ergebnisse

Da in diesem Anwendungsbeispiel die Cloud-Vorlagenentwicklung an die Entwickler delegiert werden muss, fügen Sie weitere Organisationsmitglieder hinzu. Sie haben sie als vRealize Automation Cloud Assembly-Benutzer festgelegt. Anschließend haben Sie sie zu Mitgliedern relevanter Projekte gemacht, sodass sie Cloud-Vorlagen erstellen und bereitstellen können. Als Projektmitglieder können sie die Infrastruktur, die weiterhin Sie verwalten, nicht sehen oder ändern, aber Sie haben ihnen vollständige Dienst-Viewer-Berechtigungen erteilt, damit sie die Einschränkungen der Infrastruktur verstehen können, für die sie Blueprints entwerfen.

In diesem Anwendungsbeispiel konfigurieren Sie Benutzer mit verschiedenen Rollen, darunter den vRealize Automation Service Broker-Administrator und Benutzer. Anschließend stellen Sie die Nicht-Entwickler-Benutzer mit dem vRealize Automation Service Broker-Katalog bereit.

Nächste Schritte

Informationen zum Definieren und Zuweisen benutzerdefinierter Rollen zu Benutzern finden Sie unter [Anwendungsbeispiel für Benutzerrolle 3: Einrichten benutzerdefinierter vRealize Automation-Benutzerrollen zur Optimierung von Systemrollen](#).

Anwendungsbeispiel für Benutzerrolle 3: Einrichten benutzerdefinierter vRealize Automation-Benutzerrollen zur Optimierung von Systemrollen

Als vRealize Automation-Organisationsbesitzer oder -Dienstadministrator verwalten Sie den Benutzerzugriff mithilfe der Organisations- und Dienstsysteemrollen. Sie möchten jedoch auch benutzerdefinierte Rollen für diese ausgewählten Benutzer erstellen und Aufgaben ausführen oder Inhalte anzeigen, die sich außerhalb der Systemrollen befinden.

In diesem Szenario wird davon ausgegangen, dass Sie mit den Rollen für Dienstbenutzer und Viewer sowie mit den Rollen für Projektmitglieder und Viewer vertraut sind, die in Anwendungsbeispiel 2 definiert sind. Sie stellen fest, dass diese Rollen restriktiver sind als die Dienst- und Projektadministratorrollen in Anwendungsbeispiel 1. Zu diesem Zeitpunkt haben Sie

bestimmte lokale Anwendungsbeispiele ermittelt, in denen einige Benutzer uneingeschränkte Verwaltungsberechtigungen für bestimmte Funktionen, andere Benutzer Leseberechtigungen und wiederum andere überhaupt keine Berechtigungen aufweisen. Sie verwenden benutzerdefinierte Rollen, um diese Berechtigungen zu definieren.

Dieses Anwendungsbeispiel basiert auf drei möglichen lokalen Anwendungsbeispielen. In diesem Verfahren erhalten Sie Anweisungen zum Erstellen von Berechtigungen für die folgenden benutzerdefinierten Rollen.

- **Eingeschränkter Infrastrukturadministrator.** Bestimmte Dienstbenutzer, die nicht als Dienstadministratoren fungieren, sollen umfassendere Infrastrukturberechtigungen erhalten. Als Administrator möchten Sie, dass diese Benutzer Cloud-Zonen, Images und Typen einrichten. Darüber hinaus sollen sie in der Lage sein, erkannte Ressourcen zu integrieren und zu verwalten. Beachten Sie, dass diese Benutzer keine Cloud-Konten oder Integrationen hinzufügen können. Sie können ausschließlich die Infrastruktur für diese Endpoints definieren.
- **Erweiterbarkeitsentwickler.** Bestimmte Dienstbenutzer sollen uneingeschränkte Berechtigungen zur Verwendung der Erweiterbarkeitsaktionen und Abonnements im Rahmen der Cloud-Vorlagenentwicklung für ihr Projektteam und für andere Projekte erhalten. Sie entwickeln auch benutzerdefinierte Ressourcentypen und benutzerdefinierte Aktionen für mehrere Projekte.
- **XaaS-Entwickler.** Bestimmte Dienstbenutzer sollen uneingeschränkte Berechtigungen zum Entwickeln von benutzerdefinierten Ressourcentypen und benutzerdefinierten Aktionen für mehrere Projekte erhalten.
- **Fehlerbehebung bei Bereitstellungen.** Ihren Projektadministratoren sollen Berechtigungen erteilt werden, die sie zur Fehlerbehebung und zur Durchführung der Ursachenanalyse bei fehlgeschlagenen Bereitstellungen benötigen. Sie erteilen ihnen Berechtigungen für nicht destruktive oder kostengünstigere Kategorien wie z. B. Image- und Typzuordnungen. Darüber hinaus sollen die Projektadministratoren berechtigt sein, Genehmigungen und Tag-2-Richtlinien im Rahmen der Rolle zur Fehlerbehebung bei fehlgeschlagenen Bereitstellungen festzulegen.

Voraussetzungen

- Überprüfen Sie die Tabellen mit den Dienst- und Projektrollen für vRealize Automation Cloud Assembly und vRealize Automation Service Broker in [Definition der vRealize Automation-Benutzerrollen](#). Sie benötigen Einblick in die Möglichkeiten der Benutzerrollen in diesen Diensten.
- Befassen Sie sich mit den Beschreibungen unter [Benutzerdefinierte Benutzerrollen in vRealize Automation](#), um weitere Informationen zur Optimierung der Berechtigungen für Ihre Benutzer zu erhalten.
- Sehen Sie sich den ersten Anwendungsfall an, damit Sie die Organisationsrollen und die Dienstadministratorrollen verstehen. Weitere Informationen hierzu finden Sie unter [Benutzerrollen-Anwendungsbeispiel 1: Einrichten von vRealize Automation-Benutzerrollen zur Unterstützung eines kleinen Anwendungsentwicklungsteams](#).

- Im zweiten Anwendungsbeispiel können Sie sich mit den Rollen für Dienstbenutzer und Projektmitglieder vertraut machen. Weitere Informationen hierzu finden Sie unter [Anwendungsbeispiel für Benutzerrollen 2: Einrichten von vRealize Automation-Benutzerrollen zur Unterstützung größerer Entwicklungsteams und des Katalogs](#).
- Machen Sie sich mit vRealize Automation Service Broker vertraut. Weitere Informationen finden Sie unter [Hinzufügen von Inhalt zum Katalog](#).

Verfahren

- 1 Weisen Sie Ihren Cloud-Vorlagen-Entwicklerbenutzern Organisationsmitglied-Rollen zu.

Wenn Sie Anweisungen benötigen, finden Sie weitere Informationen im [Benutzerrollen-Anwendungsbeispiel 1: Einrichten von vRealize Automation-Benutzerrollen zur Unterstützung eines kleinen Anwendungsentwicklungsteams](#).

- 2 Weisen Sie den Cloud-Vorlagenentwicklern und Katalogverbrauchern die Dienstrollen vRealize Automation Cloud Assembly und vRealize Automation Service Broker zu.

Wenn Sie Anweisungen benötigen, finden Sie weitere Informationen im [Anwendungsbeispiel für Benutzerrollen 2: Einrichten von vRealize Automation-Benutzerrollen zur Unterstützung größerer Entwicklungsteams und des Katalogs](#).

- 3 Erstellen Sie Projekte in vRealize Automation Cloud Assembly, die Sie zum Gruppieren von Ressourcen und Benutzern verwenden.

Die folgenden Schritte für die benutzerdefinierten Rollen enthalten auch Projektrollen.

Wenn Sie Anweisungen zum Erstellen von Projekten benötigen, finden Sie weitere Informationen im [Anwendungsbeispiel für Benutzerrollen 2: Einrichten von vRealize Automation-Benutzerrollen zur Unterstützung größerer Entwicklungsteams und des Katalogs](#).

- 4 Erstellen Sie Cloud-Vorlagen und geben Sie sie für jedes Projektteam frei.

Wenn Sie Anweisungen benötigen, finden Sie weitere Informationen im [Benutzerrollen-Anwendungsbeispiel 1: Einrichten von vRealize Automation-Benutzerrollen zur Unterstützung eines kleinen Anwendungsentwicklungsteams](#).

- 5 Melden Sie sich bei vRealize Automation Cloud Assembly als Dienstadministrator an und wählen Sie **Infrastruktur > Verwaltung > Benutzerdefinierte Rollen** aus.

- 6 Erstellen Sie eine Rolle vom Typ „Eingeschränkter Infrastrukturadministrator“.

In diesem Beispiel gibt es einen Benutzer namens Tony, der sich mit der Einrichtung von Infrastrukturen für verschiedene Projekte besonders gut auskennt. Dennoch soll Tony keine uneingeschränkten Dienstberechtigungen erhalten. Stattdessen erstellt Tony die

Kerninfrastruktur, die die Arbeit aller Projekte unterstützt. Sie erteilen ihm eingeschränkte Berechtigungen zur Verwaltung der Infrastruktur. Tony oder ein externer Auftragsnehmer verfügen unter Umständen über vergleichbare Berechtigungen, um erkannte Maschinen zu integrieren und diese in vRealize Automation zu verwalten.

- a Fügen Sie Tony als Dienstbenutzer und Viewer zu vRealize Automation Cloud Assembly hinzu.

Mithilfe der Viewer-Berechtigungen kann Tony die zugrunde liegenden Cloud-Konten und Integrationen anzeigen, wenn er Probleme beheben muss. Änderungen können von ihm jedoch nicht vorgenommen werden.

- b Erstellen Sie ein Projekt und fügen Sie Tony als Projektmitglied hinzu.
- c Wählen Sie zum Erstellen der benutzerdefinierten Rolle die Optionen **Infrastruktur > Verwaltung > Benutzerdefinierte Rollen** aus und klicken Sie auf **Neue benutzerdefinierte Rolle**.
- d Geben Sie den Namen **Eingeschränkter Infrastrukturadministrator** ein und wählen Sie die folgenden Berechtigungen aus.

Berechtigung	Mögliche Aktionen des Benutzers
Infrastruktur > Cloud-Zonen verwalten	Cloud-Zonen erstellen, aktualisieren und löschen.
Infrastruktur > Typzuordnungen verwalten	Typzuordnungen erstellen, aktualisieren und löschen.
Infrastruktur > Image-Zuordnungen verwalten	Image-Zuordnungen erstellen, aktualisieren und löschen.

- e Klicken Sie auf **Erstellen**.
- f Wählen Sie auf der Seite „Benutzerdefinierte Rollen“ die Rolle „Eingeschränkter Infrastrukturadministrator“ aus und klicken Sie auf **Zuweisen**.
- g Geben Sie Tonys E-Mail-Konto ein und klicken Sie auf **Hinzufügen**.
Geben Sie beispielsweise Tony@ihrunternehmen.com ein.
Sie können auch alle definierten Active Directory-Benutzergruppen eingeben.
- h Tony muss bei der Anmeldung sicherstellen, dass er Werte in den durch die benutzerdefinierte Rolle festgelegten Bereichen hinzufügen, bearbeiten und löschen kann.

7 Erstellen Sie eine Rolle vom Typ „Erweiterbarkeitsentwickler“.

In diesem Beispiel verfügen Sie über zwei Cloud-Vorlagenentwickler, Sylvia und Igor, die mit der Verwendung von Erweiterbarkeitsaktionen und Abonnements zur Verwaltung täglicher Entwicklungsaufgaben vertraut sind. Da sich Sylvia und Igor auch mit vRealize Orchestrator

auskennen, können Sie sie mit der Bereitstellung benutzerdefinierter Ressourcen und Aktionen für verschiedene Projekte beauftragen. Sie erteilen ihnen zusätzliche Berechtigungen zur Verwaltung von Erweiterbarkeit, indem Sie benutzerdefinierte Ressourcen und Aktionen sowie Erweiterbarkeitsaktionen und Abonnements verwalten.

- a Fügen Sie Sylvia und Igor als vRealize Automation Cloud Assembly-Benutzer hinzu.
- b Fügen Sie sie als Mitglieder der Projekte hinzu, in denen sie ihre Kenntnisse im Bereich Erweiterbarkeit zur Verfügung stellen können.
- c Erstellen Sie eine benutzerdefinierte Benutzerrolle mit der Bezeichnung **Erweiterbarkeitsentwickler** und wählen Sie die folgenden Berechtigungen aus.

Berechtigung	Mögliche Aktionen des Benutzers
XaaS > Benutzerdefinierte Ressourcen verwalten	Benutzerdefinierte Ressourcen erstellen, aktualisieren oder löschen.
XaaS > Ressourcenaktionen verwalten	Benutzerdefinierte Aktionen erstellen, aktualisieren oder löschen.
Erweiterbarkeit > Erweiterbarkeitsressourcen verwalten	Erweiterbarkeitsaktionen und Abonnements erstellen, aktualisieren oder löschen. Abonnements deaktivieren. Aktionsausführungen abbrechen und löschen.

- d Klicken Sie auf **Erstellen**.
 - e Weisen Sie Sylvia und Igor die Rolle „Erweiterbarkeitsentwickler“ zu.
 - f Stellen Sie sicher, dass Sylvia und Igor die benutzerdefinierten Ressourcen und Aktionen sowie die verschiedenen Optionen auf der Registerkarte „Erweiterbarkeit“ verwalten können.
- 8** Erstellen Sie eine Rolle vom Typ „Fehlerbehebung bei Bereitstellung“.

In diesem Beispiel erteilen Sie den Projektadministratoren erweiterte Berechtigungen, damit diese Bereitstellungsfehler für ihre Teams beheben können.

- a Fügen Sie die Projektadministratoren Shauna, Pratap und Wei als vRealize Automation Cloud Assembly- und vRealize Automation Service Broker-Dienstbenutzer hinzu.
- b Fügen Sie sie in den jeweiligen Projekten als Projektadministratoren hinzu.

- c Erstellen Sie eine benutzerdefinierte Benutzerrolle mit der Bezeichnung **Fehlerbehebung bei Bereitstellung** und wählen Sie die folgenden Berechtigungen aus.

Berechtigung	Mögliche Aktionen des Benutzers
Infrastruktur > Typzuordnungen verwalten	Typzuordnungen erstellen, aktualisieren und löschen.
Infrastruktur > Image-Zuordnungen verwalten	Image-Zuordnungen erstellen, aktualisieren und löschen.
Bereitstellungen > Bereitstellungen verwalten	Zeigen Sie projektübergreifend alle Bereitstellungen an und führen Sie alle Tag-2-Aktionen für Bereitstellungen und Bereitstellungskomponenten aus.
Richtlinie > Richtlinien verwalten	Richtliniendefinitionen erstellen, aktualisieren oder löschen.

- d Klicken Sie auf **Erstellen**.
- e Weisen Sie Shauna, Pratap und Wei die Rolle „Fehlerbehebung bei Bereitstellung“ zu.
- f Stellen Sie sicher, dass sie die Typzuordnungen, die Image-Zuordnungen und die Richtlinien in vRealize Automation Service Broker verwalten können.

Ergebnisse

In diesem Anwendungsbeispiel konfigurieren Sie verschiedene Benutzer mit verschiedenen Rollen, einschließlich benutzerdefinierter Rollen, die die jeweiligen Dienst- und Projektrollen erweitern.

Nächste Schritte

Erstellen Sie benutzerdefinierte Rollen, die sich für Ihre lokalen Anwendungsbeispiele eignen.

Hinzufügen von Cloud-Konten zu vRealize Automation Cloud Assembly

Bei Cloud-Konten handelt es sich um die konfigurierten Berechtigungen, die von vRealize Automation Cloud Assembly zum Erfassen von Daten aus den Regionen oder Datencentern und zum Bereitstellen von Cloud-Vorlagen für diese Regionen verwendet werden.

Die erfassten Daten enthalten die Regionen, die Sie später mit Cloud-Zonen verknüpfen.

Wenn Sie Cloud-Zonen, Zuordnungen und Profile zu einem späteren Zeitpunkt konfigurieren, wählen Sie das Cloud-Konto aus, dem sie zugeordnet sind.

Als Cloud-Administrator erstellen Sie Cloud-Konten für die Projekte, in denen Teammitglieder arbeiten. Ressourceninformationen, wie z. B. Inhalte zu Netzwerk und Sicherheit, Berechnungen, Speicher und Tags, werden aus Ihren Cloud-Konten abgerufen.

Hinweis Wenn das Cloud-Konto über zugeordnete Maschinen verfügt, die bereits in der Region bereitgestellt wurden, können Sie diese Maschinen mithilfe eines Onboarding-Plans in die vRealize Automation Cloud Assembly-Verwaltung integrieren. Weitere Informationen hierzu finden Sie unter [Definition von Onboarding-Plänen in vRealize Automation Cloud Assembly](#).

Wenn Sie ein in einer Bereitstellung verwendetes Cloud-Konto entfernen, werden zu dieser Bereitstellung gehörende Ressourcen nicht mehr verwaltet.

Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich

Zum Arbeiten mit und Konfigurieren von Cloud-Konten in vRealize Automation müssen Sie sicherstellen, dass Sie über die folgenden Anmeldedaten verfügen.

Erforderliche Anmeldedaten für Cloud-Konto

Aufgabe	Voraussetzungen
Registrieren und Anmelden bei vRealize Automation Cloud Assembly.	<p>Eine VMware-ID.</p> <ul style="list-style-type: none"> ■ Einrichten eines My VMware-Kontos unter Verwendung Ihrer geschäftlichen E-Mail-Adresse.
Herstellen einer Verbindung zu vRealize Automation-Diensten	<p>Offener HTTPS-Port 443 für ausgehenden Datenverkehr mit Zugriff über die Firewall auf:</p> <ul style="list-style-type: none"> ■ *.vmwareidentity.com ■ gaz.csp-vidm-prod.com ■ *.vmware.com <p>Weitere Informationen zu Ports und Protokollen finden Sie unter VMware-Ports und -Protokolle.</p> <p>Weitere Informationen zu den erforderlichen Ports und Protokollen finden Sie unter Portanforderungen.</p>

Aufgabe	Voraussetzungen
Hinzufügen eines Amazon Web Services (AWS)-Cloud-Kontos	<p>Bereitstellen eines Hauptbenutzerkontos mit Lese- und Schreibberechtigungen. Das Benutzerkonto muss Mitglied der Zugriffsrichtlinie für Hauptbenutzer (PowerUserAccess) im AWS-IAM-System (Identity and Access Management) sein.</p> <ul style="list-style-type: none"> ■ 20-stellige Zugriffsschlüssel-ID und entsprechender geheimer Zugriffsschlüssel <p>Wenn Sie einen externen HTTP-Internet-Proxy verwenden, muss dieser für IPv4 konfiguriert sein.</p> <p>Möglicherweise sind für die aktionsbasierte Erweiterbarkeit (ABX) und die externe IPAM-Integration von vRealize Automation zusätzliche Berechtigungen erforderlich.</p> <p>Die folgenden AWS-Berechtigungen werden empfohlen, um automatische Skalierungsfunktionen zuzulassen:</p> <ul style="list-style-type: none"> ■ Aktionen für die automatische Skalierung: <ul style="list-style-type: none"> ■ autoscaling:DescribeAutoScalingInstances ■ autoscaling:AttachInstances ■ autoscaling>DeleteLaunchConfiguration ■ autoscaling:DescribeAutoScalingGroups ■ autoscaling>CreateAutoScalingGroup ■ autoscaling:UpdateAutoScalingGroup ■ autoscaling>DeleteAutoScalingGroup ■ autoscaling:DescribeLoadBalancers ■ Ressourcen für die automatische Skalierung: <ul style="list-style-type: none"> ■ * <p>Stellen Sie alle Berechtigungen für Ressourcen für die automatische Skalierung bereit.</p> <p>Die folgenden Berechtigungen sind erforderlich, damit die Funktionen des AWS Security Token Service (AWS STS) temporäre Anmeldedaten mit eingeschränkten Rechten für AWS-Identität und -Zugriff unterstützen können:</p> <ul style="list-style-type: none"> ■ AWS STS-Ressourcen: <ul style="list-style-type: none"> ■ * <p>Stellen Sie alle Berechtigungen für STS-Ressourcen bereit.</p> <p>Die folgenden AWS-Berechtigungen sind erforderlich, um EC2-Funktionen zuzulassen:</p> <ul style="list-style-type: none"> ■ EC2-Aktionen: <ul style="list-style-type: none"> ■ ec2:AttachVolume ■ ec2:AuthorizeSecurityGroupIngress ■ ec2>DeleteSubnet ■ ec2>DeleteSnapshot ■ ec2:DescribeInstances ■ ec2>DeleteTags ■ ec2:DescribeRegions ■ ec2:DescribeVolumesModifications ■ ec2>CreateVpc ■ ec2:DescribeSnapshots ■ ec2:DescribeInternetGateways ■ ec2>DeleteVolume ■ ec2:DescribeNetworkInterfaces ■ ec2:StartInstances ■ ec2:DescribeAvailabilityZones ■ ec2:CreateInternetGateway

Aufgabe	Voraussetzungen
	<ul style="list-style-type: none"> ■ ec2:CreateSecurityGroup ■ ec2:DescribeVolumes ■ ec2:CreateSnapshot ■ ec2:ModifyInstanceAttribute ■ ec2:DescribeRouteTables ■ ec2:DescribeInstanceType ■ ec2:DescribeInstanceTypeOfferings ■ ec2:DescribeInstanceState ■ ec2:DetachVolume ■ ec2:RebootInstances ■ ec2:AuthorizeSecurityGroupEgress ■ ec2:ModifyVolume ■ ec2:TerminateInstances ■ ec2:DescribeSpotFleetRequestHistory ■ ec2:DescribeTags ■ ec2:CreateTags ■ ec2:RunInstances ■ ec2:DescribeNatGateways ■ ec2:StopInstances ■ ec2:DescribeSecurityGroups ■ ec2:CreateVolume ■ ec2:DescribeSpotFleetRequests ■ ec2:DescribeImages ■ ec2:DescribeVpcs ■ ec2>DeleteSecurityGroup ■ ec2>DeleteVpc ■ ec2:CreateSubnet ■ ec2:DescribeSubnets ■ ec2:RequestSpotFleet <hr/> <p>Hinweis Die SpotFleet-Anforderungsberechtigung ist für die aktionsbasierte Erweiterbarkeit (ABX) oder die externen IPAM-Integrationen von vRealize Automation nicht erforderlich.</p> <hr/> <ul style="list-style-type: none"> ■ EC2-Ressourcen: <ul style="list-style-type: none"> ■ * <p>Stellen Sie alle Berechtigungen für EC2-Ressourcen bereit.</p> <p>Die folgenden AWS-Berechtigungen sind erforderlich, um Funktionen für den elastischen Lastausgleich zuzulassen:</p> <ul style="list-style-type: none"> ■ Lastausgleichsdienstaktionen: <ul style="list-style-type: none"> ■ elasticloadbalancing:DeleteLoadBalancer ■ elasticloadbalancing:DescribeLoadBalancers ■ elasticloadbalancing:RemoveTags ■ elasticloadbalancing:CreateLoadBalancer ■ elasticloadbalancing:DescribeTags ■ elasticloadbalancing:ConfigureHealthCheck ■ elasticloadbalancing:AddTags

Aufgabe	Voraussetzungen
	<ul style="list-style-type: none"> ■ elasticloadbalancing:CreateTargetGroup ■ elasticloadbalancing>DeleteLoadBalancerListeners ■ elasticloadbalancing:DeregisterInstancesFromLoadBalancer ■ elasticloadbalancing:RegisterInstancesWithLoadBalancer ■ elasticloadbalancing>CreateLoadBalancerListeners ■ Lastausgleichsdienstressourcen: <ul style="list-style-type: none"> ■ * <p>Stellen Sie alle Berechtigungen für Lastausgleichsdienstressourcen bereit.</p> <p>Die folgenden Berechtigungen für die Identitäts- und Zugriffsverwaltung (IAM) von AWS können aktiviert werden, sind aber nicht erforderlich:</p> <ul style="list-style-type: none"> ■ iam:SimulateCustomPolicy ■ iam:GetUser ■ iam:ListUserPolicies ■ iam:GetUserPolicy ■ iam:ListAttachedUserPolicies ■ iam:GetPolicyVersion ■ iam:ListGroupsForUser ■ iam:ListGroupPolicies ■ iam:GetGroupPolicy ■ iam:ListAttachedGroupPolicies ■ iam:ListPolicyVersions

Aufgabe	Voraussetzungen
Hinzufügen eines Microsoft Azure-Cloud-Kontos	<p>Konfigurieren Sie eine Instanz von Microsoft Azure und rufen Sie ein gültiges Microsoft Azure-Abonnement ab, dessen Abonnement-ID verwendet werden kann.</p> <p>Erstellen Sie eine Active Directory-Anwendung entsprechend der Beschreibung unter Vorgehensweise für die Verwendung des Portals zum Erstellen einer Azure AD-Anwendung und eines Dienstprinzipals für den Zugriff auf Ressourcen in der Microsoft Azure-Produktdokumentation.</p> <p>Wenn Sie einen externen HTTP-Internet-Proxy verwenden, muss dieser für IPv4 konfiguriert sein.</p> <p>Notieren Sie sich die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Abonnement-ID <p>Ermöglicht den Zugriff auf Ihre Microsoft Azure-Abonnements.</p> ■ Mandanten-ID <p>Der Autorisierungs-Endpoint für die Active Directory-Anwendungen, die Sie in Ihrem Microsoft Azure-Konto erstellen.</p> ■ Client-Anwendungs-ID <p>Bietet Zugriff auf Microsoft Active Directory in Ihrem individuellen Microsoft Azure-Konto.</p> ■ Geheimer Schlüssel der Client-Anwendung <p>Der eindeutige geheime Schlüssel, der zur Kopplung mit Ihrer Client-Anwendungs-ID erzeugt wurde.</p> <p>Die folgenden Berechtigungen sind für das Erstellen und Validieren von Microsoft Azure-Cloud-Konten erforderlich:</p> <ul style="list-style-type: none"> ■ Microsoft Compute <ul style="list-style-type: none"> ■ Microsoft.Compute/virtualMachines/extensions/write ■ Microsoft.Compute/virtualMachines/extensions/read ■ Microsoft.Compute/virtualMachines/extensions/delete ■ Microsoft.Compute/virtualMachines/deallocate/action ■ Microsoft.Compute/virtualMachines/delete ■ Microsoft.Compute/virtualMachines/powerOff/action ■ Microsoft.Compute/virtualMachines/read ■ Microsoft.Compute/virtualMachines/restart/action ■ Microsoft.Compute/virtualMachines/start/action ■ Microsoft.Compute/virtualMachines/write ■ Microsoft.Compute/availabilitySets/write ■ Microsoft.Compute/availabilitySets/read ■ Microsoft.Compute/availabilitySets/delete ■ Microsoft.Compute/disks/delete ■ Microsoft.Compute/disks/read ■ Microsoft.Compute/disks/write ■ Microsoft Network <ul style="list-style-type: none"> ■ Microsoft.Network/loadBalancers/backendAddressPools/join/action ■ Microsoft.Network/loadBalancers/delete ■ Microsoft.Network/loadBalancers/read ■ Microsoft.Network/loadBalancers/write ■ Microsoft.Network/networkInterfaces/join/action ■ Microsoft.Network/networkInterfaces/read ■ Microsoft.Network/networkInterfaces/write ■ Microsoft.Network/networkInterfaces/delete

Aufgabe	Voraussetzungen
	<ul style="list-style-type: none"> ■ Microsoft.Network/networkSecurityGroups/join/action ■ Microsoft.Network/networkSecurityGroups/read ■ Microsoft.Network/networkSecurityGroups/write ■ Microsoft.Network/networkSecurityGroups/delete ■ Microsoft.Network/publicIPAddresses/delete ■ Microsoft.Network/publicIPAddresses/join/action ■ Microsoft.Network/publicIPAddresses/read ■ Microsoft.Network/publicIPAddresses/write ■ Microsoft.Network/virtualNetworks/read ■ Microsoft.Network/virtualNetworks/subnets/delete ■ Microsoft.Network/virtualNetworks/subnets/join/action ■ Microsoft.Network/virtualNetworks/subnets/read ■ Microsoft.Network/virtualNetworks/subnets/write ■ Microsoft.Network/virtualNetworks/write ■ Microsoft Resources <ul style="list-style-type: none"> ■ Microsoft.Resources/subscriptions/resourcegroups/delete ■ Microsoft.Resources/subscriptions/resourcegroups/read ■ Microsoft.Resources/subscriptions/resourcegroups/write ■ Microsoft Storage <ul style="list-style-type: none"> ■ Microsoft.Storage/storageAccounts/delete ■ Microsoft.Storage/storageAccounts/listKeys/action ■ Microsoft.Storage/storageAccounts/read ■ Microsoft.Storage/storageAccounts/write ■ Microsoft Web <ul style="list-style-type: none"> ■ Microsoft.Web/sites/read ■ Microsoft.Web/sites/write ■ Microsoft.Web/sites/delete ■ Microsoft.Web/sites/config/read ■ Microsoft.Web/sites/config/write ■ Microsoft.Web/sites/config/list/action ■ Microsoft.Web/sites/publishxml/action ■ Microsoft.Web/serverfarms/write ■ Microsoft.Web/serverfarms/delete ■ Microsoft.Web/sites/hostruntime/functions/keys/read ■ Microsoft.Web/sites/hostruntime/host/read ■ Microsoft.web/sites/functions/masterkey/read <p>Wenn Sie Microsoft Azure mit aktionsbasierter Erweiterbarkeit verwenden, sind neben den minimalen Berechtigungen die folgenden Berechtigungen erforderlich:</p> <ul style="list-style-type: none"> ■ Microsoft.Web/sites/read ■ Microsoft.Web/sites/write ■ Microsoft.Web/sites/delete ■ Microsoft.Web/sites/*/action ■ Microsoft.Web/sites/config/read ■ Microsoft.Web/sites/config/write ■ Microsoft.Web/sites/config/list/action

Aufgabe	Voraussetzungen
	<ul style="list-style-type: none">■ Microsoft.Web/sites/publishxml/action■ Microsoft.Web/serverfarms/write■ Microsoft.Web/serverfarms/delete■ Microsoft.Web/sites/hostruntime/functions/keys/read■ Microsoft.Web/sites/hostruntime/host/read■ Microsoft.Web/sites/functions/masterkey/read■ Microsoft.Web/apimanagementaccounts/apis/read■ Microsoft.Authorization/roleAssignments/read■ Microsoft.Authorization/roleAssignments/write■ Microsoft.Authorization/roleAssignments/delete <p>Wenn Sie Microsoft Azure mit aktionsbasierter Erweiterbarkeit mit Erweiterungen verwenden, sind die folgenden Berechtigungen ebenfalls erforderlich:</p> <ul style="list-style-type: none">■ Microsoft.Compute/virtualMachines/extensions/write■ Microsoft.Compute/virtualMachines/extensions/read■ Microsoft.Compute/virtualMachines/extensions/delete

Aufgabe	Voraussetzungen
Hinzufügen eines Google Cloud Platform (GCP)-Cloud-Kontos	<p>Das Cloud-Konto von Google Cloud Platform interagiert mit der Computing-Engine von Google Cloud Platform.</p> <p>Zum Erstellen und Validieren von Google Cloud Platform-Cloud-Konten sind die Anmeldedaten des Projektadministrators und des Projektbesitzers erforderlich.</p> <p>Wenn Sie einen externen HTTP-Internet-Proxy verwenden, muss dieser für IPv4 konfiguriert sein.</p> <p>Der Computing-Engine-Dienst muss aktiviert werden. Verwenden Sie beim Erzeugen des Cloud-Kontos in vRealize Automation das Dienstkonto, das beim Initialisieren der Computing-Engine erstellt wurde.</p> <p>Außerdem sind die folgenden Berechtigungen für die Computing-Engine erforderlich, je nachdem, welche Aktionen der Benutzer durchführen darf:</p> <ul style="list-style-type: none"> ■ <code>roles/compute.admin</code> <p>Bietet vollständige Kontrolle über alle Computing-Engine-Ressourcen.</p> ■ <code>roles/iam.serviceAccountUser</code> <p>Bietet Zugriff auf Benutzer, die VM-Instanzen verwalten, die für die Ausführung als Dienstkonto konfiguriert sind. Gewährt Zugriff auf die folgenden Ressourcen und Dienste:</p> <ul style="list-style-type: none"> ■ <code>compute.*</code> ■ <code>resourceManager.projects.get</code> ■ <code>resourceManager.projects.list</code> ■ <code>serviceUsage.quotas.get</code> ■ <code>serviceUsage.services.get</code> ■ <code>serviceUsage.services.list</code> ■ <code>roles/compute.imageUser</code> <p>Bietet ausschließlich die Berechtigung zum Auflisten und Lesen von Images, jedoch keine anderen Berechtigungen für das Image. Wenn die Rolle „compute.imageUser“ auf Projektebene zugewiesen wird, haben Benutzer die Möglichkeit, alle Images im Projekt aufzulisten. Außerdem können Benutzer Ressourcen (z. B. Instanzen und persistente Festplatten) auf der Basis von Images im Projekt erstellen.</p> <ul style="list-style-type: none"> ■ <code>compute.images.get</code> ■ <code>compute.images.getFromFamily</code> ■ <code>compute.images.list</code> ■ <code>compute.images.useReadOnly</code> ■ <code>resourceManager.projects.get</code> ■ <code>resourceManager.projects.list</code> ■ <code>serviceUsage.quotas.get</code> ■ <code>serviceUsage.services.get</code> ■ <code>serviceUsage.services.list</code> ■ <code>roles/compute.instanceAdmin</code> <p>Bietet Berechtigungen zum Erstellen, Ändern und Löschen von VM-Instanzen. Dazu gehören Berechtigungen zum Erstellen, Ändern und Löschen von Festplatten sowie zum Konfigurieren von abgeschirmten VMBETA-Einstellungen.</p> <p>Erteilen Sie diese Rolle Benutzern, die VM-Instanzen (aber keine Netzwerk- oder Sicherheitseinstellungen oder -instanzen, die als Dienstkonto ausgeführt werden) verwalten, für die Organisation, den Ordner oder das Projekt, welche die Instanzen enthalten, oder für die einzelnen Instanzen.</p> <p>Benutzer, die VM-Instanzen verwalten, welche für die Ausführung als Dienstkonto konfiguriert sind, benötigen zudem die Rolle <code>roles/iam.serviceAccountUser</code>.</p> <ul style="list-style-type: none"> ■ <code>compute.acceleratorTypes</code>

Aufgabe	Voraussetzungen
	<ul style="list-style-type: none"> ■ compute.addresses.get ■ compute.addresses.list ■ compute.addresses.use ■ compute.autoscalers ■ compute.diskTypes ■ compute.disks.create ■ compute.disks.createSnapshot ■ compute.disks.delete ■ compute.disks.get ■ compute.disks.list ■ compute.disks.resize ■ compute.disks.setLabels ■ compute.disks.update ■ compute.disks.use ■ compute.disks.useReadOnly ■ compute.globalAddresses.get ■ compute.globalAddresses.list ■ compute.globalAddresses.use ■ compute.globalOperations.get ■ compute.globalOperations.list ■ compute.images.get ■ compute.images.getFromFamily ■ compute.images.list ■ compute.images.useReadOnly ■ compute.instanceGroupManagers ■ compute.instanceGroups ■ compute.instanceTemplates ■ compute.instances ■ compute.licenses.get ■ compute.licenses.list ■ compute.machineTypes ■ compute.networkEndpointGroups ■ compute.networks.get ■ compute.networks.list ■ compute.networks.use ■ compute.networks.useExternallp ■ compute.projects.get ■ compute.regionOperations.get ■ compute.regionOperations.list ■ compute.regions ■ compute.reservations.get ■ compute.reservations.list ■ compute.subnetworks.get ■ compute.subnetworks.list ■ compute.subnetworks.use

Aufgabe	Voraussetzungen
	<ul style="list-style-type: none"> ■ compute.subnetworks.useExternalIp ■ compute.targetPools.get ■ compute.targetPools.list ■ compute.zoneOperations.get ■ compute.zoneOperations.list ■ compute.zones ■ resourcemanager.projects.get ■ resourcemanager.projects.list ■ serviceusage.quotas.get ■ serviceusage.services.get ■ serviceusage.services.list ■ roles/compute.instanceAdmin.v1 <p>Bietet vollständige Kontrolle über Instanzen, Instanzgruppen, Festplatten, Snapshots und Images der Computing-Engine. Bietet auch Lesezugriff auf alle Netzwerkressourcen der Computing-Engine.</p> <hr/> <p>Hinweis Wenn Sie einem Benutzer diese Rolle auf der Instanzebene zuweisen, kann dieser Benutzer keine neuen Instanzen erstellen.</p> <hr/> <ul style="list-style-type: none"> ■ compute.acceleratorTypes ■ compute.addresses.get ■ compute.addresses.list ■ compute.addresses.use ■ compute.autoscalers ■ compute.backendBuckets.get ■ compute.backendBuckets.list ■ compute.backendServices.get ■ compute.backendServices.list ■ compute.diskTypes ■ compute.disks ■ compute.firewalls.get ■ compute.firewalls.list ■ compute.forwardingRules.get ■ compute.forwardingRules.list ■ compute.globalAddresses.get ■ compute.globalAddresses.list ■ compute.globalAddresses.use ■ compute.globalForwardingRules.get ■ compute.globalForwardingRules.list ■ compute.globalOperations.get ■ compute.globalOperations.list ■ compute.healthChecks.get ■ compute.healthChecks.list ■ compute.httpHealthChecks.get ■ compute.httpHealthChecks.list ■ compute.httpsHealthChecks.get ■ compute.httpsHealthChecks.list

Aufgabe	Voraussetzungen
	<ul style="list-style-type: none"> ■ compute.images ■ compute.instanceGroupManagers ■ compute.instanceGroups ■ compute.instanceTemplates ■ compute.instances ■ compute.interconnectAttachments.get ■ compute.interconnectAttachments.list ■ compute.interconnectLocations ■ compute.interconnects.get ■ compute.interconnects.list ■ compute.licenseCodes ■ compute.licenses ■ compute.machineTypes ■ compute.networkEndpointGroups ■ compute.networks.get ■ compute.networks.list ■ compute.networks.use ■ compute.networks.useExternallp ■ compute.projects.get ■ compute.projects.setCommonInstanceMetadata ■ compute.regionBackendServices.get ■ compute.regionBackendServices.list ■ compute.regionOperations.get ■ compute.regionOperations.list ■ compute.regions ■ compute.reservations.get ■ compute.reservations.list ■ compute.resourcePolicies ■ compute.routers.get ■ compute.routers.list ■ compute.routes.get ■ compute.routes.list ■ compute.snapshots ■ compute.sslCertificates.get ■ compute.sslCertificates.list ■ compute.sslPolicies.get ■ compute.sslPolicies.list ■ compute.sslPolicies.listAvailableFeatures ■ compute.subnetworks.get ■ compute.subnetworks.list ■ compute.subnetworks.use ■ compute.subnetworks.useExternallp ■ compute.targetHttpProxies.get ■ compute.targetHttpProxies.list ■ compute.targetHttpsProxies.get

Aufgabe	Voraussetzungen
	<ul style="list-style-type: none"> ■ compute.targetHttpsProxies.list ■ compute.targetInstances.get ■ compute.targetInstances.list ■ compute.targetPools.get ■ compute.targetPools.list ■ compute.targetSslProxies.get ■ compute.targetSslProxies.list ■ compute.targetTcpProxies.get ■ compute.targetTcpProxies.list ■ compute.targetVpnGateways.get ■ compute.targetVpnGateways.list ■ compute.urlMaps.get ■ compute.urlMaps.list ■ compute.vpnTunnels.get ■ compute.vpnTunnels.list ■ compute.zoneOperations.get ■ compute.zoneOperations.list ■ compute.zones ■ resourcemanager.projects.get ■ resourcemanager.projects.list ■ serviceusage.quotas.get ■ serviceusage.services.get ■ serviceusage.services.list
Hinzufügen eines NSX-T-Cloud-Kontos	<p>Bereitstellen eines Kontos mit den folgenden Lese- und Schreibberechtigungen:</p> <ul style="list-style-type: none"> ■ NSX-T-Enterprise-Administrator-Rolle und -Zugriffsanmeldedaten ■ IP-Adresse oder FQDN von NSX-T <p>Administratoren benötigen <i>außerdem</i> Zugriff auf den vCenter Server. Der folgende Abschnitt <i>Anforderungen des vSphere-Agenten für vCenter-basierte Cloud-Konten</i> auf dieser Seite enthält eine Beschreibung hierzu.</p>
Hinzufügen eines NSX-V-Cloud-Kontos	<p>Bereitstellen eines Kontos mit den folgenden Lese- und Schreibberechtigungen:</p> <ul style="list-style-type: none"> ■ NSX-V-Enterprise-Administrator-Rolle und -Zugriffsanmeldedaten ■ IP-Adresse oder FQDN von NSX-V <p>Administratoren benötigen <i>außerdem</i> Zugriff auf den vCenter Server. Der folgende Abschnitt <i>Anforderungen des vSphere-Agenten für vCenter-basierte Cloud-Konten</i> auf dieser Seite enthält eine Beschreibung hierzu.</p>

Aufgabe	Voraussetzungen
Hinzufügen eines vCenter-Cloud-Kontos	<p>Bereitstellen eines Kontos mit den folgenden Lese- und Schreibberechtigungen:</p> <ul style="list-style-type: none"> ■ IP-Adresse oder FQDN von vCenter <p>Administratoren benötigen <i>außerdem</i> Zugriff auf den vCenter Server. Der folgende Abschnitt <i>Anforderungen des vSphere-Agenten für vCenter-basierte Cloud-Konten</i> auf dieser Seite enthält eine Beschreibung hierzu.</p>
Hinzufügen eines VMC-Cloud-Kontos (VMware Cloud on AWS)	<p>Bereitstellen eines Kontos mit den folgenden Lese- und Schreibberechtigungen:</p> <ul style="list-style-type: none"> ■ Des Kontos „cloudadmin@vmc.local“ oder eines beliebigen Benutzerkontos in der Gruppe „CloudAdmin“ ■ NSX-Enterprise-Administrator-Rolle und -Zugriffsanmeldedaten ■ NSX-Cloud-Administratorzugriff auf die VMware Cloud on AWS-SDDC-Umgebung Ihres Unternehmens ■ Administratorzugriff auf die VMware Cloud on AWS-SDDC-Umgebung Ihres Unternehmens ■ Das VMware Cloud on AWS-API-Token für Ihre VMware Cloud on AWS-Umgebung im VMware Cloud on AWS-Dienst Ihres Unternehmens ■ IP-Adresse oder FQDN von vCenter <p>Administratoren benötigen <i>auch</i> Zugriff auf das vCenter, das von dem VMware Cloud on AWS-Ziel-SDDC verwaltet wird, dessen gesamte Berechtigungen im folgenden Abschnitt <i>Anforderungen des vSphere-Agenten für vCenter-basierte Cloud-Konten</i> auf dieser Seite aufgelistet sind.</p> <p>Weitere Informationen zu den Berechtigungen, die zum Erstellen und Verwenden von VMware Cloud on AWS-Cloud-Konten erforderlich sind, finden Sie unter <i>Verwalten des VMware Cloud on AWS-Datencenters</i> in der VMware Cloud on AWS -Produktdokumentation.</p>

Anforderungen des vSphere-Agenten für vCenter-basierte Cloud-Konten

In der folgenden Tabelle werden die Berechtigungen aufgeführt, die zum Verwalten von VMware Cloud on AWS- und vCenter-Cloud-Konten erforderlich sind. Die Berechtigungen müssen für alle Cluster im vCenter Server und nicht nur für Cluster aktiviert sein, die Endpoints hosten.

Für alle vCenter Server-basierten Cloud-Konten, einschließlich NSX-V, NSX-T, vCenter und VMware Cloud on AWS, muss der Administrator über Anmeldedaten des vSphere-Endpoints oder diejenigen Anmeldedaten verfügen, unter denen der Agent-Dienst in vCenter ausgeführt wird und die administrativen Zugriff auf den Host-vCenter Server bereitstellen.

Weitere Informationen zu den Anforderungen des vSphere-Agenten finden Sie in der [VMware vSphere-Produktdokumentation](#).

Tabelle 3-12. Erforderliche Berechtigungen für vSphere-Agenten zur Verwaltung von vCenter Server-Instanzen

Attributwert	Berechtigung
Datenspeicher	<ul style="list-style-type: none"> ■ Speicher zuteilen ■ Datenspeicher durchsuchen ■ Dateivorgänge auf niedriger Ebene
Datenspeicher-Cluster	Einen Datenspeicher-Cluster konfigurieren
Ordner	<ul style="list-style-type: none"> ■ Ordner erstellen ■ Ordner löschen

Tabelle 3-12. Erforderliche Berechtigungen für vSphere-Agenten zur Verwaltung von vCenter Server-Instanzen (Fortsetzung)

Attributwert	Berechtigung
Global	<ul style="list-style-type: none"> ■ Benutzerdefinierte Attribute verwalten ■ Benutzerdefiniertes Attribut festlegen
Netzwerk	Netzwerk zuweisen
Berechtigungen	Berechtigung ändern
Ressource	<ul style="list-style-type: none"> ■ VM zu Ressourcenpool zuweisen ■ Ausgeschaltete virtuelle Maschine migrieren ■ Einschaltete virtuelle Maschine migrieren
Inhaltsbibliothek	<p>Um eine Berechtigung für eine Inhaltsbibliothek zuzuweisen, muss ein Administrator dem Benutzer die Berechtigung als globale Berechtigung erteilen. Weitere Informationen finden Sie im Abschnitt Hierarchische Vererbung von Berechtigungen für Inhaltsbibliotheken unter <i>Verwaltung virtueller vSphere-Maschinen</i> in der VMware vSphere-Dokumentation.</p> <ul style="list-style-type: none"> ■ Bibliothekselement hinzufügen ■ Lokale Bibliothek erstellen ■ Abonnierte Bibliothek erstellen ■ Bibliothekselement löschen ■ Lokale Bibliothek löschen ■ Abonnierte Bibliothek löschen ■ Dateien herunterladen ■ Bibliothekselement entfernen ■ Abonnierte Bibliothek entfernen ■ Abonnementinformationen prüfen ■ Speicherinfos lesen ■ Bibliothekselement synchronisieren ■ Abonnierte Bibliothek synchronisieren ■ Selbstüberprüfung des Typs ■ Konfigurationseinstellungen aktualisieren ■ Dateien aktualisieren ■ Bibliothek aktualisieren ■ Bibliothekselement aktualisieren ■ Lokale Bibliothek aktualisieren ■ Abonnierte Bibliothek aktualisieren ■ Konfigurationseinstellungen anzeigen

Tabelle 3-12. Erforderliche Berechtigungen für vSphere-Agenten zur Verwaltung von vCenter Server-Instanzen (Fortsetzung)

Attributwert	Berechtigung
Tags	<ul style="list-style-type: none"> ■ vSphere-Tag zuweisen oder Zuweisung aufheben ■ vSphere-Tag erstellen ■ Kategorie für vSphere-Tag erstellen ■ vSphere-Tag löschen ■ Kategorie für vSphere-Tag löschen ■ vSphere-Tag bearbeiten ■ Kategorie für vSphere-Tag bearbeiten ■ UsedBy-Feld für Kategorie ändern ■ UsedBy-Feld für Tag ändern
vApp	<ul style="list-style-type: none"> ■ Importieren ■ vApp-Anwendungskonfiguration <p>Die Anwendungskonfiguration <code>vApp.Import</code> ist für OVF-Vorlagen und für die Bereitstellung von VMs aus der Inhaltsbibliothek erforderlich.</p> <p>Die Anwendungskonfiguration <code>vApp.vApp</code> ist erforderlich, wenn Sie cloud-init für Cloud-Konfigurationsskripts verwenden. Diese Einstellung ermöglicht das Ändern der internen Struktur einer vApp, wie z. B. zugehöriger Produktinformationen und Eigenschaften.</p>
Virtuelle Maschine – Bestandsliste	<ul style="list-style-type: none"> ■ Aus vorhandener erstellen ■ Neue erstellen ■ Verschieben ■ Entfernen
Virtuelle Maschine – Interaktion	<ul style="list-style-type: none"> ■ CD-Medien konfigurieren ■ Konsoleninteraktion ■ Geräteverbindung ■ Ausschalten ■ Einschalten ■ Zurücksetzen ■ Anhalten ■ Tools installieren

Tabelle 3-12. Erforderliche Berechtigungen für vSphere-Agenten zur Verwaltung von vCenter Server-Instanzen (Fortsetzung)

Attributwert	Berechtigung
Virtuelle Maschine – Konfiguration	<ul style="list-style-type: none"> ■ Vorhandene Festplatte hinzufügen ■ Neue Festplatte hinzufügen ■ Festplatte entfernen ■ Erweitert ■ CPU-Anzahl ändern ■ Ressource ändern ■ Virtuelle Festplatte erweitern ■ Festplattenänderungsverfolgung ■ Arbeitsspeicher ■ Geräteeinstellungen ändern ■ Umbenennen ■ Anmerkung festlegen ■ Einstellungen ■ Platzierung der Auslagerungsdatei
Virtuelle Maschine – Bereitstellung	<ul style="list-style-type: none"> ■ Anpassen ■ Vorlage klonen ■ Virtuelle Maschine klonen ■ Vorlage bereitstellen ■ Anpassungsspezifikationen lesen
Virtuelle Maschine – Zustand	<ul style="list-style-type: none"> ■ Snapshot erstellen ■ Snapshot entfernen ■ Snapshot wiederherstellen

Konfigurieren von Microsoft Azure für die Verwendung mit vRealize Automation Cloud Assembly

Sie müssen einige Informationen erfassen und einige Konfigurationsschritte durchführen, um ein Microsoft Azure Cloud-Konto in vRealize Automation Cloud Assembly zu erstellen.

Verfahren

- 1 Suchen Sie nach Ihrem Microsoft Azure-Abonnement und Ihren Mandanten-IDs und schreiben Sie sie auf.
 - Abonnement-ID: Klicken Sie auf das Symbol „Abonnements“ in der linken Symbolleiste in Ihrem Azure-Portal, um die Abonnement-ID anzuzeigen.
 - Mandanten-ID: Klicken Sie auf das Hilfesymbol und wählen Sie „Diagnose anzeigen“ in Ihrem Azure-Portal aus. Suchen Sie nach einem Mandanten und notieren Sie sich dessen ID.

- 2 Sie können ein neues Speicherkonto und eine Ressourcengruppe erstellen, um zu beginnen. Alternativ können Sie diese später in Blueprints erstellen.

- Speicherkonto: Verwenden Sie das folgende Verfahren, um ein Konto zu konfigurieren.
 - 1 Suchen Sie in Ihrem Azure-Portal das Symbol „Speicherkonten“ auf der Seitenleiste. Stellen Sie sicher, dass das richtige Abonnement ausgewählt ist, und klicken Sie auf **Hinzufügen**. Sie können auch im Azure-Suchfeld nach „Speicherkonto“ suchen.
 - 2 Geben Sie die erforderlichen Informationen für das Speicherkonto ein. Sie benötigen Ihre Abonnement-ID.
 - 3 Wählen Sie aus, ob eine vorhandene Ressourcengruppe verwendet oder eine neue erstellt werden soll. Notieren Sie sich Ihren Ressourcengruppennamen zur späteren Verwendung.

Hinweis Speichern Sie den Speicherort Ihres Speicherkontos, da Sie es später benötigen werden.

- 3 Erstellen Sie ein virtuelles Netzwerk. Alternativ können Sie auch ein geeignetes vorhandenes Netzwerk auswählen.

Wenn Sie ein Netzwerk erstellen, müssen Sie „Vorhandene Ressourcengruppe verwenden“ auswählen und die Gruppe angeben, die Sie im vorherigen Schritt erstellt haben. Wählen Sie außerdem denselben Speicherort aus, den Sie zuvor angegeben haben. Microsoft Azure stellt keine virtuellen Maschinen oder anderen Objekte bereit, wenn der Speicherort nicht für alle zutreffenden Komponenten übereinstimmt, die das Objekt nutzen wird.

- a Suchen Sie im linken Fensterbereich das Symbol für das virtuelle Netzwerk und klicken Sie darauf oder suchen Sie nach einem virtuellen Netzwerk. Stellen Sie sicher, dass Sie das richtige Abonnement auswählen, und klicken Sie auf **Hinzufügen**.
 - b Geben Sie einen eindeutigen Namen für Ihr neues virtuelles Netzwerk ein und notieren Sie ihn für später.
 - c Geben Sie im Feld **Adressraum** die entsprechende IP-Adresse für Ihr virtuelles Netzwerk ein.
 - d Stellen Sie sicher, dass das richtige Abonnement ausgewählt ist, und klicken Sie auf **Hinzufügen**.
 - e Geben Sie die verbleibenden grundlegenden Konfigurationsinformationen ein.
 - f Sie können die anderen Optionen nach Bedarf ändern, aber für die meisten Konfigurationen können Sie die Standardeinstellungen beibehalten.
 - g Klicken Sie auf **Erstellen**.
- 4 Richten Sie eine Azure Active Directory-Anwendung ein, damit vRA authentifiziert werden kann.
- a Suchen Sie das Active Directory-Symbol im linken Azure-Menü und klicken Sie darauf.
 - b Klicken Sie auf **App-Registrierungen** und wählen Sie **Hinzufügen** aus.

- c Geben Sie einen Namen für Ihre Anwendung ein, der mit der Validierung des Azure-Namens übereinstimmt.
 - d Belassen Sie Web-App/API als Anwendungstyp.
 - e Die Anmelde-URL kann alles sein, was für Ihre Nutzung geeignet ist.
 - f Klicken Sie auf **Erstellen**.
- 5 Erstellen Sie einen geheimen Schlüssel, um die Anwendung in Cloud Assembly zu authentifizieren.
- a Klicken Sie auf den Namen Ihrer Anwendung in Azure.
Notieren Sie sich Ihre Anwendungs-ID für die spätere Verwendung.
 - b Klicken Sie auf **Alle Einstellungen** im nächsten Fensterbereich und wählen Sie „Schlüssel“ aus der Einstellungsliste aus.
 - c Geben Sie eine Beschreibung für den neuen Schlüssel ein und wählen Sie eine Dauer aus.
 - d Klicken Sie auf **Speichern** und stellen Sie sicher, dass Sie den Schlüsselwert an einen sicheren Speicherort kopieren, da Sie ihn später nicht mehr abrufen können.
 - e Wählen Sie im linken Menü die Option **API-Berechtigungen** für die Anwendung und klicken Sie auf **Berechtigung hinzufügen**, um eine neue Berechtigung zu erstellen.
 - f Wählen Sie auf der Seite „API auswählen“ die Option „Azure Service Management“ aus.
 - g Klicken Sie auf **Delegierte Berechtigungen**.
 - h Wählen Sie unter „Berechtigungen auswählen“ die Option „user_impersonation“ und klicken Sie dann auf **Berechtigungen hinzufügen**.
- 6 Autorisieren Sie Ihre Active Directory-Anwendung für die Herstellung einer Verbindung mit Ihrem Azure-Abonnement, damit Sie virtuelle Maschinen bereitstellen und verwalten können.
- a Klicken Sie im linken Menü auf das Abonnements-Symbol und wählen Sie Ihr neues Abonnement aus.

Sie müssen möglicherweise auf den Text des Namens klicken, um das Fenster zu verschieben.
 - b Wählen Sie die Zugriffssteuerungsoption (IAM) aus, um die Berechtigungen für Ihr Abonnement anzuzeigen.
 - c Klicken Sie unter der Überschrift „Rollenzuweisung hinzufügen“ auf **Hinzufügen**.
 - d Wählen Sie in der Dropdown-Liste „Rolle“ die Option „Beitragender“ aus.
 - e Belassen Sie die Standardauswahl im Dropdown-Menü „Zugriff zuweisen“.
 - f Geben Sie den Namen Ihrer Anwendung in das Auswahlfeld ein.
 - g Klicken Sie auf **Speichern**.

- h Fügen Sie zusätzliche Rollen hinzu, damit Ihre neue Anwendung über Besitzer-, Beitragender- und Leser-Rollen verfügt.
- i Klicken Sie auf **Speichern**.

Nächste Schritte

Sie müssen die Tools der Microsoft Azure-Befehlszeilenschnittstelle installieren. Diese Tools sind für Windows- und Mac-Betriebssysteme kostenlos erhältlich. Weitere Informationen zum Herunterladen und Installieren dieser Tools finden Sie in der Microsoft-Dokumentation.

Nachdem die Befehlszeilenschnittstelle installiert ist, müssen Sie sich bei Ihrem neuen Abonnement authentifizieren.

- 1 Öffnen Sie ein Terminal-Fenster und geben Sie Ihre Microsoft Azure-Anmeldung ein. Sie erhalten eine URL und einen Kurzcode, um sich zu authentifizieren.
- 2 Geben Sie in einem Browser den Code ein, den Sie von der Anwendung auf Ihrem Gerät erhalten haben.
- 3 Geben Sie Ihren Authentifizierungscode ein und klicken Sie auf **Weiter**.
- 4 Wählen Sie Ihr Azure-Konto aus und melden Sie sich an.

Wenn Sie über mehrere Abonnements verfügen, stellen Sie mit dem Befehl `azure account set <subscription-name>` sicher, dass das richtige ausgewählt wurde.

- 5 Bevor Sie fortfahren, müssen Sie den Microsoft.Compute-Anbieter für Ihr neues Azure-Abonnement mit dem Befehl `azure provider register microsoft.compute` registrieren.

Wenn beim ersten Ausführen des Befehls eine Zeitüberschreitung auftritt und ein Fehler generiert wird, führen Sie ihn erneut aus.

Nachdem Sie die Konfiguration abgeschlossen haben, können Sie den Befehl `azure vm image list` verwenden, um die verfügbaren Image-Namen für virtuelle Maschinen abzurufen. Sie können das gewünschte Image auswählen und den dafür bereitgestellten URN aufzeichnen und später in Blueprints verwenden.

Erstellen Sie ein Microsoft Azure-Cloud-Konto in vRealize Automation.

Als Cloud-Administrator können Sie ein Microsoft Azure-Cloud-Konto für Kontoregionen erstellen, in denen Ihr Team vRealize Automation-Cloud-Vorlagen bereitstellt.

Ein Anwendungsbeispiel zur Funktionsweise eines Microsoft Azure-Cloud-Kontos in vRealize Automation finden Sie im [Lernprogramm: Einrichten und Testen einer Multi-Cloud-Infrastruktur und von Bereitstellungen in vRealize Automation Cloud Assembly](#).

Voraussetzungen

- Stellen Sie sicher, dass Sie über die erforderlichen Administratoranmeldedaten verfügen und dass der HTTPS-Zugriff auf Port 443 aktiviert wurde. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Stellen Sie sicher, dass Sie über die erforderliche Benutzerrolle verfügen. Weitere Informationen finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Konfigurieren Sie ein Microsoft Azure-Konto zur Verwendung mit vRealize Automation. Weitere Informationen hierzu finden Sie unter [Konfigurieren von Microsoft Azure für die Verwendung mit vRealize Automation Cloud Assembly](#).
- Wenn Sie nicht über externen Internetzugang verfügen, konfigurieren Sie einen Internet-Proxyserver. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Integrieren eines Internet-Proxyservers für vRealize Automation](#).

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Cloud-Konten** aus und klicken Sie auf **Cloud-Konto hinzufügen**.
- 2 Wählen Sie den Microsoft Azure-Kontotyp aus und geben Sie Anmeldedaten und andere Werte ein.
- 3 Klicken Sie auf **Validieren**.
Die dem Konto zugeordneten Kontobereiche werden erfasst.
- 4 Wählen Sie die Regionen aus, in denen diese Ressource bereitgestellt werden soll.
- 5 Klicken Sie aus Effizienzgründen auf **Cloud-Zone für die ausgewählten Regionen erstellen**.
- 6 Wenn Sie zur Unterstützung einer Tagging-Strategie Tags hinzufügen müssen, geben Sie Funktions-Tags ein. Weitere Informationen finden Sie unter [Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen](#) und [Erstellen einer Tagging-Strategie](#).



Weitere Informationen dazu, wie mithilfe von Funktions- und Einschränkungs-Tags Bereitstellungsplatzierungen gesteuert werden können, finden Sie im Video-Tutorial [Einschränkungs-Tags und Platzierung](#).

- 7 Klicken Sie auf **Speichern**.

Ergebnisse

Das Konto wird zu vRealize Automation hinzugefügt und die ausgewählten Regionen stehen für die angegebene Cloud-Zone zur Verfügung.

Nächste Schritte

Erstellen Sie Infrastrukturressourcen für dieses Cloud-Konto.

Erstellen eines Amazon Web Services-Cloud-Kontos in vRealize Automation

Als Cloud-Administrator können Sie ein Amazon Web Services-Cloud-Konto (AWS) für Kontoregionen erstellen, in denen Ihr Team vRealize Automation-Cloud-Vorlagen bereitstellt.

Die AWS-Cloud-Konten unterstützen für autorisierte Benutzer den Zugriff auf die AWS GovCloud-Konfiguration. Diese Konfiguration bietet Unterstützung für die meisten Standardfunktionen der vRealize Automation-Cloud-Konten im Rahmen von Projektkonfiguration, Tags und Infrastruktur. In Cloud Assembly-Cloud-Vorlagen wird die Verwendung von AWS PaaS-Eigenschaften (Platform as a Service) unterstützt.

Im folgenden Verfahren wird die Konfiguration eines AWS-Cloud-Kontos beschrieben.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die erforderlichen Administratoranmeldedaten verfügen und dass der HTTPS-Zugriff auf Port 443 aktiviert wurde. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Stellen Sie sicher, dass Sie über die erforderliche Benutzerrolle verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Stellen Sie sicher, dass Sie über die notwendigen AWS-Administratoranmeldedaten verfügen.
- Wenn Sie nicht über externen Internetzugriff verfügen, konfigurieren Sie einen Internet-Proxyserver. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Integrieren eines Internet-Proxyservers für vRealize Automation](#).

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Cloud-Konten** aus und klicken Sie auf **Cloud-Konto hinzufügen**.
- 2 Wählen Sie den AWS-Kontotyp aus und geben Sie Anmeldedaten und andere Werte ein.
- 3 Klicken Sie auf **Validieren**.
Die dem Konto zugeordneten Kontobereiche werden erfasst.
- 4 Wählen Sie die Regionen aus, in denen diese Ressource bereitgestellt werden soll.
- 5 Klicken Sie aus Effizienzgründen auf **Cloud-Zone für die ausgewählten Regionen erstellen**.
- 6 Wenn Sie zur Unterstützung einer Tagging-Strategie Tags hinzufügen müssen, geben Sie Funktions-Tags ein. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen](#) und [Erstellen einer Tagging-Strategie](#).



Weitere Informationen dazu, wie mithilfe von Funktions- und Einschränkungs-Tags Bereitstellungsplatzierungen gesteuert werden können, finden Sie im Video-Tutorial [Einschränkungs-Tags und Platzierung](#).

7 Klicken Sie auf **Hinzufügen**.

Ergebnisse

Das Konto wird zu vRealize Automation hinzugefügt und die ausgewählten Regionen stehen für die angegebene Cloud-Zone zur Verfügung.

Nächste Schritte

Konfigurieren Sie Infrastrukturressourcen für dieses Cloud-Konto.

Erstellen Sie ein Google Cloud Platform-Cloud-Konto in vRealize Automation.

Als Cloud-Administrator können Sie ein Google Cloud Platform-Cloud-Konto (GCP) für Kontoregionen erstellen, in denen Ihr Team vRealize Automation-Cloud-Vorlagen bereitstellt.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die erforderlichen Administratoranmeldedaten verfügen und dass der HTTPS-Zugriff auf Port 443 aktiviert wurde. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Stellen Sie sicher, dass Sie über die erforderliche Benutzerrolle verfügen. Weitere Informationen finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Stellen Sie sicher, dass Sie Zugriff auf den JSON-Sicherheitsschlüssel von Google Cloud Platform haben.
- Stellen Sie sicher, dass Sie über die erforderlichen Sicherheitsinformationen für Ihre Google Cloud Platform-Instanz verfügen. Sie können die meisten dieser Informationen aus Ihrer Instanz oder aus der Google-Dokumentation abrufen.
- Wenn Sie nicht über externen Internetzugriff verfügen, konfigurieren Sie einen Internet-Proxyserver. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Integrieren eines Internet-Proxyservers für vRealize Automation](#).

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Cloud-Konten** aus und klicken Sie auf **Cloud-Konto hinzufügen**.
- 2 Wählen Sie den Google Cloud Platform-Kontotyp aus und geben Sie die entsprechenden Anmeldedaten und zugehörigen Informationen ein. Verwenden Sie das Dienstkonto, das beim Initialisieren der Computing-Engine des GCP-Quellkontos erstellt wurde.

Wie im obigen Abschnitt **Voraussetzungen** angegeben, stehen die Anforderungen an die Anmeldedaten unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#) zur Verfügung. Zur erfolgreichen Erstellung des Cloud-Kontos in vRealize Automation muss der Computing-Engine-Dienst für das GCP-Quellkonto aktiviert sein.

In vRealize Automation ist die Projekt-ID Teil des Google Cloud Platform-Endpoints. Sie geben sie bei der Erstellung des Cloud-Kontos an. Während der Datenerfassung projektspezifischer privater Images fragt der GCP-Adapter von vRealize Automation die Google Cloud Platform-API ab.

3 Klicken Sie auf **Validieren**.

Die dem Konto zugeordneten Kontobereiche werden erfasst.

4 Wählen Sie die Regionen aus, in denen diese Ressource bereitgestellt werden soll.

5 Klicken Sie aus Effizienzgründen auf **Cloud-Zone für die ausgewählten Regionen erstellen**.

6 Wenn Sie zur Unterstützung einer Tagging-Strategie Tags benötigen, geben Sie Funktions-Tags ein. Weitere Informationen finden Sie unter [Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen](#) und [Erstellen einer Tagging-Strategie](#).



Weitere Informationen dazu, wie mithilfe von Funktions- und Einschränkungs-Tags Bereitstellungsplatzierungen gesteuert werden können, finden Sie im Video-Tutorial [Einschränkungs-Tags und Platzierung](#).

7 Klicken Sie auf **Hinzufügen**.

Ergebnisse

Das Konto wird zu vRealize Automation hinzugefügt und die ausgewählten Regionen stehen für die angegebene Cloud-Zone zur Verfügung.

Nächste Schritte

Erstellen Sie Infrastrukturressourcen für dieses Cloud-Konto.

Erstellen Sie ein vCenter-Cloud-Konto in vRealize Automation.

Sie fügen ein vCenter-Cloud-Konto für die Kontoregionen hinzu, in denen Sie vRealize Automation-Cloud-Vorlagen bereitstellen möchten.

Zu Netzwerk- und Sicherheitszwecken können Sie ein vCenter-Cloud-Konto mit einem NSX-T- oder einem NSX-V-Cloud-Konto verknüpfen.

Ein NSX-T-Cloud-Konto kann einem oder mehreren vCenter-Cloud-Konten zugeordnet werden. Ein NSX-V-Cloud-Konto kann jedoch nur mit einem vCenter-Cloud-Konto verknüpft werden.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die erforderlichen Administratoranmeldedaten verfügen und dass der HTTPS-Zugriff auf Port 443 aktiviert wurde. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Stellen Sie sicher, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).

- Stellen Sie sicher, dass Ihre Ports und Protokolle ordnungsgemäß zur Unterstützung des Cloud-Kontos konfiguriert wurden. Weitere Informationen finden Sie im Thema *Ports und Protokolle für vRealize Automation* unter *Installieren von vRealize Automation mit dem vRealize Easy-Installationsprogramm* und im Thema *Portanforderungen* im *vRealize Automation-Handbuch zur Referenzarchitektur* in der [vRealize Automation-Produktdokumentation](#).

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Cloud-Konten** aus und klicken Sie auf **Cloud-Konto hinzufügen**.
- 2 Wählen Sie den vCenter-Kontotyp aus und geben Sie die IP-Adresse des vCenter Server-Hosts ein.
- 3 Geben Sie Ihre vCenter Server-Administratoranmeldedaten ein und klicken Sie auf **Validieren**.

Alle Datencenter, die dem Konto zugeordnet sind, werden erfasst. Die Daten folgender Elemente werden erfasst, ebenso wie alle vSphere-Tags für die folgenden Elemente:

- Maschinen
- Cluster und Hosts
- Portgruppen
- Datenspeicher

- 4 Wählen Sie mindestens ein verfügbares Datencenter auf dem angegebenen vCenter Server aus, um die Bereitstellung für dieses Cloud-Konto zuzulassen.
- 5 Erstellen Sie aus Effizienzgründen eine Cloud-Zone zur Bereitstellung in den ausgewählten Datencentern.

Sie können Cloud-Zonen auch in einem separaten Schritt gemäß der Cloud-Strategie Ihrer Organisation erstellen.

Informationen über Cloud-Zonen finden Sie unter [Weitere Informationen zu vRealize Automation Cloud Assembly-Cloud-Zonen](#).

- 6 Wählen Sie ein vorhandenes NSX-Cloud-Konto aus.

Sie können das NSX-Konto jetzt oder später auswählen, wenn Sie das Cloud-Konto bearbeiten.

Informationen über NSX-V-Cloud-Konten finden Sie unter [Erstellen eines NSX-V-Cloud-Kontos in vRealize Automation](#).

Informationen über NSX-T-Cloud-Konten finden Sie unter [Erstellen eines NSX-T-Cloud-Kontos in vRealize Automation](#).

Weitere Informationen zu Zuordnungsänderungen, nachdem Sie eine Cloud-Vorlage bereitgestellt haben, finden Sie unter [Was passiert, wenn die Verknüpfung eines NSX-Cloud-Kontos in vRealize Automation entfernt wird](#).

- 7 Wenn Sie zur Unterstützung einer Tagging-Strategie Tags hinzufügen möchten, geben Sie Funktions-Tags ein.

Sie können Tags jetzt oder später hinzufügen, wenn Sie das Cloud-Konto bearbeiten. Weitere Informationen zum Tagging finden Sie unter [Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen](#).



Weitere Informationen dazu, wie mithilfe von Funktions- und Einschränkungs-Tags Bereitstellungsplatzierungen gesteuert werden können, finden Sie im Video-Tutorial [Einschränkungs-Tags und Platzierung](#).

- 8 Klicken Sie auf **Speichern**.

Ergebnisse

Das Cloud-Konto wird hinzugefügt und die ausgewählten Datacenter stehen für die angegebene Cloud-Zone zur Verfügung. Erfasste Daten, wie z. B. Maschinen, Netzwerke, Speicher und Volumes, werden im Abschnitt **Ressourcen** der Registerkarte **Infrastruktur** aufgeführt.

Nächste Schritte

Konfigurieren Sie verbleibende Infrastrukturressourcen für dieses Cloud-Konto. Weitere Informationen hierzu finden Sie unter [Kapitel 4 Erstellen der vRealize Automation Cloud Assembly-Ressourceninfrastruktur](#).

Erstellen eines NSX-V-Cloud-Kontos in vRealize Automation

Zu Netzwerk- und Sicherheitszwecken können Sie ein NSX-V-Cloud-Konto erstellen und mit einem vCenter-Cloud-Konto verknüpfen.

Ein NSX-V-Cloud-Konto kann nur mit einem vCenter-Cloud-Konto verknüpft werden.

Die Verknüpfung zwischen NSX-V und einem vCenter-Cloud-Konto muss außerhalb von vRealize Automation konfiguriert werden, insbesondere in Ihrer NSX-Anwendung. vRealize Automation erstellt keine Verknüpfung zwischen NSX und vCenter. In vRealize Automation geben Sie eine Verknüpfung an, die bereits in NSX vorhanden ist.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die erforderlichen Administratoranmeldedaten verfügen und dass der HTTPS-Zugriff auf Port 443 aktiviert wurde. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Stellen Sie sicher, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Stellen Sie sicher, dass Sie über ein vCenter-Cloud-Konto für die Verwendung mit diesem NSX-Cloud-Konto verfügen. Weitere Informationen hierzu finden Sie unter [Erstellen Sie ein vCenter-Cloud-Konto in vRealize Automation](#).

- Stellen Sie sicher, dass Ihre Ports und Protokolle ordnungsgemäß zur Unterstützung des Cloud-Kontos konfiguriert wurden. Weitere Informationen finden Sie im Thema *Ports und Protokolle für vRealize Automation* unter *Installieren von vRealize Automation mit dem vRealize Easy-Installationsprogramm* und im Thema *Portanforderungen* im *vRealize Automation-Handbuch zur Referenzarchitektur* in der [vRealize Automation-Produktdokumentation](#).

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Cloud-Konten** aus und klicken Sie auf **Cloud-Konto hinzufügen**.
- 2 Wählen Sie den NSX-V-Kontotyp aus und geben Sie die IP-Adresse des NSX-V-Hosts ein.
- 3 Geben Sie Ihre NSX-Administratoranmeldedaten ein und klicken Sie auf **Validieren**.
Die dem Konto zugeordneten Objekte werden erfasst.
Wenn die IP-Adresse des NSX-Hosts nicht verfügbar ist, schlägt die Validierung fehl.
- 4 Wählen Sie gegebenenfalls den vCenter-Endpoint aus, der das vCenter-Cloud-Konto darstellt, das Sie diesem NSX-V-Konto zuordnen.

Nur vCenter-Cloud-Konten, die aktuell nicht mit einem NSX-T- oder NSX-V-Cloud-Konto verknüpft sind, stehen zur Auswahl zur Verfügung.

Weitere Informationen zu Zuordnungsänderungen, nachdem Sie eine Cloud-Vorlage bereitgestellt haben, finden Sie unter [Was passiert, wenn die Verknüpfung eines NSX-Cloud-Kontos in vRealize Automation entfernt wird](#).

- 5 Wenn Sie zur Unterstützung einer Tagging-Strategie Tags hinzufügen möchten, geben Sie Funktions-Tags ein.

Sie können Funktions-Tags auch noch später hinzufügen oder entfernen. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen](#).



Informationen dazu, wie mithilfe von Funktions- und Einschränkungs-Tags Bereitstellungsplatzierungen gesteuert werden können, finden Sie im Video-Tutorial [Einschränkungs-Tags und Platzierung](#).

- 6 Klicken Sie auf **Speichern**.

Nächste Schritte

Sie können ein vCenter-Cloud-Konto erstellen oder bearbeiten, um es diesem NSX-Cloud-Konto zuzuordnen. Weitere Informationen hierzu finden Sie unter [Erstellen Sie ein vCenter-Cloud-Konto in vRealize Automation..](#)

Erstellen und konfigurieren Sie eine oder mehrere Cloud-Zonen für die Verwendung mit den Datencentern, die von diesem Cloud-Konto verwendet werden. Weitere Informationen hierzu finden Sie unter [Weitere Informationen zu vRealize Automation Cloud Assembly-Cloud-Zonen](#).

Konfigurieren Sie Infrastrukturressourcen für dieses Cloud-Konto. Weitere Informationen hierzu finden Sie unter [Kapitel 4 Erstellen der vRealize Automation Cloud Assembly-Ressourceninfrastruktur](#).

Erstellen eines NSX-T-Cloud-Kontos in vRealize Automation

Zu Netzwerk- und Sicherheitszwecken können Sie ein NSX-T-Cloud-Konto erstellen und mit einem oder mehreren vCenter-Cloud-Konten verknüpfen.

Ein NSX-T-Cloud-Konto kann einem oder mehreren vCenter-Cloud-Konten zugeordnet werden. Ein NSX-V-Cloud-Konto kann jedoch nur mit einem vCenter-Cloud-Konto verknüpft werden.

Die Verknüpfung zwischen NSX-T und einem oder mehreren vCenter-Cloud-Konten muss außerhalb von vRealize Automation konfiguriert werden, insbesondere in Ihrer NSX-Anwendung. vRealize Automation erstellt keine Verknüpfung zwischen NSX und vCenter. In vRealize Automation geben Sie eine oder mehrere Konfigurationsverknüpfungen an, die bereits in NSX vorhanden sind.

Sie können ein NSX-T-Cloud-Konto zur Unterstützung der NSX-T Manager-API-Methode oder der NSX-T-Richtlinien-API-Methode konfigurieren. Details zu den beiden Methoden finden Sie in Themen wie etwa *Übersicht über NSX Manager* im *Administratorhandbuch für NSX-T Data Center* in der [Produktdokumentation zu NSX-T Data Center](#). Informationen werden auch in der folgenden Schrittabfolge bereitgestellt.

Nachdem Sie das NSX-T-Cloud-Konto erstellt haben, können Sie es nicht mehr von einer API-Methode in die andere konvertieren. Stattdessen müssen Sie das Cloud-Konto löschen und mithilfe des anderen API-Modus neu erstellen.

Um Fault Tolerance und Hochverfügbarkeit in Bereitstellungen zu vereinfachen, stellt jeder NSX-T-Datencenter-Endpoint einen Cluster aus drei NSX Managern dar.

- vRealize Automation kann auf einen der NSX Manager verweisen. Bei dieser Option empfängt ein NSX Manager die API-Aufrufe von vRealize Automation.
- vRealize Automation kann auf die virtuelle IP des Clusters verweisen. Bei Verwendung dieser Option übernimmt ein NSX Manager die Steuerung der VIP. Dieser NSX Manager empfängt die API-Aufrufe von vRealize Automation. Bei einem Ausfall übernimmt ein anderer Knoten im Cluster die Steuerung der VIP und empfängt die API-Aufrufe von vRealize Automation.

Weitere Informationen zur VIP-Konfiguration für NSX finden Sie unter *Konfigurieren einer VIP-Adresse (Virtual IP) für einen Cluster* im *Installationshandbuch für NSX-T Data Center* in der [Dokumentation zu VMware NSX-T Data Center](#).

- vRealize Automation kann auf eine Lastausgleichsdienst-VIP verweisen, um die Last der Aufrufe auf die drei NSX Manager zu verteilen. Bei dieser Option empfangen alle drei NSX Manager API-Aufrufe von vRealize Automation.

Sie können die VIP auf einem Lastausgleichsdienst eines Drittanbieters oder auf einem NSX-T-Lastausgleichsdienst konfigurieren.

In großen Umgebungen sollten Sie diese Option verwenden, um die vRealize Automation-API-Aufrufe auf die drei NSX Manager zu verteilen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die erforderlichen Administratoranmeldedaten verfügen und dass der HTTPS-Zugriff auf Port 443 aktiviert wurde. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Stellen Sie sicher, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Stellen Sie sicher, dass Sie über ein vCenter-Cloud-Konto für die Verwendung mit diesem NSX-Cloud-Konto verfügen. Weitere Informationen hierzu finden Sie unter [Erstellen Sie ein vCenter-Cloud-Konto in vRealize Automation](#).
- Stellen Sie sicher, dass Ihre Ports und Protokolle ordnungsgemäß zur Unterstützung des Cloud-Kontos konfiguriert wurden. Weitere Informationen finden Sie im Thema *Ports und Protokolle für vRealize Automation* unter *Installieren von vRealize Automation mit dem vRealize Easy-Installationsprogramm* und im Thema *Portanforderungen* im *vRealize Automation-Handbuch zur Referenzarchitektur* in der [vRealize Automation-Produktdokumentation](#).

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Cloud-Konten** aus und klicken Sie auf **Cloud-Konto hinzufügen**.
- 2 Wählen Sie den NSX-T-Kontotyp aus und geben Sie die Host-IP-Adresse für die Instanz des NSX-T-Endpoint-Managers oder die VIP ein (weiter oben finden Sie Informationen zum erwarteten Verhalten im Zusammenhang mit den NSX Manager- und VIP-Optionen).
- 3 Geben Sie den NSX-Benutzernamen und das zugehörige Kennwort Ihrer Administratoranmeldedaten ein und klicken Sie auf **Validieren**.

Die dem Konto zugeordneten Objekte werden erfasst.

Wenn die IP-Adresse des NSX-Hosts nicht verfügbar ist, schlägt die Validierung fehl.

- 4 Wählen Sie unter **NSX-T-API-Methode** entweder die Methode **Manager** oder die Methode **Richtlinie** aus.

- API-Methode „Manager“

Bestehende NSX-T-Endpoints oder Cloud-Konten, die aus einer früheren Version von vRealize Automation per Onboarding hinzugefügt oder migriert werden, werden als NSX-T-Cloud-Konten mit der Manager-API-Methode behandelt.

Die Manager-API-Methode wird für NSX-T 2.4, NSX-T 3.0 und NSX-T 3.1 und nachfolgende Versionen unterstützt.

Wenn Sie jetzt die NSX-T Manager-API-Methode verwenden, sollten Sie mit der Verwendung der Manager-API-Methode fortfahren, bis vRealize Automation einen Migrationspfad von der Manager-API zur Richtlinien-API einführt.

Einige vRealize Automation-Optionen für NSX-T erfordern NSX-T 3.0 oder höher. Dazu gehört das Hinzufügen von Tags für Netzwerkkartenkomponenten virtueller Maschinen in der Cloud-Vorlage.

- API-Methode „Richtlinie“ (Standard)

Die Richtlinien-API-Methode steht für NSX-T 3.0 und NSX-T 3.1 und nachfolgende Versionen zur Verfügung. Mithilfe dieser Option kann vRealize Automation die zusätzlichen Funktionen verwenden, die in der NSX-T-Richtlinien-API verfügbar sind.

Wenn Sie über vorhandene NSX-T-Cloud-Konten verfügen, die vor der Einführung der Richtlinien-API-Methode in vRealize Automation 8.2 erstellt wurden, verwenden diese die Manager-API-Methode. Es wird empfohlen, zu warten, bis das Manager-API- zu Richtlinien-API-Migrationstool in vRealize Automation zur Verfügung steht. Wenn Sie nicht warten möchten, sollten Sie Ihre vorhandenen NSX-T-Cloud-Konten durch neue NSX-T-Cloud-Konten ersetzen, die die Richtlinien-API-Methode angeben.

- 5 Fügen Sie unter **Verknüpfungen** mindestens ein vCenter-Cloud-Konto hinzu, das mit diesem NSX-T-Cloud-Konto verknüpft werden soll. Sie können auch vorhandene Verknüpfungen mit vCenter-Cloud-Konten entfernen.

Nur vCenter-Cloud-Konten, die aktuell in vRealize Automation nicht mit einem NSX-T- oder NSX-V-Cloud-Konto verknüpft sind, stehen zur Auswahl zur Verfügung.

Weitere Informationen hierzu finden Sie unter [Wozu dienen NSX-T-Zuordnungen zu mehreren vCentern in vRealize Automation](#).

Informationen zum Vornehmen von Zuordnungsänderungen nach dem Bereitstellen einer Cloud-Vorlage oder Löschen eines Cloud-Kontos nach dem Bereitstellen einer Cloud-Vorlage finden Sie unter [Was passiert, wenn die Verknüpfung eines NSX-Cloud-Kontos in vRealize Automation entfernt wird](#).

- 6 Wenn Sie zur Unterstützung einer Tagging-Strategie Tags hinzufügen möchten, geben Sie Funktions-Tags ein.

Sie können Funktions-Tags auch noch später hinzufügen oder entfernen. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen](#).



Weitere Informationen dazu, wie mithilfe von Funktions- und Einschränkungs-Tags Bereitstellungsplatzierungen gesteuert werden können, finden Sie im Video-Tutorial [Einschränkungs-Tags und Platzierung](#).

- 7 Klicken Sie auf **Speichern**.

Nächste Schritte

Sie können ein vCenter-Cloud-Konto erstellen oder bearbeiten, um es diesem NSX-Cloud-Konto zuzuordnen. Weitere Informationen hierzu finden Sie unter [Erstellen Sie ein vCenter-Cloud-Konto in vRealize Automation](#).

Erstellen und konfigurieren Sie eine oder mehrere Cloud-Zonen für die Verwendung mit den Datencentern, die von diesem Cloud-Konto verwendet werden. Weitere Informationen hierzu finden Sie unter [Weitere Informationen zu vRealize Automation Cloud Assembly-Cloud-Zonen](#).

Konfigurieren Sie Infrastrukturressourcen für dieses Cloud-Konto. Weitere Informationen hierzu finden Sie unter [Kapitel 4 Erstellen der vRealize Automation Cloud Assembly-Ressourceninfrastruktur](#).

Erstellen Sie ein VMware Cloud on AWS-Cloud-Konto in vRealize Automation.

Als Cloud-Administrator können Sie ein VMware Cloud on AWS-Cloud-Konto für Kontoregionen erstellen, in denen Ihr Team vRealize Automation-Cloud-Vorlagen bereitstellt.

VMware Cloud on AWS erfordert bestimmte eindeutige Konfigurationsverfahren in vRealize Automation. Informationen zum ordnungsgemäßen Konfigurieren von vRealize Automation für VMware Cloud on AWS, einschließlich der Festlegung von API-Token-Werten für das Cloud-Konto und der Angabe von Gateway-Firewallregeln für den zugehörigen Cloud-Proxy, finden Sie im Workflow [Lernprogramm: Konfigurieren von VMware Cloud on AWS für vRealize Automation](#).

Voraussetzungen

- Stellen Sie sicher, dass Sie über die erforderlichen Administratoranmeldedaten für VMware Cloud on AWS verfügen, einschließlich VMware Cloud on AWS-CloudAdmin-Anmeldedaten für das Ziel-SDDC in vCenter, und dass der HTTPS-Zugriff auf Port 443 aktiviert wurde. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Stellen Sie sicher, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Wenn Sie nicht über externen Internetzugriff verfügen, konfigurieren Sie einen Internet-Proxyserver. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Integrieren eines Internet-Proxyservers für vRealize Automation](#).
- Stellen Sie sicher, dass Sie die erforderlichen Zugriffs- und Firewallregeln im SDDC konfiguriert haben. Weitere Informationen hierzu finden Sie unter [Vorbereiten des VMware Cloud on AWS-SDDC für die Verbindung mit VMware Cloud on AWS-Cloud-Konten in vRealize Automation](#).

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Cloud-Konten** aus, klicken Sie auf **Cloud-Konto hinzufügen** und wählen Sie den Kontotyp VMware Cloud on AWS aus.

- 2 Fügen Sie das **VMC-API-Token** für Ihre Organisation hinzu, um auf die verfügbaren SDDCs zuzugreifen.

Sie können auf der verknüpften Seite **API-Token** für Ihre Organisation ein neues Token erstellen oder ein vorhandenes Token verwenden. Weitere Informationen finden Sie unter [Erstellen eines VMware Cloud on AWS-Cloud-Kontos in vRealize Automation innerhalb eines Beispiel-Workflows](#).

- 3 Wählen Sie das SDDC aus, das für Bereitstellungen verfügbar sein soll.

NSX-V-SDDCs werden nicht unterstützt und nicht in der Liste angezeigt.

Die Werte für Manager-IP-Adresse/FQDN in vCenter und NSX-T werden basierend auf dem SDDC automatisch befüllt.

- 4 Geben Sie Ihren vCenter-Benutzernamen und das zugehörige Kennwort für das angegebene SDDC ein, wenn diese sich vom Standardwert „cloudadmin@vmc.local“ unterscheiden.
- 5 Klicken Sie auf **Validieren**, um Ihre Zugriffsrechte für das angegebene vCenter zu bestätigen, und stellen Sie sicher, dass das vCenter ausgeführt wird.

Die dem Konto zugeordneten Datacenter werden erfasst.

- 6 Erstellen Sie aus Effizienzgründen eine Cloud-Zone zur Bereitstellung im ausgewählten SDDC.

Sie können Cloud-Zonen auch in einem separaten Schritt gemäß der Cloud-Strategie Ihrer Organisation erstellen.

- 7 Wenn Sie zur Unterstützung einer Tagging-Strategie Tags hinzufügen möchten, geben Sie Funktions-Tags ein.

Sie können Funktions-Tags auch noch später hinzufügen oder entfernen. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen](#).



Weitere Informationen dazu, wie mithilfe von Funktions- und Einschränkungs-Tags Bereitstellungsplatzierungen gesteuert werden können, finden Sie im Video-Tutorial [Einschränkungs-Tags und Platzierung](#).

- 8 Klicken Sie auf **Speichern**.

Ergebnisse

Das Cloud-Konto wird hinzugefügt, und das ausgewählte SDDC ist für die angegebene Cloud-Zone verfügbar.

Nächste Schritte

Informationen zum ordnungsgemäßen Konfigurieren von vRealize Automation für VMware Cloud on AWS finden Sie unter [Lernprogramm: Konfigurieren von VMware Cloud on AWS für vRealize Automation](#).

Weitere Informationen zu VMware Cloud on AWS außerhalb von vRealize Automation finden Sie in der [Dokumentation zu VMware Cloud on AWS](#).

Erstellen eines VMware Cloud Foundation-Cloud-Kontos

Sie können eine VMware Cloud Foundation (VCF) als ein Cloud-Konto in vRealize Automation Cloud Assembly für die Verwendung der Arbeitslastdomänen konfigurieren.

Ein VCF-Cloud-Konto ermöglicht es Ihnen, eine VCF-Arbeitslast in Cloud Assembly einzubinden, um eine umfassende Hybrid Cloud-Verwaltungslösung zu ermöglichen. Cloud Assembly bietet mehrere Einstiegspunkte, von denen Sie die Konfigurationsseite für das VCF-Cloud-Konto aktivieren können. Wenn Sie auf diese Seite über die Schaltfläche **Cloud-Konto hinzufügen** auf der Registerkarte „Arbeitslastdomäne“ der SDDC-Integration zugreifen, ist die Arbeitslast vorab ausgewählt, da dies die grundlegende Information für vCenter und NSX Manager ist.

Voraussetzungen

Eine Instanz von VMware SDDC Manager 4.1 oder höher muss als vRealize Automation Cloud Assembly-Integration für die Verwendung mit diesem Cloud-Konto konfiguriert sein. Weitere Informationen finden Sie unter [Konfigurieren einer VMware SDDC Manager-Integration](#).

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Cloud-Konten** aus und klicken Sie auf **Cloud-Konto hinzufügen**.
- 2 Wählen Sie den VCF-Cloud-Kontotyp aus und geben Sie einen **Namen** und eine **Beschreibung** ein.
- 3 Geben Sie den FQDN und die Anmeldedaten für die SDDC Manager-Instanz ein, die Sie mit diesem Cloud-Konto verwenden.

Sie können diesen Schritt überspringen, wenn Sie die SDDC-Manager-Instanz bereits konfiguriert haben, die Sie mit diesem Konto verwenden werden.

- 4 Wählen Sie eine oder mehr Arbeitslastdomänen aus, die Sie mit diesem VCF-Cloud-Konto verwenden möchten.
- 5 Wenn Cloud Assembly von Cloud Foundation verwaltete Dienstanmeldedaten für vCenter und NSX verwenden soll, wählen Sie **Dienstanmeldedaten automatisch erstellen**. Wenn Sie diese Anmeldedaten später ändern möchten, müssen Sie den VCF-Mechanismus für die Kennwortverwaltung verwenden.

Wenn Sie diese Option auswählen, können Sie die Schritte 7 und 8 überspringen.

- 6 Geben Sie die erforderlichen Anmeldedaten für den Zugriff auf das mit diesem Cloud-Konto verknüpfte vCenter ein.
- 7 Geben Sie unter der Überschrift „NSX Manager“ NSX-Anmeldedaten ein, wenn Sie die Anmeldedaten für das VCF-Cloud-Konto manuell eingeben möchten, oder klicken Sie auf „Dienstanmeldedaten erstellen und validieren“, um NSX-Anmeldedaten von Cloud Assembly erstellen und validieren zu lassen.

- 8 Geben Sie die erforderlichen Anmeldedaten für den Zugriff auf das NSX-T Netzwerk ein, das diesem Cloud-Konto zugeordnet ist.
- 9 Wählen Sie ggf. den NSX-Modus aus.
- 10 Klicken Sie auf **Validieren**, um eine Verbindung mit dem SDDC Manager zu bestätigen.
- 11 Wählen Sie ggf. die Datencenter, für die die Bereitstellung erfolgen soll, unter der Überschrift „Konfiguration“ aus. Aktivieren Sie das Kontrollkästchen, wenn Sie eine Cloud-Zone für die ausgewählten Datencenter erstellen möchten.
- 12 Wenn Sie zur Unterstützung einer Tagging-Strategie Tags verwenden, geben Sie Funktions-Tags ein. Weitere Informationen finden Sie unter [Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen](#) und [Erstellen einer Tagging-Strategie](#).
- 13 Klicken Sie auf **Speichern**.

Ergebnisse

Dieses Cloud-Konto bringt die ausgewählte Arbeitslastdomäne, die dem angegebenen SDDC Manager zugeordnet ist, zur Verwendung in vRealize Automation Cloud Assembly.

Wenn Sie zusätzliche Arbeitslastdomänen mithilfe von vRealize Automation verwalten möchten, müssen Sie diesen Prozess für jede einzelne Domäne wiederholen.

Nächste Schritte

Nachdem Sie das VCF-Cloud-Konto konfiguriert haben, können Sie das Konto auf der Cloud-Konto-Hauptseite auswählen und auf **Cloud einrichten** klicken, um den Assistenten für den Schnellstart von VMware Cloud Foundation zu initiieren, der Ihre Cloud konfigurieren wird.

Weitere Informationen über den Assistenten für den Schnellstart finden Sie unter [../Getting-Started-Cloud-Assembly/GUID-BDC673B9-D2AD-47BC-93C5-8C500074F931.html](#).

Integrieren von vRealize Automation mit anderen Anwendungen

Integrationen ermöglichen das Hinzufügen externer Systeme zu vRealize Automation.

Zu den Integrationen gehören vRealize Orchestrator, Konfigurationsverwaltung und andere externe Systeme, wie z. B. GitHub, Ansible und Puppet, sowie externe IPAM-Drittanbieter, wie z. B. Infoblox.

Hinweis Wenn Sie nicht über externen Internetzugriff verfügen, dieser von der Integration aber benötigt wird, können Sie einen Internet-Proxyserver konfigurieren. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Integrieren eines Internet-Proxyservers für vRealize Automation](#).

Vorgehensweise zum Verwenden der Git-Integration in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly unterstützt die Integration mit GitLab-, GitHub- und BitBucket-Repositories, damit Sie VMware Cloud Templates und Aktionsskripts in der Quellcodeverwaltung verwalten können. Diese Funktion erleichtert die Überwachung und Nachprüfbarkeit von Prozessen rund um die Bereitstellung.

vRealize Automation Cloud Assembly bietet drei verschiedene Git-Integrationstypen: GitLab, GitHub und BitBucket. Bei jeder dieser Optionen handelt es sich um eine separate Integration.

Die Konfiguration eines geeigneten lokalen Git-Repositorys mit Zugriff für alle benannten Benutzer ist Voraussetzung für die Einrichtung der Git-Integration mit vRealize Automation Cloud Assembly. Außerdem müssen Sie Cloud-Vorlagen in einer bestimmten Struktur speichern, damit sie von Git erkannt werden. Wählen Sie zum Erstellen einer Integration mit GitLab oder GitHub die Optionen **Infrastruktur > Verbindungen > Integrationen** in vRealize Automation Cloud Assembly aus und treffen Sie dann die entsprechende Auswahl. Sie benötigen die URL und das Token für das Ziel-Repository.

Wenn die Git-Integration mit einem vorhandenen Repository konfiguriert ist, werden alle Cloud-Vorlagen, die mit den ausgewählten Projekten verknüpft sind, qualifizierten Benutzern zur Verfügung gestellt. Sie können diese Vorlagen mit einer vorhandenen Bereitstellung oder als Grundlage einer neuen Bereitstellung verwenden. Wenn Sie ein Projekt hinzufügen, müssen Sie einige Eigenschaften für den Speicherort und die Art der Speicherung in Git auswählen.

Sie können Aktionen in einem Git-Repository direkt aus vRealize Automation Cloud Assembly speichern. Aktionsskripte für Versionen können Sie entweder direkt in Git erstellen, oder Sie können Versionen in vRealize Automation Cloud Assembly erstellen. Wenn Sie eine Version einer Aktion in vRealize Automation Cloud Assembly erstellen, wird diese automatisch als Version in Git gespeichert. Cloud-Vorlagen sind etwas komplizierter, da Sie sie nicht direkt von vRealize Automation Cloud Assembly aus zu einer Git-Integration hinzufügen können. Stattdessen müssen Sie sie direkt in einer Git-Instanz speichern. Anschließend können Sie sie von Git abrufen, wenn Sie mit der Seite „Cloud-Vorlagenverwaltung“ in vRealize Automation Cloud Assembly arbeiten.

Vorbereitungen

Sie müssen Cloud-Vorlagen in einer bestimmten Struktur erstellen und speichern, damit sie von GitLab oder GitHub erkannt werden.

- Konfigurieren und speichern Sie Cloud-Vorlagen zur ordnungsgemäßen Integration in GitLab. Nur gültige Vorlagen werden in GitLab importiert.
 - Erstellen Sie einen oder mehrere Ordner für die Cloud-Vorlagen.
 - Alle Cloud-Vorlagen müssen in `blueprint.yaml`-Dateien gespeichert werden.
 - Stellen Sie sicher, dass oben in Ihren Vorlagen die Eigenschaften `name:` und `version:` enthalten sind.

- Extrahieren Sie einen API-Schlüssel für das entsprechende Repository. Wählen Sie in Ihrem Git-Konto oben rechts Ihre Anmeldung aus und navigieren Sie zum Menü „Einstellungen“. Wählen Sie **Zugriffstoken** aus, benennen Sie Ihr Token um und legen Sie ein Ablaufdatum fest. Wählen Sie dann API aus und erstellen Sie das Token. Kopieren Sie den Ergebniswert und speichern Sie ihn.

Die folgenden Richtlinien müssen für alle Cloud-Vorlagen beachtet werden, die bei der Git-Integration verwendet werden.

- Jede Cloud-Vorlage muss sich in einem separaten Ordner befinden.
- Alle Cloud-Vorlagen müssen den Namen `blueprint.yaml` tragen.
- In allen Cloud-Vorlagen-YAML-Dateien müssen die Felder `name` und `version` verwendet werden.
- Nur gültige Cloud-Vorlagen werden importiert.
- Wenn Sie einen von Git importierten Entwurf einer Cloud-Vorlage aktualisieren und deren Inhalt sich von dem in der höchsten Version unterscheidet, wird der Entwurf bei nachfolgenden Synchronisierungen nicht aktualisiert und es wird eine neue Version erstellt. Wenn Sie eine Vorlage aktualisieren und auch weitere Synchronisierungen von Git zulassen möchten, müssen Sie nach den abschließenden Änderungen eine neue Version erstellen.

- [Konfigurieren der GitLab-Integration mit Cloud-Vorlagen in vRealize Automation Cloud Assembly](#)

In diesem Verfahren wird dargestellt, wie Sie eine GitLab-Integration in vRealize Automation Cloud Assembly so konfigurieren, dass Sie im Repository mit Cloud-Vorlagen arbeiten und gespeicherte Vorlagen automatisch herunterladen können, die zugewiesenen Projekten zugeordnet sind. Zur Verwendung von Cloud-Vorlagen mit GitLab müssen Sie eine Verbindung zu einer geeigneten GitLab-Instanz herstellen und die gewünschten Vorlagen dann in dieser Instanz speichern.

- [Konfigurieren der GitHub-Integration in vRealize Automation Cloud Assembly](#)

Sie können den cloudbasierten Repository-Hosting-Dienst von GitHub in vRealize Automation Cloud Assembly integrieren.

- [Konfigurieren der Bitbucket-Integration in vRealize Automation Cloud Assembly](#)

vRealize Automation Cloud Assembly unterstützt die Integration mit Bitbucket zur Verwendung als Git-basiertes Repository für ABX-Aktionsskripts und VMware Cloud Templates.

Konfigurieren der GitLab-Integration mit Cloud-Vorlagen in vRealize Automation Cloud Assembly

In diesem Verfahren wird dargestellt, wie Sie eine GitLab-Integration in vRealize Automation Cloud Assembly so konfigurieren, dass Sie im Repository mit Cloud-Vorlagen arbeiten und gespeicherte Vorlagen automatisch herunterladen können, die zugewiesenen Projekten zugeordnet sind. Zur Verwendung von Cloud-Vorlagen mit GitLab müssen Sie eine Verbindung zu

einer geeigneten GitLab-Instanz herstellen und die gewünschten Vorlagen dann in dieser Instanz speichern.

Wenn die GitLab-Integration mit einem vorhandenen Repository konfiguriert ist, werden alle Cloud-Vorlagen, die mit den ausgewählten Projekten verknüpft sind, qualifizierten Benutzern zur Verfügung gestellt. Sie können diese Vorlagen mit einer vorhandenen Bereitstellung oder als Grundlage einer neuen Bereitstellung verwenden. Wenn Sie ein Projekt hinzufügen, müssen Sie einige Eigenschaften für den Speicherort und die Art der Speicherung in GitLab auswählen.

Hinweis Sie können keine neuen oder aktualisierten Cloud-Vorlagen aus vRealize Automation Cloud Assembly in das Git-Repository übertragen. Sie können auch keine neuen Vorlagen aus vRealize Automation Cloud Assembly in das Repository übertragen. Um Cloud-Vorlagen zu einem Repository hinzuzufügen, müssen Entwickler die Git-Schnittstelle verwenden.

Wenn Sie einen von Git importierten Entwurf einer Cloud-Vorlage aktualisieren und deren Inhalt sich von dem in der höchsten Version unterscheidet, wird der Entwurf bei nachfolgenden Synchronisierungen nicht aktualisiert und es wird eine neue Version erstellt. Wenn Sie eine Cloud-Vorlage aktualisieren und auch weitere Synchronisierungen von Git zulassen möchten, müssen Sie nach den abschließenden Änderungen eine neue Version erstellen.

Nachdem Sie Ihre Cloud-Vorlagen für die Verwendung mit GitLab eingerichtet und die erforderlichen Informationen erfasst haben, müssen Sie die GitLab-Instanz integrieren. Anschließend können Sie die vorgesehenen Cloud-Vorlagen in GitLab importieren. Sie können eine Videovorführung dieses Verfahrens unter <https://www.youtube.com/watch?v=hOvqo63Sdgg> anzeigen.

Voraussetzungen

- Extrahieren Sie einen API-Schlüssel für das entsprechende Repository. Wählen Sie in Ihrem GitLab-Konto oben rechts Ihre Anmeldung aus und navigieren Sie zum Menü „Einstellungen“. Wählen Sie „Zugriffstoken“ aus, benennen Sie Ihr Token und legen Sie ein Ablaufdatum fest. Wählen Sie dann API aus und erstellen Sie das Token. Kopieren Sie den Ergebniswert und speichern Sie ihn.

Die Konfiguration eines geeigneten lokalen Git-Repositorys mit Zugriff für alle benannten Benutzer ist Voraussetzung für die Einrichtung der Git-Integration mit vRealize Automation Cloud Assembly. Außerdem müssen Sie Cloud-Vorlagen in einer bestimmten Struktur erstellen und speichern, damit sie von GitLab erkannt werden.

- Konfigurieren und speichern Sie Cloud-Vorlagen zur ordnungsgemäßen Integration in GitLab. Nur gültige Vorlagen werden in GitLab importiert. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Verwenden der Git-Integration in vRealize Automation Cloud Assembly](#).

Verfahren

- 1 Richten Sie die Integration mit Ihrer GitLab-Umgebung in vRealize Automation Cloud Assembly ein.
 - a Wählen Sie **Infrastruktur > Integrationen > Neue hinzufügen** und dann „GitLab“ aus.
 - b Geben Sie die **URL** für Ihre GitLab-Instanz ein. Für eine GitLab-SaaS-Instanz (Software as a Service) lautet diese in den meisten Fällen „gitlab.com“.
 - c Geben Sie das **Token**, das auch als API-Schlüssel bezeichnet wird, für die angegebene GitLab-Instanz ein. Informationen zum Extrahieren des Tokens aus Ihrer GitLab-Instanz finden Sie in den obigen Voraussetzungen.
 - d Fügen Sie einen geeigneten Namen und eine geeignete Beschreibung hinzu.
 - e Klicken Sie auf **Überprüfen**, um die Verbindung zu überprüfen.
 - f Fügen Sie bei Bedarf Funktions-Tags hinzu. Weitere Informationen hierzu finden Sie unter [Verwenden von Funktions-Tags in vRealize Automation Cloud Assembly](#).
 - g Klicken Sie auf **Hinzufügen**.
- 2 Konfigurieren Sie die GitLab-Verbindung so, dass Cloud-Vorlagen in einem geeigneten Repository akzeptiert werden.
 - a Wählen Sie **Infrastruktur > Integrationen** und dann die entsprechende GitLab-Integration aus.
 - b Wählen Sie **Projekte** aus.
 - c Wählen Sie **Neues Projekt** aus und erstellen Sie einen Namen für das Projekt.
 - d Geben Sie den Pfad des **Repositorys** innerhalb von GitLab ein. In der Regel ist dies der Benutzername des Hauptkontos, der an den Namen des Repositorys angehängt wird.
 - e Geben Sie die entsprechende GitLab-**Verzweigung** ein, die verwendet werden soll.
 - f Geben Sie gegebenenfalls unter **Ordner** einen Namen ein. Wenn Sie dieses Feld leer lassen, stehen alle Ordner zur Verfügung.
 - g Geben Sie einen geeigneten **Typ** ein. Geben Sie gegebenenfalls einen Ordnernamen ein. Wenn Sie dieses Feld leer lassen, stehen alle Ordner zur Verfügung.
 - h Klicken Sie auf **Weiter**, um das Hinzufügen des Repositorys abzuschließen.

Wenn Sie auf **Weiter** klicken, wird eine automatisierte Synchronisierungsaufgabe initiiert, die Cloud-Vorlagen in die Plattform importiert.

Nach Abschluss der Synchronisierungsaufgaben wird eine Meldung mit dem Hinweis angezeigt, dass die Cloud-Vorlagen importiert wurden.

Ergebnisse

Sie können jetzt Cloud-Vorlagen aus GitLab abrufen.

Konfigurieren der GitHub-Integration in vRealize Automation Cloud Assembly

Sie können den cloudbasierten Repository-Hosting-Dienst von GitHub in vRealize Automation Cloud Assembly integrieren.

Sie benötigen ein gültiges GitHub-Token, um die GitHub-Integration in vRealize Automation Cloud Assembly zu konfigurieren. Weitere Informationen zum Erstellen und Suchen Ihres Tokens finden Sie in der GitHub-Dokumentation.

Voraussetzungen

- Dazu müssen Sie Zugriff auf GitHub haben.
- Konfigurieren und speichern Sie Cloud-Vorlagen zur ordnungsgemäßen Integration in GitHub. Nur gültige Cloud-Vorlagen werden in GitHub importiert. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Verwenden der Git-Integration in vRealize Automation Cloud Assembly](#).

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Integrationen** aus und klicken Sie auf **Integration hinzufügen**.
- 2 Wählen Sie „GitHub“ aus.
- 3 Geben Sie auf der GitHub-Konfigurationsseite die erforderlichen Informationen ein.
- 4 Klicken Sie auf **Validieren**, um die Integration zu überprüfen.
- 5 Wenn Sie zur Unterstützung einer Tagging-Strategie Tags hinzufügen müssen, geben Sie Funktions-Tags ein. Weitere Informationen finden Sie unter [Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen](#) und [Erstellen einer Tagging-Strategie](#).
- 6 Klicken Sie auf **Hinzufügen**.
- 7 Konfigurieren Sie die GitLab-Verbindung so, dass Cloud-Vorlagen in einem geeigneten Repository akzeptiert werden.
 - a Wählen Sie **Infrastruktur > Integrationen** und dann die entsprechende GitHub-Integration aus.
 - b Wählen Sie **Projekte** aus.
 - c Wählen Sie **Neues Projekt** aus und erstellen Sie einen Namen für das Projekt.
 - d Geben Sie den **Repository**-Pfad innerhalb von GitHub ein. In der Regel ist dies der Benutzername des Hauptkontos, der an den Namen des Repositories angehängt wird.
 - e Geben Sie die entsprechende GitHub-**Verzweigung** ein, die verwendet werden soll.
 - f Geben Sie gegebenenfalls unter **Ordner** einen Namen ein. Wenn Sie dieses Feld leer lassen, stehen alle Ordner zur Verfügung.

- g Geben Sie einen geeigneten **Typ** ein.
- h Klicken Sie auf **Weiter**, um das Hinzufügen des Repositorys abzuschließen.

Es wird eine automatisierte Synchronisierungsaufgabe initiiert, die Cloud-Vorlagen in die Plattform importiert.

Nach Abschluss der Synchronisierungsaufgaben wird eine Meldung mit dem Hinweis angezeigt, dass die Cloud-Vorlagen importiert wurden.

Ergebnisse

GitHub ist für die Verwendung in vRealize Automation Cloud Assembly-Blueprints verfügbar.

Nächste Schritte

Sie können jetzt Cloud-Vorlagen aus GitHub abrufen.

Konfigurieren der Bitbucket-Integration in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly unterstützt die Integration mit Bitbucket zur Verwendung als Git-basiertes Repository für ABX-Aktionsskripts und VMware Cloud Templates.

In vRealize Automation Cloud Assembly können Sie mithilfe der Bitbucket-Integration mit zwei Arten von Repository-Objekten arbeiten: VMware Cloud Templates und ABX-Aktionsskripts. Vor der Verwendung einer Bitbucket-Integration müssen Sie Projekte synchronisieren, mit denen Sie arbeiten möchten. ABX-Aktionen unterstützen Rückschreibvorgänge in das Bitbucket-Repository. Cloud-Vorlagen können jedoch nicht aus der Integration rückgeschrieben werden. Wenn Sie neue Versionen von Cloud-Vorlagendateien erstellen möchten, müssen Sie dies manuell tun.

Voraussetzungen

- Richten Sie eine lokale Bitbucket Serverbereitstellung mit einem oder mehreren auf ABX oder Cloud-Vorlagen basierten Projekten ein, die mit ihren Bereitstellungen verwendet werden sollen. Bitbucket Cloud wird derzeit nicht unterstützt.
- Erstellen oder geben Sie ein vRealize Automation Cloud Assembly-Projekt an, mit dem die Bitbucket-Integration verknüpft werden soll.
- Mit einer Bitbucket-Integration zu synchronisierende Cloud-Vorlagendateien müssen die Bezeichnung `blueprint.yaml` erhalten.

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Integrationen** aus und klicken Sie auf **Integration hinzufügen**.
- 2 Wählen Sie Bitbucket aus.
- 3 Geben Sie die Zusammenfassung und Bitbucket-Anmeldedaten auf der Bitbucket-Seite „Zusammenfassung der neuen Integration“ ein.
- 4 Klicken Sie zum Überprüfen der Integration auf **Validieren**.

- 5 Wenn Sie zur Unterstützung einer Tagging-Strategie Add-Tags verwenden, geben Sie Funktions-Tags ein. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen](#) und [Erstellen einer Tagging-Strategie](#).
- 6 Klicken Sie auf **Hinzufügen**.
- 7 Wählen Sie die Registerkarte „Projekte“ auf der Hauptseite für die Bitbucket-Integration aus, um ein Projekt mit dieser Bitbucket-Integration zu verknüpfen.
- 8 Wählen Sie das mit dieser Bitbucket-Integration zu verknüpfende Projekt aus.
- 9 Klicken Sie auf **Weiter**, um ein Repository zum Bitbucket-Projekt hinzuzufügen, und geben Sie den hinzuzufügenden Repository-Typ an. Geben Sie anschließend den **Repository**-Namen und die **Verzweigung** sowie den **Ordner** an.
- 10 Klicken Sie auf **Hinzufügen**.

Wenn Sie einem Projekt ein oder mehrere Repositories hinzufügen möchten, klicken Sie auf **Repository hinzufügen**.

Ergebnisse

Die Bitbucket-Integration ist mit der angegebenen Repository-Konfiguration konfiguriert, und Sie können die in konfigurierten Repositories enthaltenen ABX-Aktionen und Cloud-Vorlagen anzeigen und bearbeiten. Wenn Sie ein Projekt zu einer Bitbucket-Integration hinzufügen, wird eine Synchronisierung ausgeführt, um die aktuellen Versionen der ABX-Aktionsskripts und Cloud-Vorlagendateien aus dem vorgesehenen Repository abzurufen. Auf der Registerkarte „Verlauf“ der Seite „Bitbucket-Integration“ werden Datensätze aller Synchronisierungsvorgänge für die Integration angezeigt. Standardmäßig werden Dateien automatisch alle 15 Minuten synchronisiert. Sie können eine Datei jedoch jederzeit manuell synchronisieren, indem Sie sie auswählen und auf **SYNCHRONISIEREN** klicken.

Nächste Schritte

Sie können mit den ABX-Aktionen auf der vRealize Automation Cloud Assembly-Seite „Erweiterbarkeit“ und mit Cloud-Vorlagen auf der Seite „Design“ arbeiten. Wenn Sie eine geänderte Version einer ABX-Aktion im Bereich „Erweiterbarkeit“ von vRealize Automation Cloud Assembly speichern, wird die neue Version des Skripts erstellt und in das Repository zurückgeschrieben.

Vorgehensweise zum Konfigurieren einer externen IPAM-Integration in vRealize Automation

Sie können einen anbieterspezifischen externen IPAM-Integrationspunkt erstellen, um die in Ihren Cloud-Vorlagenbereitstellungen verwendeten IP-Adressen zu verwalten. Bei Verwendung eines externen IPAM-Integrationspunkts werden IP-Adressen vom benannten IPAM-Anbieter und nicht von vRealize Automation abgerufen und verwaltet.

Sie können einen anbieterspezifischen IPAM-Integrationspunkt erstellen, um IP-Adressen und DNS-Einstellungen für Cloud-Vorlagenbereitstellungen und VMs in vRealize Automation zu verwalten.

Informationen zum Konfigurieren der Voraussetzungen und ein Beispiel für die Erstellung eines anbieterspezifischen externen IPAM-Integrationspunkts im Kontext eines Beispielworkflows finden Sie unter [Hinzufügen einer externen IPAM-Integration für Infoblox in vRealize Automation](#) . Beachten Sie, dass dieser Workflow für eine Infoblox IPAM-Integration gilt, aber als Referenz für jeden externen IPAM-Anbieter verwendet werden kann.

Informationen zum Erstellen der erforderlichen Elemente, damit externe IPAM-Partner und -Anbieter ihre IPAM-Lösung in vRealize Automation integrieren können, finden Sie unter [Vorgehensweise zum Verwenden des IPAM-SDK zur Erstellung eines anbieterspezifischen, externen IPAM-Integrationspakets für vRealize Automation](#).

Voraussetzungen

- Vergewissern Sie sich, dass Sie über Cloud-Administratoranmeldedaten verfügen. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Stellen Sie sicher, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Stellen Sie sicher, dass Sie über ein Konto beim externen IPAM-Anbieter verfügen, z. B. [Infoblox](#) oder [BlueCat](#), und dass Sie über die korrekten Zugriffsberechtigungen für das Konto Ihrer Organisation beim IPAM-Anbieter verfügen.
- Vergewissern Sie sich, dass Sie Zugriff auf ein bereitgestelltes Integrationspaket für den IPAM-Anbieter haben, wie z. B. Infoblox oder BlueCat. Das bereitgestellte Paket wird zunächst als ZIP-Download von Ihrem IPAM-Anbieter oder vom vRealize Automation-Marketplace abgerufen und anschließend in vRealize Automation bereitgestellt.
- Vergewissern Sie sich, dass Sie auf eine konfigurierte Ausführungsumgebung für den IPAM-Anbieter zugreifen können.
- Wenn Sie eine lokale eingebettete Ausführungsumgebung mit aktionsbasierter Erweiterbarkeit (ABX) verwenden, müssen Sie sicherstellen, dass im vRealize Automation-Netzwerk ein HTTP-Proxyserver vorhanden ist, der ausgehenden Datenverkehr an externe Sites wie „gcr.io“ und „storage.googleapis.com“ weiterleiten kann. Weitere Informationen finden Sie unter [Abrufen von Docker-Images hinter einem Proxy in vRealize Automation 8.x \(75180\)](#).
- Stellen Sie sicher, dass Sie über die erforderlichen Benutzeranmeldedaten für den Zugriff auf das IPAM-Anbieterprodukt verfügen. Informationen zu den erforderlichen Benutzerberechtigungen finden Sie in der Produktdokumentation Ihres Integrationsanbieters.

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Integrationen** aus und klicken Sie auf **Integration hinzufügen**.

2 Klicken Sie auf **IPAM**.

3 Wählen Sie im Dropdown-Menü **Anbieter** ein konfiguriertes IPAM-Anbieterpaket aus der Liste aus.

Wenn die Liste leer ist, klicken Sie auf **Anbieterpaket importieren**, navigieren Sie zur ZIP-Datei eines vorhandenen Anbieterpakets und wählen Sie sie aus. Wenn Sie nicht über die ZIP-Datei verfügen, können Sie sie von der Website Ihres Anbieters oder über die Registerkarte **Marketplace** in vRealize Automation abrufen.

4 Geben Sie Ihren Administratorbenutzernamen und das zugehörige Kennwort für Ihr Konto beim externen IPAM-Anbieter sowie die Informationen für alle anderen obligatorischen Felder (sofern vorhanden) ein, z. B. den Hostnamen Ihres Anbieters.

5 Wählen Sie in der Dropdown-Liste **Laufende Umgebung** eine vorhandene Ausführungsumgebung aus, z. B. den lokalen aktionsbasierten Erweiterbarkeits-Integrationspunkt.

Die Ausführungsumgebung unterstützt die Kommunikation zwischen vRealize Automation und dem IPAM-Anbieter.

Das IPAM-Framework unterstützt nur eine lokale eingebettete Ausführungsumgebung mit aktionsbasierter Erweiterbarkeit (ABX).

Hinweis Wenn Sie ein Amazon Web Services- oder ein Microsoft Azure-Cloud-Konto als Ausführungsumgebung der Integration verwenden, stellen Sie sicher, dass auf die IPAM-Anbieter-Appliance über das Internet zugegriffen werden kann, dass sie sich nicht hinter einer NAT oder Firewall befindet und dass sie einen öffentlich auflösbaren DNS-Namen aufweist. Wenn auf den IPAM-Anbieter nicht zugegriffen werden kann, können die Amazon Web Services-Lambda- oder Microsoft Azure-Funktionen keine Verbindung zu ihm herstellen und die Integration schlägt fehl.

6 Klicken Sie auf **Validieren**.

7 Wenn Sie dazu aufgefordert werden, dem selbstsignierten Zertifikat vom externen IPAM-Anbieter zu vertrauen, klicken Sie auf **Akzeptieren**.

Nachdem Sie das selbstsignierte Zertifikat akzeptiert haben, kann die Validierungsaktion bis zum Abschluss fortgesetzt werden.

8 Geben Sie einen Namen für diesen IPAM-Integrationspunkt ein und klicken Sie auf **Hinzufügen**, um den neuen IPAM-Integrationspunkt zu speichern.

Eine Datenerfassungsaktion wird initiiert. Die Daten von Netzwerken und IP-Adressen werden vom externen IPAM-Anbieter erfasst.

Vorgehensweise zum Upgrade auf ein neueres externes IPAM-Integrationspaket in vRealize Automation

Sie können einen vorhandenen externen IPAM-Integrationspunkt aktualisieren, um eine aktuellere Version des anbieterspezifischen IPAM-Integrationspakets zu erhalten.

Ein externer IPAM-Anbieter oder VMware kann ein IPAM-Quellintegrationspaket für einen bestimmten Anbieter aktualisieren. Das externe IPAM-Integrationspaket für Infoblox wurde beispielsweise mehrmals aktualisiert. Zur Beibehaltung aller vorhandenen vRealize Automation-Infrastruktureinstellungen, die einen benannten IPAM-Integrationspunkt verwenden, können Sie einen IPAM-Integrationspunkt bearbeiten, um das aktualisierte IPAM-Integrationspaket zu beziehen, statt einen neuen IPAM-Integrationspunkt zu erstellen.

Voraussetzungen

In diesem Verfahren wird davon ausgegangen, dass Sie bereits einen externen IPAM-Integrationspunkt erstellt haben und ein Upgrade für diesen Integrationspunkt durchführen möchten, um eine aktuellere Version des IPAM-Integrationspakets des Anbieters zu verwenden.

Informationen zum Erstellen eines externen IPAM-Integrationspunkts finden Sie unter [Hinzufügen einer externen IPAM-Integration für Infoblox in vRealize Automation](#).

- Vergewissern Sie sich, dass Sie über Cloud-Administratoranmeldedaten verfügen. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).
- Stellen Sie sicher, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Stellen Sie sicher, dass Sie über ein Konto beim externen IPAM-Anbieter sowie über die korrekten Zugriffsberechtigungen für das Konto Ihrer Organisation bei diesem IPAM-Anbieter verfügen.
- Vergewissern Sie sich, dass Sie auf ein bereitgestelltes Integrationspaket für Ihren IPAM-Anbieter zugreifen können. Das bereitgestellte Paket wird zunächst als ZIP-Download von Ihrer IPAM-Anbieter-Website oder vom vRealize Automation-Marketplace abgerufen und anschließend in vRealize Automation bereitgestellt.

Informationen dazu, wie Sie die ZIP-Datei des Anbieterpakets herunterladen und bereitstellen und das Paket als Wert für **Anbieter** auf der Seite „IPAM-Integration“ zur Verfügung stellen, finden Sie unter [Herunterladen und Bereitstellen eines externen IPAM-Anbieterpakets zur Verwendung in vRealize Automation](#).

- Vergewissern Sie sich, dass Sie auf eine konfigurierte Ausführungsumgebung für den IPAM-Anbieter zugreifen können. Bei der Ausführungsumgebung handelt es sich in der Regel um einen lokalen eingebetteten Integrationspunkt mit aktionsbasierter Erweiterbarkeit.

Informationen zu den Merkmalen der Ausführungsumgebung finden Sie unter [Erstellen einer Ausführungsumgebung für einen IPAM-Integrationspunkt in vRealize Automation](#).

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Integrationen IPAM** aus und öffnen Sie den vorhandenen IPAM-Integrationspunkt.
- 2 Klicken Sie auf **Anbieter verwalten**.
- 3 Navigieren Sie zum aktualisierten IPAM-Integrationspaket und importieren Sie es.

- 4 Klicken Sie auf **Validieren** und anschließend auf **Speichern**.

Konfigurieren der MyVMware-Integration in vRealize Automation Cloud Assembly

Sie können MyVMware in vRealize Automation Cloud Assembly integrieren, um VMware-bezogene Aktionen und Funktionen, wie z. B. den Zugriff auf das VMware Download-Center für Cloud-Vorlagen, zu unterstützen.

Sie können für jede Organisation nur eine My VMware-Integration erstellen.

Voraussetzungen

Sie müssen über ein Benutzerkonto mit den entsprechenden Berechtigungen für My VMware verfügen.

- Informationen zum Einladen eines Benutzers zu einem My VMware-Konto finden Sie unter [KB 2070555](#).
- Informationen zum Zuweisen von Benutzerberechtigungen in einem My VMware-Konto finden Sie unter [KB 2006977](#).

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Integrationen** aus und klicken Sie auf **Integration hinzufügen**.
- 2 Wählen Sie „My VMware“ aus.
- 3 Geben Sie die erforderlichen Informationen auf der Konfigurationsseite von My VMware ein.
- 4 Wenn Sie zur Unterstützung einer Tagging-Strategie Tags benötigen, geben Sie Funktions-Tags ein. Weitere Informationen finden Sie unter [Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen](#) und [Erstellen einer Tagging-Strategie](#).
- 5 Klicken Sie auf **Hinzufügen**.

Ergebnisse

My VMware ist für die Verwendung mit Cloud-Vorlagen verfügbar.

Nächste Schritte

Fügen Sie eine My VMware-Komponente zu den gewünschten Cloud-Vorlagen hinzu.

Konfigurieren der vRealize Orchestrator-Integration in Cloud Assembly

Sie können eine oder mehrere vRealize Orchestrator-Integrationen konfigurieren, um Workflows als Teil der Erweiterbarkeit zu verwenden.

vRealize Automation enthält eine vorkonfigurierte vRealize Orchestrator-Instanz, die für Erweiterbarkeitsabonnements verwendet werden kann. Sie können auch über die vRealize Automation Cloud Services-Konsole auf den Client des eingebetteten vRealize Orchestrator zugreifen.

Mit der vRealize Orchestrator-Integration in vRealize Automation Cloud Assembly können Sie eine externe vRealize Orchestrator-Instanz hinzufügen und die im Lieferumfang enthaltene Workflow-Bibliothek in Erweiterungsabonnements verwenden. Weitere Informationen finden Sie unter [Abonnements für Erweiterbarkeits-Workflows](#).

Voraussetzungen

- Vergewissern Sie sich, dass Sie über Cloud-Administratoranmeldedaten verfügen. Weitere Informationen finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Führen Sie ein Upgrade oder eine Migration auf vRealize Orchestrator 8.1 durch. Weitere Informationen finden Sie unter *Upgrade und Migrieren von VMware vRealize Orchestrator*.

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Integrationen** aus.
- 2 Klicken Sie auf **Integration hinzufügen**.
- 3 Wählen Sie vRealize Orchestrator aus.
- 4 Geben Sie in vRealize Automation Cloud Assembly die URL der vRealize Orchestrator-Instanz ein.
- 5 Klicken Sie zum Überprüfen der Integration auf **Validieren**.
- 6 Geben Sie einen Namen für die vRealize Orchestrator-Integration ein.
- 7 (Optional) Geben Sie eine Beschreibung für die vRealize Orchestrator-Integration ein.
- 8 (Optional) Fügen Sie Funktions-Tags hinzu. Weitere Informationen zu Funktions-Tags finden Sie unter [Verwenden von Funktions-Tags in vRealize Automation Cloud Assembly](#).

Hinweis Funktions-Tags können zum Verwalten mehrerer vRealize Orchestrator-Integrationen verwendet werden. Weitere Informationen hierzu finden Sie unter [Verwalten mehrerer vRealize Orchestrator-Integrationen mit Projekteinschränkungen](#).

- 9 Klicken Sie auf **Hinzufügen**.

Die vRealize Orchestrator-Integration wird gespeichert.

Nächste Schritte

Um zu überprüfen, ob die Integration konfiguriert ist und die Workflows hinzugefügt wurden, wählen Sie **Erweiterbarkeit > Bibliothek > Workflows** aus.

Verwalten mehrerer vRealize Orchestrator-Integrationen mit Projekteinschränkungen

Mithilfe von Projekteinschränkungen können Sie steuern, welche vRealize Orchestrator-Integrationen in Workflow-Abonnements verwendet werden.

vRealize Automation Cloud Assembly unterstützt die Integration mehrerer vRealize Orchestrator-Server, die in Workflow-Abonnements verwendet werden können. Sie können steuern, welche vRealize Orchestrator-Integrationen in von Ihrem Projekt bereitgestellten Cloud-Vorlagen mit flexiblen oder strengen Projekteinschränkungen verwendet werden. Weitere Informationen zu Projekteinschränkungen finden Sie unter [Verwenden von vRealize Automation Cloud Assembly-Projekt-Tags und benutzerdefinierten Eigenschaften](#).

Voraussetzungen

- Vergewissern Sie sich, dass Sie über Cloud-Administratoranmeldedaten verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Konfigurieren Sie mindestens zwei vRealize Orchestrator-Integrationen in vRealize Automation Cloud Assembly. Weitere Informationen hierzu finden Sie unter [Konfigurieren der vRealize Orchestrator-Integration in Cloud Assembly](#).
- Fügen Sie Ihren vRealize Orchestrator-Integrationen Funktions-Tags hinzu. Weitere Informationen hierzu finden Sie unter [Verwenden von Funktions-Tags in vRealize Automation Cloud Assembly](#).

Verfahren

- 1 Navigieren Sie zu **Infrastruktur > Verwaltung > Projekte** und wählen Sie Ihr Projekt aus.
- 2 Wählen Sie die Registerkarte **Bereitstellung** aus.
- 3 Geben Sie die Funktions-Tags Ihrer vRealize Orchestrator-Integrationen in das Textfeld **Erweiterbarkeitseinschränkungen** ein und legen Sie sie als flexible oder strenge Projekteinschränkungen fest.
- 4 Klicken Sie auf **Speichern**.

Ergebnisse

Wenn Sie eine Cloud-Vorlage bereitstellen, steuert vRealize Automation Cloud Assembly anhand der Projekteinschränkungen, welche vRealize Orchestrator-Integrationen in Workflow-Abonnements verwendet werden.

Nächste Schritte

Alternativ können Sie Funktions-Tags verwenden, um mehrere vRealize Orchestrator-Integrationen auf der Ebene eines Cloud-Kontos zu verwalten. Weitere Informationen finden Sie unter [Verwalten mehrerer vRealize Orchestrator-Integrationen mit Cloud-Konto-Funktions-Tags](#).

Verwalten mehrerer vRealize Orchestrator-Integrationen mit Cloud-Konto-Funktions-Tags

Mithilfe von Funktions-Tags können Sie steuern, welche vRealize Orchestrator-Integrationen in Workflow-Abonnements verwendet werden.

vRealize Automation Cloud Assembly unterstützt die Integration mehrerer vRealize Orchestrator-Server, die in Workflow-Abonnements verwendet werden können. Durch Hinzufügen von Funktions-Tags zu Ihrem Cloud-Konto können Sie steuern, welche vRealize Orchestrator-Integrationen in Workflow-Abonnements verwendet werden.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über Cloud-Administratoranmeldedaten verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Konfigurieren Sie mindestens zwei vRealize Orchestrator-Integrationen in vRealize Automation Cloud Assembly. Weitere Informationen finden Sie unter [Konfigurieren der vRealize Orchestrator-Integration in Cloud Assembly](#).
- Fügen Sie Ihren vRealize Orchestrator-Integrationen Funktions-Tags hinzu. Weitere Informationen hierzu finden Sie unter [Verwenden von Funktions-Tags in vRealize Automation Cloud Assembly](#).

Verfahren

- 1 Navigieren Sie zu **Infrastruktur > Verbindungen > Cloud-Konten**.
- 2 Wählen Sie Ihr Cloud-Konto aus.
- 3 Geben Sie die Funktions-Tags der vRealize Orchestrator-Integrationen ein, die Sie verwenden möchten.

Die Funktions-Tags werden automatisch in flexible Einschränkungen umgewandelt. Um strenge Einschränkungen bei der Verwaltung Ihrer Integrationen zu verwenden, müssen Sie Projekteinschränkungen verwenden. Weitere Informationen finden Sie unter [Verwalten mehrerer vRealize Orchestrator-Integrationen mit Projekteinschränkungen](#).

- 4 Klicken Sie auf **Speichern**.

Ergebnisse

Wenn Sie eine Cloud-Vorlage bereitstellen, verwendet vRealize Automation Cloud Assembly das Tagging im zugeordneten Cloud-Konto, um zu steuern, welche vRealize Orchestrator-Integrationen in Workflow-Abonnements verwendet werden.

Vorgehensweise zum Arbeiten mit Kubernetes in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly bietet verschiedene Optionen zum Verwalten und Bereitstellen von Kubernetes-Ressourcen.

Es gibt zwei primäre Optionen für die Arbeit mit Kubernetes-Ressourcen in vRealize Automation Cloud Assembly. Sie können VMware Tanzu Kubernetes Grid Integrated Edition (TKGI, zuvor PKS) oder Red Hat OpenShift mit vRealize Automation Cloud Assembly integrieren, um Kubernetes-Ressourcen zu konfigurieren, zu verwalten und bereitzustellen. Mit der zweiten Option können Sie ein vCenter-Cloud-Konto für den Zugriff auf Supervisor-Namespaces nutzen, um in vSphere Project Pacific mit Kubernetes-basierten Funktionen zu arbeiten. Sie können auch externe Kubernetes-Ressourcen in vRealize Automation Cloud Assembly integrieren.

Arbeiten mit VMware Tanzu Kubernetes Grid Integrated Edition- (TKGI) oder OpenShift-Integrationen

Für TKGI, externe Cluster oder OpenShift-Konfigurationen stellt vRealize Automation Cloud Assembly eine kubeconfig-Datei bereit, mit der Benutzer auf entsprechende Kubernetes-Cluster zugreifen können.

Nachdem Sie eine TKGI- oder OpenShift-Integration erstellt haben, werden entsprechende Kubernetes-Cluster in vRealize Automation Cloud Assembly verfügbar. Sie können Kubernetes-Komponenten erstellen und zu vRealize Automation Cloud Assembly hinzufügen, um die Verwaltung von Cluster- und Containeranwendungen zu unterstützen. Diese Anwendungen bilden die Basis für Self-Service-Bereitstellungen, die im Service Broker-Katalog verfügbar sind.

Arbeiten mit Kubernetes-Clustern in vSphere Project Pacific

Project Pacific ist eine vSphere-Erweiterung, die Kubernetes als Steuerungsebene verwendet. Dadurch können Sie sowohl virtuelle Maschinen als auch Container über eine Schnittstelle verwalten. vRealize Automation Cloud Assembly ermöglicht es Benutzern, die in vSphere eingebetteten Pacific-Kubernetes-Funktionen zu nutzen. Sie können auf die Pacific-Funktionalität zugreifen, indem Sie eine Integration mit einer vCenter-Bereitstellung unter Verwendung einer vSphere-Implementierung erstellen, die Supervisor-Cluster enthält. In Pacific können Sie sowohl konventionelle virtuelle Maschinen als auch Kubernetes-Cluster aus vCenter verwalten.

Für Pacific-basierte Supervisor-Namespaces müssen die Benutzer Zugriff auf eine entsprechende vSphere SSO-Instanz haben, damit sie sich über einen bereitgestellten Link anmelden und auf die Details zum Supervisor-Namespace zugreifen können. Anschließend können sie ein angepasstes kubectI-Plug-In mit vSphere-Authentifizierung herunterladen, um ihren Supervisor-Namespace verwenden zu können.

Um diese Funktionalität nutzen zu können, müssen Sie über einen vCenter mit einem vSphere-Cloud-Konto verfügen, auf dem Supervisor-Namespaces konfiguriert sind. Nachdem sich ein Benutzer angemeldet hat, kann er geeignete Namespaces verwenden.

■ [Konfigurieren der PKS-Integration in vRealize Automation Cloud Assembly](#)

Sie können eine PKS-Ressourcenverbindung lokal und in der Cloud konfigurieren, um Integrations- und Verwaltungsfunktionen von Kubernetes in vRealize Automation Cloud Assembly zu unterstützen.

- [Konfigurieren der Red Hat OpenShift-Integration in vRealize Automation Cloud Assembly](#)

Sie können eine Red Hat OpenShift-Ressourcenverbindung lokal und in der Cloud konfigurieren, um in vRealize Automation Cloud Assembly die Integrations- und Verwaltungsfunktionen von Kubernetes auf Unternehmensebene zu unterstützen.

- [Konfigurieren einer Kubernetes-Zone in vRealize Automation Cloud Assembly](#)

Mit Kubernetes-Zonen können Cloud-Administratoren die richtlinienbasierte Platzierung von Kubernetes-Clustern und -Namespaces sowie von Supervisor-Namespaces definieren, die in vRealize Automation Cloud Assembly-Bereitstellungen verwendet werden. Ein Administrator kann diese Seite verwenden, um anzugeben, welche Cluster für die Bereitstellung von Kubernetes-Namespaces verfügbar sind und welche Eigenschaften für Cluster akzeptabel sind.

- [Verwenden von Pacific-Supervisor-Clustern und -Namespaces mit vRealize Automation Cloud Assembly](#)

Administratoren können vRealize Automation Cloud Assembly so konfigurieren, dass es Supervisor-Namespaces von einer vorhandenen Pacific-fähigen vSphere-Integration verwendet. Auf diese Weise können Benutzer Namespaces in Cloud-Vorlagen bereitstellen und sie im Service Broker-Katalog anfordern.

- [Arbeiten mit Kubernetes-Clustern und -Namespaces in vRealize Automation Cloud Assembly](#)

Sie können die Konfiguration von generischen und Pacific-basierten Kubernetes-Clustern und -Namespaces, die als Basis für Kubernetes-Bereitstellungen in vRealize Automation Cloud Assembly dienen, hinzufügen, anzeigen und verwalten.

- [Hinzufügen von Kubernetes-Komponenten zu Cloud-Vorlagen in vRealize Automation Cloud Assembly](#)

Beim Hinzufügen von Kubernetes-Komponenten zu einer vRealize Automation Cloud Assembly-Cloud-Vorlage können Sie Cluster hinzufügen oder Benutzern das Erstellen von Namespaces in verschiedenen Konfigurationen ermöglichen. Diese Auswahl hängt in der Regel von Ihren Anforderungen an die Zugriffssteuerung, von der Konfiguration Ihrer Kubernetes-Komponenten und von Ihren Bereitstellungsanforderungen ab.

- [Verwenden der Erweiterbarkeit von vRealize Automation Cloud Assembly mit Kubernetes](#)

vRealize Automation Cloud Assembly bietet einen Standardsatz von Ereignisthemen, die typischen Aktionen im Zusammenhang mit der Bereitstellung von Kubernetes-Clustern entsprechen. Benutzer können diese Themen nach Bedarf abonnieren und erhalten eine Benachrichtigung, wenn das Ereignis im Zusammenhang mit dem abonnierten Thema auftritt. Sie können vRO-Workflows auch so konfigurieren, dass sie auf der Grundlage von Ereignisbenachrichtigungen ausgeführt werden.

Konfigurieren der PKS-Integration in vRealize Automation Cloud Assembly

Sie können eine PKS-Ressourcenverbindung lokal und in der Cloud konfigurieren, um Integrations- und Verwaltungsfunktionen von Kubernetes in vRealize Automation Cloud Assembly zu unterstützen.

Mit den PKS-Integrationen können Sie sowohl PKS-Instanzen lokal und in der Cloud als auch auf PKS bereitgestellte Kubernetes-Cluster und externe Cluster verwalten. Sie müssen ein Kubernetes-Profil erstellen und es mit einem Projekt verknüpfen, um die richtlinienbasierte Platzierung von Ressourcen zu unterstützen.

Voraussetzungen

- Sie müssen über einen entsprechend konfigurierten PKS-Server (Pivotal Container Service) verfügen, der mit UAA-Authentifizierung eingerichtet ist.
- Vergewissern Sie sich, dass Sie über Cloud-Administratoranmeldedaten verfügen. Weitere Informationen finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Integrationen** aus und klicken Sie auf **Integration hinzufügen**.
- 2 Wählen Sie VMware Enterprise PKS aus.
- 3 Geben Sie die IP-Adresse oder den FQDN und die PKS-Adresse für das PKS-Cloud-Konto ein, das Sie erstellen.
 - Die IP-Adresse ist der FQDN oder die IP-Adresse des PKS-Benutzerauthentifizierungsservers.
 - Die PKS-Adresse ist der FQDN oder die IP-Adresse für den Haupt-PKS-Server.
- 4 Wählen Sie aus, ob dieser PKS-Server lokal ist oder sich in der Public Cloud oder in einer Private Cloud befindet.
- 5 Geben Sie einen entsprechenden **Benutzernamen** und ein **Kennwort** für den PKS-Server und weitere zugehörige Informationen ein.
- 6 Wenn Sie zur Unterstützung einer Tagging-Strategie Tags verwenden, geben Sie Funktions-Tags ein. Weitere Informationen finden Sie unter [Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen](#) und [Erstellen einer Tagging-Strategie](#).
- 7 Klicken Sie auf **Hinzufügen**.

Ergebnisse

Sie können neue Kubernetes-Zonen erstellen und einem Projekt zuweisen. Alternativ können Sie externe Kubernetes-Cluster erkennen und diese Projekten zuweisen. Darüber hinaus können Sie Kubernetes-Namespace hinzufügen oder erstellen, die die Verwaltung von Clustern zwischen großen Gruppen und Organisationen vereinfachen.

Nächste Schritte

Erstellen oder wählen Sie die entsprechenden Kubernetes-Zonen aus. Wählen Sie dann einen oder mehrere Cluster oder Namespaces aus und weisen Sie sie einem Projekt zu. Anschließend können Sie Cloud-Vorlagen erstellen und veröffentlichen, um Benutzern die Erstellung von Self-Service-Bereitstellungen zu ermöglichen, die Kubernetes verwenden.

Konfigurieren der Red Hat OpenShift-Integration in vRealize Automation Cloud Assembly

Sie können eine Red Hat OpenShift-Ressourcenverbindung lokal und in der Cloud konfigurieren, um in vRealize Automation Cloud Assembly die Integrations- und Verwaltungsfunktionen von Kubernetes auf Unternehmensebene zu unterstützen.

vRealize Automation Cloud Assembly unterstützt die Integration mit OpenShift-Versionen 3.x.

Voraussetzungen

- Sie müssen über eine entsprechend konfigurierte Red Hat OpenShift-Implementierung verfügen.
- Vergewissern Sie sich, dass Sie über Cloud-Administratoranmeldedaten verfügen. Weitere Informationen finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- VMware stellt Ressourcen bereit, die Sie verwenden können, um einen OpenShift-Cluster mit einer Cloud-Vorlage an folgendem Speicherort zu erstellen: <https://flings.vmware.com/enterprise-openshift-as-a-service-on-cloud-automation-services>. Sie können mit diesen Ressourcen erstellte Cluster als globale Cluster in den Kubernetes-Zonen verwenden, um Self-Service-Namespaces zu erstellen.

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Integrationen** aus und klicken Sie auf **Integration hinzufügen**.
- 2 Wählen Sie „Red Hat OpenShift“ aus.
- 3 Geben Sie die **Adresse** und den **Speicherort** des OpenShift-Servers ein.
- 4 Wählen Sie den geeigneten **Anmeldedatentyp** aus und geben Sie die entsprechenden Anmeldedaten ein.

Die OpenShift-Integration unterstützt entweder den OAuth-Benutzernamen/das OAuth-Kennwort, den öffentlichen Schlüssel oder die Bearer-Token-Authentifizierung.
- 5 Geben Sie einen geeigneten **Namen** und eine **Beschreibung** für die OpenShift-Integration ein.
- 6 Wenn Sie zur Unterstützung einer Tagging-Strategie Tags verwenden, geben Sie die geeigneten Funktions-Tags ein. Weitere Informationen finden Sie unter [Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen](#) und [Erstellen einer Tagging-Strategie](#).
- 7 Klicken Sie auf **Hinzufügen**.

Ergebnisse

Wenn eine Integration erstellt wird, werden neue Kubernetes-Cluster im entsprechenden Abschnitt der Kubernetes-Seite angezeigt. Sie können Kubernetes-Zonen erstellen und sie einem Projekt zuweisen. Darüber hinaus können Sie Kubernetes-Namespaces konfigurieren, die die Verwaltung von Clustern zwischen großen Gruppen und Organisationen vereinfachen.

Nächste Schritte

Erstellen oder wählen Sie die entsprechenden Kubernetes-Zonen aus. Wählen Sie dann einen oder mehrere Cluster oder Namespaces aus und weisen Sie sie einem Projekt zu. Anschließend können Sie Cloud-Vorlagen erstellen und veröffentlichen, um Benutzern die Erstellung von Self-Service-Bereitstellungen zu ermöglichen, die Kubernetes verwenden.

Konfigurieren einer Kubernetes-Zone in vRealize Automation Cloud Assembly

Mit Kubernetes-Zonen können Cloud-Administratoren die richtlinienbasierte Platzierung von Kubernetes-Clustern und -Namespaces sowie von Supervisor-Namespaces definieren, die in vRealize Automation Cloud Assembly-Bereitstellungen verwendet werden. Ein Administrator kann diese Seite verwenden, um anzugeben, welche Cluster für die Bereitstellung von Kubernetes-Namespaces verfügbar sind und welche Eigenschaften für Cluster akzeptabel sind.

Cloud-Administratoren können Kubernetes-Zonen mit PKS-Cloud-Konten verknüpfen, die für Cloud Assembly konfiguriert wurden, oder mit externen Kubernetes-Clustern, die keinem Projekt zugeordnet sind.

Wenn Sie eine Kubernetes-Zone erstellen, können Sie der Zone mehrere anbieterspezifische Ressourcen zuweisen. Diese Ressourcen geben vor, welche Eigenschaften für die neu bereitgestellten Cluster in Bezug auf die Anzahl der Worker, Masters, verfügbaren CPU, Arbeitsspeicher und andere Konfigurationseinstellungen festgelegt werden können. Für PKS-Anbieter entsprechen diese den PKS-Plänen. Ein Administrator kann auch mehrere Cluster zu einer Kubernetes-Zone zuweisen, die für die Platzierung von neu bereitgestellten Kubernetes-Namespaces verwendet wird. Der Administrator kann nur Cluster zuweisen, die nicht integriert sind oder nicht von CMX verwaltet werden und die über den vorgewählten Cluster-Anbieter bereitgestellt werden. Der Administrator kann einem einzelnen Projekt mehrere Kubernetes-Zonen zuweisen, sodass sie alle für Platzierungsvorgänge verfügbar sind, die in diesem Projekt durchgeführt werden.

Ein Cloud-Administrator kann Prioritäten auf mehreren Ebenen zuweisen:

- Kubernetes-Zonenpriorität innerhalb eines Projekts.
- Ressourcenpriorität innerhalb einer Kubernetes-Zone.
- Cluster-Priorität innerhalb einer Kubernetes-Zone.

Der Cloud-Administrator kann auch Tags auf mehreren Ebenen zuweisen:

- Funktions-Tags pro Kubernetes-Zone.
- Tags pro Ressourcenzuweisung.

■ Tags pro Cluster-Zuweisung.

Sie können in vSphere Kubernetes-Zonen mit Supervisor-Namespaces in derselben Weise erstellen, wie Sie dies tun, wenn Sie mit generischen Kubernetes-Namespaces arbeiten. Um einer Kubernetes-Zone einen Supervisor-Namespace hinzuzufügen, müssen Sie die Zone einem vSphere 7-Endpoint zuweisen, der die gewünschten Pacific-Namespace-Ressourcen enthält.

Service Broker enthält eine Version der Seite „Kubernetes-Zone“, um Service Broker-Administratoren Zugriff auf vorhandene Kubernetes-Zonen zu ermöglichen, damit sie Platzierungsrichtlinien für Kubernetes-Namespaces und -Cluster erstellen können, die über den Katalog bereitgestellt werden.

Voraussetzungen

Konfigurieren Sie die Integration mit einer geeigneten PKS-Bereitstellung. Weitere Informationen finden Sie unter [Konfigurieren der PKS-Integration in vRealize Automation Cloud Assembly](#)

Verfahren

- 1 Wählen Sie **Infrastruktur > Konfigurieren > Kubernetes-Zone** aus und klicken Sie dann auf **Neue Kubernetes-Zone**.
- 2 Geben Sie den Namen des **Kontos** der PKS-Integration an, für das diese Zone gelten soll.
Hiermit wird das Cloud-Konto oder der Endpoint definiert, der der Zone zugewiesen ist. Sie können jeder Zone nur einen Endpoint zuweisen. Wenn Sie mit einem Supervisor-Namespace in vSphere arbeiten, können Sie nur vSphere-Instanzen auswählen, die Supervisor-Namespaces enthalten.
- 3 Fügen Sie einen **Namen** und eine **Beschreibung** für die Kubernetes-Zone hinzu.
- 4 Fügen Sie bei Bedarf Funktions-Tags hinzu. Weitere Informationen hierzu finden Sie unter [Verwenden von Funktions-Tags in vRealize Automation Cloud Assembly](#).
- 5 Klicken Sie auf **Speichern**.
- 6 Klicken Sie auf die Registerkarte „Bedarfsgesteuert“ und fügen Sie der Zone entsprechende PKS-Pläne hinzu, die für die Cluster-Bereitstellung verwendet werden sollen.
Sie können einen oder mehrere Pläne auswählen und ihnen Prioritäten zuweisen. Niedrigere Zahlen entsprechen höherer Priorität. Prioritätszuweisungen sind für die Tag-basierte Auswahl sekundär.
- 7 Klicken Sie auf die Registerkarte „Cluster“ und anschließend auf die Schaltfläche **Berechnung hinzufügen**, um der Zone Kubernetes- oder Supervisor-Cluster hinzuzufügen. Wenn Sie mit einem externen Cluster arbeiten, wird er automatisch in vRealize Automation Cloud Assembly integriert, wenn Sie ihn auswählen.

Sie können Kubernetes-Namespaces auf der Seite „Kubernetes-Cluster“ in vRealize Automation Cloud Assembly zum Cluster hinzufügen.

Ergebnisse

Kubernetes-Zonen sind für die Verwendung mit vRealize Automation Cloud Assembly-Bereitstellungen konfiguriert.

Nächste Schritte

Weisen Sie die Kubernetes-Zone einem Projekt zu.

- 1 Wählen Sie **Infrastruktur > Verwaltung > Projekte** aus und wählen Sie dann das Projekt aus, das Sie Ihrer Kubernetes-Zone zuordnen möchten.
- 2 Klicken Sie auf der Seite „Projekt“ auf die Registerkarte „Kubernetes-Bereitstellung“.
- 3 Klicken Sie auf **Kubernetes Zone hinzufügen** und fügen Sie die soeben erstellte Zone hinzu. Sie können bei Bedarf mehrere Zonen hinzufügen und auch die Priorität für die Zonen festlegen.
- 4 Klicken Sie auf **Speichern**.

Nachdem Sie einem Projekt eine Zone zugewiesen haben, können Sie die Seite „Cloud-Vorlagen“ auf der Registerkarte „Design“ verwenden, um eine Bereitstellung basierend auf der Kubernetes-Zone und der Projektkonfiguration bereitzustellen. Diese Seite „Cloud-Vorlagen“ enthält Optionen zum Hinzufügen eines K8S-Clusters, eines K8S-Namespace und eines Supervisor-Namespace. Wählen Sie die entsprechende Option für die Kubernetes-Ressource aus, mit der Sie arbeiten.

Verwenden von Pacific-Supervisor-Clustern und -Namespaces mit vRealize Automation Cloud Assembly

Administratoren können vRealize Automation Cloud Assembly so konfigurieren, dass es Supervisor-Namespaces von einer vorhandenen Pacific-fähigen vSphere-Integration verwendet. Auf diese Weise können Benutzer Namespaces in Cloud-Vorlagen bereitstellen und sie im Service Broker-Katalog anfordern.

In dieser Aufgabe wird beschrieben, wie Sie Supervisor-Cluster mit vRealize Automation Cloud Assembly für die Verwendung in Bereitstellungen hinzufügen und wie Sie Namespaces erstellen oder hinzufügen, mit denen vRealize Automation Cloud Assembly-Projekte und -Benutzer festgelegt werden, die auf bestimmte Kubernetes-Ressourcen zugreifen können. Diese Funktion basiert auf einem geeigneten vSphere-Cloud-Konto statt einer Integration wie z. B. PKS oder OpenShift. Supervisor-Cluster sind mit vSphere verknüpfte benutzerdefinierte Kubernetes-Cluster. Sie machen Kubernetes-APIs für Endbenutzer verfügbar und verwenden ESXi anstelle von Linux als Plattform für Worker-Knoten. Supervisor-Namespaces erleichtern die Zugriffssteuerung für Kubernetes-Ressourcen, da es in der Regel einfacher ist, Richtlinien auf Namespaces anzuwenden als auf einzelne virtuelle Maschinen. Sie können mehrere Namespaces für jeden Supervisor-Cluster erstellen.

Bei Verwendung mit Pacific-fähigen vSphere-Instanzen definieren Kubernetes-Zonen, welche Supervisor-Cluster für die Bereitstellung mit einem Supervisor-Namespace verfügbar sind. Supervisor-Namespaces sind spezifisch für Pacific-fähige vSphere-Instanzen. Sie können eine generische Kubernetes-Ressource nicht für eine Pacific-fähige vSphere-Instanz bereitstellen.

vRealize Automation Cloud Assembly-Benutzer, die als Projekt-Viewer festgelegt wurden, haben nur Anzeigezugriff auf Namespaces, während Projektmitglieder sie bearbeiten können.

Bei Bedarf können Sie die den Namespaces zugeordneten Supervisor-Cluster konfigurieren.

Voraussetzungen

- Um Pacific-Namespaces mit vRealize Automation Cloud Assembly verwenden zu können, müssen Sie einen vSphere 7.x-Endpoint konfiguriert haben. vSphere wird als Teil eines vCenter-Cloud-Kontos installiert. Weitere Informationen hierzu finden Sie unter [Erstellen Sie ein vCenter-Cloud-Konto in vRealize Automation..](#)
- Project Pacific muss in dem vSphere-Cloud-Konto aktiviert sein, und es muss entsprechende Supervisor-Namespaces enthalten.
- Ihr vCenter und Ihre vRealize Automation-Bereitstellung sollten dasselbe Active Directory zum Synchronisieren von Benutzern verwenden. Ist dies nicht der Fall ist, erhalten vRealize Automation-Benutzer keinen automatischen Zugriff auf den Namespace, auch wenn die Bereitstellung weiterhin funktioniert.

Verfahren

- 1 Wählen Sie **Infrastruktur > Konfigurieren > Kubernetes-Zone** in vRealize Automation Cloud Assembly aus.

Auf dieser Seite werden verwaltete Cluster angezeigt, die verwendet werden können. Außerdem erhalten Sie auf dieser Seite die Möglichkeit, zusätzliche Cluster hinzuzufügen. Sie können auf einen der Cluster klicken, um die zugehörigen Details anzuzeigen.

- 2 Wählen Sie **Neue Kubernetes-Zone** aus.
- 3 Geben Sie die Details zum **Konto** für das vSphere-Cloud-Zielkonto an.
- 4 Klicken Sie auf das Suchsymbol im Textfeld, um entweder alle vSphere-Konten anzuzeigen oder nach Namen nach einem Konto zu suchen.
- 5 Geben Sie einen **Namen** und eine **Beschreibung** für die neue Zone ein.
- 6 Fügen Sie bei Bedarf Funktions-Tags hinzu. Weitere Informationen hierzu finden Sie unter [Verwenden von Funktions-Tags in vRealize Automation Cloud Assembly.](#)
- 7 Klicken Sie auf die Registerkarte „Bereitstellung“, um den Supervisor-Cluster auszuwählen, der den Namespaces zugeordnet werden soll.
- 8 Klicken Sie auf **Berechnung hinzufügen**, um die verfügbaren Supervisor-Cluster anzuzeigen und auszuwählen.
- 9 Klicken Sie auf **Hinzufügen**.
- 10 Wählen Sie **Infrastruktur > Verwaltung > Projekte** aus und wählen Sie dann das Projekt aus, das Sie Ihrer Kubernetes-Zone zuordnen möchten.
- 11 Klicken Sie auf der Seite „Projekt“ auf die Registerkarte „Kubernetes-Bereitstellung“.

12 Klicken Sie auf **Kubernetes Zone hinzufügen** und fügen Sie die soeben erstellte Zone hinzu. Sie können bei Bedarf mehrere Zonen hinzufügen und auch die Priorität für die Zonen festlegen.

13 Klicken Sie auf **Speichern**.

Nächste Schritte

Nachdem ein Namespace konfiguriert wurde, wird er auf der Seite **Infrastruktur > Ressourcen > Kubernetes** in vRealize Automation Cloud Assembly für die entsprechenden Benutzer angezeigt. Benutzer können auf der Seite „Übersicht“ auf den Link „Adresse“ klicken, um die vSphere Kubernetes-CLI-Tools zum Verwalten des Namespace zu öffnen. Benutzer müssen als Cloud-Administrator oder Mitglied des Namespace für das angegebene Projekt fungieren, um auf einen Link zu den Details des Supervisor-Namespace zugreifen zu können. Darüber hinaus können Benutzer ein benutzerdefiniertes Kubectl-Plug-In herunterladen, um den Supervisor-Namespace zu verwenden. Benutzer können sich beim Supervisor-Namespace anmelden und ihn wie alle anderen Namespaces verwenden. Anschließend können sie Cloud-Vorlagen erstellen und Anwendungen bereitstellen.

Um den Namespace einer Cloud-Vorlage hinzuzufügen, wählen Sie **Design > Cloud-Vorlage** und wählen eine vorhandene Cloud-Vorlage aus oder erstellen eine neue. Anschließend können Sie das Element „Supervisor-Namespace“ im Menü links auswählen und auf die Arbeitsfläche ziehen.

Nach der Bereitstellung von Cloud-Vorlagen, die einen Supervisor-Namespace enthalten, können Benutzer auch Supervisor-Namespaces aus dem Service Broker-Katalog anfordern. Sie können auch auf die Seite „Bereitstellungen“ in Cloud Assembly klicken, um Informationen zur Bereitstellung anzuzeigen und auf einen Link zuzugreifen, der den Befehl zum Ausführen von der kubectl-Instanz für den Namespace auf vSphere enthält.

Arbeiten mit Kubernetes-Clustern und -Namespaces in vRealize Automation Cloud Assembly

Sie können die Konfiguration von generischen und Pacific-basierten Kubernetes-Clustern und -Namespaces, die als Basis für Kubernetes-Bereitstellungen in vRealize Automation Cloud Assembly dienen, hinzufügen, anzeigen und verwalten.

Sie können Kubernetes-Cluster und -Namespaces anzeigen, hinzufügen und verwalten, auf die Sie auf der Seite **Infrastruktur > Ressourcen > Kubernetes** zugreifen können. In der Regel erleichtert diese Seite die Verwaltung von bereitgestellten Clustern und Namespaces.

- **Cluster:** Ein Cluster ist eine Gruppe von Kubernetes-Knoten, die über eine oder mehrere physische Maschinen verteilt sind. Auf dieser Seite werden bereitgestellte und nicht bereitgestellte Cluster angezeigt, die für die Verwendung in Ihrer vRealize Automation Cloud Assembly-Instanz konfiguriert wurden. Sie können auf einen Cluster klicken, um Informationen über den aktuellen Status anzuzeigen. Wenn Sie einen Cluster bereitstellen, enthält er einen Link zu einer Kubconfig-Datei, auf die nur Cloud-Administratoren zugreifen können. Diese Datei gewährt vollständige Administratorrechte für den Cluster, einschließlich einer Liste von Namespaces.

Supervisor-Cluster sind für vSphere-Instanzen eindeutig und verwenden ESXi anstelle von Linux als Worker-Knoten.

- **Namespaces:** Namespaces sind virtuelle Cluster, die Administratoren die Möglichkeit bieten, Clusterressourcen aufzuteilen. Sie erleichtern die Verwaltung von Ressourcen in großen Gruppen von Benutzern und Organisationen. Als eine Form der rollenbasierten Zugriffssteuerung kann ein Cloud-Administrator Benutzern ermöglichen, Namespaces zu einem Projekt hinzuzufügen, wenn eine Bereitstellung angefordert wird, und diese Namespaces dann später auf der Seite „Kubernetes-Cluster“ zu verwalten. Wenn Sie einen Namespace bereitstellen, enthält er einen Link zu einer kubeconfig-Datei, mit der gültige Benutzer, wie z. B. Entwickler, einige Aspekte dieses Namespace anzeigen und verwalten können.

Supervisor-Namespaces sind nur auf vSphere-Instanzen vorhanden und bieten Kubernetes-ähnlichen Zugriff auf vSphere-Objekte.

Wenn Sie einen neuen oder vorhandenen Cluster konfigurieren, müssen Sie auswählen, ob eine Verbindung mit einer Master-IP-Adresse oder einem Master-Hostnamen hergestellt werden soll.

Arbeiten mit generischen Kubernetes-Clustern in vRealize Automation Cloud Assembly

Sie können mithilfe der Optionen auf dieser Seite neue, vorhandene oder externe Cluster zu vRealize Automation Cloud Assembly hinzufügen.

- 1 Wählen Sie **Infrastruktur > Ressourcen > Kubernetes** aus und bestätigen Sie, dass die Registerkarte „Cluster“ aktiv ist.

Wenn derzeit Cluster für Ihre vRealize Automation Cloud Assembly-Instanz konfiguriert sind, werden diese auf dieser Seite angezeigt.

- 2 Wenn Sie einen neuen oder vorhandenen Cluster hinzufügen oder einen Cluster bereitstellen, wählen Sie die entsprechende Option gemäß der folgenden Tabelle aus.

Option	Beschreibung	Details
Bereitstellen	Neue Cluster zu vRealize Automation Cloud Assembly hinzufügen	Sie müssen das TKGI-Cloud-Konto angeben, dem dieser Cluster bereitgestellt werden soll, sowie den gewünschten Plan und die Anzahl der Knoten.
Vorhandene hinzufügen	Konfigurieren Sie einen vorhandenen Cluster für Ihr Projekt.	Sie müssen das TKGI-Cloud-Konto, den zu verwendenden Cluster und das entsprechende Projekt für den jeweiligen Entwickler angeben. Außerdem müssen Sie den Freigabebereich angeben. Bei globalen Freigaben müssen Sie Ihre Kubernetes-Zonen und -Namespaces entsprechend konfigurieren.
Externe hinzufügen	Fügen Sie vRealize Automation Cloud Assembly einen Vanilla-Kubernetes-Cluster hinzu, der möglicherweise nicht mit TKGI verknüpft ist.	Sie müssen ein Projekt benennen, dem der Cluster zugeordnet ist, die IP-Adresse für den gewünschten Cluster eingeben und einen Cloud-Proxy und die erforderlichen Zertifikatsinformationen eingeben, die zum Herstellen einer Verbindung mit diesem Cluster erforderlich sind.

- 3 Klicken Sie auf **Hinzufügen**, um den Cluster innerhalb von vRealize Automation Cloud Assembly verfügbar zu machen.

Arbeiten mit Kubernetes-Namespace in vRealize Automation Cloud Assembly

Wenn Sie ein Cloud-Administrator sind, helfen Ihnen Namespaces dabei, Kubernetes-Clusterressourcen zu gruppieren und zu verwalten. Wenn Sie ein Benutzer sind, sind Namespaces der Bereich in Kubernetes-Clustern für Ihre Bereitstellungen. Administratoren und Benutzer können auf der Registerkarte „Namespaces“ auf der Seite **Infrastruktur > Ressourcen > Kubernetes** auf Namespaces zugreifen.

gibt es mehrere Möglichkeiten, Kubernetes-Namespace zu Ressourcen in vRealize Automation Cloud Assembly hinzuzufügen. Im folgenden Verfahren wird eine typische Methode beschrieben.

- 1 Wählen Sie **Infrastruktur > Ressourcen > Kubernetes** aus und klicken Sie auf die Registerkarte „Namespaces“.
- 2 Um einen neuen Namespace hinzuzufügen, klicken Sie auf **Neuer Namespace**. Um einen vorhandenen Namespace hinzuzufügen, klicken Sie auf **Namespace hinzufügen**.
- 3 Geben Sie einen **Namen** und eine **Beschreibung** für den Namespace ein.
An dieser Stelle haben Sie einen Namespace für die Verwendung mit Kubernetes-Ressourcen hinzugefügt, aber er ist mit nichts verknüpft.
- 4 Geben Sie den **Cluster** an, den Sie diesem Namespace zuordnen möchten.
- 5 Klicken Sie auf **Erstellen**, um den Namespace zu vRealize Automation Cloud Assembly hinzuzufügen.

Arbeiten mit Supervisor-Clustern und Supervisor-Namespace

Sie können die Konfiguration von Supervisor-Clustern und -Namespaces auf der Kubernetes-Seite in vRealize Automation Cloud Assembly anzeigen und ändern.

- 1 Wählen Sie **Infrastruktur > Ressourcen > Kubernetes** in vRealize Automation Cloud Assembly.
- 2 Wählen Sie **Supervisor-Cluster hinzufügen** aus.
- 3 Geben Sie die Kontodetails für das vSphere-Cloud-Zielkonto an.
- 4 Klicken Sie auf das Suchsymbol im Textfeld für den Supervisor-Cluster, um entweder alle Supervisor-Cluster anzuzeigen oder nach Namen nach einem Cluster zu suchen.
- 5 Wählen Sie den gewünschten Cluster aus und klicken Sie auf **Hinzufügen**.
- 6 Wählen Sie die Registerkarte „Supervisor-Namespace“ aus und klicken Sie auf die Schaltfläche **Neuer Supervisor-Namespace**, um einen neuen Namespace hinzuzufügen.
- 7 Wählen Sie die Registerkarte „Supervisor-Namespace“ aus und klicken Sie auf die Schaltfläche **Neuer Supervisor-Namespace**, um einen neuen Namespace hinzuzufügen.
 - a Wenn Sie einen neuen Namespace erstellen, geben Sie unter **Name** und **Beschreibung** die erforderlichen Informationen ein.

- b Wählen Sie das entsprechende Cloud-**Konto** aus, um es mit dem Namespace zu verknüpfen.
 - c Wählen Sie den **Supervisor-Cluster** aus, um ihn mit diesem Namespace zu verknüpfen.
 - d Wählen Sie das **Projekt** aus, um es mit dem Namespace zu verknüpfen.
 - e Klicken Sie auf **Erstellen**.
- 8 Überprüfen Sie die relevanten Details für den neuen Namespace.

Benutzer und Gruppen, die aktuell auf den Namespace in vSphere zugreifen können, werden auf der Registerkarte „Benutzer“ aufgelistet. Wenn dem Projekt neue Benutzer oder Gruppen hinzugefügt werden, klicken Sie auf die Schaltfläche **Benutzer aktualisieren** auf dieser Registerkarte, um die Liste zu aktualisieren. Die Liste wird nicht automatisch aktualisiert. Daher müssen Sie die Schaltfläche verwenden, um sie zu aktualisieren.

Hinweis Die Synchronisierung von Benutzern ist nur dann sinnvoll, wenn vRealize Automation Cloud Assembly und vCenter mit einem gemeinsamen Active Directory-/LDAP-Dienst konfiguriert sind.

Nachdem ein Namespace konfiguriert wurde, wird er auf der Seite **Infrastruktur > Ressourcen > Kubernetes** in vRealize Automation Cloud Assembly für die entsprechenden Benutzer angezeigt. Benutzer können auf der Seite „Übersicht“ auf den Link „Adresse“ klicken, um die vSphere Kubernetes-CLI-Tools zum Verwalten des Namespace zu öffnen. Benutzer müssen als Cloud-Administrator oder Mitglied des Namespace für das angegebene Projekt fungieren, um auf einen Link zu den Details des Supervisor-Namespace zugreifen zu können. Darüber hinaus können Benutzer ein benutzerdefiniertes Kubectl-Plug-In herunterladen, um den Supervisor-Namespace zu verwenden. Benutzer können sich beim Supervisor-Namespace anmelden und ihn wie alle anderen Namespaces verwenden. Anschließend können sie Cloud-Vorlagen erstellen und Anwendungen bereitstellen.

Hinzufügen von Kubernetes-Komponenten zu Cloud-Vorlagen in vRealize Automation Cloud Assembly

Beim Hinzufügen von Kubernetes-Komponenten zu einer vRealize Automation Cloud Assembly-Cloud-Vorlage können Sie Cluster hinzufügen oder Benutzern das Erstellen von Namespaces in verschiedenen Konfigurationen ermöglichen. Diese Auswahl hängt in der Regel von Ihren Anforderungen an die Zugriffssteuerung, von der Konfiguration Ihrer Kubernetes-Komponenten und von Ihren Bereitstellungsanforderungen ab.

Zum Hinzufügen einer Kubernetes-Komponente zu einer Cloud-Vorlage in vRealize Automation Cloud Assembly wählen Sie **Design > Cloud-Vorlagen** aus, klicken auf **Neu**, suchen anschließend nach der Kubernetes-Option im linken Menü und erweitern die Option. Nehmen Sie dann die gewünschte Auswahl vor, entweder „Cluster“ oder „KBS-Namespace“, indem Sie sie auf die Arbeitsfläche ziehen.

Das Hinzufügen eines mit einem Projekt verknüpften Kubernetes-Clusters zu einer Cloud-Vorlage stellt die einfachste Methode dar, Kubernetes-Ressourcen für gültige Benutzer zur Verfügung zu stellen. Wie andere Cloud Assembly-Ressourcen können Sie Tags in Clustern verwenden, um deren Bereitstellungsort zu steuern. Sie können Tags zum Auswählen einer Zone und eines VMware Tanzu Kubernetes Grid Integrated Edition-Plans (TKGI) während der Zuteilungsphase der Clusterbereitstellung verwenden.

Sobald Sie einen Cluster auf diese Weise hinzugefügt haben, steht er automatisch allen gültigen Benutzern zur Verfügung.

Beispiele für Cloud-Vorlagen

Das erste Beispiel zeigt eine Vorlage für eine einfache Kubernetes-Bereitstellung, die durch Tagging gesteuert wird. Eine Kubernetes-Zone wurde mit zwei Bereitstellungsplänen erstellt, die auf der Seite „Neue Kubernetes-Zone“ konfiguriert wurden. In diesem Fall wurde der Zone ein Tag mit dem Namen `placement:tag` als Funktion hinzugefügt, das zum Abgleichen der analogen Einschränkung in der Cloud-Vorlage verwendet wurde. Wenn mehr als eine Zone mit dem Tag konfiguriert ist, wird diejenige mit der niedrigsten Prioritätsnummer ausgewählt.

```
formatVersion: 1
inputs: {}
resources:
  Cluster_provisioned_from_tag:
    type: Cloud.K8S.Cluster
    properties:
      hostname: 109.129.209.125
      constraints:
        -tag: 'placement tag'
      port: 7003
      workers: 1
      connectBy: hostname
```

Im zweiten Beispiel wird die Einrichtung einer Cloud-Vorlage mit einer Variable mit dem Namen `$(input.hostname)` dargestellt, damit Benutzer beim Anfordern einer Bereitstellung den gewünschten Cluster-Hostnamen eingeben können. Tags können auch verwendet werden, um eine Zone und einen TKGI-Plan während der Ressourcenzuteilungsphase der Clusterbereitstellung auszuwählen.

```
formatVersion: 1
inputs:
  hostname:
    type: string
    title: Cluster hostname
resources:
  Cloud_K8S_Cluster_1:
    type: Cloud.K8S.Cluster
    properties:
      hostname: ${input.hostname}
      port: 8443
      connectBy: hostname
      workers: 1
```

Wenn Sie Namespaces zum Verwalten der Cluster-Nutzung verwenden möchten, können Sie in der Cloud-Vorlage eine Variable mit dem Namen *name: \${input.name}* einrichten, um den Namespace-Namen zu ersetzen, den ein Benutzer beim Anfordern einer Bereitstellung eingibt. Für diese Art der Bereitstellung erstellen Sie eine Vorlage ähnlich dem folgenden Beispiel:

```

1 formatVersion: 1
2 inputs:
3 name:
4   type: string
5   title: "Namespace name"
6 resources:
7   Cloud_K8S_Namespace_1:
8     type: Cloud.K8S.Namespace
9     properties:
10      name: ${input.name}

```

Benutzer können bereitgestellte Cluster über kubeconfig-Dateien verwalten, auf die von der Seite **Infrastruktur > Ressourcen > Kubernetes-Cluster** zugegriffen werden kann. Suchen Sie die Karte auf der Seite für den gewünschten Cluster und klicken Sie auf **Kubeconfig**.

Supervisor-Namespaces in VMware Cloud Templates

Nachstehend finden Sie das Schema für einen einfachen Supervisor-Namespace in einer vRealize Automation Cloud Assembly-Cloud-Vorlage.

```

{
  "title": "Supervisor namespace schema",
  "description": "Request schema for provisioning of Supervisor namespace resource",
  "type": "object",
  "properties": {
    "name": {
      "title": "Name",
      "description": "Alphabetic (a-z and 0-9) string with maximum length of 63 characters. The character '-' is allowed anywhere except the first or last position of the identifier.",
      "type": "string",
      "pattern": "^[a-z0-9-]{1,63}$",
      "ignoreOnUpdate": true
    },
    "description": {
      "title": "Description",
      "description": "An optional description of this Supervisor namespace.",
      "type": "string",
      "ignoreOnUpdate": true
    },
    "constraints": {
      "title": "Constraints",
      "description": "To target the correct resources, blueprint constraints are matched against infrastructure capability tags. Constraints must include the key name. Options include value, negative [!], and hard or soft requirement.",
      "type": "array",
      "recreateOnUpdate": true,
      "items": {
        "type": "object",

```

```

    "properties": {
      "tag": {
        "title": "Tag",
        "description": "Constraint definition in syntax `[!]tag_key[:tag_value]`  
[:hard|soft]` \nExamples:\n```\n!location:eu:hard\n location:us:soft\n!pci\n```\n",
        "type": "string",
        "recreateOnUpdate": true
      }
    }
  },
  "limits": {
    "title": "Limits",
    "description": "Defines namespace resource limits such as pods, services, etc.",
    "type": "array",
    "recreateOnUpdate": false,
    "items": {
      "type": "object",
      "properties": {
        "stateful_set_count": {
          "title": "stateful_set_count",
          "description": "This represents the new value for 'statefulSetCount' option which  
is the maximum number of StatefulSets in the namespace.",
          "type": "integer",
          "recreateOnUpdate": false
        },
        "deployment_count": {
          "title": "deployment_count",
          "description": "This represents the new value for 'deploymentCount' option which  
is the maximum number of deployments in the namespace.",
          "type": "integer",
          "recreateOnUpdate": false
        },
        "cpu_limit_default": {
          "title": "cpu_limit_default",
          "description": "This represents the new value for the default CPU limit (in Mhz)  
for containers in the pod. If specified, this limit should be at least 10 Mhz.",
          "type": "integer",
          "recreateOnUpdate": false
        },
        "config_map_count": {
          "title": "config_map_count",
          "description": "This represents the new value for 'configMapCount' option which  
is the maximum number of ConfigMaps in the namespace.",
          "type": "integer",
          "recreateOnUpdate": false
        },
        "pod_count": {
          "title": "pod_count",
          "description": "This represents the new value for 'podCount' option which is the  
maximum number of pods in the namespace.",
          "type": "integer",
          "recreateOnUpdate": false
        },
        "job_count": {

```

```

        "title": "job_count",
        "description": "This represents the new value for 'jobCount' option which is the
maximum number of jobs in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "secret_count": {
        "title": "secret_count",
        "description": "This represents the new value for 'secretCount' option which is
the maximum number of secrets in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "cpu_limit": {
        "title": "cpu_limit",
        "description": "This represents the new value for 'limits.cpu' option which is
equivalent to the maximum CPU limit (in MHz) across all pods in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "cpu_request_default": {
        "title": "cpu_request_default",
        "description": "This represents the new value for the default CPU request (in
Mhz) for containers in the pod. If specified, this field should be at least 10 MHz.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "memory_limit_default": {
        "title": "memory_limit_default",
        "description": "This represents the new value for the default memory limit (in
mebibytes) for containers in the pod.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "memory_limit": {
        "title": "memory_limit",
        "description": "This represents the new value for 'limits.memory' option which is
equivalent to the maximum memory limit (in mebibytes) across all pods in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "memory_request_default": {
        "title": "memory_request_default",
        "description": "This represents the new value for the default memory request (in
mebibytes) for containers in the pod.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "service_count": {
        "title": "service_count",
        "description": "This represents the new value for 'serviceCount' option which is
the maximum number of services in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },

```

```

        "replica_set_count": {
            "title": "replica_set_count",
            "description": "This represents the new value for 'replicaSetCount' option which
is the maximum number of ReplicaSets in the namespace.",
            "type": "integer",
            "recreateOnUpdate": false
        },
        "replication_controller_count": {
            "title": "replication_controller_count",
            "description": "This represents the new value for 'replicationControllerCount'
option which is the maximum number of ReplicationControllers in the namespace.",
            "type": "integer",
            "recreateOnUpdate": false
        },
        "storage_request_limit": {
            "title": "storage_request_limit",
            "description": "This represents the new value for 'requests.storage' which is the
limit on storage requests (in mebibytes) across all persistent volume claims from pods in the
namespace.",
            "type": "integer",
            "recreateOnUpdate": false
        },
        "persistent_volume_claim_count": {
            "title": "persistent_volume_claim_count",
            "description": "This represents the new value for 'persistentVolumeClaimCount'
option which is the maximum number of PersistentVolumeClaims in the namespace.",
            "type": "integer",
            "recreateOnUpdate": false
        },
        "daemon_set_count": {
            "title": "daemon_set_count",
            "description": "This represents the new value for 'daemonSetCount' option which
is the maximum number of DaemonSets in the namespace.",
            "type": "integer",
            "recreateOnUpdate": false
        }
    },
    "additionalProperties": false
}
},
"required": [
    "name"
]
}

```

VMware Cloud Templates unterstützen die Verwendung von Grenzwerten in Verbindung mit Supervisor-Namespace. Mit Grenzwerten können Sie die Ressourcennutzung für CPUs und Arbeitsspeicher sowie die maximale Anzahl von Pods, die im Namespace von den bereitgestellten Maschinen zugelassen werden, steuern.

```

formatVersion: 1
inputs: {}
resources:

```



```
Cloud_SV_Namespace_1:
  type: Cloud.SV.Namespace
  properties:
    name: '${env.deploymentName}'
    limits:
      - cpu_limit: 1000
        cpu_request_default: 800
        memory_limit: 2000
        memory_limit_default: 1500
        pod_count: 200
```

Verwenden der Erweiterbarkeit von vRealize Automation Cloud Assembly mit Kubernetes

vRealize Automation Cloud Assembly bietet einen Standardsatz von Ereignisthemen, die typischen Aktionen im Zusammenhang mit der Bereitstellung von Kubernetes-Clustern entsprechen. Benutzer können diese Themen nach Bedarf abonnieren und erhalten eine Benachrichtigung, wenn das Ereignis im Zusammenhang mit dem abonnierten Thema auftritt. Sie können vRO-Workflows auch so konfigurieren, dass sie auf der Grundlage von Ereignisbenachrichtigungen ausgeführt werden.

Die folgenden Themen sind zum Abonnieren auf der Seite **Erweiterbarkeit > Bibliothek > Ereignisthemen** in vRealize Automation Cloud Assembly verfügbar. Um diese Themen anzuzeigen, suchen Sie im Textfeld „Ereignisthemen suchen“ nach Kubernetes.

- Kubernetes-Cluster-Zuteilung
- Kubernetes-Cluster nach Bereitstellung
- Kubernetes-Cluster nach Entfernung
- Kubernetes-Cluster-Bereitstellung
- Kubernetes-Cluster-Entfernung

Klicken Sie auf eines der Themen, um das Schema für dieses Thema anzuzeigen, das alle erfassten und übermittelten Informationen anzeigt. Sie können alle dieser Schemainformationen verwenden, um verschiedene Benachrichtigungen und Verwaltungs- sowie Berichterstellungsaufgaben einzurichten.

Sie können Aktionsskripts für CMX-bezogene Aktionen auf der Seite **Erweiterbarkeit > Bibliothek > Aktionen** einrichten. Aktionsskripts können für verschiedene Zwecke verwendet werden: z. B. zum Erstellen eines DNS-Eintrags für die Kubernetes-Cluster-Bereitstellung. Wenn Sie einen DNS-Datensatz erstellen, können Sie das Feld `masternodeips` aus dem Thema „Kubernetes-Cluster nach Bereitstellung“ mit einem Rest-Befehl in einem Aktionsskript zum Erstellen eines DNS-Datensatzes verwenden.

Auf der Seite „Abonnements“ wird die Beziehung zwischen den Ereignisthemen und Aktionsskripten definiert. Sie können diese Komponenten auf der Seite „Abonnements“ in vRealize Automation Cloud Assembly anzeigen und verwalten.

Definition der Konfigurationsverwaltung in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly unterstützt die Integration mit Puppet Enterprise, Ansible Open Source und Ansible Tower, wodurch Bereitstellungen für Konfigurationsabweichungen verwaltet werden können.

Puppet-Integration

Zur Integration der Puppet-basierten Konfigurationsverwaltung muss eine gültige Instanz von Puppet Enterprise in einer Public oder Private Cloud mit einer vSphere-Arbeitslast installiert sein. Sie müssen eine Verbindung zwischen diesem externen System und der vRealize Automation Cloud Assembly-Instanz erstellen. Anschließend können Sie die Puppet-Konfigurationsverwaltung in vRealize Automation Cloud Assembly zur Verfügung stellen, indem Sie sie zu entsprechenden Blueprints hinzufügen.

Der Puppet-Anbieter des vRealize Automation Cloud Assembly-Blueprint-Diensts installiert, konfiguriert und führt den Puppet-Agent in einer bereitgestellten Computing-Ressource aus. Der Puppet-Anbieter unterstützt sowohl SSH- als auch WinRM-Verbindungen mit den folgenden Voraussetzungen:

- SSH-Verbindungen:
 - Zur Ausführung von Befehlen mit `NOPASSWD` muss als Benutzername ein Superuser oder ein Benutzer mit sudo-Berechtigungen angegeben werden.
 - Deaktivieren Sie `requiretty` für den angegebenen Benutzer.
 - cURL muss in der Computing-Ressource der Bereitstellung verfügbar sein.
- WinRM-Verbindungen:
 - PowerShell 2.0 muss in der Computing-Ressource der Bereitstellung verfügbar sein.
 - Konfigurieren Sie die Windows-Vorlage gemäß der Beschreibung in der vRealize Orchestrator-Dokumentation.

Der DevOps-Administrator ist für die Verwaltung der Verbindungen mit einem Puppet Master und für die Anwendung von Puppet-Rollen oder Konfigurationsregeln auf bestimmte Bereitstellungen zuständig. Nach der Bereitstellung werden virtuelle Maschinen, die zur Unterstützung der Konfigurationsverwaltung konfiguriert wurden, beim zugewiesenen Puppet-Master registriert.

Wenn virtuelle Maschinen bereitgestellt werden, können Benutzer einen Puppet-Master als externes System hinzufügen bzw. löschen oder Projekte aktualisieren, die dem Puppet-Master zugewiesen sind. Schließlich können entsprechende Benutzer die Registrierung bereitgestellter virtueller Maschinen mithilfe des Puppet-Masters aufheben, wenn die Maschinen außer Betrieb genommen werden.

Ansible Open Source-Integration

Beim Einrichten einer Ansible-Integration installieren Sie Ansible Open Source gemäß den Installationsanweisungen für Ansible. Weitere Informationen zur Installation finden Sie in der Ansible-Dokumentation.

Ansible aktiviert standardmäßig die Überprüfung von Host-Schlüsseln. Wenn ein Host mit einem anderen Schlüssel in der `known_hosts`-Datei neu installiert wird, wird eine Fehlermeldung angezeigt. Wenn ein Host nicht in der `known_hosts`-Datei aufgeführt ist, müssen Sie den Schlüssel beim Start angeben. Mit der folgenden Einstellung in der Datei `/etc/ansible/ansible.cfg` oder `~/.ansible.cfg` können Sie die Hostschlüsselüberprüfung deaktivieren:

```
[defaults]
host_key_checking = False
localhost_warning = False

[paramiko_connection]
record_host_keys = False

[ssh_connection]
#ssh_args = -C -o ControlMaster=auto -o ControlPersist=60s
ssh_args = -o UserKnownHostsFile=/dev/null
```

Um Fehler bei der Überprüfung der Hostschlüssel zu vermeiden, legen Sie `host_key_checking` und `record_host_keys` auf „False“ fest und fügen eine zusätzliche Option `UserKnownHostsFile=/dev/null` hinzu, die in `ssh_args` festgelegt wird. Wenn die Bestandsliste anfänglich leer ist, warnt Ansible außerdem, dass die Hostliste leer ist. Dies führt dazu, dass die Überprüfung der Playbook-Syntax fehlschlägt.

Im Ansible-Tresor können Sie vertrauliche Informationen, wie z. B. Kennwörter oder Schlüssel, in verschlüsselten Dateien statt in Form von Klartext speichern. Der Tresor ist mit einem Kennwort verschlüsselt. In vRealize Automation Cloud Assembly werden Daten von Ansible wie SSH-Kennwörter für Host-Maschinen im Tresor verschlüsselt. Ansible setzt dabei voraus, dass der Pfad zum Tresor-Kennwort festgelegt wurde.

Sie können die Datei `ansible.cfg` ändern, um den Speicherort der Kennwortdatei anzugeben. Verwenden Sie folgendes Format.

```
vault_password_file = /path to/file.txt
```

Außerdem können Sie die Umgebungsvariable `ANSIBLE_VAULT_PASSWORD_FILE` so festlegen, dass Ansible automatisch nach dem Kennwort sucht. Beispiel:

```
ANSIBLE_VAULT_PASSWORD_FILE=~/.vault_pass.txt.
```

Da die Ansible-Bestandslistendatei von vRealize Automation Cloud Assembly verwaltet wird, müssen Sie sicherstellen, dass der vRealize Automation Cloud Assembly-Benutzer über `rw`-Zugriff auf die Bestandslistendatei verfügt.

```
cat ~/var/tmp/vmware/provider/user_defined_script/${ls -t ~/var/tmp/vmware/provider/
user_defined_script/ | head -1}/log.txt
```

Wenn Sie einen Nicht-Root-Benutzer mit vRealize Automation Cloud Assembly-Open Source-Integration verwenden möchten, benötigen die Benutzer eine Reihe von Berechtigungen zum Ausführen der Befehle, die vom Open Source-Anbieter von vRealize Automation Cloud Assembly verwendet werden. Die folgenden Befehle müssen in der Sudoers-Datei des Benutzers festgelegt werden.

```
Defaults:myuser !requiretty
```

Wenn der Benutzer nicht zu einer Admin-Gruppe gehört, für die keine askpass-Anwendung angegeben ist, legen Sie den folgenden Befehl in der Sudoers-Datei des Benutzers fest:

```
myuser ALL=(ALL) NOPASSWD: ALL
```

Wenn Sie beim Einrichten der Ansible-Integration auf Fehler oder andere Probleme stoßen, finden Sie weitere Informationen in der `log.txt`-Datei auf der Ansible-Steuerungsmaschine. Diese Datei befindet sich im Verzeichnis `'cat~/var/tmp/vmware/provider/user_defined_script/$(ls -t ~/var/tmp/vmware/provider/user_defined_script/ | head -1)/'`.

Ansible Tower-Integration

Unterstützte Betriebssystemtypen

- Red Hat Enterprise Linux 8.0 oder höher 64-Bit (x86), unterstützt nur Ansible Tower 3.5 und höher.
- Red Hat Enterprise Linux 7.4 oder höher 64-Bit (x86).
- CentOS 7.4 oder höher 64-Bit (x86).

Im Folgenden finden Sie eine Beispiel-Bestandslistendatei, die bei der Installation von Ansible Tower generiert wird. Möglicherweise müssen Sie sie für vRealize Automation Cloud Assembly-Integrationszwecke ändern.

```
[root@cava-env8-dev-001359 ansible-tower-setup-bundle-3.5.2-1.el8]# pwd

/root/ansible-tower-install/ansible-tower-setup-bundle-3.5.2-1.el8

[root@cava-env8-dev-001359 ansible-tower-setup-bundle-3.5.2-1.el8]# cat inventory

[tower]

localhost ansible_connection=local


[database]
```

```
[all:vars]

admin_password='VMware1!'

pg_host=''

pg_port=''

pg_database='awx'

pg_username='awx'

pg_password='VMware1!'

rabbitmq_port=5672

rabbitmq_vhost=tower

rabbitmq_username=tower

rabbitmq_password='VMware1!'

rabbitmq_cookie=cookiemonster

# Needs to be true for fqdns and ip addresses

rabbitmq_use_long_name=false

# Isolated Tower nodes automatically generate an RSA key for authentication;

# To disable this behavior, set this value to false

# isolated_key_generation=true
```

Konfigurieren der Puppet Enterprise-Integration in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly unterstützt die Integration mit der Puppet Enterprise-Konfigurationsverwaltung.

Wenn Sie Puppet Enterprise als externes System zu Cloud Assembly hinzufügen, steht es standardmäßig in allen Projekten zur Verfügung. Sie können Puppet auf bestimmte Projekte beschränken.

Zum Hinzufügen einer Puppet Enterprise-Integration müssen Sie über den Namen des Puppet-Masters und den Hostnamen oder die IP-Adresse des Masters verfügen.

Sie finden Puppet-Protokolle am folgenden Speicherort, falls Sie sie auf Fehler überprüfen oder zu Informationszwecken ansehen möchten.

Beschreibung	Speicherort des Protokolls
Protokoll zum Erstellen und Installieren von verwandten Ereignissen	Die Protokolle befinden sich auf der bereitgestellten Maschine im Pfad <code>~/var/tmp/vmware/provider/user_defined_script/\$(ls -t ~/var/tmp/vmware/provider/user_defined_script/ head -1)/</code> . Die vollständigen Protokolle finden Sie in der Datei log.txt . Detaillierte Informationen zu den Puppet-Agentprotokollen finden Sie unter https://puppet.com/docs/puppet/4.8/services_agent_unix.html#logging .
Protokoll für Aufgaben in Bezug auf das Löschen und Ausführen von Puppet	Die Protokolle befinden sich auf der PE unter dem Pfad <code>~/var/tmp/vmware/provider/user_defined_script/\$(ls -t ~/var/tmp/vmware/provider/user_defined_script/ head -1)/</code> . Die vollständigen Protokolle finden Sie in der Datei log.txt .

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Integrationen** aus und klicken Sie auf **Integration hinzufügen**.
- 2 Wählen Sie „Puppet“ aus.
- 3 Geben Sie die erforderlichen Informationen auf der Konfigurationsseite von Puppet ein.
- 4 Klicken Sie auf **Validieren**, um die Integration zu überprüfen.
- 5 Klicken Sie auf **Hinzufügen**.

Ergebnisse

Puppet ist für die Verwendung mit Cloud-Vorlagen verfügbar.

Nächste Schritte

Fügen Sie Puppet-Komponenten zu den gewünschten Cloud-Vorlagen hinzu.

- 1 Wählen Sie unter „Cloud Assembly-Cloud-Vorlagen“ die Option „Puppet“ unter der Überschrift „Inhaltsverwaltung“ im Cloud-Vorlagenmenü aus und ziehen Sie die Puppet-Komponente auf die Arbeitsfläche.
- 2 Geben Sie Puppet-Eigenschaften im Fensterbereich auf der rechten Seite ein.

Eigenschaft	Beschreibung
Master	Geben Sie den Namen der primären Puppet-Maschine ein, die mit dieser Cloud-Vorlage verwendet werden soll.
Umgebung	Wählen Sie die Umgebung für die primäre Puppet-Maschine aus.
Rolle	Wählen Sie die Puppet-Rolle aus, die mit dieser Cloud-Vorlage verwendet werden soll.
Agent-Ausführungsintervall	Die Häufigkeit, mit der der Puppet-Agent die primäre Puppet-Maschine bezüglich Konfigurationsdetails abfragen soll, die auf bereitgestellte, mit dieser Cloud-Vorlage verknüpfte virtuelle Maschinen angewendet werden sollen.

- 3 Klicken Sie im rechten Fensterbereich auf die Registerkarte „Code“, um den YAML-Code für die Eigenschaften der Puppet-Konfiguration anzuzeigen.

Konfigurieren der Ansible Open Source-Integration in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly unterstützt die Integration mit der Ansible Open Source-Konfigurationsverwaltung. Nachdem Sie die Integration konfiguriert haben, können Sie Ansible-Komponenten zu neuen oder vorhandenen Bereitstellungen hinzufügen.

Wenn Sie Ansible Open Source mit vRealize Automation Cloud Assembly integrieren, können Sie es so konfigurieren, dass ein oder mehrere Ansible-Playbooks in einer bestimmten Reihenfolge ausgeführt werden, wenn eine neue Maschine zur Automatisierung der Konfigurationsverwaltung bereitgestellt wird. Sie geben die gewünschten Playbooks in der Cloud-Vorlage für eine Bereitstellung an.

Beim Einrichten einer Ansible-Integration müssen Sie die Ansible Open Source-Hostmaschine sowie den Pfad der Bestandslistendatei angeben, in der Informationen für die Ressourcenverwaltung definiert sind. Darüber hinaus müssen Sie einen Namen und ein Kennwort für den Zugriff auf die Ansible Open Source-Instanz angeben. Wenn Sie eine Ansible-Komponente später zu einer Bereitstellung hinzufügen, können Sie die Verbindung aktualisieren, um die schlüsselbasierte Authentifizierung zu verwenden.

Standardmäßig verwendet Ansible SSH zum Herstellen einer Verbindung mit den physischen Maschinen. Falls Sie Windows-Maschinen wie in der Cloud-Vorlage mit der Windows-Eigenschaft „osType“ angegeben verwenden, wird die Variable `connection_type` automatisch auf `winrm` festgelegt.

Anfänglich verwendet die Ansible-Integration die in der Integration bereitgestellten Benutzer-/Kennwort- oder Benutzer-/Schlüsselanmeldedaten, um eine Verbindung mit der Ansible-Steuerungsmaschine herzustellen. Nach erfolgreicher Verbindungsherstellung werden die bereitgestellten Playbooks in der Cloud-Vorlage auf ihre Syntax überprüft.

Bei erfolgreicher Überprüfung wird in der Ansible-Steuerungsmaschine unter `~/var/tmp/vmware/provider/user_defined_script/` ein Ausführungsordner erstellt. Hierbei handelt es sich um den Speicherort, über den Skripts ausgeführt werden, um den Host zur Bestandsliste hinzuzufügen, die Variablendateien des Hosts zu erstellen, einschließlich der Einrichtung des Authentifizierungsmodus zum Herstellen einer Verbindung mit dem Host, und schließlich die Playbooks auszuführen. An diesem Punkt werden die in der Cloud-Vorlage bereitgestellten Anmeldedaten verwendet, um über die Ansible-Steuerungsmaschine eine Verbindung zum Host herzustellen.

Die Ansible-Integration unterstützt physische Maschinen, die keine IP-Adresse verwenden. Bei Maschinen, die in Public Clouds wie AWS, Azure und GCP bereitgestellt werden, wird die Adresseigenschaft in der erstellten Ressource erst dann mit der öffentlichen IP-Adresse der Maschine versehen, wenn die Maschine mit einem öffentlichen Netzwerk verbunden ist. Für Maschinen, die nicht mit einem öffentlichen Netzwerk verbunden sind, sucht die Ansible-Integration nach der IP-Adresse im Netzwerk, das mit der Maschine verbunden ist. Wenn mehrere Netzwerke angeschlossen sind, sucht die Ansible-Integration nach dem Netzwerk mit dem niedrigsten `deviceIndex`, d. h., dem Index der Netzwerkschnittstellenkarte (NIC), die mit der Maschine verbunden ist. Wenn die Eigenschaft „`deviceIndex`“ nicht im Blueprint angegeben ist, verwendet die Integration das erste angeschlossene Netzwerk.

Unter [Definition der Konfigurationsverwaltung in vRealize Automation Cloud Assembly](#) erhalten Sie weitere Informationen zum Konfigurieren von Ansible Open Source für die Integration in vRealize Automation Cloud Assembly.

Voraussetzungen

- Die Ansible-Steuerungsmaschine muss Ansible Version 2.6.0 oder höher verwenden.
- Der Benutzer muss über Lese-/Schreibzugriff auf das Verzeichnis verfügen, in dem sich die Ansible-Bestandslistendatei befindet. Darüber hinaus muss der Benutzer über Lese-/Schreibzugriff auf die Bestandslistendatei verfügen, sofern sie bereits vorhanden ist.
- Stellen Sie bei Verwendung eines Nicht-Root-Benutzers mit der Option „`sudo`“ sicher, dass Folgendes in der Sudoers-Datei festgelegt ist:

```
Defaults:user_name !requiretty
```

und

```
username ALL=(ALL) NOPASSD: ALL
```

- Stellen Sie sicher, dass die Überprüfung des Hostschlüssels deaktiviert ist, indem Sie `host_key_checking = False` unter `/etc/ansible/ansible.cfg` oder `~/ .ansible.cfg` festlegen.
- Stellen Sie sicher, dass das Tresor-Kennwort festgelegt ist, indem Sie der Datei `/etc/ansible/ansible.cfg` oder `~/ .ansible.cfg` die folgende Zeile hinzufügen:

```
vault password_file = /path/to/password_file
```


Die Tresor-Kennwortdatei enthält das Kennwort im Klartext und wird nur verwendet, wenn Cloud-Vorlagen oder Bereitstellungen eine Kombination aus Benutzername und Kennwort zur Verwendung zwischen ACM und dem Knoten bereitstellen. Siehe hierzu folgendes Beispiel.

```
echo 'myStr0ng9@88w0rd' > ~/.ansible_vault_password.txt
echo 'ANSIBLE_VAULT_PASSWORD_FILE=~/.ansible_vault_password.txt' > ~/.profile
# Instead of this way, you can also set it setting
'vault_password_file=~/.ansible_vault_password.txt' in either /etc/ansible/ansible.cfg or
~/.ansible.cfg
```

- Um bei der Ausführung von Playbooks Ausfälle des Hostschlüssels zu vermeiden, empfiehlt sich die Aufnahme der folgenden Einstellungen in die Datei `/etc/ansible/ansible`.

```
[paramiko_connection]
record_host_keys = False

[ssh_connection]
#ssh_args = -C -o ControlMaster=auto -o ControlPersist=60s
ssh_args = -o UserKnownHostsFile=/dev/null # If you already have any
options set for ssh_args, just add the additional option shown here at the end.
```

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Integrationen** aus und klicken Sie auf **Integration hinzufügen**.
 - 2 Klicken Sie auf „Ansible“.
- Die Seite zum Konfigurieren von Ansible wird angezeigt.
- 3 Geben Sie den Hostnamen, den Pfad der Bestandslistendatei und andere erforderliche Informationen für die Ansible Open Source-Instanz ein.
 - 4 Klicken Sie auf **Validieren**, um die Integration zu überprüfen.
 - 5 Klicken Sie auf **Hinzufügen**.

Ergebnisse

Ansible ist für die Verwendung mit Cloud-Vorlagen verfügbar.

Nächste Schritte

Fügen Sie Ansible-Komponenten zu den gewünschten Cloud-Vorlagen hinzu.

- 1 Wählen Sie auf der Seite mit der Cloud-Vorlagen-Arbeitsfläche im Menü der Cloud-Vorlagenoptionen unter der Überschrift „Konfigurationsverwaltung“ den Eintrag „Ansible“ aus und ziehen Sie die Ansible-Komponente auf die Arbeitsfläche.
- 2 Konfigurieren Sie im Bereich auf der rechten Seite die entsprechenden Ansible-Eigenschaften. Geben Sie beispielsweise die auszuführenden Playbooks an.

In Ansible können Benutzer einem einzelnen Host eine Variable zuweisen und diese dann später in Playbooks verwenden. Mit der Ansible Open Source-Integration können Sie diese Host-Variable in Cloud-Vorlagen angeben. Die Eigenschaft `hostVariables` muss im korrekten YAML-Format vorliegen, wie von der Ansible-Steuerungsmaschine erwartet, und diese Inhalte werden an folgendem Speicherort platziert:

```
parent_directory_of_inventory_file/host_vars/host_ip_address/vra_user_host_vars.yml
```

Der Standardspeicherort der Ansible-Bestandslistendatei wird im Ansible-Konto definiert, wie auf der Seite „Integrationen“ in Cloud Assembly hinzugefügt. Die Ansible-Integration validiert die YAML-Syntax für `hostVariable` in der Cloud-Vorlage nicht, die Ansible-Steuerungsmaschine löst aber im Falle eines falschen Formats oder einer falschen Syntax eine Ausnahme aus, wenn Sie ein Playbook ausführen.

Der folgende Cloud-Vorlagen-YAML-Ausschnitt zeigt ein Beispiel für die Nutzung der Eigenschaft `hostVariables`.

```
Cloud_Ansible_1:
  type: Cloud.Ansible
  properties:
    host: '${resource.AnsibleLinuxVM.*}'
    osType: linux
    account: ansible-CAVA
    username: ${input.username}
    password: ${input.password}
    maxConnectionRetries: 20
    groups:
      - linux_vms
    playbooks:
      provision:
        - /root/ansible-playbooks/install_web_server.yml
    hostVariables: |
      message: Hello ${env.requestedBy}
      project: ${env.projectName}
```

Bei Ansible-Integrationen wird erwartet, dass Anmeldedaten für die Authentifizierung auf eine der folgenden Arten in einer Cloud-Vorlage vorhanden sind:

- Benutzername und Kennwort in der Ansible Ressource.
- Benutzername und `privateKeyFile` in der Ansible-Ressource.
- Benutzername in der Ansible-Ressource und im `privateKey` in der Computing-Ressource durch Angeben von `remoteAccess` auf `generatedPublicPrivateKey`.

Stellen Sie in den Cloud-Vorlagen sicher, dass dem Benutzer, der im Integrationskonto angegeben ist, der Pfad zum Ansible Playbook zugänglich ist. Sie können einen absoluten Pfad verwenden, um den Speicherort des Playbooks anzugeben. dies ist jedoch nicht erforderlich. Es wird ein absoluter Pfad zum Benutzerstartordner empfohlen, damit der Pfad gültig bleibt, auch wenn die Anmeldedaten für die Ansible-Integration im Laufe der Zeit geändert werden.

Konfigurieren der Ansible Tower-Integration in vRealize Automation Cloud Assembly

Sie können Ansible Tower mit vRealize Automation Cloud Assembly integrieren, um die Konfigurationsverwaltung der bereitgestellten Ressourcen zu unterstützen. Nachdem Sie die Integration konfiguriert haben, können Sie mithilfe des Cloud-Vorlagen-Editors Ansible-Komponenten zu neuen oder vorhandenen Bereitstellungen hinzufügen.

vRealize Automation Cloud Assembly unterstützt die Integration mit den Ansible Tower-Versionen 3.5, 3.6 und 3.7.

Voraussetzungen

- Gewähren Sie anderen als Administratorbenutzern die entsprechenden Berechtigungen für den Zugriff auf Ansible Tower. Es gibt zwei Optionen, die für die meisten Konfigurationen funktionieren. Wählen Sie die Option, die für Ihre Konfiguration am besten geeignet ist.
 - Weisen Sie Benutzern die Rollen „Bestandslistenadministrator“ und „Auftragsvorlagenadministrator“ auf Organisationsebene zu.
 - Gewähren Sie Benutzern Administratorberechtigungen für eine bestimmte Bestandsliste und die Rolle „Ausführen“ für alle für die Bereitstellung verwendeten Auftragsvorlagen.
- Sie müssen in Ansible Tower die entsprechenden Anmeldedaten und Vorlagen für die Verwendung mit Ihren Bereitstellungen konfigurieren. Vorlagen definieren die Bestandsliste und das Playbook für die Verwendung mit einer Bereitstellung. Zwischen einer Auftragsvorlage und einem Playbook besteht eine 1:1-Zuordnung. Playbooks verwenden eine YAML-ähnliche Syntax, um mit der Vorlage verknüpfte Aufgaben zu definieren. Verwenden Sie für die meisten typischen Bereitstellungen Maschinenanmeldedaten zur Authentifizierung.
 - a Melden Sie sich bei Ansible Tower an und navigieren Sie zum Abschnitt „Auftragsvorlagen“.
 - b Wählen Sie „Neue Auftragsvorlage hinzufügen“ aus.
 - Wählen Sie die bereits erstellten Anmeldedaten aus. Hierbei handelt es sich um die Anmeldedaten der Maschine, die von Ansible Tower verwaltet werden soll. Für jede Auftragsvorlage kann ein Anmeldedatenobjekt vorhanden sein.
 - Wählen Sie für „Grenzwert“ die Option „Eingabeaufforderung beim Start“ aus. Hiermit wird sichergestellt, dass die Auftragsvorlage für den Knoten ausgeführt wird, der von vRealize Automation Cloud Assembly bereitgestellt oder dessen Bereitstellung aufgehoben wird. Bei nicht ausgewählter Option wird ein Fehler vom Typ „Kein Grenzwert festgelegt“ angezeigt, wenn der Blueprint mit der Auftragsvorlage bereitgestellt wird.
- Sie können die Ausführung der von vRealize Automation Cloud Assembly aufgerufenen Auftragsvorlagen auf der Registerkarte „Ansible Tower-Aufträge“ anzeigen.

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Integrationen** aus und klicken Sie auf **Integration hinzufügen**.
- 2 Klicken Sie auf „Ansible Tower“.
Die Seite zum Konfigurieren von Ansible wird angezeigt.
- 3 Geben Sie unter **Hostname** einen Hostnamen, beispielsweise eine IP-Adresse, sowie andere erforderliche Informationen für die Ansible Tower-Instanz ein.
- 4 Geben Sie den **Benutzernamen** und das **Kennwort** der benutzeroberflächenbasierten Authentifizierung für die entsprechende Ansible Tower-Instanz ein.
- 5 Klicken Sie auf **Überprüfen**, um die Integration zu überprüfen.
- 6 Geben Sie einen geeigneten **Namen** und eine **Beschreibung** für die Integration ein.
- 7 Klicken Sie auf **Hinzufügen**.

Ergebnisse

Ansible Tower ist für die Verwendung mit Cloud-Vorlagen verfügbar.

Nächste Schritte

Fügen Sie Ansible Tower-Komponenten zu den gewünschten Cloud-Vorlagen hinzu. Stellen Sie sicher, dass Sie die entsprechende Auftragsvorlage mit der Ausführungsberechtigung für den im Integrationskonto angegebenen Benutzer angeben.

- 1 Wählen Sie auf der Seite mit der Cloud-Vorlagen-Arbeitsfläche im Menü der Blueprint-Optionen unter der Überschrift „Konfigurationsverwaltung“ den Eintrag „Ansible“ aus und ziehen Sie die Ansible Tower-Komponente auf die Arbeitsfläche.
- 2 Konfigurieren Sie im Bereich auf der rechten Seite die entsprechenden Ansible-Eigenschaften, wie z. B. Auftragsvorlagen.

Vorgehensweise zum Erstellen einer Active Directory-Integration in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly unterstützt die Integration mit Active Directory-Servern, um die sofortige Erstellung von Computerkonten in einer bestimmten Organisationseinheit (OE) innerhalb eines Active Directory-Servers vor der Bereitstellung einer virtuellen Maschine zu ermöglichen. Active Directory unterstützt eine LDAP-Verbindung zum Active Directory-Server.

Eine Active Directory-Richtlinie, die mit einem Projekt verknüpft ist, wird auf alle virtuellen Maschinen angewendet, die im Geltungsbereich dieses Projekts bereitgestellt werden. Benutzer können ein oder mehrere Tags zur selektiven Anwendung der Richtlinie auf virtuelle Maschinen festlegen, die in den Cloud-Zonen mit übereinstimmenden Funktions-Tags bereitgestellt werden.

Für lokale Bereitstellungen ermöglicht die Active Directory-Integration die Einrichtung einer Integritätsüberprüfung, die den Status der Integration und der zugrunde liegenden ABX-Integration anzeigt, auf die diese sich stützt, einschließlich des erforderlichen Erweiterbarkeits-Cloud-Proxy. Bevor Sie eine Active Directory-Richtlinie anwenden, prüft vRealize Automation Cloud Assembly den Status der zugrunde liegenden Integrationen. Wenn die Integration fehlerfrei ist, erstellt vRealize Automation Cloud Assembly die bereitgestellten Computerobjekte im angegebenen Active Directory. Wenn die Integration fehlerhaft ist, überspringt der Bereitstellungsvorgang die Active Directory-Phase während der Bereitstellung.

Voraussetzungen

- Die Active Directory-Integration erfordert eine LDAP-Verbindung zum Active Directory-Server.
- Wenn Sie eine Active Directory-Integration mit einem vCenter lokal konfigurieren, müssen Sie eine ABX-Integration mit einem Erweiterbarkeits-Cloud-Proxy konfigurieren. Wählen Sie **Erweiterbarkeit > Aktivität > Integrationen** und anschließend **Lokale Erweiterbarkeitsaktionen** aus.
- Wenn Sie eine Integration mit Active Directory in der Cloud konfigurieren, müssen Sie über ein Microsoft Azure- oder Amazon Web Services-Konto verfügen.
- Sie müssen über ein mit den entsprechenden Cloud-Zonen konfiguriertes Projekt sowie über Image- und Typzuordnungen für die Verwendung mit der Active Directory-Integration verfügen.
- Die gewünschte OE in Ihrem Active Directory muss vorab erstellt werden, bevor Sie Ihre Active Directory-Integration mit einem Projekt verknüpfen.

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Integrationen** und dann **Neue Integration** aus.
- 2 Klicken Sie auf **Active Directory**.
- 3 Geben Sie auf der Registerkarte **Übersicht** die entsprechenden Namen für LDAP-Host und Umgebung ein.
- 4 Geben Sie den Benutzernamen und das Kennwort für den LDAP-Server an.
- 5 Geben Sie den entsprechenden Basis-DN für die gewünschten Benutzer und Gruppen in Ihrem Active Directory ein.

Hinweis Sie können pro Active Directory-Integration nur einen DN angeben.

- 6 Klicken Sie auf **Validieren**, um sicherzustellen, dass die Integration funktioniert.
- 7 Geben Sie einen Namen und eine Beschreibung für diese Integration ein.
- 8 Klicken Sie auf **Speichern**.

- 9 Klicken Sie auf die Registerkarte **Projekt**, um der Active Directory-Integration ein Projekt hinzuzufügen.

Im Dialogfeld **Projekte hinzufügen** müssen Sie einen Projektnamen und einen relativen DN auswählen. Dieser DN befindet sich innerhalb des auf der Registerkarte „Übersicht“ angegebenen Basis-DN.

- 10 Klicken Sie auf **Speichern**.

Ergebnisse

Sie können das Projekt nun mit Active Directory-Integration mit einer Cloud-Vorlage verknüpfen. Wenn eine Maschine mithilfe dieser Cloud-Vorlage bereitgestellt wird, wird sie im angegebenen Active Directory und in der angegebenen Organisationseinheit vorab bereitgestellt.

Sie können auch eine Tag-basierte Integritätsprüfung für lokale Active Directory-Integrationen wie folgt implementieren.

- 1 Erstellen Sie eine Active Directory-Integration, wie in den vorhergehenden Schritten beschrieben.
- 2 Klicken Sie auf die Registerkarte **Projekt**, um der Active Directory-Integration ein Projekt hinzuzufügen.
- 3 Wählen Sie im Dialogfeld „Projekte hinzufügen“ einen Projektnamen und einen relativen DN aus. Der relative DN muss innerhalb des angegebenen Basis-DN vorhanden sein.
- 4 Fügen Sie entsprechende Tags hinzu. Diese Tags gelten für die Cloud-Zone, auf die die Active Directory-Richtlinie angewendet werden kann.
- 5 Klicken Sie auf „Speichern“.

Der Status der Active Directory-Integration wird für jede Integration auf der Seite **Infrastruktur > Verbindungen > Integrationen** in vRealize Automation Cloud Assembly angezeigt.

Sie können das Projekt mit Active Directory-Integration mit einer Cloud-Vorlage verknüpfen. Wenn eine Maschine mithilfe dieser Vorlage bereitgestellt wird, wird sie im angegebenen Active Directory und in der angegebenen Organisationseinheit vorab bereitgestellt.

Konfigurieren einer VMware SDDC Manager-Integration

Sie können eine VMware SDDC Manager-Integration zu vRealize Automation hinzufügen, um die Verwendung von Arbeitslastdomänen als Teil von VCF-Cloud-Konten (VMware Cloud Foundation) in vRealize Automation zu vereinfachen.

Voraussetzungen

- vRealize Automation unterstützt die Integration nur mit VMware SDDC Manager 4.1 und höher.

Verfahren

- 1 Wählen Sie **Infrastruktur > Verbindungen > Integrationen** aus und klicken Sie auf **Integration hinzufügen**.

2 Wählen Sie SDDC Manager aus.

Die Konfigurationsseite für die SDDC Manager-Integration wird angezeigt.

3 Geben Sie im Abschnitt „Übersicht“ einen **Namen** und eine **Beschreibung** der Integration ein.

4 Geben Sie im Abschnitt „SDDC Manager-Anmeldedaten“ **IP-Adresse/FQDN für SDDC Manager** für die SDDC Manager-Servermaschine ein.

5 Geben Sie den Benutzernamen und das Kennwort für das Administratorkonto ein, das für die erste Verbindung mit dem SDDC Manager verwendet werden soll. Es hat sich bewährt, die Verwendung des Administratorkontos bei der Verbindungsherstellung zu vermeiden. Verwenden Sie ein anderes Konto mit Administratorberechtigungen in SDDC Manager, um Dienstrollen zu erstellen.

Diese Anmeldedaten werden verwendet, um erstmals eine Verbindung mit dem SDDC Manager einzurichten. Dann werden Dienstanmeldedaten erstellt, die bei der Herstellung einer Verbindung mit einem VCF-Cloud-Konto verwendet werden.

6 Klicken Sie auf **Validieren**, um die Verbindung mit dem SDDC Manager zu überprüfen.

7 Klicken Sie auf **Hinzufügen**.

Ergebnisse

Nachdem die Integration erstellt wurde, können Sie die dem SDDC zugeordneten Arbeitslasten auf der Registerkarte „Arbeitslastdomäne“ anzeigen, die auf der Seite der abgeschlossenen Integration angezeigt wird. Darüber hinaus können Sie mit der Integration verknüpfte Arbeitslasten anzeigen und auswählen und dann auf die Schaltfläche **Cloud-Konto hinzufügen** klicken, um eine Seite zum Erstellen eines VCF-Cloud-Kontos zu öffnen, das die ausgewählte Arbeitslast verwenden wird.

Nächste Schritte

Nachdem Sie das VCF-Cloud-Konto konfiguriert haben, wird die Schaltfläche **Cloud einrichten** oben auf der Seite angezeigt. Klicken Sie auf diese Schaltfläche, um den Assistenten für die Einrichtung der VCF-Cloud zu starten.

Integrieren in vRealize Operations Manager

vRealize Automation kann mit vRealize Operations Manager zusammenarbeiten, um eine erweiterte Arbeitslastplatzierung durchzuführen, Metriken zur Bereitstellungsintegrität und zu den virtuellen Maschinen bereitzustellen und die Preisgestaltung anzuzeigen.

Anzahl und Typ der Integrationen

Die Integration zwischen den beiden Produkten muss lokal zu lokal und nicht mit einer Kombination aus lokal und Cloud erfolgen.

Sie können eine vRealize Automation-Instanz in mehrere vRealize Operations Manager-Instanzen integrieren, aber eine vRealize Operations Manager-Instanz kann nur mit einer vRealize Automation-Instanz verbunden werden.

Es ist nicht möglich, ein aggregiertes vRealize Operations Manager-Cluster mit vRealize Automation zu verbinden.

Grundanforderungen für die Integration

Navigieren Sie zur Integration mit vRealize Operations Manager zu **Infrastruktur > Verbindungen > Integrationen**. Zum Hinzufügen der Integration benötigen Sie die vRealize Operations Manager-URL und die Anmeldedaten für das im nächsten Abschnitt beschriebene Anmeldekonto. Darüber hinaus müssen vRealize Automation und vRealize Operations Manager denselben vSphere-Endpoint verwalten.

Anmeldekonto für Integration

In vRealize Operations Manager benötigen Sie ein lokales oder nicht lokales vRealize Operations Manager-Anmeldekonto für die zu verwendende Integration. Das Konto benötigt schreibgeschützte Rechte für die vCenter-Adapterinstanz des vSphere-Endpoints. Beachten Sie, dass ein nicht lokales Konto unter Umständen in vRealize Operations Manager importiert und ihm die schreibgeschützte Rolle zugewiesen werden muss. Für die Integration lautet das Format des Benutzernamens für die Anmeldung mit nicht lokalen Konten *username@domain@authenticated-source*, wie z. B. *jdoe@company.com@workspaceone*. Authentifizierte Ressourcen werden während der Ersteinrichtung des vRealize Operations Manager-Servers definiert.

Weitere Informationen finden Sie in den folgenden Abschnitten. Informationen zur Preisgestaltung finden Sie unter [Definition von Preisgestaltungskarten](#).

Erweiterte Arbeitslastplatzierung mit vRealize Operations Manager

vRealize Automation und vRealize Operations Manager können zusammenarbeiten, um Bereitstellungsarbeitslasten optimal zu positionieren.

Sie aktivieren die Arbeitslastplatzierung auf der Ebene der vSphere-basierten Cloud-Zone. Nur DRS-fähige (Distributed Resource Scheduler) Cluster einer Cloud-Zone eignen sich für erweiterte Platzierung mithilfe von vRealize Operations Manager.

- **vRealize Automation-Platzierung** – Das vRealize Automation-Platzierungsmodul basiert auf der Priorität „Anwendung“. Es berücksichtigt tag-basierte Einschränkungen, Projektmitgliedschaften und die zugehörigen Cloud-Zonen sowie Affinitätsfilter mit Bezug auf Netzwerk, Speicher und Computing. Die Ressourcenplatzierung hängt von all diesen Faktoren und dem Vorhandensein anderer, verwandter Zielressourcen in derselben Bereitstellung ab.
- **vRealize Operations Manager-Platzierung** – vRealize Operations Manager verwendet die Priorität „Betrieb“ für eine optimale Platzierung. Bei der Priorität „Betrieb“ können vergangene Arbeitslasten und hypothetische Vorhersagen in Betracht gezogen werden.

Bei Verwendung erweiterter Arbeitslastplatzierung müssen Sie vRealize Automation-Tagging anwenden, um Geschäftszweckentscheidungen zu implementieren, statt die Optionen des vRealize Operations Manager-Geschäftszwecks zu verwenden.

Bei der Integration in vRealize Operations Manager verfolgt vRealize Automation weiterhin die Priorität „Anwendung“ sowie die zugehörigen Einschränkungen, um Filter für die Zielplatzierung zu erstellen. Ausgehend von diesen Ergebnissen wird dann die Empfehlung von vRealize Operations Manager verwendet, um die Platzierung weiter zu optimieren.

In Ermangelung einer Empfehlung

Wenn Sie eine erweiterte Arbeitslastplatzierung aktivieren und die vRealize Operations Manager-Analyse keine Empfehlungen zurückgibt, können Sie vRealize Automation so konfigurieren, dass in diesem Fall die von der Anwendung vorgesehene Standardplatzierung erfolgt.

Einschränkungen bei der Platzierung der Arbeitslast

Bei der Verwendung von vRealize Operations Manager zum Platzieren von Arbeitslasten gelten bestimmte Einschränkungen.

- vRealize Operations Manager unterstützt keine Platzierung von Arbeitslasten in Ressourcenpools in vCenter Server.
- Wenn vRealize Operations Manager nicht ausgeführt wird, läuft die für die Arbeitslastplatzierung verwendete Zeitüberschreitung zum Aufrufen von vRealize Operations Manager möglicherweise ab.
- Die Platzierung erfolgt nicht über mehrere Cloud-Zonen hinweg. vRealize Automation sendet eine Cloud-Zone an vRealize Operations Manager, um Platzierungsempfehlungen innerhalb dieser Cloud-Zone bereitzustellen.

Aktivieren der Arbeitslastplatzierung

Um die Arbeitslastplatzierung zu aktivieren, müssen Sie für vSphere, vRealize Operations Manager und vRealize Automation Schritte ausführen.

- 1 Stellen Sie in vRealize Automation Cloud Assembly eine Verbindung zu Ihrem vCenter Server-Cloud-Konto her.

Die Optionen befinden sich unter **Infrastruktur > Verbindungen > Cloud-Konten**.

- 2 Stellen Sie in vCenter Server sicher, dass für DRS aktivierte Cluster vorhanden und auf vollständig automatisiert festgelegt sind.
- 3 Stellen Sie in vRealize Operations Manager sicher, dass der gleiche vCenter Server verwaltet wird.

Sie benötigen vRealize Operations Manager 8 oder höher.

- 4 Fügen Sie in vRealize Automation Cloud Assembly die vRealize Operations Manager-Integration hinzu.

Die Optionen befinden sich unter **Infrastruktur > Verbindungen > Integrationen**.

Um die Integration hinzuzufügen, benötigen Sie die unten angezeigte primäre Knoten-URL für vRealize Operations Manager sowie den Benutzernamen und das Kennwort für die Anmeldung.

<https://operations-manager-IP-address-or-FQDN/suite-api>

Klicken Sie nach der Eingabe der Werte auf VALIDIEREN.

- 5 Synchronisieren Sie die Integration mit dem vCenter Server, indem Sie auf SYNCHRONISIEREN klicken.

Synchronisieren Sie auch die Uhrzeiten, zu denen vRealize Automation Cloud Assembly und vRealize Operations Manager mit der Verwaltung eines neuen vCenter Server beginnen.

- 6 Erstellen Sie in vRealize Automation Cloud Assembly eine Cloud-Zone für das vCenter Server-Konto.

Die Optionen befinden sich unter **Infrastruktur > Konfigurieren > Cloud-Zonen**.

- 7 Legen Sie auf der Registerkarte „Übersicht“ der Cloud-Zone die Platzierungsrichtlinie auf ERWEITERT fest.

- 8 Wählen Sie unter „Platzierungsrichtlinie“ aus, ob vRealize Automation zur Standardplatzierung zurückkehren soll, wenn vRealize Operations Manager keine Empfehlungen zurückgibt.

Fehlerbehebung bei der Arbeitslastplatzierung

Wenn vRealize Operations Manager die Arbeitslastplatzierung nicht wie erwartet empfiehlt, überprüfen Sie die Details der Bereitstellungsanforderung in vRealize Automation Cloud Assembly oder vRealize Automation Service Broker.

- 1 Wechseln Sie zu **Infrastruktur > Aktivität > Anforderungen** und klicken Sie auf die Anforderung.
- 2 Sehen Sie sich unter „Anforderungsdetails“ die Zuteilungsphasen an.
Suchen Sie nach Zielen, die erfolgreich oder erfolglos identifiziert wurden.
- 3 Aktivieren Sie unter „Anforderungsdetails“ oben rechts den Dev-Modus.
- 4 Folgen Sie dem Anforderungspfad, um Filterblöcke zu finden.
- 5 Klicken Sie auf einen Filterblock und überprüfen Sie den folgenden Abschnitt.

```
filterName: ComputePlacementPolicyAffinityHostFilter
  v computeLinksBefore
  v computeLinksAfter
  v filteredOutHostsReasons
```

Eintrag	Beschreibung
computeLinksBefore	Liste der potenziellen Platzierungshosts basierend auf vRealize Automation-Algorithmen.
computeLinksAfter	Ausgewählter Platzierungshost.
filteredOutHostsReasons	Meldungen, die beschreiben, warum ein Host ausgewählt oder abgelehnt wurde. Wenn vRealize Operations Manager den Host auswählt, wird die folgende Meldung angezeigt. advance policy filter: Filtered hosts based on recommendation from vROPS.

Kontinuierliche Optimierung mit vRealize Operations Manager

Wenn Sie den vRealize Automation-Adapter in vRealize Operations Manager hinzufügen, erstellt vRealize Operations Manager automatisch ein neues benutzerdefiniertes Datacenter für vRealize Automation-basierte Arbeitslasten.

Bei der kontinuierlichen Optimierung nutzen Sie den Ausgleich und die Umsetzung von Arbeitslasten und verwenden vRealize Automation mit vRealize Operations Manager über die anfängliche Arbeitslastplatzierung hinaus. Wenn Virtualisierungsressourcen verschoben werden oder stärker bzw. weniger stark belastet werden, können die von vRealize Automation bereitgestellten Arbeitslasten nach Bedarf verschoben werden.

- Die kontinuierliche Optimierung erstellt automatisch ein neues benutzerdefiniertes Datacenter in vRealize Operations Manager.

Es gibt ein neues benutzerdefiniertes Datacenter für jede vRealize Automation vSphere Cloud-Zone.

- Das neu erstellte benutzerdefinierte Datacenter enthält alle der Cloud-Zone zugeordneten von vRealize Automation verwalteten Cluster.

Hinweis Erstellen Sie nicht manuell ein gemischtes benutzerdefiniertes Datacenter von vRealize Automation- und vRealize Automation-fremden Clustern.

- Sie verwenden vRealize Operations Manager, um kontinuierliche Optimierung für das neu erstellte, benutzerdefinierte Datacenter auszuführen, das auf vRealize Automation basiert.
- Arbeitslasten können nur in derselben Cloud-Zone oder im selben benutzerdefinierten Datacenter neu verteilt oder verlagert werden.
- Die Optimierung erstellt nie einen neuen vRealize Automation- oder vRealize Operations Manager-Platzierungsverstoß.
 - Wenn Platzierungsverstöße vorliegen, können den Betriebszweck betreffende Probleme in vRealize Operations Manager mittels Optimierung behoben werden.
 - Wenn Platzierungsverstöße vorliegen, können keine den Geschäftszweck betreffenden Probleme mittels Optimierung in vRealize Operations Manager behoben werden.
 Beispiel: Wenn Sie vRealize Operations Manager zum manuellen Verschieben einer virtuellen Maschine in einen Cluster verwendet haben, der Ihre Einschränkungen nicht unterstützt, erkennt vRealize Operations Manager keinen Verstoß und versucht auch nicht, diesen zu beheben.
- Diese Version befolgt den Betriebszweck auf der Ebene des benutzerdefinierten Datacenters. Die Cluster aller vRealize Automation-Mitglieder werden für die gleichen Einstellungen optimiert.

Um einen anderen Betriebszweck für Cluster festzulegen, müssen Sie sie in gesonderten benutzerdefinierten vRealize Automation-Datencentern konfigurieren, die verschiedenen vSphere-Cloud-Zonen zugeordnet sind. Dies ist zum Beispiel der Fall, wenn Sie verschiedene Cluster zum Testen und zur Produktion haben.

- Der vRealize Automation-Anwendungszweck und die in vRealize Automation definierten Einschränkungen werden in allen Optimierungs-, Verlagerungs- oder Neuverteilungsvorgängen berücksichtigt.
- vRealize Operations Manager-Platzierungstags können nicht auf von vRealize Automation bereitgestellte Arbeitslasten angewendet werden.

Zusätzlich wird die geplante Optimierung mit mehreren Maschinen unterstützt. Regelmäßig geplante Optimierungen sind keine Alles-oder-nichts-Prozesse. Wenn Bedingungen das Verschieben der Maschinen unterbrechen, bleiben erfolgreich umgesetzte Maschinen umgesetzt, und der nächste vRealize Operations Manager-Zyklus versucht die übrigen Maschinen umzusetzen, wie bei vRealize Operations Manager üblich. Eine solche nicht vollständig abgeschlossene Optimierung hat in vRealize Automation keine negativen Auswirkungen.

Aktivieren der fortlaufenden Optimierung

Wenn Sie den vRealize Automation-Adapter in vRealize Operations Manager hinzufügen, erstellt vRealize Operations Manager automatisch ein neues, dediziertes Datacenter für vRealize Automation-basierte Arbeitslasten.

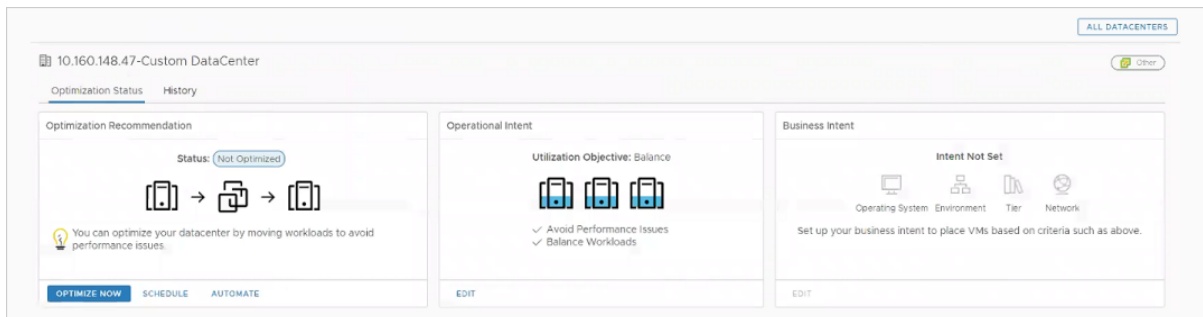
Abgesehen vom Hinzufügen der Integration innerhalb von vRealize Automation Cloud Assembly gibt es keine gesonderten Installationsschritte für die kontinuierliche Optimierung. Sie können als Erstes vRealize Operations Manager für die Umsetzung von Arbeitslasten im neuen Datacenter konfigurieren und verwenden. Weitere Informationen finden Sie im [Beispiel für kontinuierliche Optimierung](#).

Beispiel für kontinuierliche Optimierung

Das folgende Beispiel zeigt einen Ausgleichs-Workflow für die kontinuierliche Optimierung von vRealize Automation mit vRealize Operations Manager.

- 1 Klicken Sie auf der Startseite des vRealize Operations Manager auf **Arbeitslastoptimierung**.
- 2 Wählen Sie das automatisch erstellte vRealize Automation-Datencenter aus.
- 3 Klicken Sie unter **Betriebszweck** auf **Bearbeiten** und wählen Sie **Ausgleichen** aus.

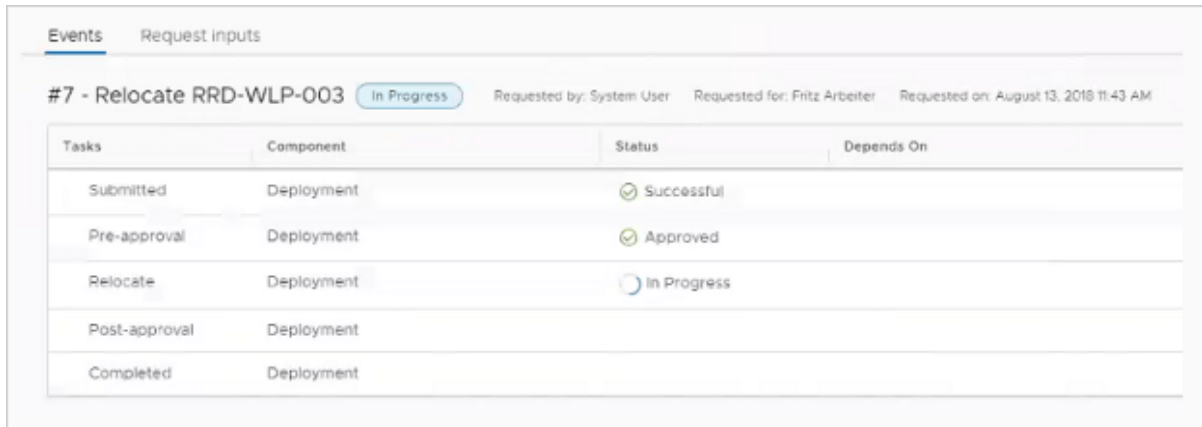
Sie können den Geschäftszweck weder auswählen noch bearbeiten, da dieser deaktiviert ist, wenn das Datacenter für die Optimierung von vRealize Automation bestimmt ist.



- 4 Klicken Sie unter **Optimierungsempfehlung** auf **Jetzt optimieren**.

vRealize Operations Manager zeigt ein Vorher-Nachher-Diagramm des vorgeschlagenen Vorgangs.

- 5 Klicken Sie auf **Weiter**.
- 6 Klicken Sie auf **Aktion beginnen**.
- 7 Überwachen Sie in vRealize Automation, den aktuell durchgeführten Vorgang, indem Sie auf **Bereitstellungen** klicken und den Ereignisstatus betrachten.

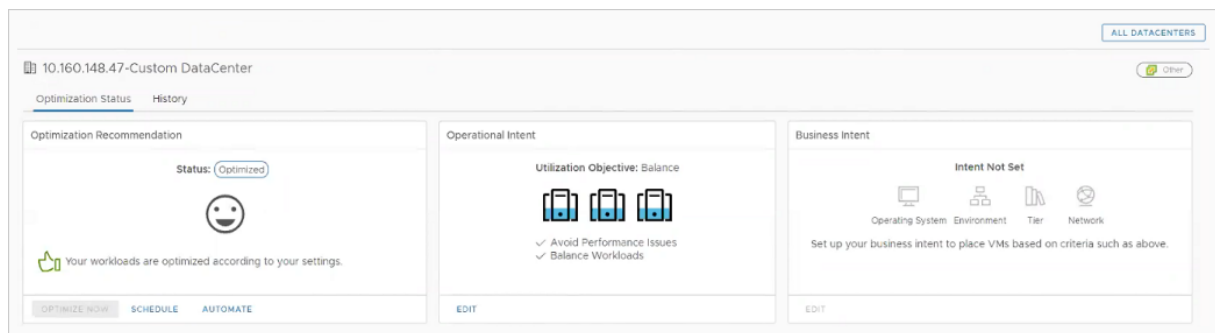


The screenshot shows the 'Events' tab in vRealize Automation. It displays a request titled '#7 - Relocate RRD-WLP-003' with a status of 'In Progress'. The request was made by 'System User' for 'Fritz Arbeiter' on 'August 13, 2018 11:43 AM'. Below this, a table lists the tasks and their statuses:

Tasks	Component	Status	Depends On
Submitted	Deployment	Successful	
Pre-approval	Deployment	Approved	
Relocate	Deployment	In Progress	
Post-approval	Deployment		
Completed	Deployment		

Wenn der Ausgleich abgeschlossen ist, wird vRealize Automation aktualisiert. Auf der Seite „Computing-Ressourcen“ wird angezeigt, dass Maschinen verschoben wurden.

In vRealize Operations Manager aktualisiert die nächste Datensammlung die Anzeige, um zu zeigen, dass die Optimierung abgeschlossen ist.



The screenshot shows the 'Optimization Status' page in vRealize Operations Manager for a custom datacenter '10.160.148.47-Custom DataCenter'. The page is divided into three main sections:

- Optimization Recommendation:** Shows a status of 'Optimized' with a smiley face icon. A message states: 'Your workloads are optimized according to your settings.' Below this are buttons for 'OPTIMIZE NOW', 'SCHEDULE', and 'AUTOMATE'.
- Operational Intent:** Shows a 'Utilization Objective: Balance' with three server icons. It lists two goals: '✓ Avoid Performance Issues' and '✓ Balance Workloads'. There is an 'EDIT' button.
- Business Intent:** Shows 'Intent Not Set' with icons for Operating System, Environment, Tier, and Network. A message says: 'Set up your business intent to place VMs based on criteria such as above.' There is an 'EDIT' button.

In vRealize Operations Manager können Sie den Vorgang mit einem Klick auf **Administration > Verlauf > Letzte Aufgaben** überprüfen.

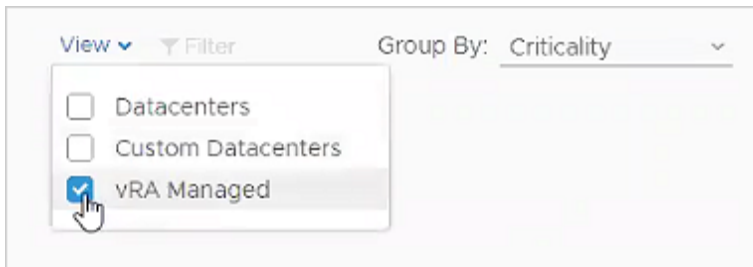
Auffinden von verwalteten vRealize Automation-Datencentern

Sie können mithilfe von vRealize Operations Manager nur die verwalteten vRealize Automation-Datencenter anzeigen.

Verfahren

- 1 Klicken Sie auf der Startseite des vRealize Operations Manager auf **Arbeitslastoptimierung**.
- 2 Klicken Sie oben rechts auf das Drop-down-Menü **Ansicht**.

- 3 Wählen Sie nur die verwalteten vRealize Automation-Datencenter aus.



Überwachung der Bereitstellung basierend auf vRealize Operations Manager

vRealize Automation kann vRealize Operations Manager-Daten über Ihre Bereitstellungen anzeigen.

Durch das Überprüfen des gefilterten Satzes von Metriken direkt in vRealize Automation ersparen Sie sich die Mühe, auf vRealize Operations Manager zuzugreifen oder ihn zu durchsuchen. Obwohl Sie vRealize Operations Manager nicht im Kontext starten können, können Sie sich natürlich anmelden und vRealize Operations Manager bei Bedarf für zusätzliche Daten verwenden.

Aktivieren von vRealize Operations Manager-Daten

Damit vRealize Automation vRealize Operations Manager-Daten anzeigt, fügen Sie die vRealize Operations Manager-Integration hinzu.

Verfahren

- 1 Öffnen Sie in vRealize Operations Manager den Menüpfad **Administration > Lösungen**.
- 2 Vergewissern Sie sich unter **Konfigurierte Adapterinstanzen**, dass Sie einen **vCenter Adapter** für die vSphere-Cloud-Zone haben, auf der vRealize Automation bereitstellt, und dass dieser Daten empfängt.
- 3 Wechseln Sie in vRealize Automation Cloud Assembly zu **Infrastruktur > Verbindungen > Integrationen**.
- 4 Geben Sie die primäre Knoten-URL für vRealize Operations Manager sowie den Benutzernamen und das Kennwort für die Anmeldung bei vRealize Operations Manager ein.
`https://operations-manager-IP-address-or-FQDN/suite-api`
- 5 Klicken Sie auf **Bereitstellungen**, wählen Sie eine Bereitstellung aus und vergewissern Sie sich, dass die Registerkarte „Überwachen“ eingeblendet wird.

Integrität und von vRealize Operations Manager bereitgestellte Warnungen

Wenn die Überwachung aktiviert ist, ruft vRealize Automation Warnungen zur vRealize Operations Manager-Integrität sowie zugehörige Warnungen zu Ihren Bereitstellungen ab.

Um auf die Überwachung zuzugreifen, klicken Sie auf eine Bereitstellung und wählen Sie die Registerkarte **Überwachen** aus. Wenn die Registerkarte fehlt, siehe [Aktivieren von vRealize Operations Manager-Daten](#).

Um Warnungen anzuzeigen, markieren Sie den Namen der Bereitstellung oben in der Komponentenstruktur im linken Fensterbereich.

- Sie können den Schweregrad und den Text der Warnungen überprüfen.
- Filtern und sortieren Sie die Daten in den Spalten, um die Bereiche von Interesse in den Fokus zu rücken.
- Nur Integritäts-Badges und Integritätswarnungen werden angezeigt. Andere Warnungstypen wie Effizienz- oder Risikowarnungen werden nicht unterstützt.

Metriken bereitgestellt durch vRealize Operations Manager

Wenn die Überwachung aktiviert ist, ruft vRealize Automation vRealize Operations Manager-Metriken zu Ihren Bereitstellungen ab.

Um auf die Überwachung zuzugreifen, klicken Sie auf eine Bereitstellung und wählen Sie die Registerkarte **Überwachen** aus. Wenn die Registerkarte fehlt, siehe [Aktivieren von vRealize Operations Manager-Daten](#).

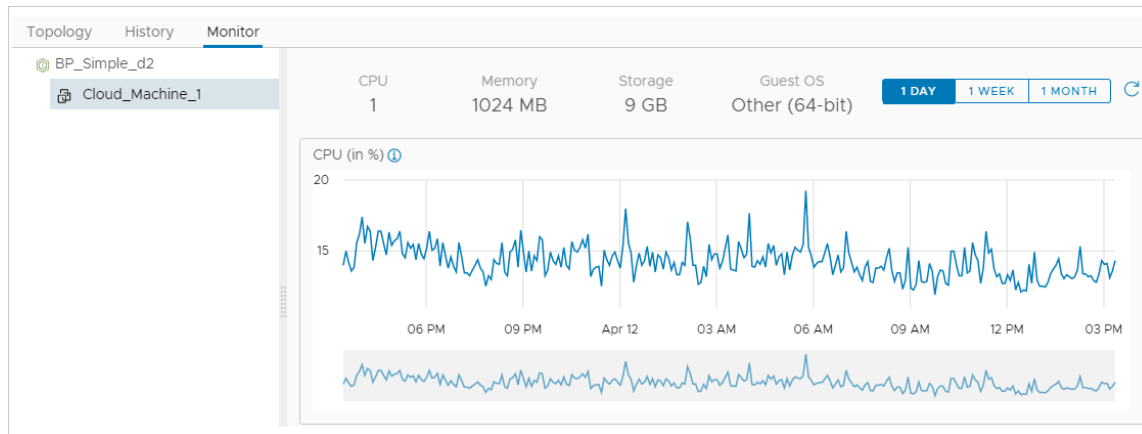
Um Metriken anzuzeigen, erweitern Sie die Komponentenstruktur auf der linken Seite und markieren eine virtuelle Maschine.

- Metriken werden nicht zwischengespeichert. Sie kommen direkt aus vRealize Operations Manager und es kann einen Moment dauern, bis sie geladen werden.
- Nur Metriken von virtuellen Maschinen werden angezeigt. Metriken von anderen Komponenten, wie vCloud Director, Software oder XaaS, werden nicht unterstützt.
- Nur Metriken von vSphere-VMs werden angezeigt. Andere Cloud-Anbieter wie AWS oder Azure werden nicht unterstützt.

Metriken werden als Zeitachsendiagramme angezeigt, die Hoch- und Tiefwerte für die folgenden Messungen anzeigen.

- CPU
- Arbeitsspeicher
- Speicher-IOPS
- Netzwerk-MBPS

Um den Namen der spezifischen Metrik anzuzeigen, klicken Sie auf das blaue Symbol für „Informationen“ oben links in der Ecke der Zeitachse.

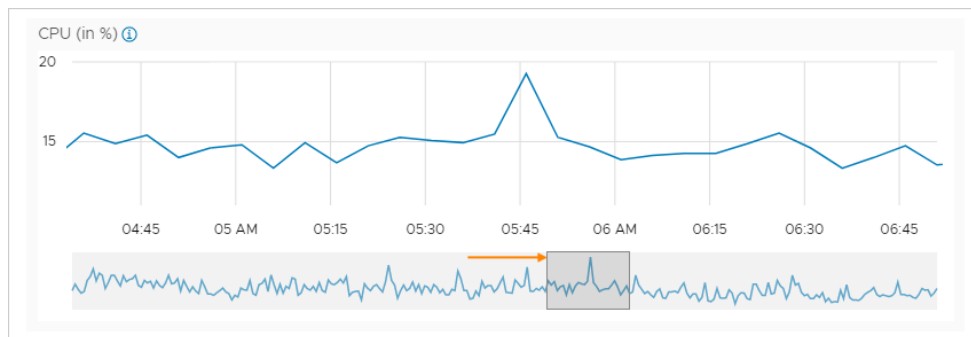


Umsetzung der von vRealize Operations Manager gelieferten Daten

Wenn von vRealize Operations Manager bereitgestellte Metriken ein Problem offen legen, können Sie Problembereiche direkt in vRealize Automation identifizieren.

Zur Anzeige der von vRealize Operations Manager gelieferten Metriken klicken Sie auf eine Bereitstellung und wählen die Registerkarte **Überwachen** aus. Wenn die Registerkarte fehlt, siehe [Aktivieren von vRealize Operations Manager-Daten](#).

Metriken für den letzten Tag, die letzte Woche oder den letzten Monat sind verfügbar. Um einen Bereich von Interesse näher zu beleuchten, wählen Sie einen kleinen Bereich im unteren, schattierten Teil unter der Zeitachse einer Metrik aus:



Definition von Onboarding-Plänen in vRealize Automation Cloud Assembly

Sie verwenden den Onboarding-Plan einer Arbeitslast zur Angabe von Maschinen, deren Daten aus einem Cloud-Kontotyp in einer Zielregion oder einem Datacenter erfasst wurden, die aber noch nicht von einem vRealize Automation Cloud Assembly-Projekt verwaltet werden.

Beim Hinzufügen eines Cloud-Kontos mit Maschinen, die außerhalb von vRealize Automation Cloud Assembly bereitgestellt wurden, werden die Maschinen erst nach ihrer Integration von Cloud Assembly verwaltet. Verwenden Sie einen Onboarding-Plan, um nicht verwaltete Maschinen in die vRealize Automation Cloud Assembly-Verwaltung einzubinden. Sie erstellen einen Plan, befüllen ihn mit Maschinen und führen ihn dann aus, um die Maschinen zu importieren. Mithilfe des Onboarding-Plans können Sie eine Cloud-Vorlage sowie eine oder mehrere Bereitstellungen erstellen.

Sie können eine oder mehrere nicht verwaltete Maschinen in einen einzelnen Plan einbinden. Sie können Maschinen manuell oder mithilfe einer Filterregel auswählen. Filterregeln wählen Maschinen für das Onboarding basierend auf Kriterien wie Maschinenname, Status, IP-Adresse und Tags aus.

- Sie können pro Stunde bis zu 3.500 nicht verwaltete Maschinen innerhalb eines einzelnen Onboarding-Plans einbinden.
- Sie können pro Stunde bis zu 17.000 nicht verwaltete Maschinen innerhalb mehrerer Onboarding-Pläne einbinden.

Maschinen, die für das Arbeitslast-Onboarding verfügbar sind, werden auf der Seite **Ressourcen > Maschinen** für einen bestimmten Cloud-Kontotyp und eine bestimmte Cloud-Region aufgelistet und in der Spalte „Ursprung“ als *Discovered* bezeichnet. Nur Maschinen, für die Daten erfasst wurden, werden aufgelistet. Nach dem Onboarding der Maschinen werden diese in der Spalte „Ursprung“ als *Deployed* angezeigt.

Der Benutzer, der den Onboarding-Plan für die Arbeitslast ausführt, wird automatisch als Maschinenbesitzer zugewiesen.

Beispiele für Onboarding

Beispiele für Onboarding-Techniken finden Sie unter [Beispiel: Integrieren ausgewählter Maschinen als Einzelbereitstellung in vRealize Automation Cloud Assembly](#) und [Beispiel: Integrieren von durch Regeln gefilterten Maschinen als separate Bereitstellungen in vRealize Automation Cloud Assembly](#).

Onboarding-Ereignisabonnements

Ein *Deployment Onboarded*-Ereignis wird erstellt, wenn Sie den Plan ausführen. Mithilfe der Optionen auf der Registerkarte „Erweiterbarkeit“ können Sie diese Bereitstellungsereignisse abonnieren und Aktionen für sie durchführen.

Beispiel: Integrieren ausgewählter Maschinen als Einzelbereitstellung in vRealize Automation Cloud Assembly

In diesem Beispiel können Sie zwei nicht verwaltete Maschinen als vRealize Automation Cloud Assembly-Einzelbereitstellung einbinden und eine einzelnen Cloud-Vorlage für alle Maschinen im Plan erstellen.

Wenn Sie ein Cloud-Konto erstellen, werden die Daten aller Maschinen, die diesem Konto zugeordnet sind, erfasst und anschließend auf der Seite **Infrastruktur > Ressourcen > Maschinen** angezeigt. Wenn das Cloud-Konto über Maschinen verfügt, die außerhalb von vRealize Automation Cloud Assembly bereitgestellt wurden, können Sie einen Onboarding-Plan verwenden, der zulässt, dass die Maschinen von vRealize Automation Cloud Assembly verwaltet werden.

Hinweis Sie können Bereitstellungen lediglich vor deren Integration umbenennen. Nach der Integration ist die Option **Umbenennen** deaktiviert.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die erforderliche Benutzerrolle verfügen. Weitere Informationen finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Weitere Informationen finden Sie unter [Definition von Onboarding-Plänen in vRealize Automation Cloud Assembly](#).
- Erstellen und bereiten Sie ein vRealize Automation Cloud Assembly-Projekt vor.
Dieses Verfahren enthält einige der Schritte aus dem grundlegenden WordPress-Anwendungsfall. Weitere Informationen hierzu finden Sie unter [Lernprogramm: Einrichten und Testen einer Multi-Cloud-Infrastruktur und von Bereitstellungen in vRealize Automation Cloud Assembly](#).
- Erstellen Sie ein Projekt, fügen Sie Benutzer hinzu und weisen Sie Benutzerrollen im Projekt zu. Weitere Informationen hierzu finden Sie unter [Teil 2: Erstellen des vRealize Automation Cloud Assembly-Beispielprojekts](#).
- Erstellen Sie ein Amazon Web Services-Cloud-Konto für das Projekt. Weitere Informationen hierzu finden Sie unter [1. Hinzufügen von Cloud-Konten](#).
Das Amazon Web Services-Cloud-Konto in diesem Verfahren enthält Maschinen, die vor dem Hinzufügen des Cloud-Kontos zu vRealize Automation Cloud Assembly von einer anderen Anwendung als vRealize Automation Cloud Assembly bereitgestellt wurden.
- Stellen Sie sicher, dass die Seite **Maschinen** zu integrierende Maschinen enthält. Weitere Informationen hierzu finden Sie unter [Maschinenressourcen in vRealize Automation](#).

Verfahren

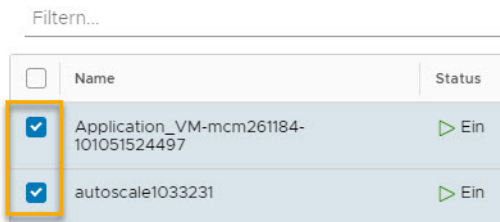
- 1 Navigieren Sie zu **Infrastruktur > Onboarding**.
- 2 Klicken Sie auf **Neuer Onboarding-Plan** und geben Sie Beispielwerte ein.

Einstellung	Beispielwert
Name des Plans	VC-sqa-Bereitstellungen
Beschreibung	Beispiel eines Onboarding-Plans für AWS-Maschine für OurCo-AWS-Cloud-Konto

Einstellung	Beispielwert
Cloud-Konto	OurCo-AWS
Standardprojekt	WordPress

- Klicken Sie auf **Erstellen**.
- Klicken Sie auf der Registerkarte **Bereitstellungen** des Plans auf **Maschinen auswählen**, wählen Sie eine oder mehrere Maschinen aus und klicken Sie auf **OK**.

Maschinen auswählen



- Wählen Sie **Eine Bereitstellung erstellen, die alle Maschinen enthält** aus und klicken Sie auf **Erstellen**.
- Aktivieren Sie das Kontrollkästchen neben dem Namen der neuen Bereitstellung und klicken Sie auf **Cloud-Vorlage...**
- Klicken Sie auf **Cloud-Vorlage im Cloud Assembly-Format erstellen**.
- Geben Sie einen Namen für die Cloud-Vorlage ein und klicken Sie auf **Speichern**.

Hinweis Wenn Ihr Onboarding-Plan eine vSphere-Maschine verwendet, müssen Sie die Cloud-Vorlage bearbeiten, nachdem der Onboarding-Vorgang abgeschlossen ist. Der Onboarding-Vorgang kann die vSphere-Quellmaschine und die zugehörige Maschinenvorlage nicht verknüpfen, und die resultierende Cloud-Vorlage enthält den Eintrag `imageRef: "no image available"` im Cloud-Vorlagencode. Die Cloud-Vorlage kann erst bereitgestellt werden, wenn Sie den korrekten Vorlagennamen im Feld `imageRef`: angeben. Um das Auffinden und Aktualisieren der Cloud-Vorlage nach Abschluss des Onboarding-Vorgangs zu vereinfachen, verwenden Sie die Option **Name der Cloud-Vorlage** auf der Seite **Cloud-Vorlagenkonfiguration** der Bereitstellung. Notieren Sie den automatisch generierten Namen der Cloud-Vorlage oder geben Sie einen Namen Ihrer Wahl ein und notieren Sie ihn. Wenn die Onboarding-Funktion abgeschlossen ist, suchen und öffnen Sie die Cloud-Vorlage und ersetzen Sie den "no image available"-Eintrag im Feld `imageRef`: durch den korrekten Vorlagennamen.

- 9 Aktivieren Sie das Kontrollkästchen neben dem Namen der Bereitstellung, klicken Sie auf **Ausführen** und dann auf der Seite **Plan ausführen** erneut auf **Ausführen**.

Die ausgewählten Amazon Web Services-Maschinen werden als Einzelbereitstellung mit einer begleitenden Cloud-Vorlage integriert.

- 10 Öffnen und untersuchen Sie die Cloud-Vorlage, indem Sie auf die Registerkarte **Cloud-Vorlagen** und dann auf den Namen der Cloud-Vorlage klicken.
- 11 Öffnen und untersuchen Sie die Bereitstellung, indem Sie auf die Registerkarte **Bereitstellungen** und dann auf den Namen der Bereitstellung klicken.

Beispiel: Integrieren von durch Regeln gefilterten Maschinen als separate Bereitstellungen in vRealize Automation Cloud Assembly

In diesem Beispiel verwenden Sie eine Filterregel zur Einbindung von Maschinen mit dem Status „Eingeschaltet“, deren Name mit den Buchstaben „BG“ beginnt. Sie erstellen auch eine separate vRealize Automation Cloud Assembly-Cloud-Vorlage und eine Bereitstellung für jede Maschine im Plan.

Wenn Sie ein Cloud-Konto erstellen, werden die Daten aller Maschinen, die diesem Konto zugeordnet sind, erfasst und anschließend auf der Seite **Infrastruktur > Ressourcen > Maschinen** angezeigt. Wenn das Cloud-Konto über Maschinen verfügt, die außerhalb von vRealize Automation Cloud Assembly bereitgestellt wurden, können Sie einen Onboarding-Plan verwenden, der zulässt, dass die Maschinen von vRealize Automation Cloud Assembly verwaltet werden.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die erforderliche Benutzerrolle verfügen. Weitere Informationen finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Weitere Informationen finden Sie unter [Definition von Onboarding-Plänen in vRealize Automation Cloud Assembly](#).
- Erstellen und bereiten Sie ein vRealize Automation Cloud Assembly-Projekt vor und befüllen Sie es mit einem oder mehreren Cloud-Konten.

Dies umfasst einige grundlegende Schritte im geführten Setup-Verfahren.

- Erstellen Sie ein Projekt, fügen Sie Benutzer hinzu und weisen Sie Benutzerrollen im Projekt zu. Weitere Informationen hierzu finden Sie unter [Teil 2: Erstellen des vRealize Automation Cloud Assembly-Beispielprojekts](#).
- Erstellen Sie ein oder mehrere Cloud-Konten in festgelegten Regionen für das Projekt.
- Stellen Sie sicher, dass die Seite **Maschinen** zu integrierende Maschinen enthält. Weitere Informationen hierzu finden Sie unter [Maschinenressourcen in vRealize Automation](#).

Verfahren

- 1 Navigieren Sie zu **Infrastruktur > Onboarding**.

2 Klicken Sie auf **Neuer Onboarding-Plan** und geben Sie Werte ein.

Einstellung	Beispielwert
Name des Plans	ob_rules_1
Beschreibung	Integration von Maschinen mit rules1
Cloud-Konto	rs-aws
Standardprojekt	rs-project

Neuer Onboarding-Plan



Planname

Beschreibung

Voraussetzung

Fügen Sie das Cloud-Konto hinzu und erstellen Sie Cloud-Zonen für Computing-Ressourcen, in denen sich die einzubindenden Maschinen befinden. Erstellen Sie ein Projekt mit mindestens einem Benutzer und erteilen Sie dem Projekt Zugriff auf die Cloud-Zonen.

Cloud-Konto  

Standardprojekt  

ABBRECHEN

ERSTELLEN

3 Klicken Sie auf **Erstellen**.

ob_rules_1

Übersicht Regeln Maschinen Bereitstellungen

Planname: ob_rules_1

Beschreibung: Machine onboarding with rules1

Planstatus:

Letzte Ausführung: Niemals

Quellinformationen

Cloud-Konto: 346test_vc_account ⓘ

Tag-Schlüssel der Bereitstellung: ⓘ

Übernehmen

Zielkonfiguration

Standardprojekt: Q_123 ⓘ ⓘ

SPEICHERN AUSFÜHREN ABBRECHEN

4 Klicken Sie auf die Registerkarte **Regeln** und dann auf **Regel hinzufügen**.

Sie können eine oder mehrere Regeln erstellen, um eine Gruppe von Maschinen für das Onboarding auf Basis bestimmter Maschineneigenschaften auszuwählen.

ob_rules_1

Übersicht Regeln Maschinen Bereitstellungen

Verwenden Sie Regeln, um diesem Plan Maschinen hinzuzufügen. ⓘ

REGEL HINZUFÜGEN BEARBEITEN LÖSCHEN

<input type="checkbox"/>	Name	Status
--------------------------	------	--------

5 Geben Sie einen Regelnamen ein, wie z. B. **ob_rules_1**.

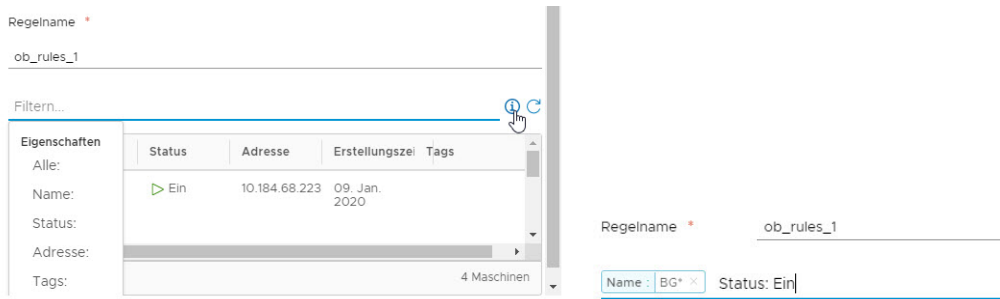
Hinzufügen Regel

Erstellen Eine filterbasierte Regel, die zum Befüllen von Maschinen in diesem Plan verwendet wird.

Regelname * ob_rules_1

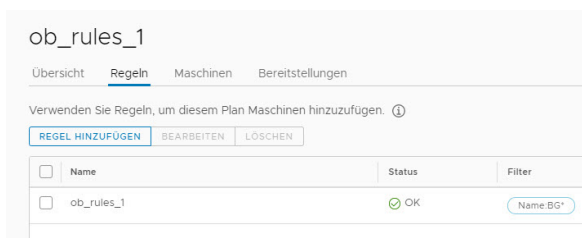
6 Erstellen Sie die Regel durch Hinzufügen von Filtern.

Für dieses Beispiel verwenden Sie die Filter **Status** und **Name** im Dropdown-Menü **Filter**, um alle Maschinen anzugeben, deren Name BG* enthält und deren Status On lautet.

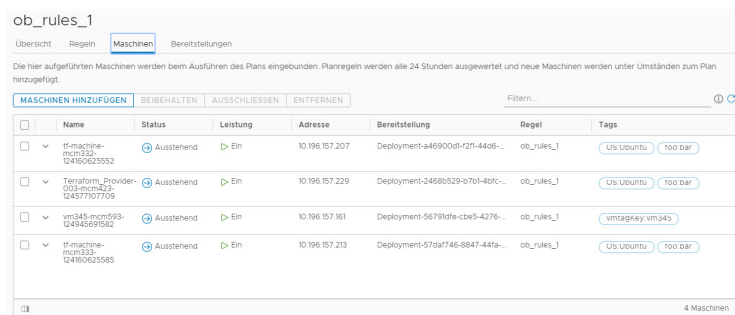


7 Klicken Sie auf **Speichern**.

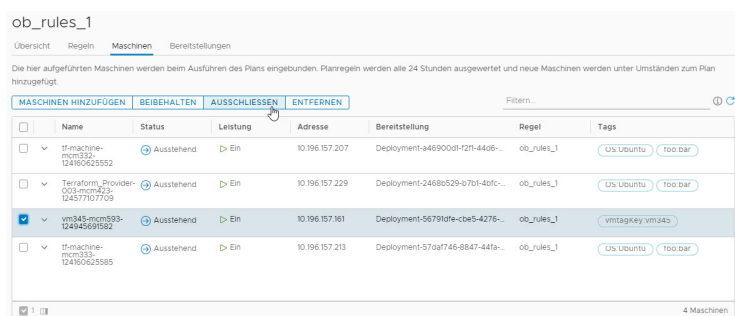
In diesem Beispiel wird eine einzige Regel verwendet. Sie können jedoch zusätzliche Regeln festlegen.



8 Klicken Sie auf die Registerkarte **Maschinen**. In diesem Beispiel werden vier Maschinen ausgewählt. Der Name dreier Maschinen beginnt mit den Buchstaben BG, und der Name einer Maschine enthält die Buchstaben BG.



9 Entfernen Sie die Maschine, deren Name nicht mit BG beginnt, indem Sie das zugehörige Kontrollkästchen aktivieren und dann auf **Ausschließen** klicken.



10 Klicken Sie auf die Registerkarte **Bereitstellungen**.

Die drei Maschinen, die mit den Buchstaben **BG** beginnen und **On** sind, können bereitgestellt werden. Standardmäßig werden für jede Maschine eine eigene Cloud-Vorlage und eine eigene Bereitstellung erstellt.

ob_rules_1

Übersicht Regeln Maschinen **Bereitstellungen**

Diese Bereitstellungen werden während der Planausführung erstellt oder aktualisiert. Standardmäßig wird jede hinzugefügte Maschine in einer eigenen Cloud Assembly-Bereitstellung platziert.

UMBENENNEN BLUEPRINT ENTFERNEN

<input type="checkbox"/>	Name der Bereitstellung	Status	Blueprint erstellen	Komponenten										
<input checked="" type="checkbox"/>	Deployment-2468b529-b701-4bfc-a0ff-a3e074a6d35	OK		1										
	<table border="1"> <thead> <tr> <th>Komponentenname</th> <th>Status</th> <th>Typ</th> <th>Adresse</th> <th>Tags</th> </tr> </thead> <tbody> <tr> <td>Terraform_Provider-003-mcm423-124577107709</td> <td>OK</td> <td>Maschine</td> <td></td> <td>Us:Ubuntu too bar</td> </tr> </tbody> </table>				Komponentenname	Status	Typ	Adresse	Tags	Terraform_Provider-003-mcm423-124577107709	OK	Maschine		Us:Ubuntu too bar
Komponentenname	Status	Typ	Adresse	Tags										
Terraform_Provider-003-mcm423-124577107709	OK	Maschine		Us:Ubuntu too bar										
<input type="checkbox"/>	Deployment-57da746-8847-44fa-86c4-4f36079fb362	OK		1										
	<table border="1"> <thead> <tr> <th>Komponentenname</th> <th>Status</th> <th>Typ</th> <th>Adresse</th> <th>Tags</th> </tr> </thead> <tbody> <tr> <td>tf-machine-mcm333-124160625585</td> <td>OK</td> <td>Maschine</td> <td></td> <td>Us:Ubuntu too bar</td> </tr> </tbody> </table>				Komponentenname	Status	Typ	Adresse	Tags	tf-machine-mcm333-124160625585	OK	Maschine		Us:Ubuntu too bar
Komponentenname	Status	Typ	Adresse	Tags										
tf-machine-mcm333-124160625585	OK	Maschine		Us:Ubuntu too bar										
<input type="checkbox"/>	Deployment-a46900d1-f2f1-4406-8906-9202785d1854	OK		1										
	<table border="1"> <thead> <tr> <th>Komponentenname</th> <th>Status</th> <th>Typ</th> <th>Adresse</th> <th>Tags</th> </tr> </thead> <tbody> <tr> <td>tf-machine-mcm332-124160625552</td> <td>OK</td> <td>Maschine</td> <td></td> <td>Us:Ubuntu too bar</td> </tr> </tbody> </table>				Komponentenname	Status	Typ	Adresse	Tags	tf-machine-mcm332-124160625552	OK	Maschine		Us:Ubuntu too bar
Komponentenname	Status	Typ	Adresse	Tags										
tf-machine-mcm332-124160625552	OK	Maschine		Us:Ubuntu too bar										

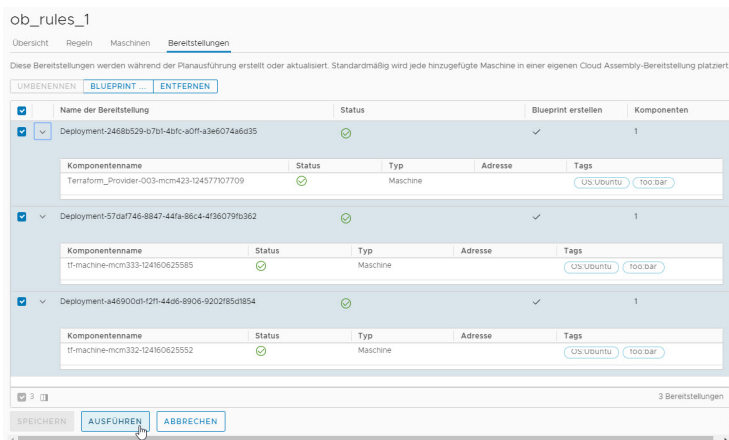
3 Bereitstellungen

SPEICHERN AUSFÜHREN ABBRECHEN

- Aktivieren Sie das Kontrollkästchen neben den drei Bereitstellungs-namen, klicken Sie auf **Cloud-Vorlagen**, dann auf **Cloud-Vorlage im Cloud Assembly-Format erstellen** und anschließend auf **Speichern**.

Hinweis Wenn Ihr Onboarding-Plan eine vSphere-Maschine verwendet, müssen Sie die Cloud-Vorlage bearbeiten, nachdem der Onboarding-Vorgang abgeschlossen ist. Der Onboarding-Vorgang kann die vSphere-Quellmaschine und die zugehörige Maschinenvorlage nicht verknüpfen, und die resultierende Cloud-Vorlage enthält den Eintrag `imageRef: "no image available"` im Cloud-Vorlagencode. Die Cloud-Vorlage kann erst bereitgestellt werden, wenn Sie den korrekten Vorlagennamen im Feld `imageRef:` angeben. Um das Auffinden und Aktualisieren der Cloud-Vorlage nach Abschluss des Onboarding-Vorgangs zu vereinfachen, verwenden Sie die Option **Name der Cloud-Vorlage** auf der Seite **Cloud-Vorlagenkonfiguration** der Bereitstellung. Notieren Sie den automatisch generierten Namen der Cloud-Vorlage oder geben Sie einen Namen Ihrer Wahl ein und notieren Sie ihn. Wenn die Onboarding-Funktion abgeschlossen ist, suchen und öffnen Sie die Cloud-Vorlage und ersetzen Sie den Eintrag `"no image available"` im Feld `imageRef:` durch den korrekten Vorlagennamen.

- 12 Aktivieren Sie auf der Seite **Bereitstellungen** das Kontrollkästchen neben den drei Bereitstellungsnamen und klicken Sie auf **Ausführen**.



- 13 Wenn Sie zur Bestätigung aufgefordert werden, klicken Sie auf **Ausführen**, um die Maschinen zu integrieren.

Plan ausführen ×

Planname	ob_rules_1
Beschreibung	Machine onboarding with rules1
Cloud-Konto	346test_vc_account
Standardprojekt	123
Bereitstellungen	3
Letzte Ausführung	Niemals

ABBRECHEN
AUSFÜHREN

Der Plan wird ausgeführt, und die Maschinen werden in vRealize Automation Cloud Assembly verwaltet. Es werden für jede Maschine eine eigene Cloud-Vorlage und eine eigene Bereitstellung erstellt.

Erweiterte Konfiguration für vRealize Automation Cloud Assembly-Umgebung

Sie können Ihre vRealize Automation Cloud Assembly-Umgebung so konfigurieren, dass Projektkonfiguration, -integration und -bereitstellung weiter unterstützt werden.

Weitere Informationen zu Verwaltungsmethoden, wie z. B. die Verwendung von Benutzern und Protokollen sowie der Beitritt zum Programm zur Verbesserung der Benutzerfreundlichkeit bzw. das Verlassen des Programms, finden Sie in der Hilfe unter [Verwalten von vRealize Automation](#).

Vorgehensweise zum Integrieren eines Internet-Proxyservers für vRealize Automation

Für vRealize Automation-Installationen in isolierten Netzwerken ohne direkten Internetzugriff können Sie einen Internet-Proxyserver so einsetzen, dass die „Internet gemäß Proxy“-Funktionen zugelassen werden. Der Internet-Proxyserver unterstützt HTTP und HTTPS.

Um Public Cloud-Anbieter wie Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) sowie externe Integrationspunkte wie IPAM, Ansible und Puppet mit vRealize Automation zu konfigurieren und zu verwenden, müssen Sie einen Internet-Proxyserver für den Zugriff auf einen internen vRealize Automation-Internet-Proxyserver konfigurieren.

vRealize Automation enthält einen internen Proxyserver, der mit Ihrem Internet-Proxyserver kommuniziert. Dieser Server kommuniziert mit Ihrem Proxyserver, wenn er mit dem Befehl `vracli proxy set ...` konfiguriert wurde. Wenn Sie keinen Internet-Proxyserver für Ihre Organisation konfiguriert haben, versucht der interne vRealize Automation-Proxyserver, eine direkte Verbindung mit dem Internet herzustellen.

Sie können vRealize Automation so einrichten, dass ein Internet-Proxyserver mithilfe des bereitgestellten Befehlszeilen-Dienstprogramms `vracli` verwendet wird. Informationen zur Verwendung der `vracli`-API finden Sie unter Verwendung des `--help`-Arguments in der `vracli`-Befehlszeile, z. B. `vracli proxy --help`.

Der Zugriff auf den Internet-Proxyserver erfordert die Verwendung von lokalen eingebetteten Steuerelementen mit aktionsbasierter Erweiterbarkeit (ABX), die in vRealize Automation integriert sind.

Hinweis Der Zugriff auf Workspace ONE Access (zuvor VMware Identity Manager) über den Internet-Proxy wird nicht unterstützt. Sie können den Befehl `vracli set vidm` nicht für den Zugriff auf Workspace ONE Access über den Internet-Proxyserver verwenden.

Der interne Proxyserver erfordert IPv4 als Standard-IP-Format. Es sind keine Internet-Protokolleinschränkungen, Authentifizierungs- oder Man-in-the-Middle-Aktionen für den TLS (HTTPS)-zertifizierten Datenverkehr erforderlich.

Voraussetzungen

- Stellen Sie sicher, dass Sie über einen vorhandenen als Internet-Proxyserver zu verwendenden HTTP- oder HTTPS-Server in dem vRealize Automation-Netzwerk verfügen, das den ausgehenden Datenverkehr an externe Sites weiterleiten kann. Die Verbindung muss für IPv4 konfiguriert werden.
- Stellen Sie sicher, dass der Ziel-Internet-Proxyserver für die Unterstützung von IPv4 statt IPv6 als IP-Standardformat konfiguriert ist.
- Wenn der Internet-Proxyserver TLS verwendet und eine HTTPS-Verbindung mit seinen Clients benötigt, müssen Sie das Serverzertifikat mithilfe eines der folgenden Befehle importieren, bevor Sie die Proxy-Konfiguration festlegen.
 - `vracli certificate proxy --set path_to_proxy_certificate.pem`

- `vracli certificate proxy --set stdin`

Verwenden Sie den Parameter `stdin` für die interaktive Eingabe.

Verfahren

- 1 Erstellen Sie eine Proxy-Konfiguration für die Pods oder Container, die von den Kubernetes verwendet werden. In diesem Beispiel wird über das HTTP-Schema auf den Proxyserver zugegriffen.

```
vracli proxy set --host http://proxy.vmware.com:3128
```

- 2 Zeigen Sie die Proxy-Konfiguration an.

```
vracli proxy show
```

Das Ergebnis ähnelt Folgendem:

```
{
  "enabled": true,
  "host": "10.244.4.51",
  "java-proxy-exclude": "*.local|*.localdomain|localhost|10.244.*|
192.168.*|172.16.*|kubernetes|sc2-rdops-vm06-dhcp-198-120.eng.vmware.com|10.192.204.9|
*.eng.vmware.com|sc2-rdops-vm06-dhcp-204-9.eng.vmware.com|10.192.213.146|sc2-rdops-vm06-
dhcp-213-146.eng.vmware.com|10.192.213.151|sc2-rdops-vm06-dhcp-213-151.eng.vmware.com",
  "java-user": null,
  "password": null,
  "port": 3128,
  "proxy-
exclude": ".local,.localdomain,localhost,10.244.,192.168.,172.16.,kubernetes,sc2-
rdops-vm06-dhcp-198-120.eng.vmware.com,10.192.204.9,.eng.vmware.com,sc2-
rdops-vm06-dhcp-204-9.eng.vmware.com,10.192.213.146,sc2-rdops-vm06-
dhcp-213-146.eng.vmware.com,10.192.213.151,sc2-rdops-vm06-dhcp-213-151.eng.vmware.com",
  "scheme": "http",
  "upstream_proxy_host": null,
  "upstream_proxy_password_encoded": "",
  "upstream_proxy_port": null,
  "upstream_proxy_user_encoded": "",
  "user": null,
  "internal.proxy.config": "dns_v4_first on \nhttp_port
0.0.0.0:3128\nlogformat squid %ts.%03tu %6tr %>a %Ss/%03>Hs
%<st %rm %ru %[un %Sh/%<a %mt\naccess_log stdio:/tmp/logger squid\ncoredump_dir /\ncache
deny all \nappend_domain .prelude.svc.cluster.local\nacl mylan src 10.0.0.0/8\nacl mylan
src 127.0.0.0/8\nacl mylan src 192.168.3.0/24\nacl proxy-exclude dstdomain .local\nacl
proxy-exclude dstdomain .localdomain\nacl proxy-exclude dstdomain localhost\nacl
proxy-exclude dstdomain 10.244.\n_acl proxy-exclude dstdomain 192.168.\n_acl proxy-exclude
dstdomain 172.16.\n_acl proxy-exclude dstdomain kubernetes\n_acl proxy-exclude dstdomain
10.192.204.9\n_acl proxy-exclude dstdomain .eng.vmware.com\n_acl proxy-exclude dstdomain
```

```
10.192.213.146\nacl proxy-exclude dstdomain 10.192.213.151\nalways_direct allow proxy-
exclude\nhttp_access allow mylan\nhttp_access deny all\n# End autogen configuration\n",
    "internal.proxy.config.type": "default"
}
```

Hinweis Wenn Sie einen Internet-Proxyserver für Ihre Organisation konfiguriert haben, wird im obigen Beispiel "internal.proxy.config.type": "non-default" anstelle von 'default' angezeigt. Aus Sicherheitsgründen wird das Kennwort nicht angezeigt.

Hinweis Wenn Sie den Parameter `--proxy-exclude` verwenden, müssen Sie die Standardwerte bearbeiten. Wenn Sie z. B. `acme.com` als Domäne hinzufügen möchten, auf die über den Internet-Proxyserver nicht zugegriffen werden kann, führen Sie die folgenden Schritte aus:

- a Geben Sie `vracli proxy default-no-proxy` ein, um die standardmäßigen `proxy-exclude`-Einstellungen zu erhalten. Dies ist eine Liste der automatisch erstellten Domänen und Netzwerke.
- b Bearbeiten Sie den Wert, der `.acme.com` hinzugefügt werden soll.
- c Geben Sie `vracli proxy set --proxy-exclude ...` ein, um die aktuellen Konfigurationseinstellungen zu aktualisieren.
- d Führen Sie den Befehl `/opt/scripts/deploy.sh` aus, um die Umgebung erneut bereitzustellen.

- 3 (Optional) Schließen Sie DNS-Domänen, FQDNs und IP-Adressen vom Zugriff durch den Internet-Proxyserver aus.

Ändern Sie immer die Standardwerte der `proxy-exclude`-Variablen mithilfe von parameter `--proxy-exclude`. Um die Domäne `exclude.vmware.com` hinzuzufügen, verwenden Sie zuerst den Befehl `vracli proxy show`, kopieren Sie dann die Variable `proxy-exclude` und fügen Sie den Domänenwert mithilfe des Befehls `vracli proxy set ...` wie folgt hinzu:

```
vracli proxy set --host http://
proxy.vmware.com:3128 --proxy-exclude "exclude.vmware.com,docker-
registry.prelude.svc.cluster.local,localhost,.local,.cluster.local,10.244.,192.,172.16.,sc-
rdops-vm11-dhcp-75-38.eng.vmware.com,10.161.75.38,.eng.vmware.com"
```

Hinweis Fügen Sie `proxy-exclude` Elemente hinzu, anstatt Werte zu ersetzen.

Wenn Sie `proxy-exclude`-Standardwerte löschen, funktioniert vRealize Automation nicht ordnungsgemäß. Sollte dies geschehen, löschen Sie die Proxy-Konfiguration und beginnen Sie von vorn.

- 4 Nachdem Sie den Internet-Proxyserver mit dem Befehl `vracli proxy set ...` festgelegt haben, können Sie mithilfe des Befehls `vracli proxy apply` die Konfiguration des Internet-Proxyservers aktualisieren und die neuesten Proxy-Einstellungen aktivieren.

- 5 Sollten Sie dies noch nicht getan haben, aktivieren Sie die Skriptänderungen, indem Sie den folgenden Befehl ausführen:

```
/opt/scripts/deploy.sh
```

- 6 (Optional) Konfigurieren Sie bei Bedarf den Proxyserver, um den externen Zugriff auf Port 22 zu unterstützen.

Um Integrationen wie Puppet und Ansible zu unterstützen, muss der Proxyserver zulassen, dass Port 22 auf die relevanten Hosts zugreift.

Beispiel: Beispiel für Squid-Konfiguration

In Bezug auf Schritt 1 können Sie, falls Sie einen Squid-Proxy einrichten, Ihre Konfiguration in `/etc/squid/squid.conf` optimieren, indem Sie sie an das folgende Beispiel anpassen:

```
acl localnet src 192.168.11.0/24

acl SSL_ports port 443

acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT

http_access allow !Safe_ports
http_access allow CONNECT !SSL_ports
http_access allow localnet

http_port 0.0.0.0:3128

maximum_object_size 5 GB
cache_dir ufs /var/spool/squid 20000 16 256
coredump_dir /var/spool/squid
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern (Release|Packages(.gz)*)$ 0 20% 2880
refresh_pattern . 0 20% 4320

client_persistent_connections on
server_persistent_connections on
```

Wozu dienen NSX-T-Zuordnungen zu mehreren vCentern in vRealize Automation

Sie können ein NSX-T-Cloud-Konto mit einem oder mehreren vCenter-Cloud-Konten verknüpfen, um verschiedene Bereitstellungsziele zu unterstützen.

Sie können dasselbe vorhandene NSX-T-Netzwerk mit Netzwerkprofilen für verschiedene vCenter verknüpfen und eine Bereitstellung basierend auf Beschränkungen in einem beliebigen vCenter bereitstellen. Im Folgenden werden einige Beispiele aufgelistet:

- Cloud-Vorlagen, die eine einzelne Maschine und mehrere Netzwerkkarten enthalten, die dasselbe Netzwerkprofil verwenden, wobei dieses Netzwerkprofil ein NSX-T-Netzwerk enthält, das sich über mehrere vCenter erstreckt.
- Cloud-Vorlagen, die eine Maschine in einem *privaten* Netzwerk enthalten, das ein Netzwerkprofil mit subnetzbasierter Isolierung und ein NSX-T-Netzwerk (*vorhanden*) verwendet, das sich über mehrere vCenter erstreckt.
- Cloud-Vorlagen, die eine einzelne Maschine in einem *privaten* Netzwerk enthalten, das ein Netzwerkprofil mit sicherheitsgruppenbasierter Isolierung und ein NSX-T-Netzwerk verwendet, das sich über mehrere vCenter erstreckt.
- Cloud-Vorlagen, die eine einzelne Maschine in einem *gerouteten* Netzwerk enthalten, das ein Netzwerkprofil mit einem NSX-T-Netzwerk verwendet, das sich über mehrere vCenter erstreckt.
- Cloud-Vorlagen, die einen bedarfsgesteuerten Lastausgleichsdienst enthalten, der in einem Netzwerkprofil definiert ist, in dem der Lastausgleichsdienst auf alle vCenter-Maschinen im Netzwerk angewendet wird.
- Cloud-Vorlagen, die ein bedarfsgesteuertes Netzwerk enthalten, das in einem Netzwerkprofil definiert ist, in dem das bedarfsgesteuerte Netzwerk von allen vCentern verwendet wird, die das Netzwerkprofil nutzen.
- Cloud-Vorlagen, die eine bedarfsgesteuerte Sicherheitsgruppe mit optionalen Firewallregeln und enthalten, wobei die Sicherheitsgruppe mit allen vCentern im Netzwerk verknüpft ist.

Sie können internes oder externes vRealize Automation-IPAM im NSX-T-Netzwerk konfigurieren und dieselbe IP-Adresse für Maschinen freigeben, die in verschiedenen vCentern bereitgestellt werden.

Wenn kein Netzwerkprofil im System definiert ist, können Sie eine Cloud-Vorlage bereitstellen, die mehrere Maschinen in verschiedenen vCenters enthält, die ein einzelnes *vorhandenes* NSX-T-Netzwerk teilen.

Was passiert, wenn die Verknüpfung eines NSX-Cloud-Kontos in vRealize Automation entfernt wird

Wenn Sie eine Verknüpfung zwischen einem NSX-Cloud-Konto und einem vCenter-Cloud-Konto entfernen, müssen Sie auch die zugehörigen Netzwerkprofile aktualisieren, um die verknüpften NSX-Objekte zu entfernen.

Wenn Sie eine Verknüpfung zwischen einem NSX-Cloud-Konto und einem vCenter-Cloud-Konto entfernen, werden die Infrastrukturelemente nicht automatisch von vRealize Automation aktualisiert. Sie müssen Ihre vorhandenen Netzwerkprofile aktualisieren, um die zugeordneten NSX-Objekte zu entfernen.

Die Benutzeroberfläche enthält Informationen, mit denen die betroffenen Netzwerkprofilelemente wie folgt hervorgehoben werden können:

- Wenn für das Netzwerkprofil ein vorhandenes NSX-Netzwerk ausgewählt ist:
 - Das Objekt wird als *ungültig* markiert und die Meldung *"Bestimmte Netzwerkobjekte fehlen oder sind ungültig"* wird angezeigt.
 - Die Objekt werden entfernt, wenn Sie das Netzwerkprofil speichern.
- Wenn für das Netzwerkprofil Anwendungsisolierung konfiguriert ist, müssen Sie die Einstellungen für die Isolierungsrichtlinie aktualisieren, bevor das Netzwerkprofil gespeichert werden kann.
- Wenn für das Netzwerkprofil Sicherheitsgruppen oder Lastausgleichsdienste ausgewählt sind, werden die Objekte beim Speichern des Netzwerkprofils entfernt.

Vorhandene Bereitstellungen funktionieren weiterhin entwurfsgemäß für vorhandene Komponenten, schlagen jedoch fehl, wenn neue Komponenten erstellt werden, z. B. bei einem horizontalen Skalierungsvorgang.

Wenn Sie die Verknüpfung erneut einrichten, wird das Netzwerkprofil neu befüllt, und vorhandene Bereitstellungen funktionieren wie geplant.

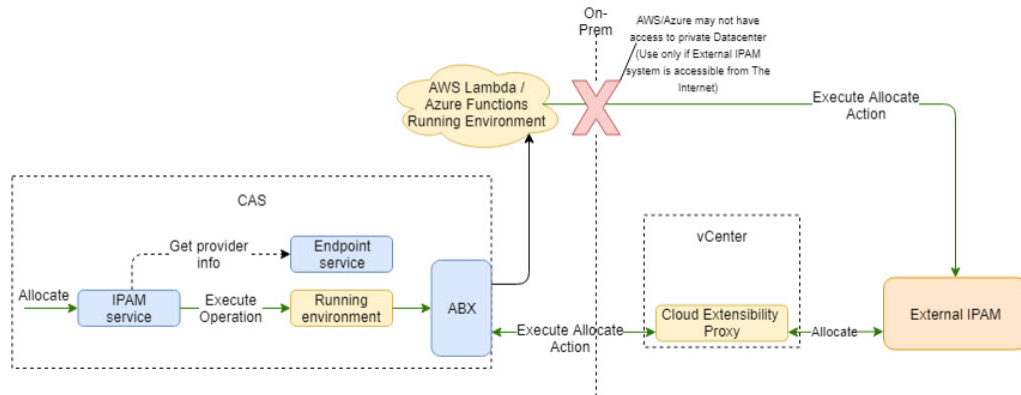
Wenn Sie das NSX-Cloud-Konto entfernen, ist das obige Verhalten identisch. Netzwerkobjekte werden jedoch als *fehlend* und nicht als *ungültig* gekennzeichnet.

Vorgehensweise zum Verwenden des IPAM-SDK zur Erstellung eines anbieterspezifischen, externen IPAM-Integrationspakets für vRealize Automation

Externe IPAM-Anbieter und -Partner können das IPAM-SDK herunterladen und verwenden, um ein IPAM-Integrationspaket zu erstellen, mit dem vRealize Automation die anbieterspezifische IPAM-Lösung unterstützen kann.

Der Vorgang zum Erstellen und Bereitstellen eines benutzerdefinierten IPAM-Pakets für vRealize Automation mithilfe des bereitgestellten IPAM-SDK wird im Dokument [Erstellen und Bereitstellen eines anbieterspezifischen IPAM-Integrationspakets für VMware Cloud Assembly](#) beschrieben. Wie im Dokument beschrieben, können Sie das neueste *VMware vRealize Automation-Drittanbieter-IPAM-SDK* über die [VMware Code](#)-Site herunterladen. Die folgenden IPAM-SDK-Pakete sind verfügbar:

- [VMware vRealize Automation Third-Party IPAM SDK 1.1.0](#)
- [VMware vRealize Automation Third-Party IPAM SDK 1.0.0](#)



Überprüfen Sie vor dem Erstellen eines anbieterspezifischen IPAM-Integrationspakets mithilfe des IPAM-SDK, ob bereits ein Paket für vRealize Automation vorhanden ist. Sie können auf der Website des IPAM-Anbieters im [VMware Marketplace](#) und auf der vRealize Automation-Registerkarte **Marketplace** nach einem anbieterspezifischen IPAM-Integrationspaket suchen.

Im anbieterspezifischen Beispiel [Lernprogramm: Konfigurieren einer anbieterspezifischen externen IPAM-Integration für vRealize Automation](#) sind hilfreiche Referenzinformationen enthalten.

Erstellen der vRealize Automation Cloud Assembly-Ressourceninfrastruktur

4

In der vRealize Automation Cloud Assembly-Ressourceninfrastruktur definieren Sie Cloud-Kontoregionen als Zonen, in denen Cloud-Vorlagen und deren Arbeitslasten bereitgestellt werden können.

Darüber hinaus beinhaltet die Ressourceninfrastruktur die Erstellung allgemeiner Zuordnungen von Images und Maschinengrößen sowie von Profilen, die Netzwerk- und Speicherfunktionen über Cloud-Kontoregionen oder Datacenter hinweg definieren.

Dieses Kapitel enthält die folgenden Themen:

- Vorgehensweise zum Hinzufügen von Cloud-Zonen, die Regionen oder Datacenter für die Platzierung des vRealize Automation Cloud Assembly-Ziels definieren
- Vorgehensweise zum Hinzufügen von Konfigurationszuordnungen in vRealize Automation, um gemeinsame Maschinengrößen anzugeben
- Vorgehensweise zum Hinzufügen von Image-Zuordnungen in vRealize Automation für den Zugriff auf gängige Betriebssysteme
- Vorgehensweise zum Hinzufügen von Netzwerkprofilen in vRealize Automation
- Vorgehensweise zum Hinzufügen von vRealize Automation Cloud Assembly-Speicherprofilen, die verschiedenen Anforderungen entsprechen
- Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen
- Vorgehensweise zum Arbeiten mit Ressourcen in vRealize Automation
- Konfigurieren von Mehrmandantenressourcen mit vRealize Automation

Vorgehensweise zum Hinzufügen von Cloud-Zonen, die Regionen oder Datacenter für die Platzierung des vRealize Automation Cloud Assembly-Ziels definieren

Eine vRealize Automation Cloud Assembly-Cloud-Zone ist eine Gruppe von Ressourcen innerhalb eines Cloud-Kontotyps, wie z. B. AWS oder vSphere.

Arbeitslasten werden von Cloud-Vorlagen in Cloud-Zonen in einer bestimmten Kontoregion bereitgestellt. Jede Cloud-Zone ist mit einem vRealize Automation Cloud Assembly-Projekt verknüpft.

Wählen Sie **Infrastruktur > Konfigurieren > Cloud-Zonen** aus und klicken Sie auf **Neue Zone hinzufügen**.

Weitere Informationen zu vRealize Automation Cloud Assembly-Cloud-Zonen

Bei vRealize Automation Cloud Assembly-Cloud-Zonen handelt es sich um Bereiche von Computing-Ressourcen, die für Ihren Cloud-Kontotyp spezifisch sind, wie z. B. AWS oder vSphere.

Cloud-Zonen sind spezifisch für eine Region und müssen einem Projekt zugewiesen werden. Zwischen Cloud-Zonen und Projekten besteht eine n:n-Beziehung. vRealize Automation Cloud Assembly unterstützt die Bereitstellung auf den beliebtesten Public Clouds, einschließlich Azure, AWS und GCP, sowie vSphere. Weitere Informationen hierzu finden Sie unter [Hinzufügen von Cloud-Konten zu vRealize Automation Cloud Assembly](#).

Zu den zusätzlichen Platzierungssteuerelementen gehören Optionen für Platzierungsrichtlinien, Funktions- und Computing-Tags.

■ Platzierungsrichtlinie

Die Platzierungsrichtlinie steuert die Hostauswahl für Bereitstellungen innerhalb der angegebenen Cloud-Zone.

- **default** – Verteilt Computing-Ressourcen nach dem Zufallsprinzip auf Cluster und Hosts. Diese Option wird auf der Ebene einer einzelnen Maschine verwendet. Beispiel: Alle Maschinen in einer bestimmten Bereitstellung werden nach dem Zufallsprinzip auf die verfügbaren Cluster und Hosts verteilt, die die Anforderungen erfüllen.
- **binpack** – Computing-Ressourcen werden auf dem am stärksten ausgelasteten Host platziert, der über genügend Ressourcen zum Ausführen der betreffenden Berechnung verfügt.
- **spread** – Stellt dem Cluster oder Host mit der geringsten Zahl an virtuellen Maschinen Computing-Ressourcen auf Bereitstellungsebene zur Verfügung. Für vSphere verteilt Distributed Resource Scheduler (DRS) die virtuellen Maschinen auf die Hosts. Beispiel: Alle angeforderten Maschinen in einer Bereitstellung werden auf demselben Cluster platziert, bei der nächsten Bereitstellung wird jedoch je nach aktueller Last gegebenenfalls ein anderer vSphere-Cluster ausgewählt.

Beispiel: Angenommen, Sie verfügen über die folgende Konfiguration:

- DRS-Cluster 1 mit 5 virtuellen Maschinen
- DRS-Cluster 2 mit 9 virtuellen Maschinen
- DRS-Cluster 3 mit 6 virtuellen Maschinen

Wenn Sie einen Cluster mit 3 virtuellen Maschinen anfordern und eine Spread-Richtlinie auswählen, sollten sie alle auf Cluster 1 platziert werden. Die aktualisierte Last für Cluster 1 wird in 8 virtuelle Maschinen geändert, während die Lasten für die Cluster 2 und 3 unverändert bei 9 und 6 bleiben.

Wenn Sie dann weitere 2 virtuelle Maschinen anfordern, werden diese auf dem DRS-Cluster 3 platziert, der dann 8 virtuelle Maschinen enthält. Die Lasten für die Cluster 1 und 3 bleiben unverändert bei 8 und 9.

Wenn zwei Cloud-Zonen alle für die Bereitstellung erforderlichen Kriterien erfüllen, wählt die Platzierungslogik diejenige mit höherer Priorität aus.

■ Funktions-Tags

Blueprints enthalten Einschränkungs-Tags, die bei der Bestimmung der Bereitstellungsplatzierung hilfreich sind. Während der Bereitstellung werden Einschränkungs-Tags des Blueprints passenden Funktions-Tags in Cloud-Zonen zugewiesen und somit die Cloud-Zonen festgelegt, die für die Platzierung der Computing-Ressourcen verfügbar sind.

■ Berechnungen

Sie können die Computing-Ressourcen anzeigen und verwalten, die für die Bereitstellung von Arbeitslasten für diese Cloud-Zone verfügbar sind, wie z. B. AWS-Verfügbarkeitszonen und vCenter-Cluster.

Wenn ein vCenter-Computing-Cluster DRS-fähig ist, wird in der Cloud-Zone nur der Cluster in der Liste der Berechnungen angezeigt und die untergeordneten Hosts werden nicht angezeigt. Wenn ein vCenter-Computing-Cluster nicht DRS-fähig ist, zeigt die Cloud-Zone nur eigenständige ESXi-Hosts an, sofern vorhanden.

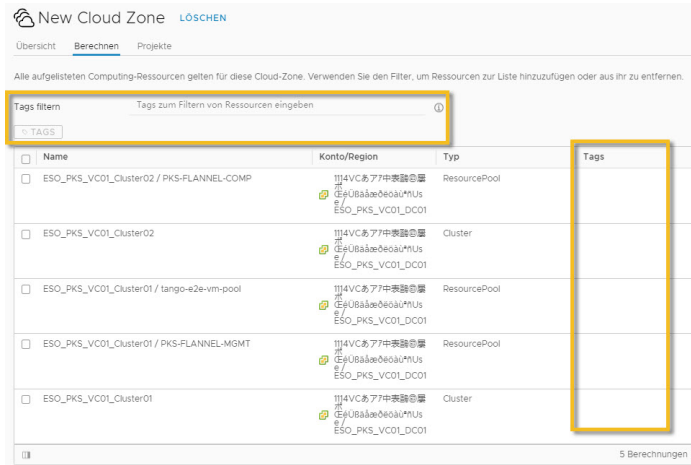
Fügen Sie den Anforderungen der Cloud-Zone entsprechend Computing-Ressourcen hinzu. Zu Beginn lautet die Filterauswahl „Alle Berechnungen einschließen“ und die Liste darunter zeigt alle verfügbaren Computing-Ressourcen an. Und diese sind alle der entsprechenden Zone zugeordnet. Sie verfügen über zwei zusätzliche Optionen zum Hinzufügen von Computing-Ressourcen zu einer Cloud-Zone.

- Berechnung manuell auswählen: Wählen Sie diese Option aus, wenn Sie Computing-Ressourcen manuell aus der Liste darunter auswählen möchten. Nachdem Sie sie ausgewählt haben, klicken Sie auf „Berechnung hinzufügen“, um die Ressourcen der Zone hinzuzufügen.
- Berechnung nach Tags dynamisch einbeziehen: Wählen Sie diese Option aus, wenn Sie eine Computing-Ressource, die der Zone hinzugefügt werden soll, basierend auf Tags auswählen möchten. Alle Computing-Ressourcen werden so lange angezeigt, bis Sie die entsprechenden Tags hinzufügen. Sie können unter der Option „Berechnung mit diesen Tags einbeziehen“ einen oder mehrere Tags auswählen.

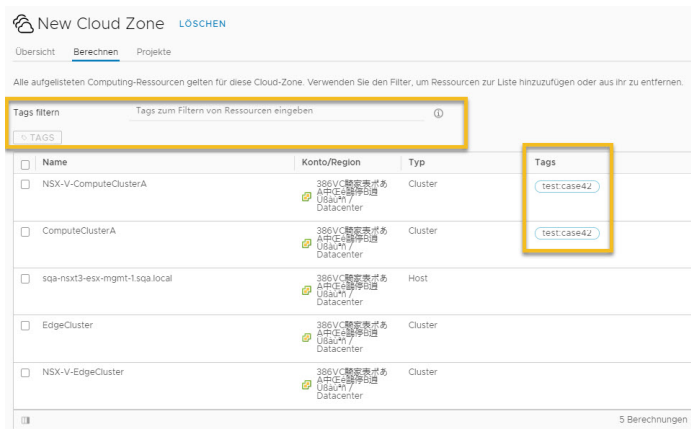
Bei beiden Computing-Optionen können Sie eine oder mehrere der auf der Seite angezeigten Computing-Ressourcen entfernen, indem Sie das Kontrollkästchen rechts aktivieren und auf „Entfernen“ klicken.

Computing-Tags helfen bei der weiteren Steuerung der Platzierung. Mithilfe von Tags können Sie verfügbare Computing-Ressourcen so filtern, dass sie nur einem oder mehreren Tags entsprechen (siehe hierzu folgende Beispiele).

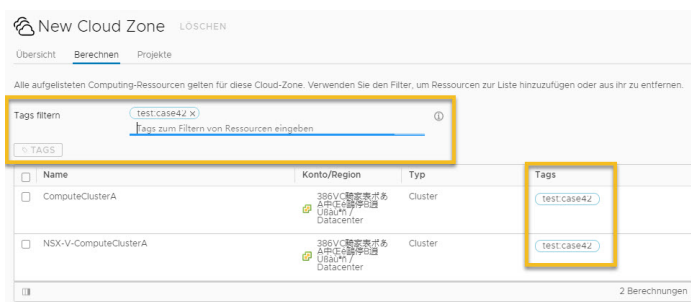
- Berechnungen enthalten keine Tags und es werden keine Filter verwendet.



- Zwei Berechnungen enthalten dasselbe Tag. Filter werden nicht verwendet.



- Zwei Berechnungen enthalten dasselbe Tag und der Tag-Filter entspricht dem Tag, das in den beiden Berechnungen verwendet wird.



- Projekte

Sie können die Projekte anzeigen, die zur Unterstützung der Arbeitslastbereitstellung in dieser Cloud-Zone konfiguriert wurden.

Nach der Erstellung einer Cloud-Zone können Sie deren Konfiguration validieren.

Vorgehensweise zum Hinzufügen von Konfigurationszuordnungen in vRealize Automation, um gemeinsame Maschinengrößen anzugeben

Sie verwenden natürliche Sprache in einer vRealize Automation-Konfigurationszuordnung, um Zielbereitstellungsgrößen für ein bestimmtes Konto/eine bestimmte Region festzulegen.

Mit Konfigurationszuordnungen werden die Bereitstellungsgrößen angegeben, die für Ihre Umgebung sinnvoll sind. Beispiel: *Klein* für 1 CPU und 2 GB Arbeitsspeicher und *Groß* für 2 CPUs und 8 GB für ein vCenter-Konto in einem benannten Datacenter und t2.nano für ein Amazon Web Services-Konto in einer benannten Region.

Wählen Sie **Infrastruktur > Konfigurieren > Konfigurationszuordnungen** aus und klicken Sie auf **Neue Konfigurationszuordnung**.

Weitere Informationen zu Konfigurationszuordnungen in vRealize Automation

In einer Konfigurationszuordnung werden mehrere Zielbereitstellungsgrößen für ein bestimmtes Cloud-Konto und/oder eine bestimmte Region in vRealize Automation mithilfe natürlicher Sprachbezeichnungen zusammengefasst.

Mit der Konfigurationszuordnung können Sie eine benannte Zuordnung erstellen, die ähnliche Konfigurationsgrößen für Ihre Kontoregionen enthält. Eine Konfigurationszuordnung mit der Bezeichnung `standard_small` kann beispielsweise eine ähnliche Konfigurationsgröße (z. B. 1 CPU, 2 GB RAM) für bestimmte oder alle verfügbaren Konten/Regionen in Ihrem Projekt aufweisen. Wählen Sie beim Erstellen einer Cloud-Vorlage eine verfügbare Konfiguration aus, die Ihren Anforderungen entspricht.

Verwalten Sie Konfigurationszuordnungen für Ihr Projekt nach Bereitstellungsabsicht.

Zum Vereinfachen der Cloud-Vorlagenerstellung können Sie eine Option zur Vorabkonfiguration auswählen, wenn Sie ein neues Cloud-Konto hinzufügen. Wenn Sie die Option zur Vorabkonfiguration auswählen, werden die beliebteste Konfigurations- und Image-Zuordnung in Ihrer Organisation für die angegebene Region verwendet.

In Bezug auf die Image-Zuordnung in Cloud-Vorlagen, die vSphere-Ressourcen enthalten, können Sie, sofern keine Konfigurationszuordnungen für eine vSphere-Cloud-Zone festgelegt sind, unbegrenzten Arbeitsspeicher und CPU konfigurieren, indem Sie die vSphere-spezifischen Einstellungen in der Cloud-Vorlage verwenden. Wenn für eine vSphere-Cloud-Zone Konfigurationszuordnungen definiert sind, dient die Konfigurationszuordnung als Grenzwert für vSphere-spezifische Konfigurationen in der Cloud-Vorlage.

Vorgehensweise zum Hinzufügen von Image-Zuordnungen in vRealize Automation für den Zugriff auf gängige Betriebssysteme

Sie verwenden natürliche Sprache in einer vRealize Automation-Image-Zuordnung, um Betriebssysteme als Zielbereitstellung für ein bestimmtes Konto/eine bestimmte Region festzulegen.

Wählen Sie **Infrastruktur > Konfigurieren > Image-Zuordnungen** aus und klicken Sie auf **Neue Image-Zuordnung**.

Weitere Informationen zu Image-Zuordnungen in vRealize Automation

In einer Image-Zuordnung werden mehrere vordefinierte Zielbetriebssystemspezifikationen für ein bestimmtes Cloud-Konto und/oder eine bestimmte Cloud-Region in vRealize Automation mithilfe natürlicher Sprachbezeichnungen zusammengefasst.

Cloud-Anbieterkonten, wie z. B. Microsoft Azure und Amazon Web Services, verwenden Images, um mehrere Zielbereitstellungsbedingungen zusammenzufassen, einschließlich Betriebssystem und zugehöriger Konfigurationseinstellungen. vCenter- und NSX-basierte Umgebungen, einschließlich VMware Cloud on AWS, verwenden einen ähnlichen Gruppierungsmechanismus, um mehrere Bereitstellungsbedingungen für Betriebssysteme zu definieren. Wenn Sie eine Cloud-Vorlage erstellen und schließlich bereitstellen und durchlaufen, wählen Sie ein verfügbares Image aus, das Ihren Anforderungen entspricht.

Verwalten Sie Image-Zuordnungen für ein Projekt anhand ähnlicher Betriebssystemeinstellungen, der Kennzeichnungsstrategie und des Zwecks der funktionalen Bereitstellung.

Zum Vereinfachen der Cloud-Vorlagenerstellung können Sie eine Option zur Vorabkonfiguration auswählen, wenn Sie ein neues Cloud-Konto hinzufügen. Wenn Sie die Option zur Vorabkonfiguration auswählen, werden die beliebteste Konfigurations- und Image-Zuordnung in Ihrer Organisation für die angegebene Region verwendet.

Wenn Sie Image-Informationen zu einer Cloud-Vorlage hinzufügen, verwenden Sie entweder den Eintrag `image` oder `imageRef` im Abschnitt `properties` der Maschinenkomponente. Wenn Sie beispielsweise einen Klon anhand eines Snapshots erstellen möchten, verwenden Sie die Eigenschaft `imageRef`.

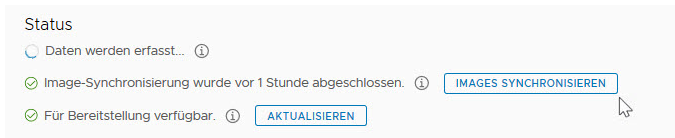
Beispiele für `image`- und `imageRef`-Einträge im Cloud-Vorlagencode finden Sie unter [Kapitel 6 Entwerfen Ihrer vRealize Automation Cloud Assembly-Bereitstellungen](#).

Um eine Berechtigung für eine Inhaltsbibliothek zuzuweisen, muss ein Administrator dem Benutzer die Berechtigung als globale Berechtigung erteilen. Weitere Informationen finden Sie im Abschnitt [Hierarchische Vererbung von Berechtigungen für Inhaltsbibliotheken](#) unter *Verwaltung virtueller vSphere-Maschinen* in der [VMware vSphere-Dokumentation](#).

Synchronisieren von Images für das Cloud-Konto/die Cloud-Region

Sie können die Image-Synchronisierung ausführen, um sicherzustellen, dass die Images, die Sie für ein bestimmtes Cloud-Konto/eine bestimmte Cloud-Region auf der Seite **Infrastruktur > Konfigurieren > Image-Zuordnung**, aktuell sind.

- 1 Öffnen Sie das/die zugeordnete **Cloud-Konto/Cloud-Region**, indem Sie **Infrastruktur > Verbindungen > Cloud-Konten** auswählen. Wählen Sie das vorhandene Cloud-Konto/die vorhandene Cloud-Region aus.
- 2 Klicken Sie auf die Schaltfläche **Images synchronisieren** und warten Sie, bis die Aktion abgeschlossen ist.



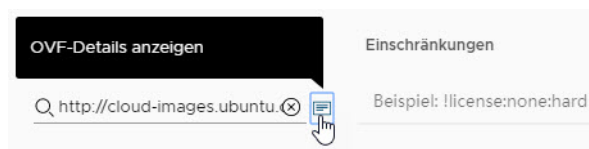
- 3 Wenn die Aktion abgeschlossen ist, klicken Sie auf **Infrastruktur > Konfigurieren > Image-Zuordnung**. Definieren Sie eine neue Image-Zuordnung oder bearbeiten Sie eine vorhandene und wählen Sie das Cloud-Konto/die Cloud-Region aus Schritt 1 aus.
- 4 Klicken Sie auf der Seite **Image-Zuordnung** auf das Symbol für die Image-Synchronisierung.



- 5 Konfigurieren Sie die Image-Zuordnungseinstellungen für das angegebene Cloud-Konto/die angegebene Cloud-Region auf der Seite **Image-Zuordnung**.

Anzeigen von OVF-Details

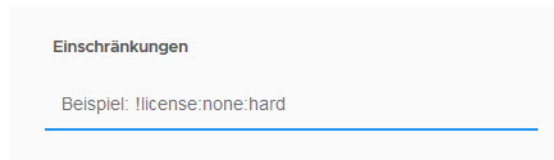
Sie können OVF-Spezifikationen in vRealize Automation Cloud Assembly-Cloud-Vorlagenobjekten, z. B. vCenter-Maschinenkomponenten und -Image-Zuordnungen, einschließen. Wenn Ihr Image eine OVF-Datei enthält, können Sie deren Inhalt ermitteln, ohne die Datei öffnen zu müssen. Bewegen Sie den Mauszeiger über die OVF, um OVF-Details anzuzeigen, einschließlich des Namens und des Speicherorts. Weitere Informationen zum OVF-Dateiformat finden Sie unter [vCenter-OVF: Eigenschaft](#).



Verwenden von Einschränkungen und Tags zur Optimierung der Image-Auswahl

Zur weiteren Optimierung der Image-Auswahl in einer Cloud-Vorlage können Sie eine oder mehrere Einschränkungen hinzufügen, um Tag-basierte Beschränkungen für den Typ des bereitzustellenden Images festzulegen. Das angegebene Beispiel für **Einschränkung**, das beim Erstellen oder Bearbeiten einer Image-Zuordnungsconfiguration angezeigt wird, ist !

`license:none:hard`. Im Beispiel wird eine Tag-basierte Einschränkung gezeigt, bei der das Image nur verwendet werden kann, wenn das `license:none`-Tag *nicht* in der Cloud-Vorlage vorhanden ist. Wenn Sie Tags wie `license:88` und `license:92` hinzufügen, kann das angegebene Image nur verwendet werden, wenn die Tags `license:88` und `license:92` *in der* Cloud-Vorlage vorhanden sind.



Verwenden eines Cloud-Konfigurationsskripts zur Steuerung der Bereitstellung

Sie können ein Cloud-Konfigurationsskript in einer Image-Zuordnung und/oder einer Cloud-Vorlage verwenden, um benutzerdefinierte Betriebssystemmerkmale zu definieren, die in einer vRealize Automation Cloud Assembly-Bereitstellung verwendet werden sollen. Je nachdem, ob Sie eine Cloud-Vorlage für eine Public Cloud oder Private Cloud bereitstellen, können Sie beispielsweise bestimmte Benutzerberechtigungen, Betriebssystemberechtigungen oder andere Bedingungen auf das Image anwenden. Ein Cloud-Konfigurationsskript verwendet ein `cloud-init`-Format für Linux-basierte Images oder ein `cloudbase-init`-Format für Windows-basierte Images. vRealize Automation Cloud Assembly unterstützt das Tool `cloud-init` für Linux-Systeme und das Tool `cloudbase-init` für Windows.

Auf Windows-Maschinen können Sie ein beliebiges Format für das Cloud-Konfigurationsskript verwenden, das von `cloudbase-init` unterstützt wird.

Die Maschinenressource im folgenden Beispiel-Cloud-Vorlagencode verwendet ein Image mit einem Cloud-Konfigurationsskript, dessen Inhalt im Eintrag `image` angezeigt wird.

```
resources:
  demo-machine:
    type: Cloud.vSphere.Machine
    properties:
      flavor: small
      image: MyUbuntu16
      https://cloud-images.ubuntu.com/releases/16.04/release-20170307/ami-ubuntu-16.04-1.10.3-00-15269239.ova
      cloudConfig: |
        ssh_pwauth: yes
        chpasswd:
          list: |
            ${input.username}:${input.password}
          expire: false
        users:
          - default
          - name: ${input.username}
            lock_passwd: false
            sudo: ['ALL=(ALL) NOPASSWD:ALL']
```



```
groups: [wheel, sudo, admin]
shell: '/bin/bash'
runcmd:
  - echo "Defaults:${input.username} !requiretty" >> /etc/sudoers.d/${input.username}
```

Zu erwartende Auswirkungen, wenn Image-Zuordnung und Cloud-Vorlage ein Cloud-Konfigurationsskript enthalten

Wenn eine Cloud-Vorlage mit einem Cloud-Konfigurationsskript eine Image-Zuordnung mit einem Cloud-Konfigurationsskript verwendet, werden beide Skripts kombiniert. Bei der Zusammenführungsaktion werden zuerst die Inhalte des Image-Zuordnungsskripts und anschließend die Inhalte des Cloud-Vorlagenskripts verarbeitet. Dabei wird berücksichtigt, ob die Skripts im `#cloud-config`-Format vorliegen oder nicht.

- Bei Skripts im `#cloud-config`-Format werden bei der Zusammenführung die Inhalte jedes Moduls (zum Beispiel `runcmd`, `users` und `write_files`) wie folgt kombiniert:
 - Bei Modulen, deren Inhalt eine Liste ist, werden die Listen der Befehle aus der Image-Zuordnung und aus der Cloud-Vorlage zusammengeführt, wobei Befehle, die in beiden Listen identisch sind, ausgeschlossen werden.
 - Bei Modulen, deren Inhalt ein Wörterbuch ist, werden die Befehle zusammengeführt, und das Ergebnis ist eine Kombination aus beiden Wörterbüchern. Wenn in beiden Wörterbüchern der gleiche Schlüssel vorhanden ist, bleibt der Schlüssel aus dem Wörterbuch für das Image-Zuordnungsskript erhalten, und der Schlüssel aus dem Wörterbuch des Cloud-Vorlagenskripts wird ignoriert.
 - Bei Modulen, deren Inhalt eine Zeichenfolge ist, werden die Inhaltswerte aus dem Image-Zuordnungsskript beibehalten, und die Inhaltswerte aus dem Cloud-Vorlagenskript werden ignoriert.
- Bei Skripts, die in einem anderen Format als `#cloud-config` vorliegen, oder wenn ein Skript das `#cloud-config`-Format aufweist und das andere nicht, werden beide Skripts so kombiniert, dass das Image-Zuordnungsskript zuerst ausgeführt wird und das Cloud-Vorlagenskript ausgeführt wird, nachdem das Image-Zuordnungsskript beendet wurde.

Weitere Informationen hierzu finden Sie unter [Zusammenführen von Abschnitten mit Benutzerdaten](#).

Weitere Informationen zum Konfigurieren und Verwenden von Cloud-Konfigurationsskripts

Weitere Informationen zum Arbeiten mit Cloud-Konfigurationsskripts finden Sie unter [Vorgehensweise zum automatischen Initialisieren einer Maschine in einer vRealize Automation Cloud Assembly-Vorlage](#).

Weitere Informationen finden Sie auch in den VMware-Blogger-Artikeln [vSphere Customization with Cloud-init While Using vRealize Automation 8 or Cloud](#) und [Customizing Cloud Assembly Deployments with Cloud-Init](#).

Vorgehensweise zum Hinzufügen von Netzwerkprofilen in vRealize Automation

Ein vRealize Automation-Netzwerkprofil beschreibt das Verhalten des bereitzustellenden Netzwerks.

Ein Netzwerk muss z. B. mit dem Internet verbunden sein, anstatt nur intern verwendet zu werden.

Netzwerke und Netzwerkprofile sind Cloud-spezifisch.

Wählen Sie **Infrastruktur > Konfigurieren > Netzwerkprofile** aus und klicken Sie auf **Neues Netzwerkprofil**.

Weitere Informationen zu Netzwerkprofilen in vRealize Automation

Ein Netzwerkprofil definiert eine Gruppe von Netzwerken und Netzwerkeinstellungen, die für ein Cloud-Konto in einer bestimmten Region oder einem bestimmten Datencenter in vRealize Automation verfügbar sind.

In der Regel definieren Sie Netzwerkprofile zur Unterstützung einer Zielbereitstellungsumgebung, zum Beispiel eine kleine Testumgebung, in der ein vorhandenes Netzwerk nur über ausgehenden Zugriff oder über eine hohe Produktionsumgebung mit Lastausgleich verfügt, die eine Reihe von Sicherheitsrichtlinien benötigt. Stellen Sie sich ein Netzwerkprofil als eine Sammlung von Arbeitslast-spezifischen Netzwerkmerkmalen vor.

Funktionen in einem Netzwerkprofil

Ein Netzwerkprofil enthält spezifische Informationen für einen benannten Cloud-Kontotyp und eine Region in vRealize Automation, einschließlich der folgenden Einstellungen:

- Benanntes Cloud-Konto/benannte Region und optionale Funktions-Tags für das Netzwerkprofil.
- Benannte vorhandene Netzwerke und zugehörige Einstellungen.
- Netzwerkrichtlinien, die bedarfsgesteuerte und andere Aspekte des Netzwerkprofils definieren.
- Optionale Einbeziehung vorhandener Lastausgleichsdienste.
- Optionale Einbeziehung vorhandener Sicherheitsgruppen.

Sie bestimmen die Verwaltungsfunktionen für die Netzwerk-IP basierend auf dem Netzwerkprofil.

Funktions-Tags des Netzwerkprofils werden mit Einschränkungs-Tags in Cloud-Vorlagen abgeglichen, um die Netzwerkauswahl zu steuern. Darüber hinaus werden alle Tags, die den vom Netzwerkprofil erfassten Netzwerken zugewiesen sind, ebenfalls mit Tags in der Cloud-Vorlage abgeglichen, um die Netzwerkauswahl bei der Bereitstellung der Cloud-Vorlage zu steuern.

Funktions-Tags sind optional. Funktions-Tags werden auf alle Netzwerke im Netzwerkprofil angewendet, allerdings nur dann, wenn die Netzwerke als Teil dieses Netzwerkprofils verwendet werden. Für Netzwerkprofile, die keine Funktions-Tags enthalten, findet der Tag-Abgleich nur auf den Netzwerk-Tags statt. Die Netzwerk- und Sicherheitseinstellungen, die im abgeglichenen Netzwerkprofil definiert sind, werden bei der Bereitstellung der Cloud-Vorlage angewendet.

Bei der Verwendung einer statischen IP wird der Adressbereich von vRealize Automation verwaltet. Für DHCP werden die IP-Start- und -Endadressen vom unabhängigen DHCP-Server verwaltet, und nicht von vRealize Automation. Bei Verwendung von DHCP oder einer gemischten Netzwerkadresszuteilung wird der Wert für die Netzwerknutzung auf null gesetzt. Ein bedarfsgesteuerter Netzwerkbereich basiert auf der im Netzwerkprofil angegebenen CIDR- und Subnetzgröße. Um sowohl statische als auch dynamische Zuweisungen in der Bereitstellung zu unterstützen, wird der zugeteilte Bereich in zwei Bereiche aufgeteilt: einen für die statische Zuteilung und einen weiteren für die dynamische Zuteilung.

Netzwerke

Netzwerke, die auch als Subnetze bezeichnet werden, sind logische Unterteilungen eines IP-Netzwerks. Ein Netzwerk gruppiert ein Cloud-Konto, eine IP-Adresse oder einen Bereich sowie Netzwerk-Tags, um zu steuern, wie und wo eine Cloud-Vorlagenbereitstellung stattfinden soll. Netzwerkparameter im Profil definieren, wie Maschinen in der Bereitstellung über IP-Ebene 3 miteinander kommunizieren können. Netzwerke können Tags aufweisen.

Sie können Netzwerke zum Netzwerkprofil hinzufügen, vom Netzwerkprofil verwendete Netzwerkaspekte bearbeiten und Netzwerke aus dem Netzwerkprofil entfernen.

Hinweis Für einen VCF-Cloud-Kontotyp (VMware Cloud Foundation) können Sie dem Netzwerkprofil ausschließlich NSX-Netzwerke, aber keine vSphere-Netzwerke hinzufügen. Die NSX-Netzwerksegmente werden lokal im NSX-T-Netzwerk und nicht als globale Netzwerke erstellt.

■ Netzwerkdomäne oder Transportzone

Die Netzwerkdomäne oder Transportzone ist der Distributed Virtual Switch (dvSwitch) für die vSphere vNetwork Distributed PortGroups (dvPortGroup). Eine *Transportzone* ist ein vorhandenes NSX-Konzept, das mit den Begriffen *dvSwitch* oder *dvPortGroup* vergleichbar ist.

Wenn Sie ein Cloud-Konto von NSX verwenden, lautet der Elementname auf der Seite **Transportzone**, andernfalls **Netzwerkdomäne**.

Bei Standard-Switches entspricht die Netzwerkdomäne oder Transportzone dem Switch. Die Netzwerkdomäne oder Transportzone definiert die Begrenzungen der Subnetze innerhalb von vCenter.

Eine Transportzone steuert, welche Hosts ein logischer NSX-Switch erreichen kann. Sie kann sich auf einen oder mehrere vSphere-Cluster erstrecken. Transportzonen steuern, welche Cluster und welche virtuellen Maschinen an der Verwendung eines bestimmten Netzwerks teilnehmen können. Subnetze, die zur selben NSX-Transportzone gehören, können für dieselben Maschinenhosts verwendet werden.

■ **Domäne**

Stellt die vCenter Single Sign-On-Domäne für eine virtuelle Zielmaschine dar. Domänen werden von einem vCenter-Administrator während der vSphere-Konfiguration konfiguriert. Die Domäne bestimmt den Bereich für die lokale Authentifizierung in vCenter.

■ **IPv4-CIDR- und IPv4-Standard-Gateway**

vSphere-Cloud-Konten und vSphere-Maschinenkomponenten in der Cloud-Vorlage unterstützen Methoden für duales IPv6 und IPv4. Beispiel: 192.168.100.14/24 stellt die IPv4-Adresse 192.168.100.14 und das zugehörige Routing-Präfix 192.168.100.0 oder entsprechend die zugehörige Subnetzmaske 255.255.255.0 dar, die 24 führende 1-Bit aufweist. Der IPv4-Block 192.168.100.0/22 stellt die 1024 IP-Adressen von 192.168.100.0 bis 192.168.103.255 dar.

■ **IPv6-CIDR- und IPv6-Standard-Gateway**

vSphere-Cloud-Konten und vSphere-Maschinenkomponenten in der Cloud-Vorlage unterstützen Methoden für duales IPv6 und IPv4. Beispiel: Bei 2001:db8::/48 handelt es sich um den IPv6-Adressblock von 2001:db8:0:0:0:0:0:0 bis 2001:db8:0:ffff:ffff:ffff:ffff:ffff.

Das IPv6-Format wird für bedarfsgesteuerte Netzwerke nicht unterstützt.

■ **DNS-Server und DNS-Suchdomänen**

■ **Öffentliche IP unterstützen**

Wählen Sie diese Option aus, um das Netzwerk als öffentlich zu kennzeichnen.

Netzwerkkomponenten in einer Cloud-Vorlage, die eine Eigenschaft vom Typ `network type: public` aufweisen, werden mit Netzwerken abgeglichen, die als öffentlich gekennzeichnet sind. Weitere Abgleiche erfolgen während der Cloud-Vorlagenbereitstellung zur Ermittlung der Netzwerkauswahl.

■ **Standardwert für Zone**

Wählen Sie diese Option aus, um das Netzwerk als Standardeinstellung für die Cloud-Zone zu kennzeichnen. Während der Bereitstellung einer Cloud-Vorlage werden Standardnetzwerke gegenüber anderen Netzwerken bevorzugt.

■ **Herkunft**

Gibt die Netzwerkquelle an.

■ **Tags**

Gibt ein oder mehrere Tags an, die dem Netzwerk zugewiesen sind. Tags sind optional. Mit dem Tag-Abgleich werden die Netzwerke bestimmt, die für Cloud-Vorlagenbereitstellungen verfügbar sind.

Netzwerk-Tags sind unabhängig vom Netzwerkprofil auf dem Netzwerkelement selbst vorhanden. Netzwerk-Tags gelten für jedes Vorkommen des Netzwerks, dem sie hinzugefügt wurden, und für alle Netzwerkprofile, die dieses Netzwerk enthalten. Netzwerke können in beliebig viele Netzwerkprofile eingeteilt werden. Unabhängig davon, wo sich das Netzwerkprofil befindet, ist ein Netzwerk-Tag mit diesem Netzwerk verknüpft, wenn das Netzwerk verwendet wird.

Wenn Sie eine Cloud-Vorlage bereitstellen, werden Einschränkungs-Tags in den Netzwerkkomponenten einer Cloud-Vorlage mit Netzwerk-Tags abgeglichen, einschließlich Funktions-Tags für Netzwerkprofile. Bei Netzwerkprofilen, die Funktions-Tags enthalten, werden die Funktions-Tags auf alle Netzwerke angewendet, die für dieses Netzwerkprofil verfügbar sind. Die Netzwerk- und Sicherheitseinstellungen, die im abgeglichenen Netzwerkprofil definiert sind, werden bei der Bereitstellung der Cloud-Vorlage angewendet.

Netzwerkrichtlinien

Über Netzwerkprofile können Sie Subnetze für vorhandene Netzwerkkomponenten definieren, die Einstellungen für statische IP-Adressen, DHCP oder eine Mischung aus statischen und DHCP-IP-Adresseinstellungen enthalten. Auf der Registerkarte **Netzwerkrichtlinien** können Sie Subnetze definieren und IP-Adresseinstellungen angeben.

Bei Einsatz von NSX-V, NSX-T oder VMware Cloud on AWS werden Netzwerkrichtlinieneinstellungen verwendet, wenn eine Cloud-Vorlage `networkType: outbound` oder `networkType: private` oder wenn ein NSX-Netzwerk `networkType: routed` benötigt.

Je nach zugehörigem Cloud-Konto können Sie Netzwerkrichtlinien verwenden, um Einstellungen für die Netzwerktypen `outbound`, `private` und `routed` sowie für bedarfsgesteuerte Sicherheitsgruppen zu definieren. Sie können auch Netzwerkrichtlinien zum Steuern von `existing`-Netzwerken verwenden, wenn ein Lastausgleichsdienst mit diesem Netzwerk verknüpft ist.

Ausgehende Netzwerke ermöglichen unidirektionalen Zugriff auf Upstream-Netzwerke. Private Netzwerke lassen keinen externen Zugriff zu. Geroutete Netzwerke ermöglichen horizontalen Datenverkehr zwischen den gerouteten Netzwerken. Die vorhandenen und öffentlichen Netzwerke im Profil werden als zugrunde liegende oder Upstream-Netzwerke verwendet.

Optionen für die folgenden bedarfsgesteuerten Auswahlen werden in der Hilfe zu **Netzwerkprofilen** beschrieben und nachfolgend zusammengefasst.

- **Kein bedarfsgesteuertes Netzwerk oder keine bedarfsgesteuerte Sicherheitsgruppe erstellen**

Sie können diese Option verwenden, wenn Sie den Netzwerktyp `existing` oder `public` angeben. Cloud-Vorlagen, die ein `outbound`, `private` oder `routed` Netzwerk benötigen, sind diesem Profil nicht zugeordnet.

- **Bedarfsgesteuertes Netzwerk erstellen**

Sie können diese Option verwenden, wenn Sie den Netzwerktyp `outbound`, `private` oder `routed` angeben.

Amazon Web Services, Microsoft Azure, NSX, vSphere und VMware Cloud on AWS unterstützen diese Option.

■ **Bedarfsgesteuerte Sicherheitsgruppe erstellen**

Sie können diese Option verwenden, wenn Sie den Netzwerktyp `outbound` oder `private` angeben.

Eine neue Sicherheitsgruppe wird für abgegliche Cloud-Vorlagen erstellt, wenn der Netzwerktyp `outbound` oder `private` lautet.

Amazon Web Services, Microsoft Azure, NSX und VMware Cloud on AWS unterstützen diese Option.

Netzwerkrichtlinieneinstellungen können spezifisch für den Cloud-Kontotyp sein. Diese Einstellungen werden in der Wegweiser-Hilfe beschrieben und nachfolgend zusammengefasst:

■ **Netzwerkdomäne oder Transportzone**

Die Netzwerkdomäne oder Transportzone ist der Distributed Virtual Switch (dvSwitch) für die vSphere vNetwork Distributed PortGroups (dvPortGroup). Eine *Transportzone* ist ein vorhandenes NSX-Konzept, das mit den Begriffen *dvSwitch* oder *dvPortGroup* vergleichbar ist.

Wenn Sie ein Cloud-Konto von NSX verwenden, lautet der Elementname auf der Seite **Transportzone**, andernfalls **Netzwerkdomäne**.

Bei Standard-Switches entspricht die Netzwerkdomäne oder Transportzone dem Switch. Die Netzwerkdomäne oder Transportzone definiert die Begrenzungen der Subnetze innerhalb von vCenter.

Eine Transportzone steuert, welche Hosts ein logischer NSX-Switch erreichen kann. Sie kann sich auf einen oder mehrere vSphere-Cluster erstrecken. Transportzonen steuern, welche Cluster und welche virtuellen Maschinen an der Verwendung eines bestimmten Netzwerks teilnehmen können. Subnetze, die zur selben NSX-Transportzone gehören, können für dieselben Maschinenhosts verwendet werden.

■ **Externes Subnetz**

Ein bedarfsgesteuertes Netzwerk mit ausgehendem Zugriff erfordert ein externes Subnetz, das über ausgehenden Zugriff verfügt. Das externe Subnetz wird zur Bereitstellung von ausgehendem Zugriff verwendet, wenn es in der Cloud-Vorlage angefordert wird – die Netzwerkplatzierung wird dadurch nicht gesteuert. Das externe Subnetz hat beispielsweise keinen Einfluss auf die Platzierung eines privaten Netzwerks.

■ **CIDR**

Bei einer CIDR-Notation handelt es sich um eine komprimierte Darstellung einer IP-Adresse und des zugehörigen Routing-Präfixes. Der CIDR-Wert gibt den bei der Bereitstellung zu verwendenden Netzwerkadressbereich für die Erstellung von Subnetzen an. Diese CIDR-Einstellung auf der Registerkarte **Netzwerkrichtlinien** akzeptiert IPv4-Notationen, die auf „in/nn“ enden und Werte zwischen 0 und 32 enthalten.

■ Subnetzgröße

Mit dieser Option wird die Größe des bedarfsgesteuerten Netzwerks unter Verwendung der IPv4-Notation für jedes isolierte Netzwerk in einer Bereitstellung festgelegt, die dieses Netzwerkprofil verwendet. Die Einstellung „Subnetzgröße“ steht für die Verwaltung interner und externer IP-Adressen zur Verfügung.

Das IPv6-Format wird für bedarfsgesteuerte Netzwerke nicht unterstützt.

■ Distributed Logical Router

Für ein geroutetes bedarfsgesteuertes Netzwerk müssen Sie beispielsweise ein verteiltes logisches Netzwerk angeben, wenn Sie ein NSX-V-Cloud-Konto verwenden.

Ein Distributed Logical Router (DLR) wird verwendet, um den horizontalen Datenverkehr zwischen bedarfsgesteuerten gerouteten Netzwerken auf NSX-V weiterzuleiten. Diese Option wird nur angezeigt, wenn der Konto-/Regionswert für das Netzwerkprofil einem NSX-V-Cloud-Konto zugeordnet ist.

■ IP-Bereichszuweisung

Die Option ist für Cloud-Konten verfügbar, die NSX oder VMware Cloud on AWS unterstützen, einschließlich vSphere.

Die Einstellung für den IP-Bereich ist verfügbar, wenn ein vorhandenes Netzwerk mit einem externen IPAM-Integrationspunkt verwendet wird.

Sie können eine der folgenden drei Optionen auswählen, um einen IP-Bereichszuweisungstyp für das Bereitstellungsnetzwerk anzugeben:

■ Statisch und DHCP

Standardwert wird empfohlen. Diese Mischoption verwendet die zugeteilten Einstellungen für **CIDR** und **Subnetzbereich**, um den DHCP-Serverpool so zu konfigurieren, dass er die Hälfte der Adressraumzuteilung mithilfe der (dynamischen) DHCP-Methode und die Hälfte der IP-Adressraumzuteilung mithilfe der statischen Methode unterstützt. Verwenden Sie diese Option, wenn einige der mit einem bedarfsgesteuerten Netzwerk verbundenen Maschinen zugewiesene, statische IP-Adressen und einige andere Maschinen dynamische IP-Adressen benötigen. Zwei IP-Bereiche werden erstellt.

Diese Option ist äußerst wirksam bei Bereitstellungen mit Maschinen, die mit einem bedarfsgesteuerten Netzwerk verbunden sind, das Maschinen mit statischen IPs und Maschinen mit dynamisch über einen NSX-DHCP-Server zugewiesenen IPs sowie Bereitstellungen enthält, bei denen die Lastausgleichsdienst-VIP statisch ist.

■ DHCP (dynamisch)

Diese Option verwendet die zugewiesene CIDR-Adresse, um einen IP-Pool auf einem DHCP-Server zu konfigurieren. Alle IP-Adressen für dieses Netzwerk werden dynamisch zugewiesen. Für jede zugewiesene CIDR-Instanz wird ein einzelner IP-Bereich erstellt.

■ Statisch

Diese Option verwendet die zugewiesene CIDR-Adresse, um IP-Adressen statisch zuzuteilen. Verwenden Sie diese Option, wenn kein konfigurierter DHCP-Server für dieses Netzwerk benötigt wird. Für jede zugewiesene CIDR-Instanz wird ein einzelner IP-Bereich erstellt.

■ **IP-Blöcke**

Die Einstellung für die IP-Blöcke ist verfügbar, wenn Sie ein bedarfsgesteuertes Netzwerk mit einem externen IPAM-Integrationspunkt verwenden.

Mithilfe der Einstellung „IP-Block“ können Sie dem Netzwerkprofil über den integrierten externen IPAM-Anbieter einen benannten IP-Block oder Bereich hinzufügen. Sie können einen hinzugefügten IP-Block auch aus dem Netzwerkprofil entfernen. Informationen zum Erstellen einer externen IPAM-Integration finden Sie unter [Hinzufügen einer externen IPAM-Integration für Infoblox in vRealize Automation](#).

Externes IPAM ist für die folgenden Typen von Cloud-Konten/Regionen verfügbar:

- vSphere
- vSphere mit NSX-T
- vSphere mit NSX-V

■ **Netzwerkressourcen – Externes Netzwerk**

Externe Netzwerke werden auch als vorhandene Netzwerke bezeichnet. Diese Netzwerke werden datentechnisch erfasst und zur Auswahl bereitgestellt.

■ **Netzwerkressourcen – Logischer Tier-0 Router**

NSX-T verwendet den logischen Tier-0-Router als Gateway zu Netzwerken, die sich außerhalb der NSX-Bereitstellung befinden. Der logische Tier-0-Router konfiguriert den ausgehenden Zugriff für bedarfsgesteuerte Netzwerke.

■ **Netzwerkressourcen – Edge-Cluster**

Der angegebene Edge-Cluster stellt Routing-Dienste bereit. Der Edge-Cluster wird zum Konfigurieren des ausgehenden Zugriffs für bedarfsgesteuerte Netzwerke und Lastausgleichsdienste verwendet. Er erkennt den Edge-Cluster oder Ressourcenpool, in dem die Edge-Appliance bereitgestellt werden soll.

■ **Netzwerkressourcen – Edge-Datenspeicher**

Der angegebene Edge-Datenspeicher, der für die Bereitstellung der Edge-Appliance verwendet wird. Diese Eigenschaft gilt nur für NSX-V.

Tags können verwendet werden, um anzugeben, welche Netzwerke für die Cloud-Vorlage verfügbar sind.

Lastausgleichsdienste

Sie können Lastausgleichsdienste zum Netzwerkprofil hinzufügen. Aufgelistete Lastausgleichsdienste sind basierend auf Informationen verfügbar, die vom Cloud-Quellkonto erfasst wurden.

Wenn ein Tag in einem der Lastausgleichsdienste im Netzwerkprofil einem Tag in einer Lastausgleichsdienstkomponente in der Cloud-Vorlage entspricht, wird der Lastausgleichsdienst während der Bereitstellung berücksichtigt. Lastausgleichsdienste in einem abgeglichenen Netzwerkprofil werden verwendet, wenn eine Cloud-Vorlage bereitgestellt wird.

Weitere Informationen finden Sie unter [Verwenden von Einstellungen des Lastausgleichsdiensts in Netzwerkprofilen in vRealize Automation Cloud Assembly](#) und [Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen](#).

Sicherheitsgruppen

Wenn eine Cloud-Vorlage bereitgestellt wird, werden die Sicherheitsgruppen im zugehörigen Netzwerkprofil auf die bereitgestellten Netzwerkkarten der Maschinen angewendet. Für ein Amazon Web Services-spezifisches Netzwerkprofil stehen die Sicherheitsgruppen im Netzwerkprofil in derselben Netzwerkdomeäne (VPC) bereit wie die Netzwerke, die auf der Registerkarte „Netzwerke“ aufgelistet sind. Wenn auf der Registerkarte „Netzwerke“ im Netzwerkprofil keine Netzwerke aufgeführt sind, werden alle verfügbaren Sicherheitsgruppen angezeigt.

Sie können eine Sicherheitsgruppe verwenden, um die Isolierungseinstellungen für ein bedarfsgesteuertes `private-` oder `outbound-`Netzwerk weiter zu definieren. Sicherheitsgruppen werden auch auf `existing-`Netzwerke angewendet.

Aufgelistete Sicherheitsgruppen sind basierend auf Informationen verfügbar, die aus dem Cloud-Quellkonto erfasst oder als bedarfsgesteuerte Sicherheitsgruppe in einer Projekt- Cloud-Vorlage hinzugefügt werden. Weitere Informationen finden Sie unter [Sicherheitsressourcen in vRealize Automation](#).

Sicherheitsgruppen werden auf alle Maschinen in der Bereitstellung angewendet, die mit dem Netzwerk verbunden sind, das mit dem Netzwerkprofil übereinstimmt. Da möglicherweise mehrere Netzwerke in einer Cloud-Vorlage vorhanden sind, die jeweils einem anderen Netzwerkprofil entsprechen, können Sie verschiedene Sicherheitsgruppen für verschiedene Netzwerke verwenden.

Durch das Hinzufügen eines Tags zu einer vorhandenen Sicherheitsgruppe können Sie die Sicherheitsgruppe in einer `Cloud.SecurityGroup`-Komponente der Cloud-Vorlage verwenden. Eine Sicherheitsgruppe muss über mindestens ein Tag verfügen, ansonsten kann sie nicht in einer Cloud-Vorlage verwendet werden. Weitere Informationen finden Sie unter [Sicherheitsressourcen in vRealize Automation](#) und [Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen](#).

Weitere Informationen zu Netzwerkprofilen, Netzwerken, Cloud-Vorlagen und Tags

Weitere Informationen zu Netzwerken finden Sie unter [Netzwerkressourcen in vRealize Automation](#).

Beispiele für Netzwerkkomponentencode in einer Cloud-Vorlage finden Sie unter [Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen](#).

Beispiele für Netzwerkautomatisierungs-Workflows finden Sie unter [Netzwerkautomatisierung mit Cloud Assembly und NSX](#).

Weitere Informationen zu Tags und Tag-Strategien finden Sie unter [Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen](#).

Verwenden von Netzwerkeinstellungen in Netzwerkprofilen und Cloud-Vorlagen in vRealize Automation

Sie verwenden Netzwerke und Netzwerkprofile in vRealize Automation, um das Verhalten der Netzwerkbereitstellung für Ihre Bereitstellungen zu definieren.

In vRealize Automation können Sie Cloud-spezifische Netzwerkprofile definieren. Weitere Informationen hierzu finden Sie unter [Weitere Informationen zu Netzwerkprofilen in vRealize Automation](#).

Über die Netzwerk- und Netzwerkprofileinstellungen können Sie steuern, wie Netzwerk-IP-Adressen in vRealize Automation-Cloud-Vorlagen und -Bereitstellungen verwendet werden.

IPv4- und IPv6-Unterstützung in vRealize Automation-Netzwerken

vRealize Automation unterstützt reines IPv4 oder Dual-Stack-IPv4 und -IPv6. Reines IPv6 wird derzeit nicht unterstützt.

Während reines IPv4 für alle Cloud-Konto- und Integrationstypen unterstützt wird, werden Dual-Stack-IPv4 und -IPv6 nur für vSphere Cloud-Konten und deren Endpoints unterstützt.

IPv6 wird derzeit nicht für die Verwendung mit Lastausgleichsdiensten, bedarfsgesteuerten NSX-Netzwerken oder externen IPAM-Drittanbietern unterstützt.

Unterstützung des externen IPAM-Anbieters

Neben der bereitgestellten internen IPAM-Unterstützung können Sie einen externen IPAM-Anbieter verwenden, um IP-Adressen für Netzwerke dynamisch oder statisch zuzuordnen – als IP-Bereiche für vorhandene Netzwerke und als IP-Blöcke für bedarfsgesteuerte Netzwerke in Ihren Cloud-Vorlagendesigns und -bereitstellungen.

Die Unterstützung von externen IPAM-Anbietern, wie z. B. Infoblox, ist für anbieterspezifische IPAM-Integrationspunkte verfügbar, die Sie über die Menüfolge **Infrastruktur > Verbindungen > Integration hinzufügen > IPAM** hinzufügen.

Optionen zum Definieren von Adressinformationen eines externen IPAM-Anbieters sind über die Option **IPAM-IP-Bereich hinzufügen** auf der Seite **Netzwerkrichtlinien > IPAM-IP-Bereich hinzufügen** verfügbar.

Informationen zum Erstellen eines externen IPAM-Integrationspunkts finden Sie unter [Vorgehensweise zum Konfigurieren einer externen IPAM-Integration in vRealize Automation](#) . Ein Beispiel für die Erstellung eines IPAM-Integrationspunkts für einen bestimmten IPAM-Anbieter finden Sie unter [Lernprogramm: Konfigurieren einer anbieterspezifischen externen IPAM-Integration für vRealize Automation](#) .

Netzwerktypen

Eine Netzwerkkomponente in einer Cloud-Vorlage ist als einer der folgenden `networkType`-Typen definiert.

Netzwerktyp	Definition
<code>existing</code>	Wählt ein vorhandenes Netzwerk aus, das auf dem zugrunde liegenden Cloud-Anbieter konfiguriert ist, wie z. B. vCenter, Amazon Web Services und Microsoft Azure. Ein vorhandenes Netzwerk ist für das bedarfsgesteuerte <code>outbound</code> -Netzwerk erforderlich. Sie können einen Bereich von statischen IP-Adressen in einem vorhandenen Netzwerk definieren.
<code>public</code>	Auf Computer in einem öffentlichen Netzwerk kann über das Internet zugegriffen werden. Diese Netzwerke werden von einem IT-Administrator definiert. Die Definition eines <code>public</code> -Netzwerks ist identisch mit der eines <code>existing</code> -Netzwerks bei Netzwerken, die Netzwerkdatenverkehr in öffentlichen Netzwerken zulassen.
<code>private</code>	Ein bedarfsgesteuerter Netzwerktyp. Schränkt den Netzwerkdatenverkehr so ein, dass er nur zwischen Ressourcen im bereitgestellten Netzwerk erfolgt. Eingehender und ausgehender Datenverkehr werden verhindert. In NSX kann er mit bedarfsgesteuerter 1:n-NAT gleichgesetzt werden.

Netzwerktyp	Definition
outbound	<p>Ein bedarfsgesteuerter Netzwerktyp.</p> <p>Schränkt den Netzwerkdatenverkehr zwischen den Computing-Ressourcen in der Bereitstellung ein, ermöglicht aber auch unidirektionalen ausgehenden Netzwerkdatenverkehr. In NSX kann er mit bedarfsgesteuerter 1:n-NAT und externer IP-Adresse gleichgesetzt werden.</p>
routed	<p>Ein bedarfsgesteuerter Netzwerktyp.</p> <p>Geroutete Netzwerke enthalten einen routingfähigen IP-Adressbereich, der auf verfügbare miteinander verknüpfte Subnetze aufgeteilt ist. Die virtuellen Maschinen, die mit gerouteten Netzwerken bereitgestellt werden und die dasselbe geroutete Netzwerkprofil aufweisen, können miteinander und mit einem externen Netzwerk kommunizieren.</p> <p>Bei gerouteten Netzwerken handelt es sich um einen bedarfsgesteuerten Netzwerktyp, der für NSX-V- und NSX-T-Netzwerke verfügbar ist. Microsoft Azure und Amazon Web Services stellen standardmäßig diese Konnektivität bereit.</p> <p>Ein <code>routed</code>-Netzwerk ist nur für die Cloud-Vorlagenspezifikation in einer <code>Cloud.NSX.Network</code>-Netzwerkkomponente verfügbar.</p>

Beispiele für aufgefüllte Cloud-Vorlagen, die Netzwerkkomponentendaten enthalten, finden Sie unter [Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen](#).

Netzwerkszenarien

Sie können folgendes Verhalten erwarten, wenn Sie eine Cloud-Vorlage bereitstellen, die die folgende Netzwerkprofilkonfiguration verwendet.

Netzwerktyp oder Szenario	Keine Netzwerkprofile für Cloud-Zone verfügbar	Für die Cloud-Zone verfügbare Netzwerkprofile
Kein Netzwerk	<p>Wenn in der Cloud-Vorlage kein Netzwerk angegeben ist, wird ein zufälliges Netzwerk aus derselben Bereitstellungsregion wie die Berechnung ausgewählt.</p> <p>Bevorzugt werden Netzwerke, die als Standard gekennzeichnet sind.</p> <p>Wenn in einer verfügbaren Bereitstellungsregion keine Netzwerke vorhanden sind, schlägt die Bereitstellung fehl.</p>	<p>Ein Netzwerk wird aus einem passenden Netzwerkprofil ausgewählt.</p> <p>Bevorzugt werden Netzwerke, die als Standard gekennzeichnet sind.</p> <p>Wenn keines der Netzwerkprofile die Kriterien erfüllt, schlägt die Bereitstellung fehl.</p>
Vorhandenes Netzwerk	<p>Wenn die Netzwerkkomponente in der Cloud-Vorlage Einschränkungs-Tags enthält, werden diese Einschränkungen zum Filtern der Liste der verfügbaren Netzwerke verwendet. Einschränkungs-Tags in der Netzwerkkomponente der Cloud-Vorlage werden mit Netzwerk-Tags und gegebenenfalls mit den Einschränkungs-Tags des Netzwerkprofils abgeglichen.</p> <p>In der gefilterten Liste der Netzwerke wird ein einzelnes Netzwerk aus derselben Bereitstellungsregion wie die Berechnung ausgewählt.</p> <p>Bevorzugt werden Netzwerke, die als Standard gekennzeichnet sind.</p> <p>Wenn nach der auf Einschränkungen basierenden Filterung keine Netzwerke in der Bereitstellungsregion vorhanden sind, schlägt die Bereitstellung fehl.</p>	<p>Ein Netzwerk wird aus einem passenden Netzwerkprofil ausgewählt.</p> <p>Bevorzugt werden Netzwerke, die als Standard gekennzeichnet sind.</p> <p>Wenn keines der Netzwerkprofile die Kriterien erfüllt, schlägt die Bereitstellung fehl.</p> <p>Netzwerkeinschränkungen können verwendet werden, um vorhandene Netzwerke im Profil basierend auf ihren vorab zugewiesenen Tags zu filtern.</p>

Netzwerktyp oder Szenario	Keine Netzwerkprofile für Cloud-Zone verfügbar	Für die Cloud-Zone verfügbare Netzwerkprofile
Öffentliches Netzwerk	<p>Verfügt das Netzwerk über Einschränkungen, werden diese Einschränkungen zum Filtern der Liste der verfügbaren Netzwerke verwendet, für die das Attribut <code>supports public IP</code> festgelegt wurde.</p> <p>In der gefilterten Liste der Netzwerke wird ein zufälliges Netzwerk aus derselben Bereitstellungsregion wie die Berechnung ausgewählt.</p> <p>Bevorzugt werden Netzwerke, die als Standard gekennzeichnet sind.</p> <p>Wenn nach der auf Einschränkungen basierenden Filterung keine öffentlichen Netzwerke in der Bereitstellungsregion vorhanden sind, schlägt die Bereitstellung fehl.</p>	<p>Ein Netzwerk mit dem Attribut <code>supports public IP</code> wird aus einem passenden Netzwerkprofil ausgewählt.</p> <p>Bevorzugt werden Netzwerke, die als Standard gekennzeichnet sind.</p> <p>Netzwerkeinschränkungen können verwendet werden, um vorhandene öffentliche Netzwerke im Profil basierend auf vorab zugewiesenen Tags zu filtern.</p>
Privates Netzwerk	Die Bereitstellung schlägt fehl, da private Netzwerke Informationen aus einem Netzwerkprofil benötigen.	<p>Ein neues Netzwerk oder eine neue Sicherheitsgruppe wird basierend auf den Einstellungen im zugeordneten Netzwerkprofil erstellt.</p> <p>Netzwerkeinschränkungs-Tags können zum Filtern von Netzwerkprofilen und Netzwerken verwendet werden.</p>
Ausgehendes Netzwerk	Die Bereitstellung schlägt fehl, da ausgehende Netzwerke Informationen aus einem Netzwerkprofil benötigen.	<p>Ein neues Netzwerk oder eine neue Sicherheitsgruppe wird basierend auf den Einstellungen im zugeordneten Netzwerkprofil erstellt.</p> <p>Netzwerkeinschränkungs-Tags können zum Filtern von Netzwerkprofilen und Netzwerken verwendet werden.</p>
Geroutetes bedarfsgesteuertes Netzwerk	Die Bereitstellung schlägt fehl, da geroutete Netzwerke Informationen aus einem Netzwerkprofil benötigen.	<p>Für NSX-V ist die Auswahl des DLR (Distributed Logical Router) erforderlich.</p> <p>Für NSX-T und VMware Cloud on AWS werden ähnliche bedarfsgesteuerte Einstellungen wie „privat“ und „ausgehend“ benötigt.</p>

Netzwerktyp oder Szenario	Keine Netzwerkprofile für Cloud-Zone verfügbar	Für die Cloud-Zone verfügbare Netzwerkprofile
Beispielhafter WordPress-Anwendungsfall mit vorhandenen oder öffentlichen Netzwerken	Die Bereitstellung erfolgt gemäß der Beschreibung für ein vorhandenes oder öffentliches Netzwerk.	Oben finden Sie Beschreibungen zum Verhalten vorhandener und öffentlicher Netzwerke. Weitere Informationen hierzu finden Sie unter Lernprogramm: Einrichten und Testen einer Multi-Cloud-Infrastruktur und von Bereitstellungen in vRealize Automation Cloud Assembly .
Beispielhafter WordPress-Anwendungsfall mit vorhandenen oder öffentlichen Netzwerken und privaten oder ausgehenden Netzwerken	Die Bereitstellung schlägt fehl, da das Netzwerk Informationen aus einem Netzwerkprofil benötigt.	Oben finden Sie Beschreibungen für ein privates und ein ausgehendes Netzwerk. Weitere Informationen hierzu finden Sie unter Lernprogramm: Einrichten und Testen einer Multi-Cloud-Infrastruktur und von Bereitstellungen in vRealize Automation Cloud Assembly .
Beispielhafter WordPress-Anwendungsfall mit Lastausgleichsdienst	Die Bereitstellung schlägt fehl, da ein Lastausgleichsdienst Informationen aus einem Netzwerkprofil benötigt. Die Bereitstellung kann stattfinden, wenn vorhandene Lastausgleichsdienste zur Verfügung stehen.	Ein neuer Lastausgleichsdienst wird basierend auf der Konfiguration des Netzwerkprofils erstellt. Sie können einen vorhandenen Lastausgleichsdienst angeben, der im Netzwerkprofil aktiviert wurde. Die Bereitstellung schlägt fehl, wenn Sie einen vorhandenen Lastausgleichsdienst anfordern, der die Einschränkungen im Netzwerkprofil nicht erfüllt. Weitere Informationen hierzu finden Sie unter Lernprogramm: Einrichten und Testen einer Multi-Cloud-Infrastruktur und von Bereitstellungen in vRealize Automation Cloud Assembly .

Verwenden von Sicherheitsgruppeneinstellungen in Netzwerkprofilen und Cloud-Vorlagendesigns in vRealize Automation Cloud Assembly

Sie können Sicherheitsgruppeneinstellungen in Netzwerkprofilen und Cloud-Vorlagendesigns definieren und ändern.

Zur Verwendung von Sicherheitsgruppenfunktionen stehen mehrere Möglichkeiten bereit:

- Vorhandene Sicherheitsgruppe, die in einem Netzwerkprofil angegeben ist

Sie können eine vorhandene Sicherheitsgruppe zu einem Netzwerkprofil hinzufügen. Wenn dieses Netzwerkprofil in einem Cloud-Vorlagendesign verwendet wird, werden die zugehörigen Maschinen als Mitglieder der Sicherheitsgruppe zusammengefasst. Bei dieser Methode muss einem Cloud-Vorlagendesign keine Sicherheitsgruppenressource hinzugefügt werden. Sie können auch einen Lastausgleichsdienst in dieser Konfiguration verwenden. Weitere Informationen hierzu finden Sie unter [Verwenden einer Lastausgleichsdienstressource in einer vRealize Automation-Cloud-Vorlage](#).

- Sicherheitsgruppenkomponente, die der Maschinenressource in einem Cloud-Vorlagendesign zugeordnet ist

Sie können eine Sicherheitsgruppenressource per Drag & Drop auf ein Cloud-Vorlagendesign verschieben und die Sicherheitsgruppenressource an eine Maschinen-Netzwerkkarte binden, indem Sie Einschränkungs-Tags in der vorhandenen Sicherheitsgruppenressource im Cloud-Vorlagendesign und in der vorhandenen Sicherheitsgruppe in der Ressource verwenden, für die Daten erfasst wurden. Sie können diese Zuordnung auch vornehmen, indem Sie die Objekte mit einer Verbindungslinie auf der Design-Arbeitsfläche für die Cloud-Vorlage verbinden, ähnlich der Vorgehensweise, mit der Sie Netzwerke Maschinen auf der Design-Arbeitsfläche zuordnen.

Wenn Sie eine Sicherheitsgruppenressource auf die Design-Arbeitsfläche der Cloud-Vorlage ziehen, kann sie vom Typ `existing` oder `new` sein. Wenn es sich um den Sicherheitsgruppentyp `existing` handelt, sollten Sie bei Aufforderung einen Tageinschränkungswert hinzufügen. Wenn es sich um den Sicherheitsgruppentyp `new` handelt, können Sie Firewallregeln konfigurieren.

- Eine vorhandene Sicherheitsgruppe, die mit Tag-Einschränkungen zugeteilt wurde und die mit einer Maschinen-Netzwerkkarte in der Cloud-Vorlage verknüpft ist

Beispielsweise können Sie eine Sicherheitsgruppenressource mit einer Maschinen-Netzwerkkarte (in einer Maschinenressource) im Cloud-Vorlagendesign verknüpfen, indem Sie die Tags zwischen den beiden Ressourcen abgleichen.

Wenn beispielsweise für NSX-T Tags im Quell-Endpoint angegeben werden, können Sie NSX-T-Tags verwenden, die in Ihrer NSX-T-Anwendung angegeben sind. Sie können dann ein NSX-T-Tag verwenden, das als Einschränkung für eine Netzwerkressource in einem Cloud-Vorlagendesign angegeben ist, wobei die Netzwerkressource mit einer Maschinen-Netzwerkkarte im Cloud-Vorlagendesign verbunden ist. Mit NSX-T-Tags können Sie Maschinen unter Verwendung eines vordefinierten NSX-T-Tags dynamisch gruppieren, dessen Daten aus dem NSX-T-Quell-Endpoint erfasst wurden. Verwenden Sie einen logischen Port, wenn Sie das NSX-T-Tag in NSX-T erstellen.

- Firewallregeln in einer bedarfsgesteuerten Sicherheitsgruppenressource in einem Cloud-Vorlagendesign

Sie können einer bedarfsgesteuerten Sicherheitsgruppe im Cloud-Vorlagendesign Firewallregeln hinzufügen.

Informationen zu verfügbaren Firewallregeln finden Sie unter [Verwenden einer Sicherheitsgruppenressource in einer vRealize Automation-Cloud-Vorlage](#).

Weitere Informationen

Informationen zum Definieren von Sicherheitsgruppen in Netzwerkprofilen finden Sie unter [Weitere Informationen zu Netzwerkprofilen in vRealize Automation](#).

Informationen zum Anzeigen und Ändern von Sicherheitsgruppeneinstellungen auf den Seiten der Infrastrukturressourcen finden Sie unter [Sicherheitsressourcen in vRealize Automation](#).

Informationen zum Definieren von Sicherheitsgruppen in Cloud-Vorlagendesigns finden Sie unter [Verwenden einer Sicherheitsgruppenressource in einer vRealize Automation-Cloud-Vorlage](#).

Beispiele für Sicherheitsgruppenressourcen in Cloud-Vorlagendesigns finden Sie unter [Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen](#).

Verwenden von Einstellungen des Lastausgleichsdiensts in Netzwerkprofilen in vRealize Automation Cloud Assembly

Sie können die Einstellungen für den Lastausgleichsdienst in der Netzwerkprofilkonfiguration konfigurieren.

Sie können einen vorhandenen Lastausgleichsdienst zu einem Netzwerkprofil hinzufügen, indem Sie die Registerkarte **Lastausgleichsdienst** verwenden.

Sie können einem Cloud-Vorlagendesign einen Lastausgleichsdienst hinzufügen, indem Sie es einem Netzwerkprofil zuordnen, das einen oder mehrere Lastausgleichsdienste enthält, oder Sie können direkt eine Lastausgleichsdienstressource auf der Cloud-Vorlagendesign-Arbeitsfläche oder im Code verwenden.

Beispiele für das Einschließen einer Lastausgleichsdienst-VIP basierend auf der Nutzung der Sicherheitsgruppe in einem Netzwerkprofil

Es gibt zwei Typen von Sicherheitsgruppen, die Sie in einem Netzwerkprofil verwenden können: eine vorhandene Sicherheitsgruppe, die Sie über die Registerkarte **Sicherheitsgruppen** auswählen, und eine bedarfsgesteuerte Sicherheitsgruppe, die Sie erstellen, indem Sie eine Isolierungsrichtlinie auf der Registerkarte **Netzwerkrichtlinien** verwenden.

Wenn eine Lastausgleichsdienst-VIP basierend auf Netzwerkprofileinstellungen mit einer Sicherheitsgruppe verknüpft ist, wird die Sicherheitsgruppenkonfiguration vom Netzwerkprofil bereitgestellt.

In der folgenden Tabelle werden einige Beispielszenarien veranschaulicht.

Topologie des Cloud-Vorlagendesigns – zugeordnete Ressourcen	Konfiguration des Netzwerkprofils	Mitgliedschaft bei der Sicherheitsgruppe
Einarmiger Lastausgleichsdienst mit VIP in einem privaten Netzwerk und einer Maschine im gleichen privaten Netzwerk.	Das ausgewählte Netzwerkprofil verwendet eine Isolierungsrichtlinie, die als bedarfsgesteuerte Sicherheitsgruppe definiert ist.	Die Netzwerkkarte der Maschine und die Lastausgleichsdienst-VIP werden der Isolierungssicherheitsgruppe hinzugefügt.
Einarmiger Lastausgleichsdienst mit VIP in einem privaten Netzwerk und einer Maschine im gleichen privaten Netzwerk.	Das ausgewählte Netzwerkprofil verwendet eine vorhandene Sicherheitsgruppe und eine Isolierungsrichtlinie, die als bedarfsgesteuerte Sicherheitsgruppe definiert ist.	Die Netzwerkkarte der Maschine und die Lastausgleichsdienst-VIP werden der Isolierungssicherheitsgruppe und der vorhandenen Sicherheitsgruppe hinzugefügt.
Zweiarmiger Lastausgleichsdienst mit VIP in einem öffentlichen Netzwerk und Maschine in einem privaten Netzwerk.	Das ausgewählte Netzwerkprofil verwendet eine vorhandene Sicherheitsgruppe und eine Isolierungsrichtlinie, die als bedarfsgesteuerte Sicherheitsgruppe definiert ist.	Die Netzwerkkarte der Maschine und die Lastausgleichsdienst-VIP werden der Isolierungssicherheitsgruppe und der vorhandenen Sicherheitsgruppe hinzugefügt.
Zweiarmiger Lastausgleichsdienst mit VIP in einem öffentlichen Netzwerk und einer Maschine in einem privaten Netzwerk.	Das ausgewählte Netzwerkprofil verwendet eine vorhandene Sicherheitsgruppe.	Die Netzwerkkarte der Maschine und die Lastausgleichsdienst-VIP werden der vorhandenen Sicherheitsgruppe hinzugefügt.
Zweiarmiger Lastausgleichsdienst, die VIP befindet sich in Netzwerk 1 und die Maschine befindet sich in Netzwerk 2.	Zwei Netzwerkprofile: <ul style="list-style-type: none"> ■ Netzwerkprofil 1: verwendet eine vorhandene Sicherheitsgruppe 1. ■ Netzwerkprofil 2: verwendet eine vorhandene Sicherheitsgruppe 2. 	Der Lastausgleichsdienst landet auf dem Netzwerkprofil 1, und die Maschine landet auf dem Netzwerkprofil 2. Die Lastausgleichsdienst-VIP wird der Sicherheitsgruppe 1 hinzugefügt, und die Netzwerkkarte der Maschine wird der Sicherheitsgruppe 2 hinzugefügt.

Weitere Informationen

Weitere Informationen zum Hinzufügen von Lastausgleichsdienstressourcen zu einem Cloud-Vorlagendesign finden Sie unter [Verwenden einer Lastausgleichsdienstressource in einer vRealize Automation-Cloud-Vorlage](#).

Beispiele für Cloud-Vorlagendesigns, die Lastausgleichsdienste enthalten, finden Sie unter [Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen](#).

Vorgehensweise zum Konfigurieren eines Netzwerkprofils zur Unterstützung eines bedarfsgesteuerten Netzwerks für eine externe IPAM-Integration in vRealize Automation

Sie können ein Netzwerkprofil zur Unterstützung von IP-Adressblöcken für ein bedarfsgesteuertes Netzwerk konfigurieren, wenn dieses Netzwerkprofil in einer vRealize Automation-Cloud-Vorlage verwendet wird, die externe IPAM-Integration verwendet.

Mithilfe einer vorhandenen Integration für einen bestimmten externen IPAM-Anbieter können Sie ein bedarfsgesteuertes Netzwerk zur Erstellung eines neuen Netzwerks im externen IPAM-System bereitstellen.

Mit diesem Vorgang konfigurieren Sie einen Block von IP-Adressen, statt übergeordnetes CIDR bereitzustellen (wie bei Verwendung des internen IPAM von vRealize Automation). Der IP-Adressblock wird während der Bereitstellung eines bedarfsgesteuerten Netzwerks verwendet, um das neue Netzwerk in Segmente aufzuteilen. Die Daten der IP-Blöcke werden über den externen IPAM-Anbieter erfasst, vorausgesetzt, die Integration unterstützt bedarfsgesteuerte Netzwerke. Wenn Sie beispielsweise eine IPAM-Integration von Infoblox verwenden, stellen-IP-Blöcke Infoblox-Netzwerkcontainer dar.

Wenn Sie ein bedarfsgesteuertes Netzwerkprofil und eine externe IPAM-Integration in einer Cloud-Vorlage verwenden, werden die folgenden Ereignisse bei der Bereitstellung der Cloud-Vorlage angezeigt:

- Ein Netzwerk wird im externen IPAM-Anbieter erstellt.
- Außerdem wird in vRealize Automation ein Netzwerk erstellt, das die neue Netzwerkkonfiguration des IPAM-Providers widerspiegelt, einschließlich CIDR-Einstellungen und Gateway-Eigenschaften.
- Die IP-Adresse für die bereitgestellte virtuelle Maschine wird aus dem neu erstellten Netzwerk abgerufen.

In diesem Beispiel für ein bedarfsgesteuertes Netzwerk konfigurieren Sie ein Netzwerkprofil, damit eine Cloud-Vorlagenbereitstellung eine Maschine in einem bedarfsgesteuerten Netzwerk in vSphere mithilfe von Infoblox als externem IPAM-Anbieter bereitstellen kann.

Informationen hierzu finden Sie unter [Vorgehensweise zum Konfigurieren eines Netzwerkprofils zur Unterstützung eines vorhandenen Netzwerks für eine externe IPAM-Integration in vRealize Automation](#). Beide Beispiele für eine Netzwerkkonfiguration passen in den anbieterspezifischen Gesamtworkflow für die externe IPAM-Integration unter [Lernprogramm: Konfigurieren von VMware Cloud on AWS für vRealize Automation](#).

Voraussetzungen

Während die folgenden Voraussetzungen für die Person gelten, die das Netzwerkprofil erstellt oder bearbeitet, ist das Netzwerkprofil selbst anwendbar, wenn es von einer Cloud-Vorlagenbereitstellung verwendet wird, die eine IPAM-Integration enthält. Weitere Informationen zu anbieterspezifischen IPAM-Integrationspunkten finden Sie unter [Vorgehensweise zum Konfigurieren einer externen IPAM-Integration in vRealize Automation](#).

Diese Abfolge von Schritten wird im Kontext eines Workflows für die IPAM-Anbieterintegration angezeigt. Weitere Informationen finden Sie unter [Lernprogramm: Konfigurieren einer anbieterspezifischen externen IPAM-Integration für vRealize Automation](#).

- Vergewissern Sie sich, dass Sie über Cloud-Administratoranmeldedaten verfügen. Weitere Informationen hierzu finden Sie unter [Zum Arbeiten mit Cloud-Konten in vRealize Automation sind Anmeldedaten erforderlich](#).

- Stellen Sie sicher, dass Sie über die Benutzerrolle des Cloud-Administrators verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Stellen Sie sicher, dass Sie über ein Konto beim externen IPAM-Anbieter verfügen, z. B. [Infoblox](#) oder [BlueCat](#), und dass Sie über die korrekten Zugriffsberechtigungen für das Konto Ihrer Organisation beim IPAM-Anbieter verfügen. In diesem Beispiel-Workflow ist der IPAM-Anbieter Infoblox.
- Stellen Sie sicher, dass Sie über einen IPAM-Integrationspunkt für den IPAM-Anbieter verfügen und dass das zum Erstellen der IPAM-Integration verwendete IPAM-Paket bedarfsgesteuerte Netzwerke unterstützt. Weitere Informationen hierzu finden Sie unter [Hinzufügen einer externen IPAM-Integration für Infoblox in vRealize Automation](#).

Obwohl das IPAM-Paket von Infoblox bedarfsgesteuerte Netzwerke unterstützt, stellen Sie bei Verwendung einer externen IPAM-Integration für einen anderen Anbieter sicher, dass das zugehörige IPAM-Integrationspaket bedarfsgesteuerte Netzwerke unterstützt.

Verfahren

- 1 Zum Konfigurieren eines Netzwerkprofils klicken Sie auf **Infrastruktur > Konfigurieren > Netzwerkprofile**.
- 2 Klicken Sie auf **Neues Netzwerkprofil**.
- 3 Klicken Sie auf die Registerkarte **Übersicht** und geben Sie die folgenden Beispieleinstellungen an:
 - Geben Sie ein/eine vSphere-Cloud-Konto/-Region an, wie z. B. **vSphere-IPAM-OnDemandA/Datacenter**.

In diesem Beispiel wird von der Verwendung eines vSphere-Cloud-Kontos ausgegangen, das keinem NSX-Cloud-Konto zugeordnet ist.
 - Geben Sie dem Netzwerkprofil einen Namen, z. B. **Infoblox-OnDemandNP**.
 - Fügen Sie ein Funktions-Tag für das Netzwerkprofil hinzu, wie z. B. **infoblox_ondemandA**.

Notieren Sie sich den Wert des Funktions-Tags, der auch als Cloud-Vorlagen-Einschränkungs-Tag verwendet werden muss, um die bei der Bereitstellung der Cloud-Vorlage zu verwendende Netzwerkprofilverknüpfung zu erstellen.
- 4 Klicken Sie auf die Registerkarte **Netzwerkrichtlinien** und geben Sie die folgenden Beispieleinstellungen an:
 - Wählen Sie im Dropdown-Menü **Isolierungsrichtlinie** die Option **Bedarfsgesteuertes Netzwerk** aus.

Mit dieser Option können Sie externe IPAM-IP-Blöcke verwenden. Je nach Cloud-Konto werden neue Optionen angezeigt. Folgende Optionen werden beispielsweise angezeigt, wenn ein vSphere-Cloud-Konto verwendet wird, das mit einem NSX-Cloud-Konto verknüpft ist:

- Transportzone
- Logischer Tier-0-Router
- Edge-Cluster

Da in diesem Beispiel das vSphere-Cloud-Konto nicht mit NSX verknüpft ist, wird die Menüoption **Netzwerkdomäne** angezeigt.

- Lassen Sie die Menüoption **Netzwerkdomäne** leer.

- 5 Klicken Sie auf **Extern** als **Quelle** der Adressverwaltung.
- 6 Klicken Sie auf **IP-Block hinzufügen**, um die Seite **IPAM-IP-Block hinzufügen** zu öffnen.
- 7 Wählen Sie im Menü **Anbieter** auf der Seite **IPAM-IP-Block hinzufügen** eine vorhandene externe IPAM-Integration aus. Wählen Sie beispielsweise den Integrationspunkt *Infoblox_Integration* unter [Hinzufügen einer externen IPAM-Integration für Infoblox in vRealize Automation](#) im Beispielworkflow aus.
- 8 Wählen Sie im Menü **Adressbereiche** einen der verfügbaren und aufgelisteten IP-Blöcke aus, z. B. **10.23.118.0/24**, und fügen Sie ihn hinzu.

Wenn der IPAM-Anbieter Adressbereiche unterstützt, wird das Menü **Adressbereiche** angezeigt. Bei einer Infoblox-Integration werden Adressbereiche durch Infoblox-Netzwerkansichten dargestellt.
- 9 Wählen Sie eine **Subnetzgröße** aus, wie z. B. **/29 (-6 IP-Adressen)**.
- 10 Klicken Sie auf **Erstellen**.

Ergebnisse

Es wird ein Netzwerkprofil erstellt, das zur Bereitstellung eines bedarfsgesteuerten Netzwerks mithilfe der angegebenen externen IPAM-Integration verwendet werden kann. Die folgende Beispiel-Cloud-Vorlage zeigt eine einzelne Maschine, die in einem Netzwerk bereitgestellt werden soll, das durch dieses neue Netzwerkprofil definiert ist.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: ubuntu
      flavor: small
      networks:
        - network: '${resource.Cloud_Network_1.id}'
          assignment: static
```

```
Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkType: private
    constraints: - tag: infoblox_ondemandA
```

Hinweis Bei der Bereitstellung der Cloud-Vorlage wird das erste verfügbare Netzwerk im angegebenen IP-Block abgerufen und als Netzwerk-CIDR angesehen. Bei Verwendung eines NSX-Netzwerks in der Cloud-Vorlage können Sie stattdessen das CIDR des Netzwerks mithilfe der unten angezeigten Netzwerkeigenschaft `networkCidr` manuell festlegen und die Einstellungen für IP-Adressen und die Subnetzgröße überschreiben, die im zugehörigen Netzwerkprofil angegeben sind.

```
Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkCidr: 10.10.0.0/16
```

Vorgehensweise zum Konfigurieren eines Netzwerkprofils zur Unterstützung eines vorhandenen Netzwerks für eine externe IPAM-Integration in vRealize Automation

Sie können ein Netzwerkprofil zur Unterstützung von IP-Adressbereichen für ein vorhandenes Netzwerk konfigurieren, wenn dieses Netzwerkprofil in einem vRealize Automation-Blueprint verwendet wird, der die externe IPAM-Integration nutzt.

Ein Beispiel wird im Rahmen eines anbieterspezifischen Beispielworkflows unter [Konfigurieren eines Netzwerks und Netzwerkprofils zur Verwendung von IPAM \(extern\) für ein vorhandenes Netzwerk in vRealize Automation](#) bereitgestellt. Der gesamte anbieterspezifische Workflow für die externe IPAM-Integration befindet sich unter [Lernprogramm: Konfigurieren von VMware Cloud on AWS für vRealize Automation](#).

Informationen hierzu finden Sie unter [Vorgehensweise zum Konfigurieren eines Netzwerkprofils zur Unterstützung eines bedarfsgesteuerten Netzwerks für eine externe IPAM-Integration in vRealize Automation](#).

Vorgehensweise zum Hinzufügen von vRealize Automation Cloud Assembly-Speicherprofilen, die verschiedenen Anforderungen entsprechen

Ein vRealize Automation Cloud Assembly-Speicherprofil beschreibt die Art des bereitzustellenden Speichers.

Für Speicher wird in der Regel ein Profil anhand von Merkmalen wie Dienstebene oder Kosten, Leistung oder Zweck (z. B. Sicherung) erstellt.

Wählen Sie **Infrastruktur > Konfigurieren > Speicherprofile** aus und klicken Sie auf **Neues Speicherprofil**.

Weitere Informationen zu Speicherprofilen in vRealize Automation

Ein Cloud-Kontobereich enthält Speicherprofile, mit denen der Cloud-Administrator Speicher für die Region in vRealize Automation festlegen kann.

Speicherprofile enthalten Festplattenanpassungen sowie eine Möglichkeit zur Angabe des Speichertyps anhand von Funktions-Tags. Tags werden dann mit den Anforderungseinschränkungen des Bereitstellungsdiensts abgeglichen, um den gewünschten Speicher zur Bereitstellungszeit zu erstellen.

Speicherprofile sind nach Cloud-spezifischen Regionen organisiert. Ein Cloud-Konto kann aus verschiedenen Regionen mit mehreren Speicherprofilen pro Region bestehen.

Anbieterunabhängige Platzierung ist möglich. Stellen Sie sich beispielsweise drei verschiedene Anbieterkonten mit einer Region pro Konto vor. Jede Region enthält ein Speicherprofil mit dem Funktions-Tag *fast*. Zur Bereitstellungszeit sucht eine Anforderung mit einem Einschränkungstyp vom Typ *fast* nach einer übereinstimmenden Funktion vom Typ *fast*. Dabei spielt es keine Rolle, welche Anbieter-Cloud die Ressourcen bereitstellt. Im Fall einer Übereinstimmung werden die Einstellungen aus dem verknüpften Speicherprofil während der Erstellung des bereitgestellten Speicherelements angewendet.

Hinweis Verschiedene Cloud-Speicher können unterschiedliche Leistungsmerkmale aufweisen, werden aber dennoch als das *fast*-Angebot des Administrators betrachtet, der sie markiert hat.

Funktions-Tags, die Sie zu Speicherprofilen hinzufügen, sollten keine tatsächlichen Ressourcenziele angeben. Stattdessen sollten sie Speichertypen beschreiben. Weitere Informationen zu tatsächlichen Ressourcen finden Sie unter [Speicherressourcen in vRealize Automation](#).

Sie können ein Speicherprofil zur Unterstützung von FCD-Speicher (First Class Disk) oder standardmäßigem Festplattenspeicher erstellen, indem Sie die Option **Festplattentyp** auf der Seite „Speicherprofil“ oder die vRealize Automation-API verwenden. Wenn Sie die Option „First Class Disk (FCD)“ auswählen, erstellen Sie effektiv ein vSphere-Speicherprofil.

■ First Class Disk

Eine First Class Disk kann unabhängig von einer vSphere-VM erstellt und verwaltet werden. Eine FCD verfügt über Lebenszyklusverwaltungsfunktionen, die auch unabhängig von einer VM funktionieren. Die FCD ist zur Verwendung mit vSphere Version 6,7 Update 2 und höher verfügbar und wird derzeit in vRealize Automation als reine API-Funktion implementiert.

Informationen zum FCD-Speicher (First Class Disk), einschließlich der Funktionen, die über die vRealize Automation-API verfügbar sind, und Links zur API-Dokumentation selbst finden Sie unter [Wozu dient First Class Disk-Speicher in vRealize Automation?](#).

■ Standardfestplatte

Der standardmäßige Festplattenspeicher wird als integrierte Komponente einer VM erstellt und verwaltet.

Informationen zum standardmäßigen Festplattenspeicher finden Sie unter [Wozu dient Standardfestplattenspeicher in vRealize Automation?](#) und [Wozu dient dauerhafter Festplattenspeicher in vRealize Automation?](#).

Vorgehensweise zum Verwenden von Tags zur Verwaltung von vRealize Automation Cloud Assembly-Ressourcen und -Bereitstellungen

Tags sind eine kritische Komponente von vRealize Automation Cloud Assembly, die die Platzierung von Bereitstellungen durch den Abgleich von Funktionen und Einschränkungen steuern. Sie müssen Tags verstehen und effektiv implementieren, um vRealize Automation Cloud Assembly optimal zu nutzen.

Grundsätzlich sind Tags Beschriftungen, die Sie zu vRealize Automation Cloud Assembly-Elementen hinzufügen. Sie können alle Tags erstellen, die für Ihre Organisation und Implementierung geeignet sind. Im Vergleich zu Beschriftungen haben Tags jedoch einen weitaus größeren Funktionsumfang, da Sie steuern, wie und wo vRealize Automation Cloud Assembly Ressourcen und Infrastruktur zum Erstellen von bereitzustellenden Diensten verwendet. Tags unterstützen auch die Steuerung innerhalb von Cloud Assembly.

Tag-Struktur

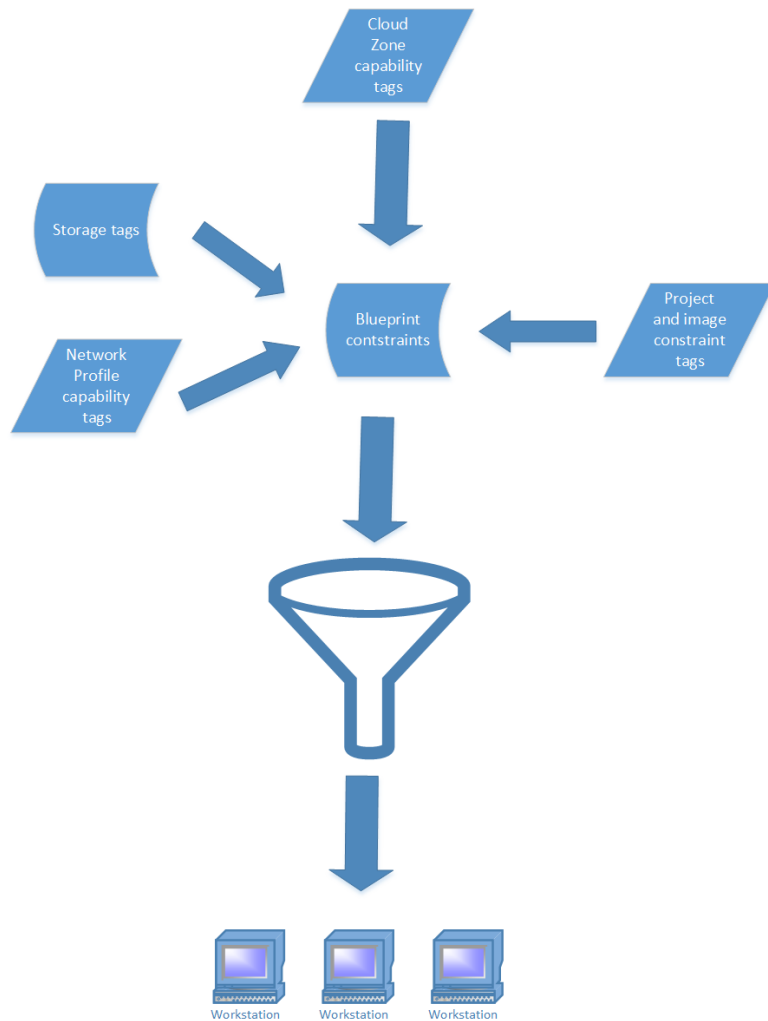
Strukturell müssen Tags der `name:value`-Paar-Konvention folgen, aber ansonsten ist ihre Konstruktion weitgehend frei. In der gesamten vRealize Automation Cloud Assembly erscheinen alle Tags gleich und die Tag-Funktionalität wird durch den Kontext bestimmt.

Beispielsweise funktionieren Tags für Infrastrukturressourcen primär als Funktions-Tags, da sie von vRealize Automation Cloud Assembly verwendet werden, um Ressourcen mit Bereitstellungen abzugleichen. In zweiter Linie bezeichnen sie auch die Ressourcen.

Tag-Funktion

Die primäre Funktion von Tags besteht darin, Funktionen und Einschränkungen auszudrücken, die vRealize Automation Cloud Assembly zum Definieren von Bereitstellungen verwendet. Der Kontext bestimmt die Funktion von Tags. Tags, die in Cloud-Zonen, Netzwerk- und Speicherprofilen und einzelnen Infrastrukturressourcen platziert werden, dienen als Funktions-Tags und definieren die gewünschten Funktionen für in Bereitstellungen verwendete Infrastruktur. Tags, die in Cloud-Vorlagen platziert werden, dienen als Einschränkungen, die Ressourcen für Bereitstellungen definieren. Darüber hinaus können Cloud-Administratoren Einschränkungs-Tags in Projekten platzieren, um eine gewisse Governance über diese Projekte auszuüben. Diese Einschränkungs-Tags werden anderen in Cloud-Vorlagen ausgedrückten Einschränkungen hinzugefügt.

Während der Bereitstellung vergleicht vRealize Automation Cloud Assembly diese Funktionen mit Einschränkungen, die auch als Tags ausgedrückt werden, in Cloud-Vorlagen, um die Bereitstellungskonfiguration zu definieren. Diese Tag-basierten Funktionen und Einschränkungen dienen als Grundlage für die Bereitstellungskonfiguration in vRealize Automation Cloud Assembly. Sie können beispielsweise Tags verwenden, um die Infrastruktur nur auf PCI-Ressourcen in einer bestimmten Region verfügbar zu machen.



Auf einer sekundären Ebene erleichtern Tags auch die Suche und Identifizierung von Speicher- und Netzwerkelementen und anderen Infrastrukturressourcen.

Angenommen Sie richten Cloud-Zonen ein und es stehen Ihnen viele Computing-Ressourcen zur Verfügung. Wenn Sie Ihre Computing-Ressourcen entsprechend gekennzeichnet haben, können Sie die Suchfunktion auf der Registerkarte „Computing“ auf der Seite „Cloud-Zone“ verwenden, um die Ressourcen zu filtern, die mit dieser bestimmten Cloud-Zone verknüpft sind.

Außerdem enthalten die Seite „Tags verwalten“ und die Seiten für die Ressourcenkonfiguration Suchfunktionen, mit denen Sie Elemente nach Tag-Namen suchen können. Die Verwendung von logischen und lesbaren Tags für diese Elemente ist der Schlüssel zur Erleichterung dieser Such- und Identifizierungsfunktion.

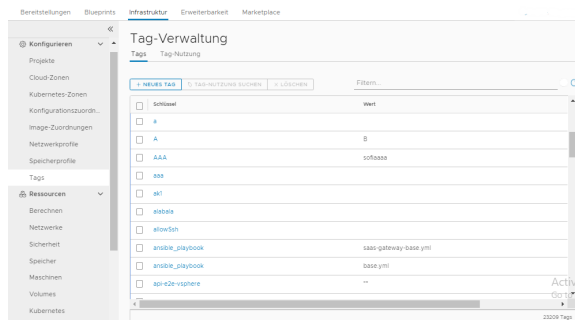
Im Folgenden YouTube-Video erhalten Sie weitere Informationen und Beispiele für die Tag-Nutzung: <https://youtu.be/4zNQ33RyQio>

Externe Tags

vRealize Automation Cloud Assembly kann auch externe Tags enthalten. Diese Tags werden automatisch aus Cloud-Konten importiert, die Sie mit einer vRealize Automation Cloud Assembly-Instanz verknüpfen. Diese Tags können aus vSphere, AWS, Azure oder anderen externen Softwareprodukten importiert werden. Wenn diese Tags importiert werden, stehen sie auf dieselbe Weise zur Verfügung wie die von Benutzern erstellten Tags.

Verwalten von Tags

Sie können die Seite „Tags verwalten“ in vRealize Automation Cloud Assembly verwenden, um Ihre Tags-Bibliothek zu überwachen und zu verwalten. Sie können auf dieser Seite auch Tags erstellen. Darüber hinaus ist die Seite „Tags verwalten“ die einzige Seite, auf der Sie externe Tags anzeigen und identifizieren können.



Tag-Strategie

Um die Verwirrung zu minimieren, sollten Sie vor dem Erstellen von Tags in vRealize Automation Cloud Assembly eine geeignete Tag-Strategie und Konventionen für die Kennzeichnung entwickeln, damit alle Benutzer, die Tags erstellen und verwenden, verstehen, was sie bedeuten und wie sie verwendet werden sollen. Weitere Informationen hierzu finden Sie unter [Erstellen einer Tagging-Strategie](#).

Erstellen einer Tagging-Strategie

Eine geeignete Tagging-Strategie muss unter Berücksichtigung der IT-Struktur und der Ziele Ihres Unternehmens sorgfältig geplant und implementiert werden, um die Cloud Assembly-Funktionen zu optimieren und Verwechslungen möglichst zu vermeiden.

Während das Tagging verschiedenen allgemeinen Zwecken dient, muss Ihre Tagging-Strategie auf die Bedürfnisse, die Struktur und die Ziele Ihrer Bereitstellung zugeschnitten werden.

Empfehlungen für Tagging

Einige allgemeine Merkmale für eine effektive Tagging-Strategie:

- Entwerfen und implementieren Sie eine einheitliche Tagging-Strategie, die die Struktur Ihres Unternehmens abbildet, und kommunizieren Sie diese Strategie an alle betreffenden Benutzer. Eine Strategie muss Ihre Bereitstellungsanforderungen unterstützen, eine klar verständliche Sprache verwenden und für alle betreffenden Benutzer schlüssig sein.
- Verwenden Sie einfache, eindeutige und aussagekräftige Namen und Werte für Tags. Beispielsweise sollten die Tag-Namen für Speicher- und Netzwerkelemente klar und verständlich sein, damit Benutzer leicht nachvollziehen können, welche Tag-Zuweisungen für eine bereitgestellte Ressource auszuwählen oder zu überprüfen sind.
- Obwohl Sie Tags mit einem Namen ohne Wert erstellen können, empfiehlt sich die Erstellung eines entsprechenden Werts für jeden Tag-Namen, da dies die Verwendung von Tags für andere Benutzer erkennbar macht.
- Vermeiden Sie das Erstellen duplizierter oder nicht relevanter Tags. Erstellen Sie z. B. nur Tags für Speicherelemente, die sich auf Speicherprobleme beziehen.

Tagging-Implementierung

Skizzieren Sie Ihre wichtigsten Überlegungen für eine grundlegende Tagging-Strategie. Die folgende Liste enthält typische Überlegungen, die beim Planen Ihrer Strategie berücksichtigt werden sollten. Beachten Sie, dass diese Überlegungen eher als Vorschlag und nicht als Weisung dienen. Unter Umständen müssen Sie bei Ihren Überlegungen andere Prioritäten für Ihre Anwendungsfälle setzen. Ihre Strategie muss für Ihre speziellen Anwendungsfälle geeignet sein.

- Anzahl der verschiedenen Umgebungen, für die eine Bereitstellung erfolgen soll. In der Regel erstellen Sie Tags für jede Umgebung.
- Struktur der Computing-Ressourcen und deren Verwendung zur Unterstützung von Bereitstellungen.
- Anzahl der verschiedenen Regionen oder Standorte, für die eine Bereitstellung erfolgen soll. In der Regel erstellen Sie Tags für diese verschiedenen Regionen und Standorte auf Profilebene.
- Anzahl der verschiedenen Speicheroptionen für Bereitstellungen und deren Eigenschaften. Diese Optionen sollten durch Tags dargestellt werden.
- Kategorisieren Sie Ihre Netzwerkoptionen und erstellen Sie Tags, um alle anwendbaren Optionen zu berücksichtigen.

- Typische Bereitstellungsvariablen. Beispielsweise die Anzahl der verschiedenen Umgebungen, für die eine Bereitstellung erfolgen soll. In der Regel verfügen die meisten Unternehmen über Test-, Entwicklungs- und Produktionsumgebungen. Sie möchten übereinstimmende Einschränkungs-Tags und Funktions-Tags für Cloud-Zonen erstellen und aufeinander abstimmen, um Bereitstellungen problemlos in einer oder mehreren dieser Umgebungen einzurichten.
- Stimmen Sie Tags in Netzwerk- und Speicherressourcen so aufeinander ab, dass sie hinsichtlich der Netzwerk- und Speicherprofile, in denen sie verwendet werden, logisch und nachvollziehbar sind. Mithilfe der Ressourcen-Tags kann die Ressourcenbereitstellung präziser gesteuert werden.
- Stimmen Sie Funktions-Tags für Cloud-Zonen und Netzwerkprofile sowie andere Funktions-Tags auf Einschränkungs-Tags ab. Im Allgemeinen erstellt Ihr Administrator zuerst Funktions-Tags für Cloud-Zonen und Netzwerkprofile. Anschließend können andere Benutzer Entwürfe mit Einschränkungen erstellen, die diesen Funktions-Tags entsprechen.

Nachdem Sie die wichtigsten Überlegungen für Ihr Unternehmen zusammengefasst haben, können Sie geeignete Tag-Namen erstellen, die diese Überlegungen in logischer Weise widerspiegeln. Erstellen Sie dann eine Übersicht über Ihre Strategie und stellen Sie sie allen Benutzern mit Berechtigungen zum Erstellen oder Bearbeiten von Tags zur Verfügung.

Ein sinnvoller Implementierungsansatz besteht darin, alle Computing-Infrastrukturressourcen einzeln mit Tags zu versehen. Verwenden Sie logische Kategorien für Tag-Namen, die sich auf die jeweilige Ressource beziehen. Sie können Speicherressourcen beispielsweise als Tier1, Tier2 usw. kennzeichnen. Sie können Computing-Ressourcen auch basierend auf dem Betriebssystem kennzeichnen, wie z. B. Windows, Linux usw.

Nach dem Taggen der Ressourcen können Sie sich eine Methode zum Erstellen von Tags für Cloud-Zonen sowie für Speicher- und Netzwerkprofile überlegen, die Ihren Anforderungen entspricht.

Verwenden von Funktions-Tags in vRealize Automation Cloud Assembly

In vRealize Automation Cloud Assembly können Sie mit Funktions-Tags Bereitstellungsfunktionen für Infrastrukturkomponenten definieren. Zusammen mit Einschränkungen fungieren Sie als Grundlage für die Platzierungslogik in vRealize Automation.

Sie können Funktions-Tags für Computing-Ressourcen, Cloud-Zonen, Images und Image-Zuordnungen sowie für Netzwerke und Netzwerkprofile erstellen. Die Seiten zum Erstellen dieser Ressourcen enthalten Optionen zum Erstellen von Funktions-Tags. Alternativ können Sie die Seite „Tag-Verwaltung“ in vRealize Automation Cloud Assembly verwenden, um Funktions-Tags zu erstellen. Funktions-Tags in Cloud-Zonen und Netzwerkprofilen wirken sich auf alle Ressourcen in diesen Zonen oder Profilen aus. Funktions-Tags auf Speicher- oder Netzwerkkomponenten wirken sich nur auf die Komponenten aus, auf die sie angewendet werden.

In der Regel können Funktions-Tags Merkmale wie den Speicherort für eine Computing-Ressource, den Adaptertyp für ein Netzwerk oder die Ebene für eine Speicherressource definieren. Sie können auch den Umgebungsstandort oder -typ und andere geschäftliche Aspekte definieren. Sie sollten Ihre Funktions-Tags genauso wie Ihre gesamte Tagging-Strategie für Ihre geschäftlichen Anforderungen logisch organisieren.

vRealize Automation Cloud Assembly gleicht zum Zeitpunkt der Bereitstellung Funktions-Tags von Cloud-Zonen mit Einschränkungen bei Cloud-Vorlagen ab. Daher müssen Sie beim Erstellen und Verwenden von Funktions-Tags verstehen und planen, wie sie entsprechende Cloud-Vorlageneinschränkungen erstellen, damit der Abgleich erwartungsgemäß stattfindet.

Im Abschnitt „Hinzufügen einer Cloud-Zone“ des Themas im [Lernprogramm: Einrichten und Testen einer Multi-Cloud-Infrastruktur und von Bereitstellungen in vRealize Automation Cloud Assembly](#), das in der Dokumentation enthalten ist, wird beispielsweise beschrieben, wie dev- und test-Tags für die Cloud-Zonen „OurCo-AWS-US-East“ und „OurCo AWS-US-West“ erstellt werden. In diesem Lernprogramm wird mit diesen Tags angegeben, dass es sich bei der Zone „OurCo-AWS-US-East“ um eine Entwicklungsumgebung und bei der Zone „OurCo AWS-US-West“ um eine Testumgebung handelt. Wenn Sie analoge Einschränkungs-Tags in Cloud-Vorlagen erstellen, können Sie mithilfe dieser Funktions-Tags Bereitstellungen an gewünschte Umgebungen weiterleiten.

Verwenden von Einschränkungs-Tags in vRealize Automation Cloud Assembly

Tags, die zu Projekten und Cloud-Vorlagen hinzugefügt werden, fungieren als Einschränkungs-Tags, wenn sie verwendet werden, um Funktions-Tags für Infrastrukturressourcen, Profile und Cloud-Zonen abzugleichen. Bei Cloud-Vorlagen nutzt vRealize Automation Cloud Assembly die Abgleichfunktion, um Ressourcen für Bereitstellungen zuzuteilen.

vRealize Automation Cloud Assembly bietet Ihnen die Möglichkeit, Einschränkungs-Tags auf zwei primäre Arten zu verwenden. Bei der ersten Möglichkeit werden Einschränkungen beim Konfigurieren von Projekten und Images angewendet. Sie können Tags als Einschränkungen verwenden, um Ressourcen mit dem Projekt oder dem Image zu verknüpfen. Bei der zweiten Möglichkeit werden in Cloud-Vorlagen, in denen Tags als Einschränkungen angegeben werden, diese zur Auswahl von Ressourcen für Bereitstellungen verwendet. Die auf diese beiden Arten angewendeten Einschränkungen werden in Cloud-Vorlagen zu einem Satz von Bereitstellungsanforderungen zusammengeführt, die die für eine Bereitstellung verfügbaren Ressourcen definieren.

Funktionsweise von Einschränkungs-Tags in Projekten

Bei der Konfiguration von vRealize Automation Cloud Assembly-Ressourcen können Cloud-Administratoren Einschränkungs-Tags auf Projekte anwenden. Auf diese Weise können Administratoren Kontrolleinschränkungen direkt auf Projektebene anwenden. Alle auf dieser Ebene hinzugefügten Einschränkungen werden auf jede für das betreffende Projekt angeforderte Cloud-Vorlage angewendet. Diese Einschränkungs-Tags haben Vorrang vor anderen Tags.

Wenn Einschränkungs-Tags im Projekt mit Einschränkungs-Tags in der Cloud-Vorlage in Konflikt stehen, haben die Projekt-Tags Vorrang, sodass der Cloud-Administrator Verwaltungsregeln erzwingen kann. Wenn beispielsweise die Cloud-Administratoren ein `location:london`-Tag für das Projekt erstellen, aber ein Entwickler ein `location:boston`-Tag auf der Cloud-Vorlage platziert, hat das erste Tag Vorrang und die Ressource wird in der Infrastruktur bereitgestellt, die das `location:london`-Tag enthält.

Sie können bis zu drei Einschränkungen für Projekte anwenden. Projekteinschränkungen können hart oder weich sein. Standardmäßig sind sie hart. Harte Einschränkungen ermöglichen es Ihnen, Bereitstellungseinschränkungen strikt durchzusetzen. Wenn eine oder mehrere harte Einschränkungen nicht erfüllt werden, schlägt die Bereitstellung fehl. Weiche Einschränkungen bieten eine Möglichkeit zum Ausdrücken von Einstellungen, die bei Verfügbarkeit ausgewählt werden. Die Bereitstellung schlägt jedoch nicht fehl, wenn weiche Einschränkungen nicht erfüllt werden.

Funktionsweise von Einschränkungs-Tags in Cloud-Vorlagen

In Cloud-Vorlagen fügen Sie Einschränkungs-Tags zu Ressourcen als YAML-Code hinzu, um die entsprechenden Funktions-Tags zu erfüllen, die Ihr Cloud-Administrator für Ressourcen, Cloud-Zonen und für Speicher- und Netzwerkprofile erstellt hat. Darüber hinaus gibt es weitere komplexere Optionen für die Implementierung von Einschränkungs-Tags. Sie können beispielsweise eine Variable verwenden, um ein oder mehrere Tags für eine Anforderung aufzufüllen. Auf diese Weise können Sie einen oder mehrere Tags zur Anforderungszeit angeben.

Erstellen Sie Einschränkungs-Tags mithilfe der `tag`-Bezeichnung unter einer Einschränkungsüberschrift im YAML-Code für die Cloud-Vorlage. Einschränkungs-Tags aus Projekten werden den in Cloud-Vorlagen erstellten Einschränkungs-Tags hinzugefügt.

vRealize Automation Cloud Assembly unterstützt eine einfache Zeichenfolgenformatierung, um die Verwendung von Einschränkungen in YAML-Dateien zu vereinfachen:

```
[!tag_key[:tag_value][:hard|soft]
```

Standardmäßig erstellt vRealize Automation Cloud Assembly eine positive Einschränkung mit harter Erzwingung. Der Tag-Wert ist optional, wird aber wie im Rest der Anwendung empfohlen.

Das folgende WordPress-mit-MySQL-Beispiel zeigt YAML-Einschränkungs-Tags, die bestimmte Standortinformationen für Computing-Ressourcen aufweisen.

```
name: "wordpressWithMySQL"
components:
  mysql:
    type: "Compute"
    data:
      name: "mysql"
      # ... skipped lines ...
  wordpress:
    type: "Compute"
    data:
      name: "wordpress"
```

```
instanceType: small
imageType: "ubuntu-server-1604"
constraints:
  - tag: "!location:eu:hard"
  - tag: "location:us:soft"
  - tag: "!pci"
# ... skipped lines ...
```

Weitere Informationen zum Arbeiten mit Cloud-Vorlagen finden Sie unter [Teil 3: Entwerfen und Bereitstellen der vRealize Automation Cloud Assembly-Beispielvorlage](#).

Funktionsweise von harten und weichen Einschränkungen in Projekten und Cloud-Vorlagen

Einschränkungen in Projekten und Cloud-Vorlagen können hart oder weich sein. Der vorangehende Codeausschnitt zeigt Beispiele für harte und weiche Einschränkungen. Standardmäßig sind alle Einschränkungen hart. Harte Einschränkungen ermöglichen es Ihnen, Bereitstellungseinschränkungen strikt durchzusetzen. Wenn eine oder mehrere harte Einschränkungen nicht erfüllt werden, schlägt die Bereitstellung fehl. Weiche Einschränkungen drücken Einstellungen aus, die gelten, wenn sie verfügbar sind. Wenn sie nicht erfüllt werden, führt dies jedoch nicht dazu, dass eine Bereitstellung fehlschlägt.

Wenn Sie über eine Reihe von harten und weichen Einschränkungen für einen bestimmten Ressourcentyp verfügen, können die weichen Einschränkungen auch als Trennung dienen. Das heißt, wenn mehrere Ressourcen eine harte Einschränkung erfüllen, werden die weichen Einschränkungen verwendet, um die tatsächlich in der Bereitstellung verwendete Ressource auszuwählen.

Sie können beispielsweise bis zu drei Einschränkungen für ein Projekt in einer beliebigen Kombination aus Netzwerk-, Speicher- und Erweiterbarkeitselementen angeben. Darüber hinaus können Sie für jede Einschränkung auswählen, ob sie hart oder weich ist. Angenommen, Sie erstellen eine Einschränkung des Festplattenspeichers mit einem `location:boston`-Tag. Wenn kein Speicher im Projekt mit dieser Einschränkung übereinstimmt, schlagen alle zugehörigen Bereitstellungen fehl.

Standard-Tags

vRealize Automation Cloud Assembly wendet Standard-Tags auf bestimmte Bereitstellungen an, um die Analyse, Überwachung und Gruppierung von bereitgestellten Ressourcen zu unterstützen.

Standard-Tags sind in vRealize Automation Cloud Assembly eindeutig. Im Gegensatz zu anderen Tags werden diese während der Bereitstellungskonfiguration nicht von Benutzern verwendet und es gelten keine Einschränkungen. Diese Tags werden automatisch während der Bereitstellung auf AWS-, Azure- und vSphere-Bereitstellungen angewendet. Diese Tags werden als benutzerdefinierte Systemeigenschaften gespeichert und den Bereitstellungen nach dem Bereitstellen hinzugefügt.

Die Liste der Standard-Tags wird im Folgenden angezeigt.

Tabelle 4-1. Standard-Tags

Beschreibung	Tag
Organisation	org:orgID
Projekt	project:projectID
Anforderer	requester:username
Bereitstellung	deployment:deploymentID
Referenz für die Cloud-Vorlage (falls zutreffen)	blueprint:blueprintID
Komponentenname in Blueprint	blueprintResourceName:CloudMachine_1
Platzierungseinschränkungen: in Blueprint, Anforderungsparametern oder über IT-Richtlinie angewendet	constraints:key:value:soft
Cloud-Konto	cloudAccount:accountID
Zone oder Profil (falls zutreffend)	zone:zoneID, networkProfile:profileID, storageProfile:profileID

Tag-Verarbeitung in vRealize Automation Cloud Assembly

In vRealize Automation Cloud Assembly drücken Tags Funktionen und Beschränkungen aus, die darüber bestimmen, wie und wo Ressourcen Bereitstellungen während des Bereitstellungsprozesses zugeteilt werden.

vRealize Automation Cloud Assembly verwendet eine bestimmte Reihenfolge und Hierarchie der Vorgänge bei der Auflösung von Tags zum Erstellen von Bereitstellungen. Wenn Sie die Grundlagen dieses Prozesses verstehen, können Sie Tags effizient einsetzen, um berechenbare Bereitstellungen zu erstellen.

Die folgende Liste umfasst die allgemeinen Vorgänge und die Abfolge, die Cloud Assembly zur Auflösung von Tags und Definition einer Bereitstellung verwendet:

- Cloud-Zonen werden nach diversen Kriterien wie Verfügbarkeit und Profilen gefiltert. An dieser Stelle werden Tags in Profilen für die Region, zu der die Zone gehört, abgeglichen.
- Zonen- und Computing-Funktions-Tags dienen zum Filtern der übrigen Cloud-Zonen nach harten Einschränkungen.
- Aus den gefilterten Zonen wird eine Cloud-Zone anhand der Priorität ausgewählt. Wenn mehrere Cloud-Zonen mit der gleichen Priorität vorhanden sind, werden diese durch Abgleich von weichen Beschränkungen sortiert. Dabei wird eine Kombination aus Cloud-Zonen- und Computing-Funktionen angewendet.
- Nach der Auswahl einer Cloud-Zone wird ein Host ausgewählt. Dies geschieht durch Abgleich einer Reihe von Filtern, darunter auch harte und weiche Einschränkungen, wie in Cloud-Vorlagen ausgedrückt.

Vorgehensweise zum Einrichten einer einfachen Tagging-Struktur

Unter diesem Thema werden grundlegende Vorgehensweisen und Optionen für die logische Tagging-Strategie in vRealize Automation Cloud Assembly beschrieben. Sie können diese Beispiele als Ausgangsbasis für eine reale Bereitstellung verwenden, oder Sie können eine andere Strategie verfolgen, die besser auf Ihre Anforderungen zugeschnitten ist.

Der Cloud-Administrator ist in der Regel der Hauptverantwortliche für das Erstellen und Pflegen von Tags.

Dieses Thema bezieht sich auf das an anderer Stelle in der vRealize Automation Cloud Assembly-Dokumentation beschriebene WordPress-Anwendungsbeispiel, bei dem veranschaulicht wird, wie Tags zu einigen wesentlichen Elementen hinzugefügt werden können. Außerdem werden mögliche Alternativen und Erweiterungen für die Tagging-Beispiele aus dem WordPress-Anwendungsbeispiel beschrieben.

Weitere Informationen zum WordPress-Anwendungsbeispiel finden Sie unter [Lernprogramm: Einrichten und Testen einer Multi-Cloud-Infrastruktur und von Bereitstellungen in vRealize Automation Cloud Assembly](#).

Im WordPress-Anwendungsbeispiel wird beschrieben, wie Tags in Cloud-Zonen und Speicher- und Netzwerkprofilen platziert werden. Diese Profile sind ähnlich wie organisierte Ressourcenpakete. In Profilen platzierte Tags gelten für alle Elemente im Profil. Sie können Tags auch bei Speicherressourcen und einzelnen Netzwerkelementen sowie bei Computing-Ressourcen platzieren. Diese Tags gelten jedoch nur für die spezifischen Ressourcen, bei denen sie platziert werden. Beim Einrichten von Tags ist es in der Regel das Beste, mit dem Taggen der Computing-Ressourcen zu beginnen. Anschließend können Sie dann Tags zu Profilen und Cloud-Zonen hinzufügen. Mithilfe dieser Tags können Sie auch die Liste der Computing-Ressourcen für eine Cloud-Zone filtern.

Sie können z. B. Tags in Speicherprofilen wie in diesem Anwendungsbeispiel dargestellt platzieren. Sie haben aber auch die Möglichkeit, Tags in einzelnen Speicherrichtlinien, Datenspeichern und Speicherkonten zu platzieren. Mit Tags in diesen Ressourcen können Sie genauer steuern, wie die Speicherressourcen bereitgestellt werden. Während der Verarbeitung zur Vorbereitung für die Bereitstellung werden diese Tags als nächste Verarbeitungsebene nach den Profil-Tags aufgelöst.

Als Beispiel dafür, wie Sie ein typisches Kundenszenario konfigurieren könnten, könnten Sie ein Tag von `region: eastern` auf einem Netzwerkprofil platzieren. Dieses Tag würde dann für alle Ressourcen in diesem Profil gelten. Anschließend können Sie ein Tag von `networktype:pci` auf einer PCI-Netzwerkressource innerhalb dieses Profils platzieren. Eine Cloud-Vorlage mit den Einschränkungen „eastern“ und „pci“ würde Bereitstellungen erstellen, die dieses PCI-Netzwerk für die Region „East“ verwenden.

Verfahren

1 Taggen Sie Ihre Computing-Infrastrukturressourcen in logischer und angemessener Weise.

Es ist besonders wichtig, dass Sie Computing-Ressourcen in logischer Weise taggen, sodass Sie sie mit der Suchfunktion auf der Registerkarte „Computing“ der Seite „Cloud-Zone erstellen“ finden können. Mithilfe dieser Suchfunktion können Sie die Computing-Ressourcen, die mit einer Cloud-Zone verknüpft sind, schnell filtern. Wenn Sie Speicher und Netzwerke auf der Profilebene taggen, brauchen Sie die einzelnen Speicher- und Netzwerkressourcen unter Umständen nicht mehr zu taggen.

- a Wählen Sie **Ressourcen > Computing** aus, um die Computing-Ressourcen anzuzeigen, die für Ihre vRealize Automation Cloud Assembly-Instanz importiert wurden.
- b Wählen Sie die einzelnen Computing-Ressourcen nach Bedarf aus und klicken Sie auf **Tags**, um ein Tag zur Ressource hinzuzufügen. Sie können jeder Ressource bei Bedarf mehrere Tags hinzufügen.
- c Wiederholen Sie den vorherigen Schritt je nach Bedarf für Speicher- und Netzwerkressourcen.

2 Erstellen Sie Funktions-Tags für Cloud-Zonen und Netzwerkprofile.

Sie können dieselben Tags für Cloud-Zonen und Netzwerkprofile verwenden. Stattdessen können Sie aber auch eindeutige Tags für jedes Objekt erstellen, wenn Ihnen das für Ihre Implementierung sinnvoller erscheint.

In Netzwerkprofilen können Sie Tags auf dem gesamten Profil platzieren. Dasselbe gilt auch für Subnetze innerhalb des Profils. Auf der Profilebene angewendete Tags gelten für alle Komponenten innerhalb des Profils, z. B. für Subnetze. Tags in Subnetzen gelten nur für das spezifische Subnetz, in dem sie platziert wurden. Bei der Tag-Verarbeitung haben die Tags der Profilebene Vorrang gegenüber den Tags der Subnetzebene.

In diesem Beispiel erstellen wir drei einfache Tags, die in der gesamten Dokumentation des Anwendungsbeispiels für vRealize Automation Cloud Assembly-Cloud-Zone- und Netzwerkprofil-Tags erscheinen. Diese Tags identifizieren die Umgebung für die Profilkomponenten.

- `zone:test`
- `zone:dev`
- `zone:prod`

3 Erstellen Sie Speicherprofil-Tags für Ihre Speicherkomponenten.

In der Regel bezeichnen Speicher-Tags die Leistungsstufe von Speicherelementen, z. B. tier1 oder tier2, oder sie bezeichnen die Art der Speicherelemente, z. B. pci.

Weitere Informationen zum Hinzufügen von Tags zu Speicherprofilen finden Sie unter [6 . Hinzufügen von Speicherprofilen](#).

- `usage:general`

- `usage:fast`

Ergebnisse

Nachdem Sie eine grundlegende Tagging-Struktur erstellt haben, können Sie damit beginnen, mit ihr zu arbeiten, und Tags entsprechend hinzufügen oder bearbeiten, um Ihre Tagging-Funktionen zu verfeinern und zu erweitern.

Vorgehensweise zum Arbeiten mit Ressourcen in vRealize Automation

Ein Cloud-Administrator kann vRealize Automation-Ressourcen überprüfen, die über die Datenerfassung offengelegt werden.

Der Cloud-Administrator kann Ressourcen mit Funktions-Tags kennzeichnen, um den Bereitstellungsort von vRealize Automation-Cloud-Vorlagen festzulegen.

Computing-Ressourcen in vRealize Automation

Ein Cloud-Administrator kann Computing-Ressourcen überprüfen, die über die Datenerfassung angezeigt werden.

Der Cloud-Administrator kann Tags direkt auf die Ressourcen anwenden, um Funktionen zu Abgleichszwecken in der vRealize Automation-Bereitstellung zu kennzeichnen.

Netzwerkressourcen in vRealize Automation

In vRealize Automation können Cloud-Administratoren die Netzwerkressourcen anzeigen und bearbeiten, deren Daten aus den Cloud-Konten und Integrationen erfasst wurden, die dem Projekt zugeordnet sind.

Nachdem Sie ein Cloud-Konto zu Ihrer vRealize Automation Cloud Assembly-Infrastruktur hinzugefügt haben, beispielsweise mithilfe der Menüabfolge **Infrastruktur > Verbindungen > Cloud-Konten**, erkennt die Datenerfassung die Netzwerk- und Sicherheitsinformationen des Cloud-Kontos.. Diese Informationen stehen dann zur Verwendung in Netzwerken, Netzwerkprofilen und anderen Definitionen zur Verfügung.

Netzwerke sind die IP-spezifischen Komponenten einer verfügbaren Netzwerktopologie oder Transportzone. Stellen Sie sich als Amazon Web Services- oder Microsoft Azure-Benutzer Netzwerke wie Subnetze vor.

Sie können Informationen zu den Netzwerken in Ihrem Projekt anzeigen, indem Sie die Seite **Infrastruktur > Ressourcen > Netzwerke** verwenden.

Die vRealize Automation Cloud Assembly-Seite **Netzwerke** enthält Informationen, wie z. B.:

- Netzwerke und Lastausgleichsdienste, die extern in der Netzwerktopologie Ihres Cloud-Kontos definiert sind, zum Beispiel in vCenter, NSX-V oder Amazon Web Services.
- Netzwerke und Lastausgleichsdienste, die vom Cloud-Administrator bereitgestellt wurden.

- IP-Bereiche und andere Netzwerkmerkmale, die von Ihrem Cloud-Administrator definiert oder geändert wurden.
- IP-Bereiche des externen IPAM-Anbieters für einen bestimmten Adressraum in einer anbieterspezifischen externen IPAM-Integration.

Weitere Informationen zu Netzwerken finden Sie in der Wegweiser-Hilfe für verschiedene Einstellungen auf der Seite **Netzwerke** und unter [Weitere Informationen zu Netzwerkprofilen in vRealize Automation](#).

Netzwerke

Sie können Netzwerke und deren Eigenschaften anzeigen und bearbeiten, zum Beispiel zum Hinzufügen von Tags oder zum Entfernen der Unterstützung für den öffentlichen IP-Zugriff. Sie können auch Netzwerkeinstellungen verwalten, wie z. B. DNS-, CIDR-, Gateway- und Tag-Werte. Sie können auch neue IP-Bereiche definieren und vorhandene IP-Bereiche in einem Netzwerk verwalten.

Für vorhandene Netzwerke können Sie den IP-Bereich und die Tag-Einstellungen ändern, indem Sie das Kontrollkästchen des Netzwerks aktivieren und entweder **IP-Bereiche verwalten** oder **Tags** auswählen. Andernfalls können Sie das Netzwerk selbst auswählen, um die jeweiligen Informationen zu bearbeiten.

Tags bieten eine Möglichkeit zum Abgleich von geeigneten Netzwerken, optional auch von Netzwerkprofilen, mit Netzwerkkomponenten in Cloud-Vorlagen. Netzwerk-Tags werden unabhängig von den Netzwerkprofilen, in denen sich das Netzwerk befinden kann, auf jede Instanz dieses Netzwerks angewendet. Netzwerke können in beliebig viele Netzwerkprofile eingeteilt werden. Unabhängig davon, wo sich das Netzwerkprofil befindet, ist ein Netzwerk-Tag mit diesem Netzwerk verknüpft, wenn das Netzwerk verwendet wird. Der Netzwerk-Tag-Abgleich erfolgt mit anderen Komponenten in der Cloud-Vorlage, nachdem die Cloud-Vorlage mit einem oder mehreren Netzwerkprofilen abgeglichen wurde.

IP-Bereiche

Verwenden Sie einen IP-Bereich, um die Start- und End-IP-Adresse für ein bestimmtes Netzwerk in Ihrer Organisation zu definieren oder Änderungen daran vorzunehmen. Sie können IP-Bereiche für aufgelistete Netzwerke anzeigen und verwalten. Wenn das Netzwerk von einem externen IPAM-Anbieter verwaltet wird, können Sie die IP-Bereiche gemeinsam mit dem zugehörigen IPAM-Integrationspunkt verwalten.

Klicken Sie auf **Neuer IP-Bereich**, um dem Netzwerk einen zusätzlichen IP-Bereich hinzuzufügen. Sie können einen **internen IP-Bereich** angeben. Wenn eine gültige IPAM-Integration vorhanden ist, können Sie auch einen **externen IP-Bereich** angeben.

Sie können das Standard-Gateway nicht in einen IP-Bereich aufnehmen. Der Subnetz-IP-Bereich kann nicht den Wert des Subnetz-Gateways enthalten.

Wenn Sie eine externe IPAM-Integration für einen bestimmten IPAM-Anbieter verwenden, können Sie den **externen IP-Bereich** zum Auswählen eines IP-Bereichs aus einem verfügbaren externen IPAM-Integrationspunkt verwenden. Dieser Vorgang wird im Kontext eines allgemeinen Workflows für die externe IPAM-Integration unter [Konfigurieren eines Netzwerks und Netzwerkprofils zur Verwendung von IPAM \(extern\) für ein vorhandenes Netzwerk in vRealize Automation](#) beschrieben.

IP-Adressen

Sie können die aktuell von Ihrer Organisation verwendeten IP-Adressen und deren Status anzeigen, wie z. B. `available` oder `allocated`. Bei den angezeigten IP-Adressen handelt es sich entweder um IP-Adressen, die intern von vRealize Automation verwaltet werden, oder um IP-Adressen, die für Bereitstellungen bestimmt sind, die eine Integration des externen IPAM-Anbieters enthalten. Externe IPAM-Anbieter verwalten ihre eigene IP-Adresszuweisung.

Wenn das Netzwerk intern von vRealize Automation und nicht von einem externen IPAM-Anbieter verwaltet wird, können Sie IP-Adressen auch freigeben.

Wenn Sie die interne IPAM verwenden und IP-Adressen freigeben (z. B. nach dem Löschen einer Maschine, die die IP-Adressen verwendet hat), entsteht ein 30-minütiger Wartezeitraum zwischen der Freigabe der Adressen und dem Zeitpunkt, ab dem sie wiederverwendet werden können. Der Wartezeitraum ermöglicht das Löschen des DNS-Caches. Die IP-Adressen können dann einer neuen Maschine zugeteilt werden. Sie können dann beispielsweise eine Maschine mit denselben IP-Adressen wie die zuvor gelöschte Maschine bereitstellen.

Lastausgleichsdienste

Sie können Informationen zu den verfügbaren Lastausgleichsdiensten für die Cloud-Konten des Kontos/der Region in Ihrer Organisation verwalten. Sie können die konfigurierten Einstellungen für jeden verfügbaren Lastausgleichsdienst öffnen und anzeigen. Sie können auch Tags für einen Lastausgleichsdienst hinzufügen und entfernen.

Netzwerkdomänen

Die Netzwerkdomänenliste enthält zugehörige und nicht überlappende Netzwerke.

Sicherheitsressourcen in vRealize Automation

Nachdem Sie ein Cloud-Konto in vRealize Automation Cloud Assembly hinzugefügt haben, erkennt die Datenerfassung die Netzwerk- und Sicherheitsinformationen des Cloud-Kontos und stellt diese Informationen zur Verwendung in Netzwerkprofilen und für andere Optionen bereit.

Sicherheitsgruppen und Firewallregeln unterstützen die Netzwerkisolierung. Sicherheitsgruppen basieren auf erfassten Daten. Firewallregeln basieren nicht auf erfassten Daten.

Sicherheitsgruppen

Mithilfe der Menüabfolge **Infrastruktur > Ressourcen > Sicherheit** können Sie in vRealize Automation Cloud Assembly-Cloud-Vorlagendesigns erstellte bedarfsgesteuerte Sicherheitsgruppen und vorhandene in Quellenwendungen erstellte Sicherheitsgruppen anzeigen, wie z. B. NSX-T und Amazon Web Services. Verfügbare Sicherheitsgruppen werden mithilfe des Datenerfassungsprozesses angezeigt.

Sie können die verfügbaren Sicherheitsgruppen anzeigen und Tags für ausgewählte Sicherheitsgruppen hinzufügen oder entfernen. Ein Cloud-Vorlagen-Autor kann einer Maschinen-Netzwerkkarte eine oder mehrere Sicherheitsgruppen zuweisen, um die Sicherheit für die Bereitstellung zu steuern.

Im Cloud-Vorlagendesign wird der Parameter `securityGroupType` in der Sicherheitsgruppenressource als `existing` für eine vorhandene Sicherheitsgruppe oder als `new` für eine bedarfsgesteuerte Sicherheitsgruppe angegeben.

Vorhandene Sicherheitsgruppen aus dem zugrunde liegenden Cloud-Konto-Endpoint, z. B. NSX-V-, NSX-T- oder Amazon Web Services-Anwendungen, stehen zur Verwendung bereit. Für bedarfsgesteuerte Sicherheitsgruppen, die in Cloud-Vorlagendesigns Ihrer Organisation erstellt wurden, werden ebenfalls Daten erfasst. Bedarfsgesteuerte Sicherheitsgruppen sind zurzeit nur für NSX-V und NSX-T verfügbar.

Vorhandene Sicherheitsgruppen werden in der Spalte **Ursprung** als `Discovered` angezeigt und klassifiziert. Bedarfsgesteuerte Sicherheitsgruppen, die Sie in vRealize Automation Cloud Assembly entweder in einer Cloud-Vorlage oder in einem Netzwerkprofil erstellen, werden in der Spalte **Ursprung** als `Managed by Cloud Assembly` angezeigt und klassifiziert. Bedarfsgesteuerte Sicherheitsgruppen, die Sie als Teil eines Netzwerkprofils erstellen, werden intern als eine Isolationssicherheitsgruppe mit vorkonfigurierten Firewallregeln eingestuft und nicht zu Cloud-Vorlagendesign als Sicherheitsgruppenressource hinzugefügt. Bedarfsgesteuerte Sicherheitsgruppen, die Sie in Cloud-Vorlagendesign erstellen und die ausdrückliche Firewallregeln enthalten können, werden als Teil einer Sicherheitsgruppenressource hinzugefügt, die als `new` eingestuft wird.

Wenn Sie eine vorhandene Sicherheitsgruppe direkt in der Quellenwendung (beispielsweise in der NSX-Quellenwendung) anstatt in vRealize Automation Cloud Assembly bearbeiten, werden die Updates in vRealize Automation Cloud Assembly erst dann angezeigt, wenn die Datenerfassung ausgeführt und Daten im zugehörigen Cloud-Konto oder Integrationspunkt innerhalb von vRealize Automation Cloud Assembly erfasst werden. Die Datenerfassung wird automatisch alle 10 Minuten durchgeführt.

Ein Cloud-Administrator kann einer vorhandenen Sicherheitsgruppe ein oder mehrere Tags zuweisen, damit diese in einer Cloud-Vorlage verwendet werden kann. Ein Cloud-Vorlagen-Autor kann eine `Cloud.SecurityGroup`-Ressource in einem Cloud-Vorlagendesign verwenden, um eine vorhandene Sicherheitsgruppe mithilfe von Tag-Einschränkungen zuzuteilen. Eine vorhandene Sicherheitsgruppe erfordert die Angabe mindestens eines Einschränkungstags in der Sicherheitsressource im Cloud-Vorlagendesign.

Verwenden von Firewallregeln in Sicherheitsgruppen

Sie können Firewallregeln für bedarfsgesteuerte Sicherheitsgruppen für NSX-V und NSX-T direkt in einer Sicherheitsgruppenressource im Code des Cloud-Vorlagendesigns erstellen.

Die Spalte **Angewendet auf** enthält keine Sicherheitsgruppen, die von einer verteilten NSX-Firewall (Distributed Firewall, DFW) klassifiziert oder verwaltet werden. Die für die Anwendungen geltenden Firewallregeln gelten für den Ost/West-DFW-Datenverkehr.

Einige Firewallregeln können nur in der Quellanwendung verwaltet und nicht in vRealize Automation Cloud Assembly bearbeitet werden. Beispielsweise werden Ethernet-, Notfall-, Infrastruktur- und Umgebungsregeln in NSX-T verwaltet.

Weitere Informationen

Weitere Informationen zur Verwendung von Sicherheitsgruppen in Netzwerkprofilen finden Sie unter [Weitere Informationen zu Netzwerkprofilen in vRealize Automation](#).

Informationen zum Definieren von Firewallregeln finden Sie unter [Verwenden von Sicherheitsgruppeneinstellungen in Netzwerkprofilen und Cloud-Vorlagendesigns in vRealize Automation Cloud Assembly](#) und [Verwenden einer Sicherheitsgruppenressource in einer vRealize Automation-Cloud-Vorlage](#).

Codebeispiele für das Cloud-Vorlagendesign, die Sicherheitsgruppen enthalten, finden Sie unter [Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen](#).

Speicherressourcen in vRealize Automation

Ein Cloud-Administrator kann mit Speicherressourcen und deren Funktionen arbeiten, die über die vRealize Automation-Datenerfassung aus verknüpften Cloud-Konten ermittelt werden.

Speicherressourcen-Funktionen werden über Tags offengelegt, die in der Regel vom Quell-Cloud-Konto stammen. Ein Cloud-Administrator kann jedoch mithilfe von vRealize Automation Cloud Assembly zusätzliche Tags direkt auf Speicherressourcen anwenden. Die zusätzlichen Tags können eine bestimmte Funktion für den Abgleich zum Zeitpunkt der Bereitstellung kennzeichnen.

vRealize Automation unterstützt Standardfestplatten- und FCD-Funktionen (First Class Disk). First Class Disk ist nur für vSphere verfügbar.

- [Wozu dient Standardfestplattenspeicher in vRealize Automation?](#)
- [Wozu dient First Class Disk-Speicher in vRealize Automation?](#)

Die Funktionen für Speicherressourcen werden im Rahmen der Definition eines vRealize Automation Cloud Assembly-Speicherprofils angezeigt. Weitere Informationen hierzu finden Sie unter [Weitere Informationen zu Speicherprofilen in vRealize Automation](#).

First Class Disks, deren Daten erfasst wurden, werden auf der Ressourcenseite **Volumes** angezeigt. Weitere Informationen hierzu finden Sie unter [Volume-Ressourcen in vRealize Automation](#).

Maschinenressourcen in vRealize Automation

In vRealize Automation können alle Benutzer Maschinenressourcen überprüfen, die über die Datenerfassung offen gelegt werden.

Alle Maschinen in Ihren Projekten werden aufgelistet. Sie können nur Ihre Maschinen auflisten oder Filter angeben, um die Anzeige der aufgelisteten Maschinen zu steuern.

Nicht verwaltete Maschinen, die Cloud-Konten in Ihren Projekten zugeordnet sind, werden in dieser Liste wie verwaltete Maschinen angezeigt. Die Spalte „Ursprung“ gibt den Maschinenstatus an.

- **Erkannt:** Maschinen, die noch nicht integriert sind.
- **Bereitgestellt –** Maschinen, die über vRealize Automation integriert oder bereitgestellt wurden und als verwaltete Maschinen gelten.

Sie können einen Arbeitslast-Onboarding-Plan verwenden, um nicht verwaltete Maschinen in die vRealize Automation-Verwaltung zu integrieren.

Getrennte Maschinen-Netzwerkkarten werden nicht aufgelistet, da vRealize Automation einen vorhandenen Netzwerk-Switch oder Subnetzinformationen benötigt, um die Ethernet-Karte aufzulisten. Wenn Sie beispielsweise eine Maschinen-Netzwerkkarte aus einer Bereitstellung entfernt haben, wird die Netzwerkkarte nicht aufgelistet.

Informationen zur Verwendung von Onboarding-Plänen zwecks Integration von nicht verwalteten Maschinen in die vRealize Automation-Verwaltung finden Sie unter [Definition von Onboarding-Plänen in vRealize Automation Cloud Assembly](#).

Volume-Ressourcen in vRealize Automation

In vRealize Automation können alle Benutzer die Volume-Ressourcen überprüfen.

vRealize Automation Cloud Assembly zeigt Volumes oder logische Laufwerke an, die aus zwei Quellen stammen:

- Durch die Datenerfassung von Quell-Cloud-Konten erkannte Volumes
- Volumes, die mit von vRealize Automation Cloud Assembly bereitgestellten Arbeitslasten verknüpft sind

Sie können die Kapazität und Funktionen nach Volume oder logischem Laufwerk überprüfen. In der Liste sind auch Funktions-Tags verfügbar, die aus dem Quell-Cloud-Konto stammen oder in vRealize Automation Cloud Assembly selbst hinzugefügt wurden. Der Status des Volumes als First Class Disk wird ebenfalls beachtet. Informationen zu First Class Disk-Speichervolumes finden Sie unter [Wozu dient First Class Disk-Speicher in vRealize Automation?](#).

Weitere Informationen zu Ressourcen in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly kann zusätzliche Informationen zu Ressourcen mit erfassten Daten bereitstellen, wie z. B. Preisgestaltungskarten.

Funktionsweise der Datenerfassung in vRealize Automation

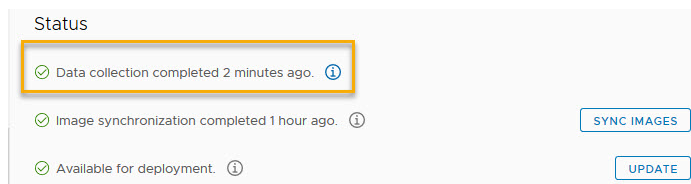
Nach der anfänglichen Datenerfassung erfolgt die Erfassung von Ressourcendaten automatisch alle 10 Minuten. Das Datenerfassungsintervall ist nicht konfigurierbar, und Sie können die Datenerfassung nicht manuell einleiten.

Sie können Informationen zur Erfassung von Ressourcendaten und zur Image-Synchronisierung für ein vorhandenes Cloud-Konto auf dessen Seite im Abschnitt „Status“ ermitteln. Wählen Sie hierzu **Infrastruktur > Verbindungen > Cloud-Konten** und klicken Sie dann auf **Öffnen** in einem beliebigen vorhandenen Cloud-Konto.

Sie können ein bestehendes Cloud-Konto öffnen und dessen verknüpfte Endpoint-Version im Abschnitt **Status** der zugehörigen Seite anzeigen. Wenn der zugeordnete Endpoint aktualisiert wurde, wird die neue Endpoint-Version während der Datenerfassung erkannt und im Abschnitt **Status** auf der Seite des Cloud-Kontos angezeigt.

Erfassen von Ressourcendaten

Die Datenerfassung erfolgt alle 10 Minuten. Jedes Cloud-Konto zeigt an, wann die Datenerfassung zuletzt abgeschlossen wurde.

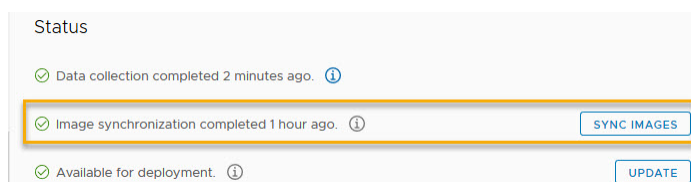


Erfassen von Image-Daten

Die Image-Synchronisierung erfolgt alle 24 Stunden. Sie können die Image-Synchronisierung für einige Cloud-Kontotypen einleiten. Um die Image-Synchronisierung einzuleiten, öffnen Sie das Cloud-Konto (**Infrastruktur > Cloud-Konten**, wählen Sie dann das gewünschte Cloud-Konto aus und öffnen Sie es) und klicken Sie auf die Schaltfläche **Images synchronisieren**. Es gibt keine Image-Synchronisierungsoption für NSX-Cloud-Konten.

Hinweis Images werden intern als „öffentlich“ oder „privat“ eingestuft. Öffentliche Images werden gemeinsam genutzt und sind nicht spezifisch für ein bestimmtes Cloud-Abonnement oder eine bestimmte Organisation. Private Images werden nicht gemeinsam genutzt und sind spezifisch für ein bestimmtes Abonnement. Öffentliche und private Images werden alle 24 Stunden automatisch synchronisiert. Eine Option auf der Seite „Cloud-Konto“ ermöglicht es Ihnen, die Synchronisierung für private Images auszulösen.

Auf der Seite „Cloud-Konto“ wird der Zeitpunkt angezeigt, an dem die Image-Synchronisierung abgeschlossen wurde.



Um Fault Tolerance und Hochverfügbarkeit in Bereitstellungen zu vereinfachen, stellt jeder NSX-T-Datencenter-Endpoint ein Cluster aus drei NSX Managern dar. Informationen hierzu finden Sie unter [Erstellen eines NSX-T-Cloud-Kontos in vRealize Automation](#).

Cloud-Konten und Onboarding-Pläne

Wenn Sie ein Cloud-Konto erstellen, werden die Daten aller Maschinen, die diesem Konto zugeordnet sind, erfasst und anschließend auf der Seite **Infrastruktur > Ressourcen > Maschinen** angezeigt. Wenn das Cloud-Konto über Maschinen verfügt, die außerhalb von vRealize Automation Cloud Assembly bereitgestellt wurden, können Sie einen Onboarding-Plan verwenden, der zulässt, dass die Maschinen von vRealize Automation Cloud Assembly verwaltet werden.

Informationen zum Hinzufügen von Cloud-Konten finden Sie unter [Hinzufügen von Cloud-Konten zu vRealize Automation Cloud Assembly](#).

Informationen zum Onboarding von nicht verwalteten Maschinen finden Sie unter [Definition von Onboarding-Plänen in vRealize Automation Cloud Assembly](#).

Wozu dient Standardfestplattenspeicher in vRealize Automation?

Standardfestplatten können persistent oder nicht persistent sein.

vRealize Automation unterstützt zwei Speicherkategorien: Standardfestplatte und First Class Disk. First Class Disk ist nur für vSphere verfügbar.

■ vSphere

vSphere unterstützt abhängige (Standard), unabhängige persistente und unabhängige nicht persistente Standardfestplatten. Informationen hierzu finden Sie unter [Wozu dient dauerhafter Festplattenspeicher in vRealize Automation?](#)

Wenn Sie eine virtuelle Maschine löschen, werden ihre abhängigen und unabhängigen nicht persistenten Festplatten ebenfalls gelöscht.

Wenn Sie eine virtuelle Maschine löschen, werden ihre unabhängigen persistenten Festplatten nicht gelöscht.

Sie können einen Snapshot von abhängigen und unabhängigen nicht persistenten Festplatten erstellen. Es ist nicht möglich, einen Snapshot einer unabhängigen persistenten Festplatte zu erstellen.

■ Amazon Web Services (AWS) EBS

Sie können ein EBS-Volume an eine AWS-Computing-Instanz anhängen oder davon trennen.

Wenn Sie eine virtuelle Maschine löschen, wird ihr angehängtes EBS-Volume getrennt, aber nicht gelöscht.

■ Microsoft Azure-VHD

Angehängte Festplatten sind immer persistent.

Wenn Sie eine virtuelle Maschine löschen, geben Sie an, ob die daran angehängten Speicherfestplatten entfernt werden sollen.

- Google Cloud Platform (GCP)

Angehängte Festplatten sind immer persistent.

Der Speicherort von persistenten Festplatten ist unabhängig von Ihren VM-Instanzen. Das heißt, Sie können persistente Festplatten trennen oder verschieben, um Ihre Daten auch nach dem Löschen Ihrer Instanzen beizubehalten.

Wenn Sie eine virtuelle Maschine löschen, wird ihre angehängte Festplatte getrennt, aber nicht gelöscht.

Informationen hierzu finden Sie unter [Weitere Informationen zu Speicherprofilen in vRealize Automation](#).

Wozu dient First Class Disk-Speicher in vRealize Automation?

Eine First Class Disk (FCD) bietet Speicher-Lebenszyklusverwaltung auf virtuellen Festplatten als „Festplatte als Dienst“ oder als EBS-ähnlicher Festplattenspeicher, mit dem Sie Festplatten unabhängig von vSphere-VMs verwalten können.

vRealize Automation unterstützt zwei Kategorien von Speicherfestplatten: Standardfestplatte und First Class Disk. Die First Class Disk-Funktion wird nur für vSphere unterstützt. vRealize Automation bietet derzeit die First Class Disk-Funktion als reine API-Funktion.

Eine First Class Disk verfügt über ihre eigenen Lebenszyklusverwaltungsfunktionen, die unabhängig von einer VM funktionieren. Ein Aspekt, in dem sich eine First Class Disk von einer unabhängigen persistenten Festplatte unterscheidet, besteht darin, dass Sie eine First Class Disk zum VM-unabhängigen Erstellen und Verwalten von Snapshots verwenden können.

Sie können ein neues vRealize Automation-Speicherprofil erstellen, um entweder First Class Disk- oder Standardfestplattenfunktionen zu unterstützen. Weitere Informationen finden Sie unter [Weitere Informationen zu Speicherprofilen in vRealize Automation](#) und [Speicherressourcen in vRealize Automation](#).

Sie können auch ein First Class Disk-Element des Typs `Cloud.vSphere.Disk` in Ihren vRealize Automation-Cloud-Vorlagen und -Bereitstellungen hinzufügen, um vSphere-First Class Disks zu unterstützen. First Class Disks, deren Daten erfasst wurden, werden auf der Ressourcenseite **Volumes** angezeigt. Weitere Informationen hierzu finden Sie unter [Volume-Ressourcen in vRealize Automation](#).

In vCenter werden First Class Disks auch als *Improved Virtual Disks (IVD)* oder *verwaltete virtuelle Festplatten* bezeichnet.

Funktionen

Mithilfe der API-Funktionen von vRealize Automation können Sie folgende Aktionen ausführen:

- First Class Disk erstellen, auflisten und löschen.
- Größe einer First Class Disk ändern.

- First Class Disk anhängen und trennen.
- First Class Disk-Snapshots erstellen und verwalten.
- Eine vorhandene Standardfestplatte in eine First Class Disk konvertieren,

Zugehörige API-Informationen zum Erstellen und Verwalten von First Class Disk-Speicher (FCD) unter Verwendung der vRealize Automation-API, einschließlich der Vorgehensweise zum Definieren eines Speicherprofils zur Verwendung von First Class Disk-Funktionen finden Sie unter code.vmware.com im Abschnitt [What are the vRealize Automation Cloud APIs and how do I use them](#), oder indem Sie in den folgenden Referenzen navigieren:

- Die API-Dokumentation für FCD ist im Abschnitt [First Class Disk \(FCD\)](#) des [Virtual Disk Development Kit-Programmierhandbuchs](#) verfügbar.
- Links zur Dokumentation zu API-Anwendungsbeispielen für FCD in vRealize Automation finden Sie auf der Seite [Dokumentation zur vRealize Automation-API](#) für Ihre vRealize Automation-Version.

Überlegungen und Einschränkungen

Überlegungen und Einschränkungen zu First Class Disks umfassen derzeit Folgendes:

- First Class Disk ist nur für vSphere-VMs verfügbar.
- vSphere 6,7 Update 2 oder höher ist für die Verwendung von First Class Disks erforderlich.
- Die Bereitstellung von First-Class-Festplatten in Datenspeicher-Clustern wird nicht unterstützt.
- Mehrfachanhängen von Volumes wird für First Class Disks nicht unterstützt.
- Die Größe von First Class Disks mit Snapshots kann nicht geändert werden.
- First Class Disks mit Snapshots können nicht gelöscht werden.
- Die Hierarchie von First Class Disk-Snapshots kann nur unter Verwendung der API-Option `createdAt` erstellt werden.
- Die Mindestversion der VM-Hardware, die zum Anhängen einer First Class Disk erforderlich ist, lautet vmx-13 (ESX 6.5-kompatibel).

Wozu dient dauerhafter Festplattenspeicher in vRealize Automation?

Auf dauerhaften Festplatten werden wichtige Daten vor versehentlichem Löschen geschützt.

In einer Cloud-Vorlage können Sie für ein Volume die Eigenschaft `persistent: true` hinzufügen, um die Festplatte vor vRealize Automation Cloud Assembly- oder vRealize Automation Service Broker-Löschvorgängen zu schützen. Dauerhafte Festplatten werden weder beim Löschen von Bereitstellungen noch während Tag-2-Vorgängen zum Löschen von Festplatten entfernt.

Aus diesem Grund können dauerhafte Festplatten auch nach dem Löschen einer Bereitstellung oder Festplatte in Ihrer Infrastruktur verbleiben. Zum Entfernen dauerhafter Festplatten stehen folgende Methoden zur Verfügung.

- Explizites Übergeben des Lösch-Flags als Abfrageparameter mithilfe der DELETE API.

- Direktes Löschen der dauerhaften Festplatten aus dem Cloud-Endpoint.

Beachten Sie, dass keine vRealize Automation Cloud Assembly- oder vRealize Automation Service Broker-Benutzeroberfläche zum Löschen der dauerhaften Festplatten vorhanden ist.

Definition von Preisgestaltungskarten

Mithilfe von vRealize Automation Cloud Assembly-Preisgestaltungskarten können Cloud-Administratoren die Preisgestaltungsrichtlinie für die finanziellen Auswirkungen einzelner Bereitstellungen definieren und zuweisen und Sie somit bei der Verwaltung von Ressourcen unterstützen.

Vor dem Erstellen oder Zuweisen von Preisgestaltungskarten müssen Sie die Preisgestaltung in vRealize Operations Manager so konfigurieren, dass sie mit vRealize Automation zusammenarbeitet. Stellen Sie beim Konfigurieren von vRealize Operations Manager mit vRealize Automation sicher, dass beide Anwendungen auf dieselbe Zeitzone festgelegt sind. Aktivieren Sie SSH zum Konfigurieren der Zeitzone in vRealize Operations und melden sich bei jedem vRealize Operations Manager-Knoten an, bearbeiten die Datei `$ALIVE_Base/user/conf/analytics/advanced.properties` und fügen `timeZoneUseInMeteringCalculation = <time zone>` hinzu.

Hinweis Damit die Preisgestaltung in Umgebungen mit mehreren Mandanten funktioniert, müssen Sie über eine separate vRealize Operations Manager-Instanz für jeden vRealize Automation -Mandanten verfügen.

Mit Preisgestaltungskarten werden die Tarife für eine Preisgestaltungsrichtlinie definiert. Die Preisgestaltungsrichtlinie kann dann bestimmten Projekten zugewiesen werden, um einen Gesamtpreis festzulegen. Nach dem Erstellen eines vRealize Operations Manager-Endpoints steht eine vordefinierte Standardpreisliste mit einer Kosten-gleich-Preis-Konfiguration auf der Registerkarte **Infrastruktur > Preisgestaltungskarten** zur Verfügung. Sie können Preisgestaltungskarten erstellen, die nur für Projekte oder für Cloud-Zonen gelten. Standardmäßig werden alle neuen Preisgestaltungskarten auf Projekte angewendet.

Hinweis Wenn Sie die Einstellung **Alle Preisgestaltungskarten werden angewendet auf** ändern, werden alle vorhandenen Zuweisungen von Preisgestaltungskarten gelöscht. Wenn der vRealize Operations Manager-Endpoint aus Cloud Assembly gelöscht wird, werden außerdem alle Preisgestaltungskarten und Zuweisungen gelöscht.

Die Kosten einer Bereitstellung im Zeitverlauf werden auf der Bereitstellungskarte als die bisherigen monatlichen Kosten angezeigt, die zu Beginn eines jeden Monats auf null zurückgesetzt werden. Die Aufschlüsselungen der Komponentenkosten sind in den Bereitstellungsdetails verfügbar. Wenn diese Informationen auf der Bereitstellungsebene bereitgestellt werden, wird der Cloud-Administrator darüber informiert. Diese Informationen sind aber auch für Mitglieder hilfreich, um die Auswirkungen ihrer Arbeit auf Budgets und langfristige Entwicklung zu verstehen.

Sie können Preisinformationen von Benutzern in Cloud Assembly und Service Broker anzeigen, indem Sie auf die Schaltfläche „Preisinformationen anzeigen“ klicken. Bei deaktivierter Option werden Cloud Assembly- und Service Broker-Benutzern die Preisinformationen nicht angezeigt.

Wie wird der Preis berechnet?

Die anfänglichen Kosten, die auf der Bereitstellungsebene für Ihre Computing- und Speicherressourcen angezeigt werden, basieren auf branchenüblichen Benchmark-Sätzen und werden dann im Laufe der Zeit berechnet. Der Kostensatz wird auf Hosts angewendet, und der Dienst berechnet die CPU- und Arbeitsspeicherraten. Der Server berechnet die Kosten alle 24 Stunden neu.

Neue Richtlinien, Zuweisungen und die Vorabpreisgestaltung werden während des nächsten vROps-Datenerfassungszyklus ermittelt. Standardmäßig wird der Datenerfassungszyklus alle 5 Minuten ausgeführt. Es kann bis zu 24 Stunden dauern, bis neue Richtlinien oder Änderungen in Projekten und Bereitstellungen aktualisiert werden.

Sie können den Preisserver auch jederzeit manuell auf der Seite „vROps-Endpoint“ unter **Infrastruktur > Integrationen > vROps-Endpoint** > aktualisieren. Klicken Sie im Abschnitt „vCenter Server“ auf **Synchronisieren**. Wenn Sie den Preisserver manuell mit der Option **Synchronisieren** aktualisieren, werden die Preise für alle Projekte in der Organisation neu berechnet. Je nach Anzahl der Projekte in Ihrer Organisation ist dieser Vorgang unter Umständen arbeits- und zeitintensiv.

Eine Liste der unterstützten Ressourcen finden Sie unter [Liste der kalkulierten Komponententypen in vRealize Automation Cloud Assembly](#).

Liste der kalkulierten Komponententypen in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly bietet standardmäßige Kosteninformationen für die folgenden Blueprint-Komponententypen.

Tabelle 4-2. Kalkulierte Komponententypen

Blueprint-Komponententyp	Dienstname/Objektyp	Blueprint-Ressourcentyp	Anmerkungen
Cloud-unabhängig	Maschine	Cloud.Machine	Wenn eine unabhängige Maschine mit vSphere konfiguriert ist, können Sie die Bereitstellungskosten anzeigen.
	Festplatte	Cloud.Volume	Wenn eine unabhängige Festplatte an eine virtuelle Maschine angehängt ist, die mit vSphere konfiguriert ist, können Sie die Bereitstellungskosten anzeigen.
vSphere	vSphere-Maschine	Cloud.vSphere.Machine	Wird mithilfe eines Cloud-spezifischen Blueprints bereitgestellt.

Tabelle 4-2. Kalkulierte Komponententypen (Fortsetzung)

Blueprint-Komponententyp	Dienstname/Objektyp	Blueprint-Ressourcentyp	Anmerkungen
	vSphere-Festplatte	Cloud.vSphere.Disk	Wird mithilfe eines Cloud-spezifischen Blueprints bereitgestellt, der an eine virtuelle Maschine angehängt ist.
VMware Managed Cloud (VMC)	vSphere-Maschine	Cloud.vSphere.Machine	VMC unterstützt nur ratenbasierte Preiskarten (kostenbasierte Preiskarten werden nicht unterstützt).
	vSphere-Festplatte	Cloud.vSphere.Disk	

Vorgehensweise zum Erstellen einer Preisgestaltungskarte in Cloud Assembly

Abhängig von der vom Cloud-Administrator festgelegten Preisgestaltungsstrategie können Sie eine Preisgestaltungskarte erstellen und sie Projekten oder Cloud-Zonen zuweisen.

Preisgestaltungskarten sind basierend auf vom Benutzer ausgewählten Parametern anpassbar. Nach dem Konfigurieren einer Preisgestaltungskarte können Sie sie einem oder mehreren von der Preisgestaltungsstrategie festgelegten Projekten und Cloud-Zonen zuweisen.

Voraussetzungen

Bevor Sie Preisgestaltungskarten erstellen oder zuweisen können, müssen Sie die Preisgestaltung konfigurieren und aktivieren und die Währung in vRealize Operations konfigurieren, um mit vRealize Automation zu arbeiten. Stellen Sie beim Konfigurieren von vRealize Operations mit vRealize Automation sicher, dass beide Anwendungen auf dieselbe Zeitzone festgelegt sind. Um die Zeitzone in vRealize Operations zu konfigurieren, aktivieren Sie SSH und melden sich bei jedem vRealize Operations-Knoten an, bearbeiten die Datei `$ALIVE_Base/user/conf/analytics/advanced.properties` und fügen `timeZoneUseInMeteringCalculation = <time zone>` hinzu.

Sie müssen einen vRealize Operations-Endpoint konfigurieren, bevor Sie die Preisgestaltungskarten konfigurieren können. Um den vRealize Operations-Endpoint zu konfigurieren, navigieren Sie zu **Infrastruktur > Verbindungen > Integrationen > Integration hinzufügen**.

Hinweis Wenn mehrere vRealize Operations-Endpoints hinzugefügt werden, dürfen diese nicht dasselbe vCenter überwachen.

Verfahren

- 1 Navigieren Sie zu **Infrastruktur > Preisgestaltungskarten > Neue Preisgestaltungskarte**.

- 2 Geben Sie auf der Registerkarte „Übersicht“ einen Namen und eine Beschreibung für die Preisgestaltungskarte ein. Sobald die Richtlinie auf der Registerkarte „Preisgestaltung“ definiert ist, wird die Übersichtstabelle mit den Sätzen der Preisgestaltungskarten gefüllt.

Hinweis Die Währungseinheit wird durch den in vRealize Operations ausgewählten Wert bestimmt.

- 3 Optional. Aktivieren Sie das Kontrollkästchen **Standardwert für nicht zugewiesene Projekte?**, um diese Preisgestaltungskarte standardmäßig allen nicht zugewiesenen Projekten zuzuweisen.

- 4 Klicken Sie auf **Preisgestaltung** und konfigurieren Sie die Details Ihrer Preisgestaltungsrichtlinie.

Tabelle 4-3. Konfiguration der Preisgestaltungsrichtlinie

Parameter	Beschreibung
Grundgebühren	<p>Geben Sie einen Namen und eine Beschreibung für Ihre Richtlinie ein. Wählen Sie kosten- oder ratenbasiert aus.</p> <ul style="list-style-type: none"> ■ Kosten: Die Kosten werden in vRealize Operations definiert. Wenn diese Option ausgewählt ist, ist ein Multiplikationsfaktor erforderlich. Wenn Sie z. B. 1,1 als Faktor auswählen, werden die Kosten mit 1,1 multipliziert, was zu einer Steigerung der berechneten Kosten um 10 % führt. Die Preisgleichung mit den Kosten lautet: $\text{Kosten} \times \text{Multiplikationsfaktor} = \text{Preis}$ ■ Rate: Wenn diese Option ausgewählt ist, müssen Sie absolute Werte verwenden, um die Kosten zu ermitteln. Die Preisgleichung mit Raten lautet: $\text{Rate} = \text{Preis}$. Wählen Sie in der Dropdown-Liste ein Ratenintervall aus, um festzulegen, wie diese Rate in Rechnung gestellt wird. <p>Im Abschnitt „Grundgebühren“ definieren Sie die Kosten oder die Rate für CPU, Arbeitsspeicher, Speicher und sonstige Kosten.</p>
Gastbetriebssysteme	<p>Sie können eine Gebühr für das Gastbetriebssystem definieren, indem Sie auf Gebühr hinzufügen klicken. Geben Sie den Namen des Gastbetriebssystems ein und definieren Sie die Gebührenmethode und den Basissatz.</p> <ul style="list-style-type: none"> ■ Wiederkehrend: Geben Sie einen Basissatz ein und definieren Sie das wiederkehrende Intervall als Gebührenzeitraum. Der absolute Wert für den Satz ist erforderlich und wird zum Gesamtpreis addiert. ■ Einmalig: Definieren Sie die einmalige Basissatzgebühr. Der absolute Wert ist erforderlich und wird als einmaliger Preis hinzugefügt. ■ Ratenfaktor: Es ist ein Multiplikationsfaktor erforderlich, der auf die ausgewählte Gebührenkategorie angewendet wird. Beispiel: Sie wählen die CPU-Gebühr und den Faktor 2 aus. Für die CPU des Gastbetriebssystems wird das 2-fache des Standardkostenwerts berechnet. <p>Sie können mehrere Gastbetriebssysteme mit unterschiedlichen Raten hinzufügen, indem Sie auf Gebühr hinzufügen klicken und eine zusätzliche Gebührenrichtlinie konfigurieren.</p> <p>Hinweis Vorabgebühren für Gastbetriebssysteme werden auf der Übersichtsseite nicht angezeigt, obwohl sie Teil der Richtlinie sind.</p>

Tabelle 4-3. Konfiguration der Preisgestaltungsrichtlinie (Fortsetzung)

Parameter	Beschreibung
Tags	<p>Sie können eine Tag-Gebühr festlegen, indem Sie auf Gebühr hinzufügen klicken.</p> <p>Wählen Sie den Tag-Namen aus und definieren Sie die Gebührenmethode und den Basissatz.</p> <ul style="list-style-type: none"> ■ Wiederkehrend: Geben Sie einen Basissatz ein und definieren Sie das wiederkehrende Intervall als Gebührenzeitraum. Der absolute Wert für den Satz ist erforderlich und wird zum Gesamtpreis addiert. ■ Einmalig: Definieren Sie die einmalige Basissatzgebühr. Der absolute Wert ist erforderlich und wird als einmaliger Preis hinzugefügt. ■ Ratenfaktor: Es ist ein Multiplikationsfaktor erforderlich, der auf die ausgewählte Gebührenkategorie angewendet wird. <p>Wählen Sie aus, wie das Tag basierend auf dem Betriebszustand berechnet werden soll.</p> <p>Sie können mehrere Tags mit unterschiedlichen Raten hinzufügen, indem Sie auf Gebühr hinzufügen klicken und eine zusätzliche Gebührenrichtlinie konfigurieren.</p> <hr/> <p>Hinweis Zusätzliche Gebühren im berechneten Endpreis umfassen Tags für VMs und keine Tags für Festplatten und Netzwerke.</p>

Tabelle 4-3. Konfiguration der Preisgestaltungsrichtlinie (Fortsetzung)

Parameter	Beschreibung
Benutzerdefinierte Eigenschaften	<p>Sie können eine Gebühr für eine benutzerdefinierte Eigenschaft definieren, indem Sie auf Gebühr hinzufügen klicken.</p> <p>Geben Sie den Eigenschaftennamen und den Wert ein und definieren Sie die Gebührenmethode und den Basissatz.</p> <ul style="list-style-type: none"> ■ Wiederkehrend: Geben Sie einen Basissatz ein und definieren Sie das wiederkehrende Intervall als Gebührenzeitraum. Der absolute Wert für den Satz ist erforderlich und wird zum Gesamtpreis addiert. ■ Einmalig: Definieren Sie die einmalige Basissatzgebühr. Der absolute Wert ist erforderlich und wird als einmaliger Preis hinzugefügt. ■ Ratenfaktor: Es ist ein Multiplikationsfaktor erforderlich, der auf die ausgewählte Gebührenkategorie angewendet wird. <p>Wählen Sie aus, wie die Gebühr für die benutzerdefinierte Eigenschaft basierend auf dem Betriebszustand berechnet wird.</p> <p>Sie können mehrere benutzerdefinierte Eigenschaften mit unterschiedlichen Raten hinzufügen, indem Sie auf Gebühr hinzufügen klicken und eine zusätzliche Gebührenrichtlinie konfigurieren.</p>
Gesamtgebühren	<p>Legen Sie alle zusätzlichen Gebühren fest, die Sie zur Preisgestaltungsrichtlinie hinzufügen möchten. Sie können eine einmalige Gebühr und wiederkehrende Gebühren hinzufügen.</p>

Hinweis Einmalige Gebühren werden nicht in der Preisschätzung eines Katalogelements oder auf der Registerkarte „Übersicht“ angezeigt. Es wird nur die tägliche Preisschätzung für ein bestimmtes Katalogelement angezeigt.

- 5 Klicken Sie auf die Registerkarte **Zuweisungen** und dann auf **Projekte zuweisen**. Wählen Sie ein oder mehrere Projekte aus, denen die Preisgestaltungskarte zugewiesen werden soll.

Hinweis Standardmäßig werden Preisgestaltungskarten auf Projekte angewendet. Auf der Registerkarte **Infrastruktur > Preisgestaltungskarten** können Sie die Preisgestaltungskarten auf Cloud-Zonen anwenden. Wenn Sie Cloud-Zonen ausgewählt haben, klicken Sie auf der Registerkarte „Zuweisungen“ auf **Cloud-Zonen zuweisen**.

- 6 Klicken Sie auf **Erstellen**, um zu speichern und Ihre Preisgestaltungsrichtlinie zu erstellen.

Ergebnisse




Ihre neue Preisgestaltungsrichtlinie wird auf der Seite „Preisgestaltungskarten“ angezeigt. Um die Richtliniendetails und die Konfiguration anzuzeigen oder zu bearbeiten, klicken Sie auf **Öffnen**.

Vorgehensweise zum Schätzen des Preises einer Bereitstellung

Vor der Bereitstellung eines Katalogelements können Sie den Vorabpreis als Preisschätzung für Ihre Bereitstellung verwenden.

Daily Price Estimate
×

Guest OS and one time prices are excluded in this estimate.

 price-service-f309c00	\$0.54
 Cloud_vSphere_Machine_1	\$0.53
Compute	\$0.39
Storage	\$0.03
Additional charges	\$0.11
 Cloud_vSphere_Disk_1	\$0.01
Storage	\$0.01

CLOSE

Bei einer Vorabpreisschätzung ist die Größe der Bootfestplatte pro VM immer 8 GB.

Bei dem Vorabpreis einer Bereitstellung handelt es sich um eine Schätzung des täglichen Preises, basierend auf der Zuteilung einer Ressource für ein bestimmtes Katalogelement, bevor es bereitgestellt wird. Nachdem ein Katalogelement bereitgestellt wurde, können Sie den Preis vom Monatsanfang bis zum aktuellen Datum als Summe des Vorabpreises auf den Registerkarten **Bereitstellung** und **Infrastruktur > Projekte** anzeigen. Der Vorabpreis wird für Private Cloud-Ressourcen wie vSphere-Maschine und vSphere-Festplatte, Cloud Assembly-Katalogelemente und Cloud-unabhängige Elemente mit vCenter, das für Private Cloud konfiguriert ist, unterstützt.

Hinweis Der Vorabpreis wird für Public Cloud-Ressourcen oder andere Private Cloud-Ressourcen als vSphere-Maschine oder -Festplatte nicht unterstützt.

Voraussetzungen

Um den Preis in vRealize Automation Cloud Assembly anzuzeigen, müssen Sie über einen vRealize Operations-Integrations-Endpoint verfügen, für den die Preisgestaltung aktiviert und die Währung voreingestellt sind.

Verfahren

- 1 Wählen Sie im Katalog ein Katalogelement aus und klicken Sie auf **Anfordern**.

Daily Price Estimate
0.00

CALCULATE
DETAILS

- 2 Geben Sie die Details für Ihre Katalogelementanforderung ein und klicken Sie auf **Berechnen**.

Daily Price Estimate	\$0.54
UPDATE	DETAILS

- 3 (Optional) Klicken Sie auf **Details**, um die Preisaufschlüsselung im Fenster mit der Schätzung des täglichen Preises anzuzeigen.

Nächste Schritte

Wenn die Schätzung des täglichen Preises akzeptabel ist, klicken Sie auf **Senden**, um die Bereitstellungsanforderung fortzusetzen.

Wie schätze ich den Preis aller meiner Projekte?

Als Cloud-Administrator möchten Sie eventuell den Gesamtpreis aller Ihrer Projekte schätzen.

Für Kostenübersichtszwecke können Sie die Preisgestaltungskarten der Projekte verwenden, um den Gesamtpreis aller Ihrer Projekte zu schätzen.

Verfahren

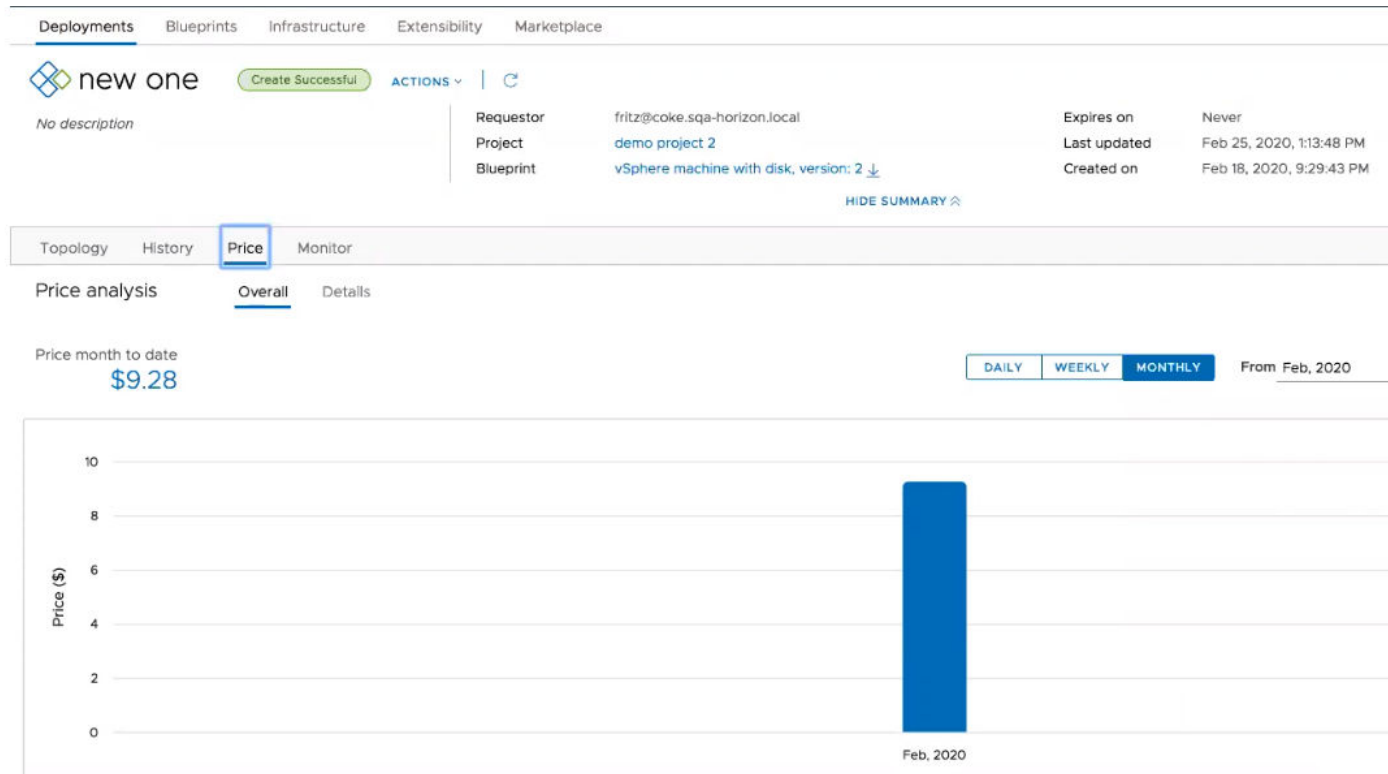
- 1 Klicken Sie auf der Seite **Infrastruktur > Preisgestaltungskarten** neben **Alle Preisgestaltungskarten werden angewendet auf:** auf **Bearbeiten** und wählen Sie **Projekte** aus.

Hinweis Wenn Sie die Einstellung **Alle Preisgestaltungskarten werden angewendet auf** ändern, werden alle vorhandenen Zuweisungen von Preisgestaltungskarten gelöscht.

- 2 Erstellen Sie Preisgestaltungskarten und Zuweisungen mithilfe eines kostenbasierten Ansatzes. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Erstellen einer Preisgestaltungskarte in Cloud Assembly](#).

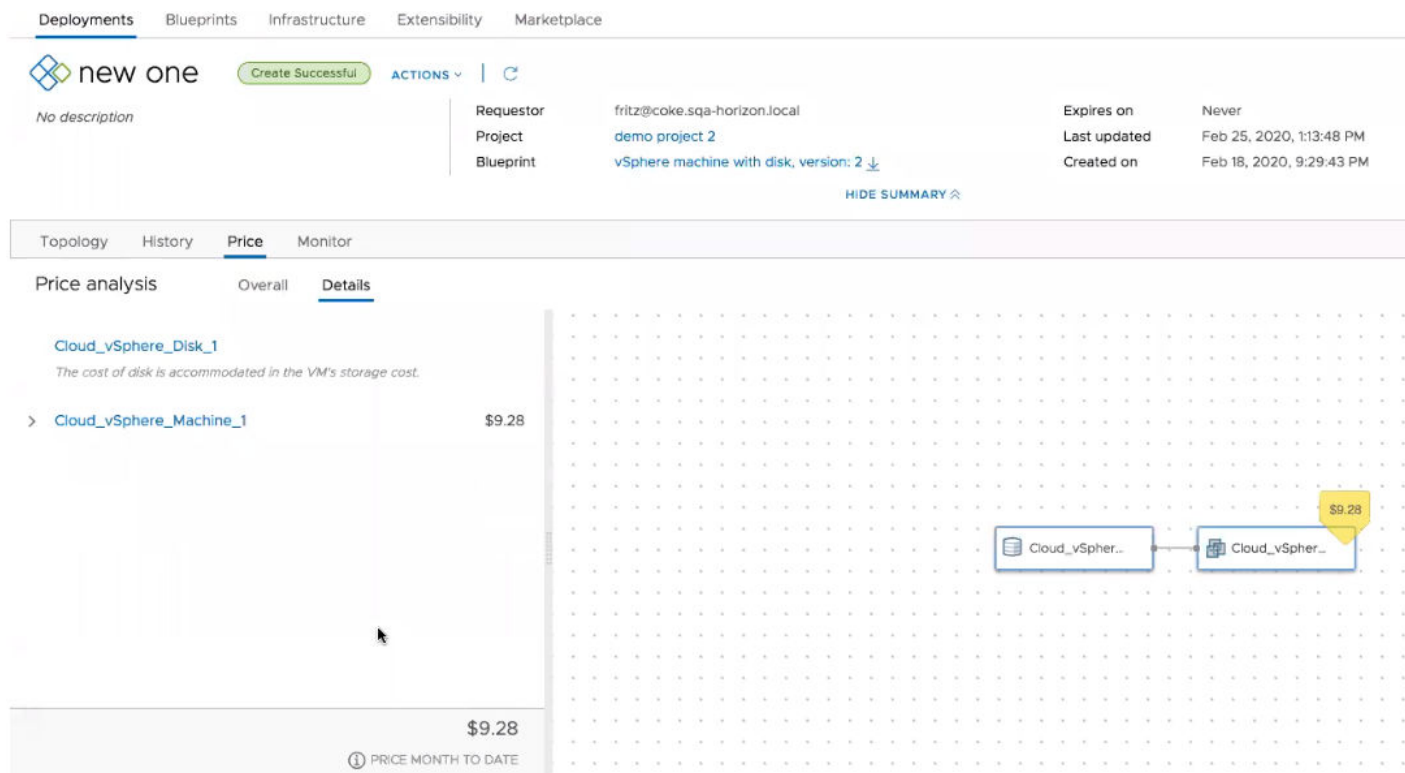
Wie kann ich den Preisverlauf meiner Bereitstellung anzeigen?

Nach dem Definieren und Zuweisen einer Preisgestaltungskarte zu einem Projekt können Sie den Preisverlauf einer einzelnen Bereitstellung im Zeitverlauf anzeigen.



Um den Preisverlauf anzuzeigen, navigieren Sie zu Ihrer Bereitstellung und klicken Sie auf **Preis**. Die Preisanalyse bietet einen Überblick und eine detaillierte Ansicht des Bereitstellungspreises zusammen mit dem Wert vom Monatsanfang bis zum aktuellen Datum. Sie können die grafische Darstellung ändern, um den Bereitstellungspreis als tägliche, wöchentliche oder monatliche Werte anzuzeigen. Darüber hinaus können Sie einen genauen Datumsbereich oder einen Monat für den Preisverlauf angeben.

Um die Preisaufschlüsselung nach Kostenkomponenten anzuzeigen, klicken Sie auf **Details**.



Konfigurieren von Mehrmandantenressourcen mit vRealize Automation

In Umgebungen mit mehreren Mandanten können Kunden die Zuteilung von Ressourcen auf Mandantenbasis mithilfe von virtuellen Privatzonen (VPZs) verwalten.

In vRealize Automation 8.x können Kunden Mehrmandanten-Umgebungen mit VMware Lifecycle Manager und Workspace ONE Access konfigurieren. Diese Tools ermöglichen es Benutzern, Mehrmandantenfähigkeit einzurichten und Mandanten zu erstellen und zu konfigurieren. Nachdem Mandanten konfiguriert wurden, können Anbieteradministratoren virtuelle Privatzonen in vRealize Automation Cloud Assembly erstellen, und dann können sie mithilfe der Mandantenverwaltungsfunktion von vRealize Automation Cloud Assembly Mandanten Zonen zuweisen.

Mehrmandantenfähigkeit basiert auf der Koordination und Konfiguration von drei verschiedenen VMware-Produkten, wie im Folgenden beschrieben:

- **Workspace ONE Access:** Dieses Produkt bietet die Infrastrukturunterstützung für Mehrmandantenfähigkeit und die Active Directory-Domänenverbindungen, die Benutzer- und Gruppenverwaltung innerhalb von Mandantenorganisationen ermöglichen.
- **vRealize Suite Lifecycle Manager:** Dieses Produkt unterstützt die Erstellung und Konfiguration von Mandanten für unterstützte Produkte, wie z. B. vRealize Automation. Darüber hinaus bietet es einige Zertifikatverwaltungsfunktionen.

- vRealize Automation: Anbieter und Benutzer melden sich bei vRealize Automation an, um auf Mandanten zuzugreifen, in denen sie Bereitstellungen erstellen und verwalten.

Bei der Konfiguration der Mehrmandantenfähigkeit sollten die Benutzer mit allen drei Produkten und der zugehörigen Dokumentationen vertraut sein.

Weitere Informationen zum Arbeiten mit Lifecycle Manager und Workspace ONE Access finden Sie unter [Benutzerverwaltung mit VMware Identity Manager](#) und [Verwalten von Benutzern und Gruppen](#).

Vorgehensweise zum Erstellen einer virtuellen privaten Zone für vRealize Automation

Anbieteradministratoren können eine virtuelle private Zone (VPZ) erstellen, um Mandanten in einer vRealize Automation-Umgebung mit mehreren Organisationen Infrastrukturressourcen zuzuteilen. Administratoren können VPZs auch verwenden, um die Ressourcenzuteilung in Bereitstellungen mit einem einzelnen Mandanten zu steuern.

Sie können VPZs verwenden, um Ressourcen wie Images, Netzwerke und Speicherressourcen zuzuteilen. Sie funktionieren sehr ähnlich wie Cloud-Zonen pro Mandant, aber sie wurden speziell für die Verwendung im Zusammenhang mit Bereitstellungen mit mehreren Mandanten entwickelt. Sie können für jedes Projekt entweder Cloud-Zonen oder VPZs verwenden, jedoch nicht beide zugleich. Außerdem gibt es immer nur eine VPZ pro Mandant. Das heißt, eine VPZ kann immer nur einem Mandanten zugewiesen werden.

Sie können eine VPZ mit oder ohne NSX erstellen. Wenn Sie eine Zone ohne NSX erstellen, gibt es auf vSphere-Endpoints Grenzwerte bezüglich Funktionen, die mit NSX zusammenhängen.

- Sicherheit (Gruppen, Firewall)
- Netzwerkkomponenten (NAT)

Voraussetzungen

- Aktivieren und konfigurieren Sie die Mehrmandantenfähigkeit in Ihrer vRealize Automation-Bereitstellung mithilfe von VMware Lifecycle Manager und VMware Workspace ONE Access.
- Erstellen Sie Mandantenadministratoren entsprechend Ihrer Mandantenkonfiguration.
- Wenn Sie NSX verwenden möchten, müssen Sie in Ihrer Anbieterorganisation ein entsprechendes NSX-Cloud-Konto erstellen.

Verfahren

- 1 Wählen Sie **Infrastruktur > Konfigurieren > Private Zonen** aus.

Auf der Seite „VPZ“ werden alle vorhandenen Zonen angezeigt, und Sie können dort Zonen erstellen.

- 2 Klicken Sie auf **Neue virtuelle private Zone**.

Es gibt links auf der Seite sechs Auswahlmöglichkeiten, die Sie zum Konfigurieren von Übersichtsinformationen und Infrastrukturkomponenten für die Zone verwenden können.

3 Geben Sie Übersichtsinformationen für die neue Zone ein.

- a Fügen Sie einen Namen und eine Beschreibung hinzu.
- b Wählen Sie ein Konto aus, für das die Zone gilt.
- c Wählen Sie die Platzierungsrichtlinie aus.

Die Platzierungsrichtlinie steuert die Hostauswahl für Bereitstellungen innerhalb der angegebenen Cloud-Zone.

- **default** – Verteilt Computing-Ressourcen nach dem Zufallsprinzip auf Cluster und Hosts. Die Auswahl dieser Option funktioniert auf der Ebene einer einzelnen Maschine. Beispiel: Alle Maschinen in einer bestimmten Bereitstellung werden nach dem Zufallsprinzip auf die verfügbaren Cluster und Hosts verteilt, die die Anforderungen erfüllen.
- **binpack** – Computing-Ressourcen werden auf dem am stärksten ausgelasteten Host platziert, der über genügend Ressourcen zum Ausführen der betreffenden Berechnung verfügt.
- **spread** – Stellt dem Cluster oder Host mit der geringsten Zahl an virtuellen Maschinen Computing-Ressourcen der Bereitstellung zur Verfügung. Für vSphere verteilt Distributed Resource Scheduler (DRS) die virtuellen Maschinen auf die Hosts. Beispiel: Alle angeforderten Maschinen in einer Bereitstellung werden auf demselben Cluster platziert, bei der nächsten Bereitstellung wird jedoch je nach aktueller Last gegebenenfalls ein anderer vSphere-Cluster ausgewählt.

4 Wählen Sie eine Computing-Ressource für die Zone aus.

Fügen Sie den Anforderungen der Cloud-Zone entsprechend Computing-Ressourcen hinzu. Zu Beginn lautet die Filterauswahl „Alle Berechnungen einschließen“ und die darauf folgende Liste zeigt alle verfügbaren Computing-Ressourcen an. Und diese sind alle der entsprechenden Zone zugeordnet. Sie verfügen über zwei zusätzliche Optionen zum Hinzufügen von Computing-Ressourcen zu einer Cloud-Zone.

- **Berechnung manuell auswählen:** Wählen Sie dieses Menüelement aus, wenn Sie Computing-Ressourcen manuell aus der Liste darunter auswählen möchten. Nachdem Sie sie ausgewählt haben, klicken Sie auf „Berechnung hinzufügen“, um die Ressourcen der Zone hinzuzufügen.
- **Berechnung nach Tags dynamisch einbeziehen:** Wählen Sie dieses Menüelement aus, wenn Sie eine Computing-Ressource, die der Zone hinzugefügt werden soll, basierend auf Tags auswählen möchten. Alle Computing-Ressourcen werden so lange angezeigt, bis Sie die entsprechenden Tags hinzufügen. Sie können unter der Option „Berechnung mit diesen Tags einbeziehen“ einen oder mehrere Tags auswählen.

Bei beiden Computing-Wahlmöglichkeiten können Sie eine oder mehrere der auf der Seite angezeigten Computing-Ressourcen entfernen, indem Sie das Kontrollkästchen rechts aktivieren und auf „Entfernen“ klicken.

- 5 Geben Sie nach Bedarf Tags ein oder wählen Sie solche aus.
- 6 Wählen Sie im linken Menü die Option „Typen“ aus und definieren Sie einen oder mehrere Typen für die Zone. Typen definieren Zielbereitstellungsgrößen für ein bestimmtes Cloud-Konto bzw. eine bestimmte Cloud-Region.
- 7 Wählen Sie im linken Menü die Option „Image“ aus und definieren Sie ein oder mehrere Images für die Zone. Images sind Maschinenvorlagen, in denen die für die Zone verfügbaren Betriebssystemspezifikationen definiert werden.
- 8 Wählen Sie im linken Menü „Speicher“ und dann die Speicherrichtlinie und andere Speicherkonfigurationen für die Zone aus.
- 9 Wählen Sie im linken Menü „Netzwerk“ aus und legen Sie die Netzwerke und optional eine in Verbindung mit dieser Zone zu verwendende Netzwerkrichtlinie fest. Sie können auch Lastausgleichsdienste und Sicherheitsgruppen für ausgewählte Netzwerkrichtlinien konfigurieren.

Netzwerk	<ul style="list-style-type: none"> ■ Alle vorhandenen Netzwerke, die mit diesem VPZ verknüpft sind, werden in der Tabelle auf der Registerkarte „Netzwerke“ angezeigt. ■ Klicken Sie auf Netzwerk hinzufügen, um alle mit der ausgewählten Region verknüpften Netzwerke anzuzeigen. Fügen Sie ein Netzwerk zur Verwendung mit dieser Zone hinzu. ■ Wählen Sie ein Netzwerk aus und klicken Sie auf Tags, um dem angegebenen Netzwerk ein oder mehr Tags hinzuzufügen. ■ Wählen Sie IP-Bereiche verwalten aus, um den IP-Bereich anzugeben, über den Benutzer auf dieses Netzwerk zugreifen können. ■ Klicken Sie, falls zutreffend, auf die Registerkarte „Netzwerkrichtlinien“ und wählen Sie eine Isolierungsrichtlinie aus.
Netzwerkrichtlinien	<p>Wählen Sie, falls konfiguriert, eine Netzwerkrichtlinie zur Verwendung mit dieser Zone aus, um eine Isolierungsrichtlinie für ausgehende und private Netzwerke zu erzwingen.</p> <ul style="list-style-type: none"> ■ Wählen Sie bei Bedarf eine Isolierungsrichtlinie aus. ■ Wählen Sie bei Bedarf einen logischen Tier-O-Router und einen Edge-Cluster aus.
Lastausgleichsdienste	Klicken Sie auf Lastausgleichsdienst hinzufügen , um Lastausgleichsdienste für die Cloud-Konten des Kontos bzw. der Region zu konfigurieren.
Sicherheitsgruppen	Klicken Sie auf Sicherheitsgruppe hinzufügen , um Sicherheitsgruppen zum Anwenden von Firewallregeln auf bereitstellte Maschinen zu verwenden.

Ergebnisse

Die virtuelle private Zone wird mit den angegebenen Ressourcenzuteilungen erstellt.

Nächste Schritte

Cloud-Administratoren können die VPZ einem Projekt zuordnen.

- 1 Wählen Sie in Cloud Assembly **Verwaltung > Projekte** aus.
- 2 Wählen Sie die Registerkarte „Bereitstellung“ aus.
- 3 Klicken Sie auf **Zone hinzufügen** und wählen Sie „Virtuelle private Zone hinzufügen“ aus.
- 4 Wählen Sie die gewünschte VPZ in der Liste aus.
- 5 Sie können die Bereitstellungspriorität und Grenzwerte für die Anzahl der Instanzen, den verfügbaren Arbeitsspeicher und die Anzahl der verfügbaren CPUs festlegen.
- 6 Klicken Sie auf **Hinzufügen**.

Verwalten der VPZ-Konfiguration für vRealize Automation-Mandanten

Anbieteradministratoren können virtuelle private Zonen (VPZs) innerhalb vRealize Automation Cloud Assembly verwalten, um die Zuteilung von Infrastrukturressourcen auf Mandantenbasis zu steuern. Über die Seite „Mandantenverwaltung“ können Administratoren Mandanten und VPZs anzeigen und VPZs für Mandanten aktivieren bzw. deaktivieren.

Standardmäßig werden VPZs keinen Mandanten zugeteilt. Sie müssen VPZs auf dieser Seite zuteilen, um sie mit Ihren Mandanten zu verwenden.

Nach ihrer Erstellung sind VPZs standardmäßig aktiviert. Eine aktivierte VPZ kann zugeteilt und mit dem angegebenen Mandanten verwendet werden. Wenn VPZs deaktiviert sind, können sie nicht für die Bereitstellung verwendet oder einem Mandanten zugeteilt werden. Eine VPZ kann deaktiviert sein, aber dennoch einem Mandanten zugeteilt werden.

Wenn ein Anbieteradministrator zur Seite „Mandantenverwaltung“ navigiert, zeigt die Seite alle verfügbaren Mandanten an, und der Administrator kann einen auswählen. Nachdem ein Mandant ausgewählt wurde, zeigt die Seite VPZs an, die derzeit diesem Mandanten zugeteilt sind, falls vorhanden. Der Administrator kann diese Seite verwenden, um dem ausgewählten Mandanten VPZs zuzuteilen.

Wenn eine VPZ zugeteilt wurde, können Mandantenadministratoren diese zu ihren Projekten hinzufügen, und sie wird für die Bereitstellung durch Mandantenbenutzer verfügbar. Nachdem eine VPZ einem Mandanten zugeteilt wurde, kann sie einem anderen Mandanten zugeteilt werden.

Nachdem eine VPZ aktiviert wurde, steht sie zur Verwendung innerhalb des angegebenen Mandanten bereit. Anbieteradministratoren können VPZs deaktivieren, um die Wartung oder die erneute Konfiguration von Mandanten zu vereinfachen, und sie können den Benutzern eine Benachrichtigung über die Deaktivierung senden. Wenn Sie eine VPZ dauerhaft für einen Mandanten nicht verfügbar machen möchten, können Sie deren Zuteilung aufheben. Wenn die Zuteilung einer vorhandenen VPZ aus irgendeinem Grund für einen Mandanten aufgehoben wird, kann sie nicht zum Erstellen von Bereitstellungen über diesen Mandanten verwendet werden.

Voraussetzungen

- Richten Sie Mehrmandantenfähigkeit ein und erstellen Sie VPZs nach Bedarf für Ihre Bereitstellung.

Verfahren

- 1 Wählen Sie in vRealize Automation Cloud Assembly „Mandanten verwalten“ aus.
Die Seite „Mandantenverwaltung“ zeigt alle für die Organisation des Administrators konfigurierten Mandanten in einer Kartenansicht an.
- 2 Klicken Sie auf einen Mandanten, um ihn auszuwählen.
- 3 Klicken Sie auf die Registerkarte „Infrastrukturverwaltung“, um alle zugewiesenen VPZs für den Mandanten zu sehen.
- 4 Wählen Sie **Virtuelle private Zone zuteilen**, um ein Dialogfeld zu öffnen, in dem alle derzeit nicht einem Mandanten zugeteilten Zonen angezeigt werden. Teilen Sie die Zone einem Mandanten zu.
- 5 Wählen Sie eine oder mehrere Zonen im Dialogfeld aus und klicken Sie auf **Dem Mandanten zuteilen**.

Nächste Schritte

Nachdem VPZs zugeteilt wurden, können Mandantenadministratoren diese den Projekten zuweisen.

Anbieteradministratoren können die Kartenansicht von Mandanten verwenden, um den Status von VPZs zu überwachen und zu verwalten.

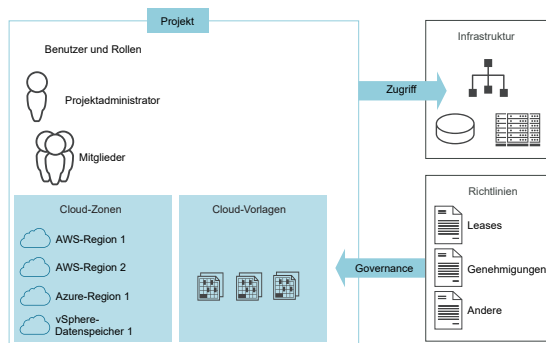
- Wenn Sie einen Mandanten deaktivieren möchten, klicken Sie auf **Deaktivieren** auf der Karte für den Mandanten.
- Um einen Mandanten zu aktivieren, klicken Sie auf **Aktivieren** auf der Karte für den Mandanten.
- Wenn Sie die Zuteilung eines Mandanten aufheben möchten, klicken Sie auf **Zuteilung aufheben** auf der Karte für diesen Mandanten.

Hinzufügen und Verwalten von vRealize Automation Cloud Assembly-Projekten

5

Mit Projekten wird gesteuert, wer Zugriff auf vRealize Automation Cloud Assembly-Cloud-Vorlagen hat und wo die Cloud-Vorlagen bereitgestellt werden. Mithilfe von Projekten verwalten und steuern Sie die Aufgaben, die von den Benutzern durchgeführt werden können, sowie die Cloud-Zonen, in denen Cloud-Vorlagen in Ihrer Cloud-Infrastruktur bereitgestellt werden können.

Cloud-Administratoren richten die Projekte ein, denen Benutzer und Cloud-Zonen hinzugefügt werden können. Jeder, der Cloud-Vorlagen erstellt und bereitstellt, muss Mitglied in mindestens einem Projekt sein.



Dieses Kapitel enthält die folgenden Themen:

- [Vorgehensweise zum Hinzufügen eines Projekts für mein vRealize Automation Cloud Assembly-Entwicklungsteam](#)
- [Weitere Informationen zu vRealize Automation Cloud Assembly-Projekten](#)

Vorgehensweise zum Hinzufügen eines Projekts für mein vRealize Automation Cloud Assembly-Entwicklungsteam

Sie erstellen ein Projekt, dem Sie Mitglieder und Cloud-Zonen hinzufügen, damit die Projektmitglieder ihre Cloud-Vorlagen in den zugeordneten Zonen bereitstellen können. Als vRealize Automation Cloud Assembly-Administrator erstellen Sie ein Projekt für ein Entwicklungsteam. Sie können dann einen Projektadministrator zuweisen oder selbst als Projektadministrator fungieren.

Wenn Sie eine Cloud-Vorlage erstellen, wählen Sie zuerst das Projekt aus, mit dem sie verknüpft werden soll. Das Projekt muss vorhanden sein. Erst dann können Sie die Cloud-Vorlage erstellen.

Stellen Sie sicher, dass Ihre Projekte die geschäftlichen Anforderungen des Entwicklungsteams unterstützen.

- Stellt das Projekt die Ressourcen bereit, die die Ziele des Teams unterstützen? Ein Beispiel für die Unterstützung einer Cloud-Vorlage durch die Infrastrukturressourcen und ein Projekt finden Sie unter [Lernprogramm: Einrichten und Testen einer Multi-Cloud-Infrastruktur und von Bereitstellungen in vRealize Automation Cloud Assembly](#).
- Erwarten die Projektmitglieder, dass die Bereitstellungen freigegeben oder privat sind, oder stellt dies eine Voraussetzung dar? Freigegebene Bereitstellungen sind für alle Projektmitglieder auf der Registerkarte „Bereitstellungen“ verfügbar, nicht nur für die bereitstellenden Mitglieder. Sie können den Freigabestatus der Bereitstellung jederzeit ändern.

Wenn Sie die Bereitstellung für Projektmitglieder freigeben, können die Mitglieder die gleiche Tag-2-Aktion ausführen. Sie können Tag-2-Richtlinien in vRealize Automation Service Broker erstellen, damit Mitglieder Tag-2-Aktionen ausführen können. Die Richtlinien gelten für vRealize Automation Cloud Assembly- und vRealize Automation Service Broker-Bereitstellungen.

Weitere Informationen zu den Tag-2-Richtlinien finden Sie unter [Vorgehensweise zum Berechtigen der Bereitstellungsbenutzer zur Ausführung von Tag-2-Aktionen mithilfe von Richtlinien](#).

Dieses Verfahren basiert auf der Erstellung eines Anfangsprojekts, das nur die grundlegenden Konfigurationen enthält. Wenn das Entwicklungsteam Cloud-Vorlagen erstellt und bereitstellt, können Sie das Projekt unter Umständen ändern. Sie können Einschränkungen, benutzerdefinierte Eigenschaften und andere Optionen hinzufügen, um die Effizienz der Bereitstellung zu steigern. Weitere Informationen finden Sie in den Artikeln unter [Weitere Informationen zu vRealize Automation Cloud Assembly-Projekten](#).

Voraussetzungen

- Stellen Sie sicher, dass Sie die Cloud-Zonen konfiguriert haben. Weitere Informationen hierzu finden Sie unter [Kapitel 4 Erstellen der vRealize Automation Cloud Assembly-Ressourceninfrastruktur](#).
- Stellen Sie sicher, dass Sie die Zuordnungen und Profile für die Regionen konfiguriert haben, die die Cloud-Zonen für dieses Projekt enthalten. Weitere Informationen hierzu finden Sie unter [Kapitel 4 Erstellen der vRealize Automation Cloud Assembly-Ressourceninfrastruktur](#).
- Stellen Sie sicher, dass Sie über die notwendigen Berechtigungen zum Durchführen dieser Aufgabe verfügen. Weitere Informationen hierzu finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).
- Bestimmen Sie den Projektadministrator. Weitere Informationen zu den Funktionen eines Projektmanagers in vRealize Automation Cloud Assembly finden Sie unter [Definition der vRealize Automation-Benutzerrollen](#).

- Wenn Sie Projekten Active Directory-Gruppen hinzufügen, müssen Sie Active Directory-Gruppen für Ihre Organisation konfiguriert haben. Weitere Informationen hierzu finden Sie unter [Rollenzuweisungen für Gruppen in vRealize Automation bearbeiten](#) in *Verwalten von vRealize Automation*. Wenn Sie versuchen, nicht synchronisierte Gruppen zu einem Projekt hinzuzufügen, sind sie nicht verfügbar.

Verfahren

- 1 Wählen Sie **Infrastruktur > Verwaltung > Projekte** aus und klicken Sie auf **Neues Projekt**.
- 2 Geben Sie den Projektnamen ein.
- 3 Klicken Sie auf die Registerkarte **Benutzer**.
 - a Damit nur der anfordernde Benutzer auf Bereitstellungen von Projektmitgliedern zugreifen kann, deaktivieren Sie **Gemeinsam genutzte Bereitstellungen**. Um sicherzustellen, dass Sie die Zuständigkeit für eine Bereitstellung einem anderen Projektmitglied zuweisen können, überprüfen Sie, ob **Gemeinsam genutzte Bereitstellungen** aktiviert ist.
 - b Fügen Sie Benutzer mit zugewiesenen Rollen hinzu.
- 4 Klicken Sie auf die Registerkarte **Bereitstellung** und fügen Sie eine oder mehrere Cloud-Zonen hinzu.

Fügen Sie alle Cloud-Zonen und virtuellen privaten Zonen mit den Ressourcen hinzu, die die von den Projektbenutzern bereitgestellten Cloud-Vorlagen unterstützen.

Sie können für jede Zone eine Zonenpriorität festlegen und Sie können die Anzahl der vom Projekt nutzbaren Ressourcen begrenzen. Zu den Ressourcen, die begrenzt werden können, gehören die Anzahl der Instanzen, der Arbeitsspeicher und die CPUs. Speichergrenzwerte können ausschließlich für vSphere-Cloud-Zonen konfiguriert werden.

Begrenzen Sie die Projektressourcen beim Hinzufügen der Zonen und Anwenden der Grenzwerte nur so weit, dass die Mitglieder ihre Cloud-Vorlagen weiterhin bereitstellen können.

Wenn Ihre Benutzer eine Bereitstellungsanforderung senden, werden die Zonen ausgewertet, um zu ermitteln, welche Zonen über die Ressourcen zur Unterstützung der Bereitstellung verfügen. Wenn mehrere Zonen die Bereitstellung unterstützen, wird die Priorität ausgewertet und die Arbeitslast wird in der Zone mit der höchsten Priorität, d. h. mit dem niedrigsten Ganzzahlwert, platziert.

- 5 Klicken Sie auf **Erstellen**.
- 6 Klicken Sie zum Testen Ihres Projekts mit den Cloud-Zonen des Projekts auf der Seite „Projekte“ auf **Testkonfiguration**.

In der Simulation wird ein standardisierter hypothetischer Bereitstellungstest für die Ressourcen der Projekt-Cloud-Zone ausgeführt. Wenn der Test fehlschlägt, können Sie die Details überprüfen und die Ressourcenkonfiguration korrigieren.

Nächste Schritte

Erste Schritte mit Cloud-Vorlagen. Weitere Informationen hierzu finden Sie unter [Kapitel 6 Entwerfen Ihrer vRealize Automation Cloud Assembly-Bereitstellungen](#).

Weitere Informationen zu vRealize Automation Cloud Assembly-Projekten

Projekte stellen die Verbindung zwischen Cloud-Vorlagen und Ressourcen dar. Je besser Sie sich mit der Funktionsweise von Projekten und den Einsatzmöglichkeiten für Ihre Zwecke auskennen, desto effektiver können Sie den Entwicklungs- und Bereitstellungsprozess in vRealize Automation Cloud Assembly gestalten.

Verwenden von vRealize Automation Cloud Assembly-Projekt-Tags und benutzerdefinierten Eigenschaften

Als Administrator können Sie Kontrolleinschränkungen auf Projektebene oder benutzerdefinierte Eigenschaften hinzufügen, wenn sich die Anforderungen des Projekts von denen der vRealize Automation Cloud Assembly-Cloud-Vorlagen unterscheiden. Neben Einschränkungs-Tags können Sie während des Bereitstellungsvorgangs Ressourcen-Tags hinzufügen, die den bereitgestellten Ressourcen hinzugefügt werden, damit Sie die Ressourcen verwalten können.

Definition von Projekt-Ressourcen-Tags

Ein Projekt-Ressourcen-Tag fungiert als standardisiertes Bezeichnungs-Tag, mit dem Sie die bereitgestellten Ressourcen verwalten und die Konformität sicherstellen können.

Die in einem Projekt definierten Ressourcen-Tags werden allen Komponentenressourcen hinzugefügt, die als Teil dieses Projekts bereitgestellt wurden. Daraufhin können Sie die Ressourcen unter Verwendung des Standard-Taggings mit anderen Anwendungen verwalten.

Als Cloud-Administrator möchten Sie z. B. mithilfe einer Anwendung wie CloudHealth die Kosten verwalten. Sie fügen das `costCenter:eu-cc-1234`-Tag einem Projekt hinzu, das zur Entwicklung eines Personalwesen-Tools in der Europäischen Union dient. Wenn das Projektteam von diesem Projekt bereitgestellt wird, wird das Tag zu den bereitgestellten Ressourcen hinzugefügt. Anschließend konfigurieren Sie das Kosten-Tool, um die Ressourcen zu bezeichnen und zu verwalten, die dieses Tag enthalten. Andere Projekte mit anderen Kostenstellen hätten alternative Werte für den Schlüssel.

Definition von Projekteinschränkungs-Tags

Eine Projekteinschränkung fungiert als Governance-Definition. Es handelt sich um ein `key:value`-Tag, das die Ressourcen definiert, die von der Bereitstellungsanforderung in den Cloud-Zonen des Projekts verwendet oder vermieden werden.

Der Bereitstellungsprozess sucht nach Tags für die Netzwerke und den Speicher, die den Projekteinschränkungen entsprechen, und führt die Bereitstellung basierend auf passenden Tags aus.

Die Erweiterbarkeitseinschränkung wird zur Angabe der integrierten vRealize Orchestrator-Instanz genutzt, die für Erweiterbarkeits-Workflows verwendet werden soll.

Berücksichtigen Sie die folgenden Formate, wenn Sie Projekteinschränkungen konfigurieren.

- **key:value** und **key:value:hard**. Verwenden Sie dieses Tag in einem der beiden Formate, wenn die Cloud-Vorlage auf Ressourcen mit dem entsprechenden Funktions-Tag bereitgestellt werden muss. Der Bereitstellungsvorgang schlägt fehl, wenn kein passendes Tag gefunden wird. Eine von den Mitgliedern eines Projekts bereitgestellte Cloud-Vorlage muss beispielsweise in einem PCI-kompatiblen Netzwerk bereitgestellt werden. Sie verwenden `security:pci`. Wenn keine Netzwerke in den Cloud-Zonen des Projekts gefunden werden, schlägt die Bereitstellung fehl. Hiermit wird sichergestellt, dass keine unsicheren Bereitstellungen vorhanden sind.
- **key:value:soft**. Verwenden Sie dieses Tag, wenn Sie eine passende Ressource zwar bevorzugen, der Bereitstellungsvorgang aber ohne Fehler fortgesetzt werden soll, indem Ressourcen akzeptiert werden, bei denen das Tag nicht passt. Sie möchten beispielsweise, dass die Projektmitglieder ihre Cloud-Vorlagen in einem kostengünstigeren Speicher bereitstellen, lehnen es aber ab, dass sich die Speicherverfügbarkeit auf deren Bereitstellungsmöglichkeiten auswirkt. Sie verwenden `tier:silver:soft`. Befindet sich in den Cloud-Zonen des Projekts kein Speicher mit dem Tag `tier:silver`, wird die Cloud-Vorlage weiterhin in anderen Speicherressourcen bereitgestellt.
- **!key:value**. Verwenden Sie dieses Tag mit „hard“ oder „soft“, wenn Sie die Bereitstellung für Ressourcen mit einem passenden Tag vermeiden möchten.

Aufgrund der höheren Priorität der Einschränkungs-Tags des Projekts überschreiben diese die Einschränkungs-Tags der Cloud-Vorlage zur Bereitstellungszeit. Bei einer Cloud-Vorlage, die nicht überschrieben werden darf, können Sie `failOnConstraintMergeConflict:true` in der Vorlage verwenden. Beispiel: Ihr Projekt weist eine Netzwerkeinschränkung vom Typ `loc:london` auf, bei der Cloud-Vorlage handelt es sich jedoch um `loc:mumbai`. Fügen Sie eine Eigenschaft ähnlich dem folgenden Beispiel hinzu, wenn die Bereitstellung mit einem Einschränkungskonflikt fehlschlagen und der Projektstandort keinen Vorrang haben soll.

```
constraints:
  - tag: 'loc:mumbai'
failOnConstraintMergeConflict:true
```

Vorgehensweise zum Verwenden benutzerdefinierter Projekteigenschaften

Sie können eine benutzerdefinierte Projekteigenschaft für die Berichterstellung, zum Auslösen und Befüllen von Erweiterbarkeitsaktionen und Workflows sowie zum Überschreiben von Eigenschaften auf Cloud-Vorlagenebene verwenden.

Durch Hinzufügen einer benutzerdefinierten Eigenschaft zu einer Bereitstellung können Sie den Wert auf der Benutzeroberfläche verwenden oder ihn mithilfe der API abrufen, um Berichte zu erzeugen.

Die Erweiterbarkeit kann auch eine benutzerdefinierte Eigenschaft für ein Erweiterbarkeitsabonnement verwenden.

Eine Cloud-Vorlage verfügt unter Umständen über einen bestimmten Eigenschaftswert, den Sie für ein Projekt ändern möchten. Sie können einen alternativen Namen und einen anderen Wert als benutzerdefinierte Eigenschaft angeben.

Funktionsweise von vRealize Automation Cloud Assembly-Projekten zur Bereitstellungszeit

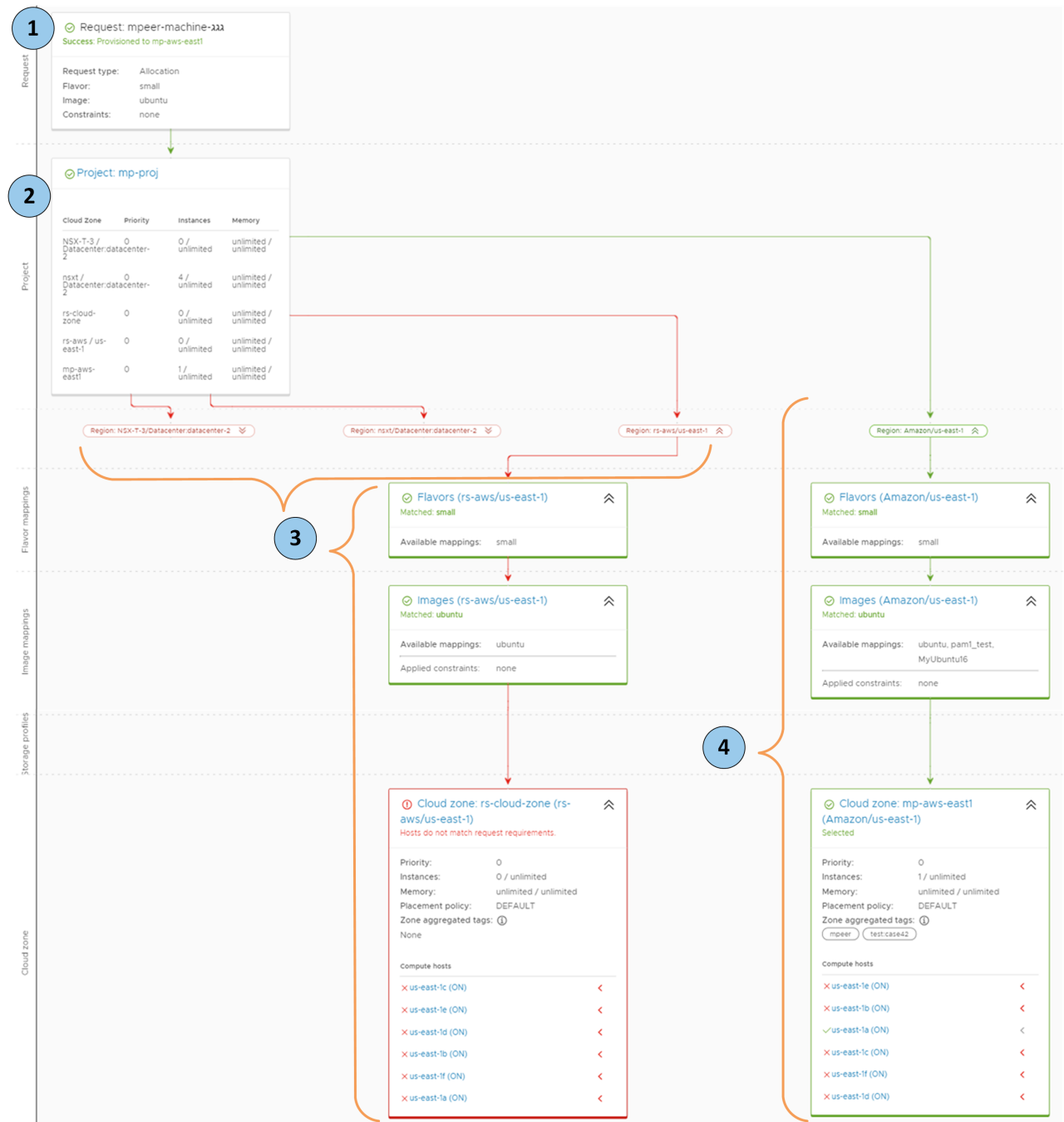
Projekte steuern den Benutzerzugriff auf die Cloud-Zonen und das Eigentum der Benutzer an den bereitgestellten Ressourcen. Unabhängig davon, ob Sie ein Cloud-Administrator oder ein Cloud-Vorlagenentwickler sind, müssen Sie verstehen, wie die Projekte zum Zeitpunkt der Bereitstellung funktionieren, damit Sie Ihre Bereitstellungen verwalten und Probleme beheben können.

Als Cloud-Administrator, der Projekte für verschiedene Teams einrichtet, müssen Sie verstehen, wie Projekte festlegen, wo Cloud-Vorlagenkomponenten bereitgestellt werden. Mit diesem Verständnis können Sie Projekte erstellen, die Cloud-Vorlagenentwickler unterstützen, und fehlerhafte Bereitstellungen beheben.

Wenn Sie eine Cloud-Vorlage erstellen, verknüpfen Sie sie zunächst mit einem Projekt. Zum Zeitpunkt der Bereitstellung werden die Cloud-Vorlagenanforderungen anhand der Cloud-Zonen des Projekts ausgewertet, um den optimalen Bereitstellungsspeicherort zu finden.

Der folgende Workflow stellt den Vorgang dar.

- 1 Sie senden eine Cloud-Vorlagen-Bereitstellungsanforderung.
- 2 Das Projekt wertet die Vorlagen- und Projektanforderungen aus, wie z. B. Konfigurations-, Image- und Einschränkungs-Tags. Die Anforderungen werden mit den Cloud-Zonen des Projekts verglichen, um eine Zone zu finden, die die Anforderungen unterstützt.
- 3 Diese Zonen verfügen nicht über die Ressourcen zur Unterstützung der Anforderung.
- 4 Diese Cloud-Zone unterstützt den Anforderungsbedarf und die Vorlage wird in dieser Cloud-Zonen-Kontoregion bereitgestellt.



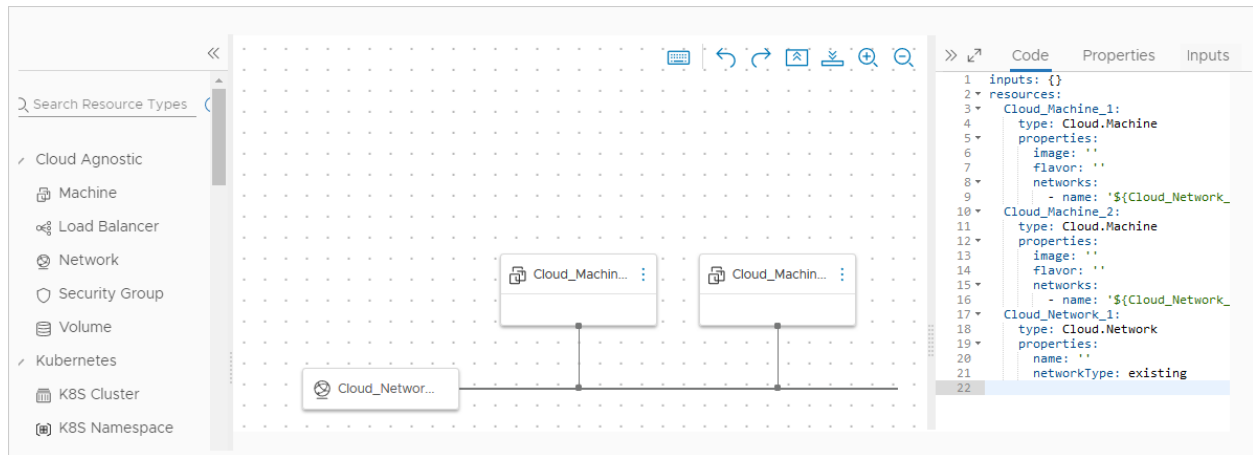
Entwerfen Ihrer vRealize Automation Cloud Assembly-Bereitstellungen

6

Bereitstellungen beginnen mit Cloud-Vorlagen (früher als Blueprints bezeichnet), den Spezifikationen, die die Maschinen, Anwendungen und Dienste definieren, die Sie für Cloud-Ressourcen mithilfe von vRealize Automation Cloud Assembly bereitstellen.

Als Cloud-Vorlagenentwickler können Sie Vorlagen entwerfen, die auf bestimmte Cloud-Anbieter abgestimmt sind. Alternativ dazu können Sie auch Cloud-unabhängige Vorlagen erstellen. Die Cloud Zonen, die Ihrem Projekt zugeordnet sind, bestimmen den zur Auswahl stehenden Ansatz. Wenden Sie sich an Ihren Cloud-Administrator, um sicherzustellen, dass Sie wissen, aus welchen Ressourcen sich Ihre Cloud Zonen zusammensetzen.

Beachten Sie, dass die vRealize Automation Cloud Assembly-Vorlagenerstellung ein „Infrastruktur-als-Code“-Prozess ist. Sie können Ressourcen in der Design-Arbeitsfläche hinzufügen und verbinden, um den Vorgang zu starten. Anschließend vervollständigen Sie die Details mit dem Code-Editor rechts neben der Arbeitsfläche. Mit dem Code-Editor können Sie Code direkt eingeben oder Eigenschaftswerte in ein Formular eingeben.



Vor dem Erstellen einer Cloud-Vorlage

Sie können jederzeit eine vRealize Automation Cloud Assembly-Vorlage erstellen. Für die Bereitstellung müssen Sie jedoch zunächst die Infrastruktur Ihrer Cloud-Ressourcen definieren.

- [Kapitel 4 Erstellen der vRealize Automation Cloud Assembly-Ressourceninfrastruktur](#)

Darüber hinaus müssen Sie ein vRealize Automation Cloud Assembly-Projekt erstellen, das diese Infrastrukturressourcen als Cloud-Zonen enthält.

■ Kapitel 5 Hinzufügen und Verwalten von vRealize Automation Cloud Assembly-Projekten

Dieses Kapitel enthält die folgenden Themen:

- Möglichkeiten zum Erstellen von Cloud-Vorlagen
- Vorgehensweise zum Erstellen einer einfachen vRealize Automation Cloud Assembly-Vorlage von Grund auf
- Vorgehensweise zum Verbessern einer einfachen vRealize Automation Cloud Assembly-Vorlage
- Vorgehensweise zum Hinzufügen von erweiterten Funktionen zu vRealize Automation Cloud Assembly-Designs
- Eigenschaften der vRealize Automation-Ressource
- Beispiele für vRealize Automation Cloud Assembly-Code
- Vorgehensweise zum Integrieren von Terraform-Konfigurationen in vRealize Automation Cloud Assembly
- Vorgehensweise zum Verwenden des vRealize Automation Cloud Assembly-Marketplace

Möglichkeiten zum Erstellen von Cloud-Vorlagen

vRealize Automation Cloud Assembly erstellt und speichert Cloud-Vorlagen als Code, mit dem Sie Vorlagen problemlos entwerfen und wiederverwenden können.

Sie können eine Cloud-Vorlage aus einer leeren Arbeitsfläche erstellen oder den vorhandenen Code nutzen.

Die vRealize Automation Cloud Assembly-Designseite

Um eine Cloud-Vorlage von Grund auf neu zu erstellen, gehen Sie zu **Design > Cloud-Vorlagen** und klicken Sie auf **Neu von > Leere Arbeitsfläche**. Ziehen Sie Ressourcen auf die Arbeitsfläche, verbinden Sie sie und schließen Sie die Konfiguration im Code-Editor ab.

Mit dem Code-Editor können Sie Code direkt eingeben, ausschneiden, kopieren und einfügen. Wenn Sie nicht gern Code bearbeiten, können Sie eine Ressource in der Design-Arbeitsfläche auswählen, auf die Registerkarte **Eigenschaften** im Code-Editor klicken und die Werte dort eingeben. Die von Ihnen eingegebenen Eigenschaftswerte werden im Code so angezeigt, als hätten Sie sie direkt eingegeben.

The screenshot shows the vRealize Automation Cloud Assembly interface. On the left, a code editor displays the YAML configuration for a 'WebTier' template. On the right, the 'Properties' tab is active, showing a configuration table for the template.

```

WebTier:
  type: Cloud.Machine
  properties:
    name: wordpress
    flavor: '${input.size}'
    image: ubuntu
    count: '${input.count}'
    constraints:
      - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
        assignPublicIpAddress: true
    storage:
      disks:
        - capacityGb: '${input.archiveDiskSize}'
          name: ArchiveDisk
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all

  packages:
    - apache2
    - php
    - php-mysql
    - libapache2-mod-php
  
```

Property	Value	Actions
Count	"\${input.count}"	[Edit] [Info]
Image Type	ubuntu	[Reset] [Edit] [Info]
Flavor *	\${input.size}	[Reset] [Edit] [Info]
Storage		
Constraints		[Add] [Info]
<div> <input type="checkbox"/> Tag </div> <div> <div>1 - 10 of 0</div> </div>		
Maximum Capacity of the disk in GB	1	[Edit] [Info]
Size of boot disk in GB	1	[Edit] [Info]
Networks		[Add] [Info]

Beachten Sie, dass Sie Code von einer Cloud-Vorlage in eine andere kopieren und einfügen können.

Cloud-Vorlagen klonen

Zum Klonen einer Vorlage wechseln Sie zu **Design**, wählen eine Quelle aus und klicken auf **Klonen**. Sie klonen eine Cloud-Vorlage, um eine Kopie basierend auf der Quelle zu erstellen. Anschließend weisen Sie den Klon einem neuen Projekt zu oder verwenden ihn als Startcode für eine neue Anwendung.

Hochladen und Herunterladen

Der vRealize Automation Cloud Assembly-Marketplace enthält fertige Cloud-Vorlagen, mit denen Sie Ihre Prozesse beschleunigen können. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Verwenden des vRealize Automation Cloud Assembly-Marketplace](#).

Darüber hinaus können Sie den YAML-Code Ihrer Cloud-Vorlagen in einer Weise hochladen, herunterladen und freigeben, die für Ihren Standort sinnvoll ist. Sie können den Vorlagencode auch mithilfe externer Editoren und Entwicklungsumgebungen ändern.

Hinweis Sie können freigegebenen Vorlagencode validieren, indem Sie ihn im vRealize Automation Cloud Assembly-Code-Editor auf der Designseite überprüfen.

Cloud Templates 22 items						
NEW FROM SYNC REPOS CLONE DEPLOY DOWNLOAD DELETE Filter...						
<input type="checkbox"/>	Name	Description	Source Control	Source Control – Last Sync	Project	Last Updated
<input checked="" type="checkbox"/>	ESFSE				65-Project	Aug 31, 2020, 4:41:52 PM
<input type="checkbox"/>	demo-clone		demo-01/admin-templat...	✓ New draft, version(s) ci	62-Project	Aug 31, 2020, 4:39:47 PM
<input type="checkbox"/>	aws-with-network		demo-01/admin-templat...	✓ New draft, version(s) ci	62-Project	Aug 30, 2020, 5:01:59 PM
<input type="checkbox"/>	test1		demo-01/admin-templat...	✓ New draft, version(s) ci	62-Project	Aug 28, 2020, 3:38:19 PM
<input type="checkbox"/>	test2		demo-01/admin-templat...	✓ New draft, version(s) ci	62-Project	Aug 28, 2020, 3:14:57 PM
<input type="checkbox"/>	test3		demo-01/admin-templat...	✓ New draft, version(s) ci	62-Project	Aug 28, 2020, 1:35:22 PM

Vorgehensweise zum Erstellen einer einfachen vRealize Automation Cloud Assembly-Vorlage von Grund auf

Auf der Seite „Entwerfen“ können Sie vRealize Automation Cloud Assembly-Vorlagenspezifikationen für die Maschinen oder Anwendungen erstellen, die bereitgestellt werden sollen.

- 1 Suchen Sie Ressourcen.
- 2 Ziehen Sie Ressourcen auf die Arbeitsfläche.
- 3 Verbinden Sie Ressourcen.
- 4 Konfigurieren Sie Ressourcen, indem Sie den Cloud-Vorlagencode bearbeiten.

The screenshot shows the vRealize Automation Cloud Assembly Designer interface. On the left, a sidebar lists resource categories: Cloud Agnostic (Machine, Load Balancer, Network, Security Group, Volume) and Kubernetes (K8S Cluster, K8S Namespace). Step 1 points to the 'Machine' resource in the Cloud Agnostic category. The main workspace shows a diagram with two 'Cloud_Machine' resources (Step 2) connected to a 'Cloud_Network' resource (Step 3). On the right, the 'Code' tab displays the CloudAssembly template code, with Step 4 pointing to the configuration for 'Cloud_Machine_1'.

```

1 inputs: {}
2 resources:
3   Cloud_Machine_1:
4     type: Cloud.Machine
5     properties:
6       image: ''
7       flavor: ''
8     networks:
9       - name: '${Cloud_Network_1.name}'
10  Cloud_Machine_2:
11    type: Cloud.Machine
12    properties:
13      image: ''
14      flavor: ''
15    networks:
16      - name: '${Cloud_Network_1.name}'
17  Cloud_Network_1:
18    type: Cloud.Network
19    properties:
20      name: ''
21    networkType: existing
22

```

Auf der Seite „Entwerfen“ können Sie auch den Cloud-Vorlagennamen und die Version ändern, Versionen wiederherstellen oder eine Vorlage klonen bzw. bereitstellen.

Vorgehensweise zum Auswählen und Hinzufügen von vRealize Automation Cloud Assembly-Ressourcen zu einer Cloud-Vorlage

Bei den vRealize Automation Cloud Assembly-Ressourcen handelt es sich um die Bausteine für Ihre Cloud-Vorlage. Auf der Seite „Entwerfen“ können Sie Cloud-unabhängige Ressourcen oder Ressourcen verwenden, die für einen Cloud-Anbieter spezifisch sind.

Ressourcen können links auf der Seite „Entwerfen“ ausgewählt werden.

Cloud-unabhängige Ressourcen

Sie können Cloud-unabhängige Ressourcen für jeden Cloud-Anbieter bereitstellen. Zur Bereitstellungszeit verwendet die Bereitstellung passende Cloud-spezifische Ressourcen. Wenn eine Cloud-Vorlage beispielsweise in AWS- und vSphere-Cloud-Zonen bereitgestellt werden soll, verwenden Sie Cloud-unabhängige Ressourcen.

Cloud-Anbieterressourcen

Anbieterressourcen, wie z. B. spezielle Ressourcen für Amazon Web Services, Microsoft Azure, Google Cloud Platform oder VMware vSphere, können nur in passenden AWS-, Azure-, GCP- oder vSphere-Cloud-Zonen bereitgestellt werden.

Sie können Cloud-unabhängige Ressourcen zu einer Cloud-Vorlage hinzufügen, die Cloud-spezifische Ressourcen für einen bestimmten Anbieter enthält. Achten Sie darauf, was von den Cloud-Zonen des Projekts in Bezug auf den Anbieter unterstützt wird.

Ressourcen der Konfigurationsverwaltung

Die Ressourcen der Konfigurationsverwaltung richten sich nach den integrierten Anwendungen. Eine Puppet-Ressource kann beispielsweise die Konfiguration der anderen Ressourcen überwachen und erzwingen.

Vorgehensweise zum Verbinden von Cloud-Vorlagenressourcen in vRealize Automation Cloud Assembly

Verwenden Sie die grafische Design-Arbeitsfläche in vRealize Automation Cloud Assembly, um Cloud-Vorlagenressourcen zu verbinden.

Sie können Ressourcen verbinden, wenn diese für eine Verbindung kompatibel sind. Beispiel:

- Verbinden eines Lastausgleichsdiensts mit einem Maschinen-Cluster.
- Verbinden einer Maschine mit einem Netzwerk.

- Verbinden des externen Speichers mit einer Maschine.

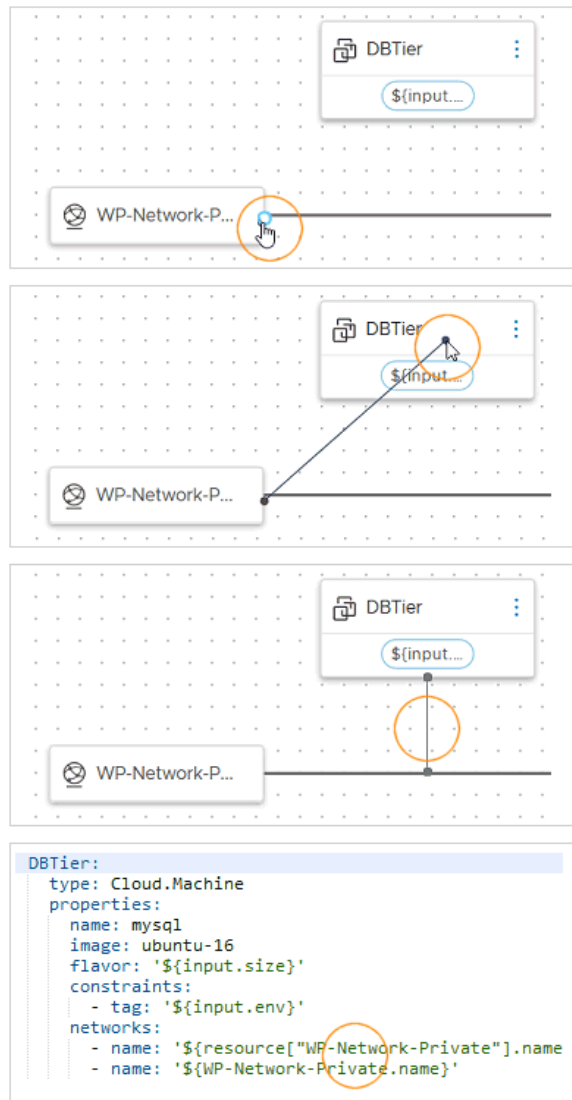
Wichtig Ein Solid-Line-Connector erfordert, dass die beiden Ressourcen in derselben Cloud-Zone bereitgestellt werden. Wenn Sie den Ressourcen widersprüchliche Einschränkungen hinzufügen, kann die Bereitstellung fehlschlagen.

Beispielsweise können Sie keine verbundenen Ressourcen bereitstellen, bei denen Einschränkungs-Tags die Platzierung der einen in einer Zone in us-west-1 und der anderen in einer Zone in us-east-1 erzwingen.

Durchgehende oder gestrichelte Pfeile weisen nur auf eine Abhängigkeit hin, nicht auf eine Verbindung. Weitere Informationen zu Abhängigkeiten finden Sie unter [Vorgehensweise zum Festlegen der Reihenfolge der Ressourcenbereitstellung in vRealize Automation Cloud Assembly](#).

Um eine Verbindung herzustellen, bewegen Sie den Mauszeiger über den Rand einer Ressource, um die Verbindungsblase anzuzeigen. Klicken Sie dann auf die Blase, ziehen Sie sie auf die Zielressource und lassen Sie sie los.

Im Code-Editor wird zusätzlicher Code für die Quellressource im Zielressourcencode angezeigt.

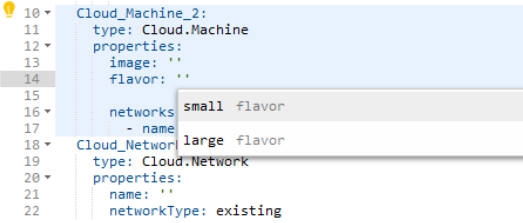
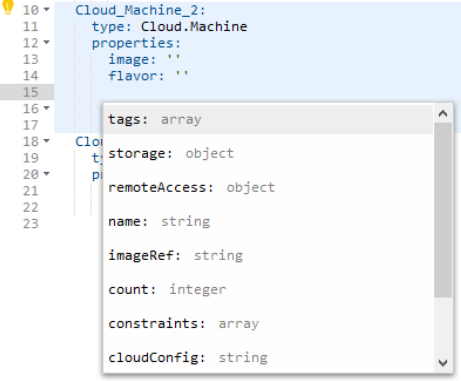
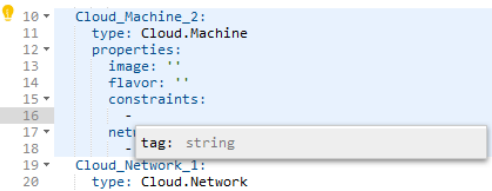
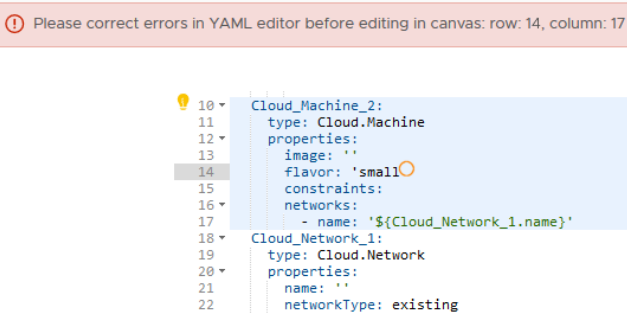
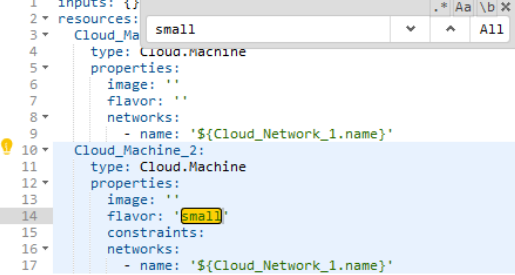


In der Abbildung sind die SQL-Maschine und das private Netzwerk verbunden, sodass sie in derselben Cloud-Zone bereitgestellt werden müssen.

Vorgehensweise zum Erstellen von gültigem Cloud-Vorlagencode in vRealize Automation Cloud Assembly

Durch das Hinzufügen von vRealize Automation Cloud Assembly-Ressourcen und das Verbinden dieser Ressourcen auf der Arbeitsfläche wird nur Startercode erstellt. Um die Komponenten vollständig zu konfigurieren, bearbeiten Sie den Code.

Mit dem Code-Editor können Sie Code direkt eingeben oder Eigenschaftswerte in ein Formular eingeben. Um die direkte Code-Erstellung zu vereinfachen, enthält der vRealize Automation Cloud Assembly-Editor Funktionen zur Syntaxvervollständigung und Fehlerüberprüfung.

Editor-Hinweise	Beispiel
Verfügbare Werte	 <pre> 10 Cloud_Machine_2: 11 type: Cloud.Machine 12 properties: 13 image: '' 14 flavor: '' 15 16 networks: 17 - name: 18 type: Cloud.Network 19 properties: 20 name: '' 21 networkType: existing 22 </pre>
Zulässige Eigenschaft	 <pre> 10 Cloud_Machine_2: 11 type: Cloud.Machine 12 properties: 13 image: '' 14 flavor: '' 15 16 tags: array 17 18 storage: object 19 20 remoteAccess: object 21 22 name: string 23 24 imageRef: string 25 26 count: integer 27 28 constraints: array 29 30 cloudConfig: string 31 </pre>
Untergeordnete Eigenschaft	 <pre> 10 Cloud_Machine_2: 11 type: Cloud.Machine 12 properties: 13 image: '' 14 flavor: '' 15 constraints: 16 - tag: string 17 18 Cloud_Network_1: 19 type: Cloud.Network 20 </pre>
Syntaxfehler	 <pre> 10 Cloud_Machine_2: 11 type: Cloud.Machine 12 properties: 13 image: '' 14 flavor: 'small' 15 constraints: 16 networks: 17 - name: '\${Cloud_Network_1.name}' 18 19 Cloud_Network_1: 20 type: Cloud.Network 21 properties: 22 name: '' 23 networkType: existing 24 </pre>
Strg+F für die Suche	 <pre> 1 inputs: {} 2 resources: 3 Cloud_Machine_2: 4 type: Cloud.Machine 5 properties: 6 image: '' 7 flavor: '' 8 networks: 9 - name: '\${Cloud_Network_1.name}' 10 11 Cloud_Machine_2: 12 type: Cloud.Machine 13 properties: 14 image: '' 15 flavor: 'small' 16 constraints: 17 networks: 18 - name: '\${Cloud_Network_1.name}' 19 </pre>

Editor-Hinweise	Beispiel
<p>Optionale Parameter</p> <p>Optionale Parameter einfügen</p> <ul style="list-style-type: none"> + attachedDisks + autoScaleConfiguration + cloudConfig + cloudConfigSettings 	<pre> 1 inputs: {} 2 resources: 3 Cloud_Machine_1: 4 type: Cloud.Machine 5 properties: 6 image: '' 7 flavor: '' 8 networks: 9 - name: '\${Cloud_Network_1.name}' 10 Cloud_Machine_2: 11 type: Cloud.Machine 12 properties: 13 image: '' 14 flavor: 'small' 15 constraints: 16 networks: 17 - name: '\${Cloud_Network_1.name}' </pre>
<p>Schema-Hilfe</p> <p>cloudConfig</p> <p>Typ</p> <p>string</p> <p>When provisioning an instance, machine cloud-init startup instructions from user data fields. Sample cloud config instructions:</p> <pre> #cloud-config repo_update: true repo_upgrade: all packages: - httpd - mariadb-server runcmd: - [sh, -c, "amazon-linux-extras install -y - systemctl start httpd - sudo systemctl enable httpd </pre>	<pre> Tier: type: Cloud.Machine properties: name: mysql image: ubuntu-16 flavor: '\${input.size}' constraints: - tag: '\${input.env}' networks: - name: '\${resource["WP-Network-Private"] - name: '\${WP-Network-Private.name}' remoteAccess: authentication: usernamePassword username: '\${input.username}' password: '\${input.userpassword}' cloudConfig: #cloud-config repo_update: true repo_upgrade: all packages: - mysql-server runcmd: - sed -e '/bind-address/ s/^#/#/' -i - service mysql restart - mysql -e "GRANT ALL PRIVILEGES ON *.* - mysql -e "FLUSH PRIVILEGES;" attachedDisks: [] bTier: type: Cloud.Machine </pre>

Speichern verschiedener Versionen mithilfe von vRealize Automation Cloud Assembly

Als Cloud-Vorlagenentwickler können Sie einen Snapshot eines funktionierenden Designs sicher erfassen, bevor Sie weitere Änderungen vornehmen.

Zur Bereitstellungszeit können Sie eine der bereitzustellenden Versionen auswählen.

Erfassen einer Version für die Cloud-Vorlage

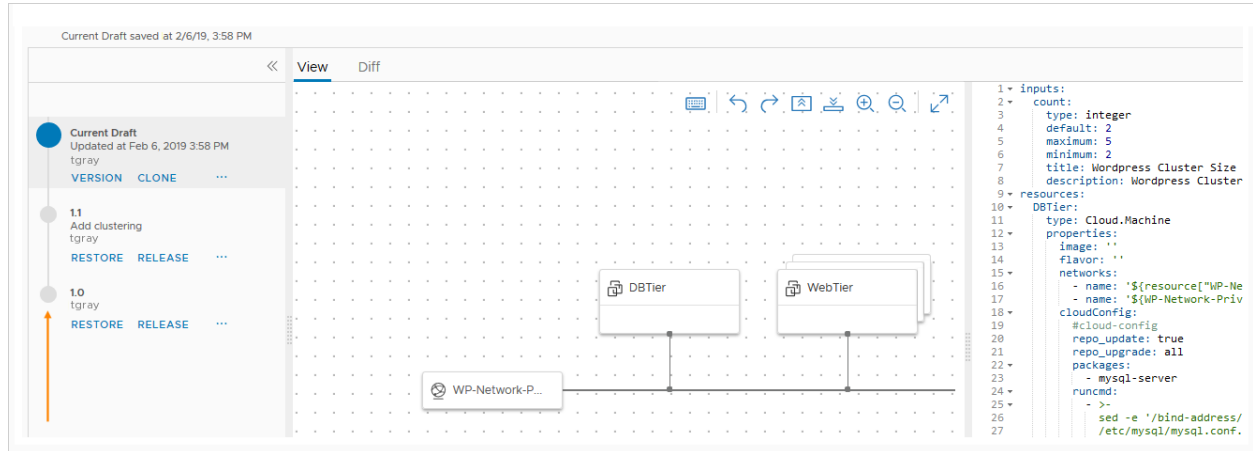
Klicken Sie auf der Entwurfsseite auf **Version** und geben Sie einen Namen an.

Der Name muss alphanumerisch sein und darf keine Leerzeichen enthalten. Nur Punkte, Bindestriche und Unterstriche sind als Sonderzeichen zulässig.

Wiederherstellen einer älteren Version

Klicken Sie auf der Entwurfsseite auf **Versionsverlauf**.

Wählen Sie auf der linken Seite eine ältere Version aus, um sie auf der Arbeitsfläche und im Code-Editor zu überprüfen. Wenn Sie die gewünschte Version gefunden haben, klicken Sie auf **Wiederherstellen**. Beim Wiederherstellen wird der aktuelle Entwurf überschrieben, ohne dass benannte Versionen entfernt werden.



Freigeben einer Version für vRealize Automation Service Broker

Klicken Sie auf der Entwurfsseite auf **Versionsverlauf**.

Wählen Sie auf der linken Seite eine Version aus und geben Sie sie frei.

Sie können einen aktuellen Entwurf erst nach der Versionierung freigeben.

Erneutes Importieren der Version in vRealize Automation Service Broker

Um die neue Version für Katalogbenutzer zu aktivieren, importieren Sie sie erneut.

Gehen Sie in vRealize Automation Service Broker zu **Inhalt und Richtlinien > Inhaltsquellen**.

Klicken Sie in der Liste der Quellen auf die Quelle für das Projekt, das die Cloud-Vorlage mit der neu veröffentlichten Version enthält.

Klicken Sie auf **Speichern und importieren**.

Vergleichen von Cloud-Vorlagenversionen

Wenn sich Änderungen und Versionen anhäufen, möchten Sie unter Umständen die Unterschiede zwischen ihnen ermitteln.

Wählen Sie in vRealize Automation Cloud Assembly in der Ansicht „Versionsverlauf“ eine Version aus und klicken Sie auf **Vergleichen**. Wählen Sie dann im Dropdown-Menü **Vergleichen mit** eine andere Version für den Vergleich aus.

Beachten Sie, dass Sie zwischen der Überprüfung von Code-Unterschieden oder Unterschieden in der visuellen Topologie umschalten können.

Abbildung 6-1. Code-Unterschiede

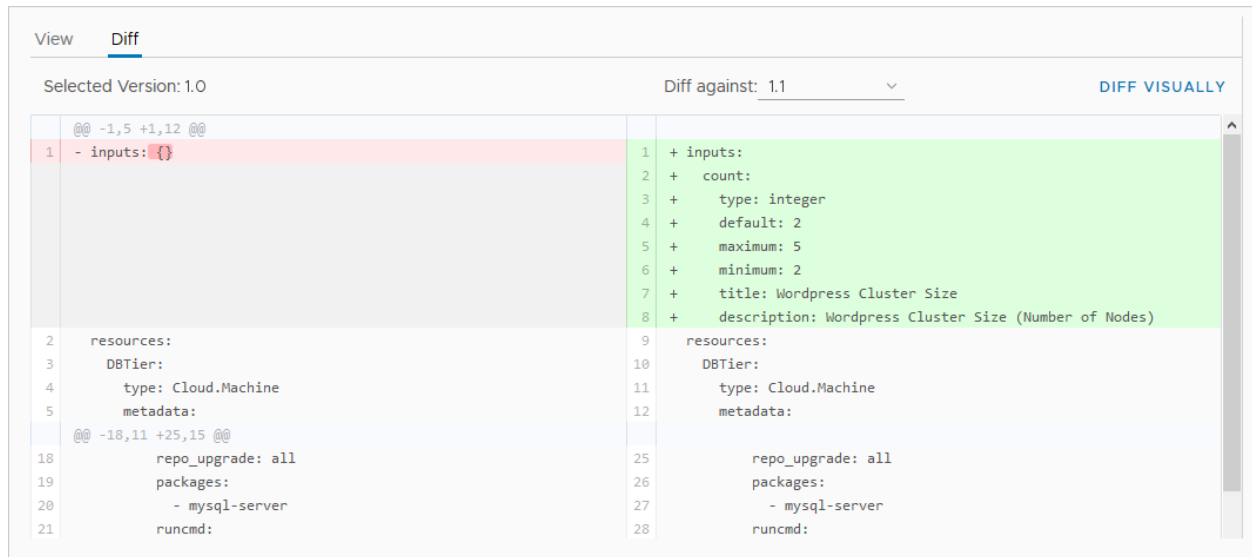
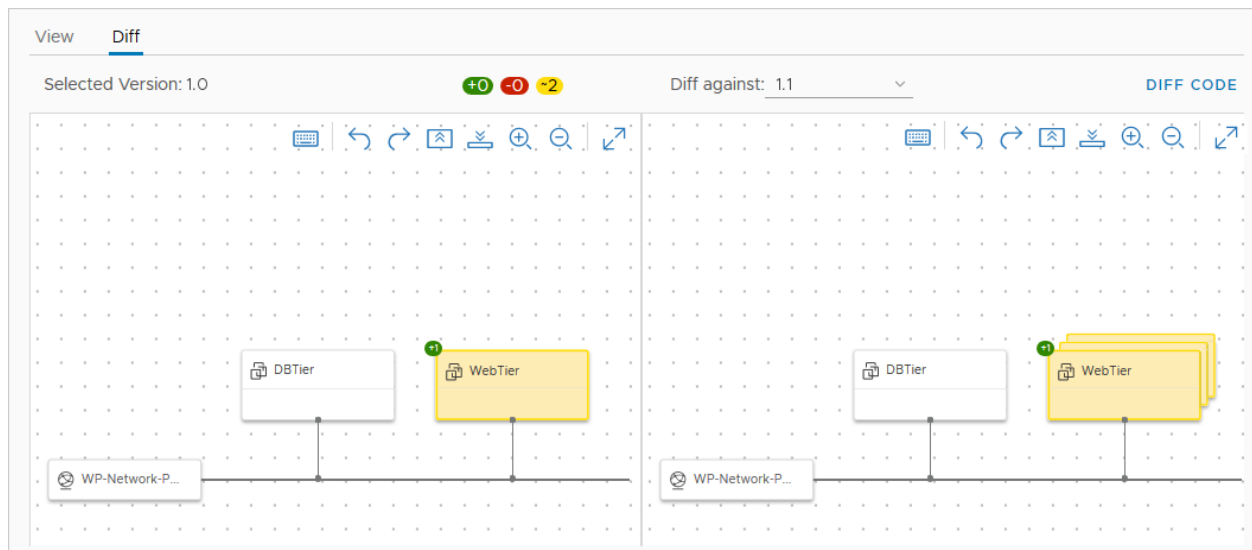


Abbildung 6-2. Unterschiede in der visuellen Topologie



Klonen einer Cloud-Vorlage

Sie können auf der Designseite mithilfe von **Aktionen > Klonen** eine Kopie der aktuellen Vorlage zur alternativen Entwicklung erstellen. Dieser Vorgang ist jedoch nicht mit dem Speichern einer Version gleichzusetzen.

Vorgehensweise zum Verbessern einer einfachen vRealize Automation Cloud Assembly-Vorlage

Es gibt Möglichkeiten für vRealize Automation Cloud Assembly-Vorlagencode, mit denen die Funktionalität einer einfachen Vorlage gesteigert werden kann.

Die hier beschriebenen Techniken erfordern entsprechende Kenntnisse im Umgang mit Infrastrukturcode. Glücklicherweise ist der vRealize Automation Cloud Assembly-Code lesbar und einfach zu verstehen.

Vorgehensweise zum Anpassen einer Cloud-Vorlage in vRealize Automation mit Benutzereingaben

Als Cloud-Vorlagendesigner verwenden Sie Eingabeparameter, damit Benutzer zur Anforderungszeit benutzerdefinierte Auswahlen vornehmen können.

Wenn Benutzer Eingaben bereitstellen, müssen nicht mehr mehrere Vorlagenkopien gespeichert werden, die sich nur geringfügig unterscheiden. Darüber hinaus können Eingaben eine Vorlage auf Tag-2-Vorgänge vorbereiten. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Verwenden von Cloud-Vorlageneingaben für Tag-2-Updates in vRealize Automation](#).

Die folgenden Eingaben zeigen, wie Sie eine Cloud-Vorlage für einen MySQL-Datenbankserver erstellen, wobei Benutzer diese eine Cloud-Vorlage in verschiedenen Cloud-Ressourcenumgebungen bereitstellen und jedes Mal andere Funktionen und Anmeldedaten anwenden können.

Vorgehensweise zum Definieren von Eingabeparametern für Cloud-Vorlagen

Fügen Sie dem Vorlagencode einen `inputs`-Abschnitt hinzu, in dem Sie die auswählbaren Werte festlegen.

Im folgenden Beispiel können Maschinengröße, Betriebssystem und Anzahl der geclusterten Server ausgewählt werden.

```
inputs:
  wp-size:
    type: string
    enum:
      - small
      - medium
    description: Size of Nodes
    title: Node Size
```

```
wp-image:
  type: string
  enum:
    - coreos
    - ubuntu
  title: Select Image/OS
wp-count:
  type: integer
  default: 2
  maximum: 5
  minimum: 2
  title: Wordpress Cluster Size
  description: Wordpress Cluster Size (Number of nodes)
```

Wenn Sie mit der Bearbeitung von Code nicht vertraut sind, können Sie auf die Registerkarte **Eingaben** des Code-Editors klicken und dort entsprechende Einstellungen vornehmen. Das folgende Beispiel zeigt bestimmte Eingaben für die bereits erwähnte MySQL-Datenbank.

The screenshot shows the 'Inputs' tab of the Cloud Template Inputs section. Below the title bar are buttons for '+ NEW', 'EDIT', and 'X DELETE'. A table lists the inputs:

<input type="checkbox"/>	Name	Title	Type	Default Value
<input type="checkbox"/>	size	Tier Machine Size	string	
<input type="checkbox"/>	username	Database Username	string	
<input type="checkbox"/>	userpassword	Database Password	string	****
<input type="checkbox"/>	databaseDiskSize	MySQL Data Disk Size	number	4

An 'Edit Cloud Template Input: size' dialog is open, showing the following fields:

- Name ***: size
- Title**: Tier Machine Size
- Description**: Size of Nodes
- Type**: string (dropdown menu)
- Encrypted**: ☐

Vorgehensweise zum Verweisen auf Eingabeparameter für Cloud-Vorlagen

Als Nächstes verweisen Sie im Abschnitt `resources` unter Verwendung der Syntax `${input.property-name}` auf einen Eingabeparameter.

Wenn ein Eigenschaftsname ein Leerzeichen enthält, trennen Sie ihn mit eckigen Klammern und doppelten Anführungszeichen ab, anstatt die Punktnotation zu verwenden: `${input["property name"]}`

Wichtig Im Cloud-Vorlagencode können Sie das Wort `input` nur verwenden, um einen Eingabeparameter anzugeben.

```
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      flavor: '${input.wp-size}'
      image: '${input.wp-image}'
      count: '${input.wp-count}'
```

Liste der Eingabeeigenschaften

Eigenschaft	Beschreibung
const	Wird mit <code>oneOf</code> verwendet. Der dem angezeigten Titel zugeordnete tatsächliche Wert.
default	Vorab befüllter Wert für die Eingabe. Der Standardwert muss den korrekten Typ aufweisen. Geben Sie kein Wort als Standardwert für eine Ganzzahl ein.
description	Benutzerhilfetext für die Eingabe.
encrypted	Gibt an, ob die vom Benutzer eingegebene Eingabe verschlüsselt werden soll, <code>True</code> oder <code>False</code> . Kennwörter werden in der Regel verschlüsselt.
enum	Ein Dropdown-Menü mit den zulässigen Werten. Verwenden Sie das folgende Beispiel als Formatierungshilfe. <div data-bbox="815 1417 1021 1493" data-label="Text"> <pre>enum: - value 1 - value 2</pre> </div>
format	Legt das erwartete Format für die Eingabe fest. Beispiel: <code>(25/04/19)</code> unterstützt Datum/Uhrzeit (<code>data-time</code>). Ermöglicht die Verwendung der Datumsauswahl in benutzerdefinierten vRealize Automation Service Broker-Formularen.
items	Deklariert Elemente innerhalb eines Arrays. Unterstützt „Zahl“, „Ganzzahl“, „Zeichenfolge“, „Boolesch“ oder „Objekt“.
maxItems	Maximale Anzahl der auswählbaren Elemente innerhalb eines Arrays.

Eigenschaft	Beschreibung
maxLength	Größte zulässige Anzahl an Zeichen für eine Zeichenfolge. Wenn Sie ein Feld beispielsweise auf 25 Zeichen begrenzen möchten, geben Sie <code>maxLength: 25</code> ein.
maximum	Größter zulässiger Wert für eine Zahl oder Ganzzahl.
minItems	Mindestanzahl der auswählbaren Elemente innerhalb eines Arrays.
minLength	Kleinste zulässige Anzahl an Zeichen für eine Zeichenfolge.
minimum	Kleinster zulässiger Wert für eine Zahl oder Ganzzahl.
oneOf	Ermöglicht, dass das Benutzereingabeformular einen Anzeigenamen (title) für einen weniger benutzerfreundlichen Wert (const) anzeigt. Wenn Sie einen Standardwert festlegen, legen Sie „const“ fest, nicht „title“. Gültig für die Verwendung mit den Typen „Zeichenfolge“, „Ganzzahl“ und „Zahl“.
pattern	Zulässige Zeichen für Zeichenfolgeneingaben in der Syntax für reguläre Ausdrücke. Beispiel: <code>'[a-z]+'</code> oder <code>'[a-z0-9A-Z@#&\$]+'</code>
Eigenschaften	Deklariert den key:value-Eigenschaftenblock für Objekte.
readOnly	Dient nur zur Bereitstellung einer Formularbezeichnung.
title	Wird mit oneOf verwendet. Der Anzeigename für einen const-Wert. Der Titel wird zum Zeitpunkt der Bereitstellung im Benutzereingabeformular angezeigt.
type	Datentyp „Zahl“, „Ganzzahl“, „Zeichenfolge“, „Boolesch“ oder „Objekt“.
writeOnly	Blendet im Formular die Tastenanschläge hinter Sternchen aus. Kann nicht mit „enum“ verwendet werden. Wird in benutzerdefinierten vRealize Automation Service Broker-Formularen als Kennwertfeld angezeigt.

Weitere Beispiele

Zeichenfolge mit Enumeration

```

image:
  type: string
  title: Operating System
  description: The operating system version to use.
  enum:
    - ubuntu 16.04
    - ubuntu 18.04
  default: ubuntu 16.04

shell:
```

```

type: string
title: Default shell
Description: The default shell that will be configured for the created user.
enum:
  - /bin/bash
  - /bin/sh

```

Ganzzahl mit Mindest- und Höchstwert

```

count:
  type: integer
  title: Machine Count
  description: The number of machines that you want to deploy.
  maximum: 5
  minimum: 1
  default: 1

```

Array von Objekten

```

tags:
  type: array
  title: Tags
  description: Tags that you want applied to the machines.
  items:
    type: object
    properties:
      key:
        type: string
        title: Key
      value:
        type: string
        title: Value

```

Zeichenfolge mit Anzeigenamen

```

platform:
  type: string
  oneOf:
    - title: AWS
      const: platform:aws
    - title: Azure
      const: platform:azure
    - title: vSphere
      const: platform:vsphere
  default: platform:aws

```

Zeichenfolge mit Mustervalidierung

```

username:
  type: string
  title: Username
  description: The name for the user that will be created when the machine is provisioned.
  pattern: ^[a-zA-Z]+$

```

Zeichenfolge als Kennwort

```
password:
  type: string
  title: Password
  description: The initial password that will be required to logon to the machine.
  Configured to reset on first login.
  encrypted: true
  writeOnly: true
```

Zeichenfolge als Textbereich

```
ssh_public_key:
  type: string
  title: SSH public key
  maxLength: 256
```

Boolesch

```
public_ip:
  type: boolean
  title: Assign public IP address
  description: Choose whether your machine should be internet facing.
  default: false
```

Kalenderauswahl für Datum und Uhrzeit

```
leaseDate:
  type: string
  title: Lease Date
  format: date-time
```

Anpassen einer Anforderung mithilfe von vRealize Automation Cloud Assembly-Ressourcen-Flags

vRealize Automation Cloud Assembly enthält mehrere Einstellungen für die Cloud-Vorlagen, über die konfiguriert wird, wie eine Ressource zur Anforderungszeit behandelt wird.

Die Einstellungen für Ressourcen-Flags sind nicht Teil des Ressourcenobjekt-Eigenschaftenschemas. Für eine bestimmte Ressource fügen Sie die Flag-Einstellungen außerhalb des Abschnitts „Eigenschaften“ wie dargestellt hinzu.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    preventDelete: true
    properties:
      image: coreos
      flavor: small
      attachedDisks:
        - source: '${resource.Cloud_Volume_1.id}'
```

```
Cloud_Volume_1:
  type: Cloud.Volume
  properties:
    capacityGb: 1
```

Ressourcen-Flag	Beschreibung
createBeforeDelete	<p>Für einige Aktualisierungsaktionen ist es erforderlich, dass die vorhandene Ressource entfernt und eine neue erstellt wird. Standardmäßig wird zuerst die Ressource entfernt. Dies kann zu Situationen führen, bei denen die alte Ressource bereits entfernt wurde, die neue jedoch auch einem beliebigen Grund noch nicht erfolgreich erstellt wurde.</p> <p>Legen Sie dieses Flag auf „true“ fest, wenn Sie sicherstellen müssen, dass die neue Ressource vor dem Löschen der vorherigen Ressource erfolgreich erstellt wurde.</p>
createTimeout	<p>Die standardmäßig Zeitüberschreitung von vRealize Automation Cloud Assembly für die Zuteilung, Erstellung und Planung von Ressourcen beträgt 2 Stunden (2h). Darüber hinaus kann ein Projektadministrator einen benutzerdefinierten Standardzeitüberschreitungswert für diese Anforderungen festlegen, der für das gesamte Projekt gilt.</p> <p>Mit diesem Flag können Sie alle Standardeinstellungen außer Kraft setzen und die individuelle Zeitüberschreitung für einen bestimmten Ressourcenvorgang festlegen. Siehe auch „updateTimeout“ und „deleteTimeout“.</p>
deleteTimeout	<p>Der Standardzeitüberschreitungswert von vRealize Automation Cloud Assembly für Löschanforderungen beträgt 2 Stunden (2h). Darüber hinaus kann ein Projektadministrator einen anderen Standardzeitüberschreitungswert für Löschanforderungen festlegen, der für das gesamte Projekt gilt.</p> <p>Mit diesem Flag können Sie alle Standardeinstellungen außer Kraft setzen und die individuelle Zeitüberschreitung für einen bestimmten Ressourcenlöschvorgang festlegen. Siehe auch „updateTimeout“ und „createTimeout“.</p>
dependsOn	<p>Dieses Flag gibt eine explizite Abhängigkeit zwischen Ressourcen an, bei denen eine Ressource vorhanden sein muss, bevor die nächste erstellt wird. Weitere Informationen finden Sie unter Vorgehensweise zum Festlegen der Reihenfolge der Ressourcenbereitstellung in vRealize Automation Cloud Assembly.</p>

Ressourcen-Flag	Beschreibung
dependsOnPreviousInstances	<p>Wenn diese Eigenschaft auf „true“ festgelegt ist, erstellen Sie nacheinander Clusterressourcen. Der Standardwert ist „false“, wodurch alle Ressourcen in einem Cluster gleichzeitig erstellt werden.</p> <p>Die sequenzielle Erstellung ist z. B. für Datenbankcluster sinnvoll, in denen primäre und sekundäre Knoten erstellt werden müssen. Die Erstellung sekundärer Knoten erfordert jedoch Konfigurationseinstellungen, die den Knoten mit einem vorhandenen, primären Knoten verbinden.</p>
forceRecreate	<p>Nicht für alle Aktualisierungsaktionen ist es erforderlich, dass die vorhandene Ressource entfernt und eine neue erstellt wird. Wenn Sie möchten, dass bei einem Update die alte Ressource entfernt und eine neue erstellt wird, unabhängig davon, ob dies bei dem Update standardmäßig der Fall ist, setzen Sie dieses Flag auf „true“.</p>
ignoreChanges	<p>Benutzer einer Ressource können diese neu konfigurieren, indem sie den Status „Bereitgestellt“ der Ressource ändern.</p> <p>Wenn Sie eine Bereitstellungsaktualisierung durchführen möchten, die geänderte Ressource aber nicht mit der Konfiguration aus der Cloud-Vorlage überschreiben möchten, setzen Sie dieses Flag auf „true“.</p>
preventDelete	<p>Wenn Sie eine Ressource vor nachfolgenden Löschanforderungen schützen müssen, setzen Sie dieses Flag auf „true“.</p>
updateTimeout	<p>Der Standardzeitüberschreitungswert von vRealize Automation Cloud Assembly für Aktualisierungsanforderungen beträgt 2 Stunden (2h). Darüber hinaus kann ein Projektadministrator einen anderen Standardzeitüberschreitungswert für Aktualisierungsanforderungen festlegen, der für das gesamte Projekt gilt.</p> <p>Mit diesem Flag können Sie alle Standardeinstellungen außer Kraft setzen und die individuelle Zeitüberschreitung für einen bestimmten Ressourcenaktualisierungsvorgang festlegen. Weitere Informationen finden Sie auch unter „deleteTimeout“ und „createTimeout“.</p>

Vorgehensweise zum Festlegen der Reihenfolge der Ressourcenbereitstellung in vRealize Automation Cloud Assembly

Wenn Sie eine vRealize Automation Cloud Assembly-Vorlage bereitstellen, benötigt eine Ressource möglicherweise eine andere Ressource, die zuerst verfügbar sein muss.

Wichtig Durchgehende oder gestrichelte Pfeile weisen nur auf eine Abhängigkeit hin, nicht auf eine Verbindung. Informationen zum Verbinden von Ressourcen für die Kommunikation finden Sie unter [Vorgehensweise zum Verbinden von Cloud-Vorlagenressourcen in vRealize Automation Cloud Assembly](#).

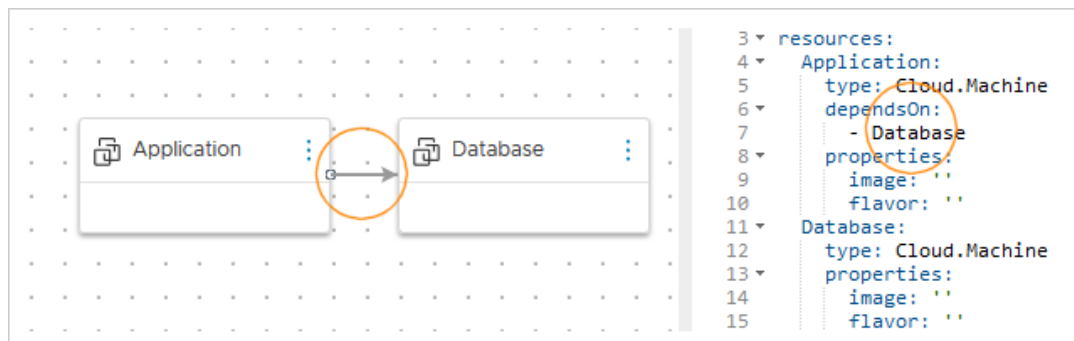
Vorgehensweise zum Erstellen einer expliziten Abhängigkeit

In bestimmten Fällen benötigt eine Ressource eine andere Ressource, die zuerst bereitgestellt werden muss. So muss beispielsweise zuerst ein Datenbankserver vorhanden sein, bevor ein Anwendungsserver erstellt und für den Zugriff darauf konfiguriert werden kann.

Eine explizite Abhängigkeit richtet die Build-Reihenfolge zum Zeitpunkt der Bereitstellung oder für vertikale oder horizontale Skalierungsaktionen ein. Sie können eine explizite Abhängigkeit mithilfe der grafischen Design-Arbeitsfläche oder des Code-Editors hinzufügen.

- Design-Arbeitsfläche – Zeichnen Sie eine Verbindung beginnend bei der abhängigen Ressource und endend bei der Ressource, die zuerst bereitgestellt werden muss.
- Code-Editor – Fügen Sie der abhängigen Ressource eine `dependsOn`-Eigenschaft hinzu und geben Sie die Ressource an, die zuerst bereitgestellt werden muss.

Eine explizite Abhängigkeit wird in Form eines durchgehenden Pfeils auf der Arbeitsfläche angegeben.



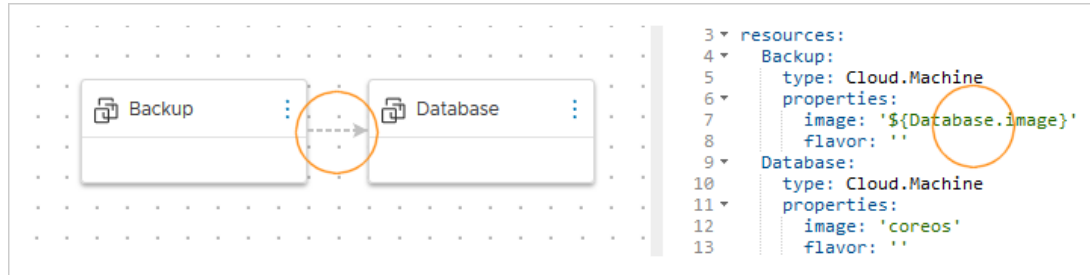
Erstellen einer impliziten Abhängigkeit oder Eigenschaftsbindung

In bestimmten Fällen benötigt eine Ressourceneigenschaft einen Wert, der sich in einer Eigenschaft einer anderen Ressource befindet. Beispiel: Ein Sicherungsserver benötigt möglicherweise das Betriebssystem-Image des zu sichernden Datenbankservers, d. h., der Datenbankserver muss zuerst vorhanden sein.

Eine implizite Abhängigkeit, die auch als Eigenschaftsbindung bezeichnet wird, steuert die Build-Reihenfolge, indem gewartet wird, bis die erforderliche Eigenschaft verfügbar ist. Erst danach wird die abhängige Ressource bereitgestellt. Sie fügen eine implizite Abhängigkeit mithilfe des Code-Editors hinzu.

- Bearbeiten Sie die abhängige Ressource, indem Sie eine Eigenschaft hinzufügen, die die Ressource und die Eigenschaft angibt, die zuerst vorhanden sein müssen.

Eine implizite Abhängigkeit oder Eigenschaftsbindung wird in Form eines gestrichelten Pfeils auf der Arbeitsfläche angegeben.



Vorgehensweise zum Verwenden von Ausdrücken zur flexibleren Gestaltung von Cloud-Vorlagencode in vRealize Automation Cloud Assembly

Zur Steigerung der Flexibilität können Sie dem vRealize Automation Cloud Assembly-Cloud-Vorlagencode Ausdrücke hinzufügen.

In Ausdrücken wird das Konstrukt `${expression}` verwendet, wie in den folgenden Beispielen gezeigt.

Die Beispiele sind so beschnitten, dass nur die wichtigen Zeilen angezeigt werden. Die gesamte unbearbeitete Cloud-Vorlage wird am Ende angezeigt.

Beispiele

Lassen Sie zu, dass der Benutzer zum Zeitpunkt der Bereitstellung den verschlüsselten Schlüssel einfügt, der für den Remote-Zugriff erforderlich ist:

```

inputs:
  sshKey:
    type: string
    maxLength: 500
resources:
  frontend:
    type: Cloud.Machine
    properties:
      remoteAccess:
        authentication: publicPrivateKey
        sshKey: '${input.sshKey}'

```


Für die Bereitstellung von in VMware Cloud on AWS legen Sie den Ordernamen auf den erforderlichen Namen von *Workload* fest:

```
inputs:
  environment:
    type: string
    enum:
      - AWS
      - vSphere
      - Azure
      - VMC
      - GCP
    default: vSphere
resources:
  frontend:
    type: Cloud.Machine
    properties:
      folderName: '${input.environment == "VMC" ? "Workload" : ""}'
```

Versehen Sie zum Zeitpunkt der Bereitstellung die Maschine mit einem nur aus Kleinbuchstaben bestehenden *env*-Tag, das der ausgewählten Umgebung entspricht:

```
inputs:
  environment:
    type: string
    enum:
      - AWS
      - vSphere
      - Azure
      - VMC
      - GCP
    default: vSphere
resources:
  frontend:
    type: Cloud.Machine
    properties:
      constraints:
        - tag: '${"env:" + to_lower(input.environment)}'
```

Legen Sie die Anzahl der Maschinen im Front-End-Cluster auf eine (small) oder zwei (large) fest. Beachten Sie, dass der umfangreiche Cluster durch Löschung festgelegt wird:

```
inputs:
  envsize:
    type: string
    enum:
      - Small
      - Large
resources:
  frontend:
    type: Cloud.Machine
    properties:
      count: '${input.envsize == "Small" ? 1 : 2}'
```

Hängen Sie Maschinen an dasselbe *Standard*netzwerk an, indem Sie sie an die in der Netzwerkressource gefundene Eigenschaft binden:

```
resources:
  frontend:
    type: Cloud.Machine
    properties:
      networks:
        - network: '${resource.Cloud_Network_1.name}'
  apitier:
    type: Cloud.Machine
    properties:
      networks:
        - network: '${resource.Cloud_Network_1.name}'
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      name: Default
      networkType: existing
```

Verschlüsseln Sie die für die API bereitgestellten Zugriffsanmeldedaten:

```
resources:
  apitier:
    type: Cloud.Machine
    properties:
      cloudConfig: |
        #cloud-config
      runcmd:
        - export apikey=${base64_encode(input.username:input.password)}
        - curl -i -H 'Accept:application/json' -H 'Authorization:Basic :$apikey' http://
example.com
```

Ermitteln Sie die Adresse der API-Maschine:

```
resources:
  frontend:
    type: Cloud.Machine
    properties:
      cloudConfig: |
        runcmd:
          - echo ${resource.apitier.networks[0].address}
  apitier:
    type: Cloud.Machine
    properties:
      networks:
        - network: '${resource.Cloud_Network_1.name}'
```

Vollständige Cloud-Vorlage

```

inputs:
  environment:
    type: string
    enum:
      - AWS
      - vSphere
      - Azure
      - VMC
      - GCP
    default: vSphere
  sshKey:
    type: string
    maxLength: 500
  envsize:
    type: string
    enum:
      - Small
      - Large
resources:
  frontend:
    type: Cloud.Machine
    properties:
      folderName: '${input.environment == "VMC" ? "Workload" : ""}'
      image: ubuntu
      flavor: medium
      count: '${input.envsize == "Small" ? 1 : 2}'
      remoteAccess:
        authentication: publicPrivateKey
        sshKey: '${input.sshKey}'
      cloudConfig: |
        packages:
          - nginx
        runcmd:
          - echo ${resource.apitier.networks[0].address}
      constraints:
        - tag: '${"env:" + to_lower(input.environment)}'
      networks:
        - network: '${resource.Cloud_Network_1.name}'
  apitier:
    type: Cloud.Machine
    properties:
      folderName: '${input.environment == "VMC" ? "Workload" : ""}'
      image: ubuntu
      flavor: small
      cloudConfig: |
        #cloud-config
        runcmd:
          - export apikey=$(base64_encode(input.username:input.password))
          - curl -i -H 'Accept:application/json' -H 'Authorization:Basic :$apikey' http://
example.com
      remoteAccess:
        authentication: publicPrivateKey
        sshKey: '${input.sshKey}'

```

```

constraints:
  - tag: '${"env:" + to_lower(input.environment)}'
networks:
  - network: '${resource.Cloud_Network_1.name}'
Cloud_Network_1:
  type: Cloud.Network
  properties:
    name: Default
    networkType: existing
  constraints:
    - tag: '${"env:" + to_lower(input.environment)}'

```

Ausdruckssyntax von Cloud-Vorlagen in vRealize Automation Cloud Assembly

Die Ausdruckssyntax zeigt alle verfügbaren Funktionen von Ausdrücken in vRealize Automation Cloud Assembly-Vorlagen.

Die Syntax wird in den Beispielen unter [Vorgehensweise zum Verwenden von Ausdrücken zur flexibleren Gestaltung von Cloud-Vorlagencode in vRealize Automation Cloud Assembly](#) nur teilweise dargestellt.

Literale

Folgende Literale werden unterstützt:

- Boolesch („true“ oder „false“)
- Ganzzahl
- Gleitkomma
- Zeichenfolge

Der umgekehrte Schrägstrich ist das Escapezeichen für doppeltes Anführungszeichen, einfaches Anführungszeichen und umgekehrten Schrägstrich selbst:

" wird wie folgt mit Escapezeichen geschützt: \"

' wird wie folgt mit Escapezeichen geschützt: \'

\ wird als \\ geschützt

Anführungszeichen müssen in einer Zeichenfolge nur dann mit Escapezeichen versehen werden, wenn die Zeichenfolge in Anführungszeichen desselben Typs eingeschlossen ist, wie im folgenden Beispiel gezeigt.

```
"I am a \"double quoted\" string inside \"double quotes\"."
```

- Null

Umgebungsvariablen

Umgebungsnamen:

- orgId

- `projectId`
- `projectName`
- `deploymentId`
- `deploymentName`
- `blueprintId`
- `blueprintVersion`
- `blueprintName`
- `requestedBy (user)`
- `requestedAt (time)`

Syntax:

```
env.ENV_NAME
```

Beispiel:

```
${env.blueprintId}
```

Ressourcenvariablen

Mithilfe von Ressourcenvariablen können Sie Bindungen mit Ressourceneigenschaften anderer Ressourcen erstellen.

Syntax:

```
resource.RESOURCE_NAME.PROPERTY_NAME
```

Beispiele:

- `${resource.db.id}`
- `${resource.db.networks[0].address}`
- `${resource.app.id}` (Gibt die Zeichenfolge für nicht geclusterte Ressourcen zurück, wobei „count“ nicht angegeben wird. Gibt das Array für geclusterte Ressourcen zurück.)
- `${resource.app[0].id}` (Gibt den ersten Eintrag für geclusterte Ressourcen zurück.)

Ressourcenvariablen vom Typ „Self“

Ressourcenvariablen vom Typ „Self“ sind nur für Ressourcen zulässig, die die Zuteilungsphase unterstützen. Ressourcenvariablen vom Typ „Self“ sind nur verfügbar (oder es wurde nur ein Wert für sie festgelegt), nachdem die Zuteilungsphase abgeschlossen ist.

Syntax:

```
self.property_name
```

Beispiel:

```
${self.address} (Gibt die Adresse zurück, die während der Zuteilungsphase zugewiesen wurde.)
```

Beachten Sie, dass für eine Ressource mit dem Namen `resource_x` `self.property_name` und `resource.resource_x.property_name` gleich sind und beide als Eigenreferenzen betrachtet werden.

Index der Clusteranzahl

Syntax:

```
count.index
```

Beispiel:

`${count.index == 0 ? "primary" : "secondary"}` (Gibt den Knotentyp für geclusterte Ressourcen zurück.)

Beschränkungen:

Die Verwendung von `count.index` für die Ressourcenzuteilung wird nicht unterstützt. Beispiel: Der folgende Kapazitätsausdruck schlägt fehl, wenn er auf die Position innerhalb eines zum Zeitpunkt der Eingabe erstellten Festplatten-Arrays verweist.

```
inputs:
  disks:
    type: array
    minItems: 0
    maxItems: 12
    items:
      type: object
      properties:
        size:
          type: integer
          title: Size (GB)
          minSize: 1
          maxSize: 2048
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: '${input.disks[count.index].size}'
      count: '${length(input.disks)}'
```

Bedingungen

Syntax:

- Gleichheitsoperatoren sind `==` und `!=`.
- Relationale Operatoren sind `<`, `>`, `<=` und `>=`.
- Logische Operatoren sind `&&`, `||` und `!`.
- In Bedingungsausdrücken wird das folgende Muster verwendet:

condition-expression ? true-expression : false-expression

Beispiele:

```
${input.count < 5 && input.size == 'small'}
```

```
${input.count < 2 ? "small" : "large"}
```

Arithmetische Operatoren

Syntax:

Operatoren sind +, -, /, * und %.

Beispiel:

```
${(input.count + 5) * 2}
```

Zeichenfolgenverkettung

Syntax:

```
${'ABC' + 'DEF'} ergibt ABCDEF.
```

Operatoren [] und .

Der Ausdruck folgt bei der Vereinheitlichung der Behandlung der Operatoren [] und . dem ECMAScript.

Also ist `expr.identifizier` äquivalent mit `expr["identifizier"]`. Der Bezeichner wird verwendet, um ein Literal zu konstruieren, dessen Wert der Bezeichner ist, und dann wird der []-Operator mit diesem Wert verwendet.

Beispiel:

```
${resource.app.networks[0].address}
```

Wenn darüber hinaus eine Eigenschaft ein Leerzeichen enthält, trennen Sie sie mit eckigen Klammern und doppelten Anführungszeichen ab, anstatt die Punktnotation zu verwenden.

Falsch:

```
input.operating system
```

Richtig:

```
input["operating system"]
```

Aufbau einer Zuordnung

Syntax:

```
${{'key1':'value1', 'key2':input.key2}}
```

Aufbau eines Arrays

Syntax:

```
${['key1', 'key2']}
```

Beispiel:

```
${[1,2,3]}
```

Funktionen

Syntax:

```
${function(arguments...)}
```

Beispiel:

```
${to_lower(resource.app.name)}
```

Tabelle 6-1. Funktionen

Funktion	Beschreibung
abs(number)	Absoluter Zahlenwert
floor(number)	Gibt den größten (am nächsten an positiv unendlich liegenden) Wert zurück, der kleiner oder gleich dem Argument und gleich einer mathematischen Ganzzahl ist
ceil(number)	Gibt den kleinsten (am nächsten an negativ unendlich liegenden) Wert zurück, der größer oder gleich dem Argument und gleich einer mathematischen Ganzzahl ist
to_lower(str)	Konvertiert eine Zeichenfolge in Kleinbuchstaben
to_upper(str)	Konvertiert eine Zeichenfolge in Großbuchstaben
contains(array, value)	Überprüft, ob ein Array einen bestimmten Wert enthält
contains(string, value)	Überprüft, ob eine Zeichenfolge einen bestimmten Wert enthält
join(array, delim)	Verknüpft ein Array von Zeichenfolgen mit einem Trennzeichen und gibt eine Zeichenfolge zurück
split(string, delim)	Teilt eine Zeichenfolge mit Trennzeichen und gibt ein Array von Zeichenfolgen zurück
slice(array, begin, end)	Gibt ein Segment eines Arrays vom Anfangsindex bis zum Endindex zurück
reverse(array)	Kehrt die Reihenfolge der Einträge eines Arrays um
starts_with(subject, prefix)	Überprüft, ob die Zeichenfolge mit einer bestimmten Präfixzeichenfolge beginnt
ends_with(subject, suffix)	Überprüft, ob die Zeichenfolge mit einer bestimmten Suffixzeichenfolge endet
replace(string, target, replacement)	Ersetzt die Zeichenfolge, die die Zielzeichenfolge enthält, mit der Zielzeichenfolge
substring(string, begin, end)	Gibt eine Teilzeichenfolge der Zeichenfolge vom Anfangsindex bis zum Endindex zurück
format(format, values...)	Gibt eine formatierte Zeichenfolge unter Verwendung des Class Formatter -Formats und der zugehörigen Werte von Java zurück.
keys(map)	Gibt die Schlüssel der Zuordnung zurück
values(map)	Gibt die Werte der Zuordnung zurück

Tabelle 6-1. Funktionen (Fortsetzung)

Funktion	Beschreibung
merge(map, map)	Gibt eine zusammengeführte Zuordnung zurück
length(string)	Gibt die Zeichenfolgenlänge zurück
length(array)	Gibt die Array-Länge zurück
max(array)	Gibt den maximalen Wert aus einem Array von Zahlen zurück
min(array)	Gibt den Mindestwert aus einem Array von Zahlen zurück
sum(array)	Gibt die Summe aller Werte aus einem Array von Zahlen zurück
avg(array)	Gibt den Durchschnittswert aller Werte aus einem Array von Zahlen zurück
digest(value, type)	Gibt einen Digest des Werts unter Verwendung des unterstützten Typs (md5, sha1, sha256, sha384, sha512) zurück
to_string(value)	Gibt eine Zeichenfolgendarstellung des Werts zurück
to_number(string)	Analysiert eine Zeichenfolge als Zahl
not_null(array)	Gibt den ersten Eintrag zurück, der nicht null ist
base64_encode(string)	Gibt einen base64-codierten Wert zurück
base64_decode(string)	Gibt einen decodierten base64-Wert zurück
now()	Gibt die aktuelle Uhrzeit im Format ISO-8601 zurück
uuid()	Gibt eine zufallsgenerierte UUID zurück
from_json(string)	Analysiert eine JSON-Zeichenfolge
to_json(value)	Serialisiert einen Wert als JSON-Zeichenfolge
json_path(value, path)	Wertet den Pfad anhand des Werts unter Verwendung von XPath for JSON aus.
matches(string, regex)	Überprüft, ob die Zeichenfolge mit einem Regex-Ausdruck übereinstimmt
url_encode(string)	Codiert eine Zeichenfolge unter Verwendung der URL-Codierungsspezifikation
trim(string)	Entfernt vorangestellte und nachgestellte Leerzeichen

Vorgehensweise zum Aktivieren des Remotezugriffs in vRealize Automation Cloud Assembly-Vorlagen

Für den Remotezugriff auf eine von vRealize Automation Cloud Assembly bereitgestellte Maschine fügen Sie vor der Bereitstellung Eigenschaften zur Cloud-Vorlage für diese Maschine hinzu.

Für den Remotezugriff können Sie eine der folgenden Authentifizierungsoptionen konfigurieren.

Hinweis Wenn Schlüssel kopiert werden müssen, können Sie auch einen cloudConfig-Abschnitt in der Cloud-Vorlage erstellen, um die Schlüssel bei der Bereitstellung automatisch zu kopieren. Die Spezifikationen sind hier nicht dokumentiert. Unter [Vorgehensweise zum automatischen Initialisieren einer Maschine in einer vRealize Automation Cloud Assembly-Vorlage](#) finden Sie jedoch allgemeine Informationen zu cloudConfig.

Erzeugen eines Schlüsselpaars zur vRealize Automation Cloud Assembly-Bereitstellungszeit

Wenn Sie nicht über ein eigenes öffentliches/privates Schlüsselpaar für die RAS-Authentifizierung verfügen, können Sie vRealize Automation Cloud Assembly veranlassen, ein Schlüsselpaar zu erzeugen.

Verwenden Sie den folgenden Code als Richtlinie.

- 1 Fügen Sie vor der Bereitstellung in vRealize Automation Cloud Assembly `remoteAccess`-Eigenschaften zur Cloud-Vorlage hinzu, wie im Beispiel gezeigt.

Der Benutzername ist optional. Wenn Sie ihn weglassen, erzeugt das System eine zufällige ID als Benutzernamen.

Beispiel:

```
type: Cloud.Machine
properties:
  name: our-vm2
  image: Linux18
  flavor: small
  remoteAccess: authentication: generatedPublicPrivateKey username: testuser
```

- 2 Stellen Sie in vRealize Automation Cloud Assembly die Maschine aus der zugehörigen Cloud-Vorlage bereit und weisen Sie ihr den Status „Gestartet“ zu.
- 3 Suchen Sie in den Eigenschaften **Bereitstellungen > Topologie** nach dem Schlüsselnamen.
- 4 Verwenden Sie die Cloud-Anbieter-Oberfläche, wie beispielsweise den vSphere Client, um auf die Befehlszeile der bereitgestellten Maschine zuzugreifen.

Der Bereitstellungsvorgang erzeugt die Schlüssel.

- 5 Erteilen Sie dem privaten Schlüssel Leseberechtigungen.

```
chmod 600 key-name
```

- 6 Navigieren Sie zur vRealize Automation Cloud Assembly-Bereitstellung, wählen Sie die Maschine aus und klicken Sie auf **Aktionen > Privaten Schlüssel abrufen**.

- 7 Kopieren Sie die Datei des privaten Schlüssels auf Ihre lokale Maschine.

Ein typischer lokaler Dateipfad lautet `/home/username/.ssh/key-name`.

- Öffnen Sie eine SSH-Remote-Sitzung und stellen Sie eine Verbindung zur bereitgestellten Maschine her.

```
ssh -i key-name user-name@machine-ip
```

Bereitstellen des eigenen öffentlichen/privaten Schlüsselpaars in vRealize Automation Cloud Assembly

Viele Unternehmen erstellen und verteilen eigene öffentliche/private Schlüsselpaare für die Authentifizierung.

Verwenden Sie den folgenden Code als Richtlinie.

- Rufen Sie in der lokalen Umgebung Ihr öffentliches/privates Schlüsselpaar ab oder erzeugen Sie es.

Im Moment müssen Sie die Schlüssel nur lokal erzeugen und speichern.

- Fügen Sie vor der Bereitstellung in vRealize Automation Cloud Assembly `remoteAccess`-Eigenschaften zur Cloud-Vorlage hinzu, wie im Beispiel gezeigt.

`sshKey` enthält den langen alphanumerischen Wert, der innerhalb der öffentlichen Schlüsseldatei `key-name.pub` gefunden wurde.

Der Benutzername ist optional und wird erstellt, damit Sie sich anmelden können. Wenn Sie ihn weglassen, erzeugt das System eine zufällige ID als Benutzernamen.

Beispiel:

```
type: Cloud.Machine
properties:
  name: our-vm1
  image: Linux18
  flavor: small
  remoteAccess:
    authentication: publicPrivateKey
    sshKey: ssh-rsa Iq+5aQgBP3ZNT4o1baP5Ii+dstIcowRRkyobbfpA1mj9ts1f
qGxvU66PX9IeZax5hZvNWFgjw6ag+Z1zndOLhVdVoW49f274/mIRild7UUW...
    username: testuser
```

- Stellen Sie in vRealize Automation Cloud Assembly die Maschine aus der zugehörigen Cloud-Vorlage bereit und weisen Sie ihr den Status „Gestartet“ zu.
- Greifen Sie mit dem Client des Cloud-Anbieters auf die bereitgestellte Maschine zu.
- Fügen Sie die Datei des öffentlichen Schlüssels zum Stammordner auf der Maschine hinzu. Verwenden Sie den Schlüssel, den Sie in `remoteAccess.sshKey` angegeben haben.
- Stellen Sie sicher, dass das Gegenstück zur privaten Schlüsseldatei auf Ihrem lokalen Computer vorhanden ist.

Der Schlüssel lautet in der Regel `/home/username/.ssh/key-name` ohne die PUB-Erweiterung.

- Öffnen Sie eine SSH-Remote-Sitzung und stellen Sie eine Verbindung zur bereitgestellten Maschine her.

```
ssh -i key-name user-name@machine-ip
```

Bereitstellen eines AWS-Schlüsselpaars in vRealize Automation Cloud Assembly

Durch Hinzufügen eines AWS-Schlüsselpaarnamens zur Cloud-Vorlage können Sie remote auf eine Maschine zugreifen, die von vRealize Automation Cloud Assembly für AWS bereitgestellt wird.

Beachten Sie, dass AWS-Schlüsselpaare regionsspezifisch sind. Wenn Sie Arbeitslasten in us-east-1 bereitstellen, muss das Schlüsselpaar in us-east-1 vorhanden sein.

Verwenden Sie den folgenden Code als Richtlinie. Diese Option steht nur für AWS-Cloud-Zonen zur Verfügung.

```
type: Cloud.Machine
properties:
  image: Ubuntu
  flavor: small
  remoteAccess: authentication: keyPairName keyPair: cas-test
constraints:
  - tag: 'cloud:aws'
```

Angeben eines Benutzernamens und Kennworts in vRealize Automation Cloud Assembly

Durch Hinzufügen eines Benutzernamens und Kennworts zur Cloud-Vorlage erhalten Sie einfachen Remote-Zugriff auf eine Maschine, die von vRealize Automation Cloud Assembly bereitgestellt wird.

Obwohl die Remoteanmeldung mit Benutzername und Kennwort weniger sicher ist, kann sie in Ihrer Situation unter Umständen notwendig sein. Denken Sie daran, dass bestimmte Cloud-Anbieter oder Konfigurationen diese weniger sichere Option unter Umständen nicht unterstützen.

- 1 Fügen Sie vor der Bereitstellung in vRealize Automation Cloud Assembly `remoteAccess-`Eigenschaften zur Cloud-Vorlage hinzu, wie im Beispiel gezeigt.

Legen Sie den Benutzernamen und das Kennwort für das Konto fest, mit dem Sie sich wahrscheinlich anmelden werden.

Beispiel:

```
type: Cloud.Machine
properties:
  name: our-vm3
  image: Linux18
  flavor: small
  remoteAccess: authentication: usernamePassword username: testuser password: admin123
```

- 2 Stellen Sie in vRealize Automation Cloud Assembly die Maschine aus der zugehörigen Cloud-Vorlage bereit und weisen Sie ihr den Status „Gestartet“ zu.
- 3 Navigieren Sie zur Schnittstelle Ihres Cloud-Anbieters und greifen Sie auf die bereitgestellte Maschine zu.

- 4 Erstellen oder aktivieren Sie das Konto auf der bereitgestellten Maschine.
- 5 Öffnen Sie über Ihren lokalen Computer eine Remotesitzung anhand der IP-Adresse oder des FQDN der bereitgestellten Maschine und melden Sie sich wie gewohnt mit dem Benutzernamen und Kennwort an.

Vorgehensweise zum Hinzufügen von erweiterten Funktionen zu vRealize Automation Cloud Assembly-Designs

Es gibt erweiterte „Infrastructure-as-Code“-Techniken und vRealize Automation Cloud Assembly-Funktionen, die die Unternehmensbereitschaft Ihrer Designs verstärken.

Einige der hier beschriebenen Funktionen erweitern die Designfunktionen von vRealize Automation Cloud Assembly, während andere direkt für die Cloud-Vorlagen-Codierungsmethoden gelten.

Vorgehensweise zum Anpassen der Namen bereitgestellter Ressourcen mithilfe von vRealize Automation Cloud Assembly

Als Cloud- oder Projektadministrator verfügen Sie über eine vorgeschriebene Benennungskonvention für Ressourcen in Ihrer Umgebung, und Sie möchten, dass die bereitgestellte Ressource diese Konvention ohne Benutzereingriff befolgt. Sie können eine Benennungsvorlage für alle Bereitstellungen aus einem vRealize Automation Cloud Assembly-Projekt erstellen.

Beispielsweise besteht Ihre Host-Benennungskonvention darin, eine Ressource mit einem Präfix wie *projectname-sitecode-costcenter-whereDeployed-identifier* zu versehen. Sie konfigurieren die benutzerdefinierte Benennungsvorlage für die Maschinen für jedes Projekt. Einige der Vorlagenvariablen werden während der Bereitstellung aus dem System abgerufen, andere basieren auf benutzerdefinierten Eigenschaften des Projekts. Die benutzerdefinierte Benennungsvorlage für das oben angegebene Präfix ähnelt dem folgenden Beispiel.

```
${project.name}-${resource.siteCode}-${resource.costCenter}-${endpoint.name}-${#####}
```

Der in der Vorlagen als `${#####}` angegebene Bezeichner ist sechsstellig. Der Bezeichner ist ein Indikator bzw. ein Zähler, der die Eindeutigkeit sicherstellt. Als globaler Indikator für die Organisation erhöht er sich schrittweise für alle Projekte, nicht nur für das aktuelle Projekt. Wenn Sie mehrere Projekte haben, erwarten Sie für Bereitstellungen in Ihrem aktuellen Projekt keine Erhöhung von 000123 auf die folgende Zahl 000124. Sie können vielmehr eine Erhöhung von 000123 auf 000127 erwarten.

Alle Ressourcennamen müssen eindeutig sein. Mit der Eigenschaft „inkrementelle Zahl“ können Sie die Eindeutigkeit gewährleisten. Die Zahlen werden für alle Bereitstellungen inkrementiert, einschließlich der von vRealize Automation Cloud Assembly benannten Bereitstellungen. Weil das System robuster wird und die benutzerdefinierte Benennung auf viele Ressourcen angewendet

wird, wie z. B. virtuelle Maschinen, Lastausgleichsdienste, Sicherheitsgruppen, NATs, Gateways, Ressourcengruppen und Festplatten, kann die Nummerierung zufällig erscheinen, die Werte sind jedoch weiterhin eindeutig. Die Nummerierung erhöht sich auch, wenn Sie eine Testbereitstellung ausführen.

Neben den hier angegebenen Beispielen können Sie auch den Benutzernamen, das verwendete Image, andere integrierte Optionen und einfache Zeichenfolgen hinzufügen. Beim Erstellen der Vorlage werden Hinweise zu möglichen Optionen angegeben.

Beachten Sie, dass es sich bei einigen der angezeigten Werte nur um Anwendungsfallbeispiele handelt. Sie können diese nicht eins zu eins auf Ihre Umgebung übertragen. Überlegen Sie sich, wo Sie Ihre eigenen Ersetzungen vornehmen würden, oder übernehmen Sie eine Hochrechnung aus den Beispielwerten, um die Anforderungen an die Verwaltung Ihrer eigenen Cloud-Infrastruktur und -Bereitstellung zu erfüllen.

Voraussetzungen

- Sie müssen die Benennungskonvention kennen, die Sie für Bereitstellungen aus einem Projekt verwenden möchten.
- Bei diesem Verfahren wird davon ausgegangen, dass Sie eine einfache Cloud-Vorlage erstellt haben oder erstellen können, mit dem Sie Ihre benutzerdefinierte Host-Präfixbenennung testen.

Verfahren

- 1 Klicken Sie auf **Infrastruktur > Projekte**.
- 2 Wählen Sie ein vorhandenes Projekt aus oder erstellen Sie ein neues Projekt.
- 3 Suchen Sie auf der Registerkarte **Bereitstellung** den Abschnitt „Benutzerdefinierte Eigenschaften“ und erstellen Sie die Eigenschaften für den Site-Code und die Kostenstellenwerte.

Hier können Sie die angezeigten Werte durch die passenden Werte für Ihre Umgebung ersetzen.

Benutzerdefinierte Eigenschaften
Geben Sie die benutzerdefinierten Eigenschaften an, die allen Anforderungen in diesem Projekt hinzugefügt werden sollen. ①

Benutzerdefinierte Eigenschaften festlegen	Name	Wert
	siteCode	BGL
	costCenter	IT-research

Benutzerdefinierte Benennung
Geben Sie die Benennungsvorlage an, die für in diesem Projekt bereitgestellte Maschinen, Netzwerke, Sicherheitsgruppen und Festplatten verwendet werden soll.

Vorlage: `${project.name}-${resource.siteCode}-${resource` ①
Hint: Avoid conflicting names by generating digits in names. `#{#####}`

- a Erstellen Sie eine benutzerdefinierte Eigenschaft mit dem Namen **siteCode** und dem Wert **BGL**.
 - b Fügen Sie eine weitere benutzerdefinierte Eigenschaft mit dem Namen **costCenter** und dem Wert **IT-Research** hinzu.
- 4 Suchen Sie den Abschnitt „Benutzerdefinierte Benennung“ und fügen Sie die folgende Vorlage hinzu.

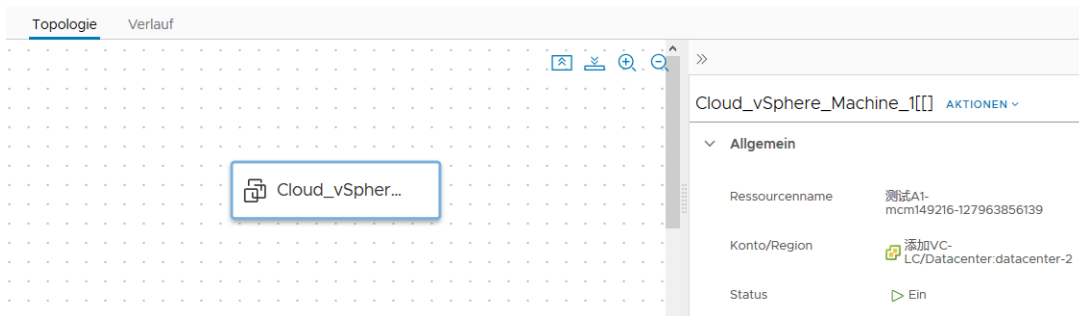
```
${project.name}-${resource.siteCode}-${resource.costCenter}-${endpoint.name}-${#####}
```

Sie können zwar die Zeichenfolge hineinkopieren, aber wenn es sich um Ihre erste Benennungsvorlage handelt, empfiehlt es sich unter Umständen, beim Erstellen der Vorlage den Hinweistext und die Schnellauswahl zu verwenden.

- 5 Stellen Sie eine Cloud-Vorlage bereit, die dem Projekt zugeordnet ist, um zu überprüfen, ob der benutzerdefinierte Name auf die Ressource angewendet wird.
 - a Klicken Sie auf die Registerkarte **Design** und dann auf eine Cloud-Vorlage, die dem Projekt zugeordnet ist.
 - b Stellen Sie die Cloud-Vorlage bereit.

Die Registerkarte **Bereitstellungen** wird geöffnet. Darauf wird Ihre in Bearbeitung befindliche Bereitstellung angezeigt.

- c Wenn die Bereitstellung abgeschlossen ist, klicken Sie auf den Namen der Bereitstellung.
- d Beachten Sie auf der Registerkarte **Topologie** im rechten Fensterbereich, dass Ihr benutzerdefinierter Name der Ressourcenname ist.



- 6 Wenn Sie eine Test-Cloud-Vorlagen zur Überprüfung der Benennungskonvention bereitgestellt haben, können Sie die Bereitstellung löschen.

Nächste Schritte

Erstellen Sie benutzerdefinierte Benennungsvorlagen für Ihre anderen Projekte.

Vorgehensweise zum automatischen Initialisieren einer Maschine in einer vRealize Automation Cloud Assembly-Vorlage

Sie können die Maschineninitialisierung in vRealize Automation Cloud Assembly anwenden, indem Sie Befehle direkt ausführen, oder wenn Sie die Bereitstellung in vSphere-basierten Cloud-Zonen mithilfe von Anpassungsspezifikationen vornehmen.

- Befehle – Ein cloudConfig-Abschnitt in Ihrem Cloud-Vorlagencode enthält die Befehle, die Sie ausführen möchten.
- Anpassungsspezifikationen – Eine Eigenschaft in Ihrem Cloud-Vorlagencode verweist anhand des Namens auf eine vSphere-Anpassungsspezifikation.

Befehle und Anpassungsspezifikationen lassen sich möglicherweise nicht kombinieren

Gehen Sie beim Bereitstellen auf vSphere umsichtig vor, wenn Sie versuchen, cloudConfig mit der Initialisierung der Anpassungsspezifikation zu kombinieren. Sie sind in formaler Hinsicht nicht kompatibel und verursachen möglicherweise inkonsistente oder unerwünschte Ergebnisse, wenn sie gemeinsam verwendet werden.

Ein Beispiel dafür, wie Befehle und Anpassungsspezifikationen interagieren, finden Sie unter [Zuweisung statischer IP-Adressen für vSphere in vRealize Automation Cloud Assembly-Cloud-Vorlagen](#).

vSphere-Anpassungsspezifikationen in vRealize Automation Cloud Assembly-Vorlagen

Bei der Bereitstellung in vSphere-Cloud-Zonen können Anpassungsspezifikationen Einstellungen des Gastbetriebssystems zum Zeitpunkt der Bereitstellung anwenden.

Vorgehensweise zum Aktivieren der Anpassungsspezifikation

Die Anpassungsspezifikation muss in vSphere auf dem Ziel vorhanden sein, auf dem die Bereitstellung erfolgt.

Bearbeiten Sie den Cloud-Vorlagencode direkt. Das folgende Beispiel verweist auf eine `cloud-assembly-linux`-Anpassungsspezifikation für einen WordPress-Host auf vSphere.

```
resources:
  WebTier:
    type: Cloud.vSphere.Machine
    properties:
      name: wordpress
      cpuCount: 2
      totalMemoryMB: 1024
      imageRef: 'Template: ubuntu-18.04'
      customizationSpec: 'cloud-assembly-linux'
      resourceGroupName: '/Datacenters/Datacenter/vm/deployments'
```

Entscheidung, ob Anpassungsspezifikationen oder cloudConfig-Befehle verwendet werden

Wenn die Bereitstellungserfahrung mit den derzeit von Ihnen in vSphere durchgeführten Aktionen übereinstimmen soll, ist die Verwendung von Anpassungsspezifikationen möglicherweise der beste Ansatz. Um jedoch eine Erweiterung auf eine Hybrid-Bereitstellung oder eine Bereitstellung mit mehreren Clouds durchzuführen, besteht ein neutralerer Ansatz in cloudConfig-Initialisierungsbefehlen.

Weitere Informationen zu cloudConfig-Abschnitten in Cloud-Vorlagen finden Sie unter [Konfigurationsbefehle in vRealize Automation Cloud Assembly-Vorlagen](#).

Befehle und Anpassungsspezifikationen lassen sich möglicherweise nicht kombinieren

Gehen Sie bei der Bereitstellung in vSphere umsichtig vor, wenn Sie versuchen, einen eingebetteten cloudConfig-Befehl mit der Initialisierung der Anpassungsspezifikation zu kombinieren. Sie sind in formaler Hinsicht nicht kompatibel und verursachen möglicherweise inkonsistente oder unerwünschte Ergebnisse, wenn sie gemeinsam verwendet werden.

Ein Beispiel dafür, wie Befehle und Anpassungsspezifikationen interagieren, finden Sie unter [Zuweisung statischer IP-Adressen für vSphere in vRealize Automation Cloud Assembly-Cloud-Vorlagen](#).

Konfigurationsbefehle in vRealize Automation Cloud Assembly-Vorlagen

Sie können einen cloudConfig-Abschnitt im vRealize Automation Cloud Assembly-Vorlagencode einfügen, dem Sie zur Bereitstellungszeit auszuführende Initialisierungsbefehle für Maschinen hinzufügen.

Art und Weise, wie cloudConfig-Befehle gebildet werden

- Linux – Initialisierungsbefehle folgen dem offenen [cloud-init](#)-Standard.
- Windows – Initialisierungsbefehle verwenden [Cloudbase-init](#).

Linux [cloud-init](#) und Windows [Cloudbase-init](#) verwenden nicht dieselbe Syntax. Ein cloudConfig-Abschnitt für ein Betriebssystem funktioniert nicht in einem Maschinen-Image des anderen Betriebssystems.

Anwendungsmöglichkeiten von cloudConfig-Befehlen

Sie verwenden Initialisierungsbefehle, um die Anwendung von Daten oder Einstellungen zum Zeitpunkt der Instanzerstellung zu automatisieren, wodurch Benutzer, Berechtigungen, Installationen oder andere befehlsbasierte Vorgänge angepasst werden können. Zu den Beispielen gehören:

- Festlegen eines Hostnamens
- Erstellen und Einrichten von privaten SSH-Schlüsseln
- Installieren von Paketen

Möglichkeiten für das Hinzufügen von cloudConfig-Befehlen

Sie können einen cloudConfig-Abschnitt dem Cloud-Vorlagencode hinzufügen, aber Sie können einen solchen Abschnitt auch im Voraus einem Maschinen-Image hinzufügen, wenn Sie die Infrastruktur konfigurieren. Alle Cloud-Vorlagen, die auf dieses Quell-Image verweisen, erhalten dieselbe Initialisierung.

Möglicherweise verfügen Sie über eine Image-Zuordnung und eine Cloud-Vorlage, die beide Initialisierungsbefehle enthalten. Zum Zeitpunkt der Bereitstellung werden die Befehle zusammengeführt. Die konsolidierten Befehle werden dann von vRealize Automation Cloud Assembly ausgeführt.

Wenn derselbe Befehl an beiden Positionen angezeigt wird, aber unterschiedliche Parameter enthält, wird nur der Image-Zuordnungsbefehl ausgeführt.

Zusätzliche Informationen hierzu finden Sie unter [Weitere Informationen zu Image-Zuordnungen in vRealize Automation](#).

Beispiel für cloudConfig-Befehle

Der folgende cloudConfig-Beispielabschnitt stammt aus dem Cloud-Vorlagencode des [Erstellen einer einfachen Cloud-Vorlage](#) für den Linux-basierten MySQL-Server.

Hinweis Um die korrekte Interpretation von Befehlen zu gewährleisten, fügen Sie immer einen senkrechten Strich (cloudConfig: |) hinzu, wie in der Abbildung gezeigt.

```
cloudConfig: |
  #cloud-config
  repo_update: true
  repo_upgrade: all
  packages:
    - apache2
    - php
    - php-mysql
    - libapache2-mod-php
    - php-mcrypt
    - mysql-client
  runcmd:
    - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
      https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
      mywordpresssite --strip-components 1
    - i=0; while [ $i -le 5 ]; do mysql --connect-timeout=3 -h $
      {DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;
      i=$((i+1)); done
    - mysql -u root -pmysqlpassword -h ${DBTier.networks[0].address} -e "create database
      wordpress_blog;"
    - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/
      mywordpresssite/wp-config.php
    - sed -i -e s/"define( 'DB_NAME', 'database_name_here' );"/"define( 'DB_NAME',
      'wordpress_blog' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
      -i -e s/"define( 'DB_USER', 'username_here' );"/"define( 'DB_USER',
      'root' );"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
      -e s/"define( 'DB_PASSWORD', 'password_here' );"/"define( 'DB_PASSWORD',
      'mysqlpassword' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
      -i -e s/"define( 'DB_HOST', 'localhost' );"/"define( 'DB_HOST', '$
      {DBTier.networks[0].address}' );"/ /var/www/html/mywordpresssite/wp-config.php
    - service apache2 reload
```

Wenn ein cloud-init-Skript unerwartetes Verhalten aufweist, überprüfen Sie die erfasste Konsolenausgabe in `/var/log/cloud-init-output.log` zur Fehlerbehebung. Weitere Informationen zu cloud-init finden Sie in der [cloud-init-Dokumentation](#).

Befehle und Anpassungsspezifikationen lassen sich möglicherweise nicht kombinieren

Gehen Sie bei der Bereitstellung in vSphere umsichtig vor, wenn Sie versuchen, einen eingebetteten cloudConfig-Befehl mit der Initialisierung der Anpassungsspezifikation zu kombinieren. Sie sind in formaler Hinsicht nicht kompatibel und verursachen möglicherweise inkonsistente oder unerwünschte Ergebnisse, wenn sie gemeinsam verwendet werden.

Ein Beispiel dafür, wie Befehle und Anpassungsspezifikationen interagieren, finden Sie unter [Zuweisung statischer IP-Adressen für vSphere in vRealize Automation Cloud Assembly-Cloud-Vorlagen](#).

Zuweisung statischer IP-Adressen für vSphere in vRealize Automation Cloud Assembly-Cloud-Vorlagen

Bei der Bereitstellung in vSphere können Sie eine statische IP-Adresse zuweisen, müssen jedoch darauf achten, dass keine Konflikte zwischen cloudConfig-Initialisierungsbefehlen und Anpassungsspezifikationen entstehen.

Beispieldesigns

In den folgenden Designs wird auf sichere Art und Weise eine statische IP-Adresse angewendet, ohne dass Konflikte zwischen Initialisierungsbefehlen für Cloud-Vorlagen und Anpassungsspezifikationen auftreten. Alle enthalten die Netzwerkeinstellung `assignment: static`.

Design	Beispiel für Cloud-Vorlagencode
<p>Zuweisen einer statischen IP-Adresse zu einer Linux-Maschine, für die kein cloud-init-Code verfügbar ist</p>	<pre>resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: linux-template networks: - name: '\${wpnet.name}' assignment: static network: '\${resource.wpnet.id}'</pre>
<p>Weisen Sie einer Linux-Maschine mit cloud-init-Code, der keine Netzwerkzuweisungsbefehle enthält, eine statische IP-Adresse zu.</p> <p>HINWEIS: Die vSphere-Anpassungsspezifikation wird angewendet, unabhängig davon, ob Sie die Eigenschaft „customizeGuestOs“ auf „true“ festlegen oder die Eigenschaft „customizeGuestOs“ weglassen.</p>	<p>Ubuntu-Beispiel</p> <pre>resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu-template customizeGuestOs: true cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: root:Pa\$\$w0rd expire: false write_files: - path: /tmpFile.txt content: \${resource.wpnet.dns} runcmd: - hostnamectl set-hostname --pretty \${self.resourceName} - touch /etc/cloud/cloud-init.disabled networks: - name: '\${wpnet.name}' assignment: static network: '\${resource.wpnet.id}'</pre> <p>CentOS-Beispiel</p> <pre>resources: wpnet: type: Cloud.Network properties:</pre>

Design**Beispiel für Cloud-Vorlagencode**

```
name: wpnet
networkType: public
constraints:
  - tag: sqa
DBTier:
type: Cloud.vSphere.Machine
properties:
  flavor: small
  image: centos-template
  customizeGuestOs: true
  cloudConfig: |
    #cloud-config
    write_files:
      - path: /test.txt
        content: |
          deploying in power off.
          then rebooting.
networks:
  - name: '${wpnet.name}'
    assignment: static
    network: '${resource.wpnet.id}'
```

Design	Beispiel für Cloud-Vorlagencode
<p>Weisen Sie einer Linux-Maschine mit cloud-init-Code, der Netzwerkzuweisungsbefehle enthält, eine statische IP-Adresse zu.</p> <p>Die Eigenschaft „customizeGuestOs“ muss „false“ sein.</p>	<p>Ubuntu-Beispiel</p> <pre> resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu-template customizeGuestOs: false cloudConfig: #cloud-config write_files: - path: /etc/netplan/99-installer- config.yaml content: network: version: 2 renderer: networkd ethernet: ens160: addresses: - \${resource.DBTier.networks[0].address}/\${ {resource.wpnet.prefixLength} gateway4: \$ {resource.wpnet.gateway} nameservers: search: \$ {resource.wpnet.dnsSearchDomains} addresses: \${resource.wpnet.dns} runcmd: - netplan apply - hostnamectl set-hostname --pretty \$ {self.resourceName} - touch /etc/cloud/cloud-init.disabled networks: - name: '\${wpnet.name}' assignment: static network: '\${resource.wpnet.id}' </pre> <p>CentOS-Beispiel</p> <pre> resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: centos-template </pre>

Design**Beispiel für Cloud-Vorlagencode**

```

customizeGuestOs: false
cloudConfig: |
  #cloud-config
  ssh_pwauth: yes
  chpasswd:
    list: |
      root:VMware1!
    expire: false
  runcmd:
    - nmcli con add type
ethernet con-name 'custom ens192'
ifname ens192 ip4 ${self.networks[0].address}/
${resource.wpnet.prefixLength} gw4 $
{resource.wpnet.gateway}
  - nmcli con mod 'custom ens192' ipv4.dns "$
{join(resource.wpnet.dns, ' ')}"
  - nmcli con mod 'custom ens192' ipv4.dns-
search "${join(resource.wpnet.dnsSearchDomains, ',')}"
  - nmcli con down 'System ens192' ; nmcli
con up 'custom ens192'
  - nmcli con del 'System ens192'
  - hostnamectl set-hostname --static `dig -x
${self.networks[0].address} +short | cut -d "." -f 1`
  - hostnamectl set-hostname --pretty $
{self.resourceName}
  - touch /etc/cloud/cloud-init.disabled
networks:
  - name: '${wpnet.name}'
    assignment: static
    network: '${resource.wpnet.id}'

```

Wenn die Bereitstellung auf einem referenzierten Image beruht, weisen Sie einer Linux-Maschine mit cloud-init-Code, der Netzwerkzuweisungsbefehle enthält, eine statische IP-Adresse zu.

Die Eigenschaft „customizeGuestOs“ muss „false“ sein.

Darüber hinaus darf die Cloud-Vorlage nicht die Eigenschaft „ovfProperties“ enthalten, die die Anpassung blockiert.

```

resources:
  wpnet:
    type: Cloud.Network
    properties:
      name: wpnet
      networkType: public
      constraints:
        - tag: sqa
  DBTier:
    type: Cloud.vSphere.Machine
    properties:
      flavor: small

imageRef: 'https://cloud-images.ubuntu.com/releases/focal/release/ubuntu-20.04-server-cloudimg-amd64.ova'
customizeGuestOs: false
cloudConfig: |
  #cloud-config
  ssh_pwauth: yes
  chpasswd:
    list: |
      root:Pa$$w0rd
      ubuntu:Pa$$w0rd
    expire: false
  write_files:
    - path: /etc/netplan/99-netcfg-vrac.yaml
      content: |
        network:
          version: 2
          renderer: networkd

```


Design**Beispiel für Cloud-Vorlagencode**

```

ethernets:
  ens192:
    dhcp4: no
    dhcp6: no
    addresses:
      - ${resource.DBTier.networks[0].address}/${
        {resource.wpnet.prefixLength}
        gateway4: $
        {resource.wpnet.gateway}
        nameservers:
          search: $
          {resource.wpnet.dnsSearchDomains}
          addresses: ${resource.wpnet.dns}
    runcmd:
      - netplan apply
      - hostnamectl set-hostname --pretty $
        {self.resourceName}
      - touch /etc/cloud/cloud-init.disabled
  networks:
    - name: '${wpnet.name}'
      assignment: static
      network: '${resource.wpnet.id}'

```

Designs, die nicht funktionieren oder zu unerwünschten Ergebnissen führen können

- Der cloud-init-Code enthält keine Netzwerkzuweisungsbefehle, und die Eigenschaft „customizeGuestOs“ ist „false“.

Es sind weder Initialisierungsbefehle noch Anpassungsspezifikationen zum Konfigurieren der Netzwerkeinstellungen vorhanden.

- Der cloud-init-Code enthält keine Netzwerkzuweisungsbefehle, und die Eigenschaft „ovfProperties“ ist festgelegt.

Initialisierungsbefehle sind nicht vorhanden, aber „ovfProperties“ hat die Anpassungsspezifikation blockiert.

- Der cloud-init-Code enthält Netzwerkzuweisungsbefehle, und die Eigenschaft „customizeGuestOs“ fehlt oder ist auf „true“ festgelegt.

Die Anwendung der Anpassungsspezifikation steht in Konflikt mit Initialisierungsbefehlen.

Andere Problemumgehungen für cloud-init und Anpassungsspezifikationen

Bei der Bereitstellung in vSphere können Sie ein Image auch so anpassen, dass Konflikte mit cloud-init und Anpassungsspezifikationen umgangen werden können. Weitere Informationen finden Sie im folgenden externen Repository.

- [vSphere Image Preparation Scripts](#)

Vorgehensweise zum Warten auf die Initialisierung einer vRealize Automation Cloud Assembly-Bereitstellung

In bestimmten Fällen muss eine virtuelle Maschine vollständig gestartet werden, bevor mit der vRealize Automation Cloud Assembly-Bereitstellung fortgefahren wird.

Das Bereitstellen einer Maschine, auf der noch Pakete installiert und ein Webserver gestartet werden, kann beispielsweise dazu führen, dass ein vorschneller Benutzer versucht, eine Anwendung zu öffnen, bevor sie verfügbar ist.

Stellen Sie bei Verwendung dieser Funktion folgende Überlegungen an.

- Die Funktion verwendet das Modul `cloud-init phone_home` und ist verfügbar, wenn Linux-Maschinen bereitgestellt werden.
- `Phone_home` steht für Windows aufgrund von `Cloudbase-init`-Einschränkungen nicht zur Verfügung.
- `Phone_home` kann sich wie eine explizite Abhängigkeit auf die Bereitstellungsreihenfolge auswirken, ist aber flexibler im Hinblick auf Zeitplanungs- und Verarbeitungsoptionen.

Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Festlegen der Reihenfolge der Ressourcenbereitstellung in vRealize Automation Cloud Assembly](#).

- Für `phone_home` ist in der Cloud-Vorlage ein `cloudConfig`-Abschnitt erforderlich.
- Ihre Kreativität spielt eine Rolle. Initialisierungsbefehle umfassen unter Umständen eine eingebettete Wartezeit zwischen Vorgängen, die zusammen mit `phone_home` verwendet werden können.
- Cloud-Vorlagen-basiertes `phone_home` funktioniert nicht, wenn die Maschinenvorlage bereits Einstellungen für das `phone_home`-Modul enthält
- Die Maschine muss über ausgehenden Kommunikationszugriff auf vRealize Automation Cloud Assembly verfügen.

Um unter Verwendung von `phone_home` in vRealize Automation Cloud Assembly auf die Initialisierung der Maschine zu warten, fügen Sie der Cloud-Vorlage einen `cloudConfigSettings`-Abschnitt hinzu:

```
cloudConfigSettings:
  phoneHomeShouldWait: true
  phoneHomeTimeoutSeconds: 600
  phoneHomeFailOnTimeout: true
```

Eigenschaft	Beschreibung
phoneHomeShouldWait	Warten auf Initialisierung, True oder False.
phoneHomeTimeoutSeconds	Zeitpunkt, an dem entschieden werden muss, ob die Bereitstellung trotz laufender Initialisierung fortgesetzt wird. Standardwert ist 10 Minuten.
phoneHomeFailOnTimeout	Fortsetzen der Bereitstellung nach einer Zeitüberschreitung, True oder False. Wenn Sie die Bereitstellung dennoch fortsetzen, beachten Sie, dass sie aus anderen Gründen fehlschlagen kann.

Vorgehensweise zum Durchführen einer Windows-Gastanpassung

Damit vRealize Automation Cloud Assembly eine Windows-Maschine bei der Bereitstellung automatisch initialisiert, bereiten Sie ein Image vor, das Cloudbase-Init unterstützt, und dann eine Cloud-Vorlage, die die entsprechenden Befehle enthält.

Der Image-Erstellungsprozess variiert je nach Cloud-Anbieter. Das hier angezeigte Beispiel gilt für vSphere.

Vorgehensweise zum Erstellen eines initialisierbaren Windows-Image für vSphere

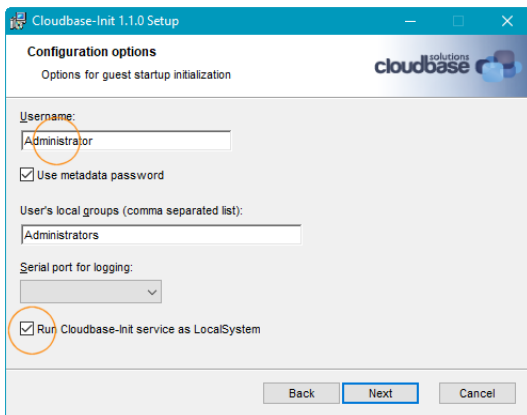
Damit vRealize Automation Cloud Assembly eine auf vSphere bereitgestellte Windows-Maschine initialisiert werden kann, muss sie auf einer Vorlage mit installiertem und konfiguriertem Cloudbase-Init basieren.

- 1 Verwenden Sie vSphere, um eine Windows-VM zu erstellen und einzuschalten.
- 2 Melden Sie sich auf der virtuellen Maschine bei Windows an.
- 3 Laden Sie Cloudbase-Init herunter.

<https://cloudbase.it/cloudbase-init/#download>

- 4 Starten Sie die MSI-Setupdatei für Cloudbase-Init.

Geben Sie während der Installation **Administrator** als Benutzernamen ein und wählen Sie die Option zum Ausführen als LocalSystem aus.



Andere Einrichtungsauswahlen können als Standardwerte beibehalten werden.

- 5 Lassen Sie die Ausführung der Installation zu, schließen Sie jedoch die Abschlussseite des Einrichtungsassistenten nicht.

Wichtig Schließen Sie die letzte Seite des Einrichtungsassistenten nicht.

- 6 Während die Abschlussseite des Einrichtungsassistenten noch geöffnet ist, navigieren Sie in Windows zum Installationspfad für Cloudbase-Init und öffnen Sie die folgende Datei in einem Texteditor.

```
conf\cloudbase-init-unattend.conf
```

- 7 Setzen Sie `metadata_services` auf `OvfService` (siehe Abbildung).

```
metadata_services=cloudbaseinit.metadata.services.ovfservice.OvfService
```

- 8 Speichern und schließen Sie `cloudbase-init-unattend.conf`.

- 9 Öffnen Sie im gleichen Ordner die nachfolgende Datei in einem Texteditor.

```
conf\cloudbase-init.conf
```

- 10 Legen Sie `first_logon_behaviour`, `metadata_services` und `plugins` fest (siehe Abbildung).

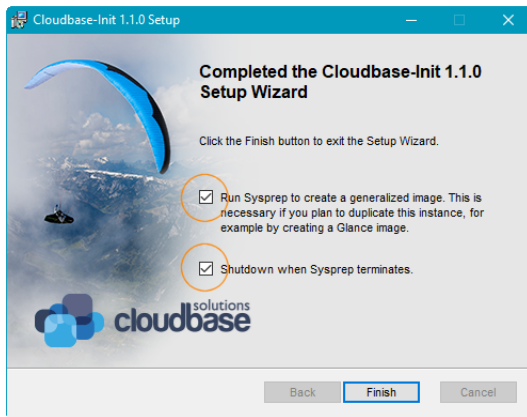
```
first_logon_behaviour=always
. . .
metadata_services=cloudbaseinit.metadata.services.ovfservice.OvfService
. . .
plugins=cloudbaseinit.plugins.windows.createuser.CreateUserPlugin,cloudbaseinit.plugins.win
dows.setuserpassword.SetUserPasswordPlugin,cloudbaseinit.plugins.common.sshpublickeys.SetUs
erSSHPublicKeysPlugin,cloudbaseinit.plugins.common.userdata.UserDataPlugin
. . .
```

- 11 Speichern und schließen Sie `cloudbase-init.conf`.
- 12 Wählen Sie auf der Abschlussseite des Einrichtungsassistenten die Optionen zum Ausführen von Sysprep und zum Herunterfahren nach Sysprep aus und klicken Sie auf **Fertig stellen**.

Hinweis VMware sind Fälle bekannt, bei denen die Ausführung von Sysprep verhindert, dass Bereitstellungen des Images funktioniert.

Bei der Bereitstellung wendet vRealize Automation Cloud Assembly eine dynamisch generierte Anpassungsspezifikation an, die die Netzwerkschnittstelle trennt. Der Status „Sysprep ausstehend“ im Image hat möglicherweise zur Folge, dass die Anpassungsspezifikation fehlschlägt und die Bereitstellung getrennt wird.

Wenn Sie vermuten, dass dies in Ihrer Umgebung der Fall ist, versuchen Sie, die Sysprep-Optionen beim Erstellen des Images deaktiviert zu lassen.



- 13 Nachdem die virtuelle Maschine heruntergefahren wurde, verwenden Sie vSphere, um sie in eine Vorlage zu verwandeln.

Zusätzliche Details

Die folgende Tabelle erläutert die während der Einrichtung vorgenommenen Konfigurationseingaben.

Konfigurationseinstellung	Zweck
Username, CreateUserPlugin und SetUserPasswordPlugin	Nach Sysprep wird beim ersten Start CreateUserPlugin verwendet, um das Administratorkonto des Benutzernamens mit einem leeren Kennwort zu erstellen. Mit SetUserPasswordPlugin kann Cloudbase-Init das leere Kennwort in das Kennwort für den Remotezugriff ändern, das in die Cloud-Vorlage aufgenommen wird.
Verhalten bei erster Anmeldung	Diese Einstellung fordert den Benutzer auf, das Kennwort bei der ersten Anmeldung zu ändern.
Metadatendienste	Wenn nur OVFSservice aufgelistet wird, versucht Cloudbase-Init nicht, andere Metadatendienste zu finden, die in vCenter nicht unterstützt werden. Dies führt zu übersichtlicheren Protokolldateien, da die Protokolle andernfalls mit Einträgen über das Nichtauffinden dieser anderen Dienste gefüllt werden.
Plug-Ins	Wenn nur Plug-Ins mit Funktionen aufgelistet werden, die von OVFSservice unterstützt werden, sind die Protokolle ebenfalls übersichtlicher. Cloudbase-Init führt Plug-Ins in der angegebenen Reihenfolge aus.
Als LocalSystem ausführen	Diese Einstellung unterstützt erweiterte Initialisierungsbefehle, für die es erforderlich sein kann, dass Cloudbase-Init unter einem dedizierten Administratorkonto ausgeführt wird.

Vorgehensweise zum Einschließen von Cloudbase-Init-Befehlen in eine Cloud-Vorlage

Um eine Windows-Maschine zu initialisieren, erstellen Sie Infrastruktur und Cloud-Vorlagen in vRealize Automation Cloud Assembly, sodass das initialisierbare Windows-Image die gewünschten Befehle ausführt.

Das hier angezeigte Beispiel basiert auf vSphere, andere Cloud-Anbieter sollten jedoch ähnlich sein.

Voraussetzungen

- Erstellen Sie die Infrastruktur. Fügen Sie in vRealize Automation Cloud Assembly Ihr vSphere-Cloud-Konto und eine zugehörige Cloud-Zone hinzu.
- Fügen Sie die Konfigurations- und Image-Zuordnungen hinzu und fügen Sie Netzwerk- und Speicherprofile hinzu.

In Ihrer Infrastruktur muss eine Image-Zuordnung auf die Windows-Vorlage verweisen, die Sie zur Unterstützung von CloudBase-Init erstellt haben. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Erstellen eines initialisierbaren Windows-Image für vSphere](#).

Wenn die Vorlage nicht aufgelistet ist, gehen Sie zu „Cloud-Konten“ und synchronisieren Sie die Images. Andernfalls wird die automatische Synchronisierung alle 24 Stunden ausgeführt.

- Fügen Sie ein Projekt hinzu, fügen Sie Benutzer hinzu und stellen Sie sicher, dass die Benutzer Ihre Cloud-Zone bereitstellen können.

Weitere Informationen zum Erstellen von Infrastruktur und Projekten finden Sie in den Beispielen im [Lernprogramm: Einrichten und Testen einer Multi-Cloud-Infrastruktur und von Bereitstellungen in vRealize Automation Cloud Assembly](#).

Verfahren

- 1 Gehen Sie in vRealize Automation Cloud Assembly zur Registerkarte **Design** und erstellen Sie eine Cloud-Vorlage.
- 2 Fügen Sie einen `cloudConfig`-Abschnitt mit den gewünschten Cloudbase-Init-Befehlen hinzu.

Mit den folgenden Befehlsbeispielen wird eine neue Datei auf dem `c:`-Laufwerk von Windows erstellt und der Hostname festgelegt.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: cloudbase-init-win-2016
      flavor: small
      remoteAccess:
        authentication: usernamePassword
        username: Administrator
        password: Password1234@$
      cloudConfig: |
        #cloud-config
        write_files:
          content: Cloudbase-Init test
          path: C:\test.txt
          set_hostname: testname
```

Weitere Informationen finden Sie in der [Dokumentation zu Cloudbase-init](#).

- 3 Fügen Sie `remoteAccess`-Eigenschaften hinzu, um die Maschine für die Erstanmeldung bei Windows zu konfigurieren.

Wie beim Erstellen der Vorlage erwähnt, wählt der Metadatendienst die Anmeldeinformationen aus und stellt sie an `CreateUserPlugin` und `SetUserPasswordPlugin` bereit. Beachten Sie, dass das Kennwort die Kennwortanforderungen von Windows erfüllen muss.

- 4 Testen und stellen Sie die Cloud-Vorlage in vRealize Automation Cloud Assembly bereit.
- 5 Verwenden Sie nach der Bereitstellung Windows RDP und die Anmeldedaten in der Vorlage, um sich bei der neuen Windows-Maschine anzumelden und die Anpassung zu überprüfen.

Im obigen Beispiel suchen Sie nach der `C:\test.txt`-Datei und prüfen die Systemeigenschaften für den Hostnamen.

Vorgehensweise zum Erstellen benutzerdefinierter Ressourcentypen zur Verwendung in vRealize Automation Cloud Assembly-Cloud-Vorlagen

Wenn Sie eine Cloud-Vorlage in vRealize Automation Cloud Assembly erstellen, enthält die Ressourcentyppalette Ressourcentypen für das unterstützte Cloud-Konto und die Integrations-Endpoints. Möglicherweise gibt es Anwendungsfälle, in denen Sie Cloud-Vorlagen basierend auf einer erweiterten Ressourcentypliste erstellen möchten. Sie können benutzerdefinierte Ressourcen erstellen, sie der Design-Arbeitsfläche hinzufügen und Cloud-Vorlagen erstellen, die Ihre Design- und Bereitstellungsanforderungen unterstützen.

Verwenden von vRealize Orchestrator zum Erstellen von benutzerdefinierten Ressourcen

Jede benutzerdefinierte Ressource basiert auf einem vRealize Orchestrator-SDK-Bestandstyp und wird von einem vRealize Orchestrator-Workflow erstellt. Dessen Ausgabe ist eine Instanz des gewünschten SDK-Typs. Primitive Typen wie `Properties`, `Date`, `string` und `number` werden für die Erstellung benutzerdefinierter Ressourcen nicht unterstützt.

Hinweis SDK-Objekttypen können anhand des Doppelpunktes („:“), mit dem der Plug-In-Name und der Typname getrennt werden, von anderen Eigenschaftstypen unterschieden werden. Beispielsweise ist `AD:UserGroup` ein SDK-Objektyp, der zur Verwaltung von Active Directory-Benutzergruppen verwendet wird.

Sie können die integrierten Workflows in vRealize Orchestrator verwenden oder Ihre eigenen erstellen. Wenn Sie vRealize Orchestrator zum Erstellen beliebiger As-a-Service-Dienste/XaaS-Workflows verwenden, können Sie beispielsweise eine Cloud-Vorlage erstellen, die Active Directory-Benutzer zur Bereitstellungszeit zu Maschinen hinzufügt, oder einen benutzerdefinierten F5-Lastausgleichsdienst zu einer Bereitstellung hinzufügen.

Ressourcenname und Ressourcentyp der benutzerdefinierten Ressource

Der Name der benutzerdefinierten Ressource identifiziert Ihre benutzerdefinierte Ressource innerhalb der Ressourcentyppalette der Cloud-Vorlage.

Der Ressourcentyp einer benutzerdefinierten Ressource muss mit **Custom.** beginnen und jeder Ressourcentyp muss eindeutig sein. Beispielsweise können Sie `Custom.ADUser` als Ressourcentyp für eine benutzerdefinierte Ressource festlegen, die Active Directory-Benutzer hinzufügt. Obwohl die Aufnahme von **Custom.** im Textfeld nicht validiert ist, wird die Zeichenfolge automatisch hinzugefügt, wenn Sie sie entfernen.

Externer Typ

Die Eigenschaft „externer Typ“ definiert den Typ Ihrer benutzerdefinierten Ressource. Wenn Sie in Ihrer benutzerdefinierten Ressource in vRealize Automation Cloud Assembly „Workflow erstellen“ auswählen, wird das Dropdown-Menü „Externer Typ“ darunter angezeigt. Das Dropdown-Menü enthält Eigenschaften des externen Typs, die aus den Ausgabeparametern des vRealize Orchestrator-Workflows ausgewählt werden. Die im Dropdown-Menü enthaltenen Ausgabeeigenschaften des ausgewählten Workflows müssen Nicht-Array-SDK-Objektypen wie `VC:VirtualMachine` oder `AD:UserGroup` sein.

Hinweis Vergewissern Sie sich beim Erstellen benutzerdefinierter Workflows, die das Plug-In „Dynamischer Typ“ verwenden, dass deren Variablen mithilfe der `DynamicTypesManager.getObject()`-Methode erstellt werden.

Wenn Sie Ihre benutzerdefinierten Ressourcen definieren, definieren Sie auch den Geltungsbereich der Verfügbarkeit des ausgewählten externen Typs. Der ausgewählte externe Typ kann:

- über Projekte hinweg gemeinsam genutzt werden.
- nur für das ausgewählte Projekt verfügbar sein.

Sie können nur einen externen Typ pro definiertem Geltungsbereich haben. Wenn Sie z. B. eine benutzerdefinierte Ressource in Ihrem Projekt erstellen, die `VC:VirtualMachine` als externen Typ verwendet, können Sie keine weitere benutzerdefinierte Ressource für dasselbe Projekt erstellen, das denselben externen Typ verwendet. Sie können auch nicht zwei gemeinsam genutzte benutzerdefinierte Ressourcen erstellen, die denselben externen Typ verwenden.

Workflow-Eingabe-/Ausgabvalidierung

Wenn Sie Workflows zum Erstellen, Löschen und Aktualisieren als Lebenszyklusaktionen zu Ihrer benutzerdefinierten Ressource hinzufügen, überprüft vRealize Automation Cloud Assembly, dass die ausgewählten Workflows korrekte Eingabe- und Ausgabeeigenschaftsdefinitionen aufweisen.

- Der Workflow „Erstellen“ muss über einen Ausgabeparameter verfügen, der ein SDK-Objektyp ist, beispielsweise `SSH:Host` oder `SQL:Database`. Wenn der ausgewählte Workflow die Validierung nicht besteht, können Sie keine Workflows zum Aktualisieren oder Löschen hinzufügen und Änderungen an der benutzerdefinierten Ressource nicht speichern.

- Der Workflow „Löschen“ muss über einen Eingabeparameter verfügen, dessen SDK-Objektyp ist mit dem externen Typ der benutzerdefinierten Ressource übereinstimmt.
- Der Workflow „Aktualisieren“ muss sowohl einen Eingabe- als auch einen Ausgabeparameter aufweisen, dessen SDK-Objektyp mit dem externen Typ der benutzerdefinierten Ressource übereinstimmt.

Eigenschaftsschema für benutzerdefinierte Ressourcen

Wenn Sie vRealize Orchestrator-Workflows zu Ihrer benutzerdefinierten Ressource hinzufügen, werden deren Eingabe- und Ausgabeparameter als Eigenschaften hinzugefügt. Sie können das Eigenschaftsschema für benutzerdefinierte Ressourcen anzeigen, indem Sie die Registerkarte **Eigenschaften** auswählen. Das Schema enthält den Namen, den Datentyp, den Eigenschaftstyp und, sofern verfügbar, die Beschreibung einer bestimmten Eigenschaft. Das Schema definiert auch, ob eine bestimmte Eigenschaft erforderlich oder optional ist.

Vorgehensweise zum Erstellen einer Cloud-Vorlage in vRealize Automation Cloud Assembly, die Benutzer zu Active Directory hinzufügt

Zusätzlich zu den vRealize Automation Cloud Assembly-Cloud-Vorlagenressourcen, die Sie bei der Erstellung von Cloud-Vorlagen verwenden, können Sie auch Ihre eigenen benutzerdefinierten Ressourcen erstellen.

Benutzerdefinierte Ressourcen sind vRealize Orchestrator-Objekte, die Sie über vRealize Automation mit den definierten Hauptworkflows für den Ressourcenbetrieb verwalten. Der Cloud-Vorlagendienst ruft automatisch die passenden vRealize Orchestrator-Workflows auf, wenn ein Erstellungs- oder Löschvorgang ausgelöst wird. Sie können die Funktionalität des Ressourcentyps erweitern, indem Sie auch vRealize Orchestrator-Workflows auswählen, die als Tag-2-Vorgänge verwendet werden können.

In diesem Anwendungsbeispiel werden integrierte, in der vRealize Orchestrator-Bibliothek bereitgestellte Workflows verwendet. Es umfasst vorgegebene Werte oder Zeichenfolgen, um darzustellen, wie der Prozess ausgeführt werden kann. Sie können sie so anpassen, dass sie sich für Ihre Umgebung eignen.

Zu Referenzzwecken verwendet dieses Anwendungsbeispiel ein Projekt mit dem Namen **DevOpsTesting**. Sie können dieses Beispielprojekt durch ein beliebiges Projekt in Ihrer Umgebung ersetzen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie eine vRealize Orchestrator-Integration konfiguriert haben. Weitere Informationen hierzu finden Sie unter [Konfigurieren der vRealize Orchestrator-Integration in Cloud Assembly](#).
- Stellen Sie sicher, dass die Workflows, die Sie für die Aktionen zum Erstellen, Aktualisieren und Löschen verwenden, und die Tag-2-Aktionen in vRealize Orchestrator vorhanden sind und erfolgreich von dort aus ausgeführt werden.

- Suchen Sie in vRealize Orchestrator den Ressourcentyp, der von den Workflows verwendet wird. Die in dieser benutzerdefinierten Ressource enthaltenen Workflows müssen alle denselben Ressourcentyp verwenden. In diesem Anwendungsbeispiel lautet der Ressourcentyp `AD:User`. Weitere Informationen zur Validierung des Ressourcentyps finden Sie unter [Vorgehensweise zum Erstellen benutzerdefinierter Ressourcentypen zur Verwendung in vRealize Automation Cloud Assembly-Cloud-Vorlagen](#).
- Konfigurieren Sie mithilfe der integrierten Active Directory-Workflows in Ihrer vRealize Orchestrator-Integration einen Active Directory-Server.
- Stellen Sie sicher, dass Sie das Verfahren zum Konfigurieren und Bereitstellen einer Maschinen-Cloud-Vorlage kennen.

Verfahren

- 1 Erstellen Sie eine benutzerdefinierte Ressource für Active Directory, um einen Benutzer in einer Gruppe hinzuzufügen.

In diesem Schritt wird die benutzerdefinierte Ressource als Ressourcentyp zur Design-Arbeitsfläche der Cloud-Vorlage hinzugefügt.

- a Wählen Sie in vRealize Automation Cloud Assembly die Option **Design > Benutzerdefinierte Ressourcen** und klicken Sie auf **Neue benutzerdefinierte Ressource**.
- b Stellen Sie die folgenden Werte bereit.

Beachten Sie, dass es sich mit Ausnahme der Workflow-Namen um Beispielwerte handelt.

Einstellung	Beispielwert
Name	AD-Benutzer Dies ist der Name, der in der Ressourcentyppalette auf der Cloud-Vorlagen-Arbeitsfläche angezeigt wird.
Ressourcentyp	Custom.ADUser Der Ressourcentyp muss mit Custom. beginnen und jeder Ressourcentyp muss eindeutig sein. Obwohl die Aufnahme von Custom. im Textfeld nicht validiert ist, wird die Zeichenfolge automatisch hinzugefügt, wenn Sie sie entfernen. Dieser Ressourcentyp wird der Ressourcentyppalette hinzugefügt, damit Sie ihn in der Cloud-Vorlage verwenden können.

- c Überprüfen Sie zum Aktivieren dieses Ressourcentyps in der Liste der Cloud-Vorlagen-Ressourcentypen, ob die Option **Aktivieren** aktiviert ist.
- d Wählen Sie die Einstellung **Geltungsbereich** aus, die den Ressourcentyp für beliebige Projekte zur Verfügung stellt.

- e Konfigurieren Sie die Workflows, die die Ressource und die Tag-2-Aktionen definieren.

Hinweis Die ausgewählten Tag-2-Workflows müssen über einen Eingabeparameter verfügen, der vom selben Typ wie der externe Typ ist. Die Eingabe des externen Typs wird nicht in dem vom Benutzer angeforderten benutzerdefinierten Formular für Tag 2 angezeigt, da sie automatisch an die benutzerdefinierte Ressource gebunden ist.

Einstellung	Beispielwert
Lebenszyklusaktionen – Erstellen	<p>Wählen Sie den Workflow Benutzer mit Kennwort in einer Organisationseinheit erstellen aus.</p> <p>Wenn Sie über mehrere vRealize Orchestrator-Integrationen verfügen, wählen Sie den Workflow der Integrationsinstanz aus, die Sie zum Ausführen dieser benutzerdefinierten Ressourcen verwenden.</p> <p>Nach dem Auswählen des Workflows wird das Dropdown-Menü für den externen Typ verfügbar und automatisch auf <code>AD:User</code> festgelegt.</p> <p>Hinweis Ein externer Quelltyp kann nur einmal bei gemeinsamer Nutzung und einmal pro Projekt verwendet werden. In diesem Anwendungsbeispiel stellen Sie dieselbe benutzerdefinierte Ressource für alle Projekte bereit. Dies bedeutet jedoch, dass Sie <code>AD:User</code> für keine anderen Ressourcentypen in allen Projekten verwenden können. Wenn Sie über andere Workflows verfügen, die den Typ <code>AD:User</code> benötigen, müssen Sie einzelne benutzerdefinierte Ressourcen für jedes Projekt erstellen.</p>
Lebenszyklusaktionen – Löschen	Wählen Sie den Workflow Benutzer löschen aus.
Zusätzliche Aktionen	<p>Wählen Sie den Workflow Benutzerkennwort löschen aus.</p> <p>Um das Anforderungsformular für die Aktion zu ändern, auf das der Benutzer antwortet, wenn er diese Aktion anfordert, klicken Sie auf das Symbol in der Spalte Anforderungsparameter.</p> <p>Hinweis Stellen Sie bei Workflows für zusätzliche Aktionen sicher, dass der Workflow über einen Eingabeparameter mit demselben Typ wie der externe Typ verfügt.</p>

In diesem Beispiel steht keine geeignete Anwendung eines Aktualisierungsworkflows zur Verfügung. Ein häufiges Beispiel für einen Aktualisierungsworkflow, bei dem Änderungen an der bereitgestellten benutzerdefinierten Ressource vorgenommen werden, ist die vertikale oder horizontale Skalierung einer Bereitstellung.

- f Überprüfen Sie den Schemaschlüssel und geben Sie Werte auf der Registerkarte **Eigenschaften** ein, um die Workflow-Eingaben zu verstehen, die in der Cloud-Vorlage konfiguriert werden können.

Das Schema listet die erforderlichen und optionalen Eingabewerte auf, die im Workflow definiert sind. Die erforderlichen Eingabewerte sind in der YAML der Cloud-Vorlage enthalten.

Im Workflow „Benutzer erstellen“ stellen `accountName`, `displayName` und `ouContainer` erforderliche Eingabewerte dar. Die anderen Schemaeigenschaften sind nicht erforderlich. Sie können das Schema auch verwenden, um zu ermitteln, wo Bindungen mit anderen Feldwerten, Workflows oder Aktionen erstellt werden sollen. Bindungen sind in diesem Anwendungsfall nicht enthalten.

- g Um die Erstellung Ihrer benutzerdefinierten Ressource abzuschließen, klicken Sie auf **Erstellen**.
- 2 Erstellen Sie eine Cloud-Vorlage, die den Benutzer bei der Bereitstellung zu einer Maschine hinzufügt.
- a Wählen Sie **Design > Cloud-Vorlagen** und klicken Sie auf **Neu von > Leere Arbeitsfläche**.
 - b Geben Sie der Cloud-Vorlage den Namen **Maschine mit AD-Benutzer**.
 - c Wählen Sie das Projekt **DevOpsTesting** aus und klicken Sie auf **Erstellen**.
 - d Fügen Sie eine vSphere-Maschine hinzu und konfigurieren Sie sie.
 - e Ziehen Sie in der Liste mit den benutzerdefinierten Ressourcen links auf der Seite „Cloud-Vorlagendesign“ den Ressourcentyp **AD-Benutzer** auf die Arbeitsfläche.

Hinweis Sie können die benutzerdefinierte Ressource auswählen, indem Sie entweder im linken Fensterbereich nach unten scrollen und sie dann auswählen, oder indem Sie im Textfeld **Ressourcentypen durchsuchen** suchen. Falls die benutzerdefinierte Ressource nicht angezeigt wird, klicken Sie auf die Schaltfläche „Aktualisieren“ neben dem Textfeld **Ressourcentypen durchsuchen**.

- f Bearbeiten Sie auf der rechten Seite den YAML-Code, um die obligatorischen Eingabewerte und das Kennwort hinzuzufügen.

Fügen Sie einen `inputs`-Abschnitt im Code hinzu, damit Benutzer den Namen der Benutzer angeben können, die sie hinzufügen. Im folgenden Beispiel handelt es sich bei einigen dieser Werte um Beispieldaten. Ihre Werte können davon abweichen.

```
inputs:
  accountName:
    type: string
    title: Account name
    encrypted: true
  displayName:
    type: string
    title: Display name
  password:
    type: string
    title: Password
    encrypted: true
  confirmPassword:
    type: string
    title: Password
    encrypted: true
  ouContainer:
    type: object
    title: AD OU container
    $data: 'vro/data/inventory/AD:OrganizationalUnit'
    properties:
      id:
        type: string
      type:
        type: string
```

- g Fügen Sie im Abschnitt `resources` den Code `${input.input-name}` hinzu, um die Benutzerauswahl zu bestätigen.

```
resources:
  Custom_ADUser_1:
    type: Custom.ADUser
    properties:
      accountName: '${input.accountName}'
      displayName: '${input.displayName}'
      ouContainer: '${input.ouContainer}'
      password: '${input.password}'
      confirmPassword: '${input.confirmPassword}'
```

- 3 Stellen Sie die Cloud-Vorlage bereit.
- Klicken Sie auf der Cloud-Vorlagen-Designseite auf **Bereitstellen**.
 - Geben Sie als **Name der Bereitstellung** **AD User Scott** ein.

- c Wählen Sie die **Cloud-Vorlagenversion** und klicken Sie auf **Weiter**.
 - d Vervollständigen Sie die Eingaben der Bereitstellung.
 - e Klicken Sie auf **Bereitstellen**.
- 4 Überwachen Sie den Bereitstellungsprozess, um sicherzustellen, dass der Benutzer zu Active Directory hinzugefügt wird.
- a Klicken Sie auf **Bereitstellungen** und suchen Sie nach der Bereitstellung **AD User Scott**.
 - b Überwachen Sie den Status der Anforderung und überprüfen Sie den Erfolg der Bereitstellung.
 - c Stellen Sie sicher, dass die Aktion „Kennwort ändern“ verfügbar ist und funktioniert.

Nächste Schritte

Wenn die getestete Cloud-Vorlage funktioniert, können Sie die benutzerdefinierte Ressource **AD-Benutzer** für andere Cloud-Vorlagen verwenden.

Vorgehensweise zum Erstellen einer Cloud-Vorlage mit SSH in Cloud Assembly

Sie können benutzerdefinierte Ressourcen erstellen, die Sie zum Anlegen von Cloud-Vorlagen mithilfe von vRealize Orchestrator-Workflows verwenden können. In diesem Anwendungsbeispiel fügen Sie eine benutzerdefinierte Ressource hinzu, die einen SSH-Host hinzufügt. Sie können die Ressource dann in Cloud-Vorlagen aufnehmen. In diesem Verfahren wird auch ein Aktualisierungsworkflow hinzugefügt, damit Benutzer nach der Bereitstellung Änderungen an der SSH-Konfiguration vornehmen können, statt einzelne Tag-2-Aktionen durchzuführen.

Benutzerdefinierte Ressourcen sind vRealize Orchestrator-Objekte, die Sie über vRealize Automation mit den definierten Hauptworkflows für den Ressourcenbetrieb verwalten. Der Cloud-Vorlagendienst ruft automatisch die entsprechenden vRealize Orchestrator-Workflows auf, wenn ein Erstellungs- oder Löschvorgang ausgelöst wird. Sie können die Funktionalität des Ressourcentyps erweitern, indem Sie auch vRealize Orchestrator-Workflows auswählen, die als Tag-2-Vorgänge verwendet werden können.

In diesem Anwendungsbeispiel werden integrierte, in der vRealize Orchestrator-Bibliothek bereitgestellte Workflows verwendet. Es umfasst vorgegebene Werte oder Zeichenfolgen, um darzustellen, wie der Prozess ausgeführt werden kann. Sie können sie so anpassen, dass sie sich für Ihre Umgebung eignen.

Zu Referenzzwecken verwendet dieses Anwendungsbeispiel ein Projekt mit dem Namen **DevOpsTesting**. Sie können das Projekt durch eines Ihrer vorhandenen Projekte ersetzen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie eine vRealize Orchestrator-Integration konfiguriert haben. Weitere Informationen hierzu finden Sie unter [Konfigurieren der vRealize Orchestrator-Integration in Cloud Assembly](#).

- Stellen Sie sicher, dass die Workflows, die Sie für die Aktionen zum Erstellen, Aktualisieren und Löschen verwenden, und die Tag-2-Aktionen in vRealize Orchestrator vorhanden sind und erfolgreich von dort aus ausgeführt werden.
- Suchen Sie in vRealize Orchestrator den Ressourcentyp, der von den Workflows verwendet wird. Die in dieser benutzerdefinierten Ressource enthaltenen Workflows müssen alle denselben Ressourcentyp verwenden. In diesem Anwendungsbeispiel lautet der Ressourcentyp `SSH:Host`. Weitere Informationen zur Validierung des Ressourcentyps finden Sie unter [Vorgehensweise zum Erstellen benutzerdefinierter Ressourcentypen zur Verwendung in vRealize Automation Cloud Assembly-Cloud-Vorlagen](#).
- Stellen Sie sicher, dass Sie das Verfahren zum Konfigurieren und Bereitstellen einer Cloud-Vorlage für Maschinen kennen.

Verfahren

- 1 Erstellen Sie eine benutzerdefinierte Ressource für einen SSH-Host, um SSH zu einer Cloud-Vorlage hinzuzufügen.

In diesem Schritt wird die benutzerdefinierte Ressource als Ressourcentyp zur Design-Arbeitsfläche der Cloud-Vorlage hinzugefügt.

- a Wählen Sie in vRealize Automation Cloud Assembly die Option **Design > Benutzerdefinierte Ressourcen** und klicken Sie auf **Neue benutzerdefinierte Ressource**.
- b Stellen Sie die folgenden Werte bereit.

Beachten Sie, dass es sich mit Ausnahme der Workflow-Namen um Beispielwerte handelt.

Tabelle 6-2.

Einstellung	Beispielwert
Name	SSH Host - DevOpsTesting Project Dies ist der Name, der in der Ressourcentyppalette der Cloud-Vorlage angezeigt wird.
Ressourcentyp	Custom.SSHHost Der Ressourcentyp muss mit Custom. beginnen und jeder Ressourcentyp muss eindeutig sein. Obwohl die Aufnahme von Custom. im Textfeld nicht validiert ist, wird die Zeichenfolge automatisch hinzugefügt, wenn Sie sie entfernen. Dieser Ressourcentyp wird der Design-Arbeitsfläche hinzugefügt, damit Sie ihn in der Cloud-Vorlage verwenden können.

- c Zum Aktivieren dieses Ressourcentyps in der Liste der Ressourcentypen für Cloud-Vorlagen stellen Sie sicher, dass die Option **Aktivieren** ausgewählt ist.
- d Wählen Sie die Einstellung **Bereich** aus, die dem Projekt **DevOpsTesting** den Ressourcentyp zur Verfügung stellt.

- e Wählen Sie die Workflows aus, die die Ressource definieren.

Einstellung	Einstellung
Lebenszyklusaktionen – Erstellen	Wählen Sie den Workflow SSH-Host hinzufügen aus. Wenn Sie über mehrere vRealize Orchestrator-Integrationen verfügen, wählen Sie den Workflow der Integrationsinstanz aus, die Sie zum Ausführen dieser benutzerdefinierten Ressourcen verwenden. Nach dem Auswählen des Workflows wird das Dropdown-Menü für den externen Typ verfügbar und automatisch auf <code>SSH:Host</code> festgelegt. Ein externer Quelltyp kann nur einmal bei gemeinsamer Nutzung und einmal pro Projekt verwendet werden. In diesem Anwendungsbeispiel stellen Sie die benutzerdefinierte Ressource nur für das Projekt DevOpsTesting bereit. Wenn Sie über andere Workflows verfügen, die den Typ <code>SSH:Host</code> benötigen, müssen Sie einzelne benutzerdefinierte Ressourcen für jedes Projekt erstellen.
Lebenszyklusaktionen – Aktualisieren	Wählen Sie den Workflow SSH-Host aktualisieren aus.
Lebenszyklusaktionen – Löschen	Wählen Sie den Workflow SSH-Host entfernen aus.

- f Überprüfen Sie den Schemaschlüssel und geben Sie Werte auf der Registerkarte **Eigenschaften** ein, um die Workflow-Eingaben zu verstehen, die in der Cloud-Vorlage konfiguriert werden können.

Das Schema listet die erforderlichen und optionalen Eingabewerte auf, die im Workflow definiert sind. Die erforderlichen Eingabewerte sind in der YAML der Cloud-Vorlage enthalten.

Erforderliche Eingabewerte im Workflow **SSH-Host hinzufügen** sind `hostname`, `port` und `username`. Die anderen Schemaeigenschaften sind nicht erforderlich. Sie können das Schema auch verwenden, um zu ermitteln, wo Bindungen mit anderen Feldwerten, Workflows oder Aktionen erstellt werden sollen. Bindungen sind in diesem Anwendungsfall nicht enthalten.

- g Um die Erstellung Ihrer benutzerdefinierten Ressource abzuschließen, klicken Sie auf **Erstellen**.
- 2 Erstellen Sie eine Cloud-Vorlage, bei deren Bereitstellung der SSH-Host hinzugefügt wird.
- Wählen Sie **Design > Cloud-Vorlagen** aus und klicken Sie auf **Neu aus > Leere Arbeitsfläche**.
 - Geben Sie der Cloud-Vorlage den Namen **Maschine mit SSH-Host**.
 - Wählen Sie das Projekt **DevOpsTesting** aus und klicken Sie auf **Erstellen**.
 - Fügen Sie eine vSphere-Maschine hinzu und konfigurieren Sie sie.

- e Ziehen Sie in der Liste der benutzerdefinierten Ressourcen links auf der Seite „Cloud-Vorlagen-Design“ den Ressourcentyp **SSH Host - DevOpsTesting Project** auf die Arbeitsfläche.

Hinweis Sie können die benutzerdefinierte Ressource auswählen, indem Sie entweder im linken Fensterbereich nach unten scrollen und sie dann auswählen, oder indem Sie im Textfeld **Ressourcentypen durchsuchen** suchen. Falls die benutzerdefinierte Ressource nicht angezeigt wird, klicken Sie auf die Schaltfläche „Aktualisieren“ neben dem Textfeld **Ressourcentypen durchsuchen**.

Eine Erinnerung daran, dass der Ressourcentyp verfügbar ist, weil er für das Projekt konfiguriert wurde. Wenn Sie eine Cloud-Vorlage für ein anderes Projekt erstellt haben, können Sie den Ressourcentyp nicht anzeigen.

- f Bearbeiten Sie auf der rechten Seite den YAML-Code, um die obligatorischen Eingabewerte hinzuzufügen.

Fügen Sie einen `inputs`-Abschnitt im Code hinzu, damit Benutzer den Benutzer- und Hostnamen zur Bereitstellungszeit angeben können. In diesem Beispiel wird 22 als Standardwert für den Port verwendet. Im folgenden Beispiel handelt es sich bei einigen dieser Werte um Beispieldaten. Ihre Werte können davon abweichen.

```
inputs:
  hostname:
    type: string
    title: The hostname of the SSH Host
  username:
    type: string
    title: Username
```

- g Fügen Sie im Abschnitt `resources` den Code `${input.input-name}` hinzu, um die Benutzerauswahl zu bestätigen.

```
resources:
  Custom_SSHTHost_1:
    type: Custom.SSHTHost
    properties:
      port: 22
      hostname: '${input.hostname}'
      username: '${input.username}'
```

- 3 Stellen Sie die Cloud-Vorlage bereit.
 - a Klicken Sie auf der Seite des Cloud-Vorlagen-Designers auf **Bereitstellen**.
 - b Geben Sie den **Bereitstellungsnamen SSH-Host-Test** ein.
 - c Wählen Sie die **Version der Cloud-Vorlage** aus und klicken Sie auf **Weiter**.

- d Vervollständigen Sie die Eingaben der Bereitstellung.
 - e Klicken Sie auf **Bereitstellen**.
- 4 Überwachen Sie den Bereitstellungsprozess, um sicherzustellen, dass der SSH-Host in der Bereitstellung enthalten ist.
- a Klicken Sie auf **Bereitstellungen** und suchen Sie nach der Bereitstellung **SSH Host Test**.
 - b Überwachen Sie den Status der Anforderung und überprüfen Sie den Erfolg der Bereitstellung.

Nächste Schritte

Wenn die getestete Cloud-Vorlage funktioniert, können Sie die benutzerdefinierte Ressource `SSH Host` mit anderen Cloud-Vorlagen verwenden.

Vorgehensweise zum Designen in vRealize Automation Cloud Assembly zur Vorbereitung der Tag-2-Änderungen

Zusätzlich zu den Tag-2-Aktionen, die bereits vRealize Automation Cloud Assembly-Ressourcentypen zugeordnet sind, verfügen Sie über Designoptionen, mit denen Sie sich vorab auf möglicherweise für die Benutzer erforderliche benutzerdefinierte Updates vorbereiten können.

Vorsicht Zum Ändern einer Bereitstellung können Sie deren Cloud-Vorlage bearbeiten und erneut anwenden oder Tag-2-Aktionen verwenden. In den meisten Fällen sollte die Kombination der beiden Ansätze jedoch vermieden werden.

Tag-2-Änderungen am Lebenszyklus, wie z. B. das Ein-/Ausschalten, sind in der Regel sicher. Andere Änderungen hingegen müssen vorsichtig durchgeführt werden, wie z. B. beim Hinzufügen von Festplatten.

Beispiel: Wenn Sie Festplatten mit einer Tag-2-Aktion hinzufügen und dann einen kombinierten Ansatz verwenden, indem Sie die Cloud-Vorlage erneut anwenden, könnte die Cloud-Vorlage die Tag-2-Änderung überschreiben, wodurch Festplatten entfernt und Datenverluste verursacht werden könnten.

Die Vorbereitung auf Tag 2 kann entweder die direkte Verwendung von Cloud-Vorlagencode oder die vRealize Automation Cloud Assembly-Designschnittstelle einbeziehen.

- Sie können Eingaben im Cloud-Vorlagencode verwenden, damit die Schnittstelle beim Aktualisieren der Bereitstellung oder der bereitgestellten Ressource neue Werte anfordert.
- Sie können vRealize Automation Cloud Assembly verwenden, um eine benutzerdefinierte Aktion basierend auf einem vRealize Orchestrator-Workflow oder einer Aktion zu entwerfen. Die Ausführung der benutzerdefinierten Aktion führt dazu, dass vRealize Orchestrator Änderungen an der Bereitstellung oder der bereitgestellten Ressource vornimmt.

Vorgehensweise zum Verwenden von Cloud-Vorlageneingaben für Tag-2-Updates in vRealize Automation

Beim Entwerfen von Cloud-Vorlagen können Tag-2-Benutzer mithilfe von vRealize Automation-Eingabeparametern Auswahlen aus der anfänglichen Bereitstellungsanforderung erneut eingeben.

Vorsicht Bestimmte Eigenschaftsänderungen führen dazu, dass eine Ressource neu erstellt wird. Wenn Sie beispielsweise `connection_string.name` unter `Cloud.Service.Azure.App.Service` ändern, wird die vorhandene Ressource gelöscht und eine neue Ressource erstellt.

Legen Sie beim Entwerfen von Eingaben zur Unterstützung von Tag-2-Änderungen fest, ob Eingaben zum Löschen und erneuten Erstellen von Ressourcen zugelassen werden sollen. Um herauszufinden, welche Eigenschaften eine Ressource neu erstellen, folgen Sie dem Schema-Link unter [Eigenschaften der vRealize Automation-Ressource](#).

Informationen zum Erstellen von Eingaben finden Sie unter [Vorgehensweise zum Anpassen einer Cloud-Vorlage in vRealize Automation mit Benutzereingaben](#).

In folgendem Abschnitt finden Sie ein spezielles Tag-2-Beispiel.

Vorgehensweise zum Verschieben einer bereitgestellten Maschine in ein anderes Netzwerk

Bei der Verwaltung von Bereitstellungen und Netzwerken müssen Sie unter Umständen in der Lage sein, mit vRealize Automation Cloud Assembly bereitgestellte Maschinen zu verlagern.

Sie können beispielsweise zuerst ein Testnetzwerk bereitstellen und dann in ein Produktionsnetzwerk wechseln. Mit der hier beschriebenen Vorgehensweise können Sie im Voraus eine Cloud-Vorlage entwerfen, um auf solche Tag-2-Aktionen vorbereitet zu sein. Beachten Sie, dass die Maschine verschoben wird. Sie wird nicht gelöscht und erneut bereitgestellt.

Dieses Verfahren gilt nur für **Cloud.vSphere.Machine**-Ressourcen. Es funktioniert nicht für Cloud-unabhängige Maschinen, die auf vSphere bereitgestellt werden.

Voraussetzungen

- Das vRealize Automation Cloud Assembly-Netzwerkprofil muss alle Subnetze enthalten, mit denen die Maschine eine Verbindung herstellen soll. In vRealize Automation Cloud Assembly können Sie Netzwerke überprüfen, indem Sie zu **Infrastruktur > Konfigurieren > Netzwerkprofile** navigieren.

Das Netzwerkprofil muss sich in einem Konto und einer Region befinden, die Teil des jeweiligen vRealize Automation Cloud Assembly-Projekts für Ihre Benutzer sind.

- Kennzeichnen Sie die beiden Subnetze mit unterschiedlichen Tags. Im folgenden Beispiel wird von **test** und **prod** als Tag-Namen ausgegangen.
- Die bereitgestellte Maschine muss denselben IP-Zuweisungstyp beibehalten. Dieser kann während der Verlagerung in ein anderes Netzwerk nicht von „Statisch“ in „DHCP“ oder umgekehrt geändert werden.

Verfahren

- 1 Navigieren Sie in vRealize Automation Cloud Assembly zu **Design** und erstellen Sie eine Cloud-Vorlage für die Bereitstellung.
- 2 Fügen Sie im Abschnitt „Eingaben“ des Codes einen Eintrag hinzu, mit dem der Benutzer ein Netzwerk auswählen kann.

```
inputs:
  net-tagging:
    type: string
    enum:
      - test
      - prod
    title: Select a network
```

- 3 Fügen Sie im Abschnitt „Ressourcen“ des Codes den Eintrag **Cloud.Network** hinzu und verbinden Sie die vSphere-Maschine damit.
- 4 Erstellen Sie unter **Cloud.Network** eine Einschränkung, die auf die Auswahl aus den Eingaben verweist.

```
resources:
  ABCServer:
    type: Cloud.vSphere.Machine
    properties:
      name: abc-server
      . . .
    networks:
      - network: '${resource["ABCNet"].id}'
  ABCNet:
    type: Cloud.Network
    properties:
      name: abc-network
      . . .
    constraints:
      - tag: '${input.net-tagging}'
```

- 5 Fahren Sie mit dem Entwurf der Vorlage fort und stellen Sie sie wie gewohnt bereit. Bei der Bereitstellung werden Sie von der Schnittstelle aufgefordert, das Netzwerk **test** oder **prod** auszuwählen.
- 6 Wenn Sie eine Tag-2-Änderung vornehmen müssen, navigieren Sie zu **Bereitstellungen** und suchen Sie nach der mit der Cloud-Vorlage verknüpften Bereitstellung.
- 7 Klicken Sie rechts neben der Bereitstellung auf **Aktionen > Aktualisieren**.
- 8 Im Fenster „Aktualisieren“ werden Sie von der Schnittstelle aufgefordert, das Netzwerk **test** oder **prod** auszuwählen.
- 9 Treffen Sie zum Ändern von Netzwerken Ihre Auswahl, klicken Sie auf **Weiter** und dann auf **Absenden**.

Vorgehensweise zum Erstellen einer benutzerdefinierten vRealize Automation Cloud Assembly-Aktion für vMotion einer virtuellen Maschine

Nachdem Sie eine Cloud-Vorlage bereitgestellt haben, können Sie Tag-2-Aktionen ausführen, die Änderungen an der Bereitstellung vornehmen. vRealize Automation Cloud Assembly umfasst zahlreiche Tag-2-Aktionen, aber möglicherweise möchten Sie andere bereitstellen. Sie können benutzerdefinierte Ressourcenaktionen erstellen und sie Benutzern als Tag-2-Aktionen zur Verfügung stellen.

Die benutzerdefinierten Ressourcenaktionen basieren auf vRealize Orchestrator-Workflows.

Dieses Beispiel für eine benutzerdefinierte Tag-2-Aktion besteht darin, Sie in den Erstellungsvorgang einzuführen. Um benutzerdefinierte Aktionen effektiv zu verwenden, müssen Sie in der Lage sein, vRealize Orchestrator-Workflows und -Aktionen zu erstellen, die die benötigten Aufgaben ausführen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie eine vRealize Orchestrator-Integration konfiguriert haben. Weitere Informationen hierzu finden Sie unter [Konfigurieren der vRealize Orchestrator-Integration in Cloud Assembly](#).
- Stellen Sie sicher, dass der Workflow, den Sie für die Tag-2-Aktion verwenden, in vRealize Orchestrator vorhanden ist und dort erfolgreich ausgeführt wird.

Verfahren

- 1 Erstellen Sie eine benutzerdefinierte Ressourcenaktion, die vMotion zum Verschieben einer virtuellen vSphere-Maschine von einem Host auf einen anderen verwendet.
 - a Wählen Sie in vRealize Automation Cloud Assembly die Option **Design > Ressourcenaktionen** und klicken Sie auf **Neue Ressourcenaktion**.
 - b Stellen Sie die folgenden Werte bereit.

Beachten Sie, dass es sich mit Ausnahme der Workflow-Namen um Beispielwerte handelt.

Einstellung	Beispielwert
Name	vSphere_VM_vMotion Hierbei handelt es sich um den in der Liste der Ressourcenaktionen angezeigten Namen.
Anzeigename	VM verschieben Dies ist der Name, der den Benutzern im Menü „Bereitstellungsaktionen“ angezeigt wird.

- c Klicken Sie auf die Option **Aktivieren**, um diese Aktion im Menü der Tag-2-Aktionen für Ressourcen zu aktivieren, die mit dem Ressourcentyp übereinstimmen.
- d Wählen Sie den Ressourcentyp und den Workflow aus, der die Tag-2-Aktion definiert.

Einstellung	Beispielwert
Ressourcentyp	<p>Wählen Sie den Ressourcentyp Cloud.vSphere.Machine aus.</p> <p>Hierbei handelt es sich um den Ressourcentyp, der als Cloud-Vorlagenkomponente und nicht notwendigerweise als Inhalt der Cloud-Vorlage bereitgestellt wird. Beispiel: Sie verfügen über eine Cloud-unabhängige Maschine in der Cloud-Vorlage. Wenn diese Maschine jedoch auf einem vCenter Server bereitgestellt wird, lautet die Maschine Cloud.vSphere.Machine. Da die Aktion auf den bereitgestellten Typ angewendet wird, verwenden Sie beim Definieren benutzerdefinierter Aktionen keine Cloud-unabhängigen Typen.</p> <p>In diesem Beispiel kann vMotion nur für vSphere-Maschinen verwendet werden. Sie verfügen unter Umständen jedoch über andere Aktionen, die Sie für mehrere Ressourcentypen durchführen möchten. Sie müssen eine Aktion für jeden Ressourcentyp erstellen.</p>
Workflow	<p>Wählen Sie den Workflow Virtuelle Maschine mit vMotion migrieren aus.</p> <p>Wenn Sie über mehrere vRealize Orchestrator-Integrationen verfügen, wählen Sie den Workflow in der Integrationsinstanz aus, die Sie zum Ausführen dieser benutzerdefinierten Ressourcenaktionen verwenden.</p>

- 2 Erstellen Sie eine Bindung für die vRealize Orchestrator-Eigenschaften an die vRealize Automation Cloud Assembly-Schemaeigenschaften. Tag-2-Aktionen für vRealize Automation Cloud Assembly können drei Typen von Bindungen enthalten.

Bindungstyp	Beschreibung
in Anforderung	Der Standardwert-Bindungstyp. Wenn diese Option ausgewählt ist, wird die Eingabeeigenschaft im Anforderungsformular angezeigt, und ihr Wert muss vom Benutzer zur Anforderungszeit angegeben werden.
mit Bindungsaktion	<p>Diese Option ist nur für Eingaben vom Referenztyp verfügbar, z. B.:</p> <ul style="list-style-type: none"> ■ VC:VirtualMachine ■ VC:Folder <p>Der Benutzer wählt eine Aktion aus, die die Bindung ausführt. Die ausgewählte Aktion muss denselben Typ wie der Eingabeparameter zurückgeben. Die korrekte Eigenschaftsdefinition ist <code>\${properties.someProperty}</code>.</p>
direkt	Diese Option ist für Eingabeeigenschaften verfügbar, die primitive Datentypen verwenden. Wenn diese Option ausgewählt ist, wird die Eigenschaft mit dem geeigneten Typ direkt aus dem Schema der Eingabeeigenschaft zugeordnet. Der Benutzer wählt die Eigenschaft aus der Schemastruktur aus. Eigenschaften mit anderen Typen sind deaktiviert.

In diesem Anwendungsbeispiel ist die Bindung eine vRealize Orchestrator-Aktion, mit der die Verbindung zwischen dem im Workflow verwendeten Eingabetyp vRealize Orchestrator `VC:VirtualMachine` und dem Ressourcentyp vRealize Automation Cloud Assembly `Cloud.vSphere.Machine` hergestellt wird. Indem Sie die Bindung einrichten, integrieren Sie die Tag-2-Aktion nahtlos für den Benutzer, der die vMotion-Aktion auf einer virtuellen vSphere-Maschine anfordert. Das System gibt den Namen im Workflow an, sodass der Benutzer dies nicht tun muss.

- a Navigieren Sie nach dem Auswählen des Workflows **Virtuelle Maschine mit vMotion migrieren** zum Bereich **Eigenschaftsbindung**.

- b Wählen Sie die Bindung der Eingabeeigenschaft `vm` aus.

- c Wählen Sie unter **Bindung** die Option **mit Bindungsaktion** aus.

Die Aktion **findVcVmByVcAndVmUuid** ist automatisch ausgewählt. Diese Aktion ist in der vRealize Orchestrator-Integration in vRealize Automation Cloud Assembly vorkonfiguriert.

- d Klicken Sie auf **Speichern**.

- 3 Um die Änderungen an Ihrer Tag-2-Aktion zu speichern, klicken Sie auf **Erstellen**.

- 4 Um die anderen Eingabeparameter im Workflow zu berücksichtigen, können Sie das Anforderungsformular anpassen, das Benutzern angezeigt wird, wenn sie die Aktion anfordern.

- a Wählen Sie unter **Ressourcenaktionen** die gerade erstellte Tag-2-Aktion aus.
- b Klicken Sie auf **Anforderungsparameter bearbeiten**.

Sie können anpassen, wie die Anforderungsseite den Benutzern angezeigt wird.

Standardfeldname	Darstellung	Werte	Einschränkungen
Zielressourcenpool für die virtuelle Maschine. Der Standardwert ist der aktuelle Ressourcenpool.	<ul style="list-style-type: none"> ■ Beschriftung = Zielressourcenpool ■ Anzeigetyp = Wertauswahl 		
Zielhost, auf den die virtuelle Maschine migriert werden soll	<ul style="list-style-type: none"> ■ Beschriftung = Zielhost ■ Anzeigetyp = Wertauswahl 		Erforderlich = Ja
Priorität der Migrationsaufgabe	Beschriftung = Priorität der Aufgabe	Wertoptionen <ul style="list-style-type: none"> ■ Wertquelle = Konstante Geben Sie im Textfeld eine kommagetrennte Liste ein. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> lowPriority Low,defaultPriority Default,highPriority High </div>	Erforderlich = Ja
(Optional) Migrieren Sie die virtuelle Maschine nur, wenn ihr Betriebszustand mit dem angegebenen Zustand übereinstimmt.	Löschen Sie dieses Textfeld. vMotion kann Maschinen in einen beliebigen Betriebszustand verschieben.		

- c Klicken Sie auf **Speichern**.

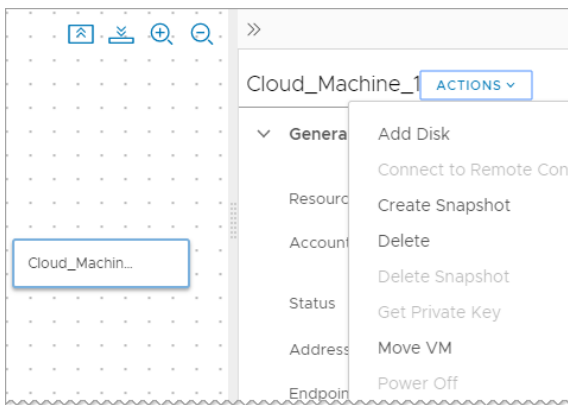
- 5 Um zu begrenzen, wann die Aktion verfügbar ist, können Sie die Bedingungen konfigurieren.

Beispiel: Sie möchten, dass die vMotion-Aktion nur dann zur Verfügung steht, wenn die Maschine vier oder weniger CPUs aufweist.

- a Aktivieren Sie **Bedingung erforderlich**.
- b Geben Sie die Bedingung ein.

Key	Operator	Wert
\${properties.cpuCount}	lessThan	4

- c Klicken Sie auf **Aktualisieren**.
- 6 Stellen Sie sicher, dass die Aktion „VM verschieben“ für bereitgestellte Maschinen verfügbar ist, die den Kriterien entsprechen.
- a Wählen Sie **Bereitstellungen** aus.
 - b Suchen Sie nach einer Bereitstellung mit einer bereitgestellten Maschine, die den Kriterien entspricht.
 - c Öffnen Sie die Bereitstellung und wählen Sie die Maschine aus.
 - d Klicken Sie im rechten Fensterbereich auf „Aktionen“ und stellen Sie sicher, dass die Aktion **Move VM** vorhanden ist.



- e Führen Sie die Aktion aus.

Vorgehensweise zum Erweitern und Automatisieren der Lebenszyklen von Anwendungen mit Erweiterbarkeit

Sie können die Lebenszyklen Ihrer Anwendungen unter Verwendung von Erweiterbarkeitsaktionen oder vRealize Orchestrator-Workflows mit Erweiterbarkeitsabonnements verlängern.

Mithilfe der vRealize Automation Cloud Assembly-Erweiterbarkeit können Sie einem Ereignis unter Verwendung von Abonnements eine Erweiterbarkeitsaktion oder einen vRealize Orchestrator-Workflow zuweisen. Wenn das angegebene Ereignis auftritt, initiiert das Abonnement die auszuführende Aktion oder den auszuführenden Workflow, und alle Abonnenten werden benachrichtigt.

Erweiterbarkeitsaktionen

Bei Erweiterbarkeitsaktionen handelt es sich um kleine, einfache Code-Skripts zur Angabe und Durchführung einer Aktion. Sie können Erweiterbarkeitsaktionen aus vordefinierten vRealize Automation Cloud Assembly-Aktionsvorlagen oder aus einer ZIP-Datei importieren. Zum Erstellen von benutzerdefinierten Skripten für Ihre Erweiterbarkeitsaktionen können Sie auch den Aktions-Editor verwenden. Durch die Verknüpfung mehrerer Aktionsskripts in einem Skript erstellen Sie einen Aktionsablauf. Mithilfe von Aktionsabläufen können Sie eine Abfolge von Aktionen erstellen. Informationen zur Verwendung von Aktionsabläufen finden Sie unter [Definition eines Aktionsablaufs](#).

vRealize Orchestrator-Workflows

Durch die Integration von vRealize Automation Cloud Assembly in Ihre vorhandene vRealize Orchestrator-Umgebung können Sie Workflows in Ihren Erweiterbarkeitsabonnements verwenden.

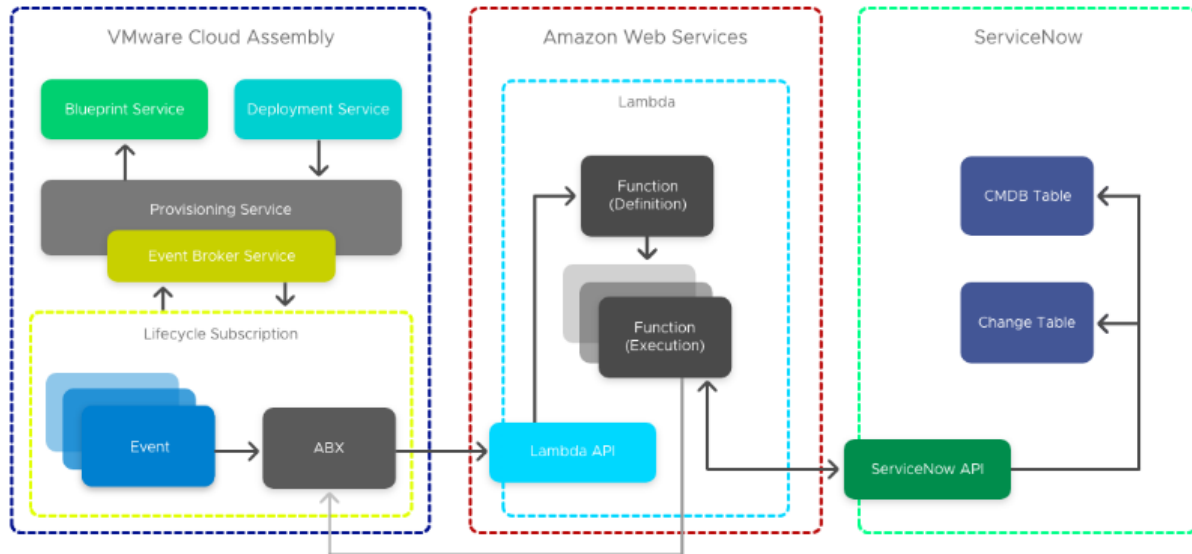
Abonnements für Erweiterbarkeitsaktionen

Sie können einem vRealize Automation Cloud Assembly-Abonnement eine Erweiterbarkeitsaktion zuweisen, um den Lebenszyklus Ihrer Anwendung zu verlängern.

Hinweis Bei den folgenden Abonnements handelt es sich um Anwendungsbeispiele. Sie umfassen nicht alle Funktionen von Erweiterbarkeitsaktionen.

Vorgehensweise zum Integrieren von Cloud Assembly in ServiceNow unter Verwendung von Erweiterbarkeitsaktionen

Mithilfe von Erweiterbarkeitsaktionen können Sie vRealize Automation Cloud Assembly mit einer ITSM-Unternehmenslösung wie ServiceNow integrieren.

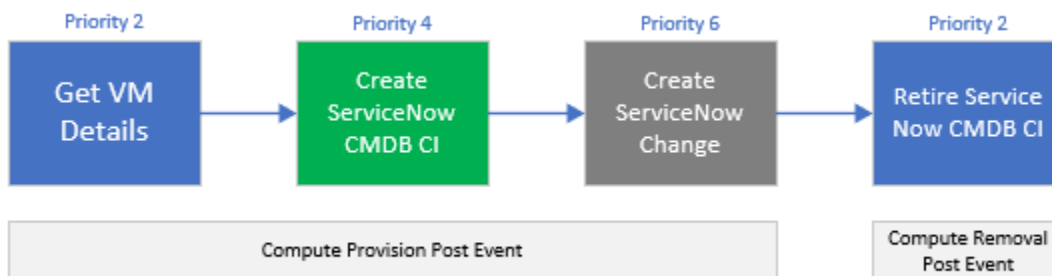


Unternehmensbenutzer integrieren ihre Cloud Management Plattform zu Übereinstimmungszwecken in der Regel mit einer ITSM- (IT Service Management) und einer CMDB-Plattform (Configuration Management Database). Gemäß diesem Beispiel können Sie vRealize Automation Cloud Assembly unter Verwendung von Erweiterbarkeitsaktionsskripts in ServiceNow für CMDB und ITSM integrieren.

Hinweis Sie können ServiceNow auch unter Verwendung von vRealize Orchestrator-Workflows in vRealize Automation Cloud Assembly integrieren. Informationen zum Integrieren von ServiceNow mithilfe von Workflows finden Sie unter [Vorgehensweise zum Integrieren von Cloud Assembly für ITSM mit ServiceNow unter Verwendung von vRealize Orchestrator-Workflows](#).

Zum Erstellen dieser Integration verwenden Sie vier Erweiterbarkeitsaktionsskripts. Die ersten drei Skripts werden nacheinander während der Bereitstellung beim Compute-Bereitstellungs-Post-Ereignis initiiert. Das vierte Skript löst das Compute-Entfernungs-Post-Ereignis aus.

Weitere Informationen zu Ereignisthemen finden Sie unter [Mit vRealize Automation Cloud Assembly bereitgestellte Ereignisthemen](#).



VM-Details abrufen

Das Skript zum Abrufen von VM-Details erfasst zusätzliche Nutzlastdetails, die für die CI-Erstellung erforderlich sind, sowie ein Identitätstoken, das in Amazon Web Services Systems Manager Parameter Store (SSM) gespeichert ist. Außerdem aktualisiert dieses Skript `customProperties` mit zusätzlichen Eigenschaften für die spätere Verwendung.

ServiceNow-CMDB-Konfigurationselement erstellen

Das Skript zum Erstellen des ServiceNow-CMDB-Konfigurationselements übergibt die Instanz-URL von ServiceNow als Eingabe und speichert die Instanz in SSM, um die Sicherheitsanforderungen zu erfüllen. Dieses Skript liest auch die Antwort der eindeutigen Datensatz-ID (`sys_id`) der ServiceNow-CMDB. Es übergibt die Antwort als Ausgabe und schreibt die benutzerdefinierte Eigenschaft `serviceNowSysId` während der Erstellung. Dieser Wert wird verwendet, um das Konfigurationselement als veraltet zu markieren, wenn die Instanz gelöscht wird.

Hinweis Unter Umständen müssen Ihrer Amazon Web Services-Rolle für vRealize Automation services zusätzliche Berechtigungen zugewiesen werden, damit Lambda auf den SSM-Parameterspeicher zugreifen kann.

ServiceNow-Änderung erstellen

Dieses Skript beendet die ITSM-Integration, indem die Instanz-URL von ServiceNow als Eingabe übergeben und die ServiceNow-Anmeldedaten als SSM gespeichert werden, um die Sicherheitsanforderungen zu erfüllen.

ServiceNow-Änderung erstellen

Das Skript zum Zurückziehen des ServiceNow-CMDB-Konfigurationselements fordert ServiceNow zum Anhalten auf und markiert das Konfigurationselement basierend auf der benutzerdefinierten Eigenschaft `serviceNowSysId`, die im Erstellungsskript erstellt wurde, als veraltet.

Voraussetzungen

- Bevor Sie diese Integration konfigurieren, filtern Sie alle Ereignisabonnements mit der bedingten Cloud-Vorlageneigenschaft: `event.data["customProperties"]`
`["enable_servicenow"] == "true"`

Hinweis Diese Eigenschaft ist in Cloud-Vorlagen vorhanden, die eine ServiceNow-Integration benötigen.

- Laden Sie Python herunter und installieren Sie es.

Weitere Informationen zum Filtern von Abonnements finden Sie unter [Erstellen eines Erweiterbarkeitsabonnements](#).

Verfahren

- 1 Öffnen Sie eine Eingabeaufforderung auf Ihrer virtuellen Maschine.

2 Führen Sie das Skript zum Abrufen von VM-Details aus.

```

from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):
    baseUrl = inputs['url']
    casToken = client.get_parameter(Name="casToken",WithDecryption=True)

    url = baseUrl + "/iaas/login"
    headers = {"Accept":"application/json","Content-Type":"application/json"}
    payload = {"refreshToken":casToken['Parameter']['Value']}

    results = requests.post(url,json=payload,headers=headers)

    bearer = "Bearer "
    bearer = bearer + results.json()["token"]

    deploymentId = inputs['deploymentId']
    resourceId = inputs['resourceIds'][0]

    print("deploymentId: " + deploymentId)
    print("resourceId: " + resourceId)

    machineUri = baseUrl + "/iaas/machines/" + resourceId
    headers = {"Accept":"application/json","Content-Type":"application/json",
"Authorization":bearer }
    resultMachine = requests.get(machineUri,headers=headers)
    print("machine: " + resultMachine.text)

    print( "serviceNowCPUCount: " + json.loads(resultMachine.text)["customProperties"]
["cpuCount"] )
    print( "serviceNowMemoryInMB: " + json.loads(resultMachine.text)["customProperties"]
["memoryInMB"] )

    #update customProperties
    outputs = {}
    outputs['customProperties'] = inputs['customProperties']
    outputs['customProperties']['serviceNowCPUCount'] = int(json.loads(resultMachine.text)
["customProperties"]["cpuCount"])
    outputs['customProperties']['serviceNowMemoryInMB'] = json.loads(resultMachine.text)
["customProperties"]["memoryInMB"]
    return outputs

```

3 Führen Sie die Aktion zur Erstellung des CMDB-Konfigurationselements aus.

```

from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):

```

```

snowUser = client.get_parameter(Name="serviceNowUserName",WithDecryption=False)
snowPass = client.get_parameter(Name="serviceNowPassword",WithDecryption=True)
table_name = "cmdb_ci_vmware_instance"
url = "https://" + inputs['instanceUrl'] + "/api/now/table/{0}".format(table_name)
headers = {'Content-type': 'application/json', 'Accept': 'application/json'}
payload = {
    'name': inputs['customProperties']['serviceNowHostname'],
    'cpus': int(inputs['customProperties']['serviceNowCPUCount']),
    'memory': inputs['customProperties']['serviceNowMemoryInMB'],
    'correlation_id': inputs['deploymentId'],
    'disks_size': int(inputs['customProperties']['provisionGB']),
    'location': "Sydney",
    'vcenter_uuid': inputs['customProperties']['vcUuid'],
    'state': 'On',
    'sys_created_by': inputs['__metadata']['userName'],
    'owned_by': inputs['__metadata']['userName']
}
results = requests.post(
    url,
    json=payload,
    headers=headers,
    auth=(snowUser['Parameter']['Value'], snowPass['Parameter']['Value'])
)
print(results.text)

#parse response for the sys_id of CMDB CI reference
if json.loads(results.text)['result']:
    serviceNowResponse = json.loads(results.text)['result']
    serviceNowSysId = serviceNowResponse['sys_id']
    print(serviceNowSysId)

#update the serviceNowSysId customProperty
outputs = {}
outputs['customProperties'] = inputs['customProperties']
outputs['customProperties']['serviceNowSysId'] = serviceNowSysId;
return outputs

```

4 Führen Sie das Erstellungsaktionsskript aus.

```

from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):
    snowUser = client.get_parameter(Name="serviceNowUserName",WithDecryption=False)
    snowPass = client.get_parameter(Name="serviceNowPassword",WithDecryption=True)
    table_name = "change_request"
    url = "https://" + inputs['instanceUrl'] + "/api/now/table/{0}".format(table_name)
    headers = {'Content-type': 'application/json', 'Accept': 'application/json'}
    payload = {
        'short_description': 'Provision CAS VM Instance'
    }
    results = requests.post(
        url,

```

```

        json=payload,
        headers=headers,
        auth=(snowUser['Parameter']['Value'], snowPass['Parameter']['Value'])
    )
    print(results.text)

```

Ergebnisse

vRealize Automation Cloud Assembly wurde erfolgreich in ITSM-Lösung ServiceNow integriert.

Nächste Schritte

Wenn Sie möchten, können Sie das Konfigurationselement mithilfe der Aktion zum Zurückziehen des CMDB-Konfigurationselements als veraltet markieren:

```

from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):
    snowUser = client.get_parameter(Name="serviceNowUserName",WithDecryption=False)
    snowPass = client.get_parameter(Name="serviceNowPassword",WithDecryption=True)
    tableName = "cmdb_ci_vmware_instance"
    sys_id =inputs['customProperties']['serviceNowSysId']
    url = "https://" + inputs['instanceUrl'] + "/api/now/"+tableName+"/"+sys_id
    headers = {'Content-type': 'application/json', 'Accept': 'application/json'}
    payload = {
        'state': 'Retired'
    }

    results = requests.put(
        url,
        json=payload,
        headers=headers,
        auth=(inputs['username'], inputs['password'])
    )
    print(results.text)

```

Weitere Informationen zur Verwendung von Erweiterbarkeitsaktionen für die Integration von ServiceNow in vRealize Automation Cloud Assembly finden Sie im Blogbeitrag [Extending Cloud Assembly with Action Based Extensibility for ServiceNow Integration](#), der die Erweiterung von Cloud Assembly mit aktionsbasierter Erweiterbarkeit für die ServiceNow-Integration behandelt.

Vorgehensweise zum Taggen virtueller Maschinen während der Bereitstellung mithilfe von Erweiterbarkeitsaktionen

Sie können Erweiterbarkeitsaktionen in Verbindung mit Abonnements verwenden, um das Tagging von VMs zu automatisieren und zu vereinfachen.

Als Cloud-Administrator können Sie Bereitstellungen, die automatisch mit bestimmten Eingaben und Ausgaben gekennzeichnet werden, unter Verwendung von Erweiterbarkeitsaktionen und -abonnements erstellen. Wenn eine neue Bereitstellung für das Projekt erstellt wird, das das Abonnement zum Kennzeichnen der VM enthält, löst das Bereitstellungsereignis die Ausführung des Skripts „VM kennzeichnen“ aus und die Tags werden automatisch angewendet. Dies spart Zeit und fördert die Effizienz bei gleichzeitiger Vereinfachung der Bereitstellungsverwaltung.

Voraussetzungen

- Zugriff auf Anmeldedaten für Cloud-Administrator.
- Amazon Web Services-Rolle für Lambda-Funktionen.

Verfahren

- 1 Navigieren Sie zu **Erweiterbarkeit > Bibliothek > Aktionen > Neue Aktion** und erstellen Sie eine Aktion mit den folgenden Parametern.

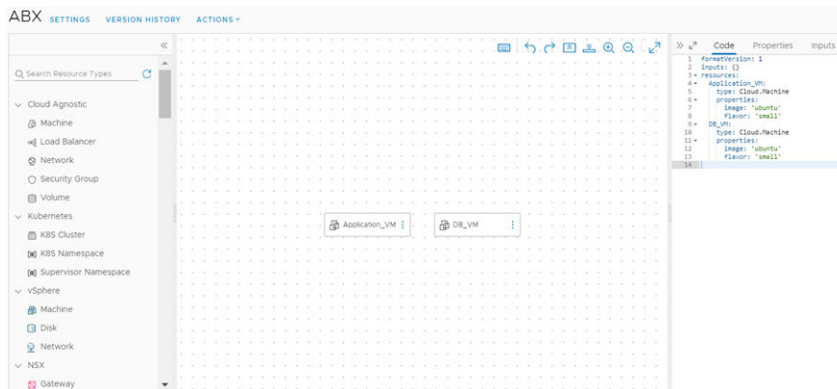
Parameter	Beschreibung
Aktionsname	Name der Erweiterbarkeitsaktion, vorzugsweise mit TagVM als Präfix oder Suffix.
Projekt	Projekt zum Testen der Erweiterbarkeitsaktion.
Aktionsvorlage	Tag VM
Laufzeit	Python
Skriptquelle	Skript schreiben

- 2 Geben Sie **Handler** als **Hauptfunktion** ein.
- 3 Fügen Sie Tagging-Eingaben zum Testen der Erweiterbarkeitsaktion hinzu.
Beispiel: `resourceNames = ["DB_VM"]` und `target = world`.
- 4 Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.
- 5 Klicken Sie auf **Test**, um die Aktion zu testen.
- 6 Klicken Sie auf **Schließen**, um den Aktions-Editor zu beenden.
- 7 Navigieren Sie zu **Erweiterbarkeit > Abonnements**.
- 8 Klicken Sie auf **Neues Abonnement**.

9 Geben Sie die folgenden Abonnementdetails ein.

Details	Einstellung
Ereignisthema	Wählen Sie ein Ereignisthema aus, das sich auf die Kennzeichnungsphase der VM bezieht. Beispiel: Computing-Zuteilung. Hinweis Tags müssen Teil der Ereignisparameter des ausgewählten Ereignisthemas sein.
Wird blockiert	Legen Sie als Zeitüberschreitung für das Abonnement 1 Minute fest.
Aktion/Workflow	Wählen Sie einen ausführbaren Typ der Erweiterbarkeitsaktion aus und wählen Sie Ihre benutzerdefinierte Erweiterbarkeitsaktion aus.

- Klicken Sie auf **Speichern**, um Ihr benutzerdefiniertes Abonnement für Erweiterbarkeitsaktionen zu speichern.
- Navigieren Sie zu **Design > Cloud-Vorlagen** und erstellen Sie eine Cloud-Vorlage auf einer leeren Arbeitsfläche.
- Fügen Sie zwei virtuelle Maschinen zur Cloud-Vorlage hinzu: `Application_VM` und `DB_VM`.



- Klicken Sie auf **Bereitstellen**, um die VMs bereitzustellen.
- Stellen Sie während der Bereitstellung sicher, dass das Ereignis initiiert und die Erweiterbarkeitsaktion ausgeführt wird.
- Um zu überprüfen, ob die Tags korrekt angewendet wurden, navigieren Sie zu **Infrastruktur > Ressourcen > Maschinen**.

Weitere Informationen zu Erweiterbarkeitsaktionen

Bei der aktionsbasierten Erweiterbarkeit (ABX) werden optimierte Codeskripts in vRealize Automation Cloud Assembly verwendet, um Erweiterbarkeitsaktionen zu automatisieren.

Die aktionsbasierte Erweiterbarkeit stellt eine einfache und flexible Laufzeit-Engine-Schnittstelle bereit, auf der Sie kleine skriptfähige Aktionen definieren und so konfigurieren können, dass sie bei Auftreten von Ereignissen, die in Erweiterbarkeitsabonnements angegeben sind, initiiert werden.

Sie können diese Erweiterbarkeitsaktionsskripts in vRealize Automation Cloud Assembly oder Ihrer lokalen Umgebung erstellen und sie Abonnements zuweisen. Erweiterbarkeitsaktionsskripts werden verwendet, um Aufgaben und Schritte schnell und einfach zu automatisieren. Weitere Informationen zur Integration von vRealize Automation Cloud Assembly in einen vRealize Orchestrator-Server finden Sie unter [Konfigurieren der vRealize Orchestrator-Integration in Cloud Assembly](#).

Die aktionsbasierte Erweiterbarkeit bietet Folgendes:

- Eine Alternative zu vRealize Orchestrator-Workflows, die kleine und wiederverwendbare skriptfähige Aktionen für einfache Integrationen und Anpassungen verwendet.
- Eine Möglichkeit zur Wiederverwendung von Aktionsvorlagen, die wiederverwendbare parametrisierte Aktionen enthalten.

Sie können Erweiterbarkeitsaktionen erstellen, indem Sie entweder einen benutzerdefinierten Aktionsskriptcode schreiben oder einen vordefinierten Skriptcode als ZIP-Paket importieren. Aktionsbasierte Erweiterbarkeit bietet Unterstützung für die Laufzeitumgebungen Node.js, Python und PowerShell. Die Node.js- und Python-Laufzeiten sind auf Amazon Web Services-Lambda angewiesen. Aus diesem Grund benötigen Sie ein aktives Abonnement bei Amazon Web Services Identity and Access Management (IAM) und müssen Amazon Web Services als Endpoint in vRealize Automation Cloud Assembly konfigurieren. Informationen zu den ersten Schritten mit Amazon Web Services Lambda finden Sie unter [ABX: Serverlose Erweiterbarkeit von Cloud Assembly-Diensten](#).

Hinweis Erweiterbarkeitsaktionen sind projektspezifisch.

Vorgehensweise zum Erstellen von Erweiterbarkeitsaktionen

Mit vRealize Automation Cloud Assembly können Sie Erweiterbarkeitsaktionen zur Verwendung in Erweiterbarkeitsabonnements erstellen.

Bei Erweiterbarkeitsaktionen handelt es sich um äußerst anpassbare, einfache und flexible Methoden zum Verlängern des Lebenszyklus einer Anwendung mithilfe von benutzerdefiniertem Skriptcode und Aktionsvorlagen. Aktionsvorlagen enthalten vordefinierte Parameter, die beim Einrichten der Grundlage Ihrer Erweiterbarkeitsaktion hilfreich sind.

Es gibt zwei Methoden zum Erstellen einer Erweiterbarkeitsaktion:

- Schreiben von benutzerdefiniertem Code für ein Skript für Erweiterbarkeitsaktionen.

Hinweis Das Schreiben von benutzerdefiniertem Code im Erweiterbarkeitsaktionseditor erfordert möglicherweise eine aktive Internetverbindung.

- Importieren eines Bereitstellungspakets als ZIP-Paket für eine Erweiterbarkeitsaktion. Informationen zum Erstellen eines ZIP-Pakets für Erweiterbarkeitsaktionen finden Sie unter [Erstellen eines ZIP-Pakets für Erweiterbarkeitsaktionen der Python-Laufzeit](#), [Erstellen eines ZIP-Pakets für Erweiterbarkeitsaktionen der Node.js-Laufzeit](#) oder [Erstellen eines ZIP-Pakets für Erweiterbarkeitsaktionen der PowerShell-Laufzeit](#).

In den folgenden Schritten wird die Vorgehensweise zum Erstellen einer Erweiterbarkeitsaktion beschrieben, die Amazon Web Services als FaaS-Anbieter verwendet.

Voraussetzungen

- Mitgliedschaft in einem aktiven und gültigen Projekt.
- Konfigurierte Amazon Web Services-Rolle für Lambda-Funktionen. Beispiel: `AWSLambdaBasicExecutionRole`.
- Aktivierte Cloud-Administratorrolle oder `iam:PassRole`-Berechtigungen.

Verfahren

- 1 Klicken Sie auf **Erweiterbarkeit > Bibliothek > Aktionen**.
- 2 Klicken Sie auf **Neue Aktion**.
- 3 Geben Sie einen Namen für die Aktion ein und wählen Sie ein Projekt aus.
- 4 Klicken Sie auf **Weiter**.
- 5 Suchen Sie nach einer Aktionsvorlage und wählen Sie sie aus.

Hinweis Um eine benutzerdefinierte Aktion ohne Verwendung einer Aktionsvorlage zu erstellen, wählen Sie **Benutzerdefiniertes Skript** aus.

Neue konfigurierbare Parameter werden angezeigt.

- 6 Wählen Sie **Skript schreiben** oder **Paket importieren** aus.
- 7 Wählen Sie die Aktionslaufzeit aus.
- 8 Geben Sie einen Namen für die **Hauptfunktion** für den Einstiegspunkt der Aktion ein.

Hinweis Für Aktionen, die aus einem ZIP-Paket importiert werden, muss die Hauptfunktion auch den Namen der Skriptdatei mit dem Einstiegspunkt enthalten. Wenn die Hauptskriptdatei beispielsweise den Namen `main.py` aufweist und `handler (context, inputs)` als Einstiegspunkt verwendet wird, muss der Name der Hauptfunktion `main.handler` lauten.

- 9 Legen Sie die **Eingabe**- und **Ausgabe**-Parameter der Aktion fest.

10 (Optional) Fügen Sie Anwendungsabhängigkeiten zur Aktion hinzu.

Hinweis Für-PowerShell-Skripts können Sie Ihre Anwendungsabhängigkeiten definieren, sodass sie über das PowerShell Gallery-Repository aufgelöst werden. Um Ihre Anwendungsabhängigkeiten so zu definieren, dass sie über das öffentliche Repository aufgelöst werden können, verwenden Sie das folgende Format:

```
@{
    Name = 'Version'
}

e.g.

@{
    Pester = '4.3.1'
}
```

Hinweis Für Aktionen, die aus einem ZIP-Paket importiert werden, werden Anwendungsabhängigkeiten automatisch hinzugefügt.

- 11 Um Zeitüberschreitungs- und Arbeitsspeichergrenzwerte festzulegen, aktivieren Sie die Option **Benutzerdefinierte Zeitüberschreitung und Grenzwerte festlegen**.
- 12 Um Ihre Aktion zu testen, klicken Sie auf **Speichern** und dann auf **Testen**.

Nächste Schritte

Nachdem Ihre Erweiterbarkeitsaktion erstellt und überprüft wurde, können Sie sie einem Abonnement zuweisen.

Hinweis Erweiterbarkeitsabonnements verwenden die neueste freigegebene Version einer Erweiterbarkeitsaktion. Nachdem Sie eine neue Version einer Aktion erstellt haben, klicken Sie oben rechts im Editor-Fenster auf **Versionen**. Um die Version der Aktion, die Sie in Ihrem Abonnement verwenden möchten, freizugeben, klicken Sie auf **Freigeben**.

Erstellen eines ZIP-Pakets für Erweiterbarkeitsaktionen der Python-Laufzeit

Sie können ein ZIP-Paket mit dem Python-Skript und Abhängigkeiten erstellen, die von Ihren vRealize Automation Cloud Assembly-Erweiterbarkeitsaktionen verwendet werden.

Zwei Methoden stehen zur Erstellung des Skripts für Ihre Erweiterbarkeitsaktionen zur Verfügung:

- Direktes Schreiben des Skripts im Erweiterbarkeitsaktionseditor in vRealize Automation Cloud Assembly.
- Erstellen des Skripts in Ihrer lokalen Umgebung und Hinzufügen des Skripts zu einem ZIP-Paket mit allen relevanten Abhängigkeiten.

Mithilfe eines ZIP-Pakets können Sie eine benutzerdefinierte vorkonfigurierte Vorlage mit Aktionsskripts und Abhängigkeiten erstellen, die Sie zur Verwendung in Erweiterbarkeitsaktionen in vRealize Automation Cloud Assembly importieren können.

Darüber hinaus können Sie ein ZIP-Paket in Szenarien verwenden, in denen Module, die mit Abhängigkeiten in Ihrem Aktionsskript verknüpft sind, nicht vom vRealize Automation Cloud Assembly-Dienst aufgelöst werden können. Dies ist beispielsweise der Fall, wenn kein Internetzugriff in Ihrer Umgebung möglich ist.

Sie können auch ein ZIP-Paket verwenden, um Erweiterbarkeitsaktionen mit mehreren Python-Skriptdateien zu erstellen. Die Verwendung mehrerer Skriptdateien kann nützlich sein, um die Struktur des Codes der Erweiterbarkeitsaktionen zu verwalten.

Voraussetzungen

Laden Sie bei Verwendung von Python 3.3 oder früher das Installationsprogramm für das PIP-Paket herunter und konfigurieren Sie es. Weitere Informationen finden Sie im [Python-Paketindex](#).

Verfahren

- 1 Erstellen Sie auf Ihrem lokalen Computer einen Ordner für das Aktionsskript und die Abhängigkeiten.
Beispiel: `/home/user1/zip-action`.
- 2 Fügen Sie dem Ordner das Python-Hauptaktionsskript oder Skripts hinzu.
Beispiel: `/home/user1/zip-action/main.py`.
- 3 (Optional) Fügen Sie dem Ordner alle Abhängigkeiten für das Python-Skript hinzu.
 - a Erstellen Sie eine Datei vom Typ `requirements.txt`, die die Abhängigkeiten enthält. Weitere Informationen finden Sie unter [Anforderungsdateien](#).
 - b Öffnen Sie eine Linux-Shell.

Hinweis Die Laufzeit der aktionsbasierten Erweiterbarkeit (ABX) in vRealize Automation Cloud Assembly ist Linux-basiert. Aus diesem Grund machen in einer Windows-Umgebung kompilierte Python-Abhängigkeiten das erzeugte ZIP-Paket für die Erstellung von Erweiterbarkeitsaktionen möglicherweise unbrauchbar. Deshalb müssen Sie eine Linux-Shell verwenden.

- c Installieren Sie die Datei `requirements.txt` im Skriptordner, indem Sie den folgenden Befehl ausführen:

```
pip install -r requirements.txt --target=home/user1/zip-action
```

- 4 Wählen Sie im zugewiesenen Ordner die Skriptelemente und gegebenenfalls die Datei `requirements.txt` aus und komprimieren Sie die Elemente in einem ZIP-Paket.

Hinweis Sowohl die Skript- als auch die Abhängigkeitselemente müssen auf der Root-Ebene des ZIP-Pakets gespeichert werden. Beim Erstellen des ZIP-Pakets in einer Linux-Umgebung tritt möglicherweise ein Problem auf, wenn der Paketinhalt nicht auf der Root-Ebene gespeichert wird. Wenn dieses Problem auftritt, erstellen Sie das Paket, indem Sie den Befehl `zip -r` in der Befehlszeilen-Shell ausführen.

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

Nächste Schritte

Verwenden Sie das ZIP-Paket, um ein Erweiterbarkeitsaktionsskript zu erstellen.

Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Erstellen von Erweiterbarkeitsaktionen](#).

Erstellen eines ZIP-Pakets für Erweiterbarkeitsaktionen der Node.js-Laufzeit

Sie können ein ZIP-Paket mit dem Skript „Node.js“ und Abhängigkeiten erstellen, die von Ihren vRealize Automation Cloud Assembly-Erweiterbarkeitsaktionen verwendet werden.

Zwei Methoden stehen zur Erstellung des Skripts für Ihre Erweiterbarkeitsaktionen zur Verfügung:

- Direktes Schreiben des Skripts im Erweiterbarkeitsaktionseditor in vRealize Automation Cloud Assembly.
- Erstellen des Skripts in Ihrer lokalen Umgebung und Hinzufügen des Skripts zu einem ZIP-Paket mit allen relevanten Abhängigkeiten.

Mithilfe eines ZIP-Pakets können Sie eine benutzerdefinierte vorkonfigurierte Vorlage mit Aktionsskripts und Abhängigkeiten erstellen, die Sie zur Verwendung in Erweiterbarkeitsaktionen in vRealize Automation Cloud Assembly importieren können.

Darüber hinaus können Sie ein ZIP-Paket in Szenarien verwenden, in denen Module, die mit Abhängigkeiten in Ihrem Aktionsskript verknüpft sind, nicht vom vRealize Automation Cloud Assembly-Dienst aufgelöst werden können. Dies ist beispielsweise der Fall, wenn kein Internetzugriff in Ihrer Umgebung möglich ist.

Weiterhin können Sie Pakete verwenden, um Erweiterbarkeitsaktionen mit mehreren Node.js-Skriptdateien zu erstellen. Die Verwendung mehrerer Skriptdateien kann nützlich sein, um die Struktur des Codes der Erweiterbarkeitsaktionen zu verwalten.

Verfahren

- 1 Erstellen Sie auf Ihrem lokalen Computer einen Ordner für das Aktionsskript und die Abhängigkeiten.

Beispiel: `/home/user1/zip-action`.

- 2 Fügen Sie dem Ordner das Hauptaktionsskript „Node.js“ oder Skripts hinzu.

Beispiel: `/home/user1/zip-action/main.js`.

- 3 (Optional) Fügen Sie dem Ordner alle Abhängigkeiten für das Skript „Node.js“ hinzu.
 - a Erstellen Sie eine Datei vom Typ `package.json` mit Abhängigkeiten im Skriptordner. Weitere Informationen finden Sie unter [Erstellen einer package.json-Datei](#) und [Angaben von „dependencies“ und „devDependencies“ in einer package.json-Datei](#).
 - b Öffnen Sie eine Befehlszeilen-Shell.
 - c Navigieren Sie zu dem Ordner, den Sie für das Aktionsskript und die Abhängigkeiten erstellt haben.

```
cd /home/user1/zip-action
```

- d Installieren Sie die Datei `package.json` im Skriptordner, indem Sie den folgenden Befehl ausführen:

```
npm install --production
```

Hinweis Mit diesem Befehl wird ein Verzeichnis vom Typ `node_modules` in Ihrem Ordner erstellt.

- 4 Wählen Sie im zugewiesenen Ordner die Skriptelemente und gegebenenfalls das Verzeichnis `node_modules` aus und komprimieren Sie die Elemente in einem ZIP-Paket.

Hinweis Sowohl die Skript- als auch die Abhängigkeitselemente müssen auf der Root-Ebene des ZIP-Pakets gespeichert werden. Beim Erstellen des ZIP-Pakets in einer Linux-Umgebung tritt möglicherweise ein Problem auf, wenn der Paketinhalt nicht auf der Root-Ebene gespeichert wird. Wenn dieses Problem auftritt, erstellen Sie das Paket, indem Sie den Befehl `zip -r` in der Befehlszeilen-Shell ausführen.

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

Nächste Schritte

Verwenden Sie das ZIP-Paket, um ein Erweiterbarkeitsaktionsskript zu erstellen. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Erstellen von Erweiterbarkeitsaktionen](#).

Erstellen eines ZIP-Pakets für Erweiterbarkeitsaktionen der PowerShell-Laufzeit
Sie können ein ZIP-Paket erstellen, das Ihr PowerShell-Skript und Abhängigkeitsmodule für die Verwendung in Erweiterbarkeitsaktionen enthält.

Zwei Methoden stehen zur Erstellung des Skripts für Ihre Erweiterbarkeitsaktionen zur Verfügung:

- Direktes Schreiben des Skripts im Erweiterbarkeitsaktionseditor in vRealize Automation Cloud Assembly.
- Erstellen des Skripts in Ihrer lokalen Umgebung und Hinzufügen des Skripts zu einem ZIP-Paket mit allen relevanten Abhängigkeiten.

Mithilfe eines ZIP-Pakets können Sie eine benutzerdefinierte vorkonfigurierte Vorlage mit Aktionsskripts und Abhängigkeiten erstellen, die Sie zur Verwendung in Erweiterbarkeitsaktionen in vRealize Automation Cloud Assembly importieren können.

Hinweis Es ist nicht erforderlich, PowerCLI-Cmdlets als Abhängigkeiten zu definieren oder sie in einem ZIP-Paket bündeln. PowerCLI-Cmdlets sind in der PowerShell-Laufzeit Ihres vRealize Automation Cloud Assembly-Dienstes vorkonfiguriert.

Darüber hinaus können Sie ein ZIP-Paket in Szenarien verwenden, in denen Module, die mit Abhängigkeiten in Ihrem Aktionsskript verknüpft sind, nicht vom vRealize Automation Cloud Assembly-Dienst aufgelöst werden können. Dies ist beispielsweise der Fall, wenn kein Internetzugriff in Ihrer Umgebung möglich ist.

Sie können auch ein ZIP-Paket verwenden, um Erweiterbarkeitsaktionen mit mehreren PowerShell-Skriptdateien zu erstellen. Die Verwendung mehrerer Skriptdateien kann nützlich sein, um die Struktur des Codes der Erweiterbarkeitsaktionen zu verwalten.

Voraussetzungen

Sie sollten mit PowerShell und PowerCLI vertraut sein. Ein Docker-Image mit PowerShell Core, PowerCLI 10, PowerNSX und mehreren Community-Modulen und Skriptbeispielen finden Sie im [Docker Hub](#).

Verfahren

- 1 Erstellen Sie auf Ihrem lokalen Computer einen Ordner für das Aktionsskript und die Abhängigkeiten.

Beispiel: `/home/user1/zip-action`.

- 2 Fügen Sie das PowerShell-Hauptskript mit einer Erweiterung vom Typ `.psm1` zum Ordner hinzu.

Das folgende Skript enthält eine einfache PowerShell-Funktion mit dem Namen `main.psm1`:

```
function handler($context, $payload) {
    Write-Host "Hello " $payload.target
}
```



```
return $payload
```

Hinweis Die Ausgabe einer PowerShell-Erweiterbarkeitsaktion basiert auf der letzten Variable, die im Textkörper der Funktion angezeigt wird. Alle anderen Variablen in der eingeschlossenen Funktion werden verworfen.

- 3 (Optional) Fügen Sie dem PowerShell-Hauptskript eine Proxy-Konfiguration mithilfe von `context`-Parametern hinzu. Weitere Informationen hierzu finden Sie unter [Verwenden von Kontextparametern zum Hinzufügen einer Proxykonfiguration zum PowerShell-Skript](#).
- 4 (Optional) Fügen Sie alle Abhängigkeiten für Ihr PowerShell-Skript hinzu.

Hinweis Ihr PowerShell-Abhängigkeitsskript muss die Erweiterung `.psm1` verwenden. Verwenden Sie denselben Namen für das Skript und den Unterordner, in dem das Skript gespeichert wird.

- a Melden Sie sich bei einer Linux PowerShell-Shell an.

Hinweis Die Laufzeit der aktionsbasierten Erweiterbarkeit (ABX) in vRealize Automation Cloud Assembly ist Linux-basiert. Durch in einer Windows-Umgebung kompilierte PowerShell-Abhängigkeiten kann das generierte ZIP-Paket unbrauchbar werden. Alle installierten Abhängigkeiten von Drittanbietern müssen mit dem VMware Photon OS kompatibel sein, da PowerShell-Skripts auf Photon OS ausgeführt werden.

- b Navigieren Sie zum Ordner `/home/user1/zip-action`.
- c Laden Sie das PowerShell-Modul mit Ihren Abhängigkeiten herunter und speichern Sie es, indem Sie das `Save-Module`-Cmdlet ausführen.

```
Save-Module -Name <module name> -Path ./
```

- d Wiederholen Sie den vorherigen Teilschritt für alle zusätzlichen Abhängigkeitsmodule.

Wichtig Stellen Sie sicher, dass sich jedes Abhängigkeitsmodul in einem eigenen Unterordner befindet. Weitere Informationen zum Schreiben und Verwalten von PowerShell-Modulen finden Sie in der [Vorgehensweise zum Schreiben eines PowerShell-Skriptmoduls](#).

- Wählen Sie im zugewiesenen Ordner die Skriptelemente und gegebenenfalls die Unterordner des Abhängigkeitsmoduls aus und komprimieren Sie die Elemente in einem ZIP-Paket.

Hinweis Sowohl die Skript- als auch die Abhängigkeitsmodul-Unterordner müssen auf der Root-Ebene des ZIP-Pakets gespeichert werden. Beim Erstellen des ZIP-Pakets in einer Linux-Umgebung tritt möglicherweise ein Problem auf, wenn der Paketinhalt nicht auf der Root-Ebene gespeichert wird. Wenn dieses Problem auftritt, erstellen Sie das Paket, indem Sie den Befehl `zip -r` in der Befehlszeilen-Shell ausführen.

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

Nächste Schritte

Verwenden Sie das ZIP-Paket, um ein Erweiterbarkeitsaktionsskript zu erstellen.

Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Erstellen von Erweiterbarkeitsaktionen](#).

Verwenden von Kontextparametern zum Hinzufügen einer Proxykonfiguration zum PowerShell-Skript

Sie können die Netzwerk-Proxykommunikation in Ihrem PowerShell-Skript mithilfe von `context`-Parametern aktivieren.

Für bestimmte PowerShell-Cmdlets muss unter Umständen ein Netzwerk-Proxy als Umgebungsvariable in der PowerShell-Funktion festgelegt werden. Proxykonfigurationen werden für die PowerShell-Funktion mit den Parametern `$context.proxy.host` und `$context.proxy.port` bereitgestellt.

Sie können diese `context`-Parameter am Anfang des PowerShell-Skripts einfügen.

```
$proxyString = "http://" + $context.proxy.host + ":" + $context.proxy.port
$Env:HTTP_PROXY = $proxyString
$Env:HTTPS_PROXY = $proxyString
```

Wenn die Cmdlets den Parameter `-Proxy` unterstützen, können Sie den Proxywert auch direkt an die spezifischen PowerShell-Cmdlets übergeben.

Konfigurieren von Cloud-spezifischen Erweiterbarkeitsaktionen

Sie können Erweiterbarkeitsaktionen so konfigurieren, dass sie mit Ihren Cloud-Konten verwendet werden können.

Beim Erstellen einer Erweiterbarkeitsaktion können Sie sie mit verschiedenen Cloud-basierten Konten konfigurieren und verknüpfen:

- Microsoft Azure
- Amazon Web Services

Voraussetzungen

Ein gültiges Cloud-Konto ist erforderlich.

Verfahren

- 1 Wählen Sie **Erweiterbarkeit > Bibliothek > Aktion**.
- 2 Klicken Sie auf **Neue Aktion**.
- 3 Geben Sie die Aktionsparameter nach Bedarf an.
- 4 Wählen Sie im Dropdown-Menü **FaaS-Anbieter** Ihren Cloud-Kontoanbieter aus oder wählen Sie **Auto** aus.

Hinweis Wenn Sie **Automatisch** auswählen, wird der FaaS-Anbieter automatisch von der Aktion festgelegt.

- 5 Klicken Sie auf **Speichern**.

Ergebnisse

Ihre Erweiterbarkeitsaktion ist für die Verwendung mit dem konfigurierten Cloud-Konto verknüpft. Konfigurieren lokaler Erweiterbarkeitsaktionen

Sie können Ihre Erweiterbarkeitsaktionen für die Verwendung eines lokalen FaaS-Anbieters anstelle eines Amazon Web Services- oder Microsoft Azure-Cloud-Kontos konfigurieren.

Indem Sie einen lokalen FaaS-Anbieter für Ihre Erweiterbarkeitsaktionen verwenden, können Sie lokale Dienste wie LDAP, CMDB oder vCenter-Datencenter in Ihren vRealize Automation Cloud Assembly-Erweiterbarkeitsabonnements verwenden.

Verfahren

- 1 Klicken Sie auf **Erweiterbarkeit > Bibliothek > Aktionen**.
- 2 Klicken Sie auf **Neue Aktion**.
- 3 Geben Sie einen Namen und ein Projekt für die Erweiterbarkeitsaktion ein.
- 4 (Optional) Geben Sie eine Beschreibung für die Erweiterbarkeitsaktion ein.
- 5 Klicken Sie auf **Weiter**.
- 6 Erstellen oder importieren Sie das Skript für die Erweiterbarkeitsaktion.
- 7 Klicken Sie auf das Dropdown-Menü **FaaS-Anbieter** und wählen Sie **Lokal** aus.
- 8 Um die neue Erweiterbarkeitsaktion zu speichern, klicken Sie auf **Speichern**.

Nächste Schritte

Verwenden Sie die zuvor erstellte Erweiterbarkeitsaktion in Ihren vRealize Automation Cloud Assembly-Erweiterbarkeitsabonnements.

Erstellen von gemeinsam genutzten Erweiterbarkeitsaktionen

Als vRealize Automation Cloud Assembly-Administrator erstellen Sie Erweiterbarkeitsaktionen, die über Projekte hinweg gemeinsam genutzt werden können, ohne dass die Aktion exportiert und importiert werden muss.

Informationen zum Exportieren und Importieren von Erweiterbarkeitsaktionen finden Sie unter [Exportieren und Importieren von Erweiterbarkeitsaktionen](#).

Voraussetzungen

Erstellen Sie zwei oder mehr Projekte in Ihrer vRealize Automation Cloud Assembly-Organisation.

Verfahren

- 1 Klicken Sie auf **Erweiterbarkeit > Bibliothek > Aktionen**.
- 2 Klicken Sie auf **Neue Aktion**.
- 3 Geben Sie einen Namen für Ihre Erweiterbarkeitsaktion ein.
- 4 (Optional) Geben Sie eine Beschreibung für Ihre Erweiterbarkeitsaktion ein.
- 5 Wählen Sie ein Projekt aus, in dem Ihre Erweiterbarkeitsaktion erstellt werden soll.
- 6 Aktivieren Sie das Kontrollkästchen **Für alle Projekte in dieser Organisation freigeben**.
- 7 Klicken Sie auf **Weiter**.
- 8 Erstellen oder importieren Sie Ihr Aktionsskript und speichern Sie Ihre Erweiterbarkeitsaktion.

Hinweis Sie können die Freigabe von **Einstellungen** aktivieren oder deaktivieren. Wenn die Erweiterbarkeitsaktion in Abonnements verwendet wird, können Sie die Freigabe nicht deaktivieren. Um die Freigabe zu deaktivieren, müssen Sie die Erweiterbarkeitsaktion aus Ihren Abonnements entfernen.

- 9 Erstellen Sie ein Erweiterbarkeitsabonnement, fügen Sie die gemeinsam genutzte Erweiterbarkeitsaktion hinzu und legen Sie den Geltungsbereich für das Abonnement auf **Jedes Projekt** fest.

Hinweis Weitere Informationen zum Erstellen von Erweiterbarkeitsabonnements finden Sie unter [Erstellen eines Erweiterbarkeitsabonnements](#).

Das Erweiterbarkeitsabonnement wird durch übereinstimmende Ereignisse in einem Ihrer Projekte ausgelöst.

Nächste Schritte

Sie können eine gemeinsam genutzte Erweiterbarkeitsaktionen auch als Inhaltsquelle in den vRealize Automation Service Broker-Katalog importieren. Wenn Sie das Quellprojekt auswählen, geben Sie das Projekt ein, in dem die Erweiterbarkeitsaktion erstellt wurde. Weitere Informationen zum Hinzufügen von Erweiterbarkeitsaktionen zu vRealize Automation Service Broker finden Sie unter [Hinzufügen von Erweiterbarkeitsaktionen zum Service Broker-Katalog](#).

Exportieren und Importieren von Erweiterbarkeitsaktionen

Mit vRealize Automation Cloud Assembly können Sie Erweiterbarkeitsaktionen für die Verwendung in unterschiedlichen Projekten exportieren und importieren.

Voraussetzungen

Eine vorhandene Erweiterbarkeitsaktion.

Verfahren

- 1 Exportieren Sie eine Erweiterbarkeitsaktion.
 - a Navigieren Sie zu **Erweiterbarkeit > Bibliothek > Aktionen**.
 - b Wählen Sie eine Erweiterbarkeitsaktion aus und klicken Sie auf **Exportieren**.
Das Aktionsskript und seine Abhängigkeiten werden als ZIP-Datei in Ihrer lokalen Umgebung gespeichert.
- 2 Importieren Sie eine Erweiterbarkeitsaktion.
 - a Navigieren Sie zu **Erweiterbarkeit > Bibliothek > Aktionen**.
 - b Klicken Sie auf **Importieren**.
 - c Wählen Sie die exportierte Erweiterbarkeitsaktion aus und weisen Sie sie einem Projekt zu.
 - d Klicken Sie auf **Importieren**.

Hinweis Wenn die importierte Erweiterbarkeitsaktion dem angegebenen Projekt bereits zugewiesen ist, werden Sie aufgefordert, eine Konfliktlösungsrichtlinie auszuwählen.

Alternative Sie können auch Aktionsskripte importieren, indem Sie die Option **Paket importieren** direkt im Aktions-Editor auswählen.

Definition eines Aktionsablaufs

Bei Aktionsabläufen handelt es sich um eine Gruppe von Erweiterbarkeitsaktionsskripten, mit deren Hilfe Lebenszyklen und Automatisierung weiter verlängert werden können.

Alle Aktionsabläufe beginnen mit `flow_start` und enden mit `flow_end`. Mithilfe der folgenden Aktionsablaufelemente können Sie mehrere Erweiterbarkeitsaktionsskripte miteinander verknüpfen:

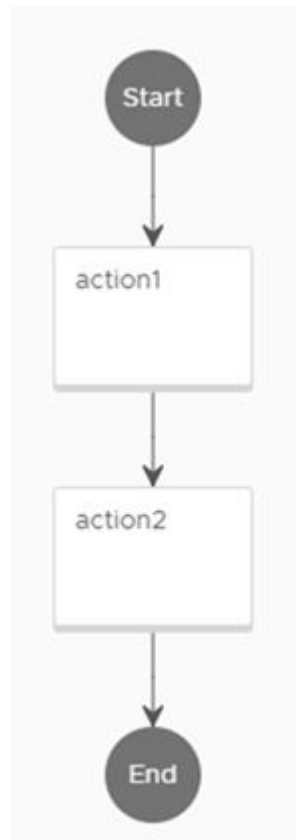
- **Sequenzielle Aktionsabläufe** – Mehrere Erweiterbarkeitsaktionsskripte werden nacheinander ausgeführt.
- **Fork-Aktionsabläufe** – Mehrere Erweiterbarkeitsaktionsskripte oder -abläufe, die über aufgeteilte Pfade zur gleichen Ausgabe beitragen.
- **Join-Aktionsabläufe** – Mehrere Erweiterbarkeitsaktionsskripte oder -abläufe, die miteinander verbunden werden und zur gleichen Ausgabe beitragen.
- **Bedingte Aktionsabläufe** – Mehrere Erweiterbarkeitsaktionsskripte oder -abläufe, die ausgeführt werden, nachdem eine Bedingung erfüllt worden ist.

Sequenzielle Aktionsabläufe

Mehrere Erweiterbarkeitsaktionsskripts, die nacheinander ausgeführt werden.

```
version: "1"
flow:
  flow_start:
    next: action1
  action1:
    action: <action_name>
    next: action2
  action2:
    action: <action_name>
    next: flow_end
```

Hinweis Sie können zu einer vorherigen Aktion zurückkehren, indem Sie sie als `next:`-Aktion zuweisen. In diesem Beispiel können Sie beispielsweise anstelle von `next: flow_end` `next: action1` eingeben, um Aktion1 erneut auszuführen und die Abfolge der Aktionen neu zu starten.



Fork-Aktionsabläufe

Mehrere Erweiterbarkeitsaktionsskripts oder -abläufe, die Pfade aufteilen, um zur gleichen Ausgabe beizutragen.

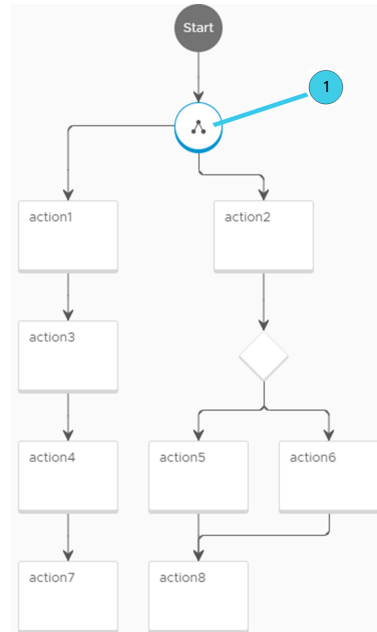
```

version: "1"
flow:
  flow_start:
    next: forkAction
  forkAction:
    fork:
      next: [action1, action2]
  action1:
    action: <action_name>
    next: action3
  action3:
    action: <action_name>
    next: action4
  action4:
    action: <action_name>
    next: action7
  action7:
    action: <action_name>
  action2:
    action: <action_name>

```

Hinweis Sie können zu einer vorherigen Aktion zurückkehren, indem Sie sie als `next:`-Aktion zuweisen.

Beispiel: Statt `next: flow_end` zum Beenden des Aktionsablaufs zu verwenden, können Sie `next: action1` eingeben, um Aktion1 erneut auszuführen und die Abfolge der Aktionen neu zu starten.



1 Fork-Element

Join-Aktionsabläufe

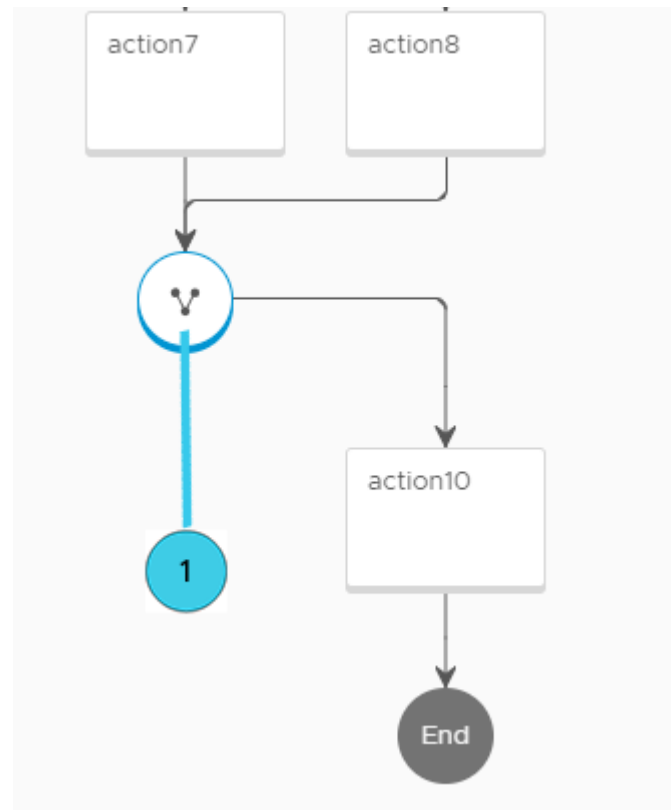
Mehrere Erweiterbarkeitsaktionsskripts oder -abläufe, die mehrere Pfade bündeln und zur gleichen Ausgabe beitragen.

```

version: "1"
action7:
  action: <action_name>
  next: joinElement
action8:
  action: <action_name>
  next: joinElement
joinElement:
  join:
    type: all
    next: action10
action10:
  action: <action_name>
  next: flow_end

```

Hinweis Sie können zu einer vorherigen Aktion zurückkehren, indem Sie sie als `next:`-Aktion zuweisen. In diesem Beispiel können Sie beispielsweise anstelle von `next: flow_end` `next: action1` eingeben, um Aktion1 erneut auszuführen und die Abfolge der Aktionen neu zu starten.



1 Join-Element

Bedingte Aktionsabläufe

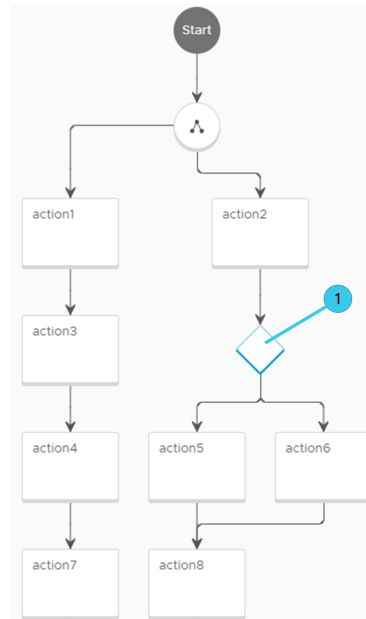
Mehrere Erweiterbarkeitsaktionsskripts oder -abläufe, die ausgeführt werden, wenn eine Bedingung mithilfe eines Switch-Elements erfüllt ist.

In bestimmten Fällen muss die Bedingung gleich `true` sein, damit die Aktion ausgeführt werden kann. In anderen Fällen (wie in diesem Beispiel) werden Parameterwerte benötigt, die erfüllt sein müssen, bevor eine Aktion ausgeführt werden kann. Wenn keine der Bedingungen erfüllt ist, schlägt der Aktionsablauf fehl.


```

version: 1
id: 1234
name: Test
inputs: ...
outputs: ...
flow:
  flow_start:
    next: forkAction
  forkAction:
    fork:
      next: [action1, action2]
  action1:
    action: <action_name>
    next: action3
  action3:
    action: <action_name>
    next: action4
  action4:
    action: <action_name>
    next: action7
  action7:
    action: <action_name>
    next: joinElement
  action2:
    action: <action_name>
    next: switchAction
  switchAction:
    switch:
      "${1 == 1}": action5
      "${1 != 1}": action6
  action5:
    action: <action_name>
    next: action8
  action6:
    action: <action_name>
    next: action8
  action8:
    action: <action_name>

```



1 Switch-Element

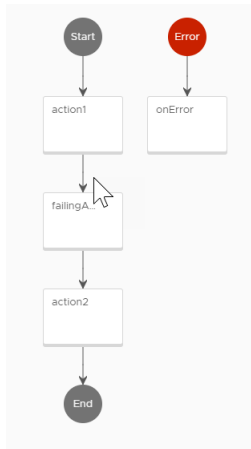
Hinweis Sie können zu einer vorherigen Aktion zurückkehren, indem Sie sie als `next:-Aktion` zuweisen.
 Beispiel: Statt `next: flow_end` zum Beenden des Aktionsablaufs zu verwenden, können Sie `next: action1` eingeben, um Aktion1 erneut auszuführen und die Abfolge der Aktionen neu zu starten.

Vorgehensweise zum Verwenden eines Fehlerhandlers in Aktionsabläufen

Indem Sie ein Fehlerbehandlungselement verwenden, können Sie Ihren Aktionsablauf so konfigurieren, dass er in bestimmten Phasen des Ablaufs einen Fehler anzeigt.

Ein Fehlerbehandlungselement erfordert zwei Eingaben:

- Angegebene Fehlermeldung der fehlgeschlagenen Aktion.
- Eingaben des Aktionsablaufs.



Wenn eine Aktion in Ihrem Ablauf fehlschlägt und der Aktionsablauf ein Fehlerbehandlungselement enthält, wird eine Fehlermeldung ausgegeben, die Sie über den Aktionsablauf informiert. Der Fehlerhandler ist eine eigene Aktion. Das folgende Skript ist ein Beispiel für einen Fehlerhandler, der in einem Aktionsablauf verwendet werden kann.

```
def handler(context, inputs):

    errorMsg = inputs["errorMsg"]
    flowInputs = inputs["flowInputs"]

    print("Flow execution failed with error {0}".format(errorMsg))
    print("Flow inputs were: {0}".format(flowInputs))

    outputs = {
        "errorMsg": errorMsg,
        "flowInputs": flowInputs
    }

    return outputs
```

Sie können die erfolgreichen und fehlgeschlagenen Ausführungen im Fenster „Aktionsausführungen“ anzeigen.

The screenshot shows the vRealize Automation Cloud Assembly interface. The top navigation bar includes 'vm Cloud Assembly', a user profile 'Paul Martini', and a 'GEFÜHRTES SETUP' button. The main navigation menu on the left includes 'Ereignisse', 'Abonnements', 'Bibliothek', and 'Aktivität'. The 'Aktivität' section is expanded, showing 'Aktionsausführungen' and 'Workflow-Ausführungen'. The 'Aktionsausführungen' window is open, displaying a table of execution results for AWS-ABX actions.

Status	Aktion	Aktions-ID
Abgeschlossen	AWS-ABX	8a769ecc6df809c7016e01a83fe204e6
Fehlgeschlagen	AWS-ABX	8a769ecc6df809c7016e01a83fe204e6
Abgeschlossen	AWS-ABX	8a769ecc6df809c7016e01a83fe204e6
Abgeschlossen	AWS-ABX	8a769ecc6df809c7016e01a83fe204e6

In diesem Beispiel wurde der Ablauf „flow-with-handler“, der das Fehlerbehandlungselement enthält, erfolgreich ausgeführt. Eine der Aktionen im Ablauf ist jedoch fehlgeschlagen, was den Fehlerhandler dazu veranlasst hat, einen Fehler zu melden.

Vorgehensweise zum Verfolgen von Aktionsausführungen

Auf der Registerkarte „Aktionsausführungen“ wird ein Protokoll mit den von Abonnements ausgelösten Erweiterbarkeitsaktionen und deren Status angezeigt.

Sie können das Protokoll der Aktionsausführungen mithilfe von **Erweiterbarkeit > Aktivität > Aktionsausführungen** anzeigen. Darüber hinaus können Sie die Liste der Aktionsausführungen gleichzeitig nach einer oder mehreren Eigenschaften filtern. Zur Anzeige weiterer Details zu einer einzelnen Aktionsausführung klicken Sie auf die Ausführungs-ID.

Fehlerbehebung bei fehlgeschlagenen Ausführungen von Erweiterbarkeitsaktionen

Wenn die Ausführung der Erweiterbarkeitsaktion fehlschlägt, können Sie zu Korrekturzwecken Fehlerbehebungsschritte durchführen.

Wenn eine Aktionsausführung fehlschlägt, erhalten Sie möglicherweise eine Fehlermeldung, einen Fehlerstatus und ein Fehlerprotokoll. Wenn Ihre Aktionsausführung fehlschlägt, ist dies entweder auf einen Bereitstellungs- oder einen Codefehler zurückzuführen.

Problem	Lösung
Bereitstellungsfehler	Diese Fehler ergeben sich aus Problemen im Zusammenhang mit der Konfiguration des Cloud-Kontos, der Aktionsbereitstellung oder anderen Abhängigkeiten, die die Bereitstellung der Aktion verhindern können. Stellen Sie sicher, dass das von Ihnen verwendete Projekt innerhalb des konfigurierten Cloud-Kontos definiert ist und Berechtigungen zum Ausführen von Funktionen erteilt wurde. Bevor Sie die Aktion erneut initiieren, können Sie die Aktion anhand eines bestimmten Projekts auf der Seite „Details“ der Aktion testen.
Codefehler	Diese Fehler sind auf ungültige Skripts oder ungültigen Code zurückzuführen. Verwenden Sie die Aktionsprotokolle zur Fehlerbehebung und Korrektur der ungültigen Skripts.

Abonnements für Erweiterbarkeits-Workflows

Sie können Ihre von vRealize Orchestrator gehosteten Workflows mit vRealize Automation Cloud Assembly verwenden, um den Lebenszyklus Ihrer Anwendung zu verlängern.

Vorgehensweise zum Ändern der Eigenschaften virtueller Maschinen mithilfe eines vRealize Orchestrator-Workflow-Abonnements

Sie können einen vorhandenen vRealize Orchestrator-Workflow verwenden, um Eigenschaften virtueller Maschinen zu ändern und virtuelle Maschinen zu Active Directory hinzuzufügen.

Mit den Parametern des Ereignisthemas wird das Format der Nutzlast für EBS-Nachrichten (Event Broker Service, Ereignisbrokerdienst) definiert. Um die EBS-Nachrichtennutzlast innerhalb eines Workflows zu empfangen und zu verwenden, müssen Sie die Eingabeparameter des `inputProperties`-Workflows definieren.

Voraussetzungen

- Cloud-Administratorbenutzerrolle
- Vorhandene lokale vRealize Orchestrator-Workflows.
- Erfolgreiche Integration und Verbindung zum vRealize Orchestrator-Clientserver.

Verfahren

- 1 Klicken Sie auf **Erweiterbarkeit > Abonnements**.
- 2 Klicken Sie auf **Neues Abonnement**.
- 3 Erstellen Sie ein Abonnement mit den folgenden Parametern:

Parameter	Wert
Name	RenameVM
Ereignisthema	Wählen Sie ein Ereignisthema aus, das für die gewünschte vRealize Orchestrator-Integration geeignet ist. Beispiel: Computing-Zuteilung.
Blockierend/Nicht blockierend	Nicht blockierend
Aktion/Workflow	Wählen Sie einen ausführbaren vRealize Orchestrator-Typ aus. Wählen Sie den gewünschten Workflow aus. Beispiel: VM-Namen festlegen.

- 4 Klicken Sie auf **Speichern**, um Ihr Abonnement zu speichern.
- 5 Weisen Sie Ihr Abonnement zu und aktivieren Sie es, indem Sie eine Cloud-Vorlage erstellen oder eine vorhandene Cloud-Vorlage bereitstellen.

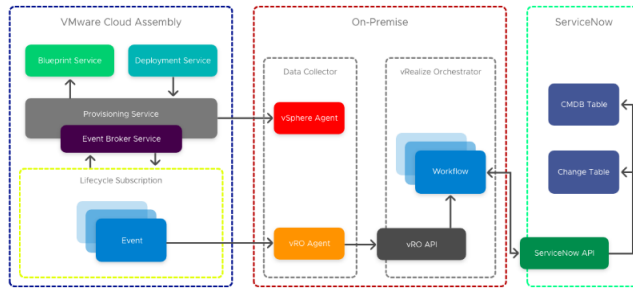
Nächste Schritte

Stellen Sie mithilfe einer der folgenden Methoden sicher, dass der Workflow erfolgreich initiiert wurde:

- Vergewissern Sie sich, dass der Workflow das Protokoll ausführt. Klicken Sie dazu auf **Erweiterbarkeit > Aktivität > Workflow-Ausführungen**.
- Öffnen Sie den vRealize Orchestrator-Client und überprüfen Sie den Workflow-Status, indem Sie zum Workflow navigieren und den Status überprüfen oder indem Sie die Registerkarte der entsprechenden Protokolle öffnen.

Vorgehensweise zum Integrieren von Cloud Assembly für ITSM mit ServiceNow unter Verwendung von vRealize Orchestrator-Workflows

Mithilfe von gehosteten vRealize Orchestrator-Workflows können Sie vRealize Automation Cloud Assembly mit ServiceNow für ITSM-Übereinstimmung integrieren.



Unternehmensbenutzer integrieren ihre Cloud Management Plattform zu Übereinstimmungszwecken in der Regel mit einer ITSM- (IT Service Management) und einer CMDB-Plattform (Configuration Management Database). Im Anschluss an dieses Beispiel können Sie vRealize Automation Cloud Assembly mit ServiceNow für CMDB und ITSM unter Verwendung von gehosteten vRealize Orchestrator-Workflows integrieren. Bei Verwendung von vRealize Orchestrator-Integrationen und -Workflows sind Funktions-Tags besonders nützlich, wenn Sie über mehrere Instanzen für verschiedene Umgebungen verfügen. Weitere Informationen zu Funktions-Tags finden Sie unter [Verwenden von Funktions-Tags in vRealize Automation Cloud Assembly](#).

Hinweis Sie können ServiceNow unter Verwendung von Erweiterbarkeitsaktionsskripts auch mit vRealize Automation Cloud Assembly integrieren. Informationen zum Integrieren von ServiceNow mithilfe von Erweiterbarkeitsaktionsskripts finden Sie unter [Vorgehensweise zum Integrieren von Cloud Assembly in ServiceNow unter Verwendung von Erweiterbarkeitsaktionen](#).

In diesem Beispiel besteht die ServiceNow-Integration aus drei Workflows auf oberster Ebene. Jeder Workflow verfügt über eigene Abonnements, sodass Sie jede Komponente einzeln aktualisieren und durchlaufen lassen können.

- Einstiegspunkt des Ereignisabonnements – Einfache Protokollierung, gibt gegebenenfalls den anfordernden Benutzer und die vCenter-VM an.
- Integrations-Workflow – trennt Objekte und speist Eingaben in den technischen Workflow ein, verarbeitet Protokollierungs-, Eigenschaften- und Ausgabeaktualisierungen.
- Technischer Workflow – nachgelagerte Systemintegration für die ServiceNow-API zum Erstellen der CMDB-CI-, CR- und vRealize Automation Cloud Assembly-IaaS-API mit zusätzlichen VM-Eigenschaften außerhalb der Nutzlast.

Voraussetzungen

- Eine eigenständige oder geclusterte vRealize Orchestrator-Umgebung.
- Eine vRealize Orchestrator-Integration in vRealize Automation Cloud Assembly. Informationen zur Integration einer eigenständigen vRealize Orchestrator-Instanz mit vRealize Automation Cloud Assembly finden Sie unter [Konfigurieren der vRealize Orchestrator-Integration in Cloud Assembly](#).

Verfahren

- 1 Erstellen und speichern Sie in vRealize Orchestrator eine Konfigurationsdatei, die eine allgemeine, in mehreren Workflows verwendete Konfiguration enthält.
- 2 Speichern Sie Ihr vRealize Automation Cloud Assembly-API-Token am selben Speicherort wie die Konfigurationsdatei aus Schritt 1.

Hinweis Das vRealize Automation Cloud Assembly-API-Token weist ein Ablaufdatum auf.

- 3 Erstellen Sie mit dem bereitgestellten Skriptelement einen Workflow in vRealize Orchestrator. Dieses Skript verweist auf einen REST-Host und sucht nach diesem. Es standardisiert auch REST-Aktionen, die einen optionalen Parameter eines Tokens verwenden, der als zusätzlicher Autorisierungs-Header hinzugefügt wird.

```
var configPath = "CS"
var configName = "environmentConfig"
var attributeName = "CASRestHost"

//get REST Host from configuration element
var restHost =
System.getModule("au.com.cs.example").getRestHostFromConfig(configPath,configName,attribute
Name)

var ConfigurationElement =
System.getModule("au.com.cs.example").getConfigurationElementByName(configName,configPath);
System.debug("ConfigurationElement:" + ConfigurationElement);
var casToken = ConfigurationElement.getAttributeWithKey("CASToken")["value"]
if(!casToken){
    throw "no CAS Token";
}
//REST Template
var opName = "casLogin";
var opTemplate = "/iaas/login";
var opMethod = "POST";

// create the REST operation:
var opLogin =
System.getModule("au.com.cs.example").createOp(restHost,opName,opMethod,opTemplate);

//cas API Token
var contentObject = {"refreshToken":casToken}
postContent = JSON.stringify(contentObject);

var loginResponse =
System.getModule("au.com.cs.example").executeOp(opLogin,null,postContent,null) ;

try{
    var tokenResponse = JSON.parse(loginResponse)['token']
    System.debug("token: " + tokenResponse);
} catch (ex) {
    throw ex + " No valid token";
}
```

```

//REST Template Machine Details
var opName = "machineDetails";
var opTemplate = "/iaas/machines/" + resourceId;
var opMethod = "GET";

var bearer = "Bearer " + tokenResponse;

var opMachine =
System.getModule("au.com.cs.example").createOp(restHost,opName,opMethod,opTemplate);

// (Rest Operation, Params, Content, Auth Token)
var vmResponse =
System.getModule("au.com.cs.example").executeOp(opMachine,null,"",bearer) ;

try{
    var vm = JSON.parse(vmResponse);
} catch (ex) {
    throw ex + " failed to parse vm details"
}

System.log("cpuCount: " + vm["customProperties"]["cpuCount"]);
System.log("memoryInMB: " + vm["customProperties"]["memoryInMB"]);

cpuCount = vm["customProperties"]["cpuCount"];
memoryMB = vm["customProperties"]["memoryInMB"];

```

Dieses Skript sendet die Ausgabe `cpuCount` und `memoryMB` an den übergeordneten Workflow und aktualisiert die vorhandenen `customProperties`-Eigenschaften. Diese Werte können bei der Erstellung der CMDB in nachfolgenden Workflows verwendet werden.

- 4 Fügen Sie das ServiceNow-CMDB-Skriptelement zum Erstellen des Konfigurationselements zu Ihrem Workflow hinzu. Dieses Element sucht mithilfe des Konfigurationselements nach dem ServiceNow-REST-Host, erstellt einen REST-Vorgang für die `cmdb_ci_vmware_instance`-Tabelle sowie basierend auf Workflow-Eingaben für Post-Daten eine Zeichenfolge aus Inhaltsobjekten und gibt die zurückgegebene `sys_id` aus.

```

var configPath = "CS"
var configName = "environmentConfig"
var attributeName = "serviceNowRestHost"
var tableName = "cmdb_ci_vmware_instance"

//get REST Host from configuration element
var restHost =
System.getModule("au.com.cs.example").getRestHostFromConfig(configPath,configName,attributeName)

//REST Template
var opName = "serviceNowCreatCI";
var opTemplate = "/api/now/table/" + tableName;
var opMethod = "POST";

// create the REST operation:

```

```

var opCI =
System.getModule("au.com.cs.example").createOp(restHost,opName,opMethod,opTemplate);

//cmdb_ci_vm_vmware table content to post;
var contentObject = {};
contentObject["name"] = hostname;
contentObject["cpus"] = cpuTotalCount;
contentObject["memory"] = MemoryInMB;
contentObject["correlation_id"]= deploymentId
contentObject["disks_size"]= diskProvisionGB
contentObject["location"] = "Sydney";
contentObject["vcenter_uuid"] = vcUuid;
contentObject["state"] = "On";
contentObject["owned_by"] = owner;

postContent = JSON.stringify(contentObject);
System.log("JSON: " + postContent);

// (Rest Operation, Params, Content, Auth Token)
var ciResponse =
System.getModule("au.com.cs.example").executeOp(opCI,null,postContent,null) ;

try{
    var cmdbCI = JSON.parse(ciResponse);
} catch (ex) {
    throw ex + " failed to parse ServiceNow CMDB response";
}

serviceNowSysId = cmdbCI['result']['sys_id'];

```

- 5 Erstellen Sie mithilfe der Ausgabe aus dem untergeordneten Workflow unter Verwendung der vorhandenen `customProperties` ein `Eigenschaftenobjekt` und überschreiben Sie die Eigenschaft `serviceNowSysId` mit dem Wert aus ServiceNow. Diese eindeutige ID wird in der CMDB verwendet, um eine Instanz beim Löschen als veraltet zu kennzeichnen.

Ergebnisse

vRealize Automation Cloud Assembly wurde erfolgreich mit ITSM-Lösung ServiceNow integriert. Weitere Informationen zur Verwendung von Workflows für die Integration von ServiceNow in vRealize Automation Cloud Assembly finden Sie im Blogbeitrag [Extending Cloud Assembly with vRealize Orchestrator for ServiceNow Integration](#), der die Erweiterung von Cloud Assembly mit vRealize Orchestrator für die ServiceNow-Integration behandelt.

Weitere Informationen zu Workflow-Abonnements

Wenn Sie die vRealize Orchestrator-Integration in vRealize Automation Cloud Assembly verwenden, können Sie die Lebenszyklen von Anwendungen mit Workflows verlängern.

vRealize Automation enthält eine eingebettete vRealize Orchestrator-Bereitstellung. Sie können die Workflow-Bibliothek der eingebetteten vRealize Orchestrator-Bereitstellung in Ihren Abonnements verwenden. Sie können Workflows nur mithilfe des vRealize Orchestrator-Clients erstellen, ändern und löschen.

Sie können auch eine externe vRealize Orchestrator-Bereitstellung in vRealize Automation Cloud Assembly integrieren. Weitere Informationen finden Sie unter *Vorgehensweise zum Integrieren eines externen vRealize Orchestrator Client in Verwenden des eingebetteten vRealize Orchestrator Client*.

Empfehlungen zum Erstellen von vRealize Orchestrator-Workflows

Ein Workflow-Abonnement basiert auf einem bestimmten Ereignisthema und den Ereignisparametern dieses Themas. Die Abonnements müssen mit den korrekten Eingabeparametern konfiguriert werden, damit sie die vRealize Orchestrator-Workflows initiieren und mit den Ereignisdaten verwendet werden können.

Workflow-Eingabeparameter

Der benutzerdefinierte Workflow kann alle Parameter oder einen einzelnen Parameter enthalten, der alle Daten in der Nutzlast verbraucht.

Zur Verwendung eines einzelnen Parameters konfigurieren Sie einen Parameter mit dem Typ `Properties` und dem Namen `inputProperties`.

Workflow-Ausgabeparameter

Der benutzerdefinierte Workflow kann Ausgabeparameter mit Relevanz für nachfolgende Ereignisse enthalten, die für ein Antwortereignisthema erforderlich sind.

Wenn ein Ereignisthema eine Antwort erwartet, müssen die Workflow-Ausgabeparameter mit den Parametern des Antwortschemas übereinstimmen.

Vorgehensweise zum Verfolgen von Workflow-Ausführungen

Im Fenster **Workflow-Ausführungen** werden die Protokolle der vom Abonnement ausgelösten Workflows sowie deren Status angezeigt.

Sie können die Protokolle der Workflow-Ausführungen anzeigen, indem Sie zu **Erweiterbarkeit > Aktivität > Workflow-Ausführungen** navigieren.

Fehlerbehebung bei fehlgeschlagenen Workflow-Abonnements

Wenn Ihr Workflow-Abonnement fehlschlägt, können Sie Fehlerbehebungsschritte durchführen, um es zu korrigieren.

Fehlgeschlagene Workflow-Ausführungen können dazu führen, dass Ihr Workflow-Abonnement nicht erfolgreich gestartet oder abgeschlossen wird. Fehler bei der Workflow-Ausführung können das Ergebnis mehrerer allgemeiner Probleme sein.

Problem	Ursache	Lösung
Ihr vRealize Orchestrator-Workflow-Abonnement wurde nicht erfolgreich gestartet oder abgeschlossen.	Sie haben ein Workflow-Abonnement konfiguriert, um beim Eingang der Ereignismeldung einen benutzerdefinierten Workflow auszuführen, aber der Workflow wird nicht erfolgreich gestartet oder abgeschlossen.	<ol style="list-style-type: none"> 1 Stellen Sie sicher, dass das Workflow-Abonnement ordnungsgemäß gespeichert wurde. 2 Stellen Sie sicher, dass die Bedingungen des Workflow-Abonnements ordnungsgemäß konfiguriert sind. 3 Stellen Sie sicher, dass vRealize Orchestrator den angegebenen Workflow enthält. 4 Stellen Sie sicher, dass der Workflow in vRealize Orchestrator ordnungsgemäß konfiguriert ist.
Die Genehmigungsanforderung für Ihr vRealize Orchestrator-Workflow-Abonnement wurde nicht ausgeführt.	Sie haben ein Workflow-Abonnement vom Typ „Vor Genehmigung“ oder „Nach Genehmigung“ konfiguriert, um einen vRealize Orchestrator-Workflow auszuführen. Der Workflow wird nicht ausgeführt, wenn eine Maschine, die den definierten Kriterien entspricht, im Service Catalog angefordert wird.	<p>Zur erfolgreichen Ausführung einer Genehmigung für ein Workflow-Abonnement müssen Sie sicherstellen, dass alle Komponenten ordnungsgemäß konfiguriert sind.</p> <ol style="list-style-type: none"> 1 Stellen Sie sicher, dass die Genehmigungsrichtlinie aktiv ist und ordnungsgemäß angewendet wurde. 2 Stellen Sie sicher, dass Ihr Workflow-Abonnement ordnungsgemäß konfiguriert und gespeichert wurde. 3 Überprüfen Sie die Ereignisprotokolle auf Meldungen im Zusammenhang mit Genehmigungen.
Die Genehmigungsanforderung für Ihr vRealize Orchestrator-Workflow-Abonnement wurde abgelehnt.	<p>Sie haben ein Workflow-Abonnement vom Typ „Vor Genehmigung“ oder „Nach Genehmigung“ konfiguriert, das einen angegebenen vRealize Orchestrator-Workflow ausführt. Die Anforderung wird jedoch auf der externen Genehmigungsebene abgelehnt.</p> <p>Eine mögliche Ursache ist ein interner Fehler bei der Workflow-Ausführung in vRealize Orchestrator. Beispielsweise fehlt der Workflow oder der vRealize Orchestrator-Server wird nicht ausgeführt.</p>	<ol style="list-style-type: none"> 1 Überprüfen Sie die Protokolle auf Meldungen im Zusammenhang mit Genehmigungen. 2 Stellen Sie sicher, dass der vRealize Orchestrator-Server ausgeführt wird. 3 Stellen Sie sicher, dass vRealize Orchestrator den angegebenen Workflow enthält.

Weitere Informationen zu Erweiterbarkeitsabonnements

Sie können die Lebenszyklen Ihrer Anwendungen verlängern, indem Sie Erweiterbarkeitsaktionen oder gehostete vRealize Orchestrator-Workflows mit Erweiterbarkeitsabonnements verwenden.

Wenn ein auslösendes Ereignis in Ihrer Umgebung auftritt, wird das Abonnement initiiert und der angegebene Workflow oder die angegebene Erweiterbarkeitsaktion wird ausgeführt. Sie können Systemereignisse im Ereignisprotokoll, Workflow-Ausführungen im Fenster „Workflow-Ausführungen“ und Aktionsausführungen im Fenster „Aktion ausführen“ anzeigen. Abonnements sind projektspezifisch, d. h., sie sind über das angegebene Projekt mit Cloud-Vorlagen und Bereitstellungen verknüpft.

Terminologie der Erweiterbarkeit

Beim Arbeiten mit Erweiterbarkeitsabonnements in vRealize Automation Cloud Assembly stoßen Sie möglicherweise auf spezielle Terminologie für die Abonnements und den Ereignisbrokerdienst.

Tabelle 6-3. Terminologie der Erweiterbarkeit

Begriff	Beschreibung
Ereignisthema	Beschreibt mehrere Ereignisse mit derselben logischen Absicht und derselben Struktur. Jedes Ereignis stellt eine Instanz eines Ereignisthemas dar. Sie können bestimmten Ereignisthemen blockierende Parameter zuweisen. Weitere Informationen finden Sie unter Blockieren von Ereignisthemen .
Ereignis	Bezeichnet eine Statusänderung beim Producer oder den Elementen, die vom Producer verwaltet werden. Beim Ereignis handelt es sich um das Element, das Informationen zum Auftreten des Ereignisses aufzeichnet.
Ereignisbrokerdienst	Mit diesem Dienst werden Nachrichten gesendet, die von einem Producer für die abonnierten Verbraucher veröffentlicht werden.
Nutzlast	Die Ereignisdaten, die alle relevanten Eigenschaften im Zusammenhang mit dem entsprechenden Ereignisthema enthalten.
Abonnement	Gibt an, dass ein Abonnent über ein Ereignis informiert werden möchte, indem ein Ereignisthema abonniert und die Kriterien definiert werden, die die Benachrichtigung auslösen. Abonnements verknüpfen Erweiterbarkeitsaktionen oder Workflows mit auslösenden Ereignissen, mit denen Teile des Anwendungslebenszyklus automatisiert werden.
Abonnent	Die Benutzer, die über die Ereignisse informiert werden, die basierend auf der Abonnementdefinition für den Ereignisbrokerdienst veröffentlicht werden. Der Abonnent kann auch als Verbraucher bezeichnet werden.

Tabelle 6-3. Terminologie der Erweiterbarkeit (Fortsetzung)

Begriff	Beschreibung
Systemadministrator	Ein Benutzer mit Berechtigungen zum Erstellen, Lesen, Aktualisieren und Löschen der Mandanten- und System-Workflow-Abonnements mithilfe von vRealize Automation Cloud Assembly.
Workflow-Abonnement	Legt das Ereignisthema und die Bedingungen fest, die einen vRealize Orchestrator-Workflow auslösen.
Aktionsabonnement	Gibt das Ereignisthema und die Bedingungen an, die die Ausführung einer Erweiterbarkeitsaktion auslösen.
Workflow	Ein vRealize Orchestrator-Workflow, der in vRealize Automation Cloud Assembly integriert ist. Sie können diese Workflows mit Ereignissen in Abonnements verknüpfen.
Erweiterbarkeitsaktion	Ein optimiertes Codeskript, das nach dem Auslösen eines Ereignisses in einem Abonnement ausgeführt werden kann. Erweiterbarkeitsaktionen ähneln Workflows, sind aber einfacher. Erweiterbarkeitsaktionen können innerhalb von vRealize Automation Cloud Assembly angepasst werden.
Aktionsausführungen	Zugreifbar über die Registerkarte Aktionsausführungen . Bei einer Aktionsausführung handelt es sich um ein detailliertes Protokoll der Erweiterbarkeitsaktionen, die als Reaktion auf auslösende Ereignisse ausgeführt wurden.

Blockieren von Ereignisthemen

Bestimmte Ereignisthemen unterstützen die Blockierung von Ereignissen. Das Verhalten eines Erweiterbarkeitsabonnements hängt davon ab, ob diese Ereignistypen vom Thema unterstützt werden und wie das Abonnement konfiguriert ist.

vRealize Automation Cloud Assembly-Erweiterbarkeitsabonnements können zwei grundlegende Typen von Ereignisthemen verwenden: nicht blockierende und blockierende Ereignisthemen. Der Typ des Ereignisthemas definiert das Verhalten des Erweiterbarkeitsabonnements.

Nicht blockierende Ereignisthemen

Mit nicht blockierenden Ereignisthemen können nur nicht blockierende Abonnements erstellt werden. Nicht blockierende Abonnements werden asynchron ausgelöst, und Sie können sich nicht auf die Reihenfolge verlassen, in der die Abonnements ausgelöst werden.

Blockieren von Ereignisthemen

Bestimmte Ereignisthemen unterstützen die Blockierung. Wenn ein Abonnement als „Blockierend“ gekennzeichnet ist, werden alle Nachrichten, die die festgelegten Bedingungen erfüllen, von keinem anderen Abonnement mit übereinstimmenden Bedingungen empfangen, bis das ausführbare Element des blockierenden Abonnements ausgeführt wird.

Blockierende Abonnements werden in der Reihenfolge der Priorität ausgeführt. Der höchste Prioritätswert ist 0 (null). Wenn Sie über mehr als ein blockierendes Abonnement für das gleiche Ereignisthema mit der gleichen Prioritätsstufe verfügen, werden die Abonnements in umgekehrter alphabetischer Reihenfolge basierend auf dem Namen des Abonnements ausgeführt. Nachdem alle blockierenden Abonnements verarbeitet wurden, wird die Nachricht gleichzeitig an alle nicht blockierenden Abonnements gesendet. Da die blockierenden Abonnements synchron ausgeführt werden, umfasst die geänderte Ereignisnutzlast das aktualisierte Ereignis, wenn die nachfolgenden Abonnements benachrichtigt werden.

Sie können blockierende Ereignisthemen verwenden, um mehrere Abonnements zu verwalten, die voneinander abhängig sind.

Sie verfügen beispielsweise über zwei Bereitstellungs-Workflow-Abonnements, bei denen das zweite Abonnement von den Ergebnissen des ersten abhängt. Beim ersten Abonnement wird während der Bereitstellung eine Eigenschaft geändert und das zweite zeichnet die neue Eigenschaft, z. B. einen Maschinennamen, in einem Dateisystem auf. Das Abonnement „ChangeProperty“ hat die Priorität 0 und „RecordProperty“ hat die Priorität 1, da das zweite Abonnement die Ergebnisse des ersten Abonnements verwendet. Bei der Bereitstellung einer Maschine wird die Ausführung des Abonnements „ChangeProperty“ gestartet. Da die Bedingungen des Abonnements „RecordProperty“ auf einer Bedingung nach der Bereitstellung basieren, löst ein Ereignis das Abonnement „RecordProperty“ aus. Da der Workflow „ChangeProperty“ aber ein blockierender Workflow ist, wird das Ereignis erst dann empfangen, wenn der Workflow abgeschlossen ist. Nachdem der Maschinenname geändert und das erste Workflow-Abonnement abgeschlossen wurde, wird das zweite Workflow-Abonnement ausgeführt und der Maschinenname im Dateisystem aufgezeichnet.

Ausführbares Wiederherstellungselement

Zum Blockieren von Ereignisthemen können Sie dem Abonnement ein ausführbares Wiederherstellungselement hinzufügen. Das ausführbare Wiederherstellungselement in einem Abonnement wird ausgeführt, wenn das primäre ausführbare Element ausfällt. Sie können beispielsweise ein Workflow-Abonnement erstellen, bei dem das primäre ausführbare Element ein Workflow ist, der Datensätze in einem CMDB-System, wie z. B. ServiceNow, erstellt. Selbst wenn das Workflow-Abonnement fehlschlägt, werden möglicherweise einige Datensätze im CMDB-System erstellt. In diesem Szenario kann ein ausführbares Wiederherstellungselement verwendet werden, um die vom fehlgeschlagenen ausführbaren Element im CMDB-System hinterlassenen Datensätze zu bereinigen.

Für Anwendungsfälle, die mehrere Abonnements enthalten, die voneinander abhängig sind, können Sie dem ausführbaren Wiederherstellungselement eine `ebs.recover.continuation`-Eigenschaft hinzufügen. Mit dieser Eigenschaft können Sie steuern, ob der Erweiterbarkeitsdienst mit dem nächsten Abonnement in Ihrer Kette fortgesetzt werden muss, falls das aktuelle Abonnement fehlschlägt.

Mit vRealize Automation Cloud Assembly bereitgestellte Ereignisthemen

vRealize Automation Cloud Assembly enthält vordefinierte Ereignisthemen.

Ereignisthemen

Ereignisthemen sind die Kategorien, in denen ähnliche Ereignisse zusammengefasst werden. Einem Abonnement zugewiesene Ereignisthemen definieren das Ereignis, das das Abonnement auslöst. Die folgenden Ereignisthemen werden standardmäßig mit vRealize Automation Cloud Assembly bereitgestellt. Alle Themen können zum Hinzufügen oder Aktualisieren benutzerdefinierter Eigenschaften oder Tags der Ressource verwendet werden. Wenn ein vRealize Orchestrator-Workflow oder eine Erweiterbarkeitsaktion fehlschlägt, schlägt die entsprechende Aufgabe ebenfalls fehl.

Tabelle 6-4. Cloud Assembly-Ereignisthemen

Ereignisthema	Blockierbar	Beschreibung
Cloud template configuration	Nein	Wird ausgegeben, wenn ein Cloud-Vorlagen-Konfigurationsereignis wie das Erstellen oder Löschen einer Cloud-Vorlage eintritt. Dieses Ereignisthema kann für die Benachrichtigung von externe Systemen über diese Ereignisse nützlich sein.
Cloud template version configuration	Nein	Wird ausgegeben, wenn ein neues Cloud-Vorlagen-Versionereignis auftritt, wie beispielsweise das Erstellen, die Freigabe, das Aufheben der Freigabe oder die Wiederherstellung einer Version. Dieses Ereignisthema kann bei der Integration von Drittanbieter-Versionskontrollsystemen nützlich sein.
Compute allocation	Ja	Wird vor der Zuteilung von <code>resourcenames</code> und <code>hostselections</code> ausgegeben. Beide Eigenschaften können in dieser Phase geändert werden.
Compute post provision	Ja	Wird nach der erfolgreichen Bereitstellung einer Ressource ausgegeben.
Compute post removal	Ja	Wird nach dem Entfernen einer Computing-Ressource ausgegeben.
Compute provision	Ja	Wird vor dem Bereitstellen der Ressource auf der Hypervisor-Ebene ausgegeben. Hinweis Sie können die zugewiesene IP-Adresse ändern.
Compute removal	Ja	Wird vor dem Entfernen der Ressource ausgegeben.

Tabelle 6-4. Cloud Assembly-Ereignisthemen (Fortsetzung)

Ereignisthema	Blockierbar	Beschreibung
Compute reservation	Ja	Wird zum Zeitpunkt der Reservierung ausgegeben. Hinweis Sie können die Reihenfolge der Platzierungen ändern.
Deployment action completed	Ja	Wird nach Abschluss einer Bereitstellungsaktion ausgegeben.
Deployment action requested	Ja	Wird vor Abschluss einer Bereitstellungsaktion ausgegeben.
Deployment completed	Ja	Wird nach der Bereitstellung einer Cloud-Vorlage oder einer Kataloganforderung ausgegeben.
Deployment onboarded	Nein	Wird bei der Integration einer neuen Bereitstellung ausgegeben.
Deployment requested	Ja	Wird vor der Bereitstellung einer Cloud-Vorlage oder einer Kataloganforderung ausgegeben.
Deployment resource action completed	Ja	Wird nach der Bereitstellung einer Ressourcenaktion ausgegeben.
Deployment resource action requested	Ja	Wird vor der Bereitstellung einer Ressourcenaktion ausgegeben.
Deployment resource completed	Ja	Wird nach der Bereitstellung einer Bereitstellungsressource ausgegeben.
Deployment resource requested	Ja	Wird vor der Bereitstellung einer Bereitstellungsressource ausgegeben.
Disk allocation	Ja	Wird für die Vorabzuteilung von Datenträgerressourcen ausgegeben.
Disk attach	Ja	Wird vor dem Anhängen einer Festplatte an eine Maschine ausgegeben. <code>Disk attach</code> ist ein Lese- und Schreibereignis. Zu den für Rückschreibfunktionen unterstützten Festplatteneigenschaften gehören: <ul style="list-style-type: none"> ■ <code>diskFullPaths</code> ■ <code>diskDatastoreNames</code> ■ <code>diskParentDirs</code> Alle drei vSphere-spezifischen Festplatteneigenschaften sind für Updates erforderlich. Alle anderen Eigenschaften sind schreibgeschützt. Hinweis Die Rückschreibfunktion ist für vSphere-Festplatten der Klasse 1 optional.

Tabelle 6-4. Cloud Assembly-Ereignisthemen (Fortsetzung)

Ereignisthema	Blockierbar	Beschreibung
Disk detach	Ja	Wird nach dem Trennen einer Festplatte von einer Maschine ausgegeben. Disk detach ist ein schreibgeschütztes Ereignis.
Disk post removal	Ja	Wird nach dem Löschen einer Datenträgerressource ausgegeben.
Disk post resize	Ja	Wird nach einer Größenänderung der Datenträgerressource ausgegeben.
EventLog	Ja	Wird für Ereignisse ausgegeben, die sich auf die Protokollierung beziehen.
Kubernetes cluster allocation	Ja	Wird für die Vorabzuteilung von Ressourcen für einen Kubernetes-Cluster ausgegeben.
Kubernetes cluster post provision	Ja	Wird nach der Bereitstellung eines Kubernetes-Clusters ausgegeben.
Kubernetes cluster post removal	Ja	Wird nach dem Löschen eines Kubernetes-Clusters ausgegeben.
Kubernetes cluster provision	Ja	Wird vor der Bereitstellung eines Kubernetes-Clusters ausgegeben.
Kubernetes cluster removal	Ja	Wird vor dem Initiieren des Prozesses zum Löschen eines Kubernetes-Clusters ausgegeben.
Load balancer post provision	Ja	Wird nach der Bereitstellung eines Lastausgleichsdiensts ausgegeben.
Load balancer post removal	Ja	Wird nach Entfernung eines Lastausgleichsdiensts ausgegeben.
Load balancer provision	Ja	Wird vor der Bereitstellung eines Lastausgleichsdiensts ausgegeben.
Load balancer removal	Ja	Wird vor dem Entfernen eines Lastausgleichsdiensts ausgegeben.
Network Configure	Ja	Wird bei der Konfiguration des Netzwerks während der Computing-Zuteilung ausgegeben. Hinweis Das Thema „Netzwerkkonfiguration“ unterstützt mehrere IP-Adressen/Netzwerkkarten.
Network post provisioning	Ja	Wird nach dem Bereitstellen einer Netzwerkressource ausgegeben.
Network post removal	Ja	Wird nach dem Entfernen einer Netzwerkressource ausgegeben.

Tabelle 6-4. Cloud Assembly-Ereignisthemen (Fortsetzung)

Ereignisthema	Blockierbar	Beschreibung
Network provisioning	Ja	Wird vor der Bereitstellung einer Netzwerkressource ausgegeben.
Network removal	Ja	Wird vor dem Entfernen einer Netzwerkressource ausgegeben.
Security group post provisioning	Ja	Wird nach dem Bereitstellen einer Sicherheitsgruppe ausgegeben.
Security group post removal	Ja	Wird nach dem Entfernen einer Sicherheitsgruppe ausgegeben.
Security group provisioning	Ja	Wird vor der Bereitstellung einer Sicherheitsgruppe ausgegeben.
Security group removal	Ja	Wird vor dem Entfernen einer Sicherheitsgruppe ausgegeben.
Project Lifecycle	Nein	Ereignisse, die beim Erstellen, Aktualisieren oder Löschen eines Projekts ausgegeben werden.

Ereignisparameter

Nach dem Hinzufügen eines Ereignisthemas können Sie die Parameter dieses Ereignisthemas anzeigen. Diese Ereignisparameter definieren die Struktur der Ereignisnutzlast oder `inputProperties`. Bestimmte Ereignisparameter können nicht geändert werden. Sie werden als schreibgeschützt markiert. Sie können diese schreibgeschützten Parameter angeben, indem Sie rechts neben dem Parameter auf das Infosymbol klicken.

Protokoll der Erweiterbarkeitereignisse

Auf der Seite „Erweiterbarkeitereignisse“ wird eine Liste aller Ereignisse angezeigt, die in Ihrer Umgebung aufgetreten sind.

Sie können die Protokolle des Erweiterbarkeitereignisses anzeigen, indem Sie zu **Erweiterbarkeit > Ereignisse** navigieren. Sie können die Liste der Ereignisse auch anhand einer oder mehrerer Eigenschaften filtern. Zur Anzeige weiterer Details für ein einzelnes Ereignis wählen Sie die Ereignis-ID aus.

ID	Timestamp	Event Topic	User Name	Target ID	Description
cbaf56ce-a324-f5ae-5dd1-66d1e5911a6	04/28/20, 1:10 PM	N/A	N/A	endpoints	CREATE
efe21151-2906-dce2-14ab-68c17132d756	03/25/20, 4:22 PM	N/A	N/A	endpoints	CREATE
468e8b55-cf27-e77e-0179-1b5b736717b3	03/25/20, 10:12 AM	N/A	N/A	endpoints	CREATE
d9482883-d1ae-5899-fb06-852c202cc178	03/20/20, 2:41 PM	N/A	N/A	endpoints	CREATE
38584d40-p663-631f-7098-3747aa528d12	01/30/20, 5:35 PM	N/A	N/A	endpoints	CREATE

Erstellen eines Erweiterbarkeitsabonnements

Indem Sie eine vRealize Orchestrator-Integration oder Erweiterbarkeitsaktionen mit vRealize Automation Cloud Assembly verwenden, können Sie Abonnements zur Erweiterung Ihrer Anwendungen erstellen.

Mithilfe von Erweiterbarkeitsabonnements können Sie Ihre Anwendungen erweitern, indem Sie Workflows oder Aktionen bei bestimmten Lebenszyklusereignissen auslösen. Sie können auch Filter auf Ihre Abonnements anwenden, um boolesche Bedingungen für das angegebene Ereignis festzulegen. Beispiel: Das Ereignis und der Workflow oder die Aktion werden nur ausgelöst, wenn der boolesche Ausdruck `'true'` lautet. Dies ist hilfreich für Szenarien, in denen der Auslösezeitpunkt von Ereignissen, Aktionen oder Workflows gesteuert werden soll.

Voraussetzungen

- Cloud-Administratorbenutzerrolle
- Bei Verwendung von vRealize Orchestrator-Workflows:
 - Die Bibliothek des eingebetteten vRealize Orchestrator-Clients oder die Bibliothek einer integrierten externen vRealize Orchestrator-Instanz.
- Bei Verwendung von Erweiterbarkeitsaktionen:
 - Vorhandene Skripts für Erweiterbarkeitsaktionen. Weitere Informationen finden Sie unter [Vorgehensweise zum Erstellen von Erweiterbarkeitsaktionen](#).

Verfahren

- 1 Klicken Sie auf **Erweiterbarkeit > Abonnements**.
- 2 Klicken Sie auf **Neues Abonnement**.
- 3 Geben Sie die Details Ihres Abonnements ein.
- 4 Wählen Sie ein **Ereignisthema** aus.
- 5 (Optional) Legen Sie die Bedingungen für das Ereignisthema fest.

Hinweis Bedingungen können mithilfe eines JavaScript-Syntaxausdrucks erstellt werden. Dieser Ausdruck kann boolesche Operatoren enthalten, wie z. B. `"&&"` (AND), `"||"` (OR), `"^"` (XOR) und `"!"` (NOT). Sie können auch arithmetische Operatoren verwenden, wie z. B. `"=="` (equal to), `"!="` (not equal to), `">="` (greater than or equal), `"<="` (less than or equal), `">"` (greater than) und `"<"` (lesser than). Komplexere boolesche Ausdrücke können anhand einfacherer Ausdrücke erstellt werden. Um auf die Nutzlast (Daten) des Ereignisses entsprechend den angegebenen Themenparametern zuzugreifen, verwenden Sie `'event.data'` oder eine der Header-Eigenschaften des Ereignisses: `sourceType`, `sourceIdentity`, `timeStamp`, `eventType`, `eventTopicId`, `correlationType`, `correlationId`, `description`, `targetType`, `targetId`, `userName` und `orgId`.

- 6 Wählen Sie unter **Aktion/Workflow** ein ausführbares Element für Ihr Erweiterbarkeitsabonnement aus.

- 7 (Optional) Konfigurieren Sie gegebenenfalls das Blockierungsverhalten für das Ereignisthema.
- 8 (Optional) Um den Projektumfang des Erweiterungsabonnements zu definieren, deaktivieren Sie **Beliebiges Projekt** und klicken Sie auf **Projekte hinzufügen**.
- 9 Klicken Sie auf **Speichern**, um Ihr Abonnement zu speichern.

Ergebnisse

Ihr Abonnement wird erstellt. Wenn ein durch das ausgewählte Ereignisthema kategorisiertes Ereignis eintritt, wird der verknüpfte vRealize Orchestrator-Workflow oder die Erweiterbarkeitsaktion initiiert und alle Abonnenten werden benachrichtigt.

Nächste Schritte

Nach dem Erstellen Ihres Abonnements können Sie eine Cloud-Vorlage erstellen oder bereitstellen, um das Abonnement zu verknüpfen und zu verwenden. Sie können den Status der Workflow-Ausführung auch auf der Registerkarte **Erweiterbarkeit** innerhalb von vRealize Automation Cloud Assembly überprüfen. Bei Abonnements mit vRealize Orchestrator-Workflows können Sie auch die Ausführungen und den Workflowstatus über den vRealize Orchestrator-Client überwachen.

Fehlerbehebung für ein Erweiterbarkeitsabonnement

Beheben Sie Fehler bei Erweiterungsabonnements.

Wenn Ihr Abonnement fehlschlägt, ist dies häufig auf Fehler bei Ihrem Workflow oder Erweiterbarkeitsaktionsskript zurückzuführen.

Anzeigen von Themenparametern und Nutzlast

Sie können ein Skript vom Typ „Sichern der Themenparameter eines Abonnements“ verwenden, um bestimmte Parameter und die Nutzlast Ihrer virtuellen Maschine in einer beliebigen Ereignisphase anzuzeigen.

Dieses Skript eignet sich vor allem zum Debuggen und Überprüfen verfügbarer Eingaben für Ihren vRealize Orchestrator-Workflow. Um alle Parameter Ihrer virtuellen Maschine anzuzeigen, verwenden Sie folgendes Skript mit Ihrem Workflow:

```
function dumpProperties(props, lvl) {
    var keys = props.keys;
    var prefix = ""
    for (var i=0; i<lvl; i++){
        prefix = prefix + " ";
    }
    for (k in keys){
        var key = keys[k];
        var value = props.get(keys[k])
        if ("Properties" == System.getObjectType(value)) {
            System.log(prefix + key + "[")
            dumpProperties(value, (lvl+2));
            System.log(prefix+ "]")
        } else {
            System.log( prefix + key + ":" + value)
        }
    }
}
```

```

    }
    }

    dumpProperties(inputProperties, 0)

    customProps = inputProperties.get("customProperties")

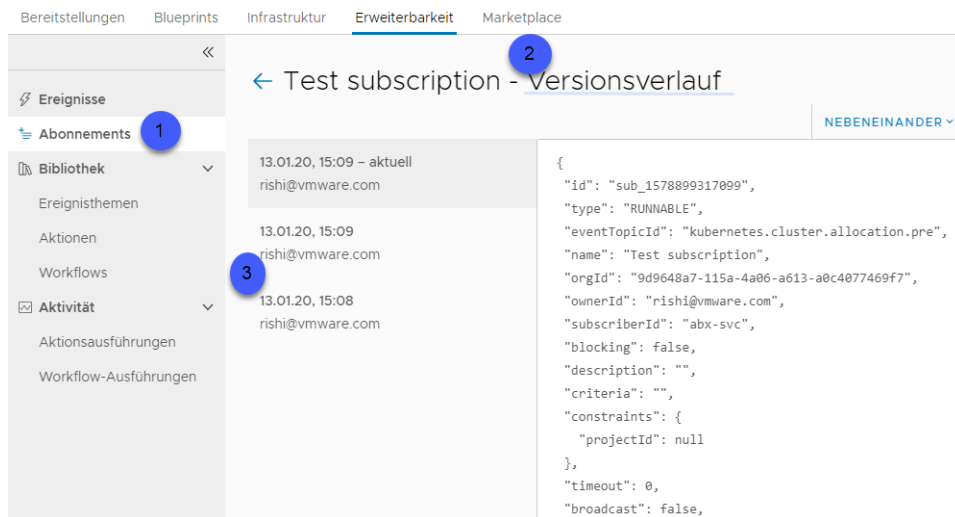
```

Versionsverlauf eines Abonnements

Wenn Ihr Abonnement fehlschlägt, können Sie den Versionsverlauf anzeigen.

Anzeigen des Versionsverlaufs des Abonnements

Auf der Registerkarte „Versionsverlauf“ können Sie den Änderungsverlauf Ihres Abonnements mit dem Benutzer und dem Änderungsdatum anzeigen. Wenn Ihr Abonnement fehlschlägt oder nicht ordnungsgemäß ausgeführt wird, kann der Versionsverlauf helfen, die Ursache zu ermitteln.



1

Öffnen Sie Ihr Abonnement auf der Registerkarte **Abonnements**.

2

Um den Versionsverlauf anzuzeigen, klicken Sie auf **Versionsverlauf**.

3

Sie können auf jeden Änderungseintrag klicken, um den entsprechenden Abonnementcode anzuzeigen, der mit der Änderung verknüpft ist.

Eigenschaften der vRealize Automation-Ressource

Mit dem vRealize Automation-Editor „Infrastruktur-als-Code“ können Sie auf die Hilfe zur Syntax und Codeergänzung klicken bzw. den Mauszeiger darüber halten. Den vollständigen Satz der Ressourceneigenschaften einer Cloud-Vorlage, die manchmal als benutzerdefinierte Eigenschaften bezeichnet werden, finden Sie im konsolidierten Ressourcenschema.

Das Schema ist auf der VMware {code}-Website verfügbar. Folgen Sie dem Link und klicken Sie auf **Modelle**, um die Ressourcenobjekte aufzuführen, die für zuvor als Blueprints bezeichnete Cloud-Vorlagen verfügbar sind.

- [vRealize Automation-Ressourcentypschemata in VMware {code}](#)

Beispiele für vRealize Automation Cloud Assembly-Code

Die Kombinations- und Anwendungsmöglichkeiten von Cloud-Vorlagencode in vRealize Automation Cloud Assembly sind nahezu unbegrenzt.

Erfolgreicher Code stellt häufig den besten Ausgangspunkt für die weitere Entwicklung dar. Wenn Sie sich an einem Beispiel orientieren, ersetzen Sie Ressourcennamen, Werte usw., um Ihre Site-Einstellungen anzuwenden.

vSphere-Ressourcenbeispiele in vRealize Automation Cloud Assembly-Cloud-Vorlagen

In diesen Codebeispielen werden vSphere-Maschinenressourcen innerhalb von vRealize Automation Cloud Assembly-Cloud-Vorlagen veranschaulicht.

Ressource	Beispiel-Cloud-Vorlage
Virtuelle vSphere-Maschine mit CPU, Arbeitsspeicher und Betriebssystem	<pre>resources: demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine cpuCount: 1 totalMemoryMB: 1024 image: ubuntu</pre>
vSphere-Maschine mit einer Datenspeicherressource	<pre>resources: demo-vsphere-disk-001: type: Cloud.vSphere.Disk properties: name: DISK_001 type: 'HDD' capacityGb: 10 dataStore: 'datastore-01' provisioningType: thick</pre>

Ressource	Beispiel-Cloud-Vorlage
vSphere-Maschine mit angehängter Festplatte	<pre> resources: demo-vsphere-disk-001: type: Cloud.vSphere.Disk properties: name: DISK_001 type: HDD capacityGb: 10 dataStore: 'datastore-01' provisioningType: thin demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine cpuCount: 2 totalMemoryMB: 2048 imageRef: >- https://bintray.com/vmware/photon/ download_file?file_path=2.0%2FRC%2Fova%2Fphoton- custom-hw11-2.0-31bb961.ova attachedDisks: - source: '\${demo-vsphere-disk-001.id}' </pre>
vSphere-Maschine mit einer dynamischen Anzahl an Festplatten	<pre> inputs: disks: type: array title: disks items: title: disk type: object properties: size: type: integer title: size maxItems: 15 resources: Cloud_Machine_1: type: Cloud.vSphere.Machine properties: image: centos7 flavor: small attachedDisks: '\$ {map_to_object(resource.Cloud_Volume_1[*].id, "source")}' Cloud_Volume_1: type: Cloud.Volume allocatePerInstance: true properties: capacityGb: '\${input.disks[count.index].size}' count: '\${length(input.disks)}' </pre>
vSphere-Maschine aus einem Snapshot-Image. Fügen Sie einen Schrägstrich und den Namen des Snapshots an. Das Image des Snapshots kann ein Linked Clone sein.	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: imageRef: 'demo-machine/snapshot-01' cpuCount: 1 totalMemoryMB: 1024 </pre>

Ressource	Beispiel-Cloud-Vorlage
vSphere-Maschine in einem bestimmten Ordner in vCenter	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine cpuCount: 2 totalMemoryMB: 1024 imageRef: ubuntu resourceGroupName: 'myFolder' </pre>
vSphere-Maschine mit mehreren Netzwerkkarten	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: image: ubuntu flavor: small networks: - network: '\${network-01.name}' deviceIndex: 0 - network: '\${network-02.name}' deviceIndex: 1 network-01: type: Cloud.vSphere.Network properties: name: network-01 network-02: type: Cloud.vSphere.Network properties: name: network-02 </pre>
vSphere-Maschine mit einem angehängten Tag in vCenter	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu tags: - key: env value: demo </pre>

Ressource	Beispiel-Cloud-Vorlage
vSphere-Maschine mit einer Anpassungsspezifikation	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine image: ubuntu flavor: small customizationSpec: Linux </pre>
vSphere-Maschine mit Remotezugriff	<pre> inputs: username: type: string title: Username description: Username default: testUser password: type: string title: Password default: VMware@123 encrypted: true description: Password for the given username resources: demo-machine: type: Cloud.vSphere.Machine properties: flavor: small imageRef: >- https://cloud-images.ubuntu.com/releases/ 16.04/release-20170307/ubuntu-16.04-server-cloudimg- amd64.ova cloudConfig: ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' runcmd: - echo "Defaults:\${input.username} ! requiretty" >> /etc/sudoers.d/\${input.username} </pre>

Dokumentiertes Beispiel für eine vRealize Automation Cloud Assembly-Vorlage

Mithilfe der umfassenden in diesem Beispiel enthaltenen Kommentare können Sie die Struktur und den Zweck der Abschnitte in einer vRealize Automation Cloud Assembly-Vorlage (früher als Blueprint bezeichnet) überprüfen.

```
# *****
#
# This WordPress cloud template is enhanced with comments to explain its
# parameters.
#
# Try cloning it and experimenting with its YAML code. If you're new to
# YAML, visit yaml.org for general information.
#
# The cloud template deploys a minimum of 3 virtual machines and runs scripts
# to install packages.
#
# *****
#
# -----
# Templates need a descriptive name and version if
# source controlled in git.
# -----
name: WordPress Template with Comments
formatVersion: 1
version: 1
#
# -----
# Inputs create user selections that appear at deployment time. Inputs
# can set placement decisions and configurations, and are referenced
# later, by the resources section.
# -----
inputs:
#
# -----
# Choose a cloud endpoint. 'Title' is the visible
# option text (oneOf allows for the friendly title). 'Const' is the
# tag that identifies the endpoint, which was set up earlier, under the
# Cloud Assembly Infrastructure tab.
# -----
platform:
  type: string
  title: Deploy to
  oneOf:
    - title: AWS
      const: aws
    - title: Azure
      const: azure
    - title: vSphere
      const: vsphere
  default: vsphere
#
# -----
```

```

# Choose the operating system. Note that the Cloud Assembly
# Infrastructure must also have an AWS, Azure, and vSphere Ubuntu image
# mapped. In this case, enum sets the option that you see, meaning there's
# no friendly title feature this time. Also, only Ubuntu is available
# here, but having this input stubbed in lets you add more operating
# systems later.
# -----
osimage:
  type: string
  title: Operating System
  description: Which OS to use
  enum:
    - Ubuntu
#
# -----
# Set the number of machines in the database cluster. Small and large
# correspond to 1 or 2 machines, respectively, which you see later,
# down in the resources section.
# -----
dbenvsize:
  type: string
  title: Database cluster size
  enum:
    - Small
    - Large
#
# -----
# Dynamically tag the machines that will be created. The
# 'array' of objects means you can create as many key-value pairs as
# needed. To see how array input looks when it's collected,
# open the cloud template and click TEST.
# -----
Mtags:
  type: array
  title: Tags
  description: Tags to apply to machines
  items:
    type: object
    properties:
      key:
        type: string
        title: Key
      value:
        type: string
        title: Value
#
# -----
# Create machine credentials. These credentials are needed in
# remote access configuration later, in the resources section.
# -----
username:
  type: string
  minLength: 4
  maxLength: 20
  pattern: '[a-z]+'

```

```

    title: Database Username
    description: Database Username
  userpassword:
    type: string
    pattern: '[a-z0-9A-Z@#\$]+'
    encrypted: true
    title: Database Password
    description: Database Password
#
# -----
# Set the database storage disk size.
# -----
databaseDiskSize:
  type: number
  default: 4
  maximum: 10
  title: MySQL Data Disk Size
  description: Size of database disk
#
# -----
# Set the number of machines in the web cluster. Small, medium, and large
# correspond to 2, 3, and 4 machines, respectively, which you see later,
# in the WebTier part of the resources section.
# -----
clusterSize:
  type: string
  enum:
    - small
    - medium
    - large
  title: Wordpress Cluster Size
  description: Wordpress Cluster Size
#
# -----
# Set the archive storage disk size.
# -----
archiveDiskSize:
  type: number
  default: 4
  maximum: 10
  title: Wordpress Archive Disk Size
  description: Size of Wordpress archive disk
#
# -----
# The resources section configures the deployment of machines, disks,
# networks, and other objects. In several places, the code pulls from
# the preceding interactive user inputs.
# -----
resources:
#
# -----
# Create the database server. Choose a cloud agnostic machine 'type' so
# that it can deploy to AWS, Azure, or vSphere. Then enter its property
# settings.
# -----

```

```

DBTier:
  type: Cloud.Machine
  properties:
#
# -----
# Descriptive name for the virtual machine. Does not become the hostname
# upon deployment.
# -----
    name: mysql
#
# -----
# Hard-coded operating system image to use. To pull from user input above,
# enter the following instead.
# image: '${input.osimage}'
# -----
    image: Ubuntu
#
# -----
# Hard-coded capacity to use. Note that the Cloud Assembly
# Infrastructure must also have AWS, Azure, and vSphere flavors
# such as small, medium, and large mapped.
# -----
    flavor: small
#
# -----
# Tag the database machine to deploy to the cloud vendor chosen from the
# user input. Tags are case-sensitive, so 'to_lower' forces the tag to
# lowercase to ensure a match with a site's tagging convention. It's
# important if platform input were to contain any upper case characters.
# -----
    constraints:
      - tag: '${"env:" + to_lower(input.platform)}'
#
# -----
# Also tag the database machine with any free-form tags that were created
# during user input.
# -----
    tags: '${input.Mtags}'
#
# -----
# Set the database cluster size by referencing the dbenvsize user
# input. Small is one machine, and large defaults to two.
# -----
    count: '${input.dbenvsize == "Small" ? 1 : 2}'
#
# -----
# Add a variable to connect the machine to a network resource based on
# a property binding to another resource. In this case, it's the
# 'WP_Network' network that gets defined further below.
# -----
    networks:
      - network: '${resource.WP_Network.id}'
#
# -----
# Enable remote access to the database server. Reference the credentials

```

```

# from the user input.
# -----
    remoteAccess:
      authentication: usernamePassword
      username: '${input.username}'
      password: '${input.userpassword}'
#
# -----
# You are free to add custom properties, which might be used to initiate
# an extensibility subscription, for example.
# -----
    ABC-Company-ID: 9393
#
# -----
# Run OS commands or scripts to further configure the database machine,
# via operations such as setting a hostname, generating SSH private keys,
# or installing packages.
# -----
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
      packages:
        - mysql-server
      runcmd:
        - sed -e '/bind-address/ s/^#*#/' -i /etc/mysql/mysql.conf.d/mysqld.cnf
        - service mysql restart
        - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'mysqlpassword';"
        - mysql -e "FLUSH PRIVILEGES;"
    attachedDisks: []
#
# -----
# Create the web server. Choose a cloud agnostic machine 'type' so that it
# can deploy to AWS, Azure, or vSphere. Then enter its property settings.
# -----
    WebTier:
      type: Cloud.Machine
      properties:
#
# -----
# Descriptive name for the virtual machine. Does not become the hostname
# upon deployment.
# -----
    name: wordpress
#
# -----
# Hard-coded operating system image to use. To pull from user input above,
# enter the following instead:
# image: '${input.osimage}'
# -----
    image: Ubuntu
#
# -----
# Hard-coded capacity to use. Note that the Cloud Assembly
# Infrastructure must also have AWS, Azure, and vSphere flavors

```

```

# such as small, medium, and large mapped.
# -----
#     flavor: small
#
# -----
# Set the web server cluster size by referencing the clusterSize user
# input. Small is 2 machines, medium is 3, and large defaults to 4.
# -----
#     count: '${input.clusterSize== "small" ? 2 : (input.clusterSize == "medium" ? 3 : 4)}'
#
# -----
# Set an environment variable to display object information under the
# Properties tab, post-deployment. Another example might be
# {env.blueprintID}
# -----
#     tags:
#       - key: cas.requestedBy
#         value: '${env.requestedBy}'
#
# -----
# You are free to add custom properties, which might be used to initiate
# an extensiblity subscription, for example.
# -----
#     ABC-Company-ID: 9393
#
# -----
# Tag the web server to deploy to the cloud vendor chosen from the
# user input. Tags are case-sensitive, so 'to_lower' forces the tag to
# lowercase to ensure a match with your site's tagging convention. It's
# important if platform input were to contain any upper case characters.
# -----
#     constraints:
#       - tag: '${"env:" + to_lower(input.platform)}'
#
# -----
# Add a variable to connect the machine to a network resource based on
# a property binding to another resource. In this case, it's the
# 'WP_Network' network that gets defined further below.
# -----
#     networks:
#       - network: '${resource.WP_Network.id}'
#
# -----
# Run OS commands or scripts to further configure the web server,
# with operations such as setting a hostname, generating SSH private keys,
# or installing packages.
# -----
#     cloudConfig: |
#       #cloud-config
#       repo_update: true
#       repo_upgrade: all
#       packages:
#         - apache2
#         - php
#         - php-mysql

```

```

- libapache2-mod-php
- php-mcrypt
- mysql-client
runcmd:
- mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
mywordpresssite --strip-components 1
- i=0; while [ $i -le 5 ]; do mysql --connect-timeout=3 -h $
{DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;
i=$((i+1)); done
- mysql -u root -pmysqlpassword -h ${resource.DBTier.networks[0].address} -e
"create database wordpress_blog;"
- mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/
mywordpresssite/wp-config.php
- sed -i -e s/"define('DB_NAME', 'database_name_here');"/"define('DB_NAME',
'wordpress_blog');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
-e s/"define('DB_USER', 'username_here');"/"define('DB_USER', 'root');"/ /var/www/html/
mywordpresssite/wp-config.php && sed -i -e s/"define('DB_PASSWORD',
'password_here');"/"define('DB_PASSWORD', 'mysqlpassword');"/ /var/www/html/mywordpresssite/
wp-config.php && sed -i -e s/"define('DB_HOST', 'localhost');"/"define('DB_HOST', '$
{resource.DBTier.networks[0].address}');"/ /var/www/html/mywordpresssite/wp-config.php
- service apache2 reload
#
# -----
# Create the network that the database and web servers connect to.
# Choose a cloud agnostic network 'type' so that it can deploy to AWS,
# Azure, or vSphere. Then enter its property settings.
# -----
WP_Network:
  type: Cloud.Network
  properties:
#
# -----
# Descriptive name for the network. Does not become the network name
# upon deployment.
# -----
name: WP_Network
#
# -----
# Set the networkType to an existing network. You could also use a
# constraint tag to target a specific, like-tagged network.
# The other network types are private or public.
# -----
networkType: existing
#
# *****
#
# VMware hopes that you found this commented template useful. Note that
# you can also access an API to create templates, or query for input
# schema that you intend to request. See the following Swagger
# documentation.
#
# www.mgmt.cloud.vmware.com/blueprint/api/swagger/swagger-ui.html
#
# *****

```

Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen

Sie können Ressourcen und Einstellungen für Netzwerk, Sicherheit und Lastausgleichsdienste in Cloud-Vorlagendesigns und Bereitstellungen verwenden.

Eine Zusammenfassung der Designcodeoptionen für Cloud-Vorlagen finden Sie unter [vRealize Automation-Ressourcentypschemata](#).

Weitere Informationen finden Sie unter:

- [Verwenden einer Netzwerkressource in einer vRealize Automation-Cloud-Vorlage](#)
- [Verwenden einer Sicherheitsgruppenressource in einer vRealize Automation-Cloud-Vorlage](#)
- [Verwenden einer Lastausgleichsdienstressource in einer vRealize Automation-Cloud-Vorlage](#)

Diese Beispiele veranschaulichen Netzwerk-, Sicherheitsgruppen- und Lastausgleichsdienstressourcen in einfachen Cloud-Vorlagendesigns.

Ressourcenszenario	Beispiel für den Designcode einer Cloud-Vorlage
vSphere-Maschine mit mehreren Netzwerkkarten, die mit einer NSX-Netzwerkressource verknüpft sind.	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: image: ubuntu flavor: small networks: - network: '\${ {resource.Cloud_vSphere_Network_1.id}}' Cloud_vSphere_Network_1: type: Cloud.vSphere.Network properties: networkType: existing Cloud_vSphere_Network_2: type: Cloud.NSX.Network properties: networkType: existing </pre>
Aktivieren Sie die NAT-Portweiterleitung, indem Sie eine Cloud.NSX.Gateway-Cloud-Vorlagenressource für ein ausgehendes Netzwerk verwenden.	<pre> ... gateway: type: Cloud.NSX.Gateway properties: networks: - \${resource.out.id} natRules: - index: 1 translatedInstance: \$ {resource.jumpbox.networks[0].id} destinationPorts: 2200 translatedPorts: 22 description: inbound ssh - index: 2 ... </pre>

Ressourcenszenario	Beispiel für den Designcode einer Cloud-Vorlage
<p>Geben Sie die Protokollierungsebene, den Algorithmus und die Größe des Lastausgleichs an.</p>	<p>NSX-Beispiellastausgleichsdienst, der die Verwendung der Protokollierungsebene, des Algorithmus und der Größe anzeigt:</p> <pre> resources: Cloud_LoadBalancer_1: type: Cloud.NSX.LoadBalancer properties: name: myapp-lb network: '\${appnet-public.name}' instances: '\${wordpress.id}' routes: - protocol: HTTP port: '80' loggingLevel: CRITICAL algorithm: LEAST_CONNECTION type: MEDIUM </pre>
<p>Verknüpfen Sie einen Lastausgleichsdienst mit einer benannten Maschine oder Maschinen-Netzwerkkarte. Sie können entweder <code>machine ID</code> oder <code>machine network ID</code> angeben, um die Maschine dem Pool der Lastausgleichsdienste hinzuzufügen. Die Eigenschaft „Instanzen“ unterstützt sowohl Maschinen (<code>machine by ID</code>) als auch Netzwerkkarten (<code>machine by network ID</code>). Im ersten Beispiel wird in der Bereitstellung die Einstellung <code>machine by ID</code> verwendet, um einen Lastausgleich der Maschine durchzuführen, wenn sie in einem beliebigen Netzwerk bereitgestellt wird. Im zweiten Beispiel wird in der Bereitstellung die Einstellung <code>machine by network ID</code> verwendet, um nur dann einen Lastausgleich der Maschine durchzuführen, wenn die Maschine auf der benannten Maschinen-Netzwerkkarte bereitgestellt wird. Das dritte Beispiel zeigt beide Einstellungen, die in derselben <code>instances</code>-Option verwendet werden.</p>	<p>Sie können die Eigenschaft <code>instances</code> zum Definieren einer Maschinen-ID oder einer Maschinennetzwerk-ID verwenden:</p> <ul style="list-style-type: none"> ■ Maschinen-ID <pre> Cloud_LoadBalancer_1: type: Cloud.LoadBalancer properties: network: '\${resource.Cloud_Network_1.id}' instances: '\$ {resource.Cloud_Machine_1.id}' </pre> ■ Maschinennetzwerk-ID <pre> Cloud_LoadBalancer_1: type: Cloud.LoadBalancer properties: network: '\${resource.Cloud_Network_1.id}' instances: '\$ {resource.Cloud_Machine_1.networks[0].id}' </pre> ■ Eine für die Einbeziehung in den Lastausgleich angegebene Maschine und eine andere für die Einbeziehung in den Lastausgleich angegebene Maschinen-Netzwerkkarte: <pre> instances: - resource.Cloud_Machine_1.id - resource.Cloud_Machine_2.networks[2].id </pre>

Ressourcenszenario	Beispiel für den Designcode einer Cloud-Vorlage
<p>Public Cloud-Maschine zur Verwendung einer internen IP-Adresse anstelle einer öffentlichen IP-Adresse. In diesem Beispiel wird eine bestimmte Netzwerk-ID verwendet.</p> <p>Hinweis: Die Option <code>network:</code> wird in der Einstellung <code>networks:</code> verwendet, um eine Zielnetzwerk-ID anzugeben. Die Option <code>name:</code> in der Einstellung <code>networks:</code> ist veraltet und sollte nicht mehr verwendet werden.</p>	<pre>resources: wf_proxy: type: Cloud.Machine properties: image: ubuntu 16.04 flavor: small constraints: - tag: 'platform:vsphere' networks: - network: '\${resource.wf_net.id}' assignPublicIpAddress: false</pre>
<p>Geroutetes Netzwerk für NSX-V oder NSX-T unter Verwendung des NSX-Netzwerkressourcentyps.</p>	<pre>Cloud_NSX_Network_1: type: Cloud.NSX.Network properties: networkType: routed</pre>
<p>Fügen Sie der Netzwerkkartenressource einer Maschine in der Cloud-Vorlage ein Tag hinzu.</p>	<pre>formatVersion: 1 inputs: {} resources: Cloud_Machine_1: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu networks: - name: '\${resource.Cloud_Network_1.name}' deviceIndex: 0 tags: - key: 'nic0' value: null - key: internal value: true - name: '\${resource.Cloud_Network_2.name}' deviceIndex: 1 tags: - key: 'nic1' value: null - key: internal value: false</pre>

Ressourcenszenario	Beispiel für den Designcode einer Cloud-Vorlage
<p>Taggen Sie logische NSX-T-Switches für ein ausgehendes Netzwerk.</p> <p>Tagging wird für NSX-T und VMware Cloud on AWS unterstützt.</p> <p>Weitere Informationen zu diesem Szenario finden Sie im Community-Blogbeitrag Erstellen von Tags in NSX mit Cloud Assembly.</p>	<pre>Cloud_NSX_Network_1: type: Cloud.NSX.Network properties: networkType: outbound tags: - key: app value: opencart</pre>
<p>Vorhandene Sicherheitsgruppe mit einem Einschränkungs-Tag, das auf eine Maschinen-Netzwerkkarte (NIC) angewendet wurde.</p> <p>Um eine vorhandene Sicherheitsgruppe zu verwenden, geben Sie <i>Vorhanden</i> für die Eigenschaft <code>securityGroupType</code> ein.</p> <p>Sie können einer <code>Cloud.SecurityGroup</code>-Ressource Tags zuweisen, um vorhandene Sicherheitsgruppen mithilfe von Tag-Einschränkungen zuzuteilen. Sicherheitsgruppen, die keine Tags enthalten, können im Cloud-Vorlagendesign nicht verwendet werden.</p> <p>Einschränkungs-Tags müssen für <code>securityGroupType: existing</code>-Sicherheitsgruppenressourcen festgelegt werden. Diese Einschränkungen müssen mit den Tags übereinstimmen, die in den vorhandenen Sicherheitsgruppen festgelegt wurden. Für <code>securityGroupType: new</code>-Sicherheitsgruppenressourcen können keine Einschränkungs-Tags festgelegt werden.</p>	<pre>formatVersion: 1 inputs: {} resources: allowSsh_sg: type: Cloud.SecurityGroup properties: securityGroupType: existing constraints: - tag: allowSsh compute: type: Cloud.Machine properties: image: centos flavor: small networks: - network: '\${resource.prod-net.id}' securityGroups: - '\${resource.allowSsh_sg.id}' prod-net: type: Cloud.Network properties: networkType: existing</pre>

Ressourcenszenario	Beispiel für den Designcode einer Cloud-Vorlage
<p>Bedarfsgesteuerte Sicherheitsgruppe mit zwei Firewallregeln, die die Zugriffsoptionen Allow und Deny veranschaulichen.</p>	<pre> resources: Cloud_SecurityGroup_1: type: Cloud.SecurityGroup properties: securityGroupType: new rules: - ports: 5000 source: 'fc00:10:000:000:000:56ff:fe89:48b4' access: Allow direction: inbound name: allow_5000 protocol: TCP - ports: 7000 source: 'fc00:10:000:000:000:56ff:fe89:48b4' access: Deny direction: inbound name: deny_7000 protocol: TCP Cloud_vSphere_Machine_1: type: Cloud.vSphere.Machine properties: image: photon cpuCount: 1 totalMemoryMB: 256 networks: - network: '\$ {resource.Cloud_Network_1.id}' assignIPv6Address: true assignment: static securityGroups: - '\$ {resource.Cloud_SecurityGroup_1.id}' Cloud_Network_1: type: Cloud.Network properties: networkType: existing </pre>

Ressourcenszenario	Beispiel für den Designcode einer Cloud-Vorlage
<p>Komplexe Cloud-Vorlage mit 2 Sicherheitsgruppen, einschließlich:</p> <ul style="list-style-type: none"> ■ 1 vorhandenen Sicherheitsgruppe ■ 1 bedarfsgesteuerte Sicherheitsgruppe mit mehreren Beispielen für Firewallregeln ■ 1 vSphere-Maschine ■ 1 vorhandenen Netzwerks <p>Dieses Beispiel veranschaulicht verschiedene Kombinationen aus Protokollen und Ports, Dienste, IP-CIDR als Quelle und Ziel, IP-Bereich als Quelle oder Ziel sowie die Optionen für „Beliebig“, „IPv6“ und (::/0).</p> <p>Für Maschinen-Netzwerkkarten können Sie das verbundene Netzwerk und die Sicherheitsgruppe(n) angeben. Sie können auch den Netzwerkkartenindex oder eine IP-Adresse angeben.</p>	<pre> formatVersion: 1 inputs: {} resources: DEMO_ESG : existing security group - security group 1) type: Cloud.SecurityGroup properties: constraints: - tag: BlockAll securityGroupType: existing (designation of existing for security group 1) DEMO_ODSG: (on-demand security group - security group 2)) type: Cloud.SecurityGroup properties: rules: (multiple firewall rules in this section) - name: IN-ANY (rule 1) source: any service: any direction: inbound access: Deny - name: IN-SSH (rule 2) source: any service: SSH direction: inbound access: Allow - name: IN-SSH-IP (rule 3) source: 33.33.33.1-33.33.33.250 protocol: TCP ports: 223 direction: inbound access: Allow - name: IPv-6-ANY-SOURCE (rule 4) source: ':::/0' protocol: TCP ports: 223 direction: inbound access: Allow - name: IN-SSH-IP (rule 5) source: 44.44.44.1/24 protocol: UDP ports: 22-25 direction: inbound access: Allow - name: IN-EXISTING-SG (rule 6) source: '\${resource["DEMO_ESG"].id}' protocol: ICMPv6 direction: inbound access: Allow - name: OUT-ANY (rule 7) destination: any service: any direction: outbound access: Deny - name: OUT-TCP-IPv6 (rule 8) destination: '2001:0db8:85a3::8a2e:0370:7334/64' protocol: TCP ports: 22 direction: outbound access: Allow </pre>

Ressourcenszenario

Beispiel für den Designcode einer Cloud-Vorlage

```

- name: IPv6-ANY-DESTINATION (rule 9)
  destination: '::/0'
  protocol: UDP
  ports: 23
  direction: outbound
  access: Allow
- name: OUT-UDP-SERVICE (rule 10)
  destination: any
  service: NTP
  direction: outbound
  access: Allow
  securityGroupType: new (designation of on-
demand for security group 2)
  DEMO_VC_MACHINE: (machine resource)
  type: Cloud.vSphere.Machine
  properties:
    image: PHOTON
    cpuCount: 1
    totalMemoryMB: 1024
    networks: (Machine network NICs)
  - network: '${resource.DEMO_NW.id}'
  securityGroups: - '${resource.DEMO_ODSG.id}' -
  '${resource.DEMO_ESG.id}'
  DEMO_NETWORK: (network resource)
  type: Cloud.vSphere.Network
  properties:
    networkType: existing
    constraints:
      - tag: nsx62

```

Ressourcenszenario	Beispiel für den Designcode einer Cloud-Vorlage
<p>Bedarfsgesteuertes Netzwerk mit einem 1-armigen Lastausgleichsdienst.</p>	<pre> inputs: {} resources: mp-existing: type: Cloud.Network properties: name: mp-existing networkType: existing mp-wordpress: type: Cloud.vSphere.Machine properties: name: wordpress count: 2 flavor: small image: tiny customizationSpec: Linux networks: - network: '\${resource["mp-private"].id}' mp-private: type: Cloud.NSX.Network properties: name: mp-private networkType: private constraints: - tag: nsxt mp-wordpress-lb: type: Cloud.LoadBalancer properties: name: wordpress-lb internetFacing: false network: '\${resource.mp-existing.id}' instances: '\${resource["mp-wordpress"].id}' routes: - protocol: HTTP port: '80' instanceProtocol: HTTP instancePort: '80' healthCheckConfiguration: protocol: HTTP port: '80' urlPath: /index.pl intervalSeconds: 60 timeoutSeconds: 30 unhealthyThreshold: 5 healthyThreshold: 2 </pre>
<p>Vorhandenes Netzwerk mit einem Lastausgleichsdienst.</p>	<pre> formatVersion: 1 inputs: count: type: integer default: 1 resources: ubuntu-vm: type: Cloud.Machine properties: name: ubuntu flavor: small image: tiny count: '\${input.count}' networks: </pre>

Ressourcenszenario	Beispiel für den Designcode einer Cloud-Vorlage
	<pre> - network: '\$ {resource.Cloud_NSX_Network_1.id}' Provider_LoadBalancer_1: type: Cloud.LoadBalancer properties: name: OC-LB routes: - protocol: HTTP port: '80' instanceProtocol: HTTP instancePort: '80' healthCheckConfiguration: protocol: HTTP port: '80' urlPath: /index.html intervalSeconds: 60 timeoutSeconds: 5 unhealthyThreshold: 5 healthyThreshold: 2 network: '\$ {resource.Cloud_NSX_Network_1.id}' internetFacing: false instances: '\${resource["ubuntu-vm"].id}' Cloud_NSX_Network_1: type: Cloud.NSX.Network properties: networkType: existing constraints: - tag: nsxt24prod </pre>

Weitere Informationen

Implementierungsszenarien für Netzwerk und Sicherheit finden Sie in den folgenden VMware-Blogs:

- [vRealize Automation Cloud Assembly-Lastausgleichsdienst mit NSX-T Deep Dive](#)
- [Netzwerkautomatisierung mit Cloud Assembly und NSX – Teil 1](#) (beinhaltet die Verwendung von NSX-T- und vCenter-Cloud-Konten und Netzwerk-CIDR)
- [Netzwerkautomatisierung mit Cloud Assembly und NSX – Teil 2](#) (beinhaltet die Verwendung vorhandener und ausgehender Netzwerktypen)
- [Netzwerkautomatisierung mit Cloud Assembly und NSX – Teil 3](#) (beinhaltet die Verwendung vorhandener und bedarfsgesteuerter Sicherheitsgruppen)
- [Netzwerkautomatisierung mit Cloud Assembly und NSX – Teil 4](#) (beinhaltet die Verwendung vorhandener und bedarfsgesteuerter Lastausgleichsdienste)

Verwenden einer Netzwerkressource in einer vRealize Automation-Cloud-Vorlage

Wenn Sie die Designs Ihrer vRealize Automation-Cloud-Vorlage erstellen oder bearbeiten, verwenden Sie die für Ihre Zwecke am besten geeigneten Netzwerkressourcen. Erfahren Sie mehr

über die NSX- und Cloud-unabhängigen Netzwerkoptionen, die in der Cloud-Vorlage verfügbar sind.

Wählen Sie basierend auf der Maschine und den zugehörigen Bedingungen im Design Ihrer vRealize Automation-Cloud-Vorlage einen der verfügbaren Netzwerkressourcentypen aus.

Cloud-unabhängige Netzwerkressource

Sie fügen ein Cloud-unabhängiges Netzwerk hinzu, indem Sie die Ressource **Cloud-unabhängig > Netzwerk** auf der Seite **Design** der Cloud-Vorlage verwenden. Die Ressource wird im Code der Cloud-Vorlage als `Cloud.Network`-Ressourcentyp angezeigt. Die Standardressource wird wie folgt angezeigt:

```
Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkType: existing
```

Verwenden Sie ein Cloud-unabhängiges Netzwerk, wenn Sie Netzwerkmerkmale für einen Zielmaschinentyp angeben möchten, der evtl. nicht mit einem NSX-Netzwerk verbunden ist.

Die Cloud-unabhängige Netzwerkressource ist für die folgenden Ressourcentypen verfügbar:

- Cloud-unabhängige Maschine
- vSphere
- Google Cloud Platform (GCP)
- Amazon Web Services (AWS)
- Microsoft Azure
- VMware Cloud on AWS (VMC)

Die Cloud-unabhängige Netzwerkressource ist für die folgenden Netzwerktypen (`networkType`) verfügbar:

- öffentlich
- privat
- ausgehend
- vorhanden

vSphere-Netzwerkressource

Sie fügen ein vSphere-Netzwerk mithilfe der Ressource **vSphere > Netzwerk** auf der Seite **Design** der Cloud-Vorlage hinzu. Die Ressource wird im Code der Cloud-Vorlage als `Cloud.vSphere.Network`-Ressourcentyp angezeigt. Die Standardressource wird wie folgt angezeigt:

```
Cloud_vSphere_Network_1:
  type: Cloud.vSphere.Network
  properties:
    networkType: existing
```

Verwenden Sie ein vSphere-Netzwerk, wenn Sie Netzwerkmerkmale für einen vSphere-Maschinentyp (`Cloud.vSphere.Machine`) angeben möchten.

Die vSphere-Netzwerkressource ist nur für einen `Cloud.vSphere.Machine`-Maschinentyp verfügbar.

Die vSphere-Ressource ist für die folgenden Netzwerktypeinstellungen (`networkType`) verfügbar:

- öffentlich
- privat
- vorhanden

Weitere Informationen zu Netzwerktypen finden Sie unter [Verwenden von Netzwerkeinstellungen in Netzwerkprofilen und Cloud-Vorlagen in vRealize Automation](#).

NSX-Netzwerkressource

Sie fügen ein NSX-Netzwerk mithilfe der Ressource **NSX > Netzwerk** auf der Seite **Design** der Cloud-Vorlage hinzu. Die Ressource wird im Code der Cloud-Vorlage als `Cloud.NSX.Network`-Ressourcentyp angezeigt. Die Standardressource wird wie folgt angezeigt:

```
Cloud_NSX_Network_1:
  type: Cloud.NSX.Network
  properties:
    networkType: existing
```

Verwenden Sie ein NSX-Netzwerk, wenn Sie eine Netzwerkressource an eine oder mehrere Maschinen anhängen möchten, die mit einem NSX-V- oder NSX-T-Cloud-Konto verknüpft sind. Mit der NSX-Netzwerkressource können Sie NSX-Netzwerkmerkmale für eine vSphere-Maschinenressource angeben, die mit einem NSX-V- oder NSX-T-Cloud-Konto verknüpft ist.

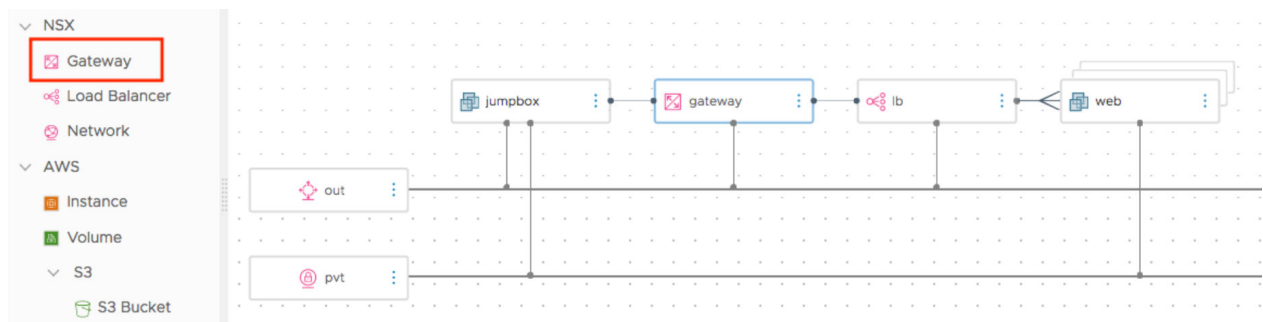
Die `Cloud.NSX.Network`-Ressource ist für die folgenden Netzwerktypeinstellungen (`networkType`) verfügbar:

- öffentlich
- privat
- ausgehend

- vorhanden
- geroutet – Geroutete Netzwerke sind nur für NSX-V und NSX-T verfügbar.

Jedes bedarfsgesteuerte NSX-T-Netzwerk erstellt einen neuen logischen Tier-1-Router. Jedes bedarfsgesteuerte NSX-V-Netzwerk erstellt eine neue Edge.

Zur Unterstützung von NAT-Regeln und der NAT-Portweiterleitung können Sie eine `Cloud.NSX.Gateway`-Cloud-Vorlagenressource hinzufügen, damit DNAT-Regeln für das Gateway bzw. den Router angegeben werden können, der mit einem ausgehenden NSX-V- oder NSX-T-Netzwerk verbunden ist. Das Gateway muss mit einem einzelnen ausgehenden Netzwerk verbunden sein und kann mit mehreren Maschinen oder Lastausgleichsdiensten verbunden werden, die mit demselben ausgehenden Netzwerk verbunden sind. Die innerhalb des Gateways angegebenen DNAT-Regeln verweisen auf diese Maschinen oder Lastausgleichsdienste als Ziel. Für geclusterte Maschinen können keine NAT-Regeln angegeben werden. Sie können aber als Tag-2-Vorgang für einzelne Maschinen innerhalb des Clusters angegeben werden.



Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen.

Optionen für externe IPAM-Integrationen

Informationen zu den Eigenschaften, die zur Verwendung mit Infoblox-IPAM-Integrationen in den Cloud-Vorlagen-Designs und Bereitstellungen zur Verfügung stehen, finden Sie unter [Verwenden Infoblox-spezifischer Eigenschaften und erweiterbarer Attribute für IPAM-Integrationen in vRealize Automation](#).

Verfügbare Tag-2-Vorgänge

Eine Liste allgemeiner Tag-2-Vorgänge, die für Cloud-Vorlagen- und Bereitstellungsressourcen verfügbar sind, finden Sie unter [Welche Aktionen kann ich auf vRealize Automation Cloud Assembly-Bereitstellungen ausführen?](#).

Ein Beispiel dafür, wie Sie von einem Netzwerk zu einem anderen wechseln, finden Sie unter [Vorgehensweise zum Verschieben einer bereitgestellten Maschine in ein anderes Netzwerk](#).

Weitere Informationen

Weitere Informationen zum Definieren von Netzwerkressourcen finden Sie unter [Netzwerkressourcen in vRealize Automation](#).

Weitere Informationen zum Definieren von Netzwerkprofilen finden Sie unter [Weitere Informationen zu Netzwerkprofilen in vRealize Automation](#).

Beispiele für Cloud-Vorlagen-Designs zur Veranschaulichung von Beispielnetzwerkressourcen und -einstellungen finden Sie unter [Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen](#).

Verwenden einer Sicherheitsgruppenressource in einer vRealize Automation-Cloud-Vorlage

Verwenden Sie beim Erstellen oder Bearbeiten Ihrer vRealize Automation-Cloud-Vorlage die für Ihre Zwecke am besten geeigneten Sicherheitsgruppenressourcen. Erfahren Sie mehr über die Sicherheitsgruppenoptionen, die in der Cloud-Vorlage verfügbar sind.

Cloud-unabhängige Sicherheitsgruppenressource

Zurzeit ist nur ein Typ von Sicherheitsgruppenressourcen vorhanden. Sie fügen eine Sicherheitsgruppenressource mithilfe der Ressource **Cloud-unabhängig > Sicherheitsgruppe** auf der Seite „Design“ der Cloud-Vorlage hinzu. Die Ressource wird im Code der Cloud-Vorlage als `Cloud.SecurityGroup`-Ressourcentyp angezeigt. Die Standardressource wird wie folgt angezeigt:

```
Cloud_SecurityGroup_1:
  type: Cloud.SecurityGroup
  properties:
    constraints: []
    securityGroupType: existing
```

Sie geben eine Sicherheitsgruppenressource im Cloud-Vorlagen-Design entweder als vorhanden (`securityGroupType: existing`) oder als bedarfsgesteuert (`securityGroupType: new`) an.

Sie können dem Cloud-Vorlagen-Design eine vorhandene Sicherheitsgruppe direkt hinzufügen. Alternativ können Sie eine vorhandene Sicherheitsgruppe verwenden, die einem Netzwerkprofil hinzugefügt wurde. Vorhandene Sicherheitsgruppen werden für verschiedene Cloud-Kontotypen unterstützt.

Für NSX-V und NSX-T können Sie eine vorhandene Sicherheitsgruppe hinzufügen oder eine neue Sicherheitsgruppe definieren, während Sie die Cloud-Vorlage entwerfen oder ändern. Bedarfsgesteuerte Sicherheitsgruppen werden nur für NSX-T und NSX-V unterstützt.

Für alle Cloud-Kontotypen außer Microsoft Azure können Sie eine oder mehrere Sicherheitsgruppen einer Netzwerkkarte der Maschine zuordnen. Eine Netzwerkkarte einer virtuellen Microsoft Azure-Maschine (*machineName*) kann nur einer Sicherheitsgruppe zugeordnet werden.

Standardmäßig ist die Sicherheitsgruppeneigenschaft `securityGroupType` auf `existing` festgelegt. Um eine bedarfsgesteuerte Sicherheitsgruppe zu erstellen, geben Sie `new` für die Eigenschaft `securityGroupType` ein. Verwenden Sie zum Angeben von Firewallregeln für eine bedarfsgesteuerte Sicherheitsgruppe die Eigenschaft `rules` im Abschnitt `Cloud.SecurityGroup` der Sicherheitsgruppenressource.

Vorhandene Sicherheitsgruppen

Vorhandene Sicherheitsgruppen werden in einer Cloud-Konto-Quellressource wie NSX-T oder Amazon Web Services erstellt. Es handelt sich um Daten, die von vRealize Automation aus der Quelle erfasst werden. Sie können eine vorhandene Sicherheitsgruppe aus einer Gruppe verfügbarer Ressourcen als Teil eines vRealize Automation-Netzwerkprofils auswählen. In Cloud-Vorlagen-Design können Sie eine vorhandene Sicherheitsgruppe grundsätzlich über ihre Mitgliedschaft in einem angegebenen Netzwerkprofil oder speziell mit einem Namen angeben, indem Sie die Einstellung `securityGroupType: existing` in einer Sicherheitsgruppenressource verwenden. Wenn Sie einem Netzwerkprofil eine Sicherheitsgruppe hinzufügen, fügen Sie dem Netzwerkprofil mindestens ein Funktions-Tag hinzu. Bedarfsgesteuerte Sicherheitsgruppenressourcen erfordern bei Verwendung im Cloud-Vorlagen-Design ein Einschränkungs-Tag.

Sie können einer oder mehreren Maschinenressourcen eine Sicherheitsgruppenressource im Cloud-Vorlagen-Design zuordnen.

Hinweis Wenn Sie beabsichtigen, eine Maschinenressource im Cloud-Vorlagen-Design zu verwenden, um eine Netzwerkkarte für eine virtuelle Microsoft Azure-Maschine (*machineName*) bereitzustellen, sollten Sie die Maschinenressource nur mit einer einzelnen Sicherheitsgruppe verknüpfen.

Bedarfsgesteuerte NSX-V- und NSX-T-Sicherheitsgruppen

Sie können bedarfsgesteuerte Sicherheitsgruppen festlegen, während Sie ein Cloud-Vorlagen-Design mithilfe der Einstellung `securityGroupType: new` im Code der Sicherheitsgruppenressource definieren oder ändern.

Sie können eine bedarfsgesteuerte NSX-V- oder NSX-T-Sicherheitsgruppe verwenden, um einen spezifischen Satz von Firewallregeln auf eine Maschinenressource im Netzwerk oder einen Satz gruppierter Ressourcen anzuwenden. Jede Sicherheitsgruppe kann mehrere benannte Firewallregeln enthalten. Sie können eine bedarfsgesteuerte Sicherheitsgruppe verwenden, um Dienste oder Protokolle und Ports anzugeben. Beachten Sie, dass Sie entweder einen Dienst oder ein Protokoll angeben können. Sie können zusätzlich zu einem Protokoll einen Port angeben. Sie können keinen Port festlegen, wenn Sie einen Dienst angeben. Wenn die Regel weder einen Dienst noch ein Protokoll enthält, wird „Beliebig“ als Standardwert für den Dienst verwendet.

Sie können auch IP-Adressen und IP-Bereiche in Firewallregeln angeben. Einige Beispiele für Firewallregeln werden in [Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen](#) gezeigt.

Wenn Sie Firewallregeln in einer NSX-V- oder einer bedarfsgesteuerten NSX-T Sicherheitsgruppe erstellen, wird standardmäßig der angegebene Netzwerkdatenverkehr, aber auch anderer Netzwerkdatenverkehr zugelassen. Um den Netzwerkdatenverkehr zu steuern, müssen Sie für jede Regel einen Zugriffstyp angeben. Die Regelzugriffstypen sind:

- Zulassen (Standard): lässt den Netzwerkdatenverkehr zu, der in dieser Firewallregel angegeben ist.

- **Verweigern:** blockiert den Netzwerkdatenverkehr, der in dieser Firewallregel angegeben ist. Gibt dem Client aktiv an, dass die Verbindung abgelehnt wird.
- **Verwerfen:** Lehnt den Netzwerkdatenverkehr ab, der in dieser Firewallregel angegeben ist. Verwirft das Paket im Hintergrund, als wäre der Listener nicht online.

Ein Beispiel für ein Design, das eine `access: Allow`- und eine `access: Deny`-Firewallregel verwendet, finden Sie unter [Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen](#).

Hinweis Ein Cloud-Administrator kann ein Cloud-Vorlage-Design mit nur einer bedarfsgesteuerten NSX-Sicherheitsgruppe erstellen und dieses Design bereitstellen, um eine wiederverwendbare vorhandene Sicherheitsgruppenressource anzulegen, die von Mitgliedern der Organisation als vorhandene Sicherheitsgruppe zu Netzwerkprofilen und Cloud-Vorlagen-Designs hinzugefügt werden kann.

Firewallregeln unterstützen CIDR-Werte für IP-Quell- und -Zieladressen sowohl im IPv4- als auch im IPv6-Format. Ein Beispieldesign, das IPv6-CIDR-Werte in einer Firewallregel verwendet, finden Sie unter [Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen](#).

Verwenden von App-Isolierungsrichtlinien in Firewallregeln der bedarfsgesteuerten Sicherheitsgruppe

Sie können eine App-Isolierungsrichtlinie verwenden, um nur internen Datenverkehr zwischen den Ressourcen zuzulassen, die von der Cloud-Vorlage bereitgestellt werden. Mit App-Isolierung können die von der Cloud-Vorlage bereitgestellten Maschinen zwar miteinander kommunizieren, aber keine Verbindung außerhalb der Firewall herstellen. Sie können eine App-Isolierungsrichtlinie im Netzwerkprofil erstellen. Sie können App-Isolierung auch in einem Cloud-Vorlagen-Design angeben, indem Sie eine bedarfsgesteuerte Sicherheitsgruppe mit einer Firewallregel vom Typ „Verweigern“ oder ein privates oder ausgehendes Netzwerk verwenden.

Eine App-Isolierungsrichtlinie wird mit einem niedrigeren Vorrang erstellt. Wenn Sie mehrere Richtlinien anwenden, werden die Richtlinien mit der höheren Gewichtung vorrangig behandelt.

Wenn Sie eine App-Isolierungsrichtlinie erstellen, wird der Richtlinie ein automatisch generierter Richtlinienname zugewiesen. Die Richtlinie wird auch für die Wiederverwendung in anderen Cloud-Vorlagen-Designs und Design-Iterationen für den zugehörigen Ressourcen-Endpoint und das Projekt zur Verfügung gestellt. Der Name der App-Isolierungsrichtlinie ist im Code des Cloud-Vorlagen-Designs nicht sichtbar, wird aber nach der Bereitstellung des Cloud-Vorlagen-Designs als benutzerdefinierte Eigenschaft auf der Projektseite angezeigt (**Infrastruktur > Verwaltung > Projekte**).

Für denselben verknüpften Endpoint in einem Projekt kann jede Bereitstellung, die eine bedarfsgesteuerte Sicherheitsgruppe für die App-Isolierung benötigt, dieselbe App-Isolierungsrichtlinie verwenden. Sobald die Richtlinie erstellt wurde, wird sie nicht mehr gelöscht. Wenn Sie eine App-Isolierungsrichtlinie angeben, sucht vRealize Automation nach der Richtlinie

innerhalb des Projekts und in Bezug auf den zugehörigen Endpoint. Wird die Richtlinie gefunden, wird sie erneut verwendet, andernfalls wird sie erstellt. Der Name der App-Isolierungsrichtlinie ist erst nach der anfänglichen Bereitstellung in der Liste der benutzerdefinierten Eigenschaften des Projekts sichtbar.

Verwenden von Sicherheitsgruppen bei der iterativen Entwicklung von Cloud-Vorlagen

Wenn Sie Sicherheitsgruppeneinschränkungen während der iterativen Entwicklung ändern und die Sicherheitsgruppe nicht mit einer Maschine in der Cloud-Vorlage verknüpft ist, wird die Sicherheitsgruppe in der Iteration wie angegeben aktualisiert. Wenn die Sicherheitsgruppe aber bereits mit einer Maschine verknüpft ist, schlägt die erneute Bereitstellung fehl. Während der iterativen Bereitstellung von Cloud-Vorlagen müssen Sie vorhandene Sicherheitsgruppen und/oder `securityGroupType`-Ressourceneigenschaften von verknüpften Maschinen trennen und zwischen jeder erneuten Bereitstellung neu verknüpfen. Der erforderliche Workflow lautet wie folgt, vorausgesetzt, die Cloud-Vorlage wurde zuerst bereitgestellt:

- 1 Trennen Sie im Cloud Assembly-Vorlagendesigner die Sicherheitsgruppe von allen verknüpften Maschinen in der Cloud-Vorlage.
- 2 Stellen Sie die Vorlagen erneut bereit, indem Sie auf **Vorhandene Bereitstellung aktualisieren** klicken.
- 3 Entfernen Sie die Einschränkungs-Tags der vorhandenen Sicherheitsgruppe und/oder `securityGroupType`-Eigenschaften in der Vorlage.
- 4 Fügen Sie der Vorlage Einschränkungs-Tags der neuen Sicherheitsgruppe und/oder `securityGroupType`-Eigenschaften hinzu.
- 5 Verknüpfen Sie die Einschränkungs-Tags der neuen Sicherheitsgruppe und/oder Instanzen der `securityGroupType`-Eigenschaft mit den Maschinen in der Vorlage.
- 6 Stellen Sie die Vorlagen erneut bereit, indem Sie auf **Vorhandene Bereitstellung aktualisieren** klicken.

Verfügbare Tag-2-Vorgänge

Eine Liste allgemeiner Tag-2-Vorgänge, die für Cloud-Vorlagen- und Bereitstellungsressourcen verfügbar sind, finden Sie unter [Welche Aktionen kann ich auf vRealize Automation Cloud Assembly-Bereitstellungen ausführen?](#).

Weitere Informationen

Weitere Informationen zur Verwendung einer Sicherheitsgruppe für die Netzwerkisolierung finden Sie unter [Sicherheitsressourcen in vRealize Automation](#).

Informationen zur Verwendung von Sicherheitsgruppeneinstellungen in einem Netzwerkprofil finden Sie unter [Weitere Informationen zu Netzwerkprofilen in vRealize Automation](#) und [Verwenden von Sicherheitsgruppeneinstellungen in Netzwerkprofilen und Cloud-Vorlagendesigns in vRealize Automation Cloud Assembly](#).

Beispiele für Cloud-Vorlagen-Designs zur Veranschaulichung von Beispielsicherheitsressourcen und -einstellungen finden Sie unter [Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen](#).

Verwenden einer Lastausgleichsdienstressource in einer vRealize Automation-Cloud-Vorlage

Verwenden Sie beim Erstellen oder Bearbeiten Ihrer vRealize Automation-Cloud-Vorlagen die für Ihre Zwecke am besten geeigneten Lastausgleichsdienstressourcen.

Sie können NSX- und Cloud-unabhängige Lastausgleichsdienstressourcen in einer Cloud-Vorlage verwenden, um den Lastausgleich in einer Bereitstellung zu steuern.

Der Cloud-unabhängige Lastausgleichsdienst kann über mehrere Clouds hinweg bereitgestellt werden. Ein Cloud-spezifischer Lastausgleichsdienst kann erweiterte Einstellungen und Funktionen angeben, die nur für eine bestimmte Cloud/Topologie verfügbar sind.

Cloud-spezifische Eigenschaften stehen im Ressourcentyp „NSX-Lastausgleichsdienst“

(Cloud.NSX.LoadBalancer) zur Verfügung. Wenn Sie diese Eigenschaften auf einem Cloud-unabhängigen Lastausgleichsdienst (Cloud.LoadBalancer) hinzufügen, werden sie bei Bereitstellung eines Amazon Web Services- oder Microsoft Azure-Lastausgleichsdiensts ignoriert. Die Eigenschaften werden aber berücksichtigt, wenn ein NSX-V- oder NSX-T-Lastausgleichsdienst bereitgestellt wird. Wählen Sie basierend auf den Bedingungen in Ihrer vRealize Automation-Cloud-Vorlage einen verfügbaren Ressourcentyp des Lastausgleichsdiensts aus.

Sie können eine Lastausgleichsdienstressource nicht direkt mit einer Sicherheitsgruppenressource auf der Design-Arbeitsfläche verbinden.

Cloud-unabhängige Lastausgleichsdienstressource

Verwenden Sie einen Cloud-unabhängigen Lastausgleichsdienst, wenn Sie Netzwerkeigenschaften für alle Typen von Zielmaschinen angeben möchten.

Sie fügen einen Cloud-unabhängigen Lastausgleichsdienst mithilfe der Ressource **Cloud-unabhängig > Lastausgleichsdienst** auf der Seite „Design“ der Cloud-Vorlage hinzu. Die Ressource wird im Code der Cloud-Vorlage als `Cloud.LoadBalancer`-Ressourcentyp angezeigt. Die Standardressource wird wie folgt angezeigt:

```
Cloud_LoadBalancer_1:
  type: Cloud.LoadBalancer
  properties:
    routes: []
    network: ''
    instances: []
    internetFacing: false
```


NSX-Lastausgleichsdienstressource

Verwenden Sie einen NSX-Lastausgleichsdienst, wenn die Cloud-Vorlage Eigenschaften enthält, die für NSX-V oder NSX-T spezifisch sind (entweder die Richtlinien-API- oder die Manager-API-Methode). Sie können mindestens einen Lastausgleichsdienst an ein NSX-V- oder NSX-T-Netzwerk oder an Maschinen anhängen, die mit einem NSX-V- oder NSX-T-Netzwerk verknüpft sind.

Zum Hinzufügen eines NSX-Lastausgleichsdiensts verwenden Sie die Ressource **NSX > Lastausgleichsdienst**. Die Ressource wird im Code der Cloud-Vorlage als `Cloud.NSX.LoadBalancer`-Ressourcentyp angezeigt. Die Standardressource wird wie folgt angezeigt:

```
Cloud_NSX_LoadBalancer_1:
  type: Cloud.NSX.LoadBalancer
  properties:
    routes: []
    network: ''
    instances: []
```

Optionen des Lastausgleichsdiensts im Code der Cloud-Vorlage

Durch Hinzufügen mindestens einer Lastausgleichsdienstressource zu Ihrer Cloud-Vorlage können Sie die folgenden Einstellungen angeben. Sie finden einige Beispiele hierzu unter [Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen](#).

■ Maschinenspezifikation

Sie können benannte Maschinenressourcen angeben, die an einem Lastausgleichspool teilnehmen sollen. Alternativ können Sie angeben, dass eine Netzwerkkarte (NIC) einer bestimmten Maschine am Lastausgleichspool teilnimmt.

Diese Option ist nur für die **NSX**-Lastausgleichsdienstressource (`Cloud.NSX.LoadBalancer`) verfügbar.

Diese Option ist für die Netzwerktypen `existing` und `public` verfügbar. Die On-Demand-Netzwerktypen `private`, `routed` und `outbound` werden ebenfalls unterstützt.

■ `resource.Cloud_Machine_1.id`

Gibt an, dass der Lastausgleichsdienst die im Code der Cloud-Vorlage als `Cloud_Machine_1` angegebene Maschine berücksichtigt.

■ `resource.Cloud_Machine_2.networks[2].id`

Gibt an, dass der Lastausgleichsdienst die im Code der Cloud-Vorlage als `Cloud_Machine_2` festgelegte Maschine nur dann einbezieht, wenn sie für die Maschinen-Netzwerkkarte `Cloud_Machine_2.networks[2]` bereitgestellt wird.

■ Protokollierungsebene

Mit dem Wert der Protokollierungsebene wird ein Schweregrad für das Fehlerprotokoll angegeben. Die Optionen lauten KEIN, NOTFALL, ALARM, KRITISCH, FEHLER, WARNUNG, INFO, DEBUGGEN und HINWEIS. Der Wert für die Protokollierungsebene gilt für alle Lastausgleichsdienste in der Cloud-Vorlage. Diese Option ist spezifisch für NSX. Für Lastausgleichsdienste mit einem übergeordneten Element überschreibt die Einstellung der übergeordneten Protokollierungsebene alle Einstellungen der Protokollierungsebene in den untergeordneten Elementen.

Weitere Informationen hierzu finden Sie in Themen wie etwa [Hinzufügen von Load Balancers](#) in der NSX-Produktdokumentation.

■ Typ

Verwenden Sie einen Lastausgleichsdiensttyp, um eine Skalierungsgröße anzugeben. Die Standardeinstellung ist „Klein“. Diese Option ist spezifisch für NSX. Für Lastausgleichsdienste mit einem übergeordneten Element überschreibt die Einstellung des übergeordneten Typs alle Einstellungen des Typs in den untergeordneten Elementen.

■ Klein

Korreliert mit „Kompakt“ in NSX-V und „Klein“ in NSX-T.

■ Mittel

Korreliert mit „Groß“ in NSX-V und „Mittel“ in NSX-T.

■ Groß

Korreliert mit „Quad Large“ in NSX-V und „Groß“ in NSX-T.

■ Besonders groß

Korreliert mit „Sehr groß“ in NSX-V und „Groß“ in NSX-T.

Weitere Informationen hierzu finden Sie in Themen wie etwa [Skalieren von Load Balancer-Ressourcen](#) in der Produktdokumentation zu NSX.

Diese Option ist nur für die **NSX**-Lastausgleichsdienstressource (`Cloud.NSX.LoadBalancer`) verfügbar.

■ Algorithmus (Serverpool)

Verwenden Sie eine algorithmische Ausgleichsmethode, um die Verteilung eingehender Verbindungen unter den Serverpoolmitgliedern zu steuern. Der Algorithmus kann auf einem Serverpool oder direkt auf einem Server verwendet werden. Alle Lastausgleichsalgorithmen überspringen Server, die eine der folgenden Bedingungen erfüllen:

- Der Admin-Zustand ist auf DISABLED festgelegt.
- Der Admin-Zustand ist auf GRACEFUL_DISABLED festgelegt, und ein übereinstimmender Persistenzeintrag ist nicht vorhanden.
- Der Zustand der aktiven oder passiven Integritätsprüfung lautet DOWN.

- Der Verbindungsgrenzwert für die maximale Anzahl gleichzeitiger Verbindungen des Serverpools ist erreicht.

Diese Option ist spezifisch für NSX.

- IP_HASH

Wählt einen Server auf der Basis eines Hash der Quell-IP-Adresse und der gesamten Gewichtung aller ausgeführten Server aus.

Korreliert mit IP-HASH in NSX-V und NSX-T.

- LEAST_CONNECTION

Verteilt Clientanforderungen basierend auf der Anzahl der bereits auf dem Server vorhandenen Verbindungen auf mehrere Server. Neue Verbindungen werden an den Server mit den wenigsten Verbindungen gesendet. Ignoriert die Gewichtungen der Serverpoolmitglieder, auch wenn diese konfiguriert sind.

Korreliert mit LEASTCONN in NSX-V und LEAST_CONNECTION in NSX-T.

- ROUND_ROBIN

Eingehende Clientanforderungen werden durch eine Liste verfügbarer Server geleitet, die die Anforderung verarbeiten können. Ignoriert die Gewichtungen der Serverpoolmitglieder, auch wenn sie konfiguriert sind. Standard.

Korreliert mit ROUND_ROBIN in NSX-V und NSX-T.

- WEIGHTED_LEAST_CONNECTION

Jedem Server wird ein Gewichtungswert zugewiesen, der die Leistung dieses Servers verglichen mit anderen Servern im Pool angibt. Mit diesem Wert wird die Anzahl der Clientanforderungen angegeben, die im Vergleich zu anderen Servern im Pool an einen Server gesendet werden. Dieser Lastausgleichsalgorithmus konzentriert sich darauf, die Last gleichmäßig auf die verfügbaren Serverressourcen zu verteilen. Standardmäßig beträgt der Wert für die Gewichtung 1, wenn der Wert nicht konfiguriert ist und langsamer Start aktiviert ist.

Korreliert mit WEIGHTED_LEAST_CONNECTION in NSX-T. In NSX-V ist keine Korrelation vorhanden.

- WEIGHTED_ROUND_ROBIN

Jedem Server wird ein Gewichtungswert zugewiesen, der die Leistung dieses Servers verglichen mit anderen Servern im Pool angibt. Mit diesem Wert wird die Anzahl der Clientanforderungen angegeben, die im Vergleich zu anderen Servern im Pool an einen Server gesendet werden. Dieser Lastausgleichsalgorithmus konzentriert sich darauf, die Last gleichmäßig auf die verfügbaren Serverressourcen zu verteilen.

Korreliert mit WEIGHTED_ROUND_ROBIN in NSX-T. In NSX-V ist keine Korrelation vorhanden.

- URI

Der linke Teil des URI ist mit einem Hashwert versehen und wird durch das Gesamtgewicht der ausgeführten Server dividiert. Das Ergebnis bestimmt, welcher Server die Anforderung erhält. Der URI ist immer an denselben Server gerichtet, solange kein Server aktiviert oder deaktiviert wird. Der URI-Algorithmusparameter verfügt über zwei Optionen: `uriLength=<len>` und `uriDepth=<dep>`. Der Bereich für den Längenparameter muss `1<=len<256` lauten. Der Bereich für den Tiefenparameter muss `1<=dep<10` lauten. Auf die Parameter für Länge und Tiefe folgt eine positive Ganzzahl. Mit diesen Optionen können Server nur auf der Basis des Anfangs des URI ausgeglichen werden. Der Längenparameter gibt an, dass der Algorithmus nur die definierten Zeichen am Anfang des URI zur Berechnung des Hash verwenden soll. Der Tiefenparameter legt die maximale Verzeichnistiefe zur Berechnung des Hash fest. Jeder Schrägstrich in der Anforderung wird als eine Ebene behandelt. Bei Angabe beider Parameter wird die Evaluierung beendet, wenn der Wert eines der beiden Parameter erreicht ist.

Korreliert mit URI in NSX-V. In NSX-T ist keine Korrelation vorhanden.

■ HTTPHEADER

Der Name des HTTP-Headers wird in jeder HTTP-Anforderung gesucht. Bei dem Header-Namen in Klammern wird die Groß- und Kleinschreibung nicht beachtet. Wenn der Header nicht vorhanden ist oder keinen Wert enthält, wird der Round-Robin-Algorithmus angewendet. Der HTTPHEADER-Algorithmusparameter verfügt über eine Option: `headerName=<name>`.

Korreliert mit HTTPHEADER in NSX-V. In NSX-T ist keine Korrelation vorhanden.

■ URL

Der im Argument angegebene URL-Parameter wird in der Abfragezeichenfolge jeder HTTP GET-Anforderung gesucht. Stehen nach dem Parameter ein Gleichheitszeichen (=) und ein Wert, erhält der Wert einen Hash und wird durch die gesamte Gewichtung der ausgeführten Server dividiert. Das Ergebnis bestimmt, 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. Wenn kein Wert oder kein Parameter gefunden wurde, wird ein Round-Robin-Algorithmus angewendet. Der URL-Algorithmusparameter verfügt über eine Option: `urlParam=<url>`.

Korreliert mit URL in NSX-V. In NSX-T ist keine Korrelation vorhanden.

Weitere Informationen hierzu finden Sie in Themen wie etwa [Hinzufügen eines Serverpools für das Load Balancing](#) in der NSX-Produktdokumentation.

NSX-V- und NSX-T-Netzwerke und Optionen des Lastausgleichsdiensts

Die Optionen des Lastausgleichsdiensts hängen von dem Netzwerk ab, mit dem die Lastausgleichsdienstressource in der Cloud-Vorlage verknüpft ist. Sie können einen Lastausgleichsdienst relativ zum Netzwerktyp und den Netzwerkbedingungen konfigurieren.

■ Ausgehendes bedarfsgesteuertes Netzwerk

Wenn die Berechnungen des Lastausgleichsdiensts mit einem bedarfsgesteuerten `outbound`-Netzwerk verbunden sind, wird ein Lastausgleichsdienst für den Tier-1-Router im bedarfsgesteuerten Netzwerk erstellt.

- Privates bedarfsgesteuertes Netzwerk

Wenn die Berechnungen des Lastausgleichsdiensts mit einem bedarfsgesteuerten `private`-Netzwerk verbunden sind, wird ein neuer Tier-1-Router erstellt und mit dem im Netzwerkprofil angegebenen Tier-0-Router verbunden. Der Lastausgleichsdienst wird dann an den Tier-1-Router angehängt. Die VIP-Ankündigung des Tier-1-Routers ist aktiviert, wenn sich die VIP in einem `existing`-Netzwerk befindet. Wenn ein `private`-Netzwerk für DHCP konfiguriert wird, verwenden das `private` Netzwerk und der Lastausgleichsdienst den Tier-1-Router gemeinsam.

- Vorhandenes Netzwerk

Wenn der Lastausgleichsdienst mit einem `existing`-Netzwerk verbunden ist, wird der Lastausgleichsdienst mit dem Tier-1-Router des vorhandenen Netzwerks erstellt. Ein neuer Lastausgleichsdienst wird erstellt, wenn kein Lastausgleichsdienst mit dem Tier-1-Router verbunden ist. Wenn der Lastausgleichsdienst bereits vorhanden ist, wird er mit neuen virtuellen Servern verbunden. Wenn das `existing`-Netzwerk nicht mit einem Tier-1-Router verbunden ist, wird ein neuer Tier-1-Router erstellt und an einen Tier-0-Router angehängt, der im Netzwerkprofil definiert ist. Die VIP-Ankündigung des Tier-1-Routers ist nicht aktiviert.

- Im Netzwerkprofil definierte Netzwerkisolierung

Für die Netzwerktypen `outbound` oder `private` können Sie Einstellungen für die Netzwerkisolierung in einem Netzwerkprofil angeben, um eine neue Sicherheitsgruppe zu emulieren. Da Maschinen mit einem vorhandenen Netzwerk verbunden sind und die Isolierungseinstellungen im Profil festgelegt sind, ähnelt diese Option einem Lastausgleichsdienst, der in einem vorhandenen Netzwerk erstellt wurde. Der Unterschied besteht darin, dass zum Aktivieren des Datenpfads die IP des Tier-1-Uplink-Ports zur Sicherheitsgruppe der Isolierung hinzugefügt wird.

Sie können Einstellungen des Lastausgleichsdiensts für mit NSX verknüpfte Netzwerke unter Verwendung einer NSX-Lastausgleichsdienstressource im Design der Cloud-Vorlage angeben.

Weitere Informationen finden Sie im VMware-Blogbeitrag [vRA Cloud Assembly-Lastausgleichsdienst mit NSX-T Deep Dive](#).

Neukonfigurieren der Einstellungen für die Protokollierungsebene oder den Typ, wenn mehrere Lastausgleichsdienste einen Tier-1-Router in NSX-T oder einen Edge-Router in NSX-V gemeinsam nutzen

Wenn Sie eine Cloud-Vorlage mit mehreren Lastausgleichsdiensten verwenden, die einen Tier-1-Router im NSX-T-Endpoint oder einen Edge-Router im NSX-V-Endpoint gemeinsam nutzen, werden bei einer Neukonfiguration der Einstellungen für die Protokollierungsebene oder den Typ in einem der Lastausgleichsdienstressourcen die Einstellungen für die anderen Lastausgleichsdienste nicht aktualisiert. Nicht übereinstimmende Einstellungen verursachen

Inkonsistenzen in NSX. Um Inkonsistenzen bei der Neukonfiguration dieser Einstellungen für die Protokollierungsebene und/oder den Typ zu vermeiden, verwenden Sie dieselben Neukonfigurationswerte für alle Lastausgleichsdienstressourcen in der Cloud-Vorlage, die in ihrem zugeordneten NSX-Endpoint einen Tier-1- oder Edge-Router gemeinsam nutzen.

Verfügbare Tag-2-Vorgänge

Wenn Sie eine Bereitstellung mit einem Lastausgleichsdienst horizontal herunter- oder hochskalieren, wird der Lastausgleichsdienst so konfiguriert, dass neu hinzugefügte Maschinen aufgenommen bzw. Lastausgleichsmaschinen, die entfernt werden sollen, angehalten werden.

Eine Liste allgemeiner Tag-2-Vorgänge, die für Cloud-Vorlagen und Bereitstellungen verfügbar sind, finden Sie unter [Welche Aktionen kann ich auf vRealize Automation Cloud Assembly-Bereitstellungen ausführen?](#).

Weitere Informationen

Informationen zum Definieren der Einstellungen für den Lastausgleichsdienst in einem Netzwerkprofil finden Sie unter [Weitere Informationen zu Netzwerkprofilen in vRealize Automation](#).

Beispiele für Cloud-Vorlagen-Designs, die Lastausgleichsdienste enthalten, finden Sie unter [Beispiele für Netzwerke, Sicherheit und Lastausgleichsdienste in vRealize Automation-Cloud-Vorlagen](#).

Puppet-fähige Cloud-Vorlage mit Zugriff auf Benutzernamen und Kennwort

In diesem Beispiel fügen Sie Puppet-Konfigurationsverwaltung zu einer Cloud-Vorlage hinzu, die auf einer vCenter-Computing-Ressource mit Zugriff auf Benutzernamen und Kennwort bereitgestellt wird.

Dieses Verfahren zeigt ein Beispiel dafür, wie Sie eine Puppet-fähige einsetzbare Ressource erstellen können, die eine Authentifizierung von Benutzernamen und Kennwort erfordert. Der Zugriff auf Benutzernamen und Kennwort bedeutet, dass sich der Benutzer manuell von der Computing-Ressource bei der primären Puppet-Maschine anmelden muss, um die Verwaltung der Puppet-Konfiguration aufzurufen.

Optional können Sie RAS-Authentifizierung konfigurieren, die die Konfigurationsverwaltung in einer Cloud-Vorlage einrichtet, sodass die Computing-Ressource die Authentifizierung mit der primären Puppet-Maschine verarbeitet. Wenn der Remotezugriff aktiviert ist, generiert die Computing-Ressource automatisch einen Schlüssel für die Kennwortauthentifizierung. Ein gültiger Benutzernamen ist weiterhin erforderlich.

Weitere Beispiele dafür, wie Sie verschiedene Puppet-Szenarien in vRealize Automation Cloud Assembly-Blueprints konfigurieren können, finden Sie unter [Cloud-Vorlagenbeispiele für die Puppet-Konfigurationsverwaltung in AWS](#) und [Beispiele für Cloud-Vorlagen für die vCenter Puppet-Konfiguration](#).

Voraussetzungen

- Richten Sie eine Puppet Enterprise-Instanz in einem gültigen Netzwerk ein.
- Fügen Sie mithilfe der Integrations-Funktion Ihre Puppet Enterprise-Instanz vRealize Automation Cloud Assembly hinzu. Weitere Informationen finden Sie unter [Konfigurieren der Puppet Enterprise-Integration in vRealize Automation Cloud Assembly](#).
- Richten Sie ein vSphere-Konto und eine vCenter-Computing-Ressource ein.

Verfahren

- 1 Fügen Sie eine Verwaltungskomponente für die Puppet-Konfiguration zu einer vSphere-Computing-Ressource auf der Arbeitsfläche für die gewünschte Cloud-Vorlage hinzu.
 - a Wählen Sie **Infrastruktur > Verwalten > Integrationen** aus.
 - b Klicken Sie auf **Integration hinzufügen** und wählen Sie „Puppet“ aus.
 - c Geben Sie auf der Seite „Puppet-Konfiguration“ die entsprechenden Informationen ein.

Konfiguration	Beschreibung	Beispielwert
Hostname	Der Hostname oder die IP-Adresse der primären Puppet-Maschine.	Puppet-Ubuntu
SSH-Port	SSH-Port für die Kommunikation zwischen vRealize Automation Cloud Assembly und der primären Puppet-Maschine. (Optional)	–
Geheimer Schlüssel für automatische Signierung	Der auf der primären Puppet-Maschine konfigurierte gemeinsame geheime Schlüssel, der von Knoten zur Unterstützung von Zertifikatsanforderungen für automatische Signierung bereitgestellt werden soll.	Benutzerspezifisch
Speicherort	Geben Sie an, ob sich die primäre Puppet-Maschine in einer Private Cloud oder Public Cloud befindet. Hinweis Die cloud-übergreifende Bereitstellung wird nur unterstützt, wenn eine Verbindung zwischen der Computing-Ressource der Bereitstellung und der primären Puppet-Maschine besteht.	
Cloud proxy	Nicht erforderlich für Public Cloud-Konten, wie zum Beispiel Microsoft Azure oder Amazon Web Services. Wenn Sie ein vCenter-basiertes Cloud-Konto verwenden, wählen Sie den entsprechenden cloud proxy für Ihr Konto aus.	–
Benutzername	SSH- und RBAC-Benutzername für primäre Puppet-Maschine.	Benutzerspezifisch. YAML-Wert ist '\$ {input.username}'
Kennwort	SSH- und RBAC-Kennwort für primäre Puppet-Maschine.	Der benutzerspezifische YAML-Wert ist '\$ {input.password}'
Sudo-Befehle für diesen Benutzer verwenden	Wählen Sie diese Option aus, um sudo-Befehle für procidd zu verwenden.	true

Konfiguration	Beschreibung	Beispielwert
Name	Name der primären Puppet-Maschine	PEMasterOnPrem
Beschreibung		

- 2 Fügen Sie die Eigenschaften für Benutzername und Kennwort zur Puppet-YAML hinzu, wie im folgenden Beispiel gezeigt.
- 3 Stellen Sie sicher, dass der Wert für die RAS-Eigenschaft der Puppet-Cloud-Vorlagen-YAML auf `authentication: username and password` festgelegt ist, wie im folgenden Beispiel gezeigt.

Beispiel: YAML-Code für vCenter-Benutzername und -Kennwort

Das folgende Beispiel zeigt den repräsentativen YAML-Code für das Hinzufügen der Benutzernamen- und Kennwortauthentifizierung für eine vCenter-Computing-Ressource.

```
inputs:
  username:
    type: string
    title: Username
    description: Username to use to install Puppet agent
    default: puppet
  password:
    type: string
    title: Password
    default: VMware@123
    encrypted: true
    description: Password for the given username to install Puppet agent
resources:
  Puppet-Ubuntu:
    type: Cloud.vSphere.Machine
    properties:
      flavor: small
      imageRef: >-
        https://cloud-images.ubuntu.com/releases/16.04/release-20170307/ubuntu-16.04-server-
cloudimg-amd64.ova
      remoteAccess:
        authentication: usernamePassword
        username: '${input.username}'
        password: '${input.password}'
  Puppet_Agent:
    type: Cloud.Puppet
    properties:
      provider: PEMasterOnPrem
      environment: production
      role: 'role::linux_webserver'
      username: '${input.username}'
      password: '${input.password}'
      host: '${Puppet-Ubuntu.*}'
      useSudo: true
      agentConfiguration:
        certName: '${Puppet-Ubuntu.address}'
```

Cloud-Vorlagenbeispiele für die Puppet-Konfigurationsverwaltung in AWS

Es gibt mehrere Optionen zum Konfigurieren von Cloud-Vorlagen zur Unterstützung der Puppet-basierten Konfigurationsverwaltung auf AWS-Computing-Ressourcen.

Puppet-Verwaltung in AWS mit Benutzername und Kennwort

Beispiel für...	Beispiel einer Blueprint-YAML
<p>Authentifizierung der Cloud-Konfiguration auf einem beliebigen unterstützten Amazon-Maschinen-Image.</p>	<pre> inputs: username: type: string title: Username default: puppet password: type: string title: Password encrypted: true default: VMware@123 resources: Webserver: type: Cloud.AWS.EC2.Instance properties: flavor: small image: centos cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' ssh-authorized-keys: - ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDytVL+Q6/+vGbmKXoRpX dmettem@dmettem-m01.vmware.com runcmd: - echo "Defaults:\${input.username} !requiretty" >> /etc/sudoers.d/\${input.username} Puppet_Agent: type: Cloud.Puppet properties: provider: PEOonAWS environment: production role: 'role::linux_webserver' host: '\${Webserver.*}' osType: linux username: '\${input.username}' password: '\${input.password}' useSudo: true </pre>
<p>Authentifizierung der Cloud-Konfiguration auf einem benutzerdefinierten Amazon-Maschinen-Image mit einem vorhandenen Benutzer.</p>	<pre> inputs: username: type: string title: Username default: puppet password: type: string title: Password encrypted: true default: VMware@123 </pre>

Beispiel für...	Beispiel einer Blueprint-YAML
	<pre> resources: Webserver: type: Cloud.AWS.EC2.Instance properties: flavor: small image: centos cloudConfig: #cloud-config runcmd: - sudo sed -e 's/.*PasswordAuthentication no.*/ PasswordAuthentication yes/' -i /etc/ssh/sshd_config - sudo service sshd restart Puppet_Agent: type: Cloud.Puppet properties: provider: PEOAWS environment: production role: 'role::linux_webserver' host: '\${Webserver.*}' osType: linux username: '\${input.username}' password: '\${input.password}' useSudo: true </pre>

Puppet-Verwaltung in AWS mit erzeugtem PublicPrivateKey

Beispiel für...	Beispiel einer Blueprint-YAML
remoteAccess.authentication- Authentifizierung in AWS mit generatedPublicPrivateKey- Zugriff	<pre> inputs: {} resources: Machine: type: Cloud.AWS.EC2.Instance properties: flavor: small imageRef: ami-a4dc46db remoteAccess: authentication: generatedPublicPrivateKey Puppet_Agent: type: Cloud.Puppet properties: provider: puppet-BlueprintProvisioningITSuite environment: production role: 'role::linux_webserver' host: '\${Machine.*}' osType: linux username: ubuntu useSudo: true agentConfiguration: runInterval: 15m certName: '\${Machine.address}' useSudo: true </pre>

Beispiele für Cloud-Vorlagen für die vCenter Puppet-Konfiguration

Es gibt mehrere Optionen zum Konfigurieren von Cloud-Vorlagen zur Unterstützung der Puppet-basierten Konfigurationsverwaltung auf vCenter-Computing-Ressourcen.

Puppet auf vSphere mit Benutzernamen- und Kennwortauthentifizierung.

Das folgende Beispiel zeigt den YAML-Code für Puppet auf einer vSphere-OVA mit Benutzernamen- und Kennwortauthentifizierung.

Tabelle 6-5.

Beispiel für...	Beispiel einer Blueprint-YAML
<p>YAML-Code für Puppet auf einer vSphere-OVA mit Benutzernamen- und Kennwortauthentifizierung.</p>	<pre> inputs: username: type: string title: Username default: puppet password: type: string title: Password encrypted: true default: VMware@123 resources: Puppet_Agent: type: Cloud.Puppet properties: provider: PEonAWS environment: dev role: 'role::linux_webserver' username: '\${input.username}' password: '\${input.password}' useSudo: true host: '\${Webserver.*}' osType: linux agentConfiguration: runInterval: 15m certName: '\${Machine.address}' Webserver: type: Cloud.vSphere.Machine properties: cpuCount: 1 totalMemoryMB: 1024 imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' ssh-authorized-keys: - ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAQDytVL+Q6+vGbmKXoRpX dmettem@dmettem-m01.vmware.com runcmd: - echo "Defaults:\${input.username} </pre>
<p>YAML-Code für Puppet auf einer vSphere-OVA mit Benutzernamen- und Kennwortauthentifizierung auf der Computing-Ressource.</p>	<pre> inputs: username: type: string title: Username default: puppet </pre>

Tabelle 6-5. (Fortsetzung)

Beispiel für...	Beispiel einer Blueprint-YAML
YAML-Code für Puppet auf einem vCenter mit aktiviertem RAS-Authentifizierungskennwort für die Computing-Ressource.	<pre> password: type: string title: Password encrypted: true default: VMware@123 resources: Puppet_Agent: type: Cloud.Puppet properties: provider: PEonAWS environment: dev role: 'role::linux_webserver' username: '\${input.username}' password: '\${input.password}' useSudo: true host: '\${Webserver.*}' osType: linux agentConfiguration: runInterval: 15m certName: '\${Machine.address}' Webserver: type: Cloud.vSphere.Machine properties: cpuCount: 1 totalMemoryMB: 1024 imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' ssh-authorized-keys: - ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDytVL+Q6+vGbmKXoRpX dmettem@dmettem-m01.vmware.com runcmd: - echo "Defaults:\${input.username} </pre>
	<pre> inputs: username: type: string title: Username description: Username to use to install Puppet agent default: puppet password: type: string title: Password default: VMware@123 encrypted: true </pre>

Tabelle 6-5. (Fortsetzung)

Beispiel für...	Beispiel einer Blueprint-YAML
	<pre> description: Password for the given username to install Puppet agent resources: Puppet-Ubuntu: type: Cloud.vSphere.Machine properties: flavor: small imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova remoteAccess: authentication: usernamePassword username: '\${input.username}' password: '\${input.password}' Puppet_Agent: type: Cloud.Puppet properties: provider: PEMasterOnPrem environment: production role: 'role::linux_webserver' username: '\${input.username}' password: '\${input.password}' host: '\${Puppet-Ubuntu.*}' useSudo: true agentConfiguration: certName: '\${Puppet-Ubuntu.address}' </pre>

Puppet auf vSphere mit generierter PublicPrivateKey-Authentifizierung

Tabelle 6-6.

Beispiel für...	Beispiel einer Blueprint-YAML
YAML-Code für Puppet auf einer vSphere-OVA mit generierter PublicPrivateKey-Authentifizierung auf der Computing-Ressource.	<pre> inputs: {} resources: Machine: type: Cloud.vSphere.Machine properties: flavor: small imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova remoteAccess: authentication: generatedPublicPrivateKey Puppet_Agent: type: Cloud.Puppet properties: provider: puppet-BlueprintProvisioningITSuite environment: production role: 'role::linux_webserver' host: '\${Machine.*}' osType: linux username: ubuntu useSudo: true agentConfiguration: runInterval: 15m certName: '\${Machine.address}' - echo "Defaults:\${input.username}" </pre>

Vorgehensweise zum Integrieren von Terraform-Konfigurationen in vRealize Automation Cloud Assembly

Sie können Terraform-Konfigurationen als Ressource in Ihren Cloud-Vorlagen in vRealize Automation Cloud Assembly einbetten.

Vorbereiten einer Terraform-Laufzeitumgebung für vRealize Automation Cloud Assembly

Entwürfe, die Terraform-Konfigurationen enthalten, benötigen Zugriff auf eine Terraform-Laufzeitumgebung, die Sie in das lokale vRealize Automation Cloud Assembly-Produkt integrieren.

Vorgehensweise zum Hinzufügen einer Laufzeit

Die Laufzeitumgebung besteht aus einem Kubernetes-Cluster, der Terraform-CLI-Befehle zur Durchführung angeforderter Vorgänge ausführt. Darüber hinaus erfasst die Laufzeit Protokolle und gibt die Ergebnisse der Terraform-CLI-Befehle zurück.

Im lokalen vRealize Automation-Produkt müssen Benutzer ihren eigenen Terraform-Laufzeit-Kubernetes-Cluster konfigurieren. Nur eine Terraform-Laufzeit pro Organisation wird unterstützt. Alle Terraform-Bereitstellungen für diese Organisation verwenden dieselbe Laufzeit.

- 1 Stellen Sie sicher, dass Sie über einen Kubernetes-Cluster verfügen, auf dem die Terraform-CLI ausgeführt werden soll.
 - Alle Benutzer können eine kubeconfig-Datei bereitstellen, um die Terraform-CLI auf einem nicht verwalteten Kubernetes-Cluster auszuführen.
 - Enterprise-Lizenzbenutzer können die Terraform-CLI auf einem von vRealize Automation verwalteten Kubernetes-Cluster ausführen.

Gehen Sie in vRealize Automation Cloud Assembly zu **Infrastruktur > Ressourcen > Kubernetes** und stellen Sie sicher, dass Sie über einen Kubernetes-Cluster verfügen. Weitere Informationen zum Hinzufügen eines Kubernetes-Clusters finden Sie unter [Vorgehensweise zum Arbeiten mit Kubernetes in vRealize Automation Cloud Assembly](#).

- 2 Wenn der Kubernetes-Cluster neu hinzugefügt oder geändert wurde, warten Sie, bis die zugehörige Datenerfassung abgeschlossen ist.

Die Datenerfassung ruft die Liste der Namespaces und andere Informationen ab, was je nach Anbieter bis zu 5 Minuten dauern kann.

- 3 Nachdem die Datenerfassung abgeschlossen ist gehen Sie zu **Infrastruktur > Integrationen > Integration hinzufügen** und wählen Sie die Karte **Terraform-Laufzeit** aus.
- 4 Geben Sie Einstellungen ein.

Abbildung 6-3. Beispiel einer Terraform-Laufzeitintegration

New Integration

Name *

Description

Terraform Runtime Integration

Kubernetes cluster *

Kubernetes namespace *

Runtime Container Settings

Image ⓘ

CPU request (Millicores)

CPU limit (Millicores)

Memory request (MB)

Memory limit (MB)

Einstellung	Beschreibung
Name	Geben Sie der Laufzeitintegration einen eindeutigen Namen.
Beschreibung	Erläutern Sie den Zweck der Integration.
Terraform-Laufzeitintegration:	
Laufzeittyp (nur Enterprise)	Enterprise-Lizenzbenutzer können angeben, ob die Terraform-CLI auf einem von vRealize Automation verwalteten Kubernetes-Cluster oder auf einem nicht verwalteten Cluster ausgeführt werden soll.
Kubernetes-kubeconfig (alle Benutzer)	<p>Fügen Sie in einem nicht verwalteten Kubernetes-Cluster den gesamten Inhalt der kubeconfig-Datei für den externen Cluster ein.</p> <p>Informationen zum Verwenden einer externen Kubernetes-Laufzeit mit einem Proxy-Server finden Sie unter Vorgehensweise zum Hinzufügen von Proxy-Unterstützung. Diese Option ist für alle Benutzer verfügbar.</p>

Einstellung	Beschreibung
Kubernetes-Cluster (nur Enterprise)	<p>Für Kubernetes, das von vRealize Automation verwaltet wird, wählen Sie den Cluster aus, in dem die Terraform-CLI ausgeführt werden soll.</p> <p>Der Cluster und die zugehörige kubeconfig-Datei müssen erreichbar sein. Sie können den Zugriff auf kubeconfig mit einem GET in <code>/cmx/api/resources/k8s/clusters/{clusterId}/kube-config</code> validieren.</p> <p>Diese Option ist nur für Enterprise-Lizenzen verfügbar.</p>
Kubernetes-Namespace	Wählen Sie den Namespace aus, der im Cluster verwendet werden soll, um Pods zu erstellen, auf denen die Terraform-CLI ausgeführt wird.
Einstellungen für Laufzeit-Container:	
Image	<p>Geben Sie den Pfad zum Container-Image der Terraform-Version ein, die ausgeführt werden soll.</p> <hr/> <p>Hinweis Mit der Schaltfläche VALIDIEREN wird das Container-Image nicht geprüft.</p>
CPU-Anforderung	Geben Sie die CPU-Menge für die Ausführung von Containern ein. Der Standardwert beträgt 250 Millicore.
CPU-Grenzwert	Geben Sie die maximal zulässige CPU für die Ausführung von Containern ein. Der Standardwert beträgt 250 Millicore.
Arbeitsspeichieranforderung	Geben Sie die Menge des Arbeitsspeichers für die Ausführung von Containern ein. Der Standard ist 512 MB.
Arbeitsspeichergrenzwert	Geben Sie den maximal zulässigen Arbeitsspeicher für die Ausführung von Containern ein. Der Standard ist 512 MB.

5 Klicken Sie auf **VALIDIEREN** ändern Sie die Einstellungen nach Bedarf.

6 Klicken Sie auf **HINZUFÜGEN**.

Die Einstellungen werden zwischengespeichert. Nach dem Hinzufügen der Integration können Sie Einstellungen wie den Cluster oder Namespace ändern. Es kann jedoch bis zu 5 Minuten dauern, bis eine Änderung erkannt und die Terraform-CLI mit den neuen Einstellungen ausgeführt wird.

Fehlerbehebung bei der Terraform-Laufzeit

Einige Probleme bei der Bereitstellung von Terraform-Konfigurationen hängen möglicherweise mit der Laufzeitintegration zusammen.

Problem	Ursache	Lösung
Die Validierung schlägt mit einer Fehlermeldung fehl, die besagt, dass der Namespace ungültig ist.	Sie haben den Cluster geändert, aber den vorherigen Namespace in der Benutzeroberfläche belassen.	Wählen Sie nach dem Ändern der Clusterauswahl immer den Namespace erneut aus.
Die Namespace-Dropdown-Liste ist leer oder zeigt neu hinzugefügte Namespaces nicht an.	Die Datenerfassung für den Cluster ist noch nicht abgeschlossen. Die Datenerfassung dauert bis zu 5 Minuten nach dem Eingeben oder Ändern des Clusters und bis zu 10 Minuten, wenn Sie den Namespace eingeben oder ändern.	Warten Sie für einen neuen Cluster mit vorhandenen Namespaces bis zu 5 Minuten, bis die Datenerfassung abgeschlossen ist. Warten Sie für einen neuen Namespace in einem vorhandenen Cluster bis zu 10 Minuten, bis die Datenerfassung abgeschlossen ist. Wenn das Problem weiterhin besteht, entfernen Sie den Cluster und fügen Sie ihn unter Infrastruktur > Ressourcen > Kubernetes erneut hinzu.
Terraform-CLI-Container werden in einem vorherigen Cluster, vorherigen Namespace oder mit vorherigen Laufzeiteinstellungen erstellt, auch wenn das Integrationskonto aktualisiert wurde.	Der von vRealize Automation verwendete Kubernetes-API-Client wird 5 Minuten lang zwischengespeichert.	Es kann bis zu 5 Minuten dauern, bis Änderungen wirksam werden.
Die Validierung oder ein Terraform-Bereitstellungsvorgang schlägt mit einer Fehlermeldung fehl, die besagt, dass kubeconfig nicht verfügbar ist.	Manchmal ereignen sich diese Fehler, weil der Cluster nicht von vRealize Automation aus erreichbar ist. In anderen Fällen sind Benutzeranmeldedaten, Token oder Zertifikate ungültig.	Der Fehler „kubeconfig“ kann aus mehreren Gründen auftreten. Möglicherweise muss zur Fehlerbehebung der technische Support kontaktiert werden.

Vorgehensweise zum Hinzufügen von Proxy-Unterstützung

Führen Sie die folgenden Schritte aus, damit Ihr externer Kubernetes-Laufzeitcluster eine Verbindung über einen Proxy-Server herstellen kann.

- 1 Melden Sie sich bei Ihrem Kubernetes-Cluster-Server an.
- 2 Erstellen Sie einen leeren Ordner.
- 3 Fügen Sie im neuen Ordner folgende Zeilen zu einer neuen Datei mit der Bezeichnung „Dockerfile“ hinzu.

```
FROM projects.registry.vmware.com/vra/terraform:latest as final
ENV https_proxy=protocol://username:password@proxy_host:proxy_port
ENV http_proxy=protocol://username:password@proxy_host:proxy_port
ENV no_proxy=.local,.localdomain,localhost
```

- 4 Ändern Sie die Platzhalterwerte, sodass die Umgebungsvariablen `https_proxy` und `http_proxy` die Proxy-Server-Einstellungen enthalten, die Sie für den Zugriff auf das Internet verwenden.

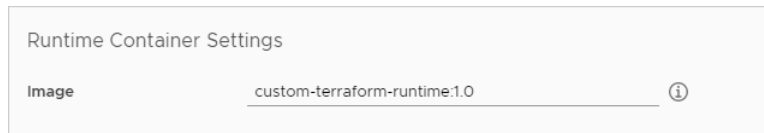
Das vom Proxy-Server verwendete *Protokoll* lautet HTTP oder HTTPS und entspricht unter Umständen nicht dem Namen der Umgebungsvariable `https_proxy` oder `http_proxy`.

- 5 Speichern und schließen Sie die Datei „Dockerfile“.
- 6 Führen Sie im leeren Ordner den folgenden Befehl aus. Abhängig von Ihren Kontoberechtigungen müssen Sie den Befehl möglicherweise im Sudo-Modus ausführen.

```
docker build --file Dockerfile --tag custom-terraform-runtime:1.0 .
```

Der Befehl erstellt ein lokales Docker-Image (custom-terraform-runtime:1.0).

- 7 Wechseln Sie in vRealize Automation Cloud Assembly unter **Infrastruktur > Verbindungen > Integrationen** zu Ihrer Terraform-Laufzeitintegration.
- 8 Erstellen oder bearbeiten Sie die Einstellungen des Laufzeit-Containers, um das Image „custom-ungform-runtime:1.0“ zu verwenden:



vRealize Automation Cloud Assembly Terraform-Laufzeit ohne Internetzugriff

vRealize Automation Cloud Assembly-Benutzer, die Terraform-Integrationen entwerfen und ausführen müssen, während sie keinen Internetzugriff haben, können ihre Laufzeitumgebung einrichten, indem sie dem nachstehenden Beispiel folgen.

Hinweis Sie müssen während der Einrichtung vorübergehend eine Verbindung zum Internet herstellen.

Bei diesem Vorgang wird davon ausgegangen, dass Sie über [Ihre eigene Docker-Registrierung](#) verfügen und über eine Internetverbindung auf deren Repositorys zugreifen können.

Erstellen des benutzerdefinierten Container-Images

- 1 Erstellen Sie ein benutzerdefiniertes Container-Image, das die Binärdateien des Terraform-Anbieter-Plug-Ins enthält.

In der folgenden Datei „Dockerfile“ ist ein Beispiel für die Erstellung eines benutzerdefinierten Images mit dem GCP-Anbieter für Terraform zu sehen.

Das Herunterladen des Basisimages `projects.registry.vmware.com/vra/terraform:latest` in die Datei „Dockerfile“ erfordert temporären Internetzugriff auf die VMware Harbor-Registrierung unter `projects.registry.vmware.com`.

Firewall- oder Proxy-Einstellungen können dazu führen, dass der Image-Build fehlschlägt. Möglicherweise müssen Sie temporären Zugriff auf releases.hashicorp.com aktivieren, um die Binärdateien des Terraform-Anbieter-Plug-Ins herunterzuladen. Sie können jedoch optional Ihre private Registrierung verwenden, um die Plug-In-Binärdateien zur Verfügung zu stellen.

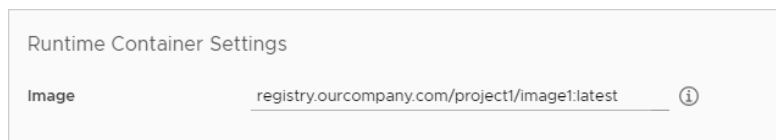
```
FROM projects.registry.vmware.com/vra/terraform:latest as final

# Create provider plug-in directory
ARG plugins=/tmp/terraform.d/plugin-cache/linux_amd64
RUN mkdir -m 777 -p $plugins

# Download and unzip all required provider plug-ins from hashicorp to provider directory
RUN cd $plugins \
    && wget -q https://releases.hashicorp.com/terraform-provider-google/3.58.0/terraform-provider-google_3.58.0_linux_amd64.zip \
    && unzip *.zip \
    && rm *.zip

# For "terraform init" configure terraform CLI to use provider plug-in directory and not
download from internet
ENV TF_CLI_ARGS_init="-plugin-dir=$plugins -get-plugins=false"
```

- 2 Erstellen, taggen und übertragen Sie das benutzerdefinierte Container-Image in Ihr eigenes Docker-Repository.
- 3 Wechseln Sie in vRealize Automation Cloud Assembly unter **Infrastruktur > Verbindungen > Integrationen** zu Ihrer Terraform-Laufzeitintegration.
- 4 Erstellen oder bearbeiten Sie die Laufzeit-Containereinstellungen, um Ihr Repository für das benutzerdefinierte Container-Image hinzuzufügen. Der Name des beispielhaft erstellten benutzerdefinierten Container-Images lautet `registry.ourcompany.com/project1/image1:latest`.



Lokales Hosten der Terraform-CLI

- 1 Laden Sie die Terraform-CLI-Binärdateien herunter.
- 2 Laden Sie die Terraform-CLI-Binärdateien auf Ihren lokalen Webserver hoch.
- 3 Wechseln Sie in vRealize Automation Cloud Assembly zu **Infrastruktur > Konfigurieren > Terraform-Versionen**.
- 4 Erstellen oder bearbeiten Sie die Terraform-Version so, dass sie die URL zu den Terraform-CLI-Binärdateien enthält, die auf Ihrem lokalen Webserver gehostet werden.

0.12.29 DELETE	
Version *	0.12.29 ⓘ
Description	<input type="text"/>
Enabled	<input checked="" type="checkbox"/> ⓘ
URL *	http://host1.ourcompany.com:8080/tf/0.12.29/terraform_0.12.29_linux_amd64.zip ⓘ
SHA256 Checksum *	872245d9c6302b24dc0d98a1e010aef60865a2d1f60102c8ad03e9d5a1d ⓘ

Entwerfen und Bereitstellen von Terraform-Konfigurationen

Sobald die Laufzeit vorhanden ist, können Sie Terraform-Konfigurationsdateien in Git hinzufügen, Cloud-Vorlagen für sie entwerfen und Bereitstellungen vornehmen.

Informationen zu den ersten Schritten finden Sie unter [Vorbereiten auf Terraform-Konfigurationen in vRealize Automation Cloud Assembly](#).

Fehlerbehebung

Öffnen Sie beim Bereitstellen die Bereitstellung in vRealize Automation Cloud Assembly. Suchen Sie auf der Registerkarte „Verlauf“ nach Terraform-Ereignissen und klicken Sie rechts auf **Protokolle anzeigen**. Wenn Ihr lokaler Terraform-Anbieter funktioniert, werden die folgenden Meldungen im Protokoll angezeigt.

```
Initializing provider plugins
```

```
Terraform has been successfully initialized
```

Für ein robusteres Protokoll können Sie den Code der Cloud-Vorlage manuell bearbeiten und `TF_LOG: DEBUG` hinzufügen, wie im folgenden Beispiel gezeigt.

```
resources:
  terraform:
    type: Cloud.Terraform.Configuration
    properties:
      providers:
        - name: google
          # List of available cloud zones: gcp/us-west1
          cloudZone: gcp/us-west1
      environment:
        # Configure terraform CLI debug log settings
        TF_LOG: DEBUG
    terraformVersion: 0.12.29
    configurationSource:
      repositoryId: fc569ef7-f013-4489-9673-6909a2791071
      commitId: 3e00279a843a6711f7857929144164ef399c7421
      sourceDirectory: gcp-simple
```

Vorbereiten auf Terraform-Konfigurationen in vRealize Automation Cloud Assembly

Bevor Sie eine Terraform-Konfiguration zu einer vRealize Automation Cloud Assembly-Vorlage hinzufügen, richten Sie Ihr Versionskontroll-Repository ein und integrieren Sie es.

- 1 [Voraussetzungen](#)
- 2 [Speichern von Terraform-Konfigurationsdateien in einem Repository für Versionskontrolle](#)
- 3 [Aktivieren der Cloud-Zonen-Zuordnung](#)
- 4 [Integrieren des Repositories mit vRealize Automation Cloud Assembly](#)

Voraussetzungen

Damit das lokale vRealize Automation-Produkt Terraform-Vorgänge ausführen kann, benötigen Sie die Terraform-Laufzeitintegration. Weitere Informationen hierzu finden Sie unter [Vorbereiten einer Terraform-Laufzeitumgebung für vRealize Automation Cloud Assembly](#).

Speichern von Terraform-Konfigurationsdateien in einem Repository für Versionskontrolle

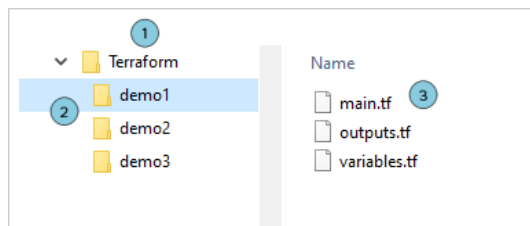
vRealize Automation Cloud Assembly unterstützt die folgenden Repositories für Versionskontrolle für Terraform-Konfigurationen.

- GitHub Cloud, lokales GitHub Enterprise
- GitLab Cloud
- Lokales BitBucket

Erstellen Sie im Repository für Versionskontrolle ein Standardverzeichnis mit einer Unterverzeichnisebene, wobei jedes Unterverzeichnis Terraform-Konfigurationsdateien enthält. Erstellen Sie ein Unterverzeichnis pro Terraform-Konfiguration.

- 1 Standardverzeichnis
- 2 Einzelne Unterverzeichnisebene
- 3 Bereitstellungsfähige Terraform-Konfigurationsdateien

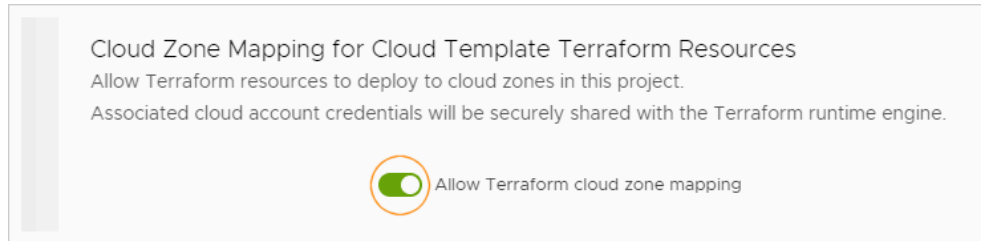
Schließen Sie keine Terraform-Statusdatei mit Konfigurationsdateien ein. Wenn `terraform.tfstate` vorhanden ist, treten bei der Bereitstellung Fehler auf.



Aktivieren der Cloud-Zonen-Zuordnung

Wenn Sie eine Bereitstellung in einem Cloud-Konto planen, benötigt die Terraform-Laufzeit-Engine die entsprechenden Cloud-Zonen-Anmeldedaten.

Aktivieren Sie auf der Registerkarte **Bereitstellung** des Projekts die Option **Zuordnung zur Terraform-Cloud-Zone** zulassen.



Obwohl die Anmeldedaten sicher übermittelt werden, sollten Sie diese Option aus Sicherheitsgründen deaktiviert lassen, wenn sie von Projektbenutzern nicht zum Bereitstellen eines Cloud-Kontos benötigt wird.

Integrieren des Repositorys mit vRealize Automation Cloud Assembly

Wechseln Sie in vRealize Automation Cloud Assembly zu **Infrastruktur > Verbindungen > Integrationen**.

Fügen Sie eine Integration zu dem Repository-Angebotstyp hinzu, in dem Sie die Terraform-Konfigurationen gespeichert haben: GitHub, GitLab oder Bitbucket.

Wenn Sie Ihr Projekt zur Integration hinzufügen, wählen Sie den Typ **Terraform-Konfigurationen** aus und geben Sie das Repository und die Verzweigung an.

Ordner ist das Standardverzeichnis Ihrer früheren Struktur.

Entwerfen für Terraform-Konfigurationen in vRealize Automation Cloud Assembly

Mit den Konfigurationsdateien für Ihr Repository und Terraform können Sie eine vRealize Automation Cloud Assembly-Vorlage für sie entwerfen.

1 Voraussetzungen

- 2 [Aktivieren der Terraform-Laufzeitversionen](#)
- 3 [Hinzufügen von Terraform-Ressourcen zum Design](#)
- 4 [Bereitstellen der Cloud- Vorlage](#)

Voraussetzungen

Richten Sie Ihr Versionskontroll-Repository ein und integrieren Sie es. Weitere Informationen hierzu finden Sie unter [Vorbereiten auf Terraform-Konfigurationen in vRealize Automation Cloud Assembly](#).

Aktivieren der Terraform-Laufzeitversionen

Sie können die Benutzern zur Verfügung stehenden Terraform-Laufzeitversionen definieren, wenn Sie Terraform-Konfigurationen bereitstellen. Beachten Sie, dass Terraform-Konfigurationen auch intern codierte Versionseinschränkungen enthalten können.

Navigieren Sie zum Erstellen der Liste zulässiger Versionen zu **Infrastruktur > Konfigurieren > Terraform-Versionen**. Nur 0.12.x-Versionen werden unterstützt.

Hinzufügen von Terraform-Ressourcen zum Design

Erstellen Sie die Cloud-Vorlage, die Terraform-Konfigurationen enthält.

- 1 Gehen Sie in vRealize Automation Cloud Assembly zu **Design > Cloud-Vorlagen** und klicken Sie auf **Neu von > Terraform**.

Der Assistent „Terraform-Konfiguration“ wird angezeigt.

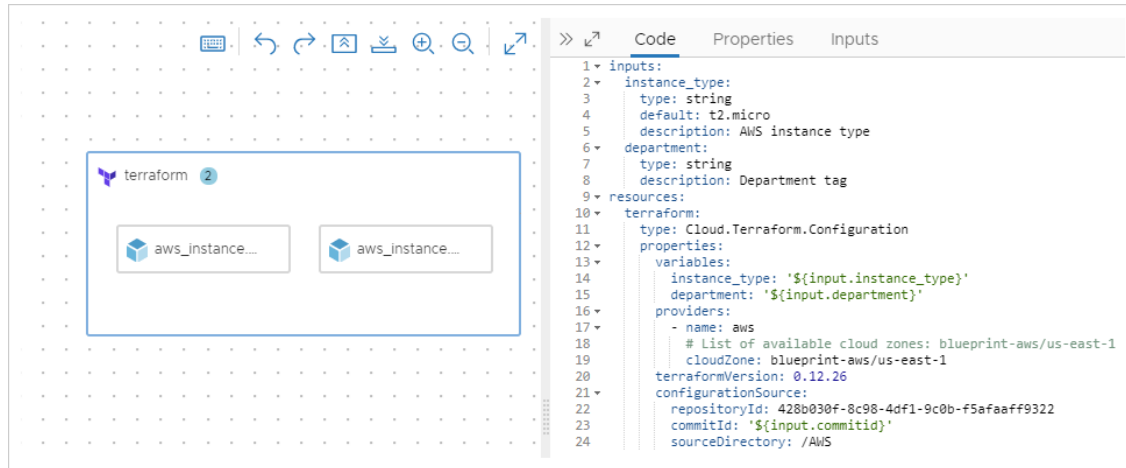
- 2 Folgen Sie den Anweisungen auf dem Bildschirm.

Seite „Assistent“	Einstellung	Wert
Neue Cloud-Vorlage	Name	Geben Sie dem Design einen aussagekräftigen Namen.
	Beschreibung	Erläutern Sie den Einsatzzweck des Designs.
	Projekt	Wählen Sie das Projekt mit der Repository-Integration aus, in der die Terraform-Konfiguration gespeichert ist.
Konfigurationsquelle	Repository	Wählen Sie das integrierte Repository aus, in dem die Terraform-Konfiguration gespeichert ist.
	Commit	Wählen Sie einen Repository-Commit aus oder lassen Sie den Eintrag leer, um die Terraform-Konfiguration aus dem Repository-Head zu verwenden. Bitbucket-Beschränkung – Die Anzahl der auswählbaren Commits wird unter Umständen aufgrund der Serverkonfiguration des Bitbucket-Repositorys gekürzt.

Seite „Assistent“	Einstellung	Wert
	Quellverzeichnis	Wählen Sie ein Unterverzeichnis aus der von Ihnen erstellten Repository-Struktur aus. Die im vorherigen Setup angezeigten Beispielunterverzeichnisse lauteten demo1, demo2 und demo3.
Konfiguration abschließen	Repository	Stellen Sie die korrekte Auswahl des Repositorys sicher.
	Quellverzeichnis	Stellen Sie die korrekte Auswahl des Verzeichnisses sicher.
	Terraform-Version	Wählen Sie die Terraform-Laufzeitumgebung aus, die beim Bereitstellen der Terraform-Konfiguration ausgeführt werden soll.
	Anbieter	Wenn die Terraform-Konfiguration eine Anbietersperre enthielt, überprüfen Sie den Anbieter und die Cloud-Zone, in der diese Cloud-Vorlage bereitgestellt wird. Wenn kein Anbieter vorhanden ist, ist dies kein Problem. Nach dem Beenden des Assistenten bearbeiten Sie einfach den Anbieter und die Cloud-Zone in den Vorlageneigenschaften, um das Bereitstellungsziel hinzuzufügen oder zu ändern.
	Variablen	Wählen Sie vertrauliche Werte für die Verschlüsselung aus, z. B. Kennwörter.
	Ausgaben	Überprüfen Sie die Ausgaben aus der Terraform-Konfiguration, die in Ausdrücke konvertiert werden, auf die Ihr Designcode weiter verweisen kann.

3 Klicken Sie auf **Erstellen**.

Die Terraform-Ressource wird auf der Arbeitsfläche der Cloud-Vorlage mit vRealize Automation Cloud Assembly-Code angezeigt, der die bereitzustellende Terraform-Konfiguration widerspiegelt.



Sie können gegebenenfalls andere vRealize Automation Cloud Assembly-Ressourcen zur Cloud-Vorlage hinzufügen, um Terraform- und Nicht-Terraform-Code in einem hybriden Design zu kombinieren.

Hinweis Die Aktualisierung von Terraform-Konfigurationen im Repository führt nicht zu einer Synchronisierung der Änderungen in Ihrer Cloud-Vorlage. Die automatische Synchronisierung kann Sicherheitsrisiken bergen, wie z. B. neu hinzugefügte sensible Variablen.

Zum Erfassen von Änderungen der Terraform-Konfiguration führen Sie den Assistenten erneut aus, legen den neuen Commit fest und geben beliebige neue sensible Variablen ein.

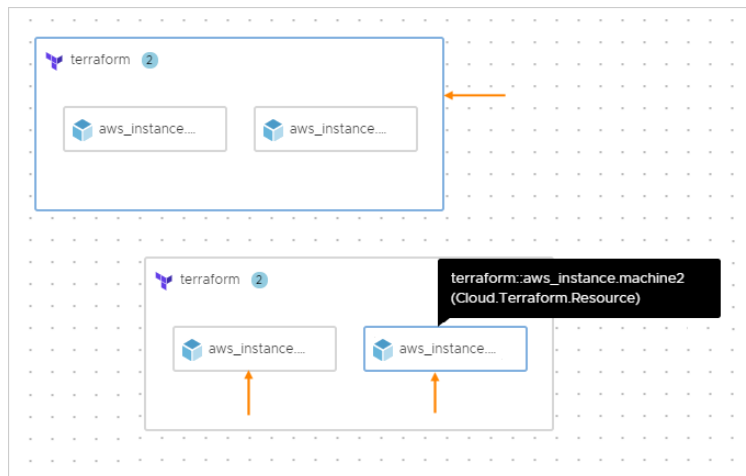
Bereitstellen der Cloud- Vorlage

Bei der Bereitstellung der Cloud-Vorlage können Sie auf der Registerkarte **Verlauf** der Bereitstellung ein Ereignis erweitern, wie z. B. eine Zuteilungs- oder Entwurfsphase, um ein Protokoll mit Nachrichten aus der Terraform-Befehlszeilenschnittstelle zu überprüfen.

Genehmigungen – Zusätzlich zu den erwarteten Terraform-Phasen wie PLANEN, ZUTEILEN oder ERSTELLEN führt vRealize Automation Cloud Assembly Governance mittels einer Genehmigungsphase ein. Weitere Informationen zu den Anforderungsgenehmigungen finden Sie unter [Vorgehensweise zum Konfigurieren von Genehmigungsrichtlinien in Service Broker](#).

Timestamp	Status	Resource type	Resource name	Details
Aug 3, 202...	PLAN_FINISHED	Cloud.Terraform.Configurati...	terraform	Creating 2 Terraform resources, updating 0 Terraform resources, deleting 0 Terraform resources
Aug 3, 202...	PLAN_IN_PROGRESS	Cloud.Terraform.Configurati...	terraform	Hide Logs
<pre> 2:24:23 PM * provider.random: version = "~> 2.3" 2:24:23 PM 2:24:23 PM Terraform has been successfully initialized! 2:24:28 PM Refreshing Terraform state in-memory prior to plan... 2:24:28 PM The refreshed state will be used to calculate this plan, but will not be 2:24:28 PM persisted to local or remote state storage. </pre>				
Aug 3, 202...	INITIALIZATION_FINISH...			
Aug 3, 202...	INITIALIZATION_IN_PRO...			

Nach der Bereitstellung wird eine äußere Ressource angezeigt, die die gesamte Terraform-Komponente mit enthaltenen untergeordneten Ressourcen für die einzelnen Komponenten darstellt, die von Terraform erstellt wurden. Die übergeordnete Terraform-Ressource steuert den Lebenszyklus der untergeordneten Ressourcen.



Weitere Informationen zu Terraform-Konfigurationen in vRealize Automation

Achten Sie auf bestimmte Einschränkungen und Fehlerbehebungen, wenn Sie Terraform-Konfigurationen als Ressource in vRealize Automation einbetten.

Einschränkungen für Terraform-Konfigurationen

- Wenn Sie ein Design mit Terraform-Konfigurationen validieren, wird mit der Schaltfläche **TESTEN** die vRealize Automation Cloud Assembly-Syntax geprüft, aber nicht die Syntax des nativen Terraform-Codes.

Darüber hinaus validiert die Schaltfläche **TESTEN** keine den Terraform-Konfigurationen zugeordneten Commit-IDs.

- Für eine Cloud-Vorlage, die Terraform-Konfigurationen enthält, erfordert das Klonen der Vorlage in ein anderes Projekt die folgende Problemumgehung.
 - a Kopieren Sie im neuen Projekt auf der Registerkarte **Integrationen** die `repositoryId` für Ihre Integration.
 - b Öffnen Sie die Klonvorlage. Ersetzen Sie im Code-Editor die `repositoryId` durch die von Ihnen kopierte ID.
- Schließen Sie im Versionskontroll-Repository keine Terraform-Statusdatei mit Konfigurationsdateien ein. Wenn `terraform.tfstate` vorhanden ist, treten bei der Bereitstellung Fehler auf.

Unterstützte Tag-2-Aktionen für die übergeordnete Terraform-Ressource

Für die übergeordnete Terraform-Ressource können Sie die Terraform-Statusdatei anzeigen oder aktualisieren. Weitere Informationen zu Statusdateiaktionen finden Sie in der umfangreichen Liste der Aktionen unter [Welche Aktionen kann ich auf vRealize Automation Cloud Assembly-Bereitstellungen ausführen?](#).

Unterstützte Tag-2-Aktionen für untergeordnete Ressourcen

Nach der Bereitstellung von Terraform-Konfigurationen verstreichen möglicherweise bis zu 20 Minuten, bevor Tag-2-Aktionen für untergeordnete Ressourcen verfügbar werden.

Für untergeordnete Ressourcen in einer Terraform-Konfiguration wird nur der folgenden Teilsatz an Tag-2-Aktionen unterstützt. Weitere Informationen zu den Aktionen finden Sie in der umfangreichen Liste der Aktionen unter [Welche Aktionen kann ich auf vRealize Automation Cloud Assembly-Bereitstellungen ausführen?](#).

Anbieter	Terraform-Ressourcentyp	Unterstützte Tag-2-Aktionen
AWS	aws_instance	Einschalten
		Ausschalten
		Neu starten
		Zurücksetzen
Azure	azurerm_virtual_machine	Einschalten
		Ausschalten
		Neu starten
		Anhalten
vSphere	vsphere_virtual_machine	Einschalten
		Ausschalten
		Neu starten

Anbieter	Terraform-Ressourcentyp	Unterstützte Tag-2-Aktionen
GCP	google_compute_instance	Zurücksetzen
		Herunterfahren
		Anhalten
		Snapshot erstellen
		Snapshot löschen
		Snapshot wiederherstellen
	google_compute_instance	Einschalten
		Ausschalten
		Snapshot erstellen
		Snapshot löschen

Fehlerbehebung bei der Verfügbarkeit von Tag-2-Aktionen

Vorkonfigurierte Tag-2-Aktionen, die fehlen oder deaktiviert sind, benötigen möglicherweise eine Fehlerbehebung.

Problem	Ursache	Lösung
Für eine Terraform-Ressource fehlt eine erwartete vorkonfigurierte Tag-2-Aktion im Menü „Aktionen“.	Die Aktion wird für den Anbieter und den Ressourcentyp wie in der vorherigen Liste aufgeführt möglicherweise nicht unterstützt. Alternativ kann es aufgrund der Ressourcenermittlung und Ressourcenzwischenspeicherung bis zu 20 Minuten dauern, bis die Aktion angezeigt wird.	Überprüfen Sie den Anbieter und den Ressourcentyp im Entwurf. Warten Sie bis zu 20 Minuten, bis die Datenerfassung abgeschlossen ist.
Auch nachdem 20 Minuten auf die Datenerfassung gewartet wurde, fehlt einer Terraform-Ressource noch eine erwartete Tag-2-Aktion.	Ein Problem mit der Ressourcenermittlung verhindert, dass die Aktion angezeigt wird. Das kann beispielsweise geschehen, wenn die Ressource versehentlich in einer Cloud-Zone außerhalb des Projekts erstellt wird. Beispielsweise enthält Ihr Projekt nur eine Cloud-Zone mit Cloud-Konto und Region us-east-1, aber die Terraform-Konfiguration enthält eine Anbietersperre für us-west-1, was Sie in der Entwurfsphase nicht geändert haben. Eine weitere Möglichkeit besteht darin, dass die Datenerfassung nicht funktioniert.	Vergleichen Sie die Cloud-Zonen des Projekts mit den Cloud-Zonen im Entwurf. Gehen Sie zu Infrastruktur > Verbindungen > Cloud-Konten und überprüfen Sie den Datenerfassungsstatus und die Zeit der letzten erfolgreichen Erfassung für das Cloud-Konto.

Problem	Ursache	Lösung
Auch wenn keine offensichtlichen Probleme mit dem Ressourcenstatus und der Datenerfassung vorliegen, ist eine Tag-2-Aktion deaktiviert (grau unterlegt).	Gelegentlich kann es vorkommen, dass zeitweilige Timing- und Datenerfassungsfehler auftreten.	Das Problem sollte innerhalb von 20 Minuten behoben sein.
Die falsche Tag-2-Aktion ist deaktiviert, die basierend auf dem Ressourcenstatus aktiv sein sollte. So ist z. B. „Ausschalten“ aktiviert und „Einschalten“ deaktiviert, obwohl die Ressource über die Benutzeroberfläche des Anbieters ausgeschaltet wurde.	Der Datenerfassungszeitpunkt kann zu einer vorübergehenden Nichtübereinstimmung führen. Wenn Sie den Betriebszustand von außerhalb vRealize Automation ändern, dauert es einige Zeit, um die Änderung korrekt wiederzugeben.	Warten Sie bis zu 20 Minuten.

Verwenden von benutzerdefinierten Terraform-Anbietern in vRealize Automation

Wenn Sie einen benutzerdefinierten Terraform-Anbieter erstellt haben und diesen verwenden möchten, führen Sie die folgenden Schritte aus.

- 1 Fügen Sie unter dem standardmäßigen Terraform-Verzeichnis im Repository für die Git-Versionskontrolle die folgende Unterverzeichnisstruktur hinzu.

```
terraform.d/plugins/linux_amd64
```

- 2 Fügen Sie dem Verzeichnis `linux_amd64` die Go-Binärdateien Ihres benutzerdefinierten Terraform-Anbieters hinzu.

Standardmäßig wird von `terraform init` in diesem Verzeichnis nach benutzerdefinierten Anbieter-Plug-ins gesucht.

Hinweis In VMware kommt es gelegentlich vor, dass ein benutzerdefinierter Terraform-Anbieter nicht ausgeführt werden kann und eine `no such file or directory`-Meldung sendet.

Versuchen Sie in diesem Fall, die Go-Binärdateien des benutzerdefinierten Anbieters bei deaktiviertem CGO (auf Null gesetzt) neu zu kompilieren. CGO wird für Go-Pakete verwendet, die C-Code aufrufen.

Vorgehensweise zum Verwenden des vRealize Automation Cloud Assembly-Marketplace

Zum Schnellstarten Ihrer Ressourcenbibliothek laden Sie Dateien aus dem vRealize Automation Cloud Assembly-Marketplace herunter. Der Marketplace stellt fertige Cloud-Vorlagen und offene Virtualisierungs-Images bereit.

Zugriff auf den Marketplace

In vRealize Automation Cloud Assembly wählen Sie **Infrastruktur > Verbindungen > Integrationen** aus. Klicken Sie auf **Integration hinzufügen**, dann auf **My VMware** und stellen Sie die Anmeldedaten für Ihr My VMware-Konto bereit.

Vorgehensweise zum Herunterladen und Verwenden von Marketplace-Cloud-Vorlagendateien

Klicken Sie auf der Registerkarte **Marketplace** auf **Abrufen** und akzeptieren Sie die Cloud-Vorlagen-Lizenzbedingungen. Anschließend können Sie die Vorlage zu einem vRealize Automation Cloud Assembly-Projekt hinzufügen oder einfach herunterladen. Sie können eine Cloud-Vorlage über die Registerkarte **Design** hochladen.

Stellen Sie sich für ein projektbasiertes Beispiel vor, dass Sie Projektadministrator für ein Big-Data-Projekt sind. Zur Unterstützung Ihres Teams suchen Sie nach einer Marketplace-Hadoop-Vorlage, die Sie dem Teamprojekt hinzufügen. Anschließend passen Sie die Cloud-Vorlage für Ihre Ressourcenumgebung an und geben sie frei. Dann importieren Sie die Vorlage in den vRealize Automation Service Broker-Katalog, damit sie vom Team bereitgestellt werden kann.

Vorgehensweise zum Herunterladen und Verwenden von Marketplace-Image-Dateien

Klicken Sie auf der Registerkarte **Marketplace** auf **Abrufen** und akzeptieren Sie die Lizenzbedingungen der OVF- oder OVA-Datei. Anschließend können Sie das OVF- oder das OVA-Image herunterladen und im Cloud-Vorlagencode darauf verweisen.

In Fortführung des vorherigen Beispiels benötigt Ihr Team möglicherweise Zugriff auf eine Hadoop-Version. Sie können eine Hadoop-OVF-Datei herunterladen und zu Cloud-Kontoressourcen wie einer vCenter Server-Inhaltsbibliothek hinzufügen. Anschließend aktualisieren Sie den gesamten Vorlagencode, der auf das OVF-Image verweisen muss.

Verwalten von vRealize Automation Cloud Assembly-Bereitstellungen

7

Als vRealize Automation Cloud Assembly-Cloud-Vorlagenentwickler verwenden Sie die Registerkarte „Bereitstellung“, um Ihre Bereitstellungen zu verwalten. Sie können Fehler in Bereitstellungsprozessen beheben, Änderungen vornehmen und nicht verwendete Bereitstellungen löschen.

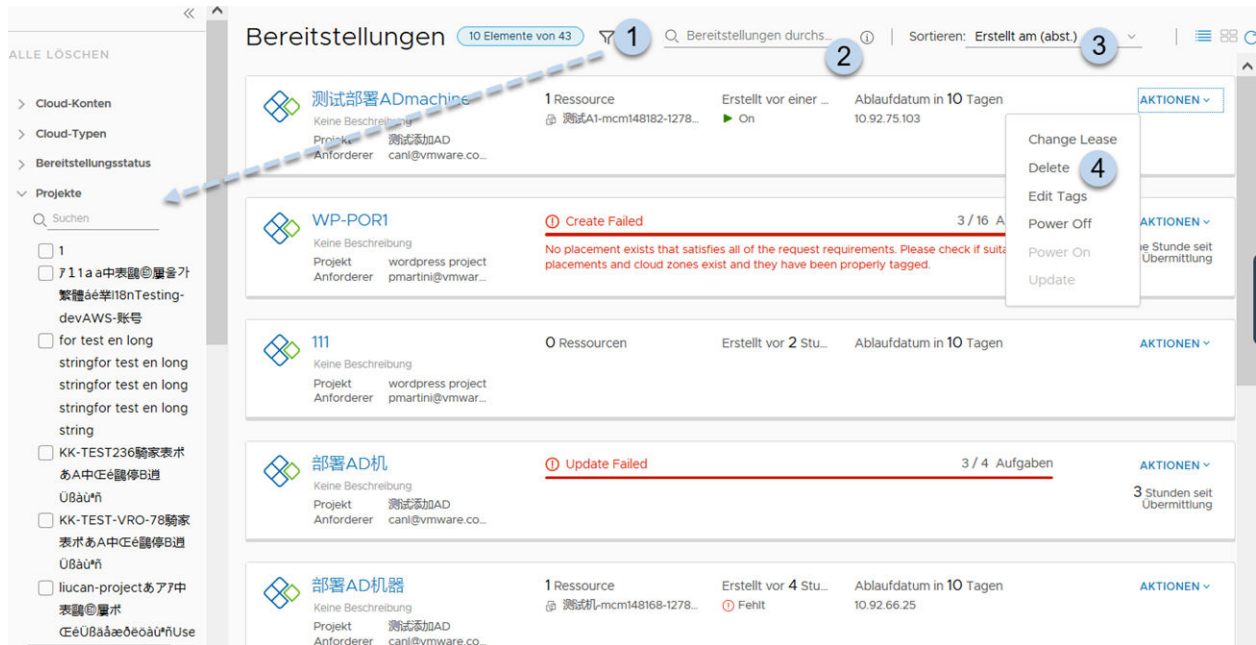
Bei Bereitstellungen handelt es sich um die bereitgestellten Instanzen von Cloud-Vorlagen. Auf der Registerkarte „Bereitstellungen“ werden erfolgreiche und fehlgeschlagene Bereitstellungen aufgeführt. Sie verwenden die Seite, um Ihre erfolgreichen Bereitstellungen zu verwalten oder um mit der Fehlerbehebung bei fehlgeschlagenen Anforderungen zu beginnen.

Arbeiten mit Bereitstellungskarten

Sie können mithilfe der Kartenliste nach Ihren Bereitstellungen suchen und diese verwalten. Sie können nach bestimmten Bereitstellungen suchen und diese filtern und anschließend Aktionen für diese Bereitstellungen ausführen.

- 1 Filtern Sie Ihre Anforderungen auf der Basis von Attributen.
- 2 Suchen Sie auf der Basis von Schlüsselwörtern oder Anforderer nach Bereitstellungen.
- 3 Sortieren Sie die Liste nach Uhrzeit oder Name.
- 4 Führen Sie Aktionen auf Bereitstellungsebene in der Bereitstellung aus, einschließlich Löschen nicht verwendeter Bereitstellungen zur Rückforderung von Ressourcen.

Sie können auch die Bereitstellungskosten, Ablaufdaten und Statusangaben anzeigen.



Dieses Kapitel enthält die folgenden Themen:

- Vorgehensweise zum Überwachen von Bereitstellungen in vRealize Automation Cloud Assembly
- Vorgehensweise beim Fehlschlagen einer vRealize Automation Cloud Assembly-Bereitstellung
- Vorgehensweise zum Verwalten des Lebenszyklus einer abgeschlossenen vRealize Automation Cloud Assembly-Bereitstellung
- Welche Aktionen kann ich auf vRealize Automation Cloud Assembly-Bereitstellungen ausführen?

Vorgehensweise zum Überwachen von Bereitstellungen in vRealize Automation Cloud Assembly

Nach dem Bereitstellen einer vRealize Automation Cloud Assembly-Cloud-Vorlage können Sie Ihre Anforderung überwachen, um sicherzustellen, dass die Ressourcen bereitgestellt und aktiv sind. Beginnend mit der Bereitstellungskarte können Sie die Bereitstellung Ihrer Ressourcen überprüfen. Als Nächstes können Sie die Bereitstellungsdetails überprüfen. Abschließend können Sie die gelöschten Bereitstellungen anzeigen.

Verfahren

- 1 Klicken Sie auf **Bereitstellungen** und suchen Sie gegebenenfalls mithilfe von Filtern und der Suchfunktion nach Ihrer aktuellen Bereitstellungskarte.

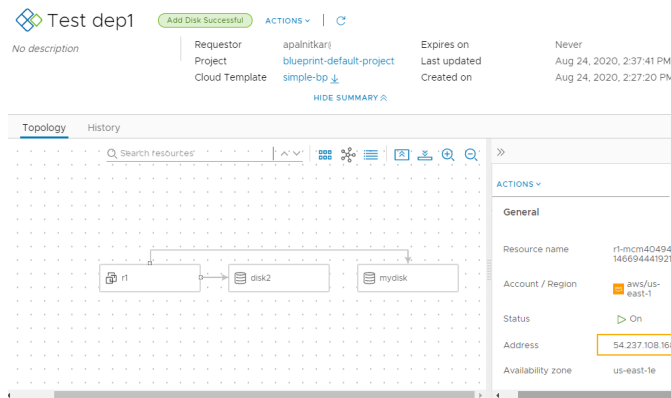
2 Überprüfen Sie den Kartenstatus.

Bei Ausführung der Bereitstellung wird auf der Prozessleiste die Anzahl der verbleibenden Aufgaben angezeigt. Bei erfolgreichem Abschluss der Bereitstellung werden auf der Karte die grundlegenden Details zur Bereitstellung angezeigt.



3 Um zu ermitteln, wo Ihre Ressourcen bereitgestellt wurden, klicken Sie auf den Namen der Bereitstellung und überprüfen Sie die Details auf der Seite „Topologie“.

Sie benötigen wahrscheinlich die IP-Adresse für die primäre Komponente. Beachten Sie beim Klicken auf jede Komponente, dass die bereitgestellten Informationen für die jeweilige Komponente spezifisch sind. In diesem Beispiel wird die IP-Adresse hervorgehoben.



Die Verfügbarkeit der externen Verknüpfung hängt vom Cloud-Anbieter ab. Wenn sie verfügbar ist, benötigen Sie die Anmeldedaten für diesen Anbieter, um auf die Komponente zuzugreifen.

Nächste Schritte

- Sie können Änderungen an Ihrer Bereitstellung vornehmen. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Verwalten des Lebenszyklus einer abgeschlossenen vRealize Automation Cloud Assembly-Bereitstellung](#).
- Wenn die Bereitstellung fehlschlägt, finden Sie weitere Informationen unter [Vorgehensweise beim Fehlschlagen einer vRealize Automation Cloud Assembly-Bereitstellung](#).

Vorgehensweise beim Fehlschlagen einer vRealize Automation Cloud Assembly-Bereitstellung

Ihre Bereitstellungsanforderung kann aus verschiedenen Gründen fehlschlagen. Ursachen können der Netzwerkdatenverkehr, ein Mangel an Ressourcen beim Anbieter der Ziel-Cloud oder eine fehlerhafte Bereitstellungsspezifikation sein. Es ist auch möglich, dass die Bereitstellung erfolgreich verlaufen ist, aber offenbar nicht funktioniert. Sie können vRealize Automation Cloud Assembly verwenden, um Ihre Bereitstellung und alle Fehlermeldungen zu überprüfen und um

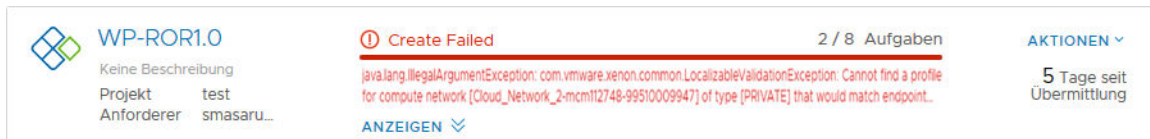
herauszufinden, ob es an der Umgebung oder der angeforderten Arbeitslastspezifikation liegt oder ob andere Gründe dafür verantwortlich sind.

Sie verwenden diesen Workflow, um mit der Recherche zu beginnen. Während dieses Prozesses finden Sie unter Umständen heraus, dass der Fehler auf ein vorübergehendes Umgebungsproblem zurückzuführen ist. Indem Sie sicherstellen, dass die Bedingungen verbessert wurden, kann dieses Problem durch eine erneute Bereitstellung der Anforderung behoben werden. In anderen Fällen müssen Sie unter Umständen andere Bereiche genau überprüfen.

Als Projektmitglied können Sie die Anforderungsdetails in vRealize Automation Cloud Assembly überprüfen.

Verfahren

- 1 Um festzustellen, ob eine Anforderung fehlgeschlagen ist, klicken Sie auf die Registerkarte **Bereitstellungen** und suchen Sie nach der Bereitstellungskarte.



Fehlgeschlagene Bereitstellungen werden auf der Karte angezeigt.

- a Schauen Sie sich die Fehlermeldung an.
- b Um weitere Informationen zu erhalten, klicken Sie auf den Bereitstellungsnamen für die Bereitstellungsdetails.

2 Klicken Sie auf der Seite mit den Bereitstellungsdetails auf die Registerkarte **Verlauf**.

WP - ROR2 Create Failed ACTIONS

No description

Requestor: fritz
Project: Tiger Team
Cloud Template: WordPress Template

Expires on: Never
Last updated: Sep 9, 2020, 12:06:42 PM
Created on: Sep 9, 2020, 12:06:38 PM

HIDE SUMMARY

Topology History

2.c

2.a

2.b

CREATE fritz

Failed Requested by: fritz Provisioning diagram

Events Request details

Timestamp	Status	Resource type	Resource name	Details
Sep 9, 2020, ...	REQUEST_FAILED			Could not find any profile to match network 'WP-Network-Private' of type 'EXISTING' with constraints '[type:isolated-net, env:dev]'.
Sep 9, 2020, ...	COMPLETION_FINISHED			
Sep 9, 2020, ...	COMPLETION_IN_PROGRE...			
Sep 9, 2020, ...	ALLOCATE_FAILED	Cloud.Network	WP-Network-Private	Could not find any profile to match...

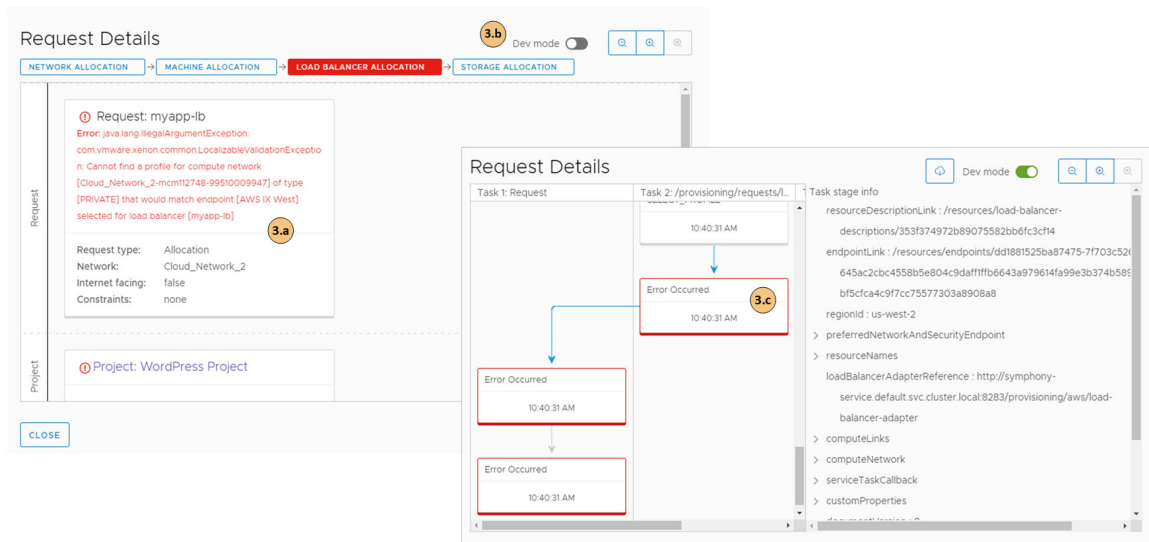
8 Events

- Überprüfen Sie die Ereignisstruktur, um herauszufinden, an welcher Stelle der Bereitstellungsvorgang fehlgeschlagen ist. Diese Struktur ist nützlich, wenn Sie eine Bereitstellung ändern, die Änderung aber fehlschlägt.

In der Struktur wird auch angezeigt, wann Sie Bereitstellungsaktionen ausführen. Sie können die Struktur auch zur Behebung der Fehler bei fehlgeschlagenen Änderungen verwenden.
- Unter **Details** finden Sie eine ausführlichere Version der Fehlermeldung.
- Wurde als Element eine vRealize Automation Cloud Assembly-Cloud-Vorlage angefordert, können Sie mithilfe der Verknüpfung rechts neben der Meldung die vRealize Automation Cloud Assembly-Anwendung öffnen und die **Anforderungsdetails** anzeigen.

3 Unter **Anforderungsdetails** finden Sie den Bereitstellungs-Workflow für fehlgeschlagene Komponenten, anhand dessen Sie das Problem untersuchen können.

Der Anforderungsverlauf wird für eine Woche aufbewahrt.

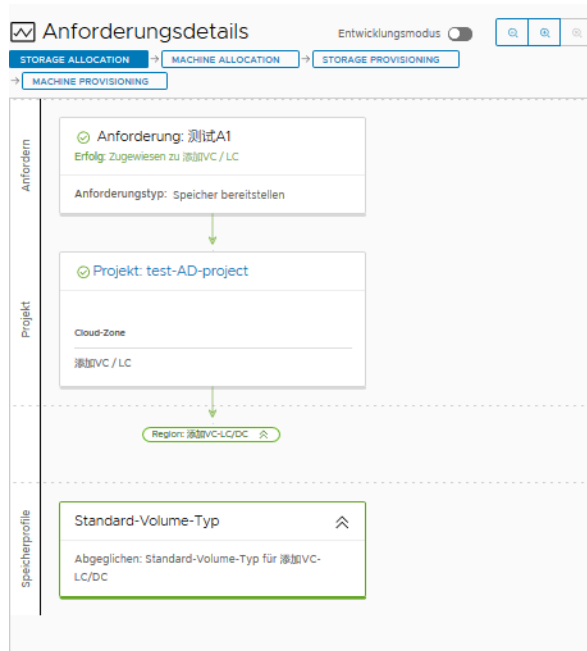


- a Schauen Sie sich die Fehlermeldung an.
 - b Sie können den **Entwicklungsmodus** aktivieren, um zwischen dem einfachen Bereitstellungs-Workflow und einem ausführlichen Flussdiagramm zu wechseln.
 - c Klicken Sie auf die Karte, um das Bereitstellungsskript zu überprüfen.
- 4 Beheben Sie die Fehler und stellen Sie die Cloud-Vorlage erneut bereit.

Die Fehler liegen möglicherweise in der Konstruktion der Vorlage oder sind auf die Konfiguration Ihrer Infrastruktur zurückzuführen.

Nächste Schritte

Nach der Behebung der Fehler und der Bereitstellung der Cloud-Vorlage werden Informationen ähnlich dem folgenden Beispiel in den Anforderungsdetails angezeigt. Zur Anzeige der Anforderungsdetails wählen Sie **Infrastruktur > Aktivität > Anforderungen** aus.



Vorgehensweise zum Verwalten des Lebenszyklus einer abgeschlossenen vRealize Automation Cloud Assembly-Bereitstellung

Nach dem Bereitstellen und Ausführen einer Bereitstellung stehen Ihnen mehrere Aktionen zur Verfügung, die Sie zum Verwalten der Bereitstellung ausführen können. Die Lebenszyklusverwaltung kann das Ein- und Ausschalten, das Ändern der Größe und das Löschen einer Bereitstellung umfassen. Sie können auch verschiedene Aktionen für einzelne Komponenten ausführen, um diese zu verwalten.

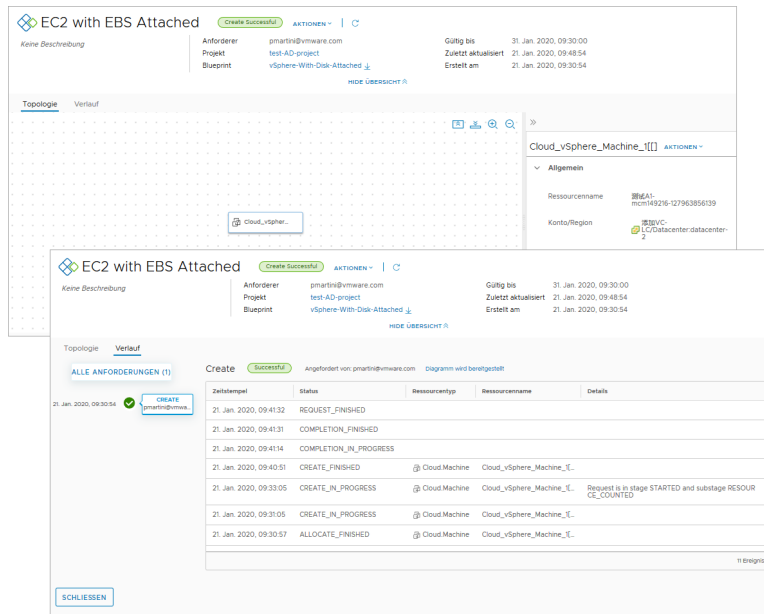
Verfahren

- 1 Klicken Sie auf **Bereitstellungen** und suchen Sie nach der Bereitstellung.
- 2 Klicken Sie für den Zugriff auf die Bereitstellungsdetails auf den Namen der Bereitstellung.

Sie können die Registerkarte „Topologie“ verwenden, um die Bereitstellungsstruktur und die Bereitstellungsressourcen anzuzeigen.

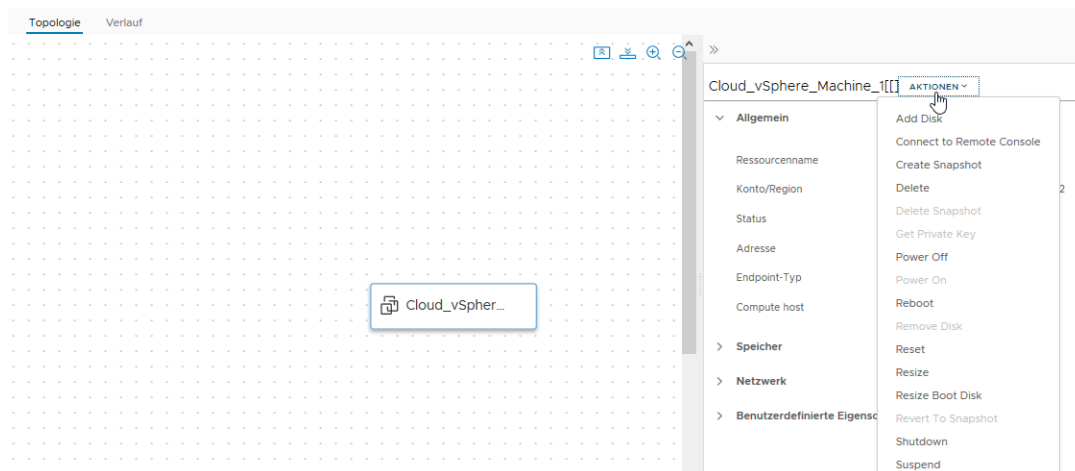
Die Registerkarte „Verlauf“ enthält alle Bereitstellungsereignisse sowie sämtliche Ereignisse, die sich auf Aktionen beziehen, die nach der Bereitstellung des angeforderten Elements ausgeführt wurden. Treten während des Bereitstellungsvorgangs Probleme auf, können Sie die Ereignisse auf der Registerkarte „Verlauf“ zur Fehlerbehebung nutzen.

Auf der Registerkarte „Kosten“ werden die aktuellen Kosten bestimmter Komponenten seit ihrer Bereitstellung angezeigt.



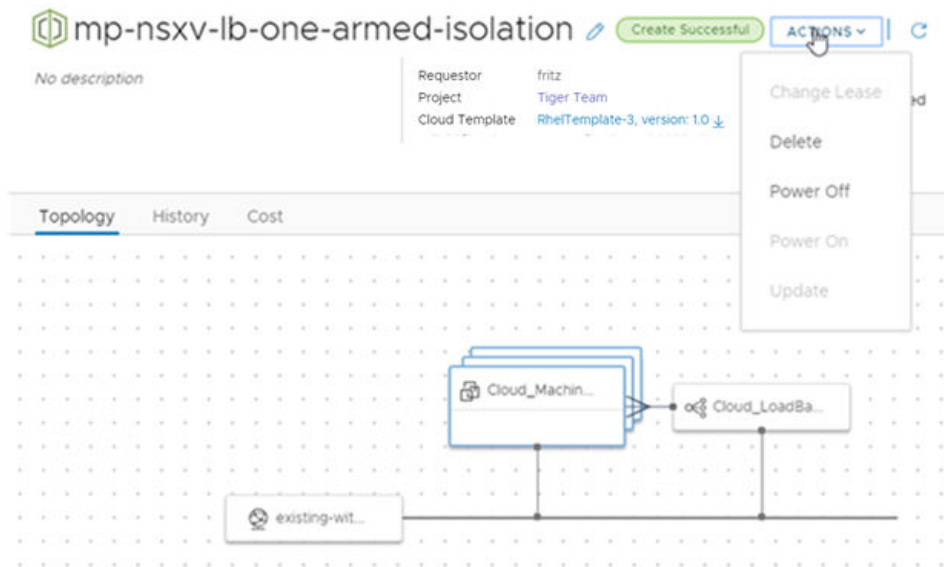
- 3 Wenn Sie feststellen, dass die aktuelle Konfiguration einer Bereitstellung zu kostspielig ist, und Sie die Größe einer Komponente ändern möchten, wählen Sie die Komponente auf der Seite „Topologie“ aus und klicken Sie dann auf der Seite zu der Komponente auf **Aktionen > Größe ändern**.

Die verfügbaren Aktionen richten sich nach der Komponente, dem Cloud-Konto und Ihren Berechtigungen.



- 4 Im Verlauf des Entwicklungslebenszyklus wird eine Ihrer Bereitstellungen nicht mehr benötigt. Um die Bereitstellung zu entfernen und Ressourcen zurückzufordern, wählen Sie **Aktionen > Löschen** aus.

Die verfügbaren Aktionen richten sich nach dem Status der Bereitstellung.



Nächste Schritte

Weitere Informationen über mögliche Aktionen finden Sie unter [Welche Aktionen kann ich auf vRealize Automation Cloud Assembly-Bereitstellungen ausführen?](#).

Welche Aktionen kann ich auf vRealize Automation Cloud Assembly-Bereitstellungen ausführen?

Nachdem Sie Cloud-Vorlagen bereitgestellt haben, können Sie Aktionen in vRealize Automation Cloud Assembly ausführen, um die Ressourcen zu verwalten. Die verfügbaren Aktionen hängen vom Ressourcentyp und davon ab, ob die Aktionen auf einem bestimmten Cloud-Konto oder einer Integrationsplattform unterstützt werden.

Welche Aktionen verfügbar sind, hängt auch davon ab, welche Ausführungsberechtigungen Ihr Administrator Ihnen erteilt hat.

Als Administrator oder Projektadministrator können Sie Richtlinien für Tag-2-Aktionen in vRealize Automation Service Broker einrichten. Weitere Informationen finden Sie im Abschnitt zur [Vorgehensweise für das Erteilen von Berechtigungen an Verbraucher für Service Broker Tag-2-Aktionsrichtlinien](#).

Möglicherweise sehen Sie auch Aktionen, die nicht in der Liste enthalten sind. Dies sind wahrscheinlich benutzerdefinierte Aktionen, die von Ihrem Administrator hinzugefügt wurden. Dies kann beispielsweise eine [Vorgehensweise zum Erstellen einer benutzerdefinierten vRealize Automation Cloud Assembly-Aktion für vMotion einer virtuellen Maschine](#) sein.

Tabelle 7-1. Liste der möglichen Aktionen

Aktion	Gilt für die folgenden Ressourcentypen	Für die folgenden Cloud-Konten oder -Integrationen	Beschreibung
Festplatte hinzufügen	Maschinen	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	Fügt vorhandenen virtuellen Maschinen zusätzliche Festplatten hinzu.
Lease ändern	Bereitstellungen	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Microsoft Azure ■ VMware vSphere 	<p>Ändert das Datum und die Uhrzeit, zu denen die Lease abläuft.</p> <p>Wenn eine Lease abläuft, wird die Bereitstellung gelöscht und die Ressourcen werden zurückgefordert.</p> <p>Lease-Richtlinien werden in vRealize Automation Service Broker festgelegt.</p>
Sicherheitsgruppen ändern	Maschinen	<ul style="list-style-type: none"> ■ VMware vSphere 	<p>Sie können Sicherheitsgruppen mit Maschinennetzwerken in einer Bereitstellung verknüpfen und deren Verknüpfung aufheben. Die Änderungsaktion wird auf vorhandene und bedarfsgesteuerte Sicherheitsgruppen für NSX-V und NSX-T angewendet. Diese Aktion ist nur für Einzelmaschinen und nicht für Maschinencluster verfügbar.</p> <p>Zum Verknüpfen einer Sicherheitsgruppe mit dem Maschinennetzwerk muss die Sicherheitsgruppe in der Bereitstellung vorhanden sein.</p> <p>Durch Trennen einer Sicherheitsgruppe von allen Netzwerken sämtlicher Maschinen in der Bereitstellung wird die Sicherheitsgruppe nicht aus der Bereitstellung entfernt.</p> <p>Diese Änderungen wirken sich nicht auf die Sicherheitsgruppen aus, die im Rahmen der Netzwerkprofile angewendet werden.</p> <p>Mit dieser Aktion wird die Sicherheitsgruppenkonfiguration der Maschine geändert, ohne dass die Maschine neu erstellt wird. Hierbei handelt es sich um eine nicht destruktive Änderung.</p> <p>Sicherheitsgruppen auf einer Maschine ändern</p> <ul style="list-style-type: none"> ■ Wählen Sie zum Ändern der Sicherheitsgruppenkonfiguration die Maschine im Topologiebereich aus. Klicken Sie dann im rechten Bereich auf das Menü Aktion und wählen Sie Sicherheitsgruppen ändern aus. Sie können die Verknüpfung der Sicherheitsgruppen mit den Maschinennetzwerken jetzt hinzufügen oder entfernen.
Mit Remote-Konsole verbinden	Maschinen	<ul style="list-style-type: none"> ■ VMware vSphere 	<p>Öffnen Sie eine Remotesitzung auf der ausgewählten Maschine.</p> <p>Überprüfen Sie die folgenden Anforderungen für eine erfolgreiche Verbindung.</p> <ul style="list-style-type: none"> ■ Stellen Sie als Verbraucher der Bereitstellung sicher, dass die bereitgestellte Maschine eingeschaltet ist.

Tabelle 7-1. Liste der möglichen Aktionen (Fortsetzung)

Aktion	Gilt für die folgenden Ressourcentypen	Für die folgenden Cloud-Konten oder -Integrationen	Beschreibung
Snapshot erstellen	Maschinen	<ul style="list-style-type: none"> ■ Google Cloud Platform ■ VMware vSphere 	<p>Erstellt einen Snapshot der virtuellen Maschine.</p> <p>Wenn Ihnen in vSphere nur zwei Snapshots zur Verfügung stehen und Sie diese bereits erstellt haben, ist dieser Befehl erst wieder verfügbar, nachdem Sie einen Snapshot gelöscht haben.</p>
Löschen	Bereitstellungen	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<p>Löscht eine Bereitstellung.</p> <p>Alle Ressourcen werden gelöscht und anschließend zurückgefordert.</p> <p>Wenn ein Löschvorgang fehlschlägt, können Sie die Löschaktion für eine Bereitstellung ein zweites Mal ausführen. Während des zweiten Versuchs können Sie Fehler beim Löschen ignorieren auswählen. Wenn Sie diese Option auswählen, wird die Bereitstellung gelöscht, aber die Ressourcen werden möglicherweise nicht zurückgefordert. Sie sollten die Systeme, auf denen die Bereitstellung erfolgt ist, daraufhin überprüfen, ob alle Ressourcen entfernt wurden. Ist dies nicht der Fall, müssen Sie die restlichen Ressourcen auf diesen Systemen manuell löschen.</p>
	NSX-Gateway	<ul style="list-style-type: none"> ■ NSX 	Löschen Sie die NAT-Portweiterleitungsregeln aus einem NSX-T- oder NSX-V-Gateway.
	Maschinen und Lastausgleichsdienste	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Microsoft Azure ■ VMware vSphere ■ VMware NSX 	Löscht eine Maschine oder einen Lastausgleichsdienst aus einer Bereitstellung. Diese Aktion könnte dazu führen, dass die Bereitstellung unbrauchbar wird.
	Sicherheitsgruppen	<ul style="list-style-type: none"> ■ NSX-T ■ NSX-V 	<p>Wenn die Sicherheitsgruppe mit keiner Maschine in der Bereitstellung verknüpft ist, entfernt der Prozess die Sicherheitsgruppe aus der Bereitstellung.</p> <ul style="list-style-type: none"> ■ Handelt es sich um eine bedarfsgesteuerte Sicherheitsgruppe, wird sie auf dem Endpoint gelöscht. ■ Handelt es sich um eine freigegebene Sicherheitsgruppe, schlägt die Aktion fehl.
Snapshot löschen	Maschinen	<ul style="list-style-type: none"> ■ VMware vSphere ■ Google Cloud Platform 	Löscht einen Snapshot der virtuellen Maschine.
Tags bearbeiten	Bereitstellungen	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Microsoft Azure ■ VMware vSphere 	Fügt Ressourcen-Tags hinzu oder ändert Ressourcen-Tags, die auf einzelne Bereitstellungsressourcen angewendet werden.

Tabelle 7-1. Liste der möglichen Aktionen (Fortsetzung)

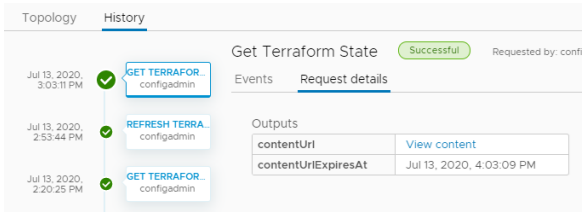
Aktion	Gilt für die folgenden Ressourcentypen	Für die folgenden Cloud-Konten oder -Integrationen	Beschreibung
Terraform-Status abrufen	Terraform-Konfiguration	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<p>Zeigen Sie die Terraform-Statusdatei an.</p> <p>Um Änderungen anzuzeigen, die an den Terraform-Maschinen auf den Cloud-Plattformen, auf denen sie bereitgestellt wurden, vorgenommen wurden, und die Bereitstellung zu aktualisieren, führen Sie zuerst die Aktion „Terraform-Status aktualisieren“ und dann die hier beschriebene Aktion „Terraform-Status abrufen“ aus.</p> <p>Wenn die Datei in einem Dialogfeld angezeigt wird, ist die Datei für ca. 1 Stunde verfügbar. Danach müssen Sie eine weitere Aktualisierungsaktion durchführen. Sie können die Datei kopieren, wenn Sie sie zur späteren Verwendung benötigen.</p> <p>Sie können die Datei auch auf der Registerkarte „Bereitstellungsverlauf“ anzeigen. Wählen Sie auf der Registerkarte „Ereignisse“ das Ereignis „Terraform-Status abrufen“ aus und klicken Sie auf Anforderungsdetails. Wenn die Datei nicht abgelaufen ist, klicken Sie auf Inhalt anzeigen. Wenn die Datei abgelaufen ist, können Sie die Aktionen zum Aktualisieren und Abrufen erneut ausführen.</p>
			
<p>Sie können für die in die Konfiguration eingebetteten Terraform-Ressourcen andere Tag-2-Aktionen ausführen. Welche Aktionen verfügbar sind, hängt vom Ressourcentyp, der Cloud-Plattform, auf der sie bereitgestellt werden, und davon ab, ob Sie dazu berechtigt sind, die Aktionen basierend auf einer Tag-2-Richtlinie auszuführen.</p>			
Ausschalten	Bereitstellungen	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Microsoft Azure ■ VMware vSphere 	Schaltet die Bereitstellung aus, ohne das Gastbetriebssystem herunterzufahren.
	Maschinen	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	Schaltet die virtuelle Maschine aus, ohne die Gastbetriebssysteme herunterzufahren.
Einschalten	Bereitstellungen	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Microsoft Azure ■ VMware vSphere 	Schaltet die Bereitstellung ein. Wenn die Ressourcen angehalten wurden, wird der normale Betrieb an dem Punkt fortgesetzt, an dem die Ressourcen angehalten wurden.

Tabelle 7-1. Liste der möglichen Aktionen (Fortsetzung)

Aktion	Gilt für die folgenden Ressourcentypen	Für die folgenden Cloud-Konten oder -Integrationen	Beschreibung
	Maschinen	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	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	Maschinen	<ul style="list-style-type: none"> ■ Amazon Web Services ■ VMware vSphere 	<p>Startet das Gastbetriebssystem auf einer virtuellen Maschine neu.</p> <p>VMware Tools muss auf einer vSphere-Maschine installiert sein, damit diese Aktion verwendet werden kann.</p>
Neu konfigurieren	Lastausgleichsdienste	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Microsoft Azure ■ VMware NSX 	<p>Ändern Sie die Größe des Lastausgleichsdiensts und die Protokollierungsebene.</p> <p>Sie können auch Routen hinzufügen oder entfernen sowie das Protokoll, den Port, die Systemzustandskonfiguration und die Mitgliederpooleinstellungen ändern.</p>
	Portweiterleitung für NSX-Gateway	<ul style="list-style-type: none"> ■ NSX-T ■ NSX-V 	Fügen Sie die NAT-Portweiterleitungsregeln zu einem NSX-T- oder NSX-V-Gateway hinzu, bearbeiten oder löschen Sie diese.
Terraform-Status aktualisieren	Terraform-Konfiguration	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<p>Rufen Sie die neueste Iteration der Terraform-Statusdatei ab.</p> <p>Um Änderungen abzurufen, die an den Terraform-Maschinen auf den Cloud-Plattformen, auf denen sie bereitgestellt wurden, vorgenommen wurden, und die Bereitstellung zu aktualisieren, führen Sie zuerst die Aktion „Terraform-Status aktualisieren“ aus.</p> <p>Um die Datei anzuzeigen, führen Sie die Aktion Terraform-Status abrufen für die Konfiguration aus.</p> <p>Verwenden Sie die Registerkarte „Bereitstellungsverlauf“, um den Aktualisierungsvorgang zu überwachen.</p>
Festplatte entfernen	Maschinen	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	Entfernt Festplatten von vorhandenen virtuellen Maschinen.
Zurücksetzen	Maschinen	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Google Cloud Platform ■ VMware vSphere 	Erzwingt den Neustart einer virtuellen Maschine, ohne das Gastbetriebssystem herunterzufahren.
Größe anpassen	Maschinen	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Microsoft Azure ■ Google Cloud Platform ■ VMware vSphere 	Erhöht oder verringert die CPU und den Arbeitsspeicher einer virtuellen Maschine.

Tabelle 7-1. Liste der möglichen Aktionen (Fortsetzung)

Aktion	Gilt für die folgenden Ressourcentypen	Für die folgenden Cloud-Konten oder -Integrationen	Beschreibung
Größe von Startlaufwerk ändern	Maschinen	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	Vergrößert oder verkleinert das Startlaufwerk.
Festplattenengröße ändern	Speicherfestplatte	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Google Cloud Platform 	Erhöht die Kapazität einer Speicherfestplatte.
Neu starten	Maschinen	<ul style="list-style-type: none"> ■ Microsoft Azure 	Führt eine ausgeführte Maschine herunter und startet sie neu.
Snapshot wiederherstellen	Maschinen	<ul style="list-style-type: none"> ■ Google Cloud Platform ■ VMware vSphere 	Stellt einen vorherigen Snapshot der Maschine wieder her. Es muss ein Snapshot vorhanden sein, damit Sie diese Aktion ausführen können.
Puppet-Aufgabe durchführen	Verwaltete Ressourcen	<ul style="list-style-type: none"> ■ Puppet Enterprise 	Führt die ausgewählte Aufgabe auf Maschinen in Ihrer Bereitstellung aus. Die Aufgaben werden in Ihrer Puppet-Instanz definiert. Sie müssen in der Lage sein, die Aufgabe zu erkennen und die Eingabeparameter anzugeben.
Herunterfahren	Maschinen	<ul style="list-style-type: none"> ■ VMware vSphere 	Führt das Gastbetriebssystem herunter und schaltet die Maschine aus. VMware Tools muss auf der Maschine installiert sein, damit diese Aktion verwendet werden kann.
Anhalten	Maschinen	<ul style="list-style-type: none"> ■ Microsoft Azure ■ VMware vSphere 	Hält die Maschine an, damit sie nicht verwendet werden kann und keine Systemressourcen außer dem verwendeten Speicher verbraucht.
Aktualisieren	Bereitstellungen	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Microsoft Azure ■ VMware vSphere 	Ändert die Bereitstellung basierend auf den Eingabeparametern. Ein Beispiel finden Sie unter Vorgehensweise zum Verschieben einer bereitgestellten Maschine in ein anderes Netzwerk .
Tags aktualisieren	Maschinen und Festplatten	<ul style="list-style-type: none"> ■ Amazon Web Services ■ Microsoft Azure ■ VMware vSphere 	Fügt ein Tag hinzu, das auf eine einzelne Ressource angewendet wird, bearbeitet es oder löscht es.