

Using and Managing vRealize Automation Cloud Assembly

October 2022

vRealize Automation 8.2

You can find the most up-to-date technical documentation on the VMware website at:

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

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

Copyright © 2022 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

1	What is vRealize Automation Cloud Assembly	7
	How does vRealize Automation Cloud Assembly work	8
2	Tutorials	11
	Setting up and testing vSphere infrastructure and deployments	13
	Configuring and provisioning a production workload	31
	Multi-cloud infrastructure and deployments	38
	Part 1: Configure the example infrastructure	39
	Part 2: Create the example project	45
	Part 3: Design and deploy the example cloud template	46
	Configuring VMware Cloud on AWS	63
	Configure a basic VMware Cloud on AWS workflow	63
	Configure an isolated network in VMware Cloud on AWS	76
	Configuring an external IPAM integration for Infoblox	80
	Add required extensible attributes in the Infoblox application before deploying the download package	82
	Download and deploy an external IPAM provider package	83
	Create a running environment for an IPAM integration point	85
	Add an external IPAM integration for Infoblox	86
	Configure a network and network profile to use external IPAM for an existing network	90
	Define and deploy a cloud template that uses an external IPAM provider range assignment	92
	Using Infoblox-specific properties for IPAM integrations	95
3	Setting up vRealize Automation Cloud Assembly for your organization	98
	What are the vRealize Automation user roles	98
	Organization and service user roles	100
	Custom user roles	114
	Use cases: How can user roles help me control access	117
	Adding cloud accounts	137
	Credentials required for working with cloud accounts	138
	Create a Microsoft Azure cloud account	155
	Create an Amazon Web Services cloud account	156
	Create a Google Cloud Platform cloud account	157
	Create a vCenter cloud account	158
	Create an NSX-V cloud account	160
	Create an NSX-T cloud account	161
	Create a VMware Cloud on AWS cloud account	164

Create a VMware Cloud Foundation cloud account	165
Integrating with other applications	167
How do I use GitLab and GitHub integration	167
How to configure an external IPAM integration	173
How to upgrade to a newer external IPAM integration package	175
Configure MyVMware integration in vRealize Automation Cloud Assembly	176
Configure vRealize Orchestrator integration in Cloud Assembly	176
How do I work with Kubernetes in vRealize Automation Cloud Assembly	179
What Is configuration management in vRealize Automation Cloud Assembly	196
How do I create an Active Directory integration in vRealize Automation Cloud Assembly	205
Configure a VMware SDDC Manager integration	207
Integrating with vRealize Operations Manager	208
What are onboarding plans	216
Onboard selected machines as a single deployment	217
Onboard rule-filtered machines as separate deployments	219
Advanced configuration	225
How do I configure an Internet proxy server	225
What can I do with NSX-T mapping to multiple vCenters	229
What happens if I remove an NSX cloud account association	230
How do I use the IPAM SDK to create a provider-specific external IPAM integration package	230

4 Building your resource infrastructure 232

How to add cloud zones	232
Learn more about cloud zones	233
How to add flavor mappings	235
Learn more about flavor mappings	236
How to add image mappings	236
Learn more about image mappings	236
How to add network profiles	239
Learn more about network profiles	240
Using network settings	246
Using security group settings	250
Using load balancer settings	252
How do I configure a network profile to support an on-demand network for an external IPAM integration	253
How do I configure a network profile to support an existing network for an external IPAM integration	256
How to add storage profiles	256
Learn more about storage profiles	256
How to use tags	257
Creating a tagging strategy	260

Using capability tags in vRealize Automation Cloud Assembly	262
Using constraint tags in vRealize Automation Cloud Assembly	262
Standard tags	264
How vRealize Automation Cloud Assembly processes tags	265
How do I set up a simple tagging structure	266
How to work with resources	268
Compute resources	268
Network resources	268
Security resources	270
Storage resources	271
Machine resources	272
Volume resources	272
Learn more about resources	273
Configuring Multi-provider tenant resources with vRealize Automation	285
How do I create a Virtual Private Zone for vRealize Automation	286
Manage VPZ configuration for vRealize Automation tenants	288
5 Adding and managing projects	291
How do I add a project for my development team	291
Learn more about projects	293
Using project tags and custom properties	293
How do projects work at deployment time	295
6 Designing your deployments	297
Ways to create cloud templates	298
How to create a simple cloud template from scratch	300
How to select and add resources to a cloud template	301
How to connect cloud template resources	301
How to create valid cloud template code	302
How to save different versions	304
How to enhance a simple cloud template	306
How user input can customize a cloud template	307
How resource flags can customize a request	312
How to set the resource deployment sequence	314
How to use expressions to make cloud template code more versatile	315
How to enable remote access in cloud templates	324
How to add advanced features to designs	327
How to customize the names of deployed resources	328
How to automatically initialize a machine in a cloud template	330
How to create custom resource types to use in cloud templates	343
How to prepare for day 2 changes	354

How to extend and automate application life cycles with extensibility	360
What are the resource properties	398
What are some code examples	399
vSphere resource examples in cloud templates	399
Reviewable cloud template	402
Network, security, and load balancer examples in cloud templates	409
Puppet enabled cloud template with username and password access	430
How to include Terraform configurations	439
Preparing a Terraform runtime environment	439
Preparing for Terraform configurations	445
Designing for Terraform configurations	447
Learn more about Terraform configurations	450
How to use the Marketplace	453
7 Managing deployments	454
How do I monitor deployments	455
What can I do if a vRealize Automation Cloud Assembly deployment fails	456
How do I manage the life cycle of a completed deployment	459
What actions can I run on deployments	461

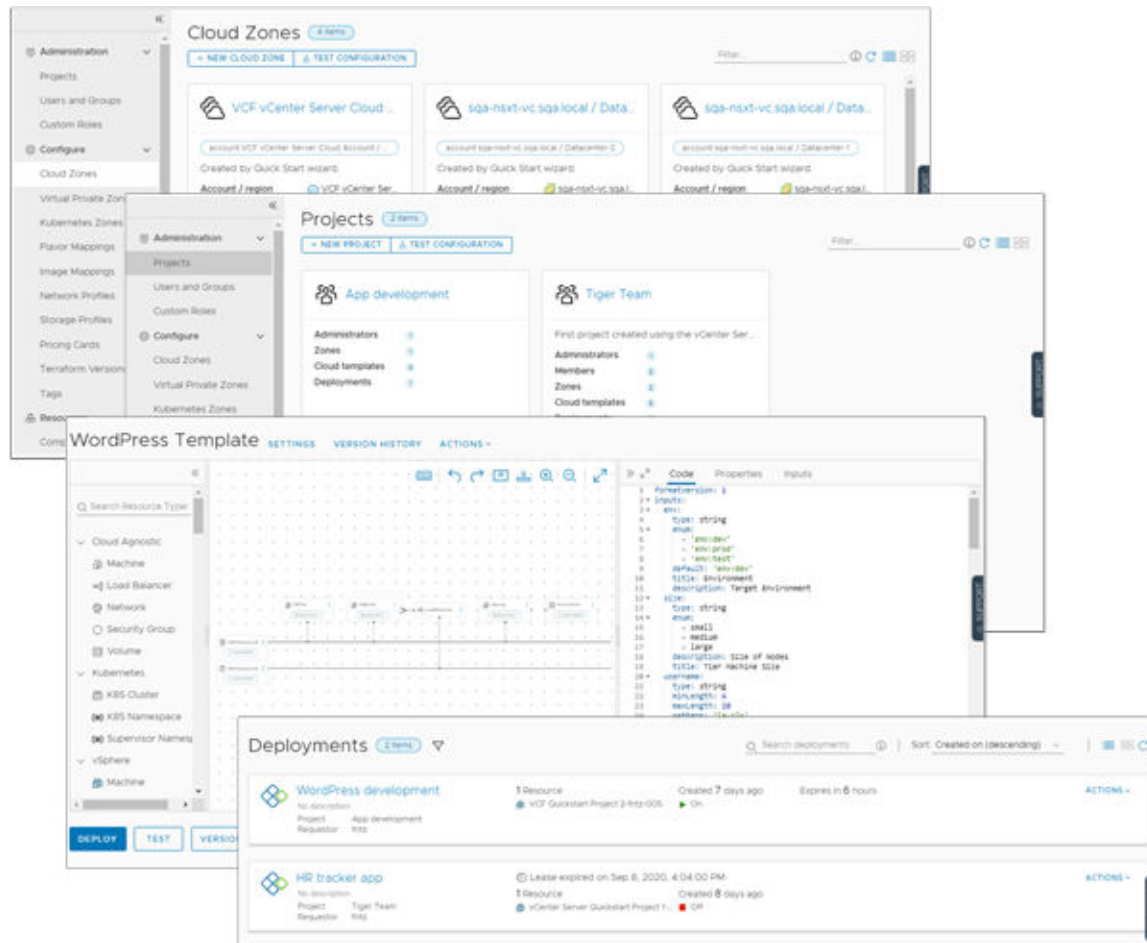
What is vRealize Automation Cloud Assembly

1

You use vRealize Automation Cloud Assembly to connect to your public and private cloud providers so that you can deploy machines, applications, and services that you create to those resources. You and your teams develop cloud-templates-as-code in an environment that supports an iterative workflow, from development to testing to production. At provisioning time, you can deploy across a range of cloud vendors. The service is a managed VMware SaaS and NaaS-based framework.

An overview of vRealize Automation Cloud Assembly includes the following basic functions.

- The Infrastructure tab is where you add and organize your cloud vendor resources and users. This tab also provides information about deployed cloud templates.
- The Marketplace tab provides VMware Solution Exchange cloud templates and images that help you build your template library and access supporting OVA or OVFs.
- The Design tab is your development home. You use the canvas and the YAML editor to develop and then deploy your machines and applications.
- The Deployments tab shows the current status of your provisioned resources. You can access details and history that you use to manage your deployments.



This chapter includes the following topics:

- [How does vRealize Automation Cloud Assembly work](#)

How does vRealize Automation Cloud Assembly work

vRealize Automation Cloud Assembly is a cloud template development and deployment service. You and your teams use the service to deploy machines, applications, and services to your cloud vendor resources.

As a Cloud Assembly administrator, generally referred to as a cloud administrator, you set up the provisioning infrastructure and create the projects that group users and resources.

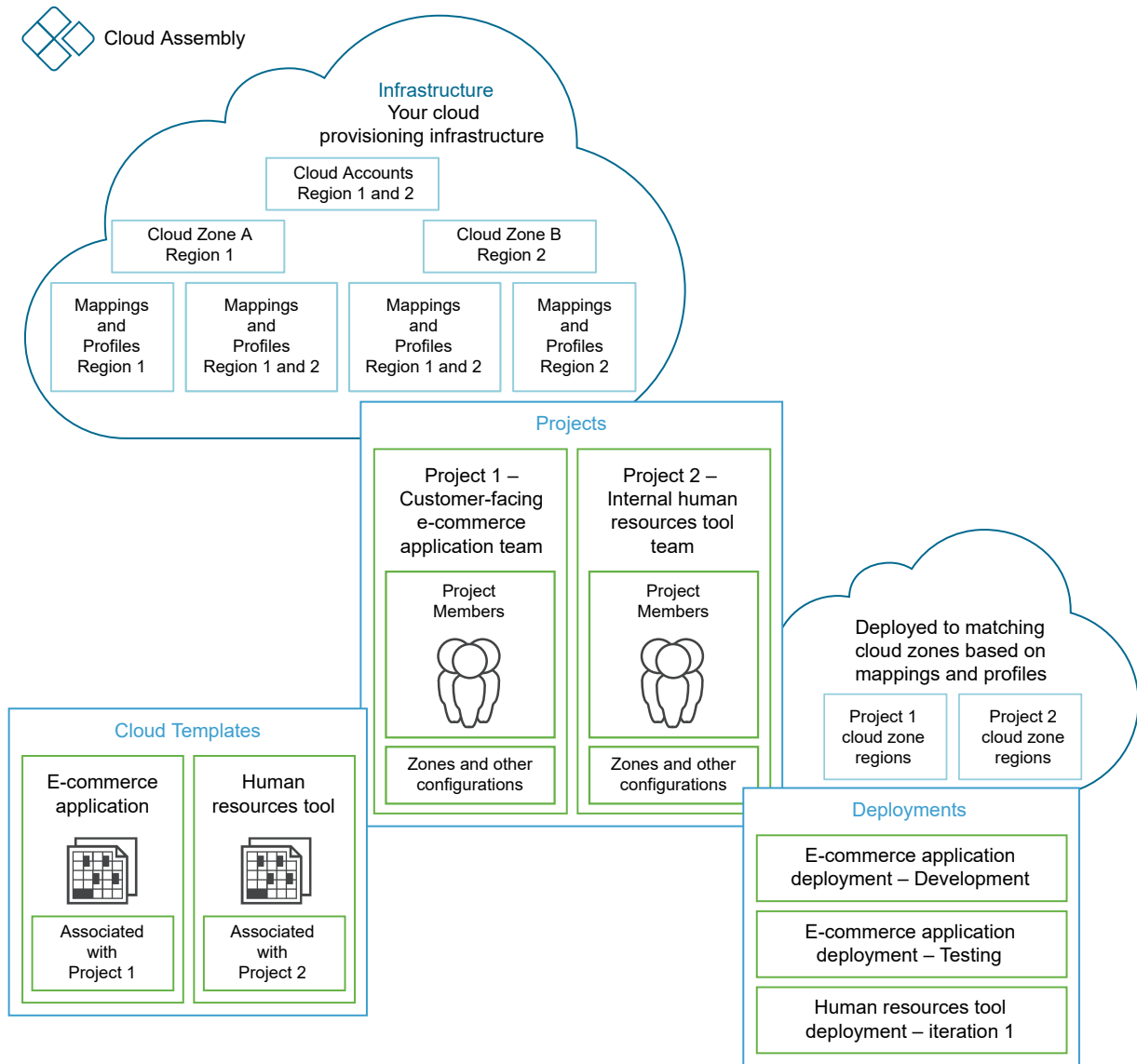
- Add your cloud vendor accounts. See [Adding cloud accounts to vRealize Automation Cloud Assembly](#).
- Determine which regions or datastores are the cloud zones that you want your developers deploying to. See [Learn more about vRealize Automation Cloud Assembly cloud zones](#).
- Create policies that define the cloud zones. See [Chapter 4 Building your vRealize Automation Cloud Assembly resource infrastructure](#).

- Create projects that group the developers with the cloud zones. See [Using vRealize Automation Cloud Assembly project tags and custom properties](#) .

As a cloud template developer, you are a member of one or more projects. You create and deploy templates to the cloud zones associated with one of your projects.

- Develop cloud templates for projects using the canvas. Your project administrator can use the marketplace to download templates and supporting images from the VMware Solution Exchange. See [Chapter 6 Designing your vRealize Automation Cloud Assembly deployments](#) and [How to use the vRealize Automation Cloud Assembly Marketplace](#) .
- Deploy your cloud templates to project cloud zones based on policies and constraints.
- Manage your deployments, including deleting unused applications. See [Chapter 7 Managing vRealize Automation Cloud Assembly deployments](#).

Welcome to vRealize Automation Cloud Assembly. If you want an example of how to define the infrastructure, and then create and deploy a cloud template, see [Tutorial: Setting up and testing multi-cloud infrastructure and deployments in vRealize Automation Cloud Assembly](#).



Cloud Assembly Tutorials

2

The tutorials show you how to perform common tasks that help you become proficient with vRealize Automation Cloud Assembly.

As you begin, a reminder that in addition to the steps in the tutorials, there is additional information in this guide. Links are provided to relevant topics.

Accessing user assistance

Equally important, user assistance is provided throughout the application. The user assistance helps you understand features and provides information that helps you make decisions about how to populate text boxes. The external documentation provides greater depth, code samples, and use cases.

Assistance type	How to access assistance	Example
Field-level signpost help	Click the Info icon (i) beside a field.	
Contextual support panel help	Click the Help icon (?) beside your name and organization.	
Access the external documentation	Click an article title that is labeled Docs or click the View More in VMware Docs.	

This chapter includes the following topics:

- Tutorial: Setting up and testing vSphere infrastructure and deployments in vRealize Automation Cloud Assembly
- Tutorial: Configuring vRealize Automation Cloud Assembly to provision a production workload
- Tutorial: Setting up and testing multi-cloud infrastructure and deployments in vRealize Automation Cloud Assembly
- Tutorial: Configuring VMware Cloud on AWS for vRealize Automation
- Tutorial: Configuring a provider-specific external IPAM integration for vRealize Automation

Tutorial: Setting up and testing vSphere infrastructure and deployments in vRealize Automation Cloud Assembly

If you are new to vRealize Automation or only need a refresher course, this tutorial guides you through the vRealize Automation Cloud Assembly configuration process. You add cloud vSphere account endpoints, define the infrastructure, add users to projects, and then design and deploy a workload by using VMware Cloud Templates based on vSphere resource types, learning the process along the way.

Although this tutorial is just the beginning, you are on the path to delivering self-service automation and iterative development that works across multiple public and private clouds. This tutorial focuses on VMware vCenter Server and NSX-T. After you finish this workflow, you can apply what you've learned to add more types of cloud accounts and deliver more sophisticated cloud templates.

As you work your way through the steps, we provide data examples. Replace the examples with values that work in your environment.

You perform all the steps in this tutorial in vRealize Automation Cloud Assembly.

This tutorial guides you as you configure each required component.

- **Step 1: Add the vCenter Server and NSX cloud accounts.** Cloud accounts are the credentials that connect vRealize Automation Cloud Assembly to your cloud vendor endpoints.
- **Step 2: Define the cloud zone compute resources.** Cloud zones are the selected compute resources in account/regions that you then assign to different projects based on the project needs and your goals for managing compliance and costs.
- **Step 3: Configure the possible resources that are available for the account/region.** Infrastructure resources are definitions of the compute, storage, network, and other resources associated with account/regions that are used in cloud templates.
- **Step 4: Create a project.** Projects are how you give your users access to the cloud zones based on the project's application development goals.
- **Step 5: Design and deploy a basic cloud template.** Cloud templates are the definitions of your application workloads that you iteratively develop and deploy.

This configuration process is the foundation of your Cloud Assembly development experience. As you build your infrastructure and mature your cloud template development skills, you will repeat and expand on this workflow.

Before you begin

- Verify that you have the Cloud Assembly Administrator role. See [Organization and service user roles in vRealize Automation](#).
- If you have not used the VMware vCenter Server or the VMware Cloud Foundation Quickstart wizards in the vRealize Automation console, you can do so now.

These wizard-driven workflows include most but not all of the configuration in this tutorial.

This tutorial is a hands-on experience that adds to your understanding of how to put together a working infrastructure and deploy a workload.

See [How do I set up Cloud Assembly](#) in the *Getting Started* guide.

- If you have not yet used the guided setup that is available in vRealize Automation Cloud Assembly, you can do it now. The guided setup takes you through most but not all of the procedures that you do in this tutorial. To open the guided setup, click **Guided Setup** on the right side of the tab bar.
- Ensure that you have vCenter Server and NSX credentials. For more information about the permissions that the credentials must have, see [Credentials required for working with cloud accounts in vRealize Automation](#). If you plan to add additional users to projects, verify that they are members of the vRealize Automation Cloud Assembly service.

Step 1: Add the vCenter Server and NSX cloud accounts

The cloud accounts provide the credentials that vRealize Automation uses to connect to vCenter Server and the associated NSX server.

1 Add the vCenter Server cloud account.

The vCenter Server cloud account provides the vCenter credentials that vRealize Automation Cloud Assembly uses to discover resources and deploy cloud templates.

For additional information about vCenter Server cloud accounts, see [Create a vCenter cloud account in vRealize Automation](#).

- a Select **Infrastructure > Connections > Cloud Accounts**.
- b Click **Add Cloud Account** and select **vCenter**.
- c Enter the values.

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 🔍 Search for cloud accounts

Capabilities

Capability tags Enter capability tags ⓘ

ADD **CANCEL**

Remember that these values are only examples. Your values will be specific to your environment.

Setting	Sample Value
Name	vCenter Server Account
vCenter IP address / FQDN	your-dev-vcenter.company.com
Username and Password	vCenterCredentials@yourCompany.com

- d To verify the credentials, click **Validate**.
 - e To **Allow provisioning to these datacenters**, select one or more data centers.
 - f Skip the NSX cloud account. We'll configure that later, linking the vCenter Server account to the NSX cloud account.
 - g Click **Add**.
- 2 Add an associated NSX cloud account.

The NSX-T cloud account provides the NSX-T credentials that vRealize Automation Cloud Assembly uses to discover network resources and deploy networks with cloud templates.

For more information about NSX-T cloud accounts, see [Create a vCenter cloud account in vRealize Automation](#).

- a Select **Infrastructure > Connections > Cloud Accounts**.
- b Click **Add Cloud Account** and select either NSX-T or NSX-V. This tutorial uses **NSX-T**.
- c Enter the values.

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

These values are only examples. Your values will be specific to your environment.

Setting	Sample Value
Name	NSX-T Account
vCenter IP address / FQDN	your-dev-NSX-vcenter.company.com
Username and Password	NSXCredentials@yourCompany.com
NSX mode	<p>Don't know what to select?</p> <p>Here's a great opportunity to use the in-product help. Click the information icon to the right of field. Notice that the field-level help includes information that can help you configure the option.</p> <p>In this example, select Policy.</p>

- d To verify the credentials, click **Validate**.
- e To associate the vCenter cloud account you created in the previous step, click **Add** and then select the **vCenter Account**.

This vCenter cloud account association ensures network security.

- f On the NSX cloud account page, click **Add**.

Step 2: Define the cloud zone compute resources


The cloud zones are groups of compute resources in an account/region that are then made available to projects. The project members deploy cloud templates by using the resources in the assigned cloud zones. If you want to have more granular control over where project cloud templates are deployed, you can create multiple cloud zones with different compute resources.

Account/regions are how cloud vendors tie resources to isolated regions or datastores. The account indicates the cloud account type and the region indicates the region or datastore. vCenter Server uses datastores and the provisioning resources are the selected clusters and resource pools.

For this tutorial, you must ensure that the cloud zones include the resources that support the goals of the project development team, and your budget and management requirements.

For more information about cloud zones, see [Learn more about vRealize Automation Cloud Assembly cloud zones](#).

- 1 Select **Infrastructure > Configure > Cloud Zones**.
- 2 Click the cloud zone that was added for your vCenter Server instance and enter the values.


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 / wld01-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

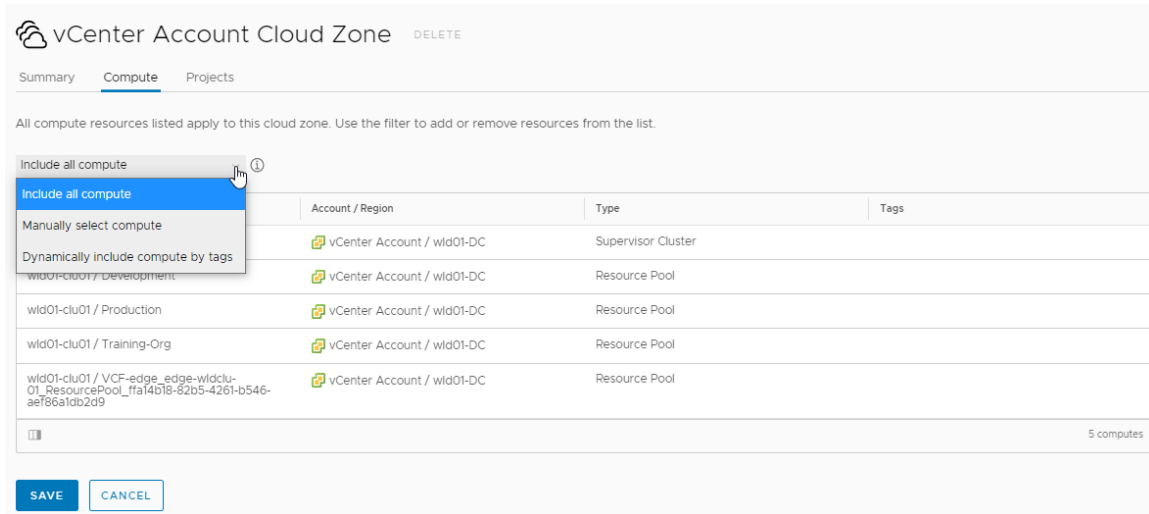
CANCEL

Setting	Sample Value
Account / region	vCenter Account / data center name
Name	vCenter Server Cloud Zone This value cannot be changed after you create it. If you want to configure a different data center for a different vCenter Server, you must create a new cloud zone where you can select the account/region.
Description	All vCenter Server compute resources for development.
Policy	Default Don't forget to consult the help if you have questions about a field value.

Remember that all values are only examples. Your zone specifics will be specific to your environment.

- Click the **Compute** tab and verify that the compute resources are all present.

If you need to exclude one, switch to **Manually select compute** and add only the ones you want to include in the cloud zone.



- 4 Click **Save**.
- 5 Repeat the process for any additional cloud zones, but you must ensure unique zone names.

Step 3: Configure the possible resources that are available for the account/region

You added the account/region to the cloud zone. Now you define the possible machine sizes (flavor mappings), image mappings, network profiles, and storage profiles for the cloud account. The mapping and profile definitions are evaluated for a match when you deploy a cloud template, ensuring that the workload includes the appropriate machine size (flavor), image, networks, and storage.

- 1 Configure the flavor mappings for the account/regions.

Flavors are sometimes referred to as t-shirt sizing. Depending on how your cloud template is configured, the applied flavor mapping determines the number of CPUs and memory.

For more information about flavor mappings, see [Learn more about flavor mappings in vRealize Automation](#).

- a Select **Infrastructure > Configure > Flavor Mappings**.
- b Click **New Flavor Mapping** and enter values that define small, medium, and large machines.

Remember, these are sample values. You must select relevant account/regions and define the sizing.

small DELETE

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

Flavor name * small

Configuration *

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

Setting	Sample Value
Flavor name	small
Account/region	vCenter Account / data center
CPU value	2
Memory value	1 GB

- c Click **Create**.
- d To create additional sizes, configure medium and large flavor mappings for the account/region.

Setting	Sample Value
Flavor name	medium
Account/region	vCenter Account / Datacenter
CPU value	4
Memory value	2 GB
Flavor name	large
Account/region	vCenter Account / Datacenter
CPU value	8
Memory value	4 GB

- 2 Configure the image mappings for the account/regions.

The images are the operating system for machines in the cloud template. When you are working with vCenter Server images, you select vCenter templates.

For more information about image mappings, see [Learn more about image mappings in vRealize Automation](#).

- a Select **Infrastructure > Configure > Image Mappings**.
- b Click **New Image Mapping** and search for the images for the account/region.

Remember, these are sample values. You must select relevant images that were discovered in your account/region.

Setting	Sample Value
Image name	centos
Account/region	vCenter Account
Image	centos7


- c Click **Create**.
- d Repeat the process to create additional image mappings. For example, an ubuntu mapping for the account/region.

3 Configure network profiles.

Network profiles define the networks and network settings that are available for an account/region. The profiles must support the target deployment environments.


This task provides the minimum configuration information for success. If you want more information about network profiles, start with [Learn more about network profiles in vRealize Automation](#).

- a Select **Infrastructure > Configure > Network Profile**.
- b Click **New Network Profile** and create a profile for the vCenter Account / Datacenter account/region.

 **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 * Network Profile


Description Networks for development teams.

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


Capability tags Enter capability tags 

Setting	Sample Value
Account/region	vCenter Account / Datacenter
Name	Network Profile
Description	Networks for development teams.







- c Click the **Networks** tab and click **Add Network**.

 **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-c8e2a5589de-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 Select the NSX networks that you want to make available for the application development team.

In this example, we had an NSX-T network named DevProject-004.

- e Click the **Network Policies** tab and create a policy.

Setting	Sample Value
Isolation policy	None
Tier-0 logical router	Tier-0-router
Edge cluster	EdgeCluster

f Click **Create**.

4 Configure storage profiles.

Storage profiles define the disks for an account/region. The profiles must support the target deployment environments.

If you want more information about storage profiles, see with [Learn more about storage profiles in vRealize Automation](#).

- a Select **Infrastructure > Configure > Storage Profile**.
- b Click **New Storage Profile** and create a profile for the vCenter Server/Datacenter account/region.

Unless specified in the table, keep the default values.

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: Q_ 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**

Setting	Sample Value
Account/region	vCenter Account / Datacenter
Name	Storage Profile
Datastore/cluster	Selected a datastore with sufficient capacity and that is accessible to all the hosts.
Preferred storage for this region	Select the check box.

- c Click **Create**.

Step 4: Create a project

This is where you really begin thinking about the project goals.

- What users need access to the compute resources so that they can create and deploy an application cloud template? For more information about what the different project roles can see and do, see [Organization and service user roles in vRealize Automation](#).
- Will the members of the project be creating applications that go from development to production? What are the necessary resources?
- What cloud zones do they need? What priority and limits should be placed on each zone for the project?

For this tutorial, we are going to support the Development team as they create and extend an in-house software application.

This task provides the minimum configuration information for success. If you want more information about projects, start with [Learn more about vRealize Automation Cloud Assembly projects](#).

- 1 Select **Infrastructure > Administration > Projects**.
- 2 Click **New Project** and enter the name **Development Project**.
- 3 Click the **Users** tab, and then click **Add Users**.

You are not required to add users at the time. But if you want other users to work with cloud templates, they must be a member of the project.

- 4 Enter email addresses to add users as project members or administrators, depending on what permissions you want each individual to have.

- 5 Click **Provisioning** and click **Add Zones > Cloud Zone**.
- 6 Add the cloud zones that the users can deploy to.

You can also set resource limits for the cloud zone in the project. In the future, you can set different limits for other projects.

Project Cloud Zone Setting	Sample Value
Cloud Zone	vCenter Account Cloud Zone
Provisioning priority	1
Instance limit	5

- 7 Add any additional cloud zones to the project.
- 8 Click **Create**.

- 9 To verify that the project was added to the cloud zone, select **Infrastructure > Configure > Cloud Zones** and open the vCenter Account Zone cloud Zone card so that you can examine the **Projects** tab. You should see the Development Project.

Step 5: Design and deploy a basic cloud template

You design and deploy the cloud template to ensure that your infrastructure is properly configured to support the template. Later you can build on the template as you create an application that meets your project needs.

The best way to build a cloud template is component-by-component, verifying that it deploys between each change. This tutorial starts with a simple machine and then iteratively adds more resources.

The examples in this procedure use the YAML code editor. It is an easier way of providing you with code snippets. However, if you prefer a use dialog box-driven user interface, click **Inputs**.

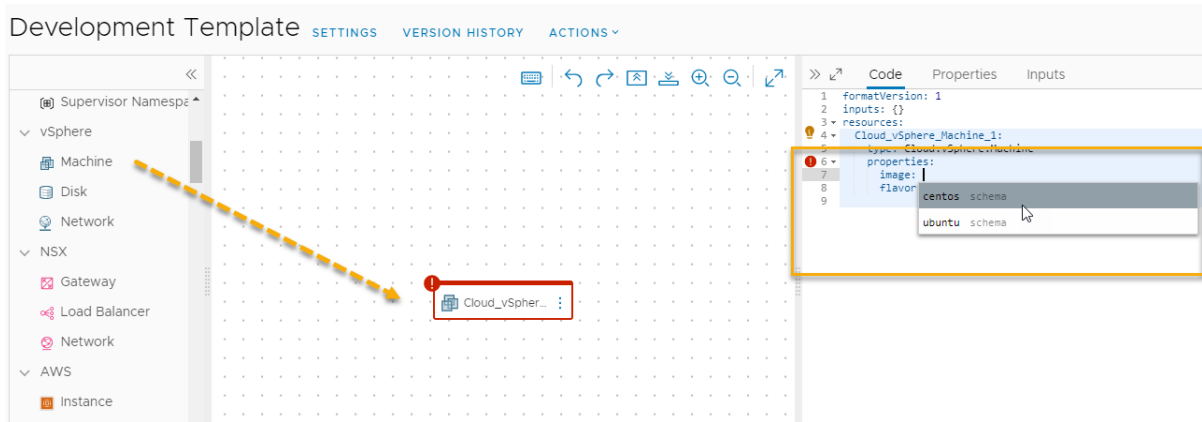
There is so much more that you can do with cloud templates than is provided in this tutorial. If you want more information, start with [Chapter 6 Designing your vRealize Automation Cloud Assembly deployments](#).

This tutorial uses vSphere and NSX resource types. These resource types can be deployed only on vCenter Server cloud account endpoints. You can also use the cloud agnostic resource types to create cloud templates that can be deployed on any endpoint. For an example of how to configure the infrastructure and design the template for any endpoint, see [Tutorial: Setting up and testing multi-cloud infrastructure and deployments in vRealize Automation Cloud Assembly](#).



For a video that illustrates the basic steps in this procedure, see [How to design and deploy a basic cloud template](#).

- 1 Select **Design > Cloud Templates**.
- 2 Select **New From > Blank Canvas**.
- 3 Enter the **Name Development Template**, select the **Project Development Project**, and click **Create**.
- 4 Add a vSphere machine to the design canvas, test, and deploy.



- a From the resource type pane, drag a **vSphere Machine** to the canvas.

Notice that the **Code** pane shows the YAML for the machine, with an empty value for image and predefined CPU and memory properties. You are going to make this template able to support flexible sizing.

- b To select an image value, put your pointer between the single quotes for `image` and select **centos** from the list of images that you configured.

Remember, these are sample values. If you did not configure a centos image, select an image that you did configure.

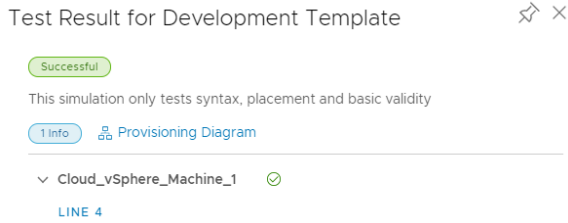
- c Create a line below the image property and enter or select `flavor`, then select the `small` from the list.
- d Delete `cpuCount` and `totalMemory`.

Your YAML should look similar to this example.

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

- e Click **Test**.

Test allows you to validate the syntax and placement of your cloud template. A successful test does not mean that you can deploy the template without errors.



If the test fails, click **Provisioning Diagram** and look for the failure points. For more information about using the diagram to troubleshoot, see [Test a basic cloud template](#).

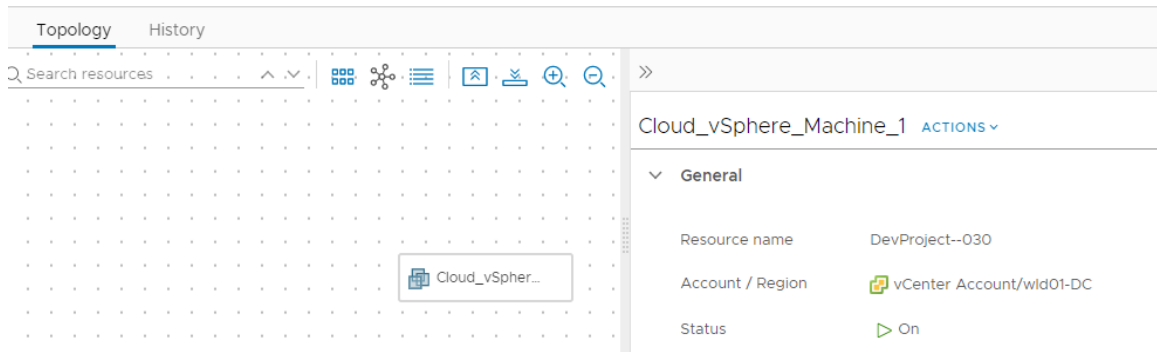
f Click **Deploy**.

g Enter **Deployment Name** as **DevTemplate - machine** and click **Deploy**.

You can track the progress of the deployment on the DevTemplate deployment details page or on the Deployments tab.

If the deployment fails, you can troubleshoot the problem and revise your template. See [What can I do if a vRealize Automation Cloud Assembly deployment fails](#).

A successful deployment looks similar to this example on the Deployments tab.



5 Version the template and add a network.

Versioning a cloud template is required to make it available in the Service Broker catalog, but it is useful to have a good version to revert to during development.

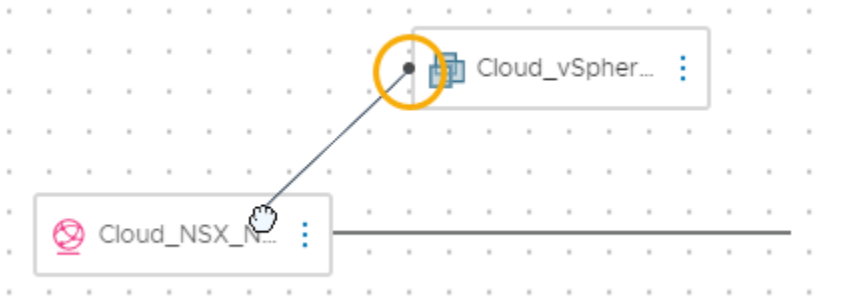
a Open the template in the design canvas.

b Click **Version**, enter a **Description** similar to **Simple deployable machine**, and click **Create**.

c From the resource type pane, drag an **NSX Network** resource type to the canvas.

d Connect the machine to the network.

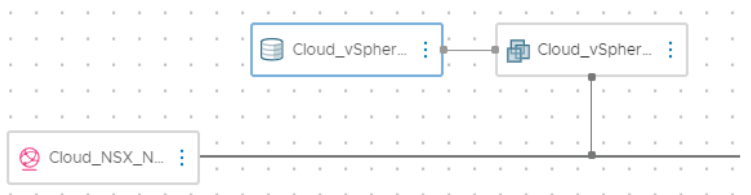
Click the small circle on the machine component and drag the connection to the network.



Notice that the YAML now looks similar to this example.

```
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 Click **Test** to validate the template.
 - f Click **Deploy**.
 - g Enter the name **DevTemplate - machine - network** and click **Deploy**.
 - h Track the progress and review the successful deployment.
- 6 Version the template and add data disk.
- a Open the template in the design canvas.
 - b Version the template.
- Enter **Machine with existing network** as the description.
- c From the resource type pane, drag an **vSphere Disk** resource type to the canvas.
 - d Connect the disk to the machine.



Notice that the YAML now looks similar to this example.

```
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 Test the template.
- f Deploy the template using the name **DevTemplate - machine - network - storage**.
- g Track the progress and review the successful deployment.
- h Version the template.

Enter **Machine with existing network and storage disk** as the description.

This final version ensures that you can add a working template to the Service Catalog.

Tutorial results

You completed the workflow that configured Cloud Assembly as a working system. You are now familiar with the following concepts.

- Cloud accounts are the credentials that connect vRealize Automation Cloud Assembly to your cloud vendor endpoints.
- Cloud zones are the selected compute resources in account/regions that you then assign to different projects based on the project needs and your goals for managing costs.
- Infrastructure resources are definitions of resources associated with account/regions that are used in cloud templates.
- Projects are how you give your users access to the cloud zones based on the project's application development goals.
- Cloud templates are the definitions of your application workloads that you iteratively develop and deploy.

This tutorial is the foundation of your vRealize Automation Cloud Assembly development experience. You can use this process to build your infrastructure and mature your cloud template development skills.

Tutorial: Configuring vRealize Automation Cloud Assembly to provision a production workload

As a cloud administrator, you want to automate the deployment process for a project so that when the cloud template designers are creating and deploying templates, vRealize Automation Cloud Assembly does the work for you. For example, the workloads are deployed with a particular custom machine naming pattern, the machines are added to a specific Active Directory organizational unit, and specific DNS and IP ranges are used.

By automating the process for the project deployments, you can more easily manage multiple projects across various data centers and cloud environments.

You are not required to complete all of the tasks. You can mix and match any of these tasks, depending on your management goals. Here's a list of the possible tasks.

- [Customize the machine names](#)
- [Create Active Directory machine records](#)
- [Set your network DNS and internal IP range](#)

Before you begin

This tutorial requires you to have your infrastructure configured and to have successfully deployed a cloud template with a machine and a network. Verify that the following are already configured on your system.

- You successfully performed all of the steps specified in the infrastructure tutorial. See [Tutorial: Setting up and testing vSphere infrastructure and deployments in vRealize Automation Cloud Assembly](#).
- You have the Cloud Assembly Administrator role. See [Organization and service user roles in vRealize Automation](#).

Customize the machine names

The goal of this task is to ensure that the deployed machines for the Development project are named based on the costcenter for the project, the resource type selected at deployment time, and incremented numbers to ensure uniqueness. For example, DevProject-centos-021.

You can adapt this example to your naming requirements.

For more about projects, see [Chapter 5 Adding and managing vRealize Automation Cloud Assembly projects](#).



For a video that illustrates this custom naming example, see [How to create a custom naming template for deployments](#).

- 1 Select **Infrastructure > Projects**.
- 2 Select an existing project or create a new one.
For this tutorial, the project name is Development Project.
- 3 Click **Create**.
- 4 On the Projects page, click the project name on the tile so that you can configure the project.
- 5 Click the **Users** tab and add the users who are members of this project.
- 6 Click the **Provisioning** tab.
 - a In the Zones section, click **Add Zone** and add the possible cloud zones where the workloads are deployed for this project.
 - b In the Custom Properties section, add a custom property with the name **costCenter** and the value **DevProject**.

Custom Properties
Specify the custom properties that should be added to all requests in this project. ⓘ

Define custom properties	Name	Value
	costCenter	DevProject

Custom Naming
Specify the naming template to be used for machines, networks, security groups and disks provisioned in this project.

Template: `${resource.costCenter}-${resource.osType}-${###}` ⓘ
Hint: Avoid conflicting names by generating digits in names. `${#####}`

- c In the Custom Naming section, add the following naming template.

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

The `${resource.osType}` is based on the operating system selected when you deploy the cloud template.

- 7 Click **Save**.
- 8 Update the cloud template with an input value for the operating system type.

Input values are the direct way that you can customize the deployment request form for users and simplify your development process. By creating input values, you can use a single cloud template to deploy workloads with different configurations. For example, size or operating system.

This example uses the Development Template from a previous tutorial. See [Step 5: Design and deploy a basic cloud template](#).

- a Select **Design** and open the Development Template.
- b In the Code pane, update the YAML with the following changes.

- In the `Inputs` section, add **osType**.

In the next step you can see that `osType` input is also used to specify the image. When you add the strings in the `enum` section, the values, in this example they are `centos` and `ubuntu`, must match the image names that you defined in **Infrastructure > Configure > Image Mappings**. For example, if your image mapping name is CentOS rather than `centos`, you should use `CentOS` in the inputs section.

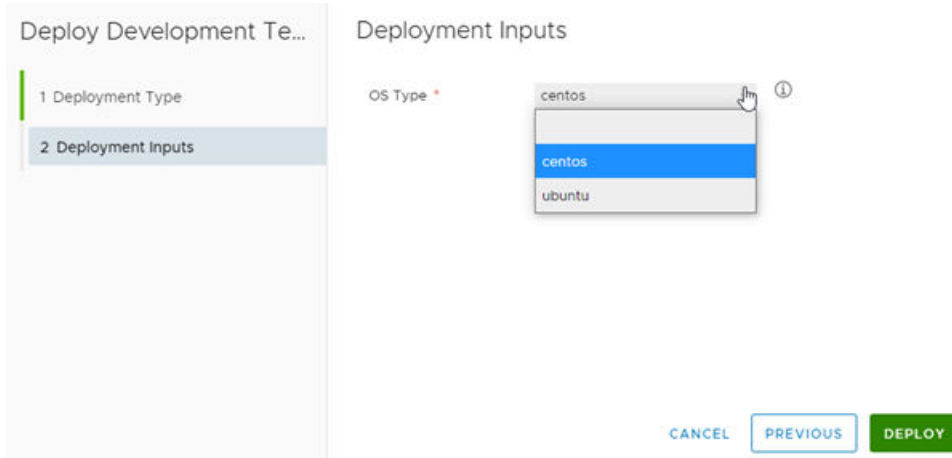
```
inputs:
  osType:
    type: string
    title: OS Type
    description: Select the operating system.
    enum:
      - centos
      - ubuntu
```

- In the `Cloud_vSphere_Machine_1` section, update the `image` to an `osType` input parameter (`${input.osType}`) and add an `osType` custom property with the same input parameter.

```
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 Click **Deploy** and enter the name **Custom name deployment test**.
- d Click **Next**.

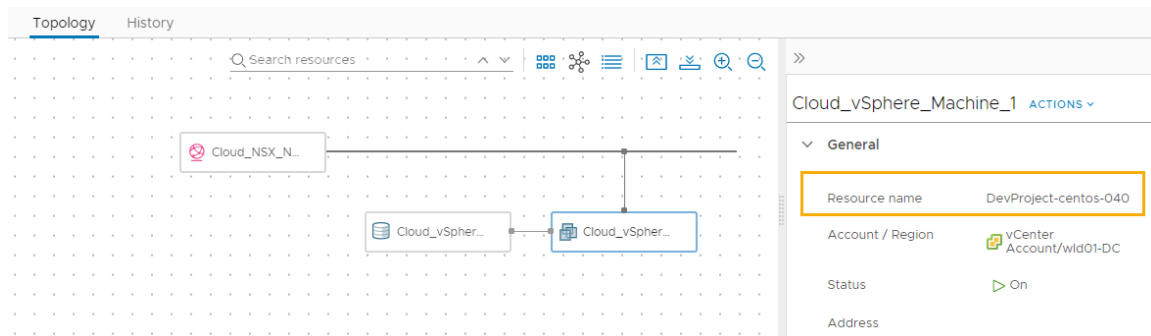
- e Select the **centos** operating system from the drop-down menu.



- f Click **Deploy**.

- 9 Track the progress and review the successful deployment.

The machine name in this example is DevProject-centos-026. Just a reminder, this example is based on the tutorial referenced at the beginning of this task.



Create Active Directory machine records

When you provision a workload, you can create machine records in Active Directory. By configuring vRealize Automation Cloud Assembly to perform this task automatically for a project deployments, you have lightened your own workload as the cloud administrator.

- 1 Add an Active Directory integration.
 - a Select **Infrastructure > Connections > Integrations**.

These steps cover the basic Active Directory configuration that is related to this AD machine records tutorial. For more about the Active Directory integration, see [How do I create an Active Directory integration in vRealize Automation Cloud Assembly](#).

- b Click **Add Integration** and click and click **Active Directory**.

- c Enter the name that you are using for this integration.
- d Enter the **LDAP host / IP** and the associated credentials.
- e Enter the **Base DN**.

In this tutorial the example is **ou=AppDev,dc=cmbu,dc=local**. AppDev is the parent OU for the computer OU that you will add for the project.

- f Click **Add**.

2 Add the project to the integration.

3 In the Active Directory integration, click the **Projects** tab and click **Add Project**.

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**).

- a Select the App Development project.
- b Enter the relative DN. For example, **OU=AppDev-Computers**.
- c Click **Add**.

4 To save your changes to the integration, click **Save**.

- 5 Deploy a cloud template for the project and verify that the machine added to the correct Active Directory OU.

Set your network DNS and internal IP range

Add or update a network profile to include your DNS servers and internal IP ranges.

You must have already created a cloud account for vSphere, NSX-V, or NSX-T. See [Tutorial: Setting up and testing vSphere infrastructure and deployments in vRealize Automation Cloud Assembly](#) or [Adding cloud accounts to vRealize Automation Cloud Assembly](#).

- 1 Select **Infrastructure > Configure > Network Profiles**.
- 2 Select an existing profile or create one.
- 3 On the **Summary** tab, select an **Account/region** and enter a name.
For this tutorial, the network profile name is Network Profile.
- 4 Add networks.
 - a Click the **Networks** tab.
 - b Click **Add Network**.
 - c Add one or more NSX or vSphere networks.
 - d Click **Add**.
- 5 Configure the DNS servers.
 - a In the networks list on the **Networks** tab, click the network name.

Summary

Networks

Network Policies

Load Balancers

Security


Networks listed here are used when provisioning to existing, on-demand, or p

+ ADD NETWORK

TAGS

MANAGE IP RANGES

REMOVE

<input type="checkbox"/>	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 Enter the DNS server IP addresses you want this network to use.

DevProject--004

DNS servers

192.168.1.22
192.168.1.23

DNS search domains

company.local

DNS Servers

Use a comma separated list or new lines.

c Click **Save**.

6 Specify the IP range for the network.

a In the networks list, select the check box next to the network name.

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	Subnet
<input type="checkbox"/>	External-mcm1343745-148168716643	NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	172.16.12.64/28	
<input type="checkbox"/>	NSX-mcm1376447-151082888186	NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	192.168.100.32/28	
<input checked="" type="checkbox"/>	NSX-mcm39835-146434698964	NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	192.168.1.0/27	

1

b Click **Manage IP Ranges**.

c In the Manage IP Ranges dialog box, click **New IP Range**.

New IP Range

Network *	NSX-mcm1376447-151082888186
Source	<input checked="" type="radio"/> Internal <input type="radio"/> External
Name *	DevProject Range
Description	<div></div>
CIDR	192.168.100.32/28
Start IP address *	192.168.100.34
End IP address *	192.168.100.46

d Enter a name.

For example, **DevProject Range**.

e To define the range, enter the **Start IP address** and **End IP address**.

f Click **Add**.

g Add additional ranges or click **Close**.

- 7 Add the cloud zone containing the associated network account/region that you configured to your Development project.
- 8 Deploy a cloud template for the project and verify that the machine is provisioned within the specified IP range.

Tutorial: Setting up and testing multi-cloud infrastructure and deployments in vRealize Automation Cloud Assembly

This end-to-end vRealize Automation Cloud Assembly tutorial shows how you might deploy in a multiple-cloud setting. You deploy the same cloud template to more than one provider, in this case AWS and Microsoft Azure.

In this example, the application is a WordPress site. Look at the sequential setup to understand the process that brings the entire design to completion.

Remember that the names and values you see are only examples. You won't be able to use them letter-by-letter in your own environment.

To fit your own cloud infrastructure and deployment needs, consider where you would make your own substitutions for the example values.

Part 1: Configure the example vRealize Automation Cloud Assembly infrastructure

First, configure the resources where vRealize Automation Cloud Assembly engineering users can later develop, test, and put the application into production.

The infrastructure includes cloud targets, and definitions around the available machines, networks, and storage that the WordPress site will need.

1. Add cloud accounts

In this step, the cloud administrator adds two cloud accounts. The example project expects to do development and testing work on AWS, and go to production on Azure.

Procedure

- 1 Go to **Infrastructure > Connections > Cloud Accounts**.
- 2 Click **Add Cloud Account**, select Amazon Web Services, and enter values.

Setting	Sample Value
Access key ID	R5SDR3PXVV2ZW8B7YNSM
Secret access key	SZXAINXU4UHNQAQ1E156S
Name	OurCo-AWS
Description	WordPress

Remember that all values are only examples. Your account specifics will vary.

- 3 To verify credentials, click **Validate**.
- 4 Click **Add**.
- 5 Edit the newly added account **Configuration**, and allow provisioning to us-east-1 and us-west-2 regions.
- 6 Click **Add Cloud Account**, select Microsoft Azure, and enter values.

Setting	Sample Value
Subscription ID	ef2avpf-dfdv-zxlugui1i-g4h0-i8ep2jwp4c9arbf
Tenant ID	dso9wv3-4zgc-5nrcy5h3m-4skf-nnovp40wfxsro22r
Client application ID	bg224oq-3ptp-mbhi6aa05-q511-uf1yjr2sttyik6bs
Client application secret key	7uqxi57-0wtn-kymgf9wcj-t2l7-e52e4nu5fig4pmd

Setting	Sample Value
Name	OurCo-Azure
Description	WordPress

- 7 To verify credentials, click **Validate**.
- 8 Click **Add**.
- 9 Edit the newly added account **Configuration**, and allow provisioning to the East US region.

2. Add cloud zones

In this example step, the cloud administrator adds three cloud zones, one each for development, testing, and production.

Cloud zones are the resources onto which the project will deploy the machines, networks, and storage to support the WordPress site.

Procedure

- 1 Go to **Infrastructure > Configure > Cloud Zones**.
- 2 Click **New Cloud Zone**, and enter values for the development environment.

Cloud Zone Setting	Sample Value
Account / region	OurCo-AWS/us-east-1
Name	OurCo-AWS-US-East
Description	WordPress
Placement policy	Default
Capability tags	env:dev

Remember that all values are only examples. Your zone specifics will vary.

- 3 Click **Compute**, and verify that the zones you expect are there.
- 4 Click **Create**.
- 5 Repeat the process twice, with values for the test and production environments.

Cloud Zone Setting	Sample Value
Account / region	OurCo-AWS/us-west-2
Name	OurCo-AWS-US-West
Description	WordPress

Cloud Zone Setting	Sample Value
Placement policy	Default
Capability tags	env:test

Cloud Zone Setting	Sample Value
Account / region	OurCo-Azure/East US
Name	OurCo-Azure-East-US
Description	WordPress
Placement policy	Default
Capability tags	env:prod

3. Add flavor mappings

In this example step, the cloud administrator adds flavor mappings to account for capacity needs that might vary depending on deployment.

Flavor mapping accounts for different size machine deployments and is informally referred to as T-shirt sizing.

Procedure

- 1 Go to **Infrastructure > Configure > Flavor Mappings**. Each cloud zone needs to allow for small, medium, and large flavors.
- 2 Click **New Flavor Mapping**, and enter values for the development cloud zone.

Setting	Sample Value
Flavor name	small
Account/region Value	OurCo-AWS/us-east-1 t2.micro
Account/region Value	OurCo-AWS/us-west-2 t2.micro
Account/region Value	OurCo-Azure/East US Standard_A0

Remember that all values are only examples. Your flavors will vary.

- 3 Click **Create**.

- 4 Repeat the process twice, with values for medium and large flavors.

Setting	Sample Value
Flavor name	medium
Account/region Value	OurCo-AWS/us-east-1 t2.medium
Account/region Value	OurCo-AWS/us-west-2 t2.medium
Account/region Value	OurCo-Azure/East US Standard_A3

Setting	Sample Value
Flavor name	large
Account/region Value	OurCo-AWS/us-east-1 t2.large
Account/region Value	OurCo-AWS/us-west-2 t2.large
Account/region Value	OurCo-Azure/East US Standard_A7

4. Add image mappings

In this example step, the cloud administrator adds an image mapping for Ubuntu, the host for the WordPress server and its MySQL database server.

Plan for the operating system by adding image mappings. Each cloud zone needs a Ubuntu image mapping.

Procedure

- 1 Go to **Infrastructure > Configure > Image Mappings**.
- 2 Click **New Image Mapping**, and enter values for Ubuntu servers.

Setting	Sample Value
Image name	ubuntu
Account/region Value	OurCo-AWS/us-east-1 ubuntu-16.04-server-cloudimg-amd64
Account/region Value	OurCo-AWS/us-west-2 ubuntu-16.04-server-cloudimg-amd64
Account/region Value	OurCo-Azure/East US azul-zulu-ubuntu-1604-923eng

Remember that all values are only examples. Your images will vary.

3 Click **Create**.

5. Add network profiles

In this example step, the cloud administrator adds a network profile to each cloud zone.

In each profile, the administrator adds a network for the WordPress machines, and a second network that will sit on the other side of an eventual load balancer. The second network will be the one that users eventually connect to.

Procedure

- 1 Go to **Infrastructure > Configure > Network Profiles**.
- 2 Click **New Network Profile**, and create a profile for the development cloud zone.

Network Profile Setting	Sample Value
Account / region	OurCo-AWS/us-east-1
Name	devnets
Description	WordPress

- 3 Click **Networks**, and click **Add Network**.
- 4 Select wpnet, appnet-public, and click **Add**.

Remember that all values are only examples. Your network names will vary.

- 5 Click **Create**.

This Wordpress example does not require that you specify network policy or network security settings.

- 6 Repeat the process twice, to create a network profile for the Wordpress example test and production cloud zones. In each case, add the wpnet and appnet-public networks.

Network Profile Setting	Sample Value
Account / region	OurCo-AWS/us-west-2
Name	testnets
Description	WordPress

Network Profile Setting	Value
Account / region	OurCo-Azure/East US
Name	prodnets
Description	WordPress

6. Add storage profiles

In this example step, the cloud administrator adds a storage profile to each cloud zone.

The administrator places fast storage at the production zone and general storage at development and test.

Procedure

- 1 Go to **Infrastructure > Configure > Storage Profiles**.
- 2 Click **New Storage Profile**, and create a profile for the development cloud zone.

Additional fields appear after you select the account/region.

Storage Profile Setting	Sample Value
Account / region	OurCo-AWS/us-east-1
Name	OurCo-AWS-US-East-Disk
Description	WordPress
Device type	EBS
Volume type	General Purpose SSD
Capability tags	storage:general

Remember that all values are only examples.

- 3 Click **Create**.
- 4 Repeat the process to create a profile for the test cloud zone.

Storage Profile Setting	Sample Value
Account / region	OurCo-AWS/us-west-2
Name	OurCo-AWS-US-West-Disk
Description	WordPress
Device type	EBS
Volume type	General Purpose SSD
Capability tags	storage:general

- 5 Repeat the process to create a profile for the production cloud zone, which has different settings because it is an Azure zone.

Storage Profile Setting	Sample Value
Account / region	OurCo-Azure/East US
Name	OurCo-Azure-East-US-Disk

Storage Profile Setting	Sample Value
Description	WordPress
Storage type	Managed disks
Disk type	Premium LRS
OS disk caching	Read only
Data disk caching	Read only
Capability tags	storage:fast

What to do next

Create a project to identify users, and to define provisioning settings. See [Part 2: Create the example vRealize Automation Cloud Assembly project](#).

Part 2: Create the example vRealize Automation Cloud Assembly project

The example vRealize Automation Cloud Assembly project enables the users who can provision, and configures how much provisioning is possible.

Projects define the user and provisioning settings.

- Users and their role level of permission
- Priority for deployments as they are being provisioned to a cloud zone
- Maximum number of deployment instances per cloud zone

Procedure

- 1 Go to **Infrastructure > Administration > Projects**.
- 2 Click **New Project**, and enter the name WordPress.
- 3 Click **Users**, and click **Add Users**.
- 4 Add email addresses and roles for the users.

To successfully add a user, a VMware Cloud Services administrator must have enabled access to vRealize Automation Cloud Assembly for the user.

Remember that addresses shown here are only examples.

- chris.ladd@ourco.com, Member
 - kerry.mott@ourco.com, Member
 - pat.tubb@ourco.com, Administrator
- 5 Click **Provisioning**, and click **Add Cloud Zone**.

6 Add the cloud zones that the users can deploy to.

Project Cloud Zone Setting	Sample Value
Cloud zone	OurCo-AWS-US-East
Provisioning priority	1
Instances limit	5
Cloud zone	OurCo-AWS-US-West
Provisioning priority	1
Instances limit	5
Cloud zone	OurCo-Azure-East-US
Provisioning priority	0
Instances limit	1

7 Click **Create**.

8 Go to **Infrastructure > Configure > Cloud Zones**, and open a zone that you created earlier.

9 Click **Projects**, and verify that WordPress is a project that is allowed to provision to the zone.

10 Check the other zones that you created.

What to do next

Create a basic cloud template.

Part 3: Design and deploy the example vRealize Automation Cloud Assembly template

Next, you define the example application—the WordPress site—in the form of a generic cloud template. The template can be deployed to different cloud vendors without needing to change its design.

The example consists of a WordPress application server, MySQL database server, and supporting resources. The template starts with a few resources, and then grows as you modify them and add more resources.

Here are the values from [Part 1: Configure the example vRealize Automation Cloud Assembly infrastructure](#), the infrastructure that was set by a cloud administrator:

- Two cloud accounts, AWS and Azure.
- Three cloud zone environments:
 - Development—OurCo-AWS-US-East
 - Test—OurCo-AWS-US-West
 - Production—OurCo-Azure-East-US
- Flavor mappings with small, medium, and large compute resources for each zone.
- Image mappings for Ubuntu configured in each zone.

- Network profiles with internal and external subnets for each zone.
- Storage on which to deploy; general storage for the development and test zone, and fast storage for the production zone.
- The example project includes all three cloud zone environments plus the users who can create designs.

Prerequisites

To follow along, you must be familiar with your own infrastructure values. This example uses AWS for development and test, and Azure for production. When creating your own cloud template, substitute your own values, typically set by your cloud administrator.

Procedure

1 Create a basic cloud template

In this vRealize Automation Cloud Assembly design example, you start with a cloud template that contains only minimal WordPress resources, such as having only one application server.

2 Test a basic cloud template

During design, you often build a cloud template by starting with the essentials, then deploying and testing as the template grows. This example demonstrates some of the in-progress testing built into vRealize Automation Cloud Assembly.

3 Expand a cloud template

After you create and test the basic vRealize Automation Cloud Assembly template for the example application, you expand it into a multiple tier application that is deployable to development, test, and eventually production.

Create a basic cloud template

In this vRealize Automation Cloud Assembly design example, you start with a cloud template that contains only minimal WordPress resources, such as having only one application server.

vRealize Automation Cloud Assembly is an infrastructure-as-code tool. You drag resources to the design canvas to get started. Then, you complete the details using the code editor to the right of the canvas.

The code editor allows you to type, cut, and paste code directly. If you're uncomfortable editing code, you can select a resource in the canvas, click the code editor **Properties** tab, and enter values there. Values that you enter appear in the code as if you had typed them directly.

Procedure

- 1 Go to **Design > Cloud Templates** and click **New from > Blank canvas**.
- 2 Name the cloud template **WordPress-BP**.
- 3 Select the **WordPress** project, and click **Create**.

- 4 From the resources on the left of the cloud template design page, drag two cloud agnostic machines onto the canvas.

The machines serve as WordPress application server (WebTier) and MySQL database server (DBTier).

- 5 On the right, edit the machine YAML code to add names, images, flavors, and constraint tags:

```
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
```

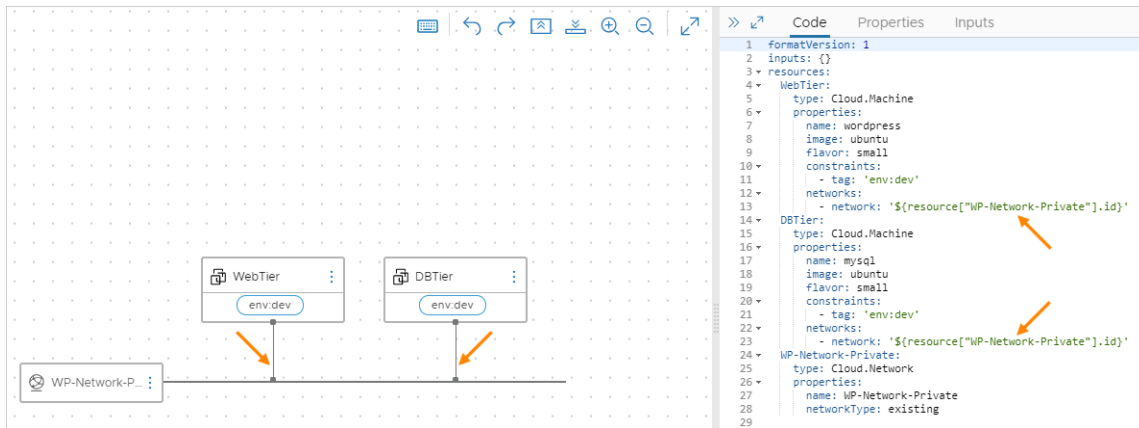
- 6 Drag a cloud agnostic network to the canvas, and edit its code:

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

- 7 Connect the machines to the network:

In the canvas, hover over the network block, click and hold the bubble where the line touches the block, drag to a machine block, and release.

When you create the connection lines, note that network code is automatically added to the machines in the editor.



8 Add user input prompting.

In some places, the example infrastructure was set up for multiple options. For example:

- Cloud zone environments for development, test, and production
- Flavor mappings for small, medium, and large machines

You might set a specific option directly in the cloud template, but a better approach is to let the user select the option at template deployment time. Prompting for user input lets you create one template that can be deployed many ways, instead of having many hard-coded templates.

- a Create an `inputs` section in the code so that users can select machine size and target environment at deployment time. Define the selectable values:

```
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 In the `resources` section of the code, add `${input.input-name}` code to prompt for the user selection:

```
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 Finally, enhance the `WebTier` and `DBTier` code using the following examples. The `WP-Network-Private` code does not need additional changes.

Note that the enhancements include login access to the database server and deployment-time `cloudConfig` initialization scripts.

Component	Example
Additional DBTier Inputs	<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 Resource	<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 Resource	<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>

Component	Example
	<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>

Example: Completed basic cloud template code example

```

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

```

What to do next

Test the cloud template by checking the syntax and deploying it.

Test a basic cloud template

During design, you often build a cloud template by starting with the essentials, then deploying and testing as the template grows. This example demonstrates some of the in-progress testing built into vRealize Automation Cloud Assembly.

To be certain that a deployment works the way that you want, you might test and deploy the cloud template several times. Gradually, you add more resources, retest, and redeploy along the way.

Prerequisites

Create the basic cloud template. See [Create a basic cloud template](#).

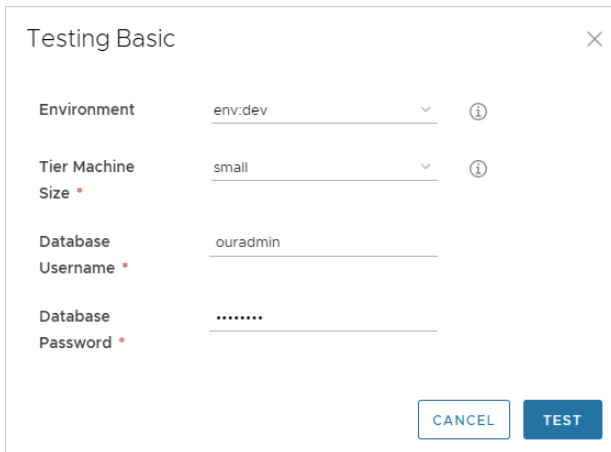
Procedure

- 1 Click **Cloud Templates**, and open the WordPress-BP cloud template.

The basic cloud template appears, in the design canvas and code editor.

- 2 To check template syntax, placement, and basic validity, click **Test** at the lower left.

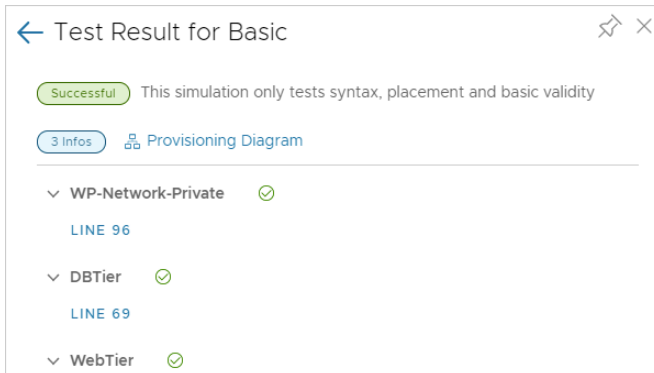
3 Enter input values, and click **Test**.



The 'Testing Basic' dialog box contains the following fields and controls:

- Environment:** A dropdown menu with 'env:dev' selected and an information icon.
- Tier Machine Size:** A dropdown menu with 'small' selected and an information icon.
- Database Username:** A text input field containing 'ouradmin'.
- Database Password:** A text input field with masked characters '.....'.
- Buttons:** 'CANCEL' and 'TEST' buttons at the bottom right.

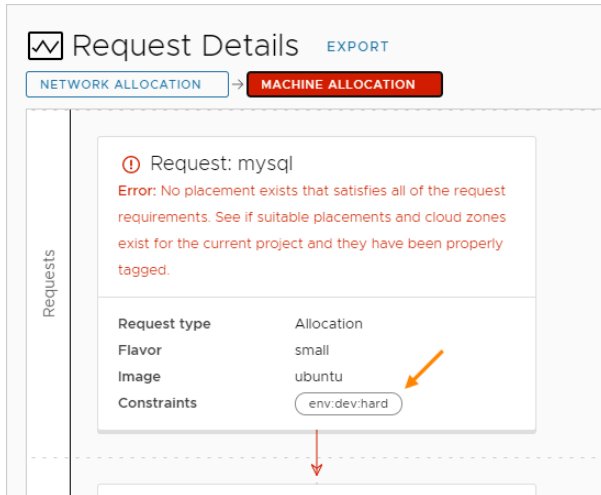
The test is only a simulation and does not actually deploy virtual machines or other resources.



The 'Test Result for Basic' dialog box displays the following information:

- Status:** A green 'Successful' badge with the text 'This simulation only tests syntax, placement and basic validity'.
- Links:** '3 Infos' and 'Provisioning Diagram' (with a diagram icon).
- Results List:**
 - WP-Network-Private:** Checked (green checkmark), with a link to 'LINE 96'.
 - DBTier:** Checked (green checkmark), with a link to 'LINE 69'.
 - WebTier:** Checked (green checkmark).

The test includes a link to a **Provisioning Diagram**, where you can inspect the simulated deployment flow and see what occurred. The simulation exposes potential issues, such as not having any resource capabilities defined that match hard constraints in the cloud template. In the example error that follows, a cloud zone of capability tag `env:dev` wasn't found anywhere in the defined infrastructure.



A successful simulation doesn't guarantee that you can deploy the template without errors.

- 4 After the template passes the simulation, click **Deploy** at the lower left.
- 5 Select **Create a new deployment**.
- 6 Name the deployment **WordPress for OurCo** and click **Next**.
- 7 Enter input values, and click **Deploy**.
- 8 To verify that the template successfully deployed, look under **Deployments > Deployments**.

If a deployment fails, click its name, and click the **History** tab to see messages that can help you troubleshoot.

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

Some history entries might have the **Provisioning Diagram** link at the far right. The diagram is similar to the simulated one, where you inspect the flow chart of vRealize Automation Cloud Assembly decision points in the provisioning process.

More flow charts are available under **Infrastructure > Activity > Requests**.

- 9 To verify that the application is working, open the WordPress start page in a browser.
 - a Wait for the WordPress servers to be fully created and initialized.
It might take 30 minutes or more for initialization, depending on the environment.
 - b To locate the site FQDN or IP address, go to **Deployments > Deployments > Topology**.
 - c On the canvas, click the WebTier, and find the IP address in the panel on the right.
 - d Enter the IP address as part of the full URL to the WordPress start page.
In this example, the full URL is:
`http://{IP-address}/mywordpresssite`
or
`http://{IP-address}/mywordpresssite/wp-admin/install.php`
- 10 After inspecting WordPress in a browser, if the application needs more work, make template changes and redeploy using the **Update an existing deployment** option.
- 11 Consider versioning the cloud template. You can revert to a working version if a change causes deployment to fail.
 - a On the cloud template design page, click **Version**.
 - b On the Creating Version page, enter **WP-1.0**.
Do not enter spaces in version names.
 - c Click **Create**.
To review or revert to a version, on the design page, click the **Version History** tab.
- 12 With a basic deployment now possible, try your first deployment-time enhancement by increasing CPU and memory on the application and database servers.
Update to a medium node size for both. Using the same template, select **medium** at deployment time, redeploy, and verify the application again.

What to do next

Expand the cloud template into a production-worthy application by adding even more resources.

Expand a cloud template

After you create and test the basic vRealize Automation Cloud Assembly template for the example application, you expand it into a multiple tier application that is deployable to development, test, and eventually production.

To expand the cloud template, you add the following enhancements.

- An option to cluster application servers for increased capacity
- A public-facing network and load balancer in front of the application servers

- A backup server with archive storage

Prerequisites

Create the basic cloud template and test it. See [Create a basic cloud template](#) and [Test a basic cloud template](#).

Procedure

- 1 Click **Cloud Templates**, and open the WordPress-BP cloud template.

The basic template appears, in the design canvas and code editor.

- 2 Make additions and changes, using the code example and figure for guidance.

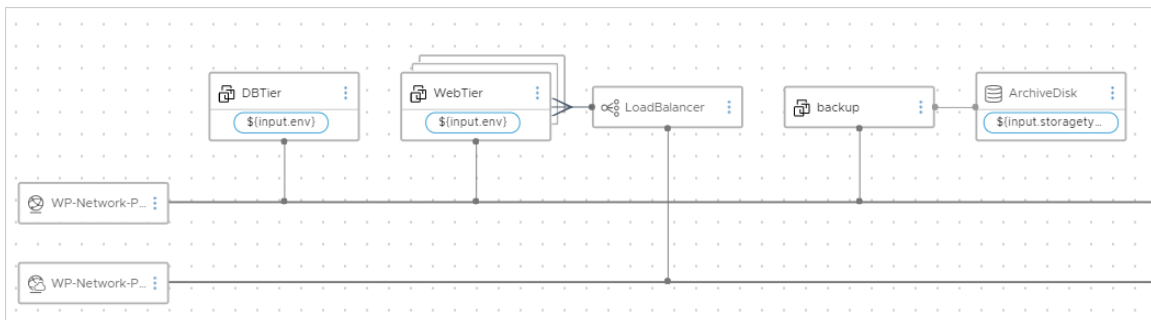
You use the GUI to drag new resources to the canvas, such as the load balancer, and then finish the configuration in the code editor.

- a Add a `count` input prompt to make the WordPress application server into a cluster.
- b Add a cloud agnostic load balancer.
- c Connect the load balancer to the WordPress application server cluster.
- d Add a cloud agnostic backup machine.
- e Connect the backup machine to the private/internal network.
- f Add a cloud agnostic public/external network.
- g Connect the load balancer to the public network.
- h Add a cloud agnostic storage volume for use as an archive disk.
- i Connect the archive disk to the backup machine.
- j Add an input prompt for the archive disk speed.

- 3 Deploy, test, and make changes in the same way that you did for the basic cloud template.

You can update existing deployments, or even deploy new instances so that you can compare deployments.

The goal is to reach a solid, repeatable template that can be used for production deployments.



Example: Completed expanded cloud template code example

```

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}'
```

What to do next

Define your own infrastructure and create your own cloud templates.

See [Chapter 4 Building your vRealize Automation Cloud Assembly resource infrastructure](#) and [Chapter 6 Designing your vRealize Automation Cloud Assembly deployments](#).

Tutorial: Configuring VMware Cloud on AWS for vRealize Automation

This vRealize Automation Cloud Assembly tutorial shows the process of defining resource infrastructure and cloud template settings for deployment to a VMware Cloud on AWS environment.

The procedure requires that a cloud administrator has already configured your organization's VMware Cloud on AWS SDDC data center as described in *Deploying and Managing a Software-Defined Data Center* in the [VMware Cloud on AWS Getting Started documentation](#).

Look at the sequential setup to understand the process for configuring your environment for VMware Cloud on AWS. Remember that the values you see are only use case examples. Think about where you would make your own substitutions, or extrapolate from the example values, in order to fit your own cloud infrastructure and deployment needs.

A detailed video of a similar workflow is available from *VMware Cloud Management Technical Marketing* at [How to Configure VMware Cloud on AWS for Cloud Assembly](#).

Procedure

1 [Configure a basic VMware Cloud on AWS workflow in vRealize Automation](#)

This use case shows the process of defining resource infrastructure and a corresponding cloud template for deployment to a VMware Cloud on AWS environment.

2 [Configure an isolated network in VMware Cloud on AWS workflow in vRealize Automation](#)

In this procedure, you add an isolated network for your VMware Cloud on AWS deployment in vRealize Automation.

Configure a basic VMware Cloud on AWS workflow in vRealize Automation

This use case shows the process of defining resource infrastructure and a corresponding cloud template for deployment to a VMware Cloud on AWS environment.

In this procedure, you configure infrastructure that supports cloud template deployment to resources in your existing VMware Cloud on AWS environment.

Prerequisites

- Before you can create and configure a VMware Cloud on AWS cloud account in vRealize Automation Cloud Assembly, you must be part of an organization in an existing VMware Cloud on AWS SDDC environment. For information about configuring the VMware Cloud on AWS service, see [VMware Cloud on AWS Documentation](#).
- To facilitate the needed connection between your existing VMware Cloud on AWS host SDDC in vCenter and a VMware Cloud on AWS cloud account in vRealize Automation Cloud Assembly, you must provide a network connection, and add firewall rules, by using a VPN or similar networking means. See [Prepare your VMware Cloud on AWS SDDC to connect with VMware Cloud on AWS cloud accounts in vRealize Automation](#).

Procedure

- 1 [Prepare your VMware Cloud on AWS SDDC to connect with VMware Cloud on AWS cloud accounts in vRealize Automation](#)

When using VMware Cloud on AWS cloud accounts in your vRealize Automation Cloud Assembly on-premises environment, you must create a network connection to support communication between your SDDC in vCenter and any VMware Cloud on AWS cloud accounts in vRealize Automation.

- 2 [Create a VMware Cloud on AWS cloud account in vRealize Automation within a sample workflow](#)

In this step, you create a VMware Cloud on AWS cloud account in vRealize Automation.

- 3 [Create a cloud zone for VMware Cloud on AWS deployments in vRealize Automation](#)

In this step, you create a cloud zone to specify a compute resource that the CloudAdmin user can access when working with VMware Cloud on AWS in vRealize Automation.

- 4 [Configure network and storage profiles for VMware Cloud on AWS deployments in vRealize Automation](#)

In this step, you configure a network profile and a storage profile to specify resources that are available to a VMware Cloud on AWS CloudAdmin user in vRealize Automation.

- 5 [Create a project to support VMware Cloud on AWS deployments in vRealize Automation](#)

In this step, you define a vRealize Automation project that can be used to control which resources are available for VMware Cloud on AWS deployments.

- 6 [Define a vCenter machine resource in a cloud template design to support VMware Cloud on AWS deployment in vRealize Automation](#)

In this step, you drag a vCenter machine resource onto the design canvas and add settings for a VMware Cloud on AWS deployment in vRealize Automation.

Prepare your VMware Cloud on AWS SDDC to connect with VMware Cloud on AWS cloud accounts in vRealize Automation

When using VMware Cloud on AWS cloud accounts in your vRealize Automation Cloud Assembly on-premises environment, you must create a network connection to support communication

between your SDDC in vCenter and any VMware Cloud on AWS cloud accounts in vRealize Automation.

To facilitate the needed connection between your existing VMware Cloud on AWS host SDDC in vCenter and a VMware Cloud on AWS cloud account in vRealize Automation, you must provide a network connection between the two elements by using a VPN or similar networking means.

Procedure

- 1 Configure a VPN connection over the public Internet or AWS Direct connect.

See *VMware Cloud on AWS Networking and Security* at [VMware Cloud on AWS Documentation](#).

- 2 Verify that the vCenter Server FQDN is resolvable at a private IP address on the management network.

See *VMware Cloud on AWS Networking and Security* at [VMware Cloud on AWS Documentation](#).

- 3 Configure needed firewall rules.

You must configure management gateway firewall rules in the SDDC's VMware Cloud on AWS console to support communication. The rules must be in the **Management Gateway** firewall rules section. Create the firewall rules by using options on the **Networking & Security** tab in the SDDC console.

- Limit network traffic to ESXi for HTTPS (TCP 443) services to the discovered IP address of the vRealize Automation appliance/server or vRealize Automation load balancer VIP.
- Limit network traffic to vCenter for ICMP (All ICMP), SSO (TCP 7444), and HTTPS (TCP 443) services to the discovered IP address of the vRealize Automation appliance/server or vRealize Automation load balancer VIP.
- Limit network traffic to the NSX-T Manager for HTTPS (TCP 443) services to the discovered IP address of the vRealize Automation appliance/server or vRealize Automation load balancer VIP.

The required firewall rules are summarized in the following table.

Table 2-1. Required Management Gateway Firewall Rules Summary

Name	Source	Destination	Service
vCenter	CIDR block of on-premises data center	vCenter	Any (All Traffic)
vCenter ping	Any	vCenter	ICMP (All ICMP)
NSX Manager	CIDR block of on-premises data center	NSX Manager	Any (All Traffic)
On premises to ESXi ping	CIDR block of on-premises data center	ESXi Management Only	ICMP (All ICMP)

Table 2-1. Required Management Gateway Firewall Rules Summary (continued)

Name	Source	Destination	Service
On Premises to ESXi remote console and provisioning	CIDR block of on-premises data center	ESXi Management Only	TCP 902
On-premises to SDDC VM	CIDR block of on-premises data center	CIDR block of SDDC logical network	Any (All Traffic)
SDDC VM to on premises	CIDR block of SDDC logical network	CIDR block of on-premises data center	Any (All Traffic)

For related information, see *VMware Cloud on AWS Networking and Security* and *VMware Cloud on AWS Operations Guide* at [VMware Cloud on AWS Documentation](#).

Results

After you have configured required gateway access and firewall rules, you can continue with the process of creating a VMware Cloud on AWS cloud account.

Create a VMware Cloud on AWS cloud account in vRealize Automation within a sample workflow

In this step, you create a VMware Cloud on AWS cloud account in vRealize Automation.

For related information, see [VMware Cloud on AWS documentation](#).

Unless otherwise indicated, the step values that you enter in this procedure are for this example workflow only.

Prerequisites

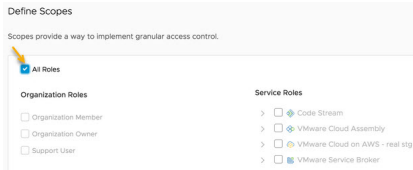
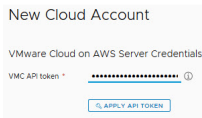
- This procedure assumes that you have the required administrator credentials, including VMware Cloud on AWS CloudAdmin credentials for the target SDDC in vCenter and that you have enabled HTTPS access on port 443. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- This procedure assumes that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).
- To facilitate the needed connection between your existing VMware Cloud on AWS host SDDC in vCenter and a VMware Cloud on AWS cloud account in vRealize Automation, you must provide a network connection, and firewall rules, by using a VPN or similar networking means. See [Prepare your VMware Cloud on AWS SDDC to connect with VMware Cloud on AWS cloud accounts in vRealize Automation](#). If you are using an external HTTP Internet proxy, it must be configured for IPv4.
- If you do not have external Internet access, configure an Internet server proxy. See [How do I configure an Internet proxy server for vRealize Automation](#).

Procedure

- 1 Select **Infrastructure > Connections > Cloud Accounts**.

2 Click **Add Cloud Account**, select VMware Cloud on AWS, and enter values.

Sample values and supporting information are provided in the following table.

Setting	Sample Value and Instruction	Description
VMC API Token	<ol style="list-style-type: none"> Click the <i>i</i> help icon at the end of the VMC API token line and click API Tokens page in the help text box to open the API Tokens tab on your organization's My Account page. Click Generate Token to display the Generate a New API Token options. Enter a new token name, for example <i>myinitials_mytoken</i>. Set the Token TTL to never expire. If you create a token that is set to expire, then the VMware Cloud on AWS operations from vRealize Automation will stop working when the token expires and continue to not work until you update the cloud account with a new token. In the Define Scopes section, select All Roles.  Click Generate. In the generated token page, click Copy and click Continue. Return to the New Cloud Account page, paste the copied token into the VMC API token row, and click Apply API token.  	<p>You can create a new token or use an existing token for your organization on the linked API Tokens page.</p> <p>In the Define Scopes section, the minimum required roles for the API token are:</p> <ul style="list-style-type: none"> ■ Organizational Roles <ul style="list-style-type: none"> ■ Organization Member ■ Organization Owner ■ Service Roles - VMware Cloud on AWS <ul style="list-style-type: none"> ■ Administrator ■ NSX Cloud Administrator ■ NSX Cloud Auditor <p>Note Copy, download, or print the generated token. Once you leave this page you cannot retrieve the generated token.</p> <p>Apply the generated or supplied token to connect to the available SDDC environment in your organization's VMware Cloud on AWS subscription and populate the list of SDDC names.</p> <p>If the vRealize Automation and VMware Cloud on AWS services are in different organizations, you should switch to the VMware Cloud on AWS organization and then generate the token.</p> <p>For more information about API tokens, see Generate API Tokens.</p>
SDDC name	<p>For this example, select Datacenter:Datacenter-abz.</p> <p>The valid SDDC name auto-populates the vCenter and NSX-T FQDN entries. If a cloud proxy was already deployed to the SDDC, the cloud proxy value also auto-populates.</p>	<p>Select from the list of available SDDCs from your VMware Cloud on AWS subscription. The list of SDDCs is based on the VMware Cloud on AWS API token.</p> <p>NSX-V SDDCs are not supported with vRealize Automation and do not appear in the list of available SDDCs.</p>

Setting	Sample Value and Instruction	Description
vCenter IP address/ FQDN	The address auto-populates based on your SDDC selection.	Enter the IP address or FQDN of the vCenter Server in the specified SDDC. The IP address defaults to the private IP address. Based on the type of network connectivity used to access your SDDC, the default address might be different than the IP address of the NSX Manager Server in the specified SDDC.
NSX Manager IP address/FQDN	The address auto-populates based on your SDDC selection.	Specifies the IP address or FQDN of the NSX Manager in the specified SDDC. The IP address defaults to the private IP address. Based on the type of network connectivity used to access your SDDC, the default address might be different than the IP address of the NSX Manager Server in the specified SDDC. VMware Cloud on AWS cloud accounts support NSX-T.
vCenter user name and password	The user name auto-populates as cloudadmin@vmc.local.	Enter your vCenter user name for the specified SDDC if it's different than the default. The specified user requires CloudAdmin credentials. The user does not require CloudGlobalAdmin credentials. Enter the user password.
Validate	Click Validate .	Validate confirms your access rights to the specified vCenter and checks that the vCenter is running.
Name and Description	Enter OurCo-VMC for the cloud account name. Enter Sample deployment for VMC for the cloud account description.	
Allow provisioning to these data centers	This information is read-only.	Lists available data centers in your specified VMware Cloud on AWS SDDC environment.
Create a cloud zone	De-select the check-box. For this example, you will create a cloud zone later in the workflow.	See Learn more about vRealize Automation Cloud Assembly cloud zones .
Capability tags	Leave this empty. This workflow does not use capability tags.	Use tags according to your organization's tag strategy. See How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments and Creating a tagging strategy .

3 Click **Add**.

Results

Resources such as machines and volumes are data-collected from the VMware Cloud on AWS SDDC data center and listed in the **Resources** section of the vRealize Automation **Infrastructure** tab.

What to do next

[Create a cloud zone for VMware Cloud on AWS deployments in vRealize Automation.](#)

Create a cloud zone for VMware Cloud on AWS deployments in vRealize Automation

In this step, you create a cloud zone to specify a compute resource that the CloudAdmin user can access when working with VMware Cloud on AWS in vRealize Automation.

In VMware Cloud on AWS, the two primary administrator credentials are CloudGlobalAdmin and CloudAdmin. vRealize Automation Cloud Assembly is designed to support the CloudAdmin user. Deploy to resources that are available to a VMware Cloud on AWS CloudAdmin user. Do not deploy to resources that require VMware Cloud on AWS CloudGlobalAdmin credentials.

Cloud zones identify the compute resources onto which a project cloud template deploys machines, networks, and storage. See [Learn more about vRealize Automation Cloud Assembly cloud zones](#).

Unless otherwise indicated, the step values that you enter in this procedure are for this example workflow only.

Prerequisites

- Complete the [Create a VMware Cloud on AWS cloud account in vRealize Automation within a sample workflow](#) procedure.
- This procedure assumes that you have the required administrator credentials, including VMware Cloud on AWS CloudAdmin credentials for the target SDDC in vCenter. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- This procedure assumes that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).

Procedure

- 1 Select **Infrastructure > Configure > Cloud Zones**.

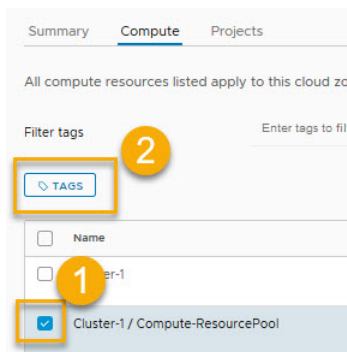
- 2 Click **New Cloud Zone**, and enter values for the VMware Cloud on AWS environment.

Setting	Sample Value
Account / region	OurCo-VMC / Datacenter:Datacenter-abz This is the cloud account and associated region that you defined in the previous step, Create a VMware Cloud on AWS cloud account in vRealize Automation within a sample workflow.
Name	VMC_cloud_zone-1
Description	VMware Cloud on AWS resources only
Placement policy	Default
Capability tags	Leave this empty. This workflow does not use capability tags.

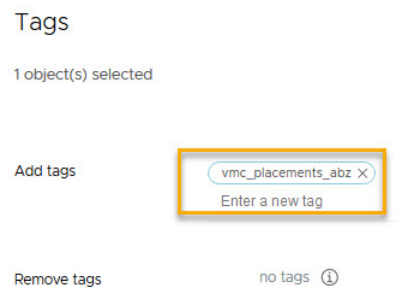
- 3 Click the **Compute** tab.

- 4 As shown in area 1 below, find and select a compute resource that is available to the CloudAdmin user. For this example, use the resource named `Cluster 1/ Compute-ResourcePool`.

`Cluster 1/ Compute-ResourcePool` is the default compute resource for VMware Cloud on AWS.






- 5 As shown in area 2 above, add the tag name `vmc_placements_abz`.



- 6 Filter the compute resources that are used in this cloud zone by entering `vmc_placements_abz` in the **Filter tags** section.

7 Click **Save**.

<input type="checkbox"/>	Name	Account / region	Type	Tags
<input type="checkbox"/>	Cluster-1		Cluster	
<input checked="" type="checkbox"/>	Cluster-1 / Compute-ResourcePool	 OurCo-VMC / SDDC_test1_abz	ResourcePool	vmc placements abz
<input type="checkbox"/>	Cluster-1 / Mgmt-ResourcePool		ResourcePool	

For this example, only the compute resource named `Cluster 1/ Compute-ResourcePool` is available to the CloudAdmin user.

What to do next

[Configure network and storage profiles for VMware Cloud on AWS deployments in vRealize Automation.](#)

Configure network and storage profiles for VMware Cloud on AWS deployments in vRealize Automation

In this step, you configure a network profile and a storage profile to specify resources that are available to a VMware Cloud on AWS CloudAdmin user in vRealize Automation.

While an image and a flavor value are also needed, there is nothing unique about them specific to VMware Cloud on AWS user credentials. For this example, you'll use a flavor value of `small` and an image value of `ubuntu-16` when you define the cloud template.

For general information about mappings and profiles, see [Chapter 4 Building your vRealize Automation Cloud Assembly resource infrastructure](#).

Unless otherwise indicated, the step values that you enter in this procedure are for this example workflow only.

Prerequisites

- Create a cloud zone. See [Create a cloud zone for VMware Cloud on AWS deployments in vRealize Automation](#).
- This procedure assumes that you have the required administrator credentials, including VMware Cloud on AWS CloudAdmin credentials for the target SDDC in vCenter. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- This procedure assumes that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).

Procedure

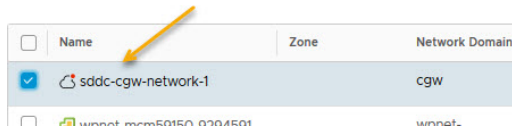
1 Define a network profile for VMware Cloud on AWS deployments.

- a Select **Infrastructure > Configure > Network Profiles** and click **New Network Profile**.

Setting	Sample value
Account / region	OurCo-VMC / Datacenter:Datacenter-abz
	Note Select the VMware Cloud on AWS cloud account, and its matched SDDC data center, that you created in Create a VMware Cloud on AWS cloud account in vRealize Automation within a sample workflow .
Name	vmc-network1
Description	Contains networks that can be accessed by cloud template administrators who have VMware Cloud on AWS CloudAdmin credentials.

- b Click the **Network** tab and click **Add Network**.
- c Select a network that a VMware Cloud on AWS user with CloudAdmin credentials can deploy to, for example `sddc-cgw-network-1`.

Add Network



<input type="checkbox"/>	Name	Zone	Network Domain
<input checked="" type="checkbox"/>	sddc-cgw-network-1		cgw
<input type="checkbox"/>	winnet		winnet

2 Save the network profile.

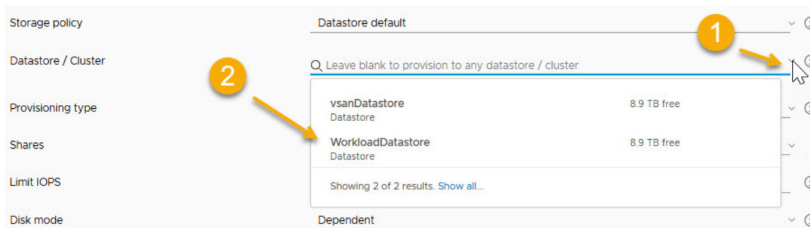
3 Define a storage profile for VMware Cloud on AWS deployments.

Configure a storage profile that targets a datastore/cluster that is accessible to the CloudAdmin user.

- a Select **Infrastructure > Configure > Storage Profiles** and click new **New Storage Profile**.

Setting	Sample Value
Account / region	OurCo-VMC / Datacenter:Datacenter-abz Select the VMware Cloud on AWS cloud account, and its matched SDDC data center, that you created in Create a VMware Cloud on AWS cloud account in vRealize Automation within a sample workflow .
Name	vmc-storage1
Description	Contains the datastore cluster that can be deployed to by cloud template administrators who have VMware Cloud on AWS CloudAdmin credentials.

- b From the **Datastore / Cluster** drop-down menu, select the **WorkloadDatastore** datastore.



For VMware Cloud on AWS in vRealize Automation Cloud Assembly, the storage policy must use the **WorkloadDatastore** datastore to support VMware Cloud on AWS deployment.

4 Save the storage profile.

What to do next

[Create a project to support VMware Cloud on AWS deployments in vRealize Automation.](#)

Create a project to support VMware Cloud on AWS deployments in vRealize Automation

In this step, you define a vRealize Automation project that can be used to control which resources are available for VMware Cloud on AWS deployments.

For information about projects, see [How do vRealize Automation Cloud Assembly projects work at deployment time](#).

Unless otherwise indicated, the step values that you enter in this procedure are for this example workflow only.

Prerequisites

- Complete the [Configure network and storage profiles for VMware Cloud on AWS deployments in vRealize Automation](#) procedure.
- This procedure assumes that you have the required administrator credentials, including VMware Cloud on AWS CloudAdmin credentials for the target SDDC in vCenter. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- This procedure assumes that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).

Procedure

- 1 Select **Infrastructure > Administration > Projects**.
- 2 Click **New Project** and enter the project name `VMC_proj-1_abz`.
- 3 Click **Users** and click **Add Users**.

The users need CloudAdmin credentials to their organization's VMware Cloud on AWS subscription.

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

- 4 Click **Provisioning** and then click **Add Cloud Zone**.
- 5 Add the cloud zone that you configured in the earlier step.

Setting	Sample Value
Cloud zone	VMC_cloud_zone-1 You created this cloud zone in the earlier step, Create a cloud zone for VMware Cloud on AWS deployments in vRealize Automation .
Provisioning priority	1
Instances limit	3

- 6 For this example, ignore the other options.

What to do next

Create a cloud template to deploy in your VMware Cloud on AWS environment. See [Define a vCenter machine resource in a cloud template design to support VMware Cloud on AWS deployment in vRealize Automation](#).

Define a vCenter machine resource in a cloud template design to support VMware Cloud on AWS deployment in vRealize Automation

In this step, you drag a vCenter machine resource onto the design canvas and add settings for a VMware Cloud on AWS deployment in vRealize Automation.

Create a cloud template design that you can deploy to available VMware Cloud on AWS resources.

Unless otherwise indicated, the step values that you enter in this procedure are for this example workflow only.

Prerequisites

- This procedure assumes that you have cloud template designer credentials. See [What are the vRealize Automation user roles](#).
- This procedure assumes that you have VMware Cloud on AWS CloudAdmin credentials for the target SDDC in vCenter (Datacenter:Datacenter-abz). See [Credentials required for working with cloud accounts in vRealize Automation](#).
- Configure the resource infrastructure and project as described in the preceding sections.

Procedure

- 1 Click the **Design** tab and then click **New**.

Setting	Sample Value
Name	vmc-bp_abz
Description	1
Project	VMC_proj-1_abz This is the project that you created earlier, which supports the cloud zone that you also created earlier. The project is now associated with the cloud zone, which in turn is associated with the VMware Cloud on AWS cloud account/region that you created earlier.

- 2 Slide a vSphere machine resource onto the canvas.
- 3 Edit the following (bold) cloud template resource code in the machine resource.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: ubuntu-1604
      cpuCount: 1
      totalMemoryMB: 1024
      folderName: Workloads
```

The `image` can be any value that is appropriate to your deployment needs.

You must add the `folderName: Workloads` statement to the cloud template design code to support VMware Cloud on AWS deployment. The `folderName: Workloads` setting supports the CloudAdmin credentials in the VMware Cloud on AWS SDDC environment and is required.

Note: While the `folderName: Workloads` setting shown in the above code sample is required, you can add it directly in the cloud template code as shown above or you can add it in the associated cloud zone or project. If the setting is specified in more than one of these three places, the precedence is as follows:

- The project setting overrides the cloud template setting and the cloud zone setting.
- The cloud template setting overrides the cloud zone setting.

Note: You can optionally replace the `cpuCount` and `totalMemoryMB` settings with a `flavor` (sizing) entry, as shown below:

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

If the cloud zone has the folder value set to **Workloads**, you do not need to set the `folderName` property in the cloud template, unless you want to override the cloud zone folder value.

What to do next

Expand on this basic VMware Cloud on AWS workflow by adding network isolation. See [Configure an isolated network in VMware Cloud on AWS workflow in vRealize Automation](#).

Configure an isolated network in VMware Cloud on AWS workflow in vRealize Automation

In this procedure, you add an isolated network for your VMware Cloud on AWS deployment in vRealize Automation.

When you define your VMware Cloud on AWS cloud account, NSX-T settings configured in your VMware Cloud on AWS service are available. For information about configuring NSX-T settings in your VMware Cloud on AWS service, see VMware Cloud on AWS [product documentation](#).

vRealize Automation supports VMware Cloud on AWS with NSX-T. It does not support VMware Cloud on AWS with NSX-V.

vRealize Automation supports network isolation for VMware Cloud on AWS deployments. It does not support other network methods for VMware Cloud on AWS.

This extension of the basic VMware Cloud on AWS workflow describes the following methods of creating an isolated network for use in your cloud template:

- Configure on-demand network-based isolation.
- Configure on-demand security group-based isolation.

Prerequisites

This procedure expands on the basic VMware Cloud on AWS workflow. It uses the same cloud account and region, cloud zone, project, and network profile that you configured in the [Tutorial: Configuring VMware Cloud on AWS for vRealize Automation](#) workflow.

Procedure

1 Define an isolated network for a VMware Cloud on AWS deployment in vRealize Automation

You can configure network isolation for a VMware Cloud on AWS deployment by using either of the following procedures:

2 Define a network component in a cloud template to support network isolation for VMware Cloud on AWS in vRealize Automation

In this step, you drag a network machine component onto a vRealize Automation cloud template canvas and add settings for an isolated network deployment to your target VMware Cloud on AWS environment.

Define an isolated network for a VMware Cloud on AWS deployment in vRealize Automation

You can configure network isolation for a VMware Cloud on AWS deployment by using either of the following procedures:

- [Configure on-demand network-based isolation in vRealize Automation](#)
- [Configure on-demand security group-based isolation in vRealize Automation](#)

Configure on-demand network-based isolation in vRealize Automation

You can configure network isolation for your VMware Cloud on AWS deployment needs by specifying and using on-demand network settings in a network profile.

You can specify an isolated network by using a security group or by using on-demand network settings. In this example, you configure network isolation by specifying on-demand network settings in the network profile. Later, you access the network in a cloud template and use the cloud template in a VMware Cloud on AWS deployment.

Unless otherwise indicated, the step values that you enter in this procedure are for this example workflow only.

Prerequisites

- Complete the [Configure a basic VMware Cloud on AWS workflow in vRealize Automation](#) workflow.
- Review [Configure an isolated network in VMware Cloud on AWS workflow in vRealize Automation](#).
- This procedure assumes that you have the required administrator credentials, including VMware Cloud on AWS CloudAdmin credentials for the target SDDC in vCenter. See [Credentials required for working with cloud accounts in vRealize Automation](#).

- This procedure assumes that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).

Procedure

- 1 Open the network profile that you used in the basic VMware Cloud on AWS workflow, for example `vmc-network1`. See [Configure network and storage profiles for VMware Cloud on AWS deployments in vRealize Automation](#).
- 2 You do not need to make any selections on the **Networks** tab.
- 3 Click the **Network Policies** tab.
- 4 Select the **Create an on-demand network** option and select the default `cgw` network domain. Specify an appropriate CIDR and subnet size.
- 5 Click **Save**.

When you use this network profile, machines are deployed to a network in the default network domain. The network is isolated from other networks by using private or outbound network access.

What to do next

Configure a network component in your cloud template. See [Define a network component in a cloud template to support network isolation for VMware Cloud on AWS in vRealize Automation](#)

Configure on-demand security group-based isolation in vRealize Automation

You can configure network isolation for your VMware Cloud on AWS deployment needs by specifying and using an on-demand security group in a network profile.

You can specify an isolated network by using a security group or by using on-demand network settings. In this example, you configure network isolation by specifying an on-demand security group in the network profile. Later, you specify the network in a cloud template and use the cloud template in a VMware Cloud on AWS deployment.

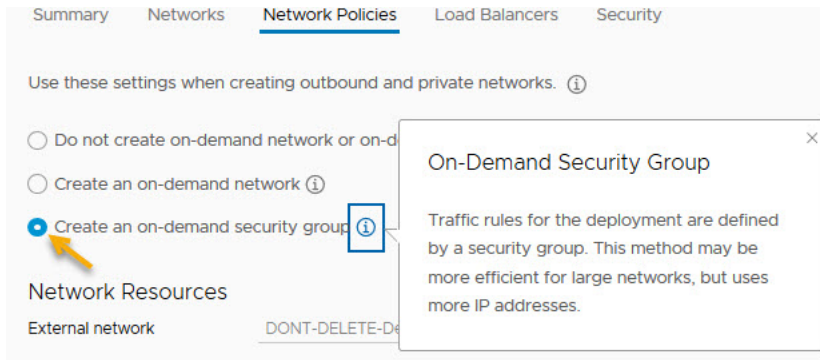
Unless otherwise indicated, the step values that you enter in this procedure are for this example workflow only.

Prerequisites

- Complete the [Configure a basic VMware Cloud on AWS workflow in vRealize Automation](#) workflow.
- Review [Configure an isolated network in VMware Cloud on AWS workflow in vRealize Automation](#).
- This procedure assumes that you have the required administrator credentials, including VMware Cloud on AWS CloudAdmin credentials for the target SDDC in vCenter. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- This procedure assumes that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).

Procedure

- 1 Open the network profile that you used in the basic VMware Cloud on AWS workflow, for example `vmc-network1`. See [Configure network and storage profiles for VMware Cloud on AWS deployments in vRealize Automation](#).
- 2 Select the existing network that you used in the basic VMware Cloud on AWS workflow, for example `sddc-cgw-network-1`. See [Configure network and storage profiles for VMware Cloud on AWS deployments in vRealize Automation](#).
- 3 Click the **Network Policies** tab.
- 4 Select the **Create an on-demand security group** option.



- 5 Click **Save**.

When you use this network profile, machines are deployed to the selected network and are isolated by a new security group policy. The new security policy allows private or outbound network access.

What to do next

Configure a network component in your cloud template. See [Define a network component in a cloud template to support network isolation for VMware Cloud on AWS in vRealize Automation](#)

Define a network component in a cloud template to support network isolation for VMware Cloud on AWS in vRealize Automation

In this step, you drag a network machine component onto a vRealize Automation cloud template canvas and add settings for an isolated network deployment to your target VMware Cloud on AWS environment.

Add network isolation to the cloud template that you created earlier. The cloud template is already associated with a project and cloud zone that support deployment to your VMware Cloud on AWS environment, as well as the network profile and network that you configured for isolation.

Unless otherwise indicated, the step values that you enter in this procedure are for this example workflow only.

Prerequisites

- Complete the [Configure on-demand security group-based isolation in vRealize Automation](#) or [Configure on-demand network-based isolation in vRealize Automation](#) procedure.
- This procedure assumes that you have cloud template designer credentials. See [What are the vRealize Automation user roles](#).
- This procedure assumes that you have VMware Cloud on AWS CloudAdmin credentials for the target SDDC in vCenter. See [Credentials required for working with cloud accounts in vRealize Automation](#).

Procedure

- 1 Open the cloud template that you created in the previous workflow. See [Define a vCenter machine resource in a cloud template design to support VMware Cloud on AWS deployment in vRealize Automation](#).
- 2 From the components on the left of the cloud template design page, drag a network component onto the canvas.
- 3 Edit the network component YAML code to specify a network type of either `private` or `outbound`, as shown in bold.

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

OR

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

What to do next

You are ready to deploy or close the cloud template.

Tutorial: Configuring a provider-specific external IPAM integration for vRealize Automation

You can use an external IPAM provider to manage IP address assignments for your cloud template deployments. This tutorial describes how to configure external IPAM integration in vRealize Automation using Infoblox as the external IPAM provider.

In this procedure, you use an existing IPAM provider package, in this case an Infoblox package, and an existing running environment to build a provider-specific IPAM integration point. You configure an existing network and create a network profile to support IP address allocation from the external IPAM provider. Finally, you create a cloud template that is matched to the network and network profile and deploy networked machines using IP values obtained from the external IPAM provider.

Information about how to obtain and configure the IPAM provider package, and how to configure a running environment that accesses a cloud extensibility proxy to support the IPAM provider integration, is included as reference.

Remember that the values you see are example values. You won't be able to use them letter-by-letter in your environment. Think about where you would make your own substitutions, or extrapolate from the example values, to fit your organization's needs.



To reference a similar vRealize Automation scenario that illustrates an Infoblox IPAM integration workflow in video form, see [Infoblox IPAM Plug-in 1.1 Integration with vRealize Automation 8.1 / vRealize Automation Cloud](#).

Procedure

1 Add required extensible attributes in the Infoblox application for integration with vRealize Automation

Before you can download and deploy the Infoblox provider package (`infoblox.zip`) for integration with vRealize Automation from either the Infoblox website or from the VMware Marketplace, you must add required extensibility attributes in Infoblox.

2 Download and deploy an external IPAM provider package for use in vRealize Automation

Before you can define an external IPAM integration point in vRealize Automation, you need a configured IPAM provider package.

3 Create a running environment for an IPAM integration point in vRealize Automation

Before you can define a external IPAM integration point in vRealize Automation, you need to create or access an existing running environment to serve as an intermediary between the IPAM provider and vRealize Automation. The running environment is commonly an Amazon Web Services or Microsoft Azure cloud account or an on-premises actions-based extensibility integration point that is associated to a cloud extensibility proxy.

4 Add an external IPAM integration for Infoblox in vRealize Automation

vRealize Automation supports integration with an external IPAM provider. This example uses Infoblox as the external IPAM provider.

5 Configure a network and network profile to use external IPAM for an existing network in vRealize Automation

You can define an existing network to use IP address values that are obtained from, and managed by, an external IPAM provider rather than internally from vRealize Automation.

6 Define and deploy a cloud template that uses an external IPAM provider range assignment in vRealize Automation

You can define a cloud template to obtain and manage IP address assignments from your external IPAM provider. This example uses Infoblox as the external IPAM provider.

7 Using Infoblox-specific properties and extensible attributes for IPAM integrations in vRealize Automation

You can use Infoblox-specific properties for vRealize Automation projects that contain external IPAM integrations for Infoblox.

Add required extensible attributes in the Infoblox application for integration with vRealize Automation

Before you can download and deploy the Infoblox provider package (`infoblox.zip`) for integration with vRealize Automation from either the Infoblox website or from the VMware Marketplace, you must add required extensibility attributes in Infoblox.

This procedure is applicable if you are creating an external IPAM integration point for Infoblox integration with vRealize Automation Cloud Assembly.

Before you can use the `infoblox.zip` download, you must log in to your Infoblox account, using your organization account administrator credentials, and pre-create the following Infoblox extensible attributes:

- VMware NIC index
- VMware resource ID
- Tenant ID
- CMP Type
- VM ID
- VM Name

Prerequisites

- Verify that you have an account with [Infoblox](#) and that you have the correct access credentials to your organization's Infoblox account.
- Confirm that the Infoblox WAPI version is supported. IPAM integration with Infoblox depends on Infoblox WAPI version v2.7. All Infoblox appliances that support WAPI v2.7 are supported.
- Review [Using Infoblox-specific properties and extensible attributes for IPAM integrations in vRealize Automation](#).

Procedure

- 1 Log in to your Infoblox account using administrator credentials.

These are the same administrator user name and password credentials that you specify when you create an external IPAM integration point in vRealize Automation Cloud Assembly using the **Infrastructure > Connections > Integrations >** menu sequence.

- 2 Use the procedure described in the Infoblox documentation to create the following required extensible attributes in your Infoblox application.

- VMware NIC index - type Integer
- VMware resource ID - type String
- Tenant ID - type String
- CMP Type - type String
- VM ID - type String
- VM Name - type String

The procedure is described in the *Adding Extensible Attributes* section of the Infoblox documentation topic [About Extensible Attributes](#). Also see [Managing Extensible Attributes](#).

What to do next

After you add the required attributes, you can resume the process of downloading and deploying the Infoblox package as described in [Download and deploy an external IPAM provider package for use in vRealize Automation](#).

Download and deploy an external IPAM provider package for use in vRealize Automation

Before you can define an external IPAM integration point in vRealize Automation, you need a configured IPAM provider package.

You can download a provider-specific integration package from your IPAM provider's website, from the [VMware solutions exchange marketplace](#) or, if available, from the vRealize Automation **Marketplace** tab.

Note This example uses the VMware-supplied Infoblox package `Infoblox.zip`, which is available for download from [VMware Marketplace](#) as follows:

- [vRA Cloud Infoblox plugin version 1.2](#) - Compatible with vRealize Automation 8.1.x and 8.2.x
- [vRA Cloud Infoblox plugin version 1.1](#) - Compatible with vRealize Automation 8.1.x
- [vRA Cloud Infoblox plugin version 1.0](#) - Compatible with vRealize Automation 8.0.1.x with or without an internet connection to the global network.
- [vRA Cloud Infoblox plugin version 0.4](#) - Compatible with vRealize Automation 8.0.0.x and 8.0.1.x when there is an internet connection with the global network.

IPAM integration with Infoblox depends on Infoblox WAPI version v2.7. All Infoblox appliances that support WAPI v2.7 are supported.

For information about how to create an IPAM integration package for other IPAM providers, if one does not already exist in the Marketplace, see [How do I use the IPAM SDK to create a provider-specific external IPAM integration package for vRealize Automation](#).

The IPAM provider package contains scripts that are packaged with metadata and other configurations. The scripts contain the source code used for the operations that vRealize Automation performs in coordination with the external IPAM provider. Example operations include `Allocate an IP address for a virtual machine`, `Fetch a list of IP ranges from the provider`, and `Update the MAC address of a host record in the provider`.

Prerequisites

- Verify that you have cloud administrator credentials. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- Verify that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).
- Verify that you have an account with the external IPAM provider, for example [Infoblox](#) or [Bluecat](#), and that you have the correct access credentials to your organization's account with the IPAM provider.
- If you are using Infoblox as your external IPAM provider, verify that you have added the required extensible attributes to your Infoblox account before continuing. See [Add required extensible attributes in the Infoblox application for integration with vRealize Automation](#).

Note A certificate chain issue exists that is derived from how the Python element in the Infoblox plug-in handles SSL handshakes. For information about the issue and its required actions, see Knowledge Base Article [vRA Cloud Infoblox Plugin throws a certificate chain error during authentication process \(88057\)](#).

Procedure

- 1 Navigate to the [vRA Cloud Infoblox plugin version 1.1](#) package page at [VMware Marketplace](#).
- 2 Log in and download the plug-in package.
- 3 If you have not already done so, add the required extensible attributes in Infoblox. See [Add required extensible attributes in the Infoblox application for integration with vRealize Automation](#).

Results

The package is now available for you to deploy by using the **Integrations > Add Integration > IPAM > Manage Providers > Import package** menu sequence as described in [Add an external IPAM integration for Infoblox in vRealize Automation](#).

Create a running environment for an IPAM integration point in vRealize Automation

Before you can define a external IPAM integration point in vRealize Automation, you need to create or access an existing running environment to serve as an intermediary between the IPAM provider and vRealize Automation. The running environment is commonly an Amazon Web Services or Microsoft Azure cloud account or an on-premises actions-based extensibility integration point that is associated to a cloud extensibility proxy.

External IPAM integration requires a running environment. When you define the IPAM integration point, you create a connection between vRealize Automation Cloud Assembly and your IPAM provider by specifying an available running environment.

IPAM integration uses a set of downloaded provider-specific scripts or plug-ins in a running environment that is facilitated by a Feature-as-a-Services (FaaS) provider such as Amazon Web Services Lambda, Microsoft Azure Functions, or an actions-based extensibility (ABX) On-Prem Embedded integration point. The running environment is used to connect to the external IPAM provider, for example Infoblox.

Note An Infoblox IPAM integration point requires an actions-based extensibility (ABX) On-Prem Embedded integration point.

Each type of runtime environment has advantages and disadvantages:

- Actions-based extensibility (ABX) integration point
 - free, no additional vendor usage costs
 - can connect to IPAM vendor appliances that reside in an on-premises data center behind a NAT/firewall that is not publicly accessible, for example Infoblox
 - slower and slightly less reliable performance than commercial cloud vendors
- Amazon Web Services
 - has associated vendor FaaS connection/usage costs

- cannot connect to IPAM vendor appliances that reside in an on-premises data center behind a NAT/firewall that is not publicly accessible
- has fast and highly reliable performance
- Microsoft Azure
 - has associated vendor FaaS connection/usage costs
 - cannot connect to IPAM vendor appliances that reside in an on-premises data center behind a NAT/firewall that is not publicly accessible
 - has fast and highly reliable performance

Prerequisites

- Verify that you have cloud administrator credentials. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- Verify that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).
- Verify that you have an account with the external IPAM provider, for example [Infoblox](#) or [Bluecat](#), and that you have the correct access credentials to your organization's account with the IPAM provider.
- Verify that you have access to a deployed integration package for your IPAM provider, such as Infoblox or BlueCat. The deployed package is initially obtained as a .zip download from your IPAM provider website or from the vRealize Automation Cloud Assembly Marketplace and then deployed in vRealize Automation Cloud Assembly.

For information about how to deploy the provider package .zip file and make it available as a **Provider** value on the IPAM Integration page, see [Download and deploy an external IPAM provider package for use in vRealize Automation](#).

Procedure

- 1 To create an On-Prem FaaS-based extensibility action to use as an IPAM integration running environment, select **Extensibility > Library > Actions**.
- 2 Click **New Action**, enter an action name and description, and specify a project.
- 3 In the **FaaS provider** drop-down menu, select **On Prem**.
- 4 Complete the form to define the extensibility action.



For related information about the running environment, see this [Infoblox IPAM Plug-in 1.1 Integration](#) blog video at approximately 24 minutes into the video.

Add an external IPAM integration for Infoblox in vRealize Automation

vRealize Automation supports integration with an external IPAM provider. This example uses Infoblox as the external IPAM provider.

You can use a provider-specific IPAM integration point to obtain and manage IP addresses and related network characteristics for cloud template deployments.

In this example, you create an external IPAM integration point to support access to your organization's account with an external IPAM provider. In this example workflow, the IPAM provider is Infoblox and the provider-specific integration package already exists. While these instructions are specific to an Infoblox integration, they can be used as reference if creating an IPAM integration for a different external IPAM provider.

You can obtain a provider-specific integration package from your IPAM provider's website, from the [VMware solutions exchange marketplace](#) or, if available, from the vRealize Automation Cloud Assembly **Marketplace** tab.

This example uses the VMware-supplied Infoblox package `Infoblox.zip`, which is available for download from the VMware solutions exchange marketplace as follows:

- [vRA Cloud Infoblox plugin version 1.1](#) - supports vRealize Automation 8.1 forward
- [vRA Cloud Infoblox plugin version 1.0](#) - supports vRealize Automation 8.0.1
- [vRA Cloud Infoblox plugin version 0.1](#) - supports vRealize Automation 8.0

Prerequisites

- Verify that you have cloud administrator credentials. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- Verify that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).
- Verify that you have an account with external IPAM provider and that you have the correct access credentials to your organization's account with the IPAM provider.
- Verify that you have access to a deployed integration package for your IPAM provider. The deployed package is initially obtained as a .zip download from your IPAM provider website, or from the VMware solutions exchange marketplace, and then deployed to vRealize Automation.

For information about how to download and deploy the provider package .zip file and make it available as a **Provider** value on the IPAM Integration page, see [Download and deploy an external IPAM provider package for use in vRealize Automation](#).

- Verify that you have access to a configured running environment for the IPAM provider. The running environment is typically an actions-based extensibility (ABX) On-Prem Embedded integration point.

For information about running environment characteristics, see [Create a running environment for an IPAM integration point in vRealize Automation](#).

- Enable required extensible attributes in your Infoblox application. See [Add required extensible attributes in the Infoblox application for integration with vRealize Automation](#).
- If you do not have external Internet access, you can configure an Internet server proxy. See [How do I configure an Internet proxy server for vRealize Automation](#).

- Verify that you have the required user credentials to access and use your Infoblox IPAM product. For example, open the Administration tab in the Infoblox appliance and customize administrator, groups, and roles entries. You must be a member of a group that has administrator or superuser permissions or a custom group that has DHCP, DNS, IPAM, and Grid permissions. These settings allow access to all the functionality that is available in the Infoblox plug-in, enabling you to create an Infoblox IPAM integration and designers to use that IPAM integration in cloud templates and deployments. For more information about user permissions, see your Infoblox product documentation.

Procedure

- 1 Select **Infrastructure > Connections > Integrations** and click **Add Integration**.
- 2 Click **IPAM**.
- 3 In the **Provider** drop-down, select a configured IPAM provider package from the list, for example *Infoblox_hrg*.

If the list is empty, click **Import Provider Package**, navigate to an existing provider package .zip file, and select it. If you do not have the provider .zip file, you can obtain it from your IPAM provider's web site or from the vRealize Automation Cloud Assembly **Marketplace** tab.

For information about how to deploy the provider package .zip file in vCenter and make it available as a **Provider** value on the Integration page, see [Download and deploy an external IPAM provider package for use in vRealize Automation](#).

For information about how to upgrade an existing IPAM integration to use a more recent version of a vendor's IPAM integration package, see [How to upgrade to a newer external IPAM integration package in vRealize Automation](#).

- 4 Enter your administrator user name and password credentials for your account with the external IPAM provider, along with all other (if any) mandatory fields, such as the host name of your provider.

In this example, you obtain the host name of your Infoblox IPAM provider using the following steps:

- a In a separate browser tab, log in to your IPAM provider account using your Infoblox administrator credentials.
- b Copy your host name URL.
- c Paste your host name URL in the **Hostname** field on the IPAM Integration page.

- 5 In the **Running Environment** drop-down list, select an existing on-premises actions-based extensibility integration point, for example *Infoblox_abx_intg*.

The running environment supports communication between vRealize Automation and the external IPAM provider.

Note If you use an Amazon Web Services or Microsoft Azure cloud account as the integration running environment, be sure that the IPAM provider appliance is accessible from the Internet and is not behind a NAT or firewall and that it has a publicly resolvable DNS name. If the IPAM provider is not accessible, the Amazon Web Services Lambda or Microsoft Azure Functions cannot connect to it and the integration will fail. For related information, see [Create a running environment for an IPAM integration point in vRealize Automation](#).

The IPAM framework only supports an actions-based extensibility (ABX) On-Prem Embedded running environment.

Note An Infoblox IPAM integration point requires an actions-based extensibility (ABX) On-Prem Embedded integration point.

The configured cloud account or integration point allows communication between vRealize Automation and the IPAM provider, in this example Infoblox, through an associated cloud extensibility proxy. You can select a provider that has already been created or you can create one.

For information about how to create a running environment, see [Create a running environment for an IPAM integration point in vRealize Automation](#).

- 6 Click **Validate**.

Because this example uses the on-premises actions-based extensibility integration for the running environment, you can view the validation action.

- a Click the **Extensibility** tab.
- b Click **Activity > Action Runs** and select either **All Runs** or **Integration runs** from the filter to note that an endpoint validation action is initiated and running.

- 7 When prompted to trust the self-signed certificate from the IPAM provider, click **Accept**.

After you accept the self-signed certificate, the validation action can continue to completion.

- 8 Enter a **Name** for this IPAM integration point, such as *Infoblox_Integration*, and a **Description**, such as *Infoblox IPAM with ABX integration for team HRG*.

- 9 Click **Add** to save the new external IPAM integration point.

A data collection action is initiated. Networks and IP ranges are data-collected from the IPAM provider. You can view the data collection action as follows:

- a Click the **Extensibility** tab.
- b Click **Activity > Action Runs** and note that a data collection action is initiated and running. You can open and view the action run content.

Results

The provider-specific external IPAM integration is now available for use with networks and network profiles.

Configure a network and network profile to use external IPAM for an existing network in vRealize Automation

You can define an existing network to use IP address values that are obtained from, and managed by, an external IPAM provider rather than internally from vRealize Automation.

You can define a network to access existing IP settings that you have defined in your organization's external IPAM provider account. This step expands on the Infoblox provider integration that you created in the previous step.

In this example, you configure a network profile with existing networks that were data-collected from vCenter. You then configure these networks to obtain IP information from an external IPAM provider, in this case Infoblox. Virtual machines that you provision from vRealize Automation that can be matched with this network profile obtain their IP and other TCP/IP related settings from the external IPAM provider.

For more information about networks, see [Network resources in vRealize Automation](#). For more information about network profiles, see [How to add network profiles in vRealize Automation](#) and [Learn more about network profiles in vRealize Automation](#).

For related information, see [How do I configure a network profile to support an on-demand network for an external IPAM integration in vRealize Automation](#).

Prerequisites

This sequence of steps is shown in the context of an IPAM provider integration workflow. See [Tutorial: Configuring a provider-specific external IPAM integration for vRealize Automation](#).

- Verify that you have cloud administrator credentials. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- Verify that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).
- Verify that you have an account with the external IPAM provider, for example [Infoblox](#) or [Bluecat](#), and that you have the correct access credentials to your organization's account with the IPAM provider. In this example workflow, the IPAM provider is Infoblox.
- Verify that you have an IPAM integration point for the IPAM provider. See [Add an external IPAM integration for Infoblox in vRealize Automation](#).

Procedure

- 1 To configure a network, click **Infrastructure > Resources > Networks**.

- 2 On the **Networks** tab, select an existing network to use with the IPAM provider integration point. In this example, the network name is *net.23.117-only-IPAM*.

Listed networks have been data-collected by vRealize Automation from a vCenter in your organization.

- 3 To obtain values from the external IPAM provider, verify that except for the **Account/region**, **Name**, and **Network domain**, all other network settings are empty, including the following:
 - Domain (See Note in step 8)
 - CIDR
 - Default gateway
 - DNS servers
 - DNS search domains
- 4 Click the **IP Ranges** tab and click **Add IPAM IP Range**.
- 5 From the **Network** menu, select the network that you just configured, for example *net.23.117-only-IPAM*.
- 6 From the **Provider** menu, select the *Infoblox_Integration* IPAM integration point that you created earlier in the workflow
- 7 From the now-visible **Address Space** drop-down menu, select one of the listed network views.

An address space in Infoblox is referred to as a network view.

The network views are obtained from your IPAM provider account. This example uses the network subnet that you just configured, for example *net.23.117-only-IPAM*, the *Infoblox_Integration* integration point that you created earlier in the workflow, and an address space named *default*.

Listed address space values are obtained from the external IPAM provider.

- 8 From the list of displayed networks that are available for the selected address space, select one or more networks, for example select 10.23.117.0/24.

For this example, the **Domains** and **DNS Servers** column values for the selected network contain values from Infoblox.

Note If you select a network in Step 3 that had a Domain specified for vRealize Automation, and then select a network from the external IPAM provider address space that contains a Domain value, the Domain value in the external IPAM provider network takes precedence over the Domain specified in vRealize Automation. If the IPAM IP range setting doesn't have a Domain value, specified in either Cloud Assembly or in the external IPAM provider as described above, provisioning fails.

For Infoblox, you can use the blueprint property `Infoblox.IPAM.Network.dnsSuffix` at the machine level to overwrite the Domain value. For related information, see [Using Infoblox-specific properties and extensible attributes for IPAM integrations in vRealize Automation](#).

- 9 Click **Add** to save the IPAM IP range for the network.

The range is visible in the **IP Ranges** table.

- 10 Click the **IP Addresses** tab.

After you provision a machine by using the new address range from the external IPAM provider, a new record will be visible in the **IP Addresses** table.

- 11 To configure a network profile to use the network, click **Infrastructure > Configure > Network Profiles**.

- 12 Name the network profile, for example *Infoblox-NP*, and add the following sample settings.

- Summary tab
 - Specify a vSphere cloud account/region.
 - Add a capability tag for the network profile, for example named *infoblox_abx*.
Make note of the capability tag, as you must also use it as a cloud template constraint tag to make the provisioning association in the cloud template.
- Networks tab
 - Add the network that you created earlier, for example *net.23.117-only-IPAM*.

- 13 Click **Save** to save the network profile with these settings.

Results

The network and network profile setting are now configured for an existing network type to be used for the Infoblox IPAM integration in a cloud template design.

Define and deploy a cloud template that uses an external IPAM provider range assignment in vRealize Automation

You can define a cloud template to obtain and manage IP address assignments from your external IPAM provider. This example uses Infoblox as the external IPAM provider.

In this final step in the external IPAM integration workflow, you define and deploy a cloud template that connects your previously defined network and network profile to your organization's Infoblox account to obtain and manage IP address assignments for deployed VMs from the external IPAM provider rather than from vRealize Automation Cloud Assembly.

This workflow uses Infoblox as the external IPAM provider and in some steps, the example values are unique to Infoblox, although the intent is that the procedure can be applied to other external IPAM integrations.



The [Automate IPAM and DNS for VMs using VMware vRealize Automation and Infoblox DDI](#) Infoblox blog provides related information.

After you deploy the cloud template and the VM is started, the IP address used for each VM in the deployment appears as a network entry in the **Resources > Networks** page, as a new host record in the IPAM provider network in your IPAM provider's account, and in the vSphere Web Client record for each deployed VM in the host vCenter.

Prerequisites

This sequence of steps is shown in the context of an external IPAM provider integration workflow. See [Tutorial: Configuring a provider-specific external IPAM integration for vRealize Automation](#) .

- Verify that you have cloud administrator credentials. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- Verify that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).
- Verify that you have an account with the external IPAM provider, for example Infoblox or BlueCat, and that you have the correct access credentials to your organization's account with the IPAM provider.
- Verify that you have administrator access to the host account and any role requirements needed to display status records in the vSphere web client record for your deployed VMs in the host vCenter.
- Verify that you have an IPAM integration point for the external IPAM provider. See [Add an external IPAM integration for Infoblox in vRealize Automation](#) .
- Verify that you have configured a vRealize Automation Cloud Assembly network and network profile that support external IPAM integration for your intended IPAM integration point. See [Configure a network and network profile to use external IPAM for an existing network in vRealize Automation](#) .
- Verify that your project and cloud zone are tagged to match tags in the IPAM integration point and network or network profile. Optionally configure the project to support custom resource naming.

For more information than provided about the role of a project and cloud zone, as well as the role of other infrastructure elements in your cloud template, see [Tutorial: Setting up and testing multi-cloud infrastructure and deployments in vRealize Automation Cloud Assembly](#). For more information about tagging, see [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments](#).

For information about custom naming VMs by using settings in your project, see [How to customize the names of deployed resources using vRealize Automation Cloud Assembly](#).

Procedure

- 1 Click **Cloud templates > New**, enter the following information in the **New cloud template** page, and click **Create**.
 - **Name** = ipam-bpa

- **Description** = Cloud template that uses Infoblox IPAM integration
 - **Project** = 123VC
- 2 For this example, add a cloud agnostic machine component and a cloud agnostic network component to the cloud template canvas and connect the two components.
 - 3 Edit the cloud template code to add a constraint tag to the network component that matches the capability tag that you added to the network profile. For this example, that tag value is *infoblox_abx*.
 - 4 Edit the cloud template code to specify that the network assignment type is *static*.

When using an external IPAM provider, the `assignment: static` setting is required.

For this example, the specified IP address 10.23.117.4 is known to be currently available in the external IPAM address space that we selected for the network in the associated network profile. While the `assignment: static` setting is required, the `address: value` setting is not. You can choose to begin external IP address selection at a particular address value, but doing so is not required. If you do not specify an `address: value` setting, the external IPAM provider selects the next available address in the external IPAM network.

- 5 Verify the cloud template code against the following example.

```
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}'
```

For examples of Infoblox properties that are available for specifying DNS and DHCP settings in cloud templates, see [Using Infoblox-specific properties and extensible attributes for IPAM integrations in vRealize Automation](#).

- 6 Click **Deploy** on the cloud template page, name the deployment *Infoblox-1*, and click **Deploy** on the **Deployment Type** page.

- 7 As the cloud template is being deployed, click the **Extensibility** tab and select **Activity > Action Runs** to see the *Infoblox_AllocateIP_n* extensibility action running.

After the extensibility action is completed and the machine is provisioned, the *Infoblox_Update_n* action propagates the MAC address to Infoblox.

- 8 You can log in to and open your Infoblox account to see the new host record for the IPAM address in the associated 10.23.117.0/24 network. You can also open the DNS tab in Infoblox to see the new DNS host record.

- 9 To verify that the VM is being provisioned, log in to your host vCenter and vSphere Web Client to locate the provisioned machine and view the DNS name and IP address.

After the provisioned VM is started, the MAC address is propagated to Infoblox by an *Infoblox_AllocateIP* extensibility action.

- 10 To view the new network record in vRealize Automation Cloud Assembly, select **Infrastructure > Resources > Networks** and click to open the **IP Addresses** tab.

- 11 If you delete the deployment, the IPAM address of VMs in the deployment are released and the IP addresses are again available to the external IPAM provider for other allocations. The extensibility action for this event in vRealize Automation Cloud Assembly is *Infoblox_Deallocate*.

Using Infoblox-specific properties and extensible attributes for IPAM integrations in vRealize Automation

You can use Infoblox-specific properties for vRealize Automation projects that contain external IPAM integrations for Infoblox.

The following Infoblox properties are available for use with your Infoblox IPAM integrations in cloud template designs and deployments. You can use them in vRealize Automation to further control IP address allocation during cloud template deployment. Use of these properties is optional.

- `Infoblox.IPAM.createFixedAddress`

This property enables you to create a fixed address record inside Infoblox. Possible values are True and False. By default, a host record is created. The default value is False.

- `Infoblox.IPAM.Network.dnsView`

This property enables you to use a DNS view when creating a host record inside Infoblox.

- `Infoblox.IPAM.Network.enableDns`

When allocating an IP in Infoblox, this property enables you to also create a DNS record. Possible values are True and False. The default value is True.

- `Infoblox.IPAM.Network.enableDhcp`

You can set this option to True to enable the DHCP configuration for the host address.

- `Infoblox.IPAM.Network.dnsSuffix`

This property enables you to overwrite the *domain* DHCP option of an Infoblox network with a new one. This capability is useful if the Infoblox network does not have the *domain* DHCP option set or if the *domain* DHCP option must be overwritten. The default value is null (empty string).

`Infoblox.IPAM.Network.dnsSuffix` is only applicable if

`Infoblox.IPAM.Network.enableDns` is set to `True`.

You can specify an Infoblox property using one of the following methods in vRealize Automation Cloud Assembly:

- You can specify properties in a project by using the **Custom Properties** section on your **Infrastructure > Administration > Projects** page. Using this method, the specified properties are applied to all machines that are provisioned in the scope of this project.
- You can specify properties on each machine component in a cloud template. Sample cloud template code illustrating use of the `Infoblox.IPAM.Network.dnsView` property is shown below:

```
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
```

- You can specify properties by using an extensibility subscription.

For related information about Infoblox extensible attributes relative to this use case, see [Add required extensible attributes in the Infoblox application for integration with vRealize Automation](#).

Using Infoblox properties on different machine NICs in a cloud template

The following Infoblox properties can have a different value for each machine NIC in the cloud template:

- `Infoblox.IPAM.Network.enableDhcp`
- `Infoblox.IPAM.Network.dnsView`

■ Infoblox.IPAM.Network.enableDns

For example, to use a different `Infoblox.IPAM.Network.dnsView` value for each NIC, use a `Infoblox.IPAM.Network<nicIndex>.dnsView` entry for each NIC. The following sample shows different values `Infoblox.IPAM.Network.dnsView` for two NICs.

```
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
```

By default, the Infoblox integration creates a DNS host record in the *default* DNS view in Infoblox. If your Infoblox administrator has created *custom* DNS views, you can overwrite the default integration behavior and specify a named view by using the `Infoblox.IPAM.Network.dnsView` property in the machine component. For example, you can add the following property to the `Cloud_Machine_1` component to specify a named DNS view in Infoblox.

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

For information about configuring and using DNS views, see [DNS Views](#) in Infoblox product documentation. For examples in the Infoblox integration workflow, see [Define and deploy a cloud template that uses an external IPAM provider range assignment in vRealize Automation](#).

Setting up vRealize Automation Cloud Assembly for your organization

3

As a Cloud Assembly administrator, you must understand the user roles and set up connections with your cloud account vendor and integration applications.

When you configure the cloud accounts and integrations, you are configuring the communication between Cloud Assembly and those target systems.

This chapter includes the following topics:

- [What are the vRealize Automation user roles](#)
- [Adding cloud accounts to vRealize Automation Cloud Assembly](#)
- [Integrating vRealize Automation with other applications](#)
- [What are onboarding plans in vRealize Automation Cloud Assembly](#)
- [Advanced configuration for vRealize Automation Cloud Assembly environment](#)

What are the vRealize Automation user roles

vRealize Automation has several levels of user roles. These different level control access to the organization, the services, the projects that produce or consume the cloud templates, catalog items, and pipelines, and the ability for users to use or see individual parts of the user interface. These different levels give cloud administrators different tools to apply any level of granularity that is required by their operational needs.

General role descriptions

The user roles are defined at different levels. The service level roles are defined for each service. More details for the service roles is provided below this table.

Role	General permissions	Where the role is defined
Organization Owner	<p>Can access the console and add users to organization.</p> <p>The organization owner cannot access a service unless they have a service role.</p> <p>More about the Organization User Roles</p>	Organization console
Organization Member	<p>Can access the console.</p> <p>The organization member cannot access a service unless they have a service role.</p> <p>More about the Organization User Roles</p>	Organization console
Service Administrator	<p>Can access the console and has full view, update, and delete privileges in the service.</p> <ul style="list-style-type: none"> ■ Cloud Assembly Service Roles ■ Service Broker Service Roles ■ Code Stream Service Roles 	Organization console
Service User	<p>Can access the console and the service with limited permissions.</p> <p>The service member has limited user interface. What they can see or do depends on their project membership.</p> <ul style="list-style-type: none"> ■ Cloud Assembly Service Roles ■ Service Broker Service Roles ■ Code Stream Service Roles 	Organization console
Service Viewer	<p>Can access the console and the service in a view-only mode.</p> <ul style="list-style-type: none"> ■ Cloud Assembly Service Roles ■ Service Broker Service Roles ■ Code Stream Service Roles 	Organization console
Executor (vRealize Automation Code Stream only)	<p>Can access the console and manage pipeline executions.</p> <p>Code Stream Service Roles</p>	Organization console
vRA Migration Assistant Administrator	<p>Can access the console and has full view, update, and delete privileges in the vRA Migration Assistant and Cloud Assembly.</p> <p>This role must also have at least the Cloud Assembly Viewer role.</p>	Organization console

Role	General permissions	Where the role is defined
vRA Migration Assistant Viewer	Can access the console, vRA Migration Assistant, and Cloud Assembly in a view-only mode. This role must also have at least the Cloud Assembly Viewer role.	Organization console
Orchestrator Administrator	Can access all vRealize Orchestrator Client features and content, including the content created by specific groups.	Organization console and in the vRealize Orchestrator Client
Orchestrator Workflow Designer	Can create, run, edit, and delete their own vRealize Orchestrator Client content. Can add their own content to their assigned group. Does not have access to the administration and troubleshooting features of the vRealize Orchestrator Client.	Organization console and in the vRealize Orchestrator client
Project roles	Can view and manage project resources depending on project role. Project roles include administrator, member, and viewer. Organization and service user roles in vRealize Automation	vRealize Automation Cloud Assembly, vRealize Automation Service Broker, and vRealize Automation Code Stream
Custom roles	The permissions are defined by the vRealize Automation Cloud Assembly for all the services. The user must have at least a service viewer role in the relevant services so that they can access the service. The custom roles take precedence over the service roles. Custom user roles in vRealize Automation	vRealize Automation Cloud Assembly and vRealize Automation Service Broker

Organization and service user roles in vRealize Automation

The organization and service user roles that are defined for the vRealize Automation Cloud Assembly, vRealize Automation Service Broker, and vRealize Automation Code Stream services determine what the user can see and do in each service.

Organization User Roles

User roles are defined for the organization in the vRealize Automation console by an organization owner. There are two types of roles, organization roles and service roles.

The organization roles are global and apply to all services in the organization. The organization-level roles are Organization owner or Organization Member role.

For more information about the organization roles, see [Administering vRealize Automation](#).

The vRealize Automation Cloud Assembly service roles, which are service-specific permissions, are also assigned at the organization level in the console.

Service Roles

These service roles are assigned by the organization owner.

This article includes information about all three services.

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

Cloud Assembly Service Roles

The vRealize Automation Cloud Assembly service roles determine what you can see and do in vRealize Automation Cloud Assembly. These service roles are defined in the console by an organization owner.

Table 3-1. vRealize Automation Cloud Assembly Service Role Descriptions

Role	Description
Cloud Assembly Administrator	A user who has read and write access to the entire user interface and API resources. This is the only user role that can see and do everything, including add cloud accounts, create new projects, and assign a project administrator.
Cloud Assembly User	A user who does not have the Cloud Assembly Administrator role. In a vRealize Automation Cloud Assembly project, the administrator adds users to projects as project members, administrators, or viewers. The administrator can also add a project administrator.
Cloud Assembly Viewer	A user who has read access to see information but cannot create, update, or delete values. This is a read-only role across all projects. Users with the viewer role can see all the information that is available to the administrator. They cannot take any action unless you make them a project administrator or a project member. If the user is affiliated with a project, they have the permissions related to the role. The project viewer would not extend their permissions the way that the administrator or member role does.

In addition to the service roles, vRealize Automation Cloud Assembly has project roles. Any project is available in all of the services.

The project roles are defined in vRealize Automation Cloud Assembly and can vary between projects.

In the following tables, which tells you what the different service and project roles can see and do, remember that the service administrators have full permission on all areas of the user interface.

The descriptions of project roles will help you decide what permissions to give your users.

- Project administrators leverage the infrastructure that is created by the service administrator to ensure that their project members have the resources they need for their development work.
- Project members work within their projects to design and deploy cloud templates.
- Project viewers are restricted to read-only access, except in a few cases where they can do non-destructive things like download cloud templates.

Table 3-2. vRealize Automation Cloud Assembly service roles and project roles

UI Context	Task	Cloud Assembly Administrator	Cloud Assembly Viewer	Cloud Assembly User User must be a project administrator or member to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
Access Cloud Assembly						
Console	In the vRA console, you can see and open Cloud Assembly	Yes	Yes	Yes	Yes	Yes
Infrastructure						
	See and open the Infrastructure tab	Yes	Yes	Yes	Yes	Yes
Configure - Projects	Create projects	Yes				
	Update, or delete values from project summary, provisioning, Kubernetes, integrations, and test project configurations.	Yes				
	Add users and groups, and assign roles in projects.	Yes		Yes. Your projects.		
	View projects	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Configure - Cloud Zones	Create, update, or delete cloud zones	Yes				
	View cloud zones	Yes	Yes			

Table 3-2. vRealize Automation Cloud Assembly service roles and project roles (continued)

UI Context	Task	Cloud Assembly Administrator	Cloud Assembly Viewer	Cloud Assembly User User must be a project administrator or member to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
Configure - Kubernetes Zones	Create, update, or delete Kubernetes zones	Yes				
	View Kubernetes zones	Yes	Yes			
Configure - Flavors	Create, update, or delete flavors	Yes				
	View flavors	Yes	Yes			
Configure - Image Mappings	Create, update, or delete image mappings	Yes				
	View image mappings	Yes	Yes			
Configure - Network Profiles	Create, update, or delete network profiles	Yes				
	View image network profiles	Yes	Yes			
Configure - Storage Profiles	Create, update, or delete storage profiles	Yes				
	View image storage profiles	Yes	Yes			
Configure - Pricing Cards	Create, update, or delete pricing cards	Yes				
	View the pricing cards	Yes	Yes			
Configure - Tags	Create, update, or delete tags	Yes				
	View tags	Yes	Yes			
Resources - Compute	Add tags to discovered compute resources	Yes				
	View discovered compute resources	Yes	Yes			

Table 3-2. vRealize Automation Cloud Assembly service roles and project roles (continued)

UI Context	Task	Cloud Assembly Administrator	Cloud Assembly Viewer	Cloud Assembly User User must be a project administrator or member to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
Resources - Networks	Modify network tags, IP ranges, IP addresses	Yes				
	View discovered network resources	Yes	Yes			
Resources - Security	Add tags to discovered security groups	Yes				
	View discovered security groups	Yes	Yes			
Resources - Storage	Add tags to discovered storage	Yes				
	View storage	Yes	Yes			
Resources - Machines	Add and delete machines	Yes				
	View machines	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Resources - Volumes	Delete discovered storage volumes	Yes				
	View discovered storage volumes	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects.
Resources - Kubernetes	Deploy or add Kubernetes clusters, and create or add namespaces	Yes				
	View Kubernetes clusters and namespaces	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Activity - Requests	Delete deployment request records	Yes				
	View deployment request records	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Activity - Event Logs	View event logs	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Connections - Cloud Accounts	Create, update, or delete cloud accounts	Yes				

Table 3-2. vRealize Automation Cloud Assembly service roles and project roles (continued)

UI Context	Task	Cloud Assembly Administrator	Cloud Assembly Viewer	Cloud Assembly User User must be a project administrator or member to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
	View cloud accounts	Yes	Yes			
Connections - Integrations	Create, update, or delete integrations	Yes				
	View integrations	Yes	Yes			
Onboarding	Create, update, or delete onboarding plans	Yes				
	View onboarding plans	Yes	Yes			Yes. Your projects
Marketplace						
	See and open the Marketplace tab	Yes	Yes			
	Use the downloaded cloud templates on the Design tab	Yes		Yes. If associated with your projects.	Yes. If associated with your projects.	
Marketplace - Cloud Templates	Download a cloud template	Yes				
	View the cloud templates	Yes	Yes			
Marketplace - Images	Download images	Yes				
	View images	Yes	Yes			
Marketplace - Downloads	View the log of all downloaded items	Yes	Yes			
Extensibility						
	See and open the Extensibility tab	Yes	Yes			Yes
Events	View extensibility events	Yes	Yes			
Subscriptions	Create, update, or delete extensibility subscriptions	Yes				
	Deactivate subscriptions	Yes				

Table 3-2. vRealize Automation Cloud Assembly service roles and project roles (continued)

UI Context	Task	Cloud Assembly Administrator	Cloud Assembly Viewer	Cloud Assembly User User must be a project administrator or member to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
	View subscriptions	Yes	Yes			
Library - Event topics	View event topics	Yes	Yes			
Library - Actions	Create, update, or delete extensibility actions	Yes				
	View extensibility actions	Yes	Yes			
Library - Workflows	View extensibility workflows	Yes	Yes			
Activity - Action Runs	Cancel or delete extensibility action runs	Yes				
	View extensibility action runs	Yes	Yes			Yes. Your projects
Activity - Workflow Runs	View extensibility workflow runs	Yes	Yes			
Design						
Design	Open the Design tab and see a list of cloud templates	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Cloud Templates	Create, update, and delete cloud templates	Yes		Yes. Your projects	Yes. Your projects	
	View cloud templates	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
	Download cloud templates	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
	Upload cloud templates	Yes		Yes. Your projects	Yes. Your projects	
	Deploy cloud templates	Yes		Yes. Your projects	Yes. Your projects	
	Version and restore cloud templates	Yes		Yes. Your projects	Yes. Your projects	
	Release cloud templates to the catalog	Yes		Yes. Your projects	Yes. Your projects	

Table 3-2. vRealize Automation Cloud Assembly service roles and project roles (continued)

UI Context	Task	Cloud Assembly Administrator	Cloud Assembly Viewer	Cloud Assembly User User must be a project administrator or member to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
Custom Resources	Create, update or delete custom resources	Yes				
	View custom resources	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Custom Actions	Create, update, or delete custom actions	Yes				
	View custom actions	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
Deployments						
	See and open the Deployments tab	Yes	Yes	Yes	Yes	Yes
	View deployments, including deployment details, deployment history, and troubleshooting information.	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
	Run day 2 actions on deployments based on policies.	Yes		Yes. Your projects	Yes. Your projects	

Service Broker Service Roles

The vRealize Automation Service Broker service roles determine what you can see and do in vRealize Automation Service Broker. These service roles are defined in the console by an organization owner.

Table 3-3. Service Broker Service Role Descriptions

Role	Description
Service Broker Administrator	Must have read and write access to the entire user interface and API resources. This is the only user role that can perform all tasks, including creating a new project and assigning a project administrator.
Service Broker User	Any user who does not have the vRealize Automation Service Broker Administrator role. In a vRealize Automation Service Broker project, the administrator adds users to projects as project members, administrators, or viewers. The administrator can also add a project administrator.
Service Broker Viewer	A user who has read access to see information but cannot create, update, or delete values. Users with the viewer role can see all the information that is available to the administrator. They cannot take any action unless you make them a project administrator or a project member. If the user is affiliated with a project, they have the permissions related to the role. The project viewer would not extend their permissions the way that the administrator or member role does.

In addition to the service roles, vRealize Automation Service Broker has project roles. Any project is available in all of the services.

The project roles are defined in vRealize Automation Service Broker and can vary between projects.

In the following tables, which tells you what the different service and project roles can see and do, remember that the service administrators have full permission on all areas of the user interface.

Use the following descriptions of project roles will help you as you decide what permissions to give your users.

- Project administrators leverage the infrastructure that is created by the service administrator to ensure that their project members have the resources they need for their development work.
- Project members work within their projects to design and deploy cloud templates.
- Project viewers are restricted to read-only access.

Table 3-4. Service Broker Service Roles and Project Roles

UI Context	Task	Service Broker Administrator	Service Broker Viewer	Service Broker User User must be a project administrator to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
Access Service Broker						
Console	In the console, you can see and open Service Broker	Yes	Yes	Yes	Yes	Yes
Infrastructure						
	See and open the Infrastructure tab	Yes	Yes			
Configure - Projects	Create projects	Yes				
	Update, or delete values from project summary, provisioning, Kubernetes, and integrations	Yes				
	Add users and groups, and assign roles in projects.	Yes		Yes. Your projects.		
	View projects	Yes	Yes			
Configure - Cloud Zones	Create, update, or delete cloud zones	Yes				
	View cloud zones	Yes	Yes			
Configure - Kubernetes Zones	Create, update, or delete Kubernetes zones	Yes				
	View Kubernetes zones	Yes	Yes			
Connections - Cloud Accounts	Create, update, or delete cloud accounts	Yes				
	View cloud accounts	Yes	Yes			
Connections - Integrations	Create, update, or delete integrations	Yes				
	View integrations	Yes	Yes			
Activity - Requests	Delete deployment request records	Yes				

Table 3-4. Service Broker Service Roles and Project Roles (continued)

UI Context	Task	Service Broker Administrator	Service Broker Viewer	Service Broker User User must be a project administrator to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
	View deployment request records	Yes				
Activity - Event Logs	View event logs	Yes				
Content and Policies						
	See and open the Content and Policies tab	Yes	Yes			
Content Sources	Create, update, or delete content sources	Yes				
	View content sources	Yes	Yes			
Content Sharing	Add or remove shared content	Yes				
	View shared content	Yes	Yes			
Content	Customize form and configure item	Yes				
	View content	Yes	Yes			
Policies - Definitions	Create, update, or delete policy definitions	Yes				
	View policy definitions	Yes	Yes			
Policies - Enforcement	View enforcement log	Yes	Yes			
Notifications - Email Server	Configure an email server	Yes				
Catalog						
	See and open the Catalog tab	Yes	Yes	Yes	Yes	Yes
	View available catalog items	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
	Request a catalog item	Yes		Yes. Your projects	Yes. Your projects	
Deployments						

Table 3-4. Service Broker Service Roles and Project Roles (continued)

UI Context	Task	Service Broker Administrator	Service Broker Viewer	Service Broker User User must be a project administrator to see and do project-related tasks.		
				Project Administrator	Project Member	Project Viewer
	See and open the Deployments tab	Yes	Yes	Yes.	Yes	Yes
	View deployments, including deployment details, deployment history, and troubleshooting information.	Yes	Yes	Yes. Your projects	Yes. Your projects	Yes. Your projects
	Run day 2 actions on deployments based on policies	Yes		Yes. Your projects	Yes. Your projects	
Approvals						
	See and open the Approvals tab	Yes	Yes	Yes	Yes	Yes
	Respond to approval requests	Yes		Service Broker user role only	Service Broker user role only	Service Broker user role only

Code Stream Service Roles

The vRealize Automation Code Stream service roles determine what you can see and do in vRealize Automation Code Stream. These roles are defined in the console by the organization owner. Any project is available in all of the services.

Table 3-5. Code Stream Service Role Descriptions

Role	Description
Code Stream Administrator	A user who has read and write access to the entire user interface and API resources. This is the only user role that can see and do everything, including create projects, integrate endpoints, add triggers, create pipelines and custom dashboards, mark endpoints and variables as restricted resources, run pipelines that use restricted resources, and request that pipelines be published in vRealize Automation Service Broker.
Code Stream Developer	A user who can work with pipelines, but cannot work with restricted endpoints or variables. If a pipeline includes a restricted endpoint or variable, this user must obtain approval on the pipeline task that uses the restricted endpoint or variable.
Code Stream Executor	A user who can run pipelines and approve or reject user operation tasks. This user can resume, pause, and cancel pipeline executions, but cannot modify pipelines.

Table 3-5. Code Stream Service Role Descriptions (continued)

Role	Description
Code Stream User	A user who can access vRealize Automation Code Stream, but does not have any other privileges in vRealize Automation Code Stream.
Code Stream Viewer	A user who has read access to see pipelines, endpoints, pipeline executions, and dashboards, but cannot create, update, or delete them. A user who also has the Service viewer role can see all the information that is available to the administrator. They cannot take any action unless you make them a project administrator or a project member. If the user is affiliated with a project, they have the permissions related to the role. The project viewer would not extend their permissions the way that the administrator or member role does.

In addition to the service roles, vRealize Automation Code Stream has project roles. Any project is available in all the services.

The project roles are defined in vRealize Automation Code Stream and can vary between projects.

In the following tables, which tell you what the different service and project roles can see and do, remember that the service administrators have full permission on all areas of the user interface.

Use the following descriptions of project roles to help you decide what permissions to give your users.

- Project administrators leverage the infrastructure that is created by the service administrator to ensure that their project members have the resources they need for their development work. The project administrator can add members.
- Project members who have a service role can use services.
- Project viewers can see projects but cannot create, update, or delete them.

All actions except restricted means this role has permission to perform create, read, update, and delete actions on entities except for restricted variables and endpoints.

Table 3-6. vRealize Automation Code Stream service role capabilities

UI Context	Capabilities	Code Stream Administrator role	Code Stream Developer role	Code Stream Executor role	Code Stream Viewer role	Code Stream User role
Pipelines						
	View pipelines	Yes	Yes	Yes	Yes	
	Create pipelines	Yes	Yes			
	Run pipelines	Yes	Yes	Yes		
	Run pipelines that include restricted endpoints or variables	Yes				
	Update pipelines	Yes	Yes			

Table 3-6. vRealize Automation Code Stream service role capabilities (continued)

UI Context	Capabilities	Code Stream Administrator role	Code Stream Developer role	Code Stream Executor role	Code Stream Viewer role	Code Stream User role
Pipeline Executions	Delete pipelines	Yes	Yes			
	View pipeline executions	Yes	Yes	Yes	Yes	
	Resume, pause, and cancel pipeline executions	Yes	Yes	Yes		
	Resume pipelines that stop for approval on restricted resources	Yes				
Custom Integrations	Create custom integrations	Yes	Yes			
	Read custom integrations	Yes	Yes			
	Update custom integrations	Yes	Yes			
Endpoints	View executions	Yes	Yes	Yes	Yes	
	Create executions	Yes	Yes			
	Update executions	Yes	Yes			
	Delete executions	Yes	Yes			
Mark resources as restricted	Mark an endpoint or variable as restricted	Yes				
Dashboards	View dashboards	Yes	Yes	Yes	Yes	
	Create dashboards	Yes	Yes			
	Update dashboards	Yes	Yes			
	Delete dashboards	Yes	Yes			

Custom user roles in vRealize Automation

As a vRealize Automation Cloud Assembly administrator, you can create custom roles that define what users can see and do in vRealize Automation. You can then assign users to those roles.

Custom User Role Permissions

Using vRealize Automation Cloud Assembly, you can define more granular user roles and then assign users to those roles. The custom roles have two categories, view and manage.

- **View.** A user assigned to a role with this permission can see all the items for all projects in the selected sections of the user interface. This role is useful for users who need to see accounts, configurations, or assigned values.
- **Manage.** A user assigned to a role with this permission can see all the items and has full add, edit, and delete permissions for all projects in the selected sections of the user interface.

These permissions extend the privileges that are granted by the other roles and are not restricted by project membership. For example, you can expand a project administrator's permissions to manage parts of the infrastructure or give a service viewer an ability to review and respond to approvals requests.

To define the user roles and assign users, open vRealize Automation Cloud Assembly or vRealize Automation Service Broker as a service administrator and select **Infrastructure > Administration > Custom Roles**. You cannot configure the custom roles in vRealize Automation Code Stream, however the roles apply to all the services.

Table 3-7. Custom Roles

User Interface	Permission	Description
Infrastructure		
	View Cloud Accounts.	View cloud accounts.
	Manage Cloud Accounts	Create, update, or delete cloud accounts.
	View Image Mappings	View image mappings.
	Manage Image Mappings	Create, update, or delete image mappings.
	View Flavor Mappings	View flavor mappings.
	Manage Flavor Mappings	Create, update, or delete flavor mappings.
	View Cloud Zones	View cloud zones.
	Manage Cloud Zones	Create, update, or delete cloud zones.
	View Machines	View machines.
	View Requests	View activity requests.

Table 3-7. Custom Roles (continued)

User Interface	Permission	Description
	Manage Requests	Delete requests from the list.
	View Integrations	View integrations.
	Manage Integrations	Create, update, or delete integrations.
	View Projects	View projects.
	Manage Projects	Create projects. Add users and assign roles in projects. Update, or delete values from project summary, users, provisioning, Kubernetes, integrations, and test project configurations.
	View Onboarding Plans	View onboarding plans
	Manage Onboarding Plans	Create, update, run, or delete onboarding plans
Catalog		
	View Content	
	Manage Content	Add, update, delete content sources. Share content. Customize the content, including the catalog icons and request forms.
Policies		
	View Policies	View policy definitions.
	Manage Policies	Create, update, or delete policy definitions.
Deployments		
	View Deployments	View all deployments, including deployment details, deployment history, and troubleshooting information.
	Manage Deployments	View all deployments and run all day 2 actions that the day 2 policies allow an administrator to run on deployments and deployment components.
Cloud Templates		
	View Cloud Templates	View cloud templates.
	Manage Cloud Templates	Create, update, test, delete, version, share cloud templates, and release/unrelease a cloud template version.

Table 3-7. Custom Roles (continued)

User Interface	Permission	Description
	Edit Cloud Templates	Create, update, test, version, share cloud templates, and release/unrelease a cloud template version. The role does not have permission to delete cloud templates.
	Deploy Cloud Templates	Test and deploy any cloud template in any project.
	Deploy In-line Cloud Template Content	Deploy any cloud template in the projects that the assignees are associated with. The project roles can be administrator, member, or viewer.
XaaS		
	View Custom Resources	View custom resources.
	Manage Custom Resources	Create, update or delete custom resources
	View Resource Actions	View custom actions.
	Manage Resource Actions	Create, update, or delete custom actions
Extensibility		
	View Extensibility Resources	View events, subscriptions, event topics, actions, workflows, action runs, and workflow runs.
	Manage Extensibility Resources	Create, update, delete, and deactivate extensibility subscriptions. Create, update, or delete extensibility actions. Cancel or delete extensibility action runs.
Pipeline		
	Manage Pipelines	Create, edit, and delete pipeline, endpoint, variable, and trigger configurations. Restricted models are excluded.
	Manage Restricted Pipelines	Create, edit, and delete pipeline, endpoint, variable, and trigger configurations. Restricted models are included.
	Manage Custom Integrations	Add, edit, and delete custom integrations.
	Execute Pipelines	Run pipeline model executions and triggers, and pause, cancel, resume, or re-run the executions and triggers.

Table 3-7. Custom Roles (continued)

User Interface	Permission	Description
	Execute Restricted Pipelines	Run pipeline model executions and triggers, and pause, cancel, resume, or re-run the executions and triggers. Resolve restricted endpoints and variables.
	Manage Executions	Run pipeline model executions and triggers, and pause, cancel, resume, or re-run the executions and triggers. Resolve restricted endpoints and variables. Delete executions.
Approval		
	Manage Approvals	View the Approvals tab where you can approve or reject approval requests. Approver with this role will not receive an email notification about an approval request unless they are an approver in the policy.

Use cases: How can user roles help me control access in vRealize Automation

As a cloud administrator, you want to control the tasks that your users can perform in vRealize Automation. Depending on your management goals and application development team responsibilities, there are different ways that you can configure the user roles to support those goals.

The following vRealize Automation Cloud Assembly and vRealize Automation Service Broker examples are based on three use cases. These examples provide only enough instruction to illustrate the application of users roles.

The target audience for these use cases is the cloud administrator, who is also considered the cloud administrator, and the service administrators.

The use cases build on each other. If you are ready to go directly to use case 3, you might need to review use cases 1 and 2 to better understand why you configure the roles in the ways specified.

The purpose of the use cases is to demonstrate user roles, not to provide detailed information about configuring your infrastructure, managing projects, creating cloud templates, and working with deployments.

Before you begin, you must understand the levels of user roles that are configured by a cloud administrator in the vRealize Automation Console.

■ Organization Roles

The organization roles control who can access the console.

As an organization owner, you must ensure that all users of any of the services are assigned at least an organization member role.

Role	Description
Organization Owner	An administrator can add users, change the role of users, and remove users from the organization. The owner manages which services users have access to.
Organization Member	A general user can log in to the organization console. To access the services, an organization owner must assign the users service roles.

■ Service Roles

The service roles control who can access their assigned services.

As an organization owner, you must ensure that the users who need access to the services are assigned the appropriate role. You use the roles to control how much the user can do in each service.

Table 3-8. vRealize Automation Cloud Assembly Service Role Descriptions

Role	Description
Cloud Assembly Administrator	A user who has read and write access to the entire user interface and API resources. This is the only user role that can see and do everything, including add cloud accounts, create new projects, and assign a project administrator.
Cloud Assembly User	A user who does not have the Cloud Assembly Administrator role. In a vRealize Automation Cloud Assembly project, the administrator adds users to projects as project members, administrators, or viewers. The administrator can also add a project administrator.
Cloud Assembly Viewer	A user who has read access to see information but cannot create, update, or delete values. This is a read-only role across all projects. Users with the viewer role can see all the information that is available to the administrator. They cannot take any action unless you make them a project administrator or a project member. If the user is affiliated with a project, they have the permissions related to the role. The project viewer would not extend their permissions the way that the administrator or member role does.

Table 3-9. Service Broker Service Role Descriptions

Role	Description
Service Broker Administrator	Must have read and write access to the entire user interface and API resources. This is the only user role that can perform all tasks, including creating a new project and assigning a project administrator.
Service Broker User	Any user who does not have the vRealize Automation Service Broker Administrator role. In a vRealize Automation Service Broker project, the administrator adds users to projects as project members, administrators, or viewers. The administrator can also add a project administrator.
Service Broker Viewer	A user who has read access to see information but cannot create, update, or delete values.

Table 3-9. Service Broker Service Role Descriptions (continued)

Role	Description
	Users with the viewer role can see all the information that is available to the administrator. They cannot take any action unless you make them a project administrator or a project member. If the user is affiliated with a project, they have the permissions related to the role. The project viewer would not extend their permissions the way that the administrator or member role does.

Table 3-10. Code Stream Service Role Descriptions

Role	Description
Code Stream Administrator	A user who has read and write access to the entire user interface and API resources. This is the only user role that can see and do everything, including create projects, integrate endpoints, add triggers, create pipelines and custom dashboards, mark endpoints and variables as restricted resources, run pipelines that use restricted resources, and request that pipelines be published in vRealize Automation Service Broker.
Code Stream Developer	A user who can work with pipelines, but cannot work with restricted endpoints or variables. If a pipeline includes a restricted endpoint or variable, this user must obtain approval on the pipeline task that uses the restricted endpoint or variable.
Code Stream Executor	A user who can run pipelines and approve or reject user operation tasks. This user can resume, pause, and cancel pipeline executions, but cannot modify pipelines.
Code Stream User	A user who can access vRealize Automation Code Stream, but does not have any other privileges in vRealize Automation Code Stream.
Code Stream Viewer	A user who has read access to see pipelines, endpoints, pipeline executions, and dashboards, but cannot create, update, or delete them. A user who also has the Service viewer role can see all the information that is available to the administrator. They cannot take any action unless you make them a project administrator or a project member. If the user is affiliated with a project, they have the permissions related to the role. The project viewer would not extend their permissions the way that the administrator or member role does.

- Project membership roles

The project membership determines what infrastructure resources and cloud templates are available.

Project membership is defined in the service by a user with a service administrator role. The service administrator must ensure that the users who need access to one or more projects are assigned the appropriate project role in each project.

Table 3-11. Project Roles

Role	Description
Project Administrator	A project administrator can manage their own projects, create and deploy cloud templates associated with their projects, and manage project deployments for all project members.
Project Member	A project member can create and deploy cloud templates associated with their projects, manage their own deployments, and manage any shared deployments.
Project Viewer	A project viewer is a member of the project with read-only access to their project resources, cloud templates, and deployments.

- Custom roles

The custom roles are created by the vRealize Automation Cloud Assembly to refine the member and viewer roles.

The procedures provided in these use cases are meant to highlight the user roles. They are not detailed or definitive procedures for setting up vRealize Automation.

As you configure roles, remember that users who are running API operations are subject to the roles that you assign here.

Prerequisites

- Verify that you have the Organization Owner role. You must see the **Identity and Access Management** tab with you log in to the console. If not, contact the organization owner.

-

- Verify that your users are added to vRealize Automation.

When you install vRealize Automation, your Active Directory users are added as part of the process.

- For a more detailed task and role list for various roles, see [Organization and service user roles in vRealize Automation](#).

Procedure

1 User role use case 1: Set up the vRealize Automation user roles to support a small application development team

As a vRealize Automation cloud administrator, you are responsible for managing the access and the budget for your infrastructure resources. You add yourself and two others as administrators. This small team can create the infrastructure and develop the cloud templates that match the business goals of the teams that consume the cloud templates. You and your small team of administrators then deploy the cloud templates for your non-administrator consumers. You don't allow non-administrators to access vRealize Automation.

2 User role use case 2: Set up vRealize Automation user roles to support larger development teams and the catalog

As a vRealize Automation organization owner, you are responsible for managing the access and the budget for your infrastructure resources. You have a team of cloud template developers who iteratively create and deploy templates for different projects until they are ready to deliver to their consumers. You then deliver the deployable resources to the consumers in a catalog.

3 User role use case 3: Set up vRealize Automation custom user roles to refine system roles

As a vRealize Automation organization owner or service administrator, you manage user access using the organization and service system roles. However, you also want to create custom roles to that selected users and perform tasks or see content that is outside of their system roles.

User role use case 1: Set up the vRealize Automation user roles to support a small application development team

As a vRealize Automation cloud administrator, you are responsible for managing the access and the budget for your infrastructure resources. You add yourself and two others as administrators. This small team can create the infrastructure and develop the cloud templates that match the business goals of the teams that consume the cloud templates. You and your small team of administrators then deploy the cloud templates for your non-administrator consumers. You don't allow non-administrators to access vRealize Automation.

In this use case, you are the organization owner and you have a small team where they all have the service administrator role.

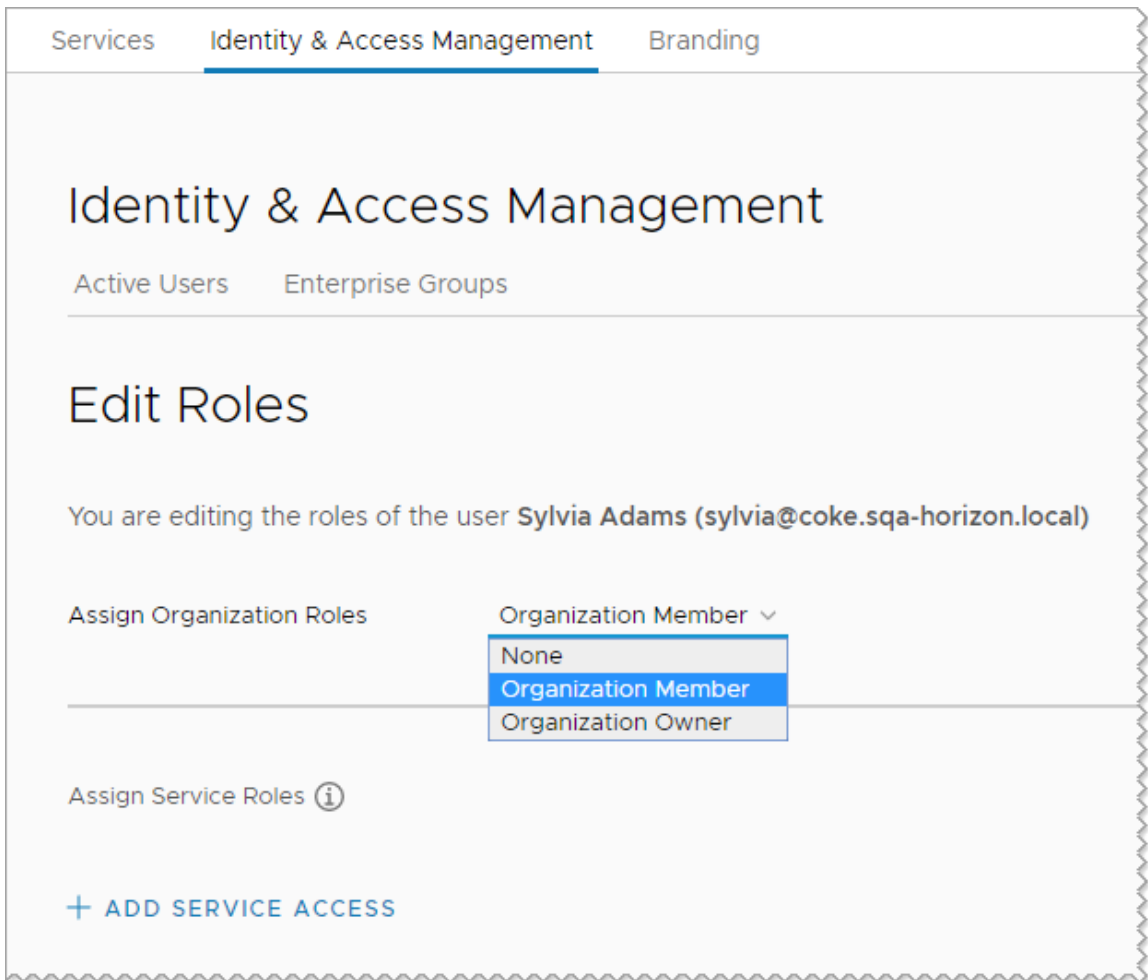
The following procedure follows one user all the way through the process. You can do each step for multiple users.

Prerequisites

- Verify that you meet all the prerequisites stipulated in the use case introduction. See [Use cases: How can user roles help me control access in vRealize Automation](#).

Procedure

- 1 Assign organization roles. Click **Identity and Access Management**.
 - a Log in to the vRealize Automation console.
 - b Click **Identity and Access Management**.
 - c Select the user name and click **Edit Roles**.
 - d In the **Assign Organization Roles** drop-down menu, select **Organization Member**.



The organization member role ensures that the user can access the console and any services that you add them to. They cannot manage organization users.

Leave the Edit Role page open for this user and continue to the next step.

- 2 Assign Cloud Assembly Administrator role to yourself and to the one or two other administrators in this scenario.

The service administrator role has full privileges to add, edit, and delete infrastructure, projects, cloud templates, and deployments. Defining an administrator role for one person and the user role for a different person is covered in Scenario 2. This example uses Sylvia.

- a Click **Add Service Access**.
- b Configure the user with the following value.

Service	Role
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 Create a project in Cloud Assembly that you use to group resources and manage resource billing for different business groups.

- a In the console, click the **Services** tab, and then click **Cloud Assembly**.
- b Select **Infrastructure > Projects > New Project**.

This user role use case is focused on providing examples of how you can implement user roles, not on creating the fully defined system.

For information about configuring the infrastructure, see [Building your resource infrastructure](#). For more about projects, see [Adding and managing projects](#).

- c Enter **WebAppTeam** as the project name.
- d Click **Users**, and then click **Add Users**.

- e Enter email addresses for the individuals who can help you build and manage the infrastructure and cloud templates.

For example, tony@mycompany.com,syliva@mycompany.com.

- f In the **Assign role** drop-down menu, select **Administrator**.

As vRealize Automation Cloud Assembly administrators, these two users already have administrator access to the cloud accounts, infrastructure, and all projects. This step helps you understand the roles used in the later scenarios. In the later scenarios, you define project administrator and project member roles, which have different permissions.

- g Click the **Provisioning** tab and add one or more cloud zones.

Another reminder. This use case is about user roles.

- 4 Develop a simple cloud template so that you can test the WebAppTeam project.

This cloud template section is abbreviated. The focus is users and user roles as defined by projects, not how to create a cloud template.

- a Select **Cloud Templates > New**.
- b For the new cloud template name, enter **WebApp**.
- c For **Project**, select WebAppTeam.

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 Select **Share only with the project**.

This setting ensures that the cloud template is only available to project members. When you are ready to provide the cloud templates to other teams, you can select Allow an administrator to share with any project in this organization. Sharing the cloud template with other projects means that you do not have to maintain duplicate instances of the same base templates. You can move cloud templates from development projects to production projects so that catalog consumers can deploy to production infrastructure resources.

- e Click **Create**.
- f In the cloud template designer, drag the **Cloud Agnostic > Machine** component to the canvas.

For more about configuring cloud templates, see [Designing your deployments](#).

- g Click **Deploy**.
 - h Continue iterating on the cloud template until you are ready to provide it to your consumers.
 - i Click **Version** and release and version the cloud template.
- 5 Send the users the log in information using your most common method.

Results

In this use case, you made your two colleagues organization members. You then made Sylvia a vRealize Automation Cloud Assembly administrator. You made Tony a WebApp project administrator. This user role configuration only works for small teams where you deliver deployed applications to your consumers rather than providing them with self-service access or a catalog.

User role use case 2: Set up vRealize Automation user roles to support larger development teams and the catalog

As a vRealize Automation organization owner, you are responsible for managing the access and the budget for your infrastructure resources. You have a team of cloud template developers who iteratively create and deploy templates for different projects until they are ready to deliver to their consumers. You then deliver the deployable resources to the consumers in a catalog.

This use case assumes that you understand that use case 1 is an administrator-only use case. You now want to expand your system to support more teams and larger goals.

- Let developers create and deploy their own application cloud templates during development. You add yourself as administrator, then add additional users with both the service user and the service viewer role. Next, you add the users as project members. The project members can develop and deploy their own cloud templates.
- Publish cloud templates to a catalog where you make them available for non-developers to deploy. Now you are assigning user roles for Service Broker. Service Broker provides a catalog for the cloud template consumers. You can also use it to create policies, including leases and entitlements, but that functionality is not part of this user role use case.

Prerequisites

- Review first use case. See [User role use case 1: Set up the vRealize Automation user roles to support a small application development team](#).
- Identify the following users based on what permissions you want them to have:
 - cloud template developers who will be vRealize Automation Cloud Assembly users and viewers
 - A vRealize Automation Service Broker administrator
 - Non-developer users who will be catalog consumers as vRealize Automation Service Broker users

Procedure

- 1 Assign organization member roles to your cloud template developer users.

If you need instructions, see the [User role use case 1: Set up the vRealize Automation user roles to support a small application development team](#).

- 2 Assign the vRealize Automation Cloud Assembly service member role to your cloud template developers.

- a Click **Add Service Access**.

- b Configure the user with the following value.

Service	Role
vRealize Automation Cloud Assembly	vRealize Automation Cloud Assembly User
vRealize Automation Cloud Assembly	vRealize Automation Cloud Assembly Viewer

In this use case, your developers need to see the infrastructure to ensure that they are building deployable cloud templates. As users that you will assign as project administrators and project members in the next step, they cannot see the infrastructure. As service viewers they can see how the infrastructure is configured, but cannot make any changes. As the cloud administrator, you remain in control, but give them access to the information they need to develop cloud templates.

- 3 Create projects in vRealize Automation Cloud Assembly that you use to group resources users.

In this use case, you create two projects. The first project is PersonnelAppDev and the second is PayrollAppDev.

- a In the console, click the **Services** tab, and then click **Cloud Assembly**.
 - b Select **Infrastructure > Projects > New Project**.

- c Enter **PersonnelAppDev** as the name.
- d Click **Users**, and then click **Add Users**.
- e Add project members and assign a project administrator.

Project Role	Description
Project User	A project member is the primary developer user role in a project. Projects determine what cloud resources are available when you are ready to test your development work by deploying a cloud template.
Project Administrator	A project administrator supports their developers by adding and removing users for your projects. You can also delete your projects. To create a project, you must have service administrator privileges.

- f For the users that you are adding as project members, enter the email address of each user, separated by a comma, and select **User** in the **Assign role** drop-down menu.

For example, 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 For the designated administrators, select **Administrator** in the **Assign role** drop-down menu and provide the necessary email address.

- h Click the **Provisioning** tab and add one or more cloud zones.

When the cloud template developers who are part of this project deploy a template, it is deployed to the resources available in the cloud zones. You must ensure that the cloud zone resources match the needs of the project development team templates.

- i Repeat the process to add the PayrollAppDev project with the necessary users and an administrator.

- 4 Provide the service user with the necessary login information and verify that the members of each project can do the following tasks.
 - a Open vRealize Automation Cloud Assembly.
 - b See the infrastructure across all projects.
 - c Create a cloud template for the project that they are a member of.
 - d Deploy the cloud template to the cloud zone resources defined in the project.
 - e Manage their deployments.
- 5 Assign organization member roles to your cloud template developer users.

If you need instructions, see the [User role use case 1: Set up the vRealize Automation user roles to support a small application development team](#).

- 6 Assign roles to a catalog administrator, catalog consumers, and cloud template developers based on their job.
 - a Click **Add Service Access**.
 - b Configure the catalog administrator with the following value.

This role might be you, the cloud administrator, or it might be someone else on your application development team.

Service	Role
vRealize Automation Service Broker	vRealize Automation Service Broker Administrator

- c Configure the cloud template consumers with the following value.

Service	Role
vRealize Automation Service Broker	vRealize Automation Service Broker User

The screenshot shows the 'Identity & Access Management' console. Under 'Active Users', 'Enterprise Groups' is selected. The 'Edit Roles' page for user 'Gloria Martinez (gloria@coke.sqa-horizon.local)' is displayed. It shows 'Assign Organization Roles' with 'Organization Member' selected. Below, 'Assign Service Roles' shows 'Service Broker' selected with the role 'Service Broker User' assigned. A '+ ADD SERVICE ACCESS' button is at the bottom.

- d Configure the cloud template developers with the following value.

Service	Role
Cloud AssemblyvRealize Automation Cloud Assembly	vRealize Automation Cloud Assembly User

- 7 Create projects in vRealize Automation Cloud Assembly that you use to group resources and users.

In this use case, you create two projects. The first project is PersonnelAppDev and the second is PayrollAppDev.

If you need instructions, see the [User role use case 2: Set up vRealize Automation user roles to support larger development teams and the catalog](#).

- 8 Create and release cloud templates for each project team.

If you need instructions, see the [User role use case 1: Set up the vRealize Automation user roles to support a small application development team](#).

- 9 Import a vRealize Automation Cloud Assembly cloud template into vRealize Automation Service Broker.

You must log in as a user with the vRealize Automation Service Broker Administrator role.

- Log in as a user with the vRealize Automation Service Broker Administrator role.
- In the console, click vRealize Automation Service Broker.

- c Select **Content and Policies > Content Sources**, and click **New**.

The screenshot shows the 'New Content Source' configuration page. On the left, a navigation pane lists 'Content Sources' as the active section. The main area contains the following fields and controls:

- Type ***: VMware Cloud Templates (with an information icon)
- Name ***: PersonnelAppImport
- Description**: An empty text area.
- Get cloud templates from**: A section containing a search bar and a dropdown menu.
- Source project ***: PersonnelAppDev
- VALIDATE**: A button to validate the configuration.
- Deploy cloud templates to**: A section with a text area and a note: 'Cloud templates will be deployed to cloud zones in projects they are shared with.'
- CREATE & IMPORT** and **CANCEL**: Buttons at the bottom.

- d Select **Cloud Assembly Cloud Template**.
- e Enter **PersonnelAppImport** as the name.
- f In the **Source project** drop-down menu, select PersonnelAppDev and click **Validate**.
- g When the source is validated, click **Create and Import**.
- h Repeat for PayrollAppDev using PayrollAppImport as the content source name.
- 10 Share an imported cloud template with a project.

Although the cloud template is already associated with a project, you share it in vRealize Automation Service Broker to make it available in the catalog.

- a Continue as a user with the vRealize Automation Service Broker administrator role.
- b In vRealize Automation Service Broker, select **Content and Policies > Content Sharing**.
- c Select the **PersonnelAppDev** project, which includes the users who must be able to deploy the cloud template from the catalog.

- d Click **Add Items** and then select the PersonnelApp cloud template to share with the project members.

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 Click **Save**.
- 11 Verify that the cloud template is available in the vRealize Automation Service Broker catalog to the project members.
- a Request that a project member log in and click the **Catalog** tab.

Catalog Items 1 item ▼



WebApp for Perso...
VMware Cloud Templates

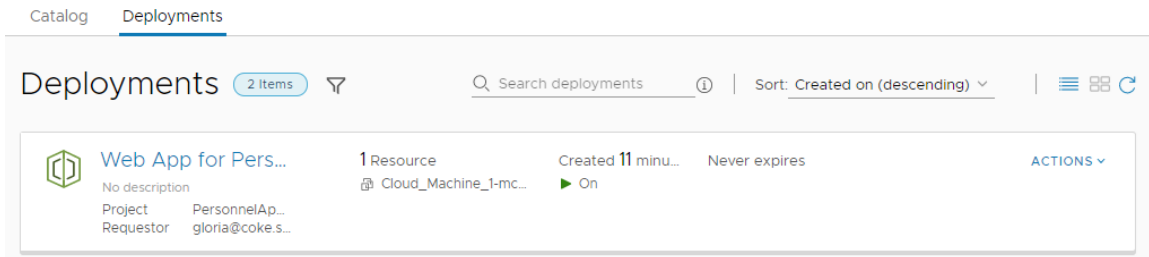
Projects: PersonnelAppDev

[REQUEST](#)

- b Click Request on the PersonnelApp cloud template card.
- c Complete the form and click **Submit**.

12 Verify that the project member can monitor the deployment process.

- a Request that the project member click the **Deployments** tab and locate their provisioning request.



- b When the cloud template is deployed, verify that the requesting user access the application.

13 Repeat the process for the additional projects.

Results

In this use case, recognizing that need to delegate the cloud template development to the developers, you add more organization members. You made them vRealize Automation Cloud Assembly users. You then made them members of relevant projects so that they can create and deploy cloud templates. As project members, they cannot see or alter the infrastructure that you continue to manage, but you gave them full service viewer permissions so that they could understand the constraints of infrastructure that they are designing for.

In this use case, you configure users with various roles, including the vRealize Automation Service Broker administrator and users. You then provide the non-developer users with the vRealize Automation Service Broker catalog.

What to do next

To learn how to define and assign custom roles to user, see [User role use case 3: Set up vRealize Automation custom user roles to refine system roles](#).

User role use case 3: Set up vRealize Automation custom user roles to refine system roles

As a vRealize Automation organization owner or service administrator, you manage user access using the organization and service system roles. However, you also want to create custom roles to that selected users and perform tasks or see content that is outside of their system roles.

This scenario assumes that you understand the service user and viewer, and the project member and viewer roles that are defined in use case 2. You can see that they are more restrictive than the service and project administrator roles used in use case 1. Now you have identified some local use cases where you want some users to have full management permissions to on some features, view permissions on others, and you do not want them to even view yet another set of features. You use custom roles define those permission.

This use case is based on three possible local use cases. This procedure shows you how to create permissions for the following custom roles.

- **Restricted Infrastructure Administrator.** You want some service users, who are not service administrators, to have broader infrastructure permissions. As the administrator, you want them to help set up cloud zones, images, and flavors. You also want them to be able on on-board and manage discovered resources. Notice they cannot add cloud accounts or integrations, they can only define the infrastructure for those endpoints.
- **Extensibility Developer.** You want some service users to have full permissions to use the extensibility actions and subscriptions as part of cloud template development for their project team and for other projects. They will also develop custom resource types and custom actions for multiple projects.
- **XaaS Developer.** You want some service users to have full permissions to develop custom resource types and custom actions for multiple projects.
- **Deployment Troubleshooter.** You want your project administrators to have permissions they need to troubleshoot and perform root cause analysis on failed deployments. You give them manage permissions on non-destructive or less expensive categories such as image and flavor mappings. You also want the project administrators to have permission to set approvals and day 2 policies as part of the failed deployment troubleshooting role.

Prerequisites

- Review the vRealize Automation Cloud Assembly and vRealize Automation Service Broker service roles and project roles tables in [What are the vRealize Automation user roles](#). You must understand what each service user role can see and do in those services.
- Review the [Custom user roles in vRealize Automation](#) descriptions so that you know more about how you can refine the permissions for your users.
- Review the first use case so that you understand organization roles and the service administrator roles. See [User role use case 1: Set up the vRealize Automation user roles to support a small application development team](#).
- Review the second use case so that you understand the service user and project member roles. See [User role use case 2: Set up vRealize Automation user roles to support larger development teams and the catalog](#).
- Familiarize yourself with vRealize Automation Service Broker. See [Adding content to the catalog](#).

Procedure

- 1 Assign organization member roles to your cloud template developer users.

If you need instructions, see the [User role use case 1: Set up the vRealize Automation user roles to support a small application development team](#).

- 2 Assign vRealize Automation Cloud Assembly and vRealize Automation Service Broker service roles for your cloud template developers and catalog consumers.

If you need instructions, see the [User role use case 2: Set up vRealize Automation user roles to support larger development teams and the catalog](#).

- 3 Create projects in vRealize Automation Cloud Assembly that you use to group resources and users.

The steps below for the custom roles also includes project roles.

If you need instructions for creating projects, see the [User role use case 2: Set up vRealize Automation user roles to support larger development teams and the catalog](#).

- 4 Create and release cloud templates for each project team.

If you need instructions, see the [User role use case 1: Set up the vRealize Automation user roles to support a small application development team](#).

- 5 Log in to vRealize Automation Cloud Assembly as a service administrator and select **Infrastructure > Administration > Custom Roles**.

- 6 Create a Restricted Infrastructure Administrator role.

In this example, you have a user, Tony, who is expert at setting up the infrastructure for various projects, but you don't want to give him full service permissions. Instead, Tony builds the core infrastructure the supports the work of all the projects. You give him limited infrastructure management permissions. Tony, or an outside contractor, might also have similar permissions for onboarding discovered machines and bringing them under vRealize Automation management.

- a Add Tony to vRealize Automation Cloud Assembly as a service user and viewer.

With his viewer permissions, he can see the underlying cloud accounts and integrations if he needs to troubleshoot his work, but he cannot make changes.

- b Create a project and add Tony as project member.

- c To create the custom role, select **Infrastructure > Administration > Custom Roles**, and click **New Custom Role**.

- d Enter the name **Restricted Infrastructure Administrator** and select the following permissions.

Select this permission ...	So that the users can ...
Infrastructure > Manage Cloud Zones	Create, update, and delete cloud zones.
Infrastructure > Manage Flavor Mappings	Create, update, and delete flavor mappings.
Infrastructure > Manage Image Mappings	Create, update, and delete image mappings.

- e Click **Create**.

- f On the Custom Roles page, select the Restricted Infrastructure Administrator role and click **Assign**.
- g Enter Tony's email account and click **Add**.

For example, enter Tony@yourcompany.com.

You can also enter any defined Active Directory user groups.

- h Have Tony verify that when he logs in, he can add, edit, and delete values in the areas defined by the custom role.

7 Create an Extensibility Developer role.

In this example, you have several cloud template developers, Sylvia and Igor, who are knowledgeable about how to use extensibility actions and subscriptions to manage daily development tasks. They are also experienced with vRealize Orchestrator, so you task them with providing custom resources and actions for various projects. You give them additional permissions manage extensibility by managing custom resources and actions, and by managing extensibility actions and subscriptions.

- a Add Sylvia and Igor as vRealize Automation Cloud Assembly users.
- b Add them as members of the projects that they are contributing their extensibility skills to.
- c Create a custom user role that you name **Extensibility Developer** and select the following permissions.

Select this permission ...	So that the users can ...
XaaS > Manage Custom Resources	Create, update, or delete custom resources.
XaaS > Manage Resource Actions	Create, update, or delete custom actions.
Extensibility > Manage Extensibility Resources	Create, update, or delete extensibility actions and subscriptions. Disable subscriptions. Cancel and delete action runs.

- d Click **Create**.
- e Assign Sylvia and Igor to the Extensibility Developer role.
- f Verify that Sylvia and Igor can manage the custom resources and actions, and that they can manage the various options on the Extensibility tab.

8 Create a Deployment Troubleshooter role.

In this example, you give your project administrators more manage permission so that they can remedy deployment failures for their teams.

- a Add your project administrators, Shauna, Pratap, and Wei, as vRealize Automation Cloud Assembly and vRealize Automation Service Broker service users.
- b In their projects, add them as project administrators.

- c Create a custom user role that you name **Deployment Troubleshooter** and select the following permissions.

Select this permission ...	So that the users can ...
Infrastructure > Manage Flavor Mappings	Create, update, and delete flavor mappings.
Infrastructure > Manage Image Mappings	Create, update, and delete image mappings.
Deployments > Manage Deployments	View all deployments, across projects, and run all day 2 actions on deployments and deployment components.
Policy > Manage Policies	Create, update, or delete policy definitions.

- d Click **Create**.
- e Assign Shauna, Pratap, and Wei to the Deployment Troubleshooter role.
- f Verify that they can manage flavor mappings, image mappings, and policies in vRealize Automation Service Broker.

Results

In this use case, you configure different users with various roles, including custom roles that expand their service and project roles.

What to do next

Create custom roles that address your local use cases.

Adding cloud accounts to vRealize Automation Cloud Assembly

Cloud accounts are the configured permissions that vRealize Automation Cloud Assembly uses to collect data from the regions or data centers, and to deploy cloud templates to those regions.

The collected data includes the regions that you later associate with cloud zones.

When you later configure cloud zones, mappings, and profiles, you select the cloud account to which they are associated.

As a cloud administrator, you create cloud accounts for the projects in which team members work. Resource information such as network and security, compute, storage, and tags content is data-collected from your cloud accounts.

Note If the cloud account has associated machines that have already been deployed in the region, you can bring those machines into vRealize Automation Cloud Assembly management by using an onboarding plan. See [What are onboarding plans in vRealize Automation Cloud Assembly](#).

If you remove a cloud account that is used in a deployment, resources that are part of that deployment become unmanaged.

Credentials required for working with cloud accounts in vRealize Automation

To configure and work with cloud accounts in vRealize Automation, verify that you have the following credentials.

Required cloud account credentials

To...	You need...
Sign up for and log in to vRealize Automation Cloud Assembly	<p>A VMware ID.</p> <ul style="list-style-type: none">■ Set up a My VMware account by using your corporate email address.
Connect to vRealize Automation services	<p>HTTPS port 443 open to outgoing traffic with access through the firewall to:</p> <ul style="list-style-type: none">■ *.vmwareidentity.com■ gaz.csp-vidm-prod.com■ *.vmware.com <p>For more information about ports and protocols, see VMware Ports and Protocols.</p> <p>For related information about required ports and protocols, see Port Requirements.</p>

To...	You need...
Add an Amazon Web Services (AWS) cloud account	<p>Provide a power user account with read and write privileges. The user account must be a member of the power access policy (PowerUserAccess) in the AWS Identity and Access Management (IAM) system.</p> <ul style="list-style-type: none"> ■ 20-digit Access Key ID and corresponding Secret Access Key <p>If you are using an external HTTP Internet proxy, it must be configured for IPv4.</p> <p>vRealize Automation actions-based extensibility (ABX) and external IPAM integration may require additional permissions.</p> <p>The following AWS permissions are suggested to allow autoscaling functions:</p> <ul style="list-style-type: none"> ■ Autoscaling actions: <ul style="list-style-type: none"> ■ autoscaling:DescribeAutoScalingInstances ■ autoscaling:AttachInstances ■ autoscaling>DeleteLaunchConfiguration ■ autoscaling:DescribeAutoScalingGroups ■ autoscaling>CreateAutoScalingGroup ■ autoscaling:UpdateAutoScalingGroup ■ autoscaling>DeleteAutoScalingGroup ■ autoscaling:DescribeLoadBalancers ■ Autoscaling resources: <ul style="list-style-type: none"> ■ * <p>Provide all autoscaling resource permissions.</p> <p>The following permissions are required to allow AWS Security Token Service (AWS STS) functions to support temporary, limited-privilege credentials for AWS identity and access:</p> <ul style="list-style-type: none"> ■ AWS STS resources: <ul style="list-style-type: none"> ■ * <p>Provide all STS resource permissions.</p> <p>The following AWS permissions are required to allow EC2 functions:</p> <ul style="list-style-type: none"> ■ EC2 actions: <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 ■ ec2:CreateSecurityGroup ■ ec2:DescribeVolumes

To...	You need...
	<ul style="list-style-type: none"> ■ ec2:CreateSnapshot ■ ec2:ModifyInstanceAttribute ■ ec2:DescribeRouteTables ■ ec2:DescribeInstanceType ■ ec2:DescribeInstanceTypeOfferings ■ ec2:DescribeInstanceStatus ■ 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>Note The SpotFleet request permission is not required for vRealize Automation actions-based extensibility (ABX) or external IPAM integrations.</p> <hr/> <ul style="list-style-type: none"> ■ EC2 resources: <ul style="list-style-type: none"> ■ * <p>Provide all EC2 resource permissions.</p> <p>The following AWS permissions are required to allow elastic load balancing functions:</p> ■ Load balancer actions: <ul style="list-style-type: none"> ■ elasticloadbalancing:DeleteLoadBalancer ■ elasticloadbalancing:DescribeLoadBalancers ■ elasticloadbalancing:RemoveTags ■ elasticloadbalancing:CreateLoadBalancer ■ elasticloadbalancing:DescribeTags ■ elasticloadbalancing:ConfigureHealthCheck ■ elasticloadbalancing:AddTags ■ elasticloadbalancing:CreateTargetGroup ■ elasticloadbalancing>DeleteLoadBalancerListeners ■ elasticloadbalancing:DeregisterInstancesFromLoadBalancer

To...	You need...
	<ul style="list-style-type: none">■ elasticloadbalancing:RegisterInstancesWithLoadBalancer■ elasticloadbalancing:CreateLoadBalancerListeners■ Load balancer resources:<ul style="list-style-type: none">■ * <p>Provide all load balancer resource permissions.</p> <p>The following AWS Identity and Access Management (IAM) permissions can be enabled, however they are not required:</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

To...	You need...
Add a Microsoft Azure cloud account	<p>Configure a Microsoft Azure instance and obtain a valid Microsoft Azure subscription from which you can use the subscription ID.</p> <p>Create an Active Directory application as described in How to: Use the portal to create an Azure AD application and service principal that can access resources in Microsoft Azure product documentation.</p> <p>If you are using an external HTTP Internet proxy, it must be configured for IPv4.</p> <p>Make note of the following information:</p> <ul style="list-style-type: none"> ■ Subscription ID <p>Allows you to access to your Microsoft Azure subscriptions.</p> ■ Tenant ID <p>The authorization endpoint for the Active Directory applications you create in your Microsoft Azure account.</p> ■ Client application ID <p>Provides access to Microsoft Active Directory in your Microsoft Azure individual account.</p> ■ Client application secret key <p>The unique secret key generated to pair with your client application ID.</p> <p>The following permissions are needed for creating and validating Microsoft Azure cloud accounts:</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 ■ Microsoft.Network/networkSecurityGroups/join/action ■ Microsoft.Network/networkSecurityGroups/read

To...	You need...
	<ul style="list-style-type: none"> ■ 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

If you are using Microsoft Azure with action-based extensibility, the following permissions are required, in addition to the minimal permissions:

- 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
- Microsoft.Web/sites/publishxml/action
- Microsoft.Web/serverfarms/write

To...	You need...
	<ul style="list-style-type: none">■ 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>If you are using Microsoft Azure with action-based extensibility with extensions, the following permissions are also needed:</p> <ul style="list-style-type: none">■ Microsoft.Compute/virtualMachines/extensions/write■ Microsoft.Compute/virtualMachines/extensions/read■ Microsoft.Compute/virtualMachines/extensions/delete

To...	You need...
Add a Google Cloud Platform (GCP) cloud account	<p>The Google Cloud Platform cloud account interacts with the Google Cloud Platform compute engine.</p> <p>The Project Admin and Owner credentials are required for creating and validating Google Cloud Platform cloud accounts.</p> <p>If you are using an external HTTP Internet proxy, it must be configured for IPv4.</p> <p>The compute engine service must be enabled. When creating the cloud account in vRealize Automation, use the service account that was created when the compute engine was initialized.</p> <p>The following compute engine permissions are also needed, depending on the actions that the user can take:</p> <ul style="list-style-type: none"> ■ roles/compute.admin <p>Provides full control of all compute engine resources.</p> ■ roles/iam.serviceAccountUser <p>Provides access to users who manage virtual machine instances that are configured to run as a service account. Grant access to the following resources and services:</p> <ul style="list-style-type: none"> ■ compute.* ■ resourcemanager.projects.get ■ resourcemanager.projects.list ■ serviceusage.quotas.get ■ serviceusage.services.get ■ serviceusage.services.list ■ roles/compute.imageUser <p>Provides permission to list and read images without having other permissions on the image. Granting the compute.imageUser role at the project level gives users the ability to list all images in the project. It also allows users to create resources, such as instances and persistent disks, based on images in the project.</p> <ul style="list-style-type: none"> ■ compute.images.get ■ compute.images.getFromFamily ■ compute.images.list ■ compute.images.useReadOnly ■ resourcemanager.projects.get ■ resourcemanager.projects.list ■ serviceusage.quotas.get ■ serviceusage.services.get ■ serviceusage.services.list ■ roles/compute.instanceAdmin <p>Provides permissions to create, modify, and delete virtual machine instances. This includes permissions to create, modify, and delete disks, and also to configure shielded VMBETA settings.</p> <p>For users that manage virtual machine instances (but not network or security settings or instances that run as service accounts), grant this role to the organization, folder, or project that contains the instances, or to the individual instances.</p> <p>Users that manage virtual machine instances that are configured to run as a service account also need the roles/iam.serviceAccountUser role.</p> <ul style="list-style-type: none"> ■ compute.acceleratorTypes ■ compute.addresses.get ■ compute.addresses.list ■ compute.addresses.use

To...	You need...
	<ul style="list-style-type: none"> ■ 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.useExternalIp ■ 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 ■ compute.subnetworks.useExternalIp ■ compute.targetPools.get ■ compute.targetPools.list

To...	You need...
	<ul style="list-style-type: none"> ■ <code>compute.zoneOperations.get</code> ■ <code>compute.zoneOperations.list</code> ■ <code>compute.zones</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.v1</code> <p>Provides full control of compute engine instances, instance groups, disks, snapshots, and images. Also provides read access to all compute engine networking resources.</p> <hr/> <p>Note If you grant a user this role at the instance level, that user cannot create new instances.</p> <hr/> <ul style="list-style-type: none"> ■ <code>compute.acceleratorTypes</code> ■ <code>compute.addresses.get</code> ■ <code>compute.addresses.list</code> ■ <code>compute.addresses.use</code> ■ <code>compute.autoscalers</code> ■ <code>compute.backendBuckets.get</code> ■ <code>compute.backendBuckets.list</code> ■ <code>compute.backendServices.get</code> ■ <code>compute.backendServices.list</code> ■ <code>compute.diskTypes</code> ■ <code>compute.disks</code> ■ <code>compute.firewalls.get</code> ■ <code>compute.firewalls.list</code> ■ <code>compute.forwardingRules.get</code> ■ <code>compute.forwardingRules.list</code> ■ <code>compute.globalAddresses.get</code> ■ <code>compute.globalAddresses.list</code> ■ <code>compute.globalAddresses.use</code> ■ <code>compute.globalForwardingRules.get</code> ■ <code>compute.globalForwardingRules.list</code> ■ <code>compute.globalOperations.get</code> ■ <code>compute.globalOperations.list</code> ■ <code>compute.healthChecks.get</code> ■ <code>compute.healthChecks.list</code> ■ <code>compute.httpHealthChecks.get</code> ■ <code>compute.httpHealthChecks.list</code> ■ <code>compute.httpsHealthChecks.get</code> ■ <code>compute.httpsHealthChecks.list</code> ■ <code>compute.images</code> ■ <code>compute.instanceGroupManagers</code> ■ <code>compute.instanceGroups</code> ■ <code>compute.instanceTemplates</code>

To...	You need...
	<ul style="list-style-type: none"> ■ 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.useExternalIp ■ 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.useExternalIp ■ compute.targetHttpProxies.get ■ compute.targetHttpProxies.list ■ compute.targetHttpsProxies.get ■ compute.targetHttpsProxies.list ■ compute.targetInstances.get ■ compute.targetInstances.list ■ compute.targetPools.get

To...	You need...
	<ul style="list-style-type: none"> ■ 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
Add an NSX-T cloud account	<p>Provide an account with the following read and write privileges:</p> <ul style="list-style-type: none"> ■ NSX-T Enterprise Administrator role and access credentials ■ NSX-T IP address or FQDN <p>Administrators <i>also</i> require access to the vCenter Server as described in the following <i>vSphere agent requirements for vCenter-based cloud accounts</i> section on this page.</p>
Add an NSX-V cloud account	<p>Provide an account with the following read and write privileges:</p> <ul style="list-style-type: none"> ■ NSX-V Enterprise Administrator role and access credentials ■ NSX-V IP address or FQDN <p>Administrators <i>also</i> require access to the vCenter Server as described in the following <i>vSphere agent requirements for vCenter-based cloud accounts</i> section on this page.</p>

To...	You need...
Add a vCenter cloud account	<p>Provide an account with the following read and write privileges:</p> <ul style="list-style-type: none"> ■ vCenter IP address or FQDN <p>Administrators <i>also</i> require access to the vCenter Server as described in the following <i>vSphere agent requirements for vCenter-based cloud accounts</i> section on this page.</p>
Add a VMware Cloud on AWS (VMC) cloud account	<p>Provide an account with the following read and write privileges:</p> <ul style="list-style-type: none"> ■ The cloudadmin@vmc.local account or any user account in the CloudAdmin group ■ NSX Enterprise Administrator role and access credentials ■ NSX Cloud Admin access to your organization's VMware Cloud on AWS SDDC environment ■ Administrator access to your organization's VMware Cloud on AWS SDDC environment ■ The VMware Cloud on AWS API token for your VMware Cloud on AWS environment in your organization's VMware Cloud on AWS service ■ vCenter IP address or FQDN <p>Administrators <i>also</i> require access to the vCenter that is used by your target VMware Cloud on AWS SDDC that has all the permissions listed in the following <i>vSphere agent requirements for vCenter-based cloud accounts</i> section on this page.</p> <p>For more information about the permissions needed to create and use VMware Cloud on AWS cloud accounts, see <i>Managing the VMware Cloud on AWS Data Center</i> in VMware Cloud on AWS product documentation.</p>

vSphere agent requirements for vCenter-based cloud accounts

The following table lists the permissions needed to manage VMware Cloud on AWS and vCenter cloud accounts. The permissions must be enabled for all clusters in the vCenter Server, not just clusters that host endpoints.

For all vCenter Server-based cloud accounts - including NSX-V, NSX-T, vCenter, and VMware Cloud on AWS - the administrator must have vSphere endpoint credentials, or the credentials under which the agent service runs in vCenter, that provide administrative access to the host vCenter Server.

For more information about vSphere agent requirements, see [VMware vSphere product documentation](#).

Table 3-12. Permissions Required for vSphere Agent to Manage vCenter Server Instance

Attribute Value	Permission
Datastore	<ul style="list-style-type: none"> ■ Allocate space ■ Browse datastore ■ Low level file operations
Datastore Cluster	Configure a datastore cluster
Folder	<ul style="list-style-type: none"> ■ Create folder ■ Delete folder
Global	<ul style="list-style-type: none"> ■ Manage custom attributes ■ Set custom attribute
Network	Assign network

Table 3-12. Permissions Required for vSphere Agent to Manage vCenter Server Instance (continued)

Attribute Value	Permission
Permissions	Modify permission
Resource	<ul style="list-style-type: none"> ■ Assign VM to Res Pool ■ Migrate powered off virtual machine ■ Migrate powered on virtual machine
Content Library	<p>To assign a permission on a content library, an administrator must grant the permission to the user as a global permission. For related information, see Hierarchical Inheritance of Permissions for Content Libraries in <i>vSphere Virtual Machine Administration</i> at VMware vSphere Documentation.</p> <ul style="list-style-type: none"> ■ Add library item ■ Create local library ■ Create subscribed library ■ Delete library item ■ Delete local library ■ Delete subscribed library ■ Download files ■ Evict library item ■ Evict subscribed library ■ Probe subscription information ■ Read storage ■ Sync library item ■ Sync subscribed library ■ Type introspection ■ Update configuration settings ■ Update files ■ Update library ■ Update library item ■ Update local library ■ Update subscribed library ■ View configuration settings
Tags	<ul style="list-style-type: none"> ■ Assign or unassign vSphere tag ■ Create a vSphere tag ■ Create a vSphere tag category ■ Delete vSphere tag ■ Delete vSphere tag category ■ Edit vSphere tag ■ Edit vSphere tag category ■ Modify UsedBy field for category ■ Modify UsedBy field for tag

Table 3-12. Permissions Required for vSphere Agent to Manage vCenter Server Instance (continued)

Attribute Value	Permission
vApp	<ul style="list-style-type: none"> ■ Import ■ vApp application configuration <p>The <code>vApp.Import</code> application configuration is required for OVF templates and to provision VMs from the content library.</p> <p>The <code>vApp.vApp</code> application configuration is required when using cloud-init for cloud configuration scripting. This setting allows for modification of a vApp's internal structure, such as its product information and properties.</p>
Virtual Machine - Inventory	<ul style="list-style-type: none"> ■ Create from existing ■ Create new ■ Move ■ Remove
Virtual Machine - Interaction	<ul style="list-style-type: none"> ■ Configure CD media ■ Console interaction ■ Device connection ■ Power off ■ Power on ■ Reset ■ Suspend ■ Tools install
Virtual Machine - Configuration	<ul style="list-style-type: none"> ■ Add existing disk ■ Add new disk ■ Remove disk ■ Advanced ■ Change CPU count ■ Change resource ■ Extend virtual disk ■ Disk change tracking ■ Memory ■ Modify device settings ■ Rename ■ Set annotation ■ Settings ■ Swapfile placement
Virtual Machine - Provisioning	<ul style="list-style-type: none"> ■ Customize ■ Clone template ■ Clone virtual machine ■ Deploy template ■ Read customization specs
Virtual Machine - State	<ul style="list-style-type: none"> ■ Create snapshot ■ Remove snapshot ■ Revert to snapshot

Configure Microsoft Azure for use with vRealize Automation Cloud Assembly

You must gather some information and perform some configuration in order to create a Microsoft Azure cloud account in vRealize Automation Cloud Assembly.

Procedure

- 1 Locate and record your Microsoft Azure subscription and tenant IDs.
 - Subscription ID - Click the Subscriptions icon on the left toolbar in your Azure portal to view the subscription ID.
 - Tenant ID - Click the Help icon and select Show Diagnostics in your Azure portal. Search for tenant and record the ID when you have located it.
- 2 You can create a new storage account and a resource group to get started. Alternatively, you can create these in blueprints later.
 - Storage Account - Use the following procedure to configure an account.
 - 1 In your Azure portal, locate the Storage Accounts icon on the sidebar. Make sure the correct subscription is selected and click **Add**. You can also, search for storage account in the Azure search field.
 - 2 Enter the required information for the storage account. You will need your subscription ID.
 - 3 Select whether to use an existing resource group or create a new one. Make note of your resource group name, as you will need it later.

Note Save the location of your storage account as you will need it later.

- 3 Create a virtual network. Alternatively, if you have a suitable existing network, you can select that one.

If you are creating a network, you must select Use an Existing Resource Group and specify the group that you created in the preceding step. Also, select the same location that you specified previously. Microsoft Azure will not deploy virtual machines or other objects if the location doesn't match between all applicable components that the object will consume.

- a Locate the Virtual Network icon on the left panel and click it or search for virtual network. Make sure to select the correct subscription and click **Add**.
- b Enter a unique name for your new virtual network and record it for later.
- c Enter the appropriate IP address for your virtual network in the **Address space** field.
- d Ensure that the correct subscription is selected and click **Add**.
- e Enter the remaining basic configuration information.
- f You can modify the other options as necessary, but for most configurations, you can leave the defaults.
- g Click **Create**.

- 4 Set up an Azure Active Directory application so that vRA can authenticate.
 - a Locate the Active Directory icon on the Azure left menu and click it.
 - b Click **App Registrations** and select **Add**.
 - c Type a name for your application that complies with Azure name validation.
 - d Leave Web app/API as the Application Type.
 - e The Sign-on URL can be anything that is appropriate for your usage.
 - f Click **Create**.
- 5 Create a secret key to authenticate the application in Cloud Assembly.
 - a Click the name of your application in Azure.
Make note of your Application ID for later use.
 - b Click **All Settings** in the next pane and select Keys from the settings list.
 - c Enter a description for the new key and choose a duration.
 - d Click **Save** and make sure to copy the key value to a safe location as you will be unable to retrieve it later.
 - e On the left menu, select **API Permissions** for the application and click **Add a Permission** to create a new permission.
 - f Select Azure Service Management on the Select an API page.
 - g Click **Delegated Permissions**.
 - h Under Select permissions select user_impersonation and then click **Add Permissions**.
- 6 Authorize your Active Directory application to connect to your Azure subscription so that you can deploy and manage virtual machines.
 - a In the left menu, click the Subscriptions icon, and select your new subscription.
You may need to click on the text of the name to get the panel to slide over.
 - b Select the Access control (IAM) option to see the permissions to your subscription.
 - c Click **Add** under the Add a Role Assignment heading.
 - d Choose Contributor from the Role drop down.
 - e Leave the default selection in the Assign Access to drop down.
 - f Type the name of your application in the Select box.
 - g Click **Save**.
 - h Add additional roles so that your new application has Owner, Contributor, and Reader roles.
 - i Click the **Save**.

What to do next

You must install the Microsoft Azure command line interface tools. These tools are freely available for both Windows and Mac operating systems. See the Microsoft documentation for more information about downloading and installing these tools.

When you have the command line interface installed, you must authenticate to your new subscription.

- 1 Open a terminal window and type your Microsoft Azure login. You will receive a URL and a shortcode that will allow you to authenticate.
- 2 In a browser, enter the code that you received from the application on your device.
- 3 Enter your Auth Code and click **Continue**.
- 4 Select your Azure account and login.

If you have multiple subscriptions, ensure that the correct one is selected using the `azure account set <subscription-name>` command.

- 5 Before you proceed, you must register the Microsoft.Compute provider to your new Azure subscription using the `azure provider register microsoft.compute` command.

If the command times out and generates an error the first time you run it, run it again.

When you have completed configuration, you can use the `azure vm image list` command to retrieve available virtual machine image names. You can choose the desired image and record the URN provided for it and later use it in blueprints.

Create a Microsoft Azure cloud account in vRealize Automation

As a cloud administrator, you can create a Microsoft Azure cloud account for account regions to which your team will deploy vRealize Automation cloud templates.

To view an example use case of how Microsoft Azure cloud account works in vRealize Automation see [Tutorial: Setting up and testing multi-cloud infrastructure and deployments in vRealize Automation Cloud Assembly](#).

Prerequisites

- Verify that you have the required administrator credentials and have enabled HTTPS access on port 443. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- Verify that you have the required user role. See [What are the vRealize Automation user roles](#).
- Configure a Microsoft Azure account for use with vRealize Automation. See [Configure Microsoft Azure for use with vRealize Automation Cloud Assembly](#).
- If you do not have external Internet access, configure an Internet server proxy. See [How do I configure an Internet proxy server for vRealize Automation](#).

Procedure

- 1 Select **Infrastructure > Connections > Cloud Accounts** and click **Add Cloud Account**.

- 2 Select the Microsoft Azure account type and enter credentials and other values.
- 3 Click **Validate**.
The account regions associated with the account are collected.
- 4 Select the regions to which you want to provision this resource.
- 5 For efficiency, click **Create a Cloud zone for the selected regions**.
- 6 If you need to add tags to support a tagging strategy, enter capability tags. See [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments](#) and [Creating a tagging strategy](#).



For more information about how capability tags and constraint tags help control deployment placements, see the [Constraint Tags and Placement](#) video tutorial.

- 7 Click **Save**.

Results

The account is added to vRealize Automation, and the selected regions are available for the specified cloud zone.

What to do next

Create infrastructure resources for this cloud account.

Create an Amazon Web Services cloud account in vRealize Automation

As a cloud administrator, you can create an Amazon Web Services (AWS) cloud account for account regions to which your team will deploy vRealize Automation cloud templates.

For authorized users, AWS cloud accounts support access to the AWS GovCloud configuration. This configuration supports most of the standard vRealize Automation cloud account functionality with regard to project configuration, tags, and infrastructure. In Cloud Assembly cloud templates, it does support use of AWS Platform as a Service (PaaS) properties.

The following procedure describes how to configure an AWS cloud account.

Prerequisites

- Verify that you have the required administrator credentials and have enabled HTTPS access on port 443. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- Verify that you have the required user role. See [What are the vRealize Automation user roles](#).
- Verify that you have required AWS administrator credentials.
- If you do not have external Internet access, configure an Internet server proxy. See [How do I configure an Internet proxy server for vRealize Automation](#).

Procedure

- 1 Select **Infrastructure > Connections > Cloud Accounts** and click **Add Cloud Account**.
- 2 Select the AWS account type, and enter credentials and other values.
- 3 Click **Validate**.
The account regions associated with the account are collected.
- 4 Select the regions to which you want to provision this resource.
- 5 For efficiency, click **Create a Cloud zone for the selected regions**.
- 6 If you need to add tags to support a tagging strategy, enter capability tags. See [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments](#) and [Creating a tagging strategy](#).



For more information about how capability tags and constraint tags help control deployment placements, see the [Constraint Tags and Placement](#) video tutorial.

- 7 Click **Add**.

Results

The account is added to vRealize Automation, and the selected regions are available for the specified cloud zone.

What to do next

Configure infrastructure resources for this cloud account.

Create a Google Cloud Platform cloud account in vRealize Automation

As a cloud administrator, you can create a Google Cloud Platform (GCP) cloud account for account regions to which your team will deploy vRealize Automation cloud templates.

Prerequisites

- Verify that you have the required administrator credentials and have enabled HTTPS access on port 443. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- Verify that you have the required user role. See [What are the vRealize Automation user roles](#).
- Verify that you have access to the Google Cloud Platform JSON security key.
- Verify that you have required security information for your Google Cloud Platform instance. You can obtain most of this information from your instance or from the Google documentation.
- If you do not have external Internet access, configure an Internet server proxy. See [How do I configure an Internet proxy server for vRealize Automation](#).

Procedure

- 1 Select **Infrastructure > Connections > Cloud Accounts** and click **Add Cloud Account**.
- 2 Select the Google Cloud Platform account type and enter the appropriate credentials and related information. Use the service account that was created when the source GCP account compute engine was initialized.

As noted in the **Prerequisites** section above, credential requirements are available at [Credentials required for working with cloud accounts in vRealize Automation](#). To successfully create the cloud account in vRealize Automation, the source GCP account must have the compute engine service enabled.

In vRealize Automation, the project ID is part of the Google Cloud Platform endpoint. You specify it when you create the cloud account. During data collection of project-specific private images, the vRealize Automation GCP adapter queries the Google Cloud Platform API.

- 3 Click **Validate**.

The account regions associated with the account are collected.

- 4 Select the regions to which you want to provision this resource.
- 5 For efficiency, click **Create a Cloud zone for the selected regions**.
- 6 If you need tags to support a tagging strategy, enter capability tags. See [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments](#) and [Creating a tagging strategy](#).



For more information about how capability tags and constraint tags help control deployment placements, see the [Constraint Tags and Placement](#) video tutorial.

- 7 Click **Add**.

Results

The account is added to vRealize Automation, and the selected regions are available for the specified cloud zone.

What to do next

Create infrastructure resources for this cloud account.

Create a vCenter cloud account in vRealize Automation

You can add a vCenter cloud account for the account regions to which you want to deploy vRealize Automation cloud templates.

For network and security purposes, you can associate a vCenter cloud account with an NSX-T or NSX-V cloud account.

An NSX-T cloud account can be associated to one or more vCenter cloud accounts. However, an NSX-V cloud account can only be associated to one vCenter cloud account.

Prerequisites

- Verify that you have the required administrator credentials and have enabled HTTPS access on port 443. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- Verify that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).
- Verify that you have properly configured your ports and protocols to support the cloud account. See the *Ports and Protocols for vRealize Automation* topic in *Installing vRealize Automation with vRealize Easy Installer* and the *Port Requirements* topic in *vRealize Automation Reference Architecture Guide* in the [vRealize Automation product documentation](#).

Procedure

- 1 Select **Infrastructure > Connections > Cloud Accounts** and click **Add Cloud Account**.
- 2 Select the vCenter account type and enter the vCenter Server host IP address.
- 3 Enter your vCenter Server administrator credentials and click **Validate**.

All data centers that are associated with the account are data-collected. The following elements are data-collected, as are all vSphere tags for the following elements:

- Machines
- Clusters and hosts
- Port groups
- Data stores

- 4 Select at least one of the available data centers on the specified vCenter Server to allow provisioning for this cloud account.
- 5 For efficiency, create a cloud zone for provisioning to the selected data centers.

You can also create cloud zones as a separate step according to your organization's cloud strategy.

For information about cloud zones, see [Learn more about vRealize Automation Cloud Assembly cloud zones](#).

- 6 Select an existing NSX cloud account.

You can select the NSX account now, or later when you edit the cloud account.

For information about NSX-V cloud accounts, see [Create an NSX-V cloud account in vRealize Automation](#).

For information about NSX-T cloud accounts, see [Create an NSX-T cloud account in vRealize Automation](#).

For information about making association changes after you have deployed a cloud template, see [What happens if I remove an NSX cloud account association in vRealize Automation](#).

- 7 If you want to add tags to support a tagging strategy, enter capability tags.

You can add tags now, or later when you edit the cloud account. For information about tagging, see [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments](#).



For more information about how capability tags and constraint tags help control deployment placements, see the [Constraint Tags and Placement](#) video tutorial.

- 8 Click **Save**.

Results

The cloud account is added and the selected data centers are available for the specified cloud zone. Collected data such as machines, networks, storage, and volumes is listed in the **Resources** section of the **Infrastructure** tab.

What to do next

Configure remaining infrastructure resources for this cloud account. See [Chapter 4 Building your vRealize Automation Cloud Assembly resource infrastructure](#).

Create an NSX-V cloud account in vRealize Automation

For network and security purposes, you can create and associate an NSX-V cloud account with a vCenter cloud account.

An NSX-V cloud account can only be associated to one vCenter cloud account.

The association between NSX-V and a vCenter cloud account must be configured outside of vRealize Automation, specifically in your NSX application. vRealize Automation doesn't create the association between NSX and vCenter. In vRealize Automation, you specify an association that already exists in NSX.

Prerequisites

- Verify that you have the required administrator credentials and have enabled HTTPS access on port 443. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- Verify that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).
- Verify that you have a vCenter cloud account to use with this NSX cloud account. See [Create a vCenter cloud account in vRealize Automation](#).
- Verify that you have properly configured your ports and protocols to support the cloud account. See the *Ports and Protocols for vRealize Automation* topic in *Installing vRealize Automation with vRealize Easy Installer* and the *Port Requirements* topic in *vRealize Automation Reference Architecture Guide* in the [vRealize Automation product documentation](#).

Procedure

- 1 Select **Infrastructure > Connections > Cloud Accounts** and click **Add Cloud Account**.

- 2 Select the NSX-V account type and enter the NSX-V host IP address.

- 3 Enter your NSX administrator credentials and click **Validate**.

The assets associated with the account are collected.

If the NSX host IP address is not available, validation fails.

- 4 If available, select the vCenter endpoint that represents the vCenter cloud account that you are associating with this NSX-V account.

Only vCenter cloud accounts that are not currently associated to an NSX-T or NSX-V cloud account are available for selection.

For information about making association changes after you have deployed a cloud template, see [What happens if I remove an NSX cloud account association in vRealize Automation](#).

- 5 If you want to add tags to support a tagging strategy, enter capability tags.

You can add or remove capability tags later. See [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments](#).



For information about how capability tags and constraint tags help control deployment placements, see the [Constraint Tags and Placement](#) video tutorial.

- 6 Click **Save**.

What to do next

You can create or edit a vCenter cloud account to associate with this NSX cloud account. See [Create a vCenter cloud account in vRealize Automation](#).

Create and configure one or more cloud zones for use with the data centers that are used by this cloud account. See [Learn more about vRealize Automation Cloud Assembly cloud zones](#).

Configure infrastructure resources for this cloud account. See [Chapter 4 Building your vRealize Automation Cloud Assembly resource infrastructure](#).

Create an NSX-T cloud account in vRealize Automation

For network and security purposes, you can create an NSX-T cloud account and associate it with one or more vCenter cloud accounts.

An NSX-T cloud account can be associated to one or more vCenter cloud accounts. However, an NSX-V cloud account can only be associated to one vCenter cloud account.

The association between NSX-T and one or more vCenter cloud accounts must be configured outside of vRealize Automation, specifically in your NSX application. vRealize Automation doesn't create the association between NSX and vCenter. In vRealize Automation, you specify one or more configuration associations that already exists in NSX.

You can define an NSX-T cloud account to support either the NSX-T Manager API method or the NSX-T Policy API method. Details about the two methods are available in topics such as *Overview of the NSX Manager* in the *NSX-T Data Center Administration Guide* in [NSX-T Data Center product documentation](#). Information is also provided below in the step sequence.

After you create the NSX-T cloud account, you cannot convert it from one API method to the other. Instead, you would need to delete the cloud account and recreate it using the other API mode.

To facilitate fault tolerance and high availability in deployments, each NSX-T data center endpoint represents a cluster of three NSX Managers.

- vRealize Automation can point to one of the NSX Managers. Using this option, one NSX Manager receives the API calls from vRealize Automation.
- vRealize Automation can point to the Virtual IP of the cluster. Using this option, one NSX Manager assumes control of the VIP. That NSX Manager receives the API calls from vRealize Automation. In case of failure, another node in the cluster assumes control of the VIP and receives the API calls from vRealize Automation.

For more information about VIP configuration for NSX, see *Configure a Virtual IP (VIP) Address for a Cluster* in the *NSX-T Data Center Installation Guide* at [VMware NSX-T Data Center Documentation](#).

- vRealize Automation can point to a load balancer VIP to load-balance the calls to the three NSX Managers. Using this option, all three NSX Managers receive API calls from vRealize Automation.

You can configure the VIP on a third-party load balancer or on an NSX-T load balancer.

For large scale environments, consider using this option to split the vRealize Automation API calls among the three NSX Managers.

Prerequisites

- Verify that you have the required administrator credentials and have enabled HTTPS access on port 443. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- Verify that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).
- Verify that you have a vCenter cloud account to use with this NSX cloud account. See [Create a vCenter cloud account in vRealize Automation](#).
- Verify that you have properly configured your ports and protocols to support the cloud account. See the *Ports and Protocols for vRealize Automation* topic in *Installing vRealize Automation with vRealize Easy Installer* and the *Port Requirements* topic in *vRealize Automation Reference Architecture Guide* in the [vRealize Automation product documentation](#).

Procedure

- 1 Select **Infrastructure > Connections > Cloud Accounts** and click **Add Cloud Account**.

- 2 Select the NSX-T account type and enter the host IP address for the NSX-T endpoint Manager instance or VIP (see above for information about the expected behavior that pertains to the NSX Manager and VIP options).

- 3 Enter your NSX user name and password administrator credentials and click **Validate**.

The assets associated with the account are collected.

If the NSX host IP address is not available, validation fails.

- 4 In **NSX-T API method**, select either the **Manager method** or the **Policy method**.

- **Manager API method**

Existing NSX-T endpoints or cloud accounts that are onboarded or migrated from an earlier version of vRealize Automation are treated as Manager API method NSX-T cloud accounts.

The Manager API method is supported for NSX-T 2.4, NSX-T 3.0, and NSX-T 3.1 forward.

If you are using NSX-T Manager API method now, it is advised that you continue using the Manager API method until vRealize Automation introduces a Manager API to Policy API migration path.

Some vRealize Automation options for NSX-T require NSX-T 3.0 or greater, including adding tags to virtual machine NIC components in the cloud template.

- **Policy API method (default)**

The Policy API method is available for NSX-T 3.0 and NSX-T 3.1 forward. This option enables vRealize Automation to use the additional capabilities available in the NSX-T Policy API.

If you have existing NSX-T cloud accounts that were created prior to the introduction of the Policy API method in vRealize Automation 8.2, they use the Manager API method. It is recommended that you wait until the Manager API to Policy API migration tool is made available in vRealize Automation. If you prefer not to wait, you should replace your existing NSX-T cloud accounts with new NSX-T cloud accounts that specify the Policy API method.

- 5 In **Associations**, add one or more vCenter cloud accounts to associate with this NSX-T cloud account. You can also remove existing vCenter cloud account associations.

Only vCenter cloud accounts that are not currently associated in vRealize Automation to an NSX-T or NSX-V cloud account are available for selection.

See [What can I do with NSX-T mapping to multiple vCenters in vRealize Automation](#).

For information about making association changes after you have deployed a cloud template, or deleting the cloud account after you have deployed a cloud template, see [What happens if I remove an NSX cloud account association in vRealize Automation](#).

- 6 If you want to add tags to support a tagging strategy, enter capability tags.

You can add or remove capability tags later. See [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments](#).



For more information about how capability tags and constraint tags help control deployment placements, see the [Constraint Tags and Placement](#) video tutorial.

7 Click **Save**.

What to do next

You can create or edit a vCenter cloud account to associate with this NSX cloud account. See [Create a vCenter cloud account in vRealize Automation](#).

Create and configure one or more cloud zones for use with the data centers that are used by this cloud account. See [Learn more about vRealize Automation Cloud Assembly cloud zones](#).

Configure infrastructure resources for this cloud account. See [Chapter 4 Building your vRealize Automation Cloud Assembly resource infrastructure](#).

Create a VMware Cloud on AWS cloud account in vRealize Automation

As a cloud administrator, you can create a VMware Cloud on AWS cloud account for account regions to which your team will deploy vRealize Automation cloud templates.

VMware Cloud on AWS requires some unique configuration procedures in vRealize Automation. To properly configure vRealize Automation for VMware Cloud on AWS, including setting an API token values for the cloud account and setting gateway firewall rules for its cloud proxy, see the [Tutorial: Configuring VMware Cloud on AWS for vRealize Automation](#) workflow.

Prerequisites

- Verify that you have the required VMware Cloud on AWS administrator credentials, including VMware Cloud on AWS CloudAdmin credentials for the target SDDC in vCenter and that you have enabled HTTPS access on port 443. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- Verify that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).
- If you do not have external Internet access, configure an Internet server proxy. See [How do I configure an Internet proxy server for vRealize Automation](#).
- Verify that you have configured needed access and firewall rules in the SDDC. See [Prepare your VMware Cloud on AWS SDDC to connect with VMware Cloud on AWS cloud accounts in vRealize Automation](#).

Procedure

- 1 Select **Infrastructure > Connections > Cloud Accounts**, click **Add Cloud Account** and select the VMware Cloud on AWS account type.

- 2 Add the **VMC API token** for your organization to access the available SDDCs.

You can create a new token or use an existing token for your organization on the linked **API Tokens** page. For details, see [Create a VMware Cloud on AWS cloud account in vRealize Automation within a sample workflow](#).

- 3 Select the SDDC to be available for deployments.

NSX-V SDDCs are not supported and do not appear in the list.

The vCenter and NSX-T Manager IP address/FQDN values are automatically populated based on the SDDC.

- 4 Enter your vCenter user name and password for the specified SDDC if other than the default value of cloudadmin@vmc.local.

- 5 Click **Validate** to confirm your access rights to the specified vCenter and check that the vCenter is running.

The data centers associated with the account are collected.

- 6 For efficiency, create a cloud zone for provisioning to the selected SDDC.

You can also create cloud zones as a separate step according to your organization's cloud strategy.

- 7 If you want to add tags to support a tagging strategy, enter capability tags.

You can add or remove capability tags later. See [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments](#).



For more information about how capability tags and constraint tags help control deployment placements, see the [Constraint Tags and Placement](#) video tutorial.

- 8 Click **Save**.

Results

The cloud account is added and the selected SDDC is available for the specified cloud zone.

What to do next

To properly configure vRealize Automation for VMware Cloud on AWS, see [Tutorial: Configuring VMware Cloud on AWS for vRealize Automation](#).

For related information about VMware Cloud on AWS outside of vRealize Automation, see [VMware Cloud on AWS documentation](#).

Create a VMware Cloud Foundation cloud account

You can configure a VMware Cloud Foundation (VCF) as a cloud account within vRealize Automation Cloud Assembly to use workload domains.

A VCF cloud account enables you to incorporate a VCF workload into Cloud Assembly to facilitate a comprehensive hybrid cloud management solution. Cloud Assembly offers several entry points from which you can activate the VCF cloud account configuration page. If you access this page using the **Add Cloud Account** button on the SDDC integration Workload Domain tab, the workload is pre-selected as is the basic information for the vCenter and NSX manager.

Prerequisites

You must have an instance of VMware SDDC Manager 4.1 or higher configured as a vRealize Automation Cloud Assembly integration for use with this cloud account. For more information, see [Configure a VMware SDDC Manager integration](#).

Procedure

- 1 Select **Infrastructure > Connections > Cloud Accounts** and click **Add Cloud Account**.
- 2 Select the VCF Cloud Account type, and enter a **Name** and **Description**.
- 3 Enter the FQDN and credentials for the SDDC manager instance that you are using with this cloud account.

You can skip this step if you have already configured the SDDC manager instance that you will use with this account.
- 4 Select one or more workload domains that you want to use with this VCF cloud account.
- 5 If you want to have Cloud Assembly use Cloud Foundation managed service credentials for vCenter and NSX, select **Automatically create service credentials**. Later, if you want to change these credentials, you must use the VCF mechanism for password management.

If you select this option, you can skip steps 7 and 8.
- 6 Enter the credentials required to access the vCenter associated with this cloud account.
- 7 Under the NSX Manager heading, enter NSX credentials if you want to manually enter credentials for the VCF cloud account, or click **Create and Validate Service Credentials** if you want Cloud Assembly to create and validate NSX credentials.
- 8 Enter the credentials required to access the NSX-T network associated with this cloud account.
- 9 If applicable, select the NSX mode.
- 10 Click **Validate** to confirm a connection to the SDDC manager.
- 11 If applicable, select the data centers that you want to provision to under the **Configuration** heading. Click the check box if you want to create a cloud zone for the selected data centers.
- 12 If you use tags to support a tagging strategy, enter capability tags. See [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments](#) and [Creating a tagging strategy](#).
- 13 Click **Save**.

Results

This cloud account brings the selected workload domain associated with the specified SDDC manager into vRealize Automation Cloud Assembly for use.

If you want to manage additional workload domains using vRealize Automation, you must repeat this process for each domain.

What to do next

After you configure the VCF cloud account, you can select the account on the main cloud account page and click **Setup Cloud** to initiate the VMware Cloud Foundation Quickstart wizard that will configure your cloud.

For more information about the Quick Start wizard, see [../Getting-Started-Cloud-Assembly/GUID-BDC673B9-D2AD-47BC-93C5-8C500074F931.html](https://docs.vmware.com/en/Getting-Started-Cloud-Assembly/GUID-BDC673B9-D2AD-47BC-93C5-8C500074F931.html).

Integrating vRealize Automation with other applications

Integrations enable you to add external systems to vRealize Automation.

Integrations include vRealize Orchestrator, configuration management and other external systems such as GitHub, Ansible, Puppet, and external IPAM providers such as Infoblox.

Note If you do not have external Internet access and your integration requires it, you can configure an Internet server proxy. See [How do I configure an Internet proxy server for vRealize Automation](#).

How do I use Git integration in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly supports integration with GitLab, GitHub, and BitBucket repositories so that you can manage VMware cloud templates and action scripts under source control. This functionality facilitates auditing and accountability of processes around deployment.

vRealize Automation Cloud Assembly offers three different flavors of Git integration: GitLab, GitHub, and BitBucket. Each of these options is a separate integration.

You must have an appropriate local Git repository configured with access for all designated users in order to set up Git integration with vRealize Automation Cloud Assembly. Also, you must save your cloud templates in a specific structure in order for them to be detected by Git. To create an integration with GitLab or GitHub, select **Infrastructure > Connections > Integrations** in vRealize Automation Cloud Assembly and then make the appropriate selection. You will need the url and token for the target repository.

When Git integration is configured with an existing repository, all cloud templates associated with selected projects become available to qualified users. You can use these templates with an existing deployment or as the basis of a new deployment. When you add a project, you must select some properties regarding where and how it is stored in Git.

You can save actions to a Git repository directly from vRealize Automation Cloud Assembly. You can version action scripts either directly to Git, or you can create versions in vRealize Automation Cloud Assembly. If you create a version of an action in vRealize Automation Cloud Assembly, then it is automatically saved to Git as a version. Cloud templates are a bit more complicated, because you cannot directly add them to a Git integration from vRealize Automation Cloud Assembly. You must save them directly to a Git instance, and then you can retrieve them from Git when working with the cloud template management page in vRealize Automation Cloud Assembly.

Before you Begin

You must create and save your cloud templates in a specific structure in order for them to be detected by GitLab or GitHub.

- Configure and store cloud templates to be integrated with GitLab correctly. Only valid templates are imported into GitLab.
 - Create one or more designated folders for the cloud templates.
 - All cloud templates must be stored within `blueprint.yaml` files.
 - Ensure that the top of your templates include the `name:` and `version:` properties.
- Extract an API key for the applicable repository. In your Git account, select your login in the upper right corner, and navigate to the Settings menu. Select **Access Tokens**, then name your token, set an expiration date. Then, select API and create the token. Copy the resulting value and save it.

The following guidelines must be observed for all cloud templates used with Git integration.

- Each cloud template must reside in a separate folder.
- All cloud templates must be named `blueprint.yaml`.
- All cloud template YAML files must use `name` and `version` fields.
- Only valid cloud templates are imported.
- If you update a draft cloud template imported from Git, and its content differs from that in the top version, the draft will not be updated in subsequent syncs and a new version is created. If you want to update a template and also allow further sync's from Git, then you must create a new version after final changes.
- [Configure GitLab cloud template integration in vRealize Automation Cloud Assembly](#)
 This procedure demonstrates configuring GitLab integration in vRealize Automation Cloud Assembly so that you can work with cloud templates in the repository and automatically download saved templates that are associated with designated projects. To use cloud templates with GitLab, you must create a connection to an appropriate GitLab instance, and then save the desired templates to that instance.
- [Configure GitHub integration in vRealize Automation Cloud Assembly](#)
 You can integrate the GitHub cloud-based repository hosting service in vRealize Automation Cloud Assembly

- [Configure Bitbucket integration in vRealize Automation Cloud Assembly](#)

vRealize Automation Cloud Assembly supports integration with Bitbucket for use as a Git-based repository for ABX action scripts and VMware cloud templates.

Configure GitLab cloud template integration in vRealize Automation Cloud Assembly

This procedure demonstrates configuring GitLab integration in vRealize Automation Cloud Assembly so that you can work with cloud templates in the repository and automatically download saved templates that are associated with designated projects. To use cloud templates with GitLab, you must create a connection to an appropriate GitLab instance, and then save the desired templates to that instance.

When GitLab integration is configured with an existing repository, all cloud templates associated with selected projects become available to qualified users. You can use these templates with an existing deployment or as the basis of a new deployment. When you add a project, you must select some properties regarding where and how it is stored in GitLab.

Note You cannot push new or updated cloud templates to the Git repository from vRealize Automation Cloud Assembly. Also, you cannot push new templates to the repository from vRealize Automation Cloud Assembly. To add cloud templates to a repository, developers must use the Git interface.

If you update a draft cloud template imported from Git, and its content differs from that in the top version, the draft will not be updated in subsequent syncs and a new version is created. If you want to update a cloud template and also allow further sync's from Git, then you must create a new version after final changes.

After you set up your cloud templates for use with GitLab and collect required information, you must set up integration with your GitLab instance. Then, you can import the designated cloud templates into GitLab. You can view a video demonstration of this procedure at <https://www.youtube.com/watch?v=h0vqo63Sdgg>.

Prerequisites

- Extract an API key for the applicable repository. In your GitLab account, select your login in the upper right corner, and navigate to the Settings menu. Select Access Tokens, then name your token, set an expiration date. Then, select API and create the token. Copy the resulting value and save it.

You must have an appropriate local Git repository configured with access for all designated users in order to set up Git integration with vRealize Automation Cloud Assembly. Also, you must create and save your cloud templates in a specific structure in order for them to be detected by GitLab.

- Configure and store cloud templates to be integrated with GitLab correctly. Only valid templates are imported into GitLab. See [How do I use Git integration in vRealize Automation Cloud Assembly](#).

Procedure

- 1 Set up integration with your GitLab environment in vRealize Automation Cloud Assembly.
 - a Select **Infrastructure > Integrations > Add New** and choose GitLab.
 - b Enter the **URL** for your GitLab instance. For a software as a service GitLab instance, in most cases, it will be gitlab.com.
 - c Enter the **Token**, also known as an API key, for the specified GitLab instance. See the prerequisites above for information about extracting the token from your GitLab instance.
 - d Add an appropriate Name and Description.
 - e Click **Validate** to verify the connection.
 - f Add capability tags if desired. See [Using capability tags in vRealize Automation Cloud Assembly](#) for more information.
 - g Click **Add**.
- 2 Configure the GitLab connection to accept cloud templates in an appropriate repository.
 - a Select **Infrastructure > Integrations** and choose the appropriate GitLab integration.
 - b Select **Projects**.
 - c Select **New Project** and create a name for the project.
 - d Enter the **Repository** path within GitLab. Typically, this is the user name of the main account appended to the repository name.
 - e Enter the appropriate GitLab **Branch** that you want to use.
 - f If applicable, enter a **Folder** name. If left blank, all folders are available.
 - g Enter an appropriate **Type**. If applicable, enter a folder name. If left blank, all folders are available.
 - h Click **Next** to finish adding the repository.

When you click **Next**, an automated synchronization task is initiated that imports cloud templates into the platform.

When the synchronization tasks are complete, a message indicates that the cloud templates have been imported.

Results

You can now retrieve cloud templates from GitLab.

Configure GitHub integration in vRealize Automation Cloud Assembly

You can integrate the GitHub cloud-based repository hosting service in vRealize Automation Cloud Assembly

You need a valid GitHub token to configure GitHub integration in vRealize Automation Cloud Assembly. See the GitHub documentation for information about creating and locating your token.

Prerequisites

- You must have access to GitHub.
- Configure and store cloud templates to be integrated with GitHub correctly. Only valid cloud templates are imported into GitHub. See [How do I use Git integration in vRealize Automation Cloud Assembly](#).

Procedure

- 1 Select **Infrastructure > Connections > Integrations** and click **Add Integration**.
- 2 Select GitHub.
- 3 Enter the required information on the GitHub configuration page.
- 4 Click **Validate** to check the integration.
- 5 If you need to add tags to support a tagging strategy, enter capability tags. See [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments](#) and [Creating a tagging strategy](#).
- 6 Click **Add**.
- 7 Configure the GitLab connection to accept cloud templates in an appropriate repository.
 - a Select **Infrastructure > Integrations** and choose the appropriate GitHub integration.
 - b Select **Projects**.
 - c Select **New Project** and create a name for the project.
 - d Enter the **Repository** path within GitHub. Typically, this is the user name of the main account appended to the repository name.
 - e Enter the appropriate GitHub **Branch** that you want to use.
 - f If applicable, enter a **Folder** name. If left blank, all folders are available.
 - g Enter an appropriate **Type**.
 - h Click **Next** to finish adding the repository.

An automated synchronization task is initiated that imports cloud templates into the platform.

When the synchronization tasks are complete, a message indicates that the cloud templates have been imported.

Results

GitHub is available for use in vRealize Automation Cloud Assembly blueprints.

What to do next

You can now retrieve cloud templates from GitHub.

Configure Bitbucket integration in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly supports integration with Bitbucket for use as a Git-based repository for ABX action scripts and VMware cloud templates.

In vRealize Automation Cloud Assembly, you can work with two types of repository items using Bitbucket integration: VMware cloud templates or ABX action scripts. You must synch projects that you want to work with before using a Bitbucket integration. ABX actions support write back to the Bitbucket repository, but you cannot write back cloud templates from the integration. If you want to create new versions of cloud template files, you must do so manually.

Prerequisites

- Set up an on premises Bitbucket Server deployment with one or more ABX or cloud template-based projects that you want to use with your deployments. Bitbucket Cloud is currently not supported.
- Create or designate vRealize Automation Cloud Assembly project to associate your Bitbucket integration.
- Cloud template files to be synched to a Bitbucket integration must be named `blueprint.yaml`.

Procedure

- 1 Select **Infrastructure > Connections > Integrations** and click **Add Integration**.
- 2 Select Bitbucket.
- 3 Enter the Summary information and Bitbucket credentials on the Bitbucket new integration Summary page.
- 4 To check the integration, click **Validate**.
- 5 If you use add tags to support a tagging strategy, enter capability tags. See [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments](#) and [Creating a tagging strategy](#).
- 6 Click **Add**.
- 7 Select the Projects tab on the main page for the Bitbucket integration to associate a project with this Bitbucket integration.
- 8 Select the Project to associate with this Bitbucket integration.
- 9 Click **Next** to add a Repository to Bitbucket project and indicate the type of repository you are adding and then specify the **Repository** name and **Branch**, as well as the **Folder**.
- 10 Click **Add**.

If you want to add one or more repositories to a project, click **Add Repository**.

Results

Bitbucket integration is configured with the specified repository configuration, and you can view and work with ABX actions and cloud templates contained in configured repositories. When you add a project to a Bitbucket integration, a synch operation runs to pull the latest versions of ABX action scripts and cloud template files from the designated repository. The History tab on the Bitbucket integration page shows records of all synch operations for the integration. By default, files are automatically synched every 15 minutes, but you can manually synch a file by selecting it and clicking **SYNCH** at any time.

What to do next

You can work with ABX actions on the vRealize Automation Cloud Assembly Extensibility page, and you can work with cloud templates on the Design page. If you save a changed version of an ABX action on the Extensibility area of vRealize Automation Cloud Assembly, the new version of the script is created and written back to the repository.

How to configure an external IPAM integration in vRealize Automation

You can create a provider-specific external IPAM integration point to manage the IP addresses used in your cloud template deployments. When using an external IPAM integration point, IP addresses are obtained from and managed by the designated IPAM provider rather than from vRealize Automation.

You can create a provider-specific IPAM integration point to manage IP addresses and DNS settings for cloud template deployments and VMs in vRealize Automation.

For information about how to configure the prerequisites, and an example of how to create a provider-specific external IPAM integration point within the context of a sample workflow, see [Add an external IPAM integration for Infoblox in vRealize Automation](#). Note that this workflow is for an Infoblox IPAM integration but can be used as reference for any external IPAM vendor.

For information about how to create the needed assets to enable external IPAM partners and vendors to integrate their IPAM solution with vRealize Automation, see [How do I use the IPAM SDK to create a provider-specific external IPAM integration package for vRealize Automation](#).

Prerequisites

- Verify that you have cloud administrator credentials. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- Verify that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).
- Verify that you have an account with the external IPAM provider, for example [Infoblox](#) or [Bluecat](#), and that you have the correct access credentials to your organization's account with the IPAM provider.

- Verify that you have access to a deployed integration package for the IPAM provider, such as Infoblox or BlueCat. The deployed package is initially obtained as a .zip download from your IPAM provider or from the vRealize Automation Marketplace and then deployed to vRealize Automation.
- Verify that you have access to a configured running environment for the IPAM provider.
- If you are using an actions-based extensibility (ABX) On-Prem Embedded running environment, verify that you have an HTTP proxy server in the vRealize Automation network that is able to pass outgoing traffic to external sites such as gcr.io and storage.googleapis.com. For details, see [Pulling Docker images behind proxy in vRealize Automation 8.x \(75180\)](#).
- Verify that you have the required user credentials to access and use the IPAM vendor product. See your integration vendor's product documentation for information about required user permissions.

Procedure

- 1 Select **Infrastructure > Connections > Integrations** and click **Add Integration**.
- 2 Click **IPAM**.
- 3 In the **Provider** drop-down, select a configured IPAM provider package from the list.
If the list is empty, click **Import Provider Package**, navigate to an existing provider package .zip file, and select it. If you do not have the .zip file, you can obtain it from your provider's web site or from the vRealize Automation **Marketplace** tab.
- 4 Enter your administrator user name and password credentials for your account with the external IPAM provider, along with all other (if any) mandatory fields, such as the host name of your provider.
- 5 In the **Running Environment** drop-down list, select an existing running environment, such as on-premises actions-based extensibility integration point.

The running environment supports communication between vRealize Automation and the IPAM provider.

The IPAM framework only supports an actions-based extensibility (ABX) On-Prem Embedded running environment.

Note If you use an Amazon Web Services or Microsoft Azure cloud account as the integration running environment, be sure that the IPAM provider appliance is accessible from the Internet and is not behind a NAT or firewall and that it has a publicly resolvable DNS name. If the IPAM provider is not accessible, the Amazon Web Services Lambda or Microsoft Azure Functions cannot connect to it and the integration will fail.

- 6 Click **Validate**.

- 7 When prompted to trust the self-signed certificate from the external IPAM provider, click **Accept**.

After you accept the self-signed certificate, the validation action can continue to completion.

- 8 Enter a name for this IPAM integration point and click **Add** to save the new IPAM integration point.

A data collection action is initiated. Networks and IP addresses are data-collected from the external IPAM provider.

How to upgrade to a newer external IPAM integration package in vRealize Automation

You can upgrade an existing external IPAM integration point to source a more recent version of the vendor-specific IPAM integration package.

An external IPAM provider or VMware may upgrade a source IPAM integration package for a particular vendor. For example, the external IPAM integration package for Infoblox has been upgraded several times. To preserve any existing vRealize Automation infrastructure settings that use a named IPAM integration point, you can edit an IPAM integration point to source the updated IPAM integration package, rather than create a new IPAM integration point.

Prerequisites

This procedure assumes that you have already created an external IPAM integration point and want to upgrade that integration point to use a more recent version of the vendor's IPAM integration package.

For information about how to create an external IPAM integration point, see [Add an external IPAM integration for Infoblox in vRealize Automation](#).

- Verify that you have cloud administrator credentials. See [Credentials required for working with cloud accounts in vRealize Automation](#).
- Verify that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).
- Verify that you have an account with the external IPAM provider and that you have the correct access credentials to your organization's account with that IPAM provider.
- Verify that you have access to a deployed integration package for your IPAM provider. The deployed package is initially obtained as a .zip download from your IPAM provider website or from the vRealize Automation Marketplace and then deployed to vRealize Automation.

For information about how to download and deploy the provider package .zip file and make it available as a **Provider** value on the IPAM Integration page, see [Download and deploy an external IPAM provider package for use in vRealize Automation](#).

- Verify that you have access to a configured running environment for the IPAM provider. The running environment is typically an actions-based extensibility (ABX) On-Prem Embedded integration point.

For information about running environment characteristics, see [Create a running environment for an IPAM integration point in vRealize Automation](#).

Procedure

- 1 Select **Infrastructure > Connections > Integrations IPAM** and open the existing IPAM integration point.
- 2 Click **Manage Providers**.
- 3 Navigate to and import the updated IPAM integration package.
- 4 Click **Validate** and click **Save**.

Configure MyVMware integration in vRealize Automation Cloud Assembly

You can integrate MyVMware with vRealize Automation Cloud Assembly to support VMware related actions and capabilities, such as accessing the VMware Marketplace for cloud templates.

You can create only one My VMware integration for each organization.

Prerequisites

You must have a user account with the appropriate permissions for MyVMware.

- For information about inviting a user to a MyVMware account, see [KB 2070555](#).
- For information about assigning user permissions in a My VMware account, see [KB 2006977](#).

Procedure

- 1 Select **Infrastructure > Connections > Integrations** and click **Add Integration**.
- 2 Select My VMware.
- 3 Enter the required information on the MyVMware configuration page.
- 4 If you require tags to support a tagging strategy, enter capability tags. See [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments](#) and [Creating a tagging strategy](#).
- 5 Click **Add**.

Results

My VMware is available for use with cloud templates.

What to do next

Add a My VMware component to the desired cloud templates.

Configure vRealize Orchestrator integration in Cloud Assembly

You can configure one or more vRealize Orchestrator integrations, so that you can use workflows as part of extensibility.

vRealize Automation includes a preconfigured vRealize Orchestrator instance that can be used for extensibility subscriptions. You can also access the client of the embedded vRealize Orchestrator from the vRealize Automation Cloud Services Console.

With the vRealize Orchestrator integration to vRealize Automation Cloud Assembly, you can add an external vRealize Orchestrator instance and use the included workflow library in extensibility subscriptions. For more information, see [Extensibility workflow subscriptions](#).

Prerequisites

- Verify that you have cloud administrator credentials. For more information, see [What are the vRealize Automation user roles](#).
- Upgrade or migrate to vRealize Orchestrator 8.1. See *Upgrading and Migrating VMware vRealize Orchestrator*.

Procedure

- 1 Select **Infrastructure > Connections > Integrations**.
- 2 Click **Add integration**.
- 3 Select vRealize Orchestrator.
- 4 In vRealize Automation Cloud Assembly, enter the URL of the vRealize Orchestrator instance.
- 5 To validate the integration, click **Validate**.
- 6 Enter a name for the vRealize Orchestrator integration.
- 7 (Optional) Enter a description for the vRealize Orchestrator integration.
- 8 (Optional) Add capability tags. For more information on capability tags, see [Using capability tags in vRealize Automation Cloud Assembly](#).

Note Capability tags can be used to manage multiple vRealize Orchestrator integrations. See [Managing multiple vRealize Orchestrator integrations with project constraints](#).

- 9 Click **Add**.

The vRealize Orchestrator integration is saved.

What to do next

To verify that the integration is configured and that the workflows are added, select **Extensibility > Library > Workflows**.

Managing multiple vRealize Orchestrator integrations with project constraints

You can use project constraints to manage what vRealize Orchestrator integrations are used in workflow subscriptions.

vRealize Automation Cloud Assembly supports the integration of multiple vRealize Orchestrator servers that can be used in workflow subscriptions. You can manage what vRealize Orchestrator integrations are used in cloud templates provisioned by your project with soft or hard project constraints. For more information on project constraints, see [Using vRealize Automation Cloud Assembly project tags and custom properties](#).

Prerequisites

- Verify that you have cloud administrator credentials. See [What are the vRealize Automation user roles](#).
- Configure two or more vRealize Orchestrator integrations in vRealize Automation Cloud Assembly. See [Configure vRealize Orchestrator integration in Cloud Assembly](#).
- Add capability tags to your vRealize Orchestrator integrations. See [Using capability tags in vRealize Automation Cloud Assembly](#).

Procedure

- 1 Navigate to **Infrastructure > Administration > Projects** and select your project.
- 2 Select the **Provisioning** tab.
- 3 Enter the capability tags of your vRealize Orchestrator integrations in the **Extensibility constraints** text box and set them as soft or hard project constraints.
- 4 Click **Save**.

Results

When you deploy a cloud template, vRealize Automation Cloud Assembly uses the project constraints to manage what vRealize Orchestrator integrations are used in workflow subscriptions.

What to do next

Alternatively, you can use capability tags to manage multiple vRealize Orchestrator integrations on a cloud account level. For more information, see [Managing multiple vRealize Orchestrator integrations with cloud account capability tags](#).

Managing multiple vRealize Orchestrator integrations with cloud account capability tags

You can use capability tags to manage what vRealize Orchestrator integrations are used in workflow subscriptions.

vRealize Automation Cloud Assembly supports the integration of multiple vRealize Orchestrator servers that can be used in workflow subscriptions. You can manage what vRealize Orchestrator integrations are used in workflow subscriptions by adding capability tags to your cloud account.

Prerequisites

- Verify that you have cloud administrator credentials. See [What are the vRealize Automation user roles](#).

- Configure two or more vRealize Orchestrator integrations in vRealize Automation Cloud Assembly. For more information, see [Configure vRealize Orchestrator integration in Cloud Assembly](#).
- Add capability tags to your vRealize Orchestrator integrations. See [Using capability tags in vRealize Automation Cloud Assembly](#).

Procedure

1 Navigate to **Infrastructure > Connections > Cloud Accounts**.

2 Select your cloud account.

3 Enter the capability tags of the vRealize Orchestrator integrations you want to use.

The capability tags are automatically converted into soft constraints. To use hard constraints in managing your integrations, you must use project constraints. For more information, see [Managing multiple vRealize Orchestrator integrations with project constraints](#).

4 Click **Save**.

Results

When you deploy a cloud template, vRealize Automation Cloud Assembly uses the tagging in the associated cloud account to manage what vRealize Orchestrator integrations are used in workflow subscriptions.

How do I work with Kubernetes in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly offers several options for managing and deploying Kubernetes resources.

There are two primary options to working with Kubernetes resources in vRealize Automation Cloud Assembly. You can integrate VMware Tanzu Kubernetes Grid Integrated Edition (TKGI), formerly PKS, or Red Hat OpenShift with vRealize Automation Cloud Assembly to configure, manage and deploy Kubernetes resources. With the second option, you can leverage a vCenter cloud account to access supervisor namespaces to work with vSphere Project Pacific Kubernetes-based functionality. You can also integrate external Kubernetes resources in vRealize Automation Cloud Assembly.

Working with VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) or Openshift Integrations

For TKGI, external clusters, or Openshift configurations, vRealize Automation Cloud Assembly provides a Kubeconfig that enables users to access applicable Kubernetes clusters.

After you create a TKGI or OpenShift integration, applicable Kubernetes clusters become available in vRealize Automation Cloud Assembly and you can add and create Kubernetes components to vRealize Automation Cloud Assembly to support management of cluster and container applications. These applications form the basis of self-service deployments that are available from the Service Broker catalog.

Working with vSphere Project Pacific Kubernetes Clusters

Project Pacific is a vSphere enhancement that uses Kubernetes as its control plane. It enables you to manage both virtual machines and containers from one interface. vRealize Automation Cloud Assembly enables users to leverage the Pacific Kubernetes capabilities that have been embedded within vSphere. You can access Pacific functionality by creating an integration with a vCenter deployment with a vSphere implementation that contains supervisor clusters. Pacific enables you to manage both conventional virtual machines and Kubernetes clusters from vCenter.

For Pacific-based supervisor namespaces, users must have access to an applicable vSphere SSO so that they can log in to a provided link to the supervisor namespace details. Then, they can download a customized Kubectl with vSphere authentication so they can use their supervisor namespace.

To use this functionality, you must have a vCenter with vSphere cloud account that has supervisor namespaces configured. After a users has logged in they can begin working with applicable namespaces.

- [Configure PKS Integration in vRealize Automation Cloud Assembly](#)

You can configure a PKS resource connection on premises and in the cloud to support Kubernetes integration and management capabilities in vRealize Automation Cloud Assembly.

- [Configure Red Hat OpenShift Integration in vRealize Automation Cloud Assembly](#)

You can configure a Red Hat OpenShift resource connection on premises and in the cloud to support enterprise-level Kubernetes integration and management capabilities in vRealize Automation Cloud Assembly.

- [Configure a Kubernetes Zone in vRealize Automation Cloud Assembly](#)

Kubernetes zones enable cloud administrators to define policy-based placement of Kubernetes clusters and namespaces and supervisor namespaces used in vRealize Automation Cloud Assembly deployments. An administrator can use this page to specify what clusters are available for provisioning of Kubernetes namespaces and what properties are acceptable for clusters.

- [Use Pacific supervisor clusters and namespaces with vRealize Automation Cloud Assembly](#)

Administrators can configure vRealize Automation Cloud Assembly to use supervisor namespaces from an existing Pacific-enabled vSphere integration so that users can deploy namespaces in cloud templates and request them in the Service Broker catalog.

- [Working with Kubernetes clusters and namespaces in vRealize Automation Cloud Assembly](#)

You can add, view, and manage the configuration of Kubernetes clusters and namespaces, both generic and Pacific-based, which are the basis of Kubernetes deployments in vRealize Automation Cloud Assembly.

- [Adding Kubernetes components to cloud templates in vRealize Automation Cloud Assembly](#)

When adding Kubernetes components to a vRealize Automation Cloud Assembly cloud template, you can choose to add clusters or enable users to create namespaces in various configurations. Typically, this choice depends on your access control requirements, how you have configured your Kubernetes components, and your deployment requirements.

- [Using vRealize Automation Cloud Assembly Extensibility with Kubernetes](#)

vRealize Automation Cloud Assembly provides a standard set of event topics that correspond to typical actions related to Kubernetes cluster deployment. Users can subscribe to these topics as desired, and they receive notification when the event related to the subscribed topic occurs. You can also configure vRO workflows to run based on event notifications.

Configure PKS Integration in vRealize Automation Cloud Assembly

You can configure a PKS resource connection on premises and in the cloud to support Kubernetes integration and management capabilities in vRealize Automation Cloud Assembly.

PKS integrations enable you to manage PKS instances on premises and in the cloud and Kubernetes clusters provisioned on PKS and external clusters. You must create a Kubernetes profile and associate it with a project to support policy-based placement of resources.

Prerequisites

- You must have an appropriately configured Pivotal Container Service (PKS) server set up with UAA authentication.
- Verify that you have cloud administrator credentials. For more information, see [What are the vRealize Automation user roles](#).

Procedure

- 1 Select **Infrastructure > Connections > Integrations** and click **Add Integration**.
- 2 Select VMware Enterprise PKS.
- 3 Enter the IP address or FQDN, and PKS address for the PKS cloud account you are creating.
 - The IP address is the FQDN or IP address of the PKS user authentication server.
 - The PKS address is the FQDN or IP address for the main PKS server.
- 4 Select whether this PKS server is local or located in the public cloud or on a private cloud.
- 5 Enter an appropriate **Username** and **Password** for the PKS server and other related information..

- 6 If you use tags to support a tagging strategy, enter capability tags. See [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments](#) and [Creating a tagging strategy](#).
- 7 Click **Add**.

Results

You can create Kubernetes zones and assign them to a project, or you can discover external Kubernetes clusters and assign those clusters to projects. In addition, you can add or create Kubernetes namespaces that facilitate management of clusters among large groups and organizations.

What to do next

Create or select the appropriate Kubernetes zones, then select one or more clusters or namespaces, and assign them to a project. After that, you can create and publish cloud templates to enable users to generate self-service deployments that use Kubernetes.

Configure Red Hat OpenShift Integration in vRealize Automation Cloud Assembly

You can configure a Red Hat OpenShift resource connection on premises and in the cloud to support enterprise-level Kubernetes integration and management capabilities in vRealize Automation Cloud Assembly.

vRealize Automation Cloud Assembly supports integration with OpenShift versions 3.x.

Prerequisites

- You must have an appropriately configured Red Hat OpenShift implementation.
- Verify that you have cloud administrator credentials. For more information, see [What are the vRealize Automation user roles](#).
- VMware supplies resources you can use to create an OpenShift cluster with a cloud template at the following location: <https://flings.vmware.com/enterprise-openshift-as-a-service-on-cloud-automation-services>. You can use clusters created with these resources as global clusters in the Kubernetes zones to create self-service namespaces.

Procedure

- 1 Select **Infrastructure > Connections > Integrations** and click **Add Integration**.
- 2 Select Red Hat OpenShift.
- 3 Enter the **Address** and **Location** for the OpenShift server.
- 4 Select the appropriate **Credential Type** and enter the appropriate credentials.
OpenShift integration supports either OAuth username/password, public key, or bearer token authentication.
- 5 Enter an appropriate **Name** and **Description** for the OpenShift integration.

- 6 If you use tags to support a tagging strategy, enter the appropriate capability tags. See [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments and Creating a tagging strategy](#).
- 7 Click **Add**.

Results

When an integration is created, new Kubernetes clusters appear in the relevant section of the Kubernetes page. You can create Kubernetes zones and assign them to a project. In addition, you can configure Kubernetes namespaces that facilitate management of clusters among large groups and organizations.

What to do next

Create or select the appropriate Kubernetes zones, then select one or more clusters or namespaces, and assign them to a project. After that, you can create and publish cloud templates to enable users to generate self-service deployments that use Kubernetes.

Configure a Kubernetes Zone in vRealize Automation Cloud Assembly

Kubernetes zones enable cloud administrators to define policy-based placement of Kubernetes clusters and namespaces and supervisor namespaces used in vRealize Automation Cloud Assembly deployments. An administrator can use this page to specify what clusters are available for provisioning of Kubernetes namespaces and what properties are acceptable for clusters.

Cloud administrators can associate Kubernetes zones with PKS cloud accounts configured for Cloud Assembly or with external Kubernetes clusters that are not associated with a project.

When you create a Kubernetes zone, you can assign multiple provider-specific resources to the zone, and these resources will dictate what properties can be set for the newly provisioned clusters in terms of the number of workers, masters, available CPU, memory, and other configuration settings. For PKS providers, these correspond to PKS plans. An administrator can also assign multiple clusters to a Kubernetes zone that will be used for placement of newly provisioned Kubernetes namespaces. The administrator can only assign clusters that are not onboarded, or not managed by CMX, and are provisioned via the preselected cluster provider. The administrator can assign multiple Kubernetes zones to a single project, thus making them all available for placement operations that happen within this project.

A cloud administrator can assign priorities on multiple levels.

- Kubernetes zone priority within a project.
- Resource priority within a Kubernetes zone.
- Cluster priority within a Kubernetes zone.

The cloud administrator can also assign tags on multiple levels:

- Capability tags per Kubernetes zone.
- Tags per resource assignment.

- Tags per cluster assignment.

You can create Kubernetes zones with supervisor namespaces on vSphere in the same way that you work with generic Kubernetes namespaces. To add a supervisor namespace to a Kubernetes zone, you must associate the zone with a vSphere 7 endpoint that contains the desired Pacific namespace resources.

Service Broker contains a version of the Kubernetes Zone page to enable Service Broker administrators to access existing Kubernetes zones so they can create placement policies for Kubernetes namespaces and clusters provisioned from the catalog.

Prerequisites

Configure integration with a suitable PKS deployment. See [Configure PKS Integration in vRealize Automation Cloud Assembly](#)

Procedure

1 Select **Infrastructure > Configure > Kubernetes Zone** and click **New Kubernetes Zone**.

2 Enter the PKS integration **Account** name to which you want this zone to apply.

This defines the cloud account or endpoint that is associated with the zone. You can assign only one endpoint to each zone. If you are working with Supervisor Namespace on vSphere, you can only select vSphere instances here that contain Supervisor namespaces.

3 Add a **Name** and **Description** for the Kubernetes Zone.

4 Add capability tags if appropriate. See [Using capability tags in vRealize Automation Cloud Assembly](#) for more information.

5 Click **Save**.

6 Click the On-demand tab and add PKS plans as appropriate for the zone to use for cluster provisioning.

You can select one or more plans and assign priorities to them. Lower numbers equal higher priority. Priority assignments are secondary to tag based selection.

7 Click the Cluster tab and then click the **Add Compute** button to add Kubernetes or supervisor clusters to the zone. If you are working with an external cluster, it is automatically onboarded to vRealize Automation Cloud Assembly when you select it.

You can add Kubernetes namespaces to the cluster on the Kubernetes Clusters page in vRealize Automation Cloud Assembly.

Results

Kubernetes zones are configured for use with vRealize Automation Cloud Assembly deployments.

What to do next

Assign the Kubernetes zone to a project.

- 1 Select **Infrastructure > Administration > Projects** and then select the project that you want to associate with your Kubernetes zone.
- 2 Click the Kubernetes Provisioning tab on the Project page.
- 3 Click **Add Kubernetes Zone** and add the zone that you just created. You can multiple zones if applicable, and you also set the priority on the zones.
- 4 Click **Save**.

After you assign a zone to a project, you can use the Cloud Templates page under the Design tab to provision a deployment based on the Kubernetes zone and project configuration. This Cloud Templates page includes options to add a K8S Cluster, K8S Namespace and Supervisor Namespace. Select the appropriate option for the Kubernetes resource you are working with.

Use Pacific supervisor clusters and namespaces with vRealize Automation Cloud Assembly

Administrators can configure vRealize Automation Cloud Assembly to use supervisor namespaces from an existing Pacific-enabled vSphere integration so that users can deploy namespaces in cloud templates and request them in the Service Broker catalog.

This task describes how to add supervisor clusters with vRealize Automation Cloud Assembly for use in deployments and how to create or add namespaces that define what vRealize Automation Cloud Assembly projects and users can access particular Kubernetes resources. This functionality relies on a suitable vSphere cloud account rather than an integration such as PKS or Openshift. Supervisor clusters are customized Kubernetes clusters associated with vSphere. They expose Kubernetes APIs to end users, and they use ESXI as a platform for worker nodes rather than Linux. Supervisor namespaces facilitate access control to Kubernetes resources, because it is typically easier to apply policies to namespaces than to individual virtual machines. You can create multiple namespaces for each supervisor cluster.

When used with Pacific enabled vSphere instances, Kubernetes zones define which supervisor clusters are available for provisioning with a supervisor namespace. Supervisor namespaces are specific to Pacific enabled vSphere instances. You cannot provision a generic Kubernetes resource to a Pacific enabled vSphere instance.

vRealize Automation Cloud Assembly users designated as project viewers have view only access to namespaces, while project members can edit them.

You can configure the supervisor clusters associated with namespaces if desired.

Prerequisites

- To use Pacific namespaces with vRealize Automation Cloud Assembly, you must have a vSphere 7.x endpoint configured. vSphere is installed as part of a vCenter cloud account. See [Create a vCenter cloud account in vRealize Automation](#).

- Project Pacific must be enabled on the vSphere cloud account, and it must contain appropriate supervisor namespaces.
- Both your vCenter and your vRealize Automation deployment should use the same Active Directory for users to be synched. Though provisioning will still function if this is not the case, vRealize Automation users will not get automatic access to the namespace.

Procedure

- 1 Select **Infrastructure > Configure > Kubernetes Zone** in vRealize Automation Cloud Assembly.

This page shows managed clusters that are available for use, and enables you to add additional clusters. You can click on any of the clusters to view their details.

- 2 Select **New Kubernetes Zone**.
- 3 Specify the **Account** details for the target vSphere cloud account.
- 4 Click the Search icon in the text box to either view all vSphere accounts or search for an account by name.
- 5 Type a **Name** and **Description** for the new zone.
- 6 Add capability tags if appropriate. See [Using capability tags in vRealize Automation Cloud Assembly](#) for more information.
- 7 Click the Provisioning tab to select the supervisor cluster that will be associated with the namespaces.
- 8 Click **Add Compute** to view and select the available supervisor clusters.
- 9 Click **Add**.
- 10 Select **Infrastructure > Administration > Projects** and then select the project that you want to associate with your Kubernetes zone.
- 11 Click the Kubernetes Provisioning tab on the Project page.
- 12 Click **Add Kubernetes Zone** and add the zone that you just created. You can multiple zones if applicable, and you also set the priority on the zones.
- 13 Click **Save**.

What to do next

After a namespace is configured, the **Infrastructure > Resources > Kubernetes** page in vRealize Automation Cloud Assembly for applicable users displays the namespace. Users can click the Address link on the Summary tab to open the vSphere Kubernetes CLI Tools to manage the namespace. Users must be a cloud administrator or a member of the namespace for the designated project to access a link to the Supervisor namespace details. Also users can download a customized Kubectl to use the Supervisor namespace. Users can log in to the supervisor namespace and use it as they would any other namespace, and then create cloud templates and deploy applications.

To add the namespace to a cloud template select **Design > Cloud Template** and select an existing cloud template or create a new one. Then you can select the Supervisor namespace item on the left menu and drag it to the canvas.

After you deploy cloud templates containing a supervisor namespace, users can also request supervisor namespaces from the Service Broker catalog. Also, you can click on the Deployments page in Cloud Assembly to view information about the deployment and access a link that contains the command to run the kubectl for the namespace on vSphere.

Working with Kubernetes clusters and namespaces in vRealize Automation Cloud Assembly

You can add, view, and manage the configuration of Kubernetes clusters and namespaces, both generic and Pacific-based, which are the basis of Kubernetes deployments in vRealize Automation Cloud Assembly.

You can view, add, and manage Kubernetes clusters and namespaces to which you are entitled access on the **Infrastructure > Resources > Kubernetes** page. Most typically, this page facilitates management of deployed clusters and namespaces.

- **Cluster:** A cluster is a group of Kubernetes nodes distributed across one or more physical machines. This page shows provisioned and undeployed clusters that have been configured for use on your vRealize Automation Cloud Assembly instance. You can click on a cluster to view information about its current status. When you deploy a cluster, it includes a link to a Kubeconfig file that is accessible only for cloud administrators. This file grants full admin privileges over the cluster including a list of namespaces.

Supervisor clusters are unique to vSphere instances and use ESXI as their worker nodes instead of Linux.

- **Namespaces:** Namespaces are virtual clusters that provide administrators with a way to segregate cluster resources. They facilitate management of resources among large groups of users and organizations. As a form of role-based access control, a cloud administrator can enable users to add namespaces to a project when they request a deployment and then later manage those namespaces from the Kubernetes Clusters page. When you deploy a namespace, it includes a link to a kubeconfig file that enables valid users, such as developers, to view and manage some aspects of that namespace.

Supervisor namespaces exist only on vSphere instances and provide Kubernetes-like access to vSphere objects.

If you are configuring new or existing cluster, you must select whether to connect with a master IP address or a master hostname.

Working with generic Kubernetes Clusters in vRealize Automation Cloud Assembly

You can add new, existing, or external clusters to vRealize Automation Cloud Assembly using the options on this page.

- 1 Select **Infrastructure > Resources > Kubernetes** and confirm that the Clusters tab is active.

If there are any clusters currently configured for your vRealize Automation Cloud Assembly instance, they appear on this page.

- 2 If you are adding a new or existing cluster, or deploying a cluster, select the appropriate option according to the following table.

Option	Description	Details
Deploy	Add new clusters to vRealize Automation Cloud Assembly	You must specify the TKGI cloud account that to which this cluster will be deployed as well as the desired plan and the number of nodes.
Add Existing	Configure an existing cluster to work with your project.	You must specify the TKGI cloud account, the cluster to use, and the appropriate project for the targeted developer. Also, you need to specify the sharing scope. If you want to share globally, you must configure your Kubernetes zones and namespaces appropriately.
Add External	Add a vanilla Kubernetes cluster, that might not be associated with TKGI, to vRealize Automation Cloud Assembly.	You must designate a project to which the cluster is associated, enter the IP address for the desired cluster and select a cloud proxy and certificate information required to connect to this cluster.

- 3 Click **Add** to make the cluster available within vRealize Automation Cloud Assembly.

Working with Kubernetes Namespaces in vRealize Automation Cloud Assembly

If you are a cloud administrator, namespaces help you group and manage Kubernetes cluster resources. If you are a user, namespaces are the area in Kubernetes clusters for your deployments. Administrators and users can access namespaces using the Namespaces tab located on the **Infrastructure > Resources > Kubernetes** page.

There are several ways to add Kubernetes namespaces to resources in vRealize Automation Cloud Assembly. The following procedure outlines one typical method.

- 1 Select **Infrastructure > Resources > Kubernetes** and click the Namespaces tab.
- 2 To add a new namespace, click **New Namespace**. To add an existing namespace click **Add Namespace**.

- 3 Enter a **Name** and **Description** for the namespace.

At this point you have added a namespace for use with Kubernetes resources, but it is not associated with anything in particular.

- 4 Specify the **Cluster** that you want to associate with this namespace.
- 5 Click **Create** to add the namespace to vRealize Automation Cloud Assembly.

Working with Supervisor clusters and Supervisor namespaces

You can view and change the configuration of supervisor clusters and namespaces on the Kubernetes page in vRealize Automation Cloud Assembly.

- 1 Select **Infrastructure > Resources > Kubernetes** in vRealize Automation Cloud Assembly.

- 2 Select **Add Supervisor Cluster**.
- 3 Specify the Account details for the target vSphere cloud account.
- 4 Click the Search icon in the Supervisor cluster text box to either view all supervisor clusters or search for a cluster by name.
- 5 Select the desired cluster and click **Add**.
- 6 Select the Supervisor Namespaces tab and click the **New Supervisor Namespace** button to add a new namespace.
- 7 Select the Supervisor Namespaces tab and click the **New Supervisor Namespace** button to add a new namespace.
 - a If you are creating a new namespace, add a **Name** and **Description**.
 - b Select the appropriate cloud **Account** to associate with the namespace.
 - c Select the **Supervisor cluster** to associate with this namespace.
 - d Select the **Project** to associate with the namespace.
 - e Click **Create**.
- 8 Review the relevant details for the new namespace.

Users and groups that currently have access to the namespace in vSphere are listed on the Users tab. If new users or groups are added to the project, click the **Update Users** button on this tab to update the list. The list is not updated automatically, so you must use the button to update.

Note Synchronization of users makes sense only if vRealize Automation Cloud Assembly and vCenter are configured with a common Active Directory/LDAP service.

After a namespace is configured, the **Infrastructure > Resources > Kubernetes** page in vRealize Automation Cloud Assembly for applicable users displays the namespace. Users can click the Address link on the Summary tab to open the vSphere Kubernetes CLI Tools to manage the namespace. Users must be a cloud administrator or a member of the namespace for the designated project to access a link to the Supervisor namespace details. Also users can download a customized Kubectl to use the Supervisor namespace. Users can log in to the supervisor namespace and use it as they would any other namespace, and then create cloud templates and deploy applications.

Adding Kubernetes components to cloud templates in vRealize Automation Cloud Assembly

When adding Kubernetes components to a vRealize Automation Cloud Assembly cloud template, you can choose to add clusters or enable users to create namespaces in various configurations. Typically, this choice depends on your access control requirements, how you have configured your Kubernetes components, and your deployment requirements.

To add a Kubernetes component to a cloud template in vRealize Automation Cloud Assembly, select **Design > Cloud Templates**, click **New**, and then locate and expand the Kubernetes option on the left menu. Then, make the desired selection, either Cluster or KBS Namespace by dragging it to the canvas.

Adding a Kubernetes cluster that is associated with a project to a cloud template is the most straightforward method of making Kubernetes resources available to valid users. You can use tags on clusters to control where they are deployed just as you do with other Cloud Assembly resources. You can use tags to select a zone and a VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) plan during the allocation phase of cluster deployment.

Once you add a cluster in this way, it is automatically available to all valid users.

Cloud template examples

The first cloud template example shows a template for a simple Kubernetes deployment that is controlled by tagging. A Kubernetes zone was created with two deployment plans, configured on the New Kubernetes Zone page. In this case, a tag called `placement:tag` was added as a capability on the zone, and it was used to match the analogous constraint on the cloud template. If there were more than one zone configured with the tag, the one with the lowest priority number would be selected.

```
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
```

The second cloud template examples shows how to set up a template with a variable called `$(input.hostname)` so that users can input the desired cluster hostname when requesting a deployment. Tags can also be used to select a zone and a TKGI plan during the resource allocation phase of cluster deployment.

```
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
```

If you want to use namespaces to manage cluster usage, you can set up a variable in the cloud template called `name: ${input.name}` to substitute for the namespace name which a user enters when requesting a deployment. For this sort of deployment, you would create a template something like the following example:

```
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}
```

Users can manage deployed clusters via kubeconfig files that are accessible from the **Infrastructure > Resources > Kubernetes Clusters** page. Locate the card on the page for the desired cluster and click **Kubeconfig**.

Supervisor Namespaces in VMware Cloud Templates

The following is the schema for a basic Supervisor namespace in a vRealize Automation Cloud Assembly cloud template.

```
{
  "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-zA-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 support the use of limits with supervisor namespaces. Limits enable you to control resource usage for CPUs and memory as well as the maximum number of pods allowed in the namespace by deployed machines.

```
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
```

Using vRealize Automation Cloud Assembly Extensibility with Kubernetes

vRealize Automation Cloud Assembly provides a standard set of event topics that correspond to typical actions related to Kubernetes cluster deployment. Users can subscribe to these topics as desired, and they receive notification when the event related to the subscribed topic occurs. You can also configure vRO workflows to run based on event notifications.

The following topics are available for subscription on the **Extensibility > Library > Event Topics** page in vRealize Automation Cloud Assembly. To view these topics, search for Kubernetes in the Event Topics Search text box.

- Kubernetes cluster allocation
- Kubernetes cluster post provision
- Kubernetes cluster post removal
- Kubernetes cluster provision
- Kubernetes cluster removal

Click one of the topics to view the schema for that topic which shows all the information that is collected and transmitted. You can use any of this schema information to set up various notifications and management and reporting tasks.

You can set up action scripts for CMX-related actions on the **Extensibility > Library > Actions** page. Action scripts can be used for various purposes: for example, to create a DNS record of Kubernetes cluster provisioning. If you are creating a DNS record, you can use the `masternodeips` field from the Kubernetes cluster post provision topic with a REST command in an Action script to create a DNS record.

The Subscriptions page defines the relationship between the event topics and action scripts. You can view and manage these components on the Subscriptions page in vRealize Automation Cloud Assembly

What Is configuration management in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly supports integration with Puppet Enterprise, Ansible Open Source, and Ansible Tower so that you can manage deployments for configuration and drift.

Puppet Integration

To integrate Puppet-based configuration management, you must have a valid instance of Puppet Enterprise installed on a public or private cloud with a vSphere workload. You must establish a connection between this external system and your vRealize Automation Cloud Assembly instance. Then you can make Puppet configuration management available to vRealize Automation Cloud Assembly by adding it to appropriate blueprints.

The vRealize Automation Cloud Assembly blueprint service Puppet provider installs, configures, and runs the Puppet agent on a deployed compute resource. The Puppet provider supports both SSH and WinRM connections with the following prerequisites:

- SSH connections:
 - The user name must be either a super user or a user with sudo permissions to run commands with NOPASSWD.
 - Disable `requiretty` for the given user.
 - cURL must be available on the deployment compute resource.
- WinRM connections:
 - PowerShell 2.0 must be available on the deployment compute resource.
 - Configure the Windows template as described in the vRealize Orchestrator documentation.

The DevOps administrator is responsible for managing the connections to a Puppet master and for applying Puppets roles, or configuration rules, to specific deployments. Following deployment, virtual machines configured to support configuration management are registered with the designated Puppet Master.

When virtual machines are deployed, users can add or delete a Puppet Master as an external system or update projects assigned to the Puppet Master. Finally, appropriate users can de-register deployed virtual machines from the Puppet Master when the machines are decommissioned.

Ansible Open Source Integration

When setting up an Ansible integration, install Ansible Open Source in accordance with the Ansible installation instructions. See the Ansible documentation for more information about installation.

Ansible enables host key checking by default. If a host is reinstalled with a different key in the `known_hosts` file, an error message appear. If a host is not listed in the `known_hosts` file, you must supply the key on start-up. You can disable host key checking with the following setting in the `/etc/ansible/ansible.cfg` or `~/.ansible.cfg` file:

```
[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
```

To avoid the host key checking errors, set `host_key_checking` and `record_host_keys` to `False` including adding an extra option `UserKnownHostsFile=/dev/null` set in `ssh_args`. In addition, if the inventory is empty initially, Ansible warns that the host list is empty. This causes the playbook syntax check to fail.

Ansible vault enables you to store sensitive information, such as passwords or keys, in encrypted files rather than as plain text. Vault is encrypted with a password. In vRealize Automation Cloud Assembly, Ansible uses Vault to encrypt data such as ssh passwords for host machines. It assumes that the path to the Vault password has been set.

You can modify the `ansible.cfg` file to specify the location of the password file using the following format.

```
vault_password_file = /path to/file.txt
```

You can also set the `ANSIBLE_VAULT_PASSWORD_FILE` environment variable so that Ansible automatically searches for the password. For example,

```
ANSIBLE_VAULT_PASSWORD_FILE=~/.vault_pass.txt
```

vRealize Automation Cloud Assembly manages the Ansible inventory file, so you must ensure that the vRealize Automation Cloud Assembly user has `rw` access on the inventory file.

```
cat ~/var/tmp/vmware/provider/user_defined_script/$(ls -t ~/var/tmp/vmware/provider/
user_defined_script/ | head -1)/log.txt
```

If you want to use a non-root user with vRealize Automation Cloud Assembly open-source integration, the users require a set of permissions to run the commands used by the vRealize Automation Cloud Assembly open-source provider. The following commands must be set in the user's `sudoers` file.

```
Defaults:myuser !requiretty
```

If the user is not part of an admin group that has no askpass application specified, set the following command in the user's sudoers file.

```
myuser ALL=(ALL) NOPASSWD: ALL
```

If you encounter errors or other problems when setting up Ansible integration, refer to the `log.txt` file at `'cat~/var/tmp/vmware/provider/user_defined_script/${ls -t ~/var/tmp/vmware/provider/user_defined_script/ | head -1) /'` on the Ansible Control Machine.

Ansible Tower Integration

Supported Operating System Types

- Red Hat Enterprise Linux 8.0 or later 64-bit (x86), supports only Ansible Tower 3.5 and greater.
- Red Hat Enterprise Linux 7.4 or later 64-bit (x86).
- CentOS 7.4 or later 64-bit (x86).

The following is a sample inventory file, which is generated during an Ansible Tower installation. You may need to modify it for vRealize Automation Cloud Assembly integration uses.

```
[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

```

Configure Puppet Enterprise integration in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly supports integration with Puppet Enterprise configuration management.

When you add Puppet Enterprise to Cloud Assembly as an external system, by default it is available on all projects. You can restrict it to specific projects.

To add a Puppet Enterprise integration, you must have the Puppet master name and the hostname or IP address of the master.

You can find Puppet logs at the following location in case you need to check them for errors or information purposes.

Description	Log Location
Log for create and install related events	Logs are on the deployed machine at <code>~/var/tmp/vmware/provider/user_defined_script/\$(ls -t ~/var/tmp/vmware/provider/user_defined_script/ head -1)/`</code> . Refer to the log.txt file for full logs. For detailed Puppet agent logs, refer to https://puppet.com/docs/puppet/4.8/services_agent_unix.html#logging
Log for Puppet delete and run related tasks	Logs are on the PE at <code>~/var/tmp/vmware/provider/user_defined_script/\$(ls -t ~/var/tmp/vmware/provider/user_defined_script/ head -1)/`</code> . Refer to the log.txt file for full logs.

Procedure

- 1 Select **Infrastructure > Connections > Integrations** and click **Add Integration**.
- 2 Select Puppet.
- 3 Enter the required information on the Puppet configuration page.
- 4 Click **Validate** to check the integration.
- 5 Click **Add**.

Results

Puppet is available for use with cloud templates.

What to do next

Add Puppet components to the desired cloud templates.

- 1 Under Cloud Templates in Cloud Assembly, select Puppet under the Content Management heading on the cloud template menu and drag the Puppet component to the canvas.
- 2 Enter Puppet Properties on the pane to the right.

Property	Description
Master	Enter the name of the Puppet primary machine to be used with this cloud template.
Environment	Select the environment for the Puppet primary machine.
Role	Select the Puppet role to be used with this cloud template.
Agent Run Interval	The frequency at which you want the Puppet agent to poll the Puppet primary machine for configuration details to be applied to deployed virtual machines related to this cloud template.

- 3 Click the Code tab on the right pane to view the YAML code for the Puppet configuration properties.

Configure Ansible Open Source integration in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly supports integration with Ansible Open Source configuration management. After configuring integration, you can add Ansible components to new or existing deployments.

When you integrate Ansible Open Source with vRealize Automation Cloud Assembly, you can configure it to run one or more Ansible playbooks in a given order when a new machine is provisioned to automate configuration management. You specify the desired playbooks in the cloud template for a deployment.

When setting up an Ansible integration, you must specify the Ansible Open Source host machine as well as the inventory file path that defines information for managing resources. In addition, you must provide a name and password to access the Ansible Open Source instance. Later, when you add an Ansible component to a deployment, you can update the connection to use key-based authentication.

By default, Ansible uses ssh to connect to the physical machines. If you are using Windows machines as specified in the cloud template with the `osType Windows` property, the `connection_type` variable is automatically set to `winrm`.

Initially, Ansible integration uses the user/password or user/key credentials provided in the integration to connect to the Ansible Control Machine. Once the connection is successful, the provided playbooks in the cloud template are validated for syntax.

If the validation is successful, then an execution folder is created on the Ansible Control Machine at `~/var/tmp/vmware/provider/user_defined_script/`. This is the location from which scripts run to add the host to the inventory, create the host vars files including setting up the authentication mode to connect to the host, and finally run the playbooks. At this point, the credentials provided in the cloud template are used to connect to the host from the Ansible Control Machine.

Ansible integration supports physical machines that do not use an IP address. For machines provisioned on public clouds such as AWS, Azure, and GCP, the address property in the created resource is populated with the machine's public IP address only when the machine is connected to a public network. For machines not connected to a public network, the Ansible integration looks for the IP address from the network attached to the machine. If there are multiple networks attached, Ansible integration looks for the network with the least deviceIndex; that is, the index of the Network Interface Card (NIC) attached to the machine. If the deviceIndex property is not specified in the blueprint, the integration uses the first network attached.

See [What Is configuration management in vRealize Automation Cloud Assembly](#) for more details on configuring Ansible Open Source for integration in vRealize Automation Cloud Assembly.

Prerequisites

- The Ansible control machine must use Ansible version 2.6.0 or later.

- The user must have read/write access to the directory where the Ansible inventory file is located. In addition, the user must have read/write access to the inventory file, if it exists already.
- If you are using a non-root user with the sudo option, ensure that the following is set in the sudoers file:

```
Defaults:user_name !requiretty
```

and

```
username ALL=(ALL) NOPASSD: ALL
```

- Ensure that host key checking is disabled by setting `host_key_checking = False` at `/etc/ansible/ansible.cfg` or `~/.ansible.cfg`.
- Ensure that the vault password is set by adding the following line to the `/etc/ansible/ansible.cfg` or `~/.ansible.cfg` file:

```
vault_password_file = /path/to/password_file
```

The vault password file contains the password in plain text and is used only when cloud templates or deployments provide the username and password combination to use between ACM and the node as show in the following example.

```
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
```

- To avoid host key failures while trying to run playbooks, it is recommended that you include the following settings in `/etc/ansible/ansible config`.

```
[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.
```

Procedure

- 1 Select **Infrastructure > Connections > Integrations** and click **Add Integration**.

- 2 Click **Ansible**.

The Ansible configuration page appears.

- 3 Enter the Hostname, Inventory File Path and other required information for the Ansible Open Source instance.
- 4 Click **Validate** to check the integration.

5 Click **Add**.

Results

Ansible is available for use with cloud templates.

What to do next

Add Ansible components to the desired cloud templates.

- 1 On the cloud template canvas page, select Ansible under the Configuration Management heading on the cloud template options menu and drag the Ansible component to the canvas.
- 2 Use the panel on the right to configure the appropriate Ansible properties such as specifying the playbooks to run.

In Ansible, users can assign a variable to a single host, and then use it later in playbooks.

Ansible Open Source integration enables you to specify these host variable in cloud templates.

The `hostVariables` property must be in proper YAML format, as expected by the Ansible control machine, and this content will be placed at the following location:

```
parent_directory_of_inventory_file/host_vars/host_ip_address/vra_user_host_vars.yml
```

The default location of the Ansible inventory file is defined in the Ansible account as added on the Integrations page in Cloud Assembly. The Ansible integration will not validate the `hostVariable` YAML syntax in the cloud template, but the Ansible Control Machine will throw an when you run a playbook in the case of incorrect format or syntax.

The following cloud template YAML snippet shows an example usage of the `hostVariables` property.

```
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}
```

Ansible integrations expect authentication credentials to be present in a cloud template in one of the following ways:

- User name and password in the Ansible resource.

- User name and `privateKeyFile` in the Ansible resource.
- Username in Ansible resource and `privatekey` in the compute resource by specifying `remoteAccess` to `generatedPublicPrivateKey`.

In cloud templates, ensure that the path to the Ansible playbook is accessible to the user specified in the integration account. You can use an absolute path to specify the playbook location, but it is not necessary. An absolute path to the user's home folder is recommended so that the path remains valid even if the Ansible integration credentials change over time.

Configure Ansible Tower Integration in vRealize Automation Cloud Assembly

You can integrate Ansible Tower with vRealize Automation Cloud Assembly to support configuration management of deployed resources. After configuring integration, you can add Ansible components to new or existing deployments from the cloud template editor.

vRealize Automation Cloud Assembly supports integration with Ansible Tower versions 3.5, 3.6, and 3.7.

Prerequisites

- Grant non-administrator users the appropriate permissions to access Ansible Tower. There are two options that work for most configurations. Choose the one that is most appropriate for your configuration.
 - Grant users Inventory Administrator and Job Template Administrator roles at the organization level.
 - Grant users Administrator permission for a particular inventory and the Execute role for all job templates used for provisioning.
- You must configure the appropriate credentials and templates in Ansible Tower for use with your deployments. Templates define the inventory and playbook for use with a deployment. There is a 1:1 mapping between a job template and a playbook. Playbooks use a YAML-like syntax to define tasks that are associated with the template. For most typical deployments, use machine credentials for authentication.
 - a Log in to Ansible Tower and navigate to the Job Templates section.
 - b Select Adding a new job template.
 - Select the credential that you already created. These are the credentials of the machine to be managed by Ansible Tower. For each job template, there can be one credential object.
 - For the Limit selection, select Prompt on Launch. This ensures that the job template runs against the node being provisioned or de-provisioned from vRealize Automation Cloud Assembly. If this option is not selected, a Limit is not set error will appear when the blueprint that contains the job template is deployed.
- You can view the execution of the Job templates invoked from vRealize Automation Cloud Assembly on the Ansible Tower Jobs tab .

Procedure

- 1 Select **Infrastructure > Connections > Integrations** and click **Add Integration**.
- 2 Click **Ansible Tower**.
The Ansible configuration page appears.
- 3 Enter the **Hostname**, which can be an IP address, and other required information for the Ansible Tower instance.
- 4 Enter the UI-based authentication **Username** and **Password** for the applicable Ansible Tower instance.
- 5 Click **Validate** to verify the integration.
- 6 Type an appropriate **Name** and **Description** for the integration.
- 7 Click **Add**.

Results

Ansible Tower is available for use in cloud templates.

What to do next

Add Ansible Tower components to the desired cloud templates. Make sure to specify the applicable job template with execute permission for the user specified in the integration account.

- 1 On the cloud template canvas page, select **Ansible** under the **Configuration Management** heading on the blueprint options menu and drag the Ansible Tower component to the canvas.
- 2 Use the panel on the right to configure the appropriate Ansible properties such as job templates.

How do I create an Active Directory integration in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly supports integration with Active Directory servers to provide out of the box creation of computer accounts in a specified Organizational Unit (OU) within an Active Directory server prior to provisioning a virtual machine. Active Directory supports an LDAP connection to the Active Directory server.

An Active Directory policy that is associated with a project is applied to all virtual machines provisioned within the scope of that project. Users can specify one or more tags to selectively apply the policy to virtual machines that are provisioned to the cloud zones with matching capability tags.

For on-premises deployments, Active Directory integration enables you to set up a health check feature that shows the status of the integration and the underlying ABX integration on which it relies, including the required extensibility cloud proxy. Prior to applying an Active Directory policy, vRealize Automation Cloud Assembly checks the status of the underlying integrations. If the integration is healthy, vRealize Automation Cloud Assembly creates the deployed computer objects in the specified Active Directory. If the integration is unhealthy, the deploy operation skips the Active Directory phase during provisioning.

Prerequisites

- Active Directory integration requires an LDAP connection to the Active Directory server.
- If you are configuring an Active Directory integration with vCenter on-premises, you must configure an ABX integration with an extensibility cloud proxy. Select **Extensibility > Activity > Integrations** and choose **Extensibility Actions On Prem**.
- If you are configuring an integration with Active Directory in the cloud, you must have a Microsoft Azure or Amazon Web Services account.
- You must have a project configured with appropriate cloud zones, and image and flavor mappings to use with the Active Directory integration.
- The desired OU on your Active Directory must be pre-created before you associated your Active Directory integration with a project.

Procedure

- 1 Select **Infrastructure > Connections > Integrations** and then **New Integration**.
- 2 Click **Active Directory**.
- 3 On the **Summary** tab, enter the appropriate LDAP host and environment names.
- 4 Enter the name and password for the LDAP server.
- 5 Enter the appropriate Base DN for the desired users and groups in your Active Directory.

Note You can specify only one DN per Active Directory integration.

- 6 Click **Validate** to ensure that the integration is functional.
- 7 Enter a Name and Description of this integration.
- 8 Click **Save**.
- 9 Click the **Project** tab to add a project to the Active Directory integration.

On the **Add Projects** dialog, you must select a project name and a relative DN, which is a DN that exists within the Base DN specified on the Summary tab.

- 10 Click **Save**.

Results

You can now associate the project with Active Directory integration to a cloud template. When a machine is provisioned using this cloud template, it is pre-staged in the specified Active Directory and Organizational Unit.

You can also implement a tag-based health check for on- premises Active Directory integrations as follows.

- 1 Create an Active Directory integration as described in the preceding steps.
- 2 Click the **Project** tab to add a project to the Active Directory integration.
- 3 Select a project name and a relative DN on the Add Projects dialog. The relative DN must exist within the specified base DN.
- 4 Add appropriate tags. These tags are applicable to the cloud zone to which the Active Directory policy may apply.
- 5 Click Save.

The Status of the Active Directory integration is displayed for each integration on the **Infrastructure > Connections > Integrations** page in vRealize Automation Cloud Assembly.

You can associate the project with Active Directory integration with a cloud template. When a machine is provisioned using this template, it is pre-staged in the specified Active Directory and OU.

Configure a VMware SDDC Manager integration

You can add a VMware SDDC Manager integration to vRealize Automation to facilitate using workload domains as part of VMware Cloud Foundation (VCF) cloud accounts within vRealize Automation.

Prerequisites

- vRealize Automation supports integration only with VMware SDDC manager 4.1 and newer.

Procedure

- 1 Select **Infrastructure > Connections > Integrations** and click **Add Integration**.
- 2 Select SDDC Manager.

The SDDC Manager integration configuration page appears.

- 3 In the Summary section, enter a **Name** and **Description** for the integration.
- 4 In the SDDC Manager Credentials section, enter the **SDDC Mgr IP address/FQDN** for the SDDC Manager server machine.

- 5 Enter the Username and Password for the admin account to be used to initially connect to the SDDC Manager. As a best practice, avoid using the administrator account to connect. Use a different account that has admin privileges in SDDC Manager to create service roles.

These credentials are used to initially set up the connection to the SDDC Manager, and then service credentials are created to use when connecting from a VCF cloud account.

- 6 Click **Validate** to verify the connection to the SDDC Manager.

- 7 Click **Add**.

Results

After the integration is created, you can view workloads associated with the SDDC on the Workload Domain tab that appears on the completed integration page. Also, you can view and select workloads associated with the integration and then click the **Add Cloud Account** button to open a page for creating a VCF cloud account that will use the selected workload.

What to do next

After you configure the VCF cloud account, a **Setup Cloud** button appears at the top of the page. Click this button to initiate the VCF cloud setup wizard.

Integrating with vRealize Operations Manager

vRealize Automation can work with vRealize Operations Manager to perform advanced workload placement, provide deployment health and virtual machine metrics, and display pricing.

Number and type of integrations

Integration between the two products must be on-premises to on-premises, not a mix of on-premises and cloud.

You can integrate one vRealize Automation instance with multiple vRealize Operations Manager instances, but a vRealize Operations Manager instance can only be connected to one vRealize Automation instance.

You cannot connect an aggregated vRealize Operations Manager cluster to vRealize Automation.

Basic requirements for integration

To integrate with vRealize Operations Manager, go to **Infrastructure > Connections > Integrations**. To add the integration, you need the vRealize Operations Manager URL and credentials for the login account described in the next section. In addition, vRealize Automation and vRealize Operations Manager need to manage the same vSphere endpoint.

Login account for integration

In vRealize Operations Manager, you need a local or non-local vRealize Operations Manager login account for the integration to use. The account requires read-only privileges to the vCenter adapter instance for the vSphere endpoint. Note that a non-local account might need to be imported in vRealize Operations Manager and have its read-only role assigned. For the integration, the username format for non-local account login is *username@domain@authenticated-source*, such as *jdoe@company.com@workspaceone*. Authenticated sources are defined during vRealize Operations Manager server initial setup.

See the following sections for details. For pricing information, see [What are Pricing Cards](#).

Advanced workload placement using vRealize Operations Manager

vRealize Automation and vRealize Operations Manager can work together to optimally place deployment workloads.

You enable workload placement at the vSphere based cloud zone level. Only Distributed Resource Scheduler (DRS) enabled clusters of a cloud zone are eligible for advanced placement using vRealize Operations Manager.

- vRealize Automation placement—The vRealize Automation placement engine is application intent based. It considers tag-based constraints, project membership and the associated cloud zones, and affinity filters related to network, storage, and compute. Resource placement depends on all of these factors plus the presence of other, related target resources in the same deployment.
- vRealize Operations Manager placement—vRealize Operations Manager considers operational intent for optimal placement. Operational intent can take past workloads and future, what-if predictions into account.

When using advanced workload placement, you must apply vRealize Automation tagging in order to implement business intent decisions, instead of using the vRealize Operations Manager business intent options.

When integrating with vRealize Operations Manager, vRealize Automation continues to follow its application intent model and its related constraints to filter for target placement. Then, from within those results, it uses the vRealize Operations Manager recommendation to further refine placement.

In the absence of a recommendation

If you enable advanced workload placement, and vRealize Operations Manager analysis returns no recommendations, you may configure vRealize Automation to fall back to its default, application intent placement.

Limitations on workload placement

Certain limitations apply when using vRealize Operations Manager to place workloads.

- vRealize Operations Manager does not support workload placement on resource pools in vCenter Server.

- If vRealize Operations Manager is down, the timeout used for workload placement to call vRealize Operations Manager might expire.
- Placement doesn't cross multiple cloud zones. vRealize Automation sends one cloud zone to vRealize Operations Manager for placement recommendations within that single cloud zone.

How to enable workload placement

To enable workload placement, there are steps to take for vSphere, vRealize Operations Manager, and vRealize Automation.

- 1 In vRealize Automation Cloud Assembly, connect to your vCenter Server cloud account.

The options are under **Infrastructure > Connections > Cloud Accounts**.

- 2 In vCenter Server, verify that DRS enabled clusters exist and are set to fully automated.

- 3 In vRealize Operations Manager, verify that the same vCenter Server is being managed.

You need vRealize Operations Manager 8 or later.

- 4 In vRealize Automation Cloud Assembly, add the vRealize Operations Manager integration.

The options are under **Infrastructure > Connections > Integrations**.

To add the integration, you need the vRealize Operations Manager primary node URL below, plus the login username and password.

`https://operations-manager-IP-address-or-FQDN/suite-api`

After entering the values, click VALIDATE.

- 5 Synchronize the integration to the vCenter Server by clicking SYNC.

Also synchronize any time that vRealize Automation Cloud Assembly and vRealize Operations Manager begin managing a new vCenter Server.

- 6 In vRealize Automation Cloud Assembly, create a cloud zone for the vCenter Server account.

The options are under **Infrastructure > Configure > Cloud Zones**.

- 7 Under the cloud zone Summary tab, set the Placement Policy to ADVANCED.

- 8 Under the Placement Policy, select whether to have vRealize Automation fall back to its default placement if vRealize Operations Manager returns no recommendations.

Troubleshooting workload placement

If vRealize Operations Manager isn't recommending workload placements the way that you expect, review the deployment request details in vRealize Automation Cloud Assembly or vRealize Automation Service Broker.

- 1 Go to **Infrastructure > Activity > Requests**, and click the request.

- 2 In Request Details, look at the allocation phases.

Look for targets that were successfully or unsuccessfully identified.

- 3 In Request Details, at the upper right, enable Dev Mode.

- 4 Follow the request path to locate filter blocks.
- 5 Click a filter block, and review the following section.

```
filterName: ComputePlacementPolicyAffinityHostFilter
  v computeLinksBefore
  v computeLinksAfter
  v filteredOutHostsReasons
```

Entry	Description
computeLinksBefore	List of potential placement hosts based on vRealize Automation algorithms.
computeLinksAfter	Selected placement host.
filteredOutHostsReasons	<p>Messages describing why a host was selected or rejected.</p> <p>When vRealize Operations Manager selects the host, the following message appears.</p> <p>advance policy filter: Filtered hosts based on recommendation from vROPS.</p>

Continuous optimization using vRealize Operations Manager

When you add the vRealize Automation adapter in vRealize Operations Manager, vRealize Operations Manager automatically creates a new custom datacenter (CDC) for vRealize Automation based workloads.

With continuous optimization, you take advantage of workload rebalancing and relocation, and use vRealize Automation with vRealize Operations Manager beyond initial workload placement. As virtualization resources move or come under heavier or lighter load, vRealize Automation provisioned workloads can move as needed.

- Continuous optimization automatically creates a new CDC in vRealize Operations Manager. There is one new CDC for each vRealize Automation vSphere cloud zone.
- The newly created CDC contains every vRealize Automation managed cluster associated with the cloud zone.

Note Do not manually create a mixed CDC of vRealize Automation and non-vRealize Automation clusters.

- You use vRealize Operations Manager to run continuous optimization for the newly created vRealize Automation based CDC.
- Workloads can only be rebalanced or relocated within the same cloud zone or CDC.
- Optimization never creates a new vRealize Automation or vRealize Operations Manager placement violation.
 - If you have existing placement violations, optimization can fix vRealize Operations Manager operational intent issues.
 - If you have existing placement violations, optimization cannot fix vRealize Operations Manager business intent issues.

For example, if you used vRealize Operations Manager to manually move a virtual machine to a cluster that doesn't support your constraints, vRealize Operations Manager doesn't detect a violation nor try to resolve it.

- This release obeys operational intent at the CDC level. All member vRealize Automation clusters are optimized to the same settings.

To set a different operational intent for clusters, you must configure them in separate vRealize Automation CDCs, associated with separate vSphere cloud zones. Having different test and production clusters might be one example situation.

- vRealize Automation application intent and the constraints defined in vRealize Automation are honored during any optimization rebalance or relocation operations.
- vRealize Operations Manager placement tags cannot be applied to vRealize Automation provisioned workloads.

In addition, scheduled optimization involving multiple machines is supported. Regularly scheduled optimizations are not all-or-nothing processes. If conditions interrupt machine movement, successfully relocated machines stay relocated, and the next vRealize Operations Manager cycle attempts to relocate the remainder as is usual for vRealize Operations Manager. Such a partially completed optimization causes no negative effect in vRealize Automation.

How to enable continuous optimization

When you add the vRealize Automation adapter in vRealize Operations Manager, vRealize Operations Manager automatically creates a new, dedicated datacenter for vRealize Automation based workloads.

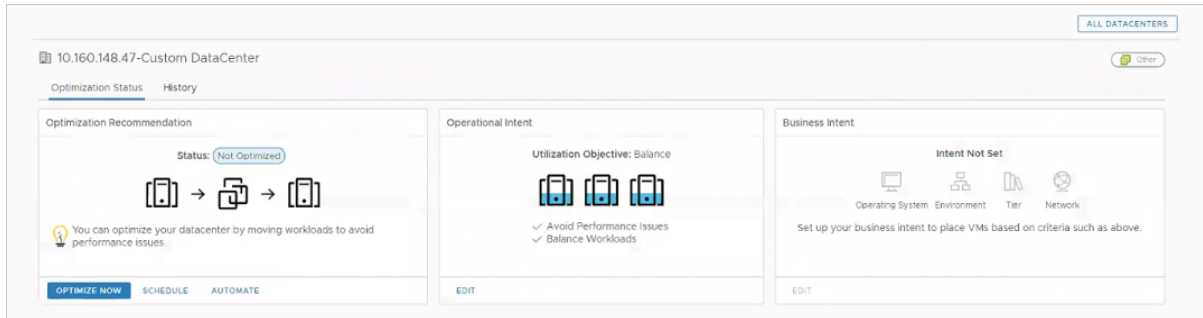
Other than adding the integration within vRealize Automation Cloud Assembly, there are no separate installation steps for continuous optimization. You may begin configuring and using vRealize Operations Manager for workload relocation in the new datacenter. See the [Continuous optimization example](#).

Continuous optimization example

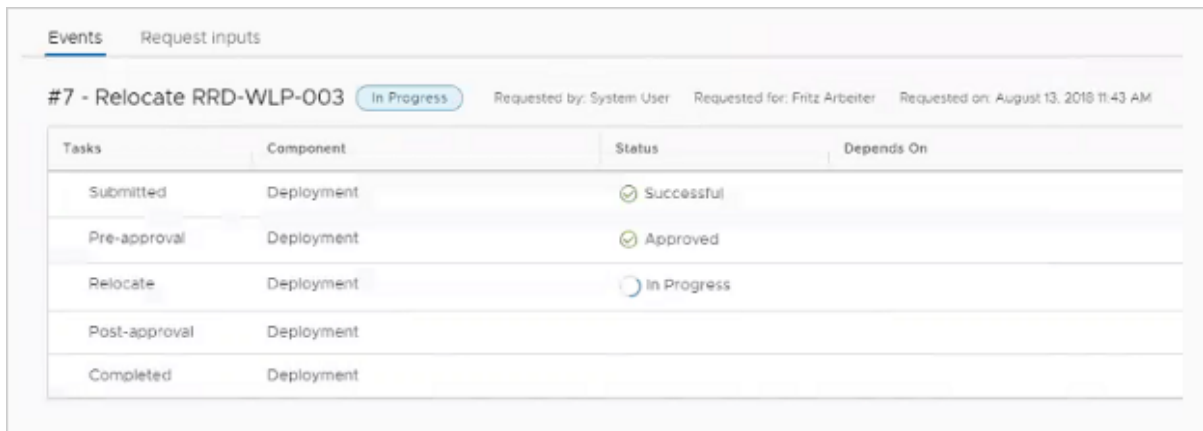
The following example shows a rebalancing workflow for vRealize Automation continuous optimization with vRealize Operations Manager.

- 1 From the vRealize Operations Manager home page, click **Workload Optimization**.
- 2 Select the automatically created vRealize Automation datacenter.
- 3 Under **Operational Intent**, click **Edit**, and select **Balance**.

You cannot select or edit Business Intent, which is disabled when the datacenter is for vRealize Automation optimization.

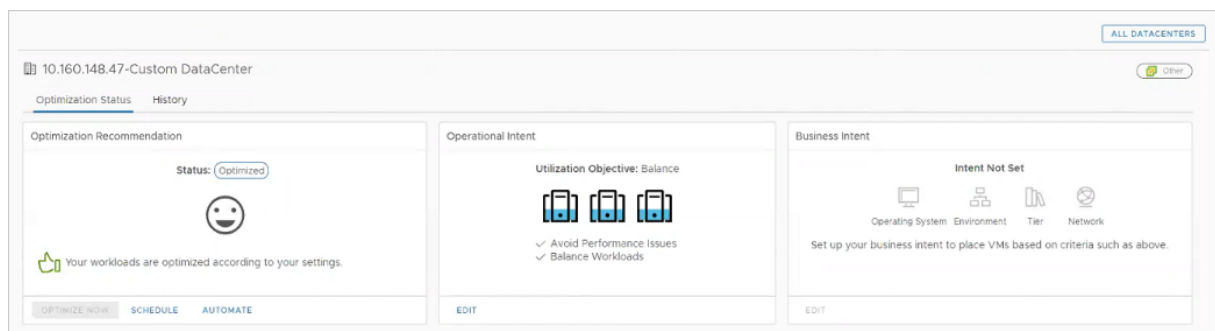


- 4 Under **Optimization Recommendation**, click **Optimize Now**.
vRealize Operations Manager displays a before-and-after diagram of the proposed operation.
- 5 Click **Next**.
- 6 Click **Begin Action**.
- 7 In vRealize Automation, monitor the operation in progress by clicking **Deployments** and looking at event status.



When rebalancing finishes, vRealize Automation refreshes. The Compute Resources page shows that machines have moved.

In vRealize Operations Manager, the next data collection refreshes the display to show that optimization is complete.



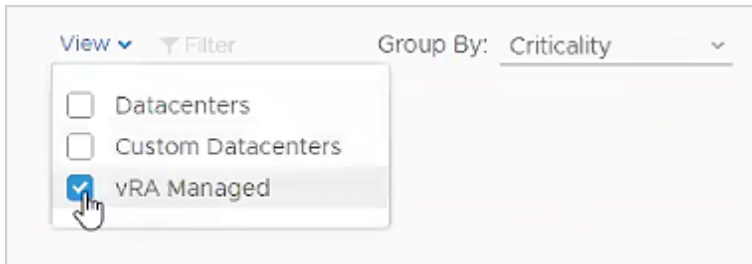
In vRealize Operations Manager, you can review the operation by clicking **Administration > History > Recent Tasks**.

Locate vRealize Automation managed datacenters

You can use vRealize Operations Manager to display only the vRealize Automation managed datacenters.

Procedure

- 1 From the vRealize Operations Manager home page, click **Workload Optimization**.
- 2 Near the top right, click the **View** drop-down.
- 3 Select only the vRealize Automation managed datacenters.



Deployment monitoring based on vRealize Operations Manager

vRealize Automation can show vRealize Operations Manager data about your deployments.

Reviewing the filtered set of metrics directly in vRealize Automation saves you the task of accessing or searching vRealize Operations Manager. Although you cannot launch in context to vRealize Operations Manager, you are of course free to log in and use vRealize Operations Manager for additional data as needed.

Enable vRealize Operations Manager data

For vRealize Automation to show vRealize Operations Manager data, you add the vRealize Operations Manager integration.

Procedure

- 1 In vRealize Operations Manager, go to **Administration > Solutions**.
- 2 Under **Configured Adapter Instances**, verify that you have a [vCenter Adapter](#) for the vSphere cloud zone that vRealize Automation provisions to and that it is receiving data.
- 3 In vRealize Automation Cloud Assembly, go to **Infrastructure > Connections > Integrations**.
- 4 Enter the vRealize Operations Manager primary node URL, plus the vRealize Operations Manager login username and password.
`https://operations-manager-IP-address-or-FQDN/suite-api`
- 5 Click **Deployments**, select a deployment, and verify that the Monitor tab appears.

Health and alerts provided by vRealize Operations Manager

When monitoring is enabled, vRealize Automation retrieves vRealize Operations Manager Health and associated alerts about your deployments.

To access monitoring, click a deployment and select the **Monitor** tab. If the tab is missing, see [Enable vRealize Operations Manager data](#).

To see alerts, highlight the deployment name at the top of the component tree in the left panel.

- You can review the severity and text of the alerts.
- To focus on areas of concern, filter and sort on data in the columns.
- Only Health badges and Health alerts appear. Other alert types such as Efficiency or Risk are not supported.

Metrics provided by vRealize Operations Manager

When monitoring is enabled, vRealize Automation retrieves vRealize Operations Manager metrics about your deployments.

To access monitoring, click a deployment and select the **Monitor** tab. If the tab is missing, see [Enable vRealize Operations Manager data](#).

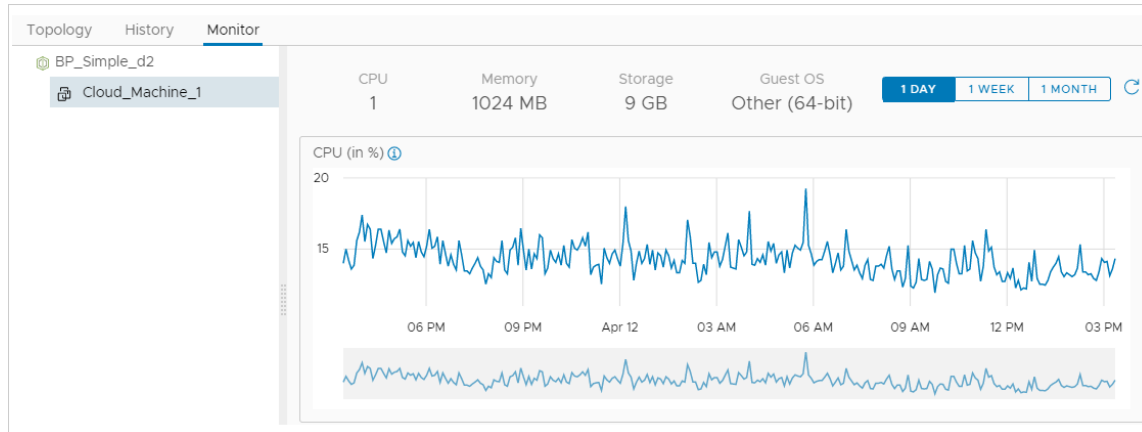
To see metrics, expand the component tree on the left, and highlight a virtual machine.

- Metrics are not cached. They come directly from vRealize Operations Manager and might take a few moments to load.
- Only virtual machine metrics appear. Metrics from other components such as vCloud Director, Software, or XaaS are not supported.
- Only vSphere virtual machine metrics appear. Other cloud providers such as AWS or Azure are not supported.

Metrics appear as timeline graphs that show highs and lows for the following measures.

- CPU
- Memory
- Storage IOPS
- Network MBPS

To reveal the specific metric name, click the blue information icon at the upper left corner of the timeline.

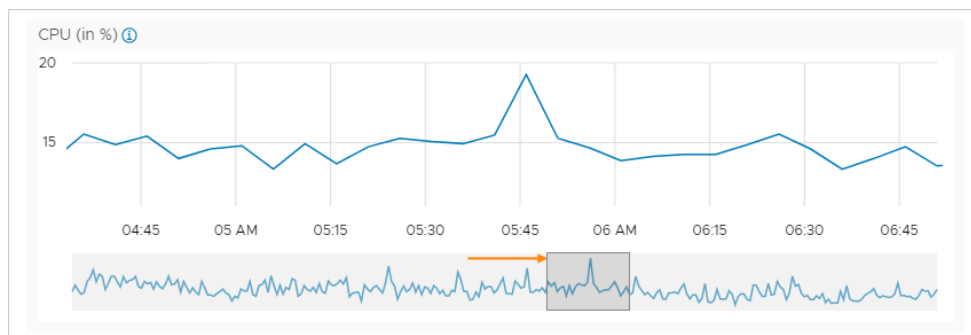


Acting on data provided by vRealize Operations Manager

When metrics provided by vRealize Operations Manager expose a problem, you can identify trouble areas directly in vRealize Automation.

To see metrics provided by vRealize Operations Manager, click a deployment and select the **Monitor** tab. If the tab is missing, see [Enable vRealize Operations Manager data](#).

Metrics for the past day, week, or month are available. To zoom in on an area of concern, select a small area in the lower, shaded part under any metric timeline:



What are onboarding plans in vRealize Automation Cloud Assembly

You use a workload onboarding plan to identify machines that have been data-collected from a cloud account type in a target region or data center but that are not yet managed by a vRealize Automation Cloud Assembly project.

When you add a cloud account that contains machines that were deployed outside of vRealize Automation Cloud Assembly, the machines are not managed by Cloud Assembly until you onboard them. Use an onboarding plan to bring unmanaged machines into vRealize Automation Cloud Assembly management. You create a plan, populate it with machines, and then run the plan to import the machines. Using the onboarding plan, you can create a cloud template and can also create one or many deployments.

You can onboard one or many unmanaged machines in a single plan. You can select machines manually or by using a filtering rule. Filtering rules select machines for onboarding based on criteria such as machine name, status, IP address, and tags.

- You can onboard up to 3,500 unmanaged machines within a single onboarding plan per hour.
- You can onboard up to 17,000 unmanaged machines concurrently within multiple onboarding plans per hour.

Machines that are available for workload onboarding are listed on the **Resources > Machines** page relative to a specific cloud account type and region and labeled as `Discovered` in the Origin column. Only machines that have been data-collected are listed. After you onboard the machines, they appear in the Origin column as `Deployed`.

The person who runs the workload onboarding plan is automatically assigned as the machine owner.

Onboarding examples

For examples of onboarding techniques, see [Example: Onboard selected machines as a single deployment in vRealize Automation Cloud Assembly](#) and [Example: Onboard rule-filtered machines as separate deployments in vRealize Automation Cloud Assembly](#).

Onboarding event subscriptions

A `Deployment Onboarded` event is created when you run the plan. Using Extensibility tab options, you can subscribe to these deployment events and perform actions on them.

Example: Onboard selected machines as a single deployment in vRealize Automation Cloud Assembly

In this example, you onboard two unmanaged machines as a single vRealize Automation Cloud Assembly deployment and create a single cloud template for all machines in the plan.

When you create a cloud account, all machines that are associated to it are data-collected and then displayed on the **Infrastructure > Resources > Machines** page. If the cloud account has machines that were deployed outside of vRealize Automation Cloud Assembly, you can use an onboarding plan to allow vRealize Automation Cloud Assembly to manage the machine deployments.

Note You can only rename deployments before they are onboarded. After onboarding, the **Rename** option is disabled.

Prerequisites

- Verify that you have the required user role. See [What are the vRealize Automation user roles](#).
- Review [What are onboarding plans in vRealize Automation Cloud Assembly](#).
- Create and prepare a vRealize Automation Cloud Assembly project.

This procedure involves some of the steps from the basic Wordpress use case. See [Tutorial: Setting up and testing multi-cloud infrastructure and deployments in vRealize Automation Cloud Assembly](#).

- Create a project, add users, and assign user roles in the project. See [Part 2: Create the example vRealize Automation Cloud Assembly project](#).
- Create an Amazon Web Services cloud account for the project. See [1. Add cloud accounts](#).

The Amazon Web Services cloud account in this procedure contains machines that were deployed before the cloud account was added to vRealize Automation Cloud Assembly and by an application other than vRealize Automation Cloud Assembly.

- Verify that the **Machines** page contains machines to onboard. See [Machine resources in vRealize Automation](#).

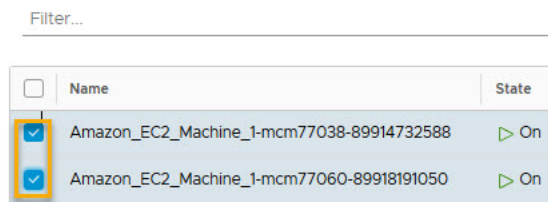
Procedure

- 1 Go to **Infrastructure > Onboarding**.
- 2 Click **New Onboarding Plan** and enter sample values.

Setting	Sample Value
Plan name	VC-sqa-deployments
Description	Sample onboarding plan for AWS machine for OurCo-AWS cloud account
Cloud account	OurCo-AWS
Default project	WordPress

- 3 Click **Create**.
- 4 On the plan's **Deployments** tab, click **Select Machines**, choose one or more machines, and click **OK**.

Select Machines



- 5 Select **Create one deployment that contains all the machines** and click **Create**.
- 6 Click the check box next to the new deployment name and click **Cloud template....**
- 7 Click **Create cloud template in Cloud Assembly format**.

- 8 Enter a cloud template name and click **Save**.

Note When your onboarding plan uses a vSphere machine, you must edit the cloud template after the onboarding process is complete. The onboarding process cannot link the source vSphere machine and its machine template, and the resultant cloud template will contain the `imageRef: "no image available"` entry in the cloud template code. The cloud template cannot be deployed until you specify the correct template name in the `imageRef:` field. To make it easier to locate and update the cloud template after the onboarding process is complete, use the **Cloud template name** option on the deployment's **Cloud template configuration** page. Record the auto-generated cloud template name or enter and record a cloud template name of your choice. When onboarding is complete, locate and open the cloud template and replace the `"no image available"` entry in the `imageRef:` field with the correct template name.

- 9 Click the deployment name check box, click **Run**, and then click **Run** again on the **Run plan** page.

The selected Amazon Web Services machines are onboarded as a single deployment, with an accompanying cloud template.

- 10 Open and examine the cloud template by clicking the **Cloud templates** tab and then clicking the cloud template name.
- 11 Open and examine the deployment by clicking the **Deployments** tab and then clicking the deployment name.

Example: Onboard rule-filtered machines as separate deployments in vRealize Automation Cloud Assembly

In this example, you use a filtering rule to onboard machines whose state is On and whose name begins with the letters BG. You also create a separate vRealize Automation Cloud Assembly cloud template and deployment for each machine in the plan.

When you create a cloud account, all machines that are associated to it are data-collected and then displayed on the **Infrastructure > Resources > Machines** page. If the cloud account has machines that were deployed outside of vRealize Automation Cloud Assembly, you can use an onboarding plan to allow vRealize Automation Cloud Assembly to manage the machine deployments.

Prerequisites

- Verify that you have the required user role. See [What are the vRealize Automation user roles](#).
- Review [What are onboarding plans in vRealize Automation Cloud Assembly](#).
- Create and prepare a vRealize Automation Cloud Assembly project and populate it with one or more cloud accounts.

This involves some of the basic steps in your guided setup procedure.

- Create a project, add users, and assign user roles in the project. See [Part 2: Create the example vRealize Automation Cloud Assembly project](#).
- Create one or more cloud accounts in designated regions for the project.
- Verify that the **Machines** page contains machines to onboard. See [Machine resources in vRealize Automation](#).

Procedure

- 1 Go to **Infrastructure > Onboarding**.
- 2 Click **New Onboarding Plan** and enter values.

Setting	Sample Value
Plan name	ob_rules_1
Description	Machine onboarding with rules1
Cloud account	rs-aws
Default project	rs-project

New Resource Onboarding Plan ×

Plan name *

Description

Machine onboarding with rules1

Prerequisite

Add the cloud account and create cloud zones for compute resources where onboarded machines are located.

Create a project with at least one user and give the project access to the cloud zones.

Cloud account * ⓘ

Default project * ⓘ

CANCEL

CREATE

3 Click **Create**.

The screenshot shows the 'ob_rules_1' configuration page with the 'Summary' tab selected. The page contains the following fields and values:

- Plan name:** ob_rules_1
- Description:** Machine onboarding with rules1
- Plan status:** OK
- Last run:** Never
- Source Information:**
 - Cloud account:** rs-aws
 - Deployment tag key:** (empty)
- Target configuration:**
 - Default project:** rs-project

At the bottom, there are three buttons: 'SAVE' (disabled), 'RUN', and 'CANCEL'.

4 Click the **Rules** tab and then click **Add Rule**.

You can create one or more rules to select a group of machines for onboarding based on specific machine characteristics.

The screenshot shows the 'ob_rules_1' configuration page with the 'Rules' tab selected. The page displays the text 'Use rules to add machines to this plan.' followed by three buttons: 'ADD RULE', 'EDIT', and 'DELETE'. A mouse cursor is pointing at the 'ADD RULE' button. Below the buttons is a table with one column labeled 'Name' and one row with an empty checkbox and the text 'Name'.

5 Enter a rule name, such as **ob_rules_1**.

Add Rule

Create a filter-based rule that will be used to populate machines in this plan.

Rule name

6 Build the rule by adding filters.

For this example, use the **Status** and **Name** filters on the **Filter** drop-down menu to specify all the machine whose name contains BG* and whose status is On.

Rule name ob_rules_1

Filter... ⓘ

Properties

- Any
- Name
- Status
- Address
- Tags

Rule name ob_rules_1

Name : BG* × Status: On +

7 Click **Save**.

Although you can make additional rules, this example uses a single rule.

ob_rules_1

Summary **Rules** Machines Deployments

Use rules to add machines to this plan. ⓘ

ADD RULE EDIT DELETE

<input type="checkbox"/>	Name	Status	Filters
<input type="checkbox"/>	ob_rules_1	OK	Name:BG*

8 Click the **Machines** tab. In this example, 4 machines are selected, 3 that begin with the letters BG and one that contains the letters BG.

ob_rules_1

Summary Rules **Machines** Deployments

Machines listed here will be onboarded when the plan runs.

ADD MACHINES KEEP EXCLUDE REMOVE

<input type="checkbox"/>	Name	Status	Power	Address	Deployment	Rule	Tags
<input type="checkbox"/>	BG-nsxvc550016	Will Onboard	▶ On	54.90.171.30	Deployment-d98fa100-7ed4-4c33-...	ob_rules_1	VCAC Owner:fritz@co... Description
<input type="checkbox"/>	BGsqa0001	Will Onboard	▶ On	54.157.176.191	Deployment-dbd6e201-65b5-43cc-...	ob_rules_1	VCAC Owner:Auto.ad... Description
<input type="checkbox"/>	BG-nsxvc550015	Will Onboard	▶ On	34.203.229.128	Deployment-26bc2f65-e01a-45ec-...	ob_rules_1	VCAC Owner:fritz@co... Description
<input type="checkbox"/>	AWS-BG0001	Will Onboard	▶ On	54.84.133.7	Deployment-14929eed-d228-4c3d-...	ob_rules_1	VCAC Owner:connie... Description

4 machines

- 9 Remove the machine whose name does not begin with BG by selecting its check box and then clicking **Exclude**.

ob_rules_1

Summary Rules **Machines** Deployments

Machines listed here will be onboarded when the plan runs.

ADD MACHINES KEEP **EXCLUDE** REMOVE

<input type="checkbox"/>	Name	Status	Power	Address	Deployment	Rule	Tags
<input type="checkbox"/>	BG-nsxvc550016	Will Onboard	▶ On	54.90.171.30	Deployment-d98fa100-7ed4-4c33-...	ob_rules_1	VCAC Owner:fritz@co... Description
<input type="checkbox"/>	BGsqa0001	Will Onboard	▶ On	54.157.176.191	Deployment-dbd6e201-65b5-43cc-...	ob_rules_1	VCAC Owner:Auto.ad... Description
<input type="checkbox"/>	BG-nsxvc550015	Will Onboard	▶ On	34.203.229.128	Deployment-26bc2f65-e01a-45ec-...	ob_rules_1	VCAC Owner:fritz@co... Description
<input checked="" type="checkbox"/>	AWS-BG0001	Will Onboard	▶ On	54.84.133.7	Deployment-14929eed-d228-4c3d-...	ob_rules_1	VCAC Owner:connie... Description

1 4 machines

- 10 Click the **Deployments** tab.

The 3 machines that begin with the letters BG and that are powered On are ready to be deployed. By default, a separate cloud template and deployment is created for each machine.

ob_rules_1

Summary Rules Machines **Deployments**

These deployments will be created when the plan runs. By default each added machine is placed in its own Cloud Assembly deployment.

RENAME BLUEPRINT... REMOVE

<input type="checkbox"/>	Deployment Name	Status	Create Blueprint	Components									
<input type="checkbox"/>	Deployment-26bc2f65-e01a-45ec-b6d0-0d8e7f988041	✓		1									
	<table border="1"> <thead> <tr> <th>Component Name</th> <th>Status</th> <th>Type</th> <th>Address</th> <th>Tags</th> </tr> </thead> <tbody> <tr> <td>BG-nsxvc550015</td> <td>✓</td> <td>Machine</td> <td></td> <td>VCAC Owner:fritz@coke.sqa-horizon.local Description</td> </tr> </tbody> </table>	Component Name	Status	Type	Address	Tags	BG-nsxvc550015	✓	Machine		VCAC Owner:fritz@coke.sqa-horizon.local Description		
Component Name	Status	Type	Address	Tags									
BG-nsxvc550015	✓	Machine		VCAC Owner:fritz@coke.sqa-horizon.local Description									
<input type="checkbox"/>	Deployment-d98fa100-7ed4-4c33-943a-20e10b0ccc40	✓		1									
	<table border="1"> <thead> <tr> <th>Component Name</th> <th>Status</th> <th>Type</th> <th>Address</th> <th>Tags</th> </tr> </thead> <tbody> <tr> <td>BG-nsxvc550016</td> <td>✓</td> <td>Machine</td> <td></td> <td>VCAC Owner:fritz@coke.sqa-horizon.local Description</td> </tr> </tbody> </table>	Component Name	Status	Type	Address	Tags	BG-nsxvc550016	✓	Machine		VCAC Owner:fritz@coke.sqa-horizon.local Description		
Component Name	Status	Type	Address	Tags									
BG-nsxvc550016	✓	Machine		VCAC Owner:fritz@coke.sqa-horizon.local Description									
<input type="checkbox"/>	Deployment-dbd6e201-65b5-43cc-b7d3-0ce95d606fd8	✓		1									
	<table border="1"> <thead> <tr> <th>Component Name</th> <th>Status</th> <th>Type</th> <th>Address</th> <th>Tags</th> </tr> </thead> <tbody> <tr> <td>BGsqa0001</td> <td>✓</td> <td>Machine</td> <td></td> <td>VCAC Owner:Auto.admin@sqa.local Description</td> </tr> </tbody> </table>	Component Name	Status	Type	Address	Tags	BGsqa0001	✓	Machine		VCAC Owner:Auto.admin@sqa.local Description		
Component Name	Status	Type	Address	Tags									
BGsqa0001	✓	Machine		VCAC Owner:Auto.admin@sqa.local Description									

3 deployments

SAVE RUN CANCEL

- 11 Click the check box next to the three deployment names, click **Cloud templates**, click **Create cloud template in Cloud Assembly format**, and click **Save**.

Note When your onboarding plan uses a vSphere machine, you must edit the cloud template after the onboarding process is complete. The onboarding process cannot link the source vSphere machine and its machine template, and the resultant cloud template will contain the `imageRef: "no image available"` entry in the cloud template code. The cloud template cannot be deployed until you specify the correct template name in the `imageRef:` field. To make it easier to locate and update the cloud template after the onboarding process is complete, use the **Cloud template name** option on the deployment's **Cloud template configuration** page. Record the auto-generated cloud template name or enter and record a cloud template name of your choice. When onboarding is complete, locate and open the cloud template and replace the `"no image available"` entry in the `imageRef:` field with the correct template name.

- 12 On the **Deployments** page, click the check box next to the three deployment names, and click **Run**.

ob_rules_1

Summary Rules Machines **Deployments**

These deployments will be created when the plan runs. By default each added machine is placed in its own Cloud Assembly deployment.

RENAME BLUEPRINT... REMOVE

Deployment Name	Status	Create Blueprint	Components										
Deployment-26bc2f65-e01a-45ec-b6d0-0d9e7f988041	✓	✓	1										
<table border="1"> <thead> <tr> <th>Component Name</th> <th>Status</th> <th>Type</th> <th>Address</th> <th>Tags</th> </tr> </thead> <tbody> <tr> <td>BG-nsvvc550015</td> <td>✓</td> <td>Machine</td> <td></td> <td>VCAC Owner:fritz@coke.sqa-horizon.local Description</td> </tr> </tbody> </table>				Component Name	Status	Type	Address	Tags	BG-nsvvc550015	✓	Machine		VCAC Owner:fritz@coke.sqa-horizon.local Description
Component Name	Status	Type	Address	Tags									
BG-nsvvc550015	✓	Machine		VCAC Owner:fritz@coke.sqa-horizon.local Description									
Deployment-d98fa100-7ed4-4c33-943a-20e10b0ccc40	✓	✓	1										
<table border="1"> <thead> <tr> <th>Component Name</th> <th>Status</th> <th>Type</th> <th>Address</th> <th>Tags</th> </tr> </thead> <tbody> <tr> <td>BG-nsvvc550016</td> <td>✓</td> <td>Machine</td> <td></td> <td>VCAC Owner:fritz@coke.sqa-horizon.local Description</td> </tr> </tbody> </table>				Component Name	Status	Type	Address	Tags	BG-nsvvc550016	✓	Machine		VCAC Owner:fritz@coke.sqa-horizon.local Description
Component Name	Status	Type	Address	Tags									
BG-nsvvc550016	✓	Machine		VCAC Owner:fritz@coke.sqa-horizon.local Description									
Deployment-dbd6e201-65b5-43cc-b7d3-0ce95d606fd8	✓	✓	1										
<table border="1"> <thead> <tr> <th>Component Name</th> <th>Status</th> <th>Type</th> <th>Address</th> <th>Tags</th> </tr> </thead> <tbody> <tr> <td>BGsqg0001</td> <td>✓</td> <td>Machine</td> <td></td> <td>VCAC Owner:Auto.admin@sqa.local Description</td> </tr> </tbody> </table>				Component Name	Status	Type	Address	Tags	BGsqg0001	✓	Machine		VCAC Owner:Auto.admin@sqa.local Description
Component Name	Status	Type	Address	Tags									
BGsqg0001	✓	Machine		VCAC Owner:Auto.admin@sqa.local Description									

3 3 3 deployments

SAVE RUN CANCEL

- 13 When prompted to confirm, click **Run** to onboard the machines.

Run Plan ×

Plan name	ob_rules_1
Description	Machine onboarding with rules1
Cloud account	rs-aws
Default project	rs-project
Deployments	3
Last Run	Never

CANCEL
RUN

The plan is run and the machines are brought into vRealize Automation Cloud Assembly management. A separate cloud template and deployment is created for each machine.

Advanced configuration for vRealize Automation Cloud Assembly environment

You can configure your vRealize Automation Cloud Assembly environment to further support project configuration, integration, and deployment.

For related and additional information about administration methods, such as using working with users and logs, and joining or leaving the Customer Experience program, see the [Administering vRealize Automation](#) help.

How do I configure an Internet proxy server for vRealize Automation

For vRealize Automation installations on isolated networks with no direct Internet access, you can use an Internet proxy server to allow Internet by proxy functionality. The Internet proxy server supports HTTP and HTTPS.

To configure and use public cloud providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) as well as external integration points such as IPAM, Ansible, and Puppet, with vRealize Automation, you must configure an Internet proxy server to access the internal vRealize Automation Internet proxy server.

vRealize Automation contains an internal proxy server that communicates with your Internet proxy server. This server communicates with your proxy server if it has been configured with the `vraccli proxy set ...` command. If you have not configured an Internet proxy server for your organization, then the vRealize Automation internal proxy server attempts to connect directly to the Internet.

You can set up vRealize Automation to use an Internet proxy server by using the supplied `vraccli` command line utility. Information about how to use the `vraccli` API is available by using the `--help` argument in the `vraccli` command line, for example `vraccli proxy --help`.

Access to the Internet proxy server requires use of the actions-based extensibility (ABX) On-Prem Embedded controls that are built into vRealize Automation.

Note Access to Workspace ONE Access (previously named VMware Identity Manager) is not supported by way of the Internet proxy. You cannot use the `vraccli set vidm` command to access Workspace ONE Access through the Internet proxy server.

The internal proxy server requires IPv4 as its default IP format. It doesn't require Internet protocol restrictions, authentication or man-in-the-middle actions on TLS (HTTPS) certificate traffic.

Prerequisites

- Verify that you have an existing HTTP or HTTPS server, that you can use as the Internet proxy server, in the vRealize Automation network that is able to pass outgoing traffic to external sites. The connection must be configured for IPv4.
- Verify that the target Internet proxy server is configured to support IPv4 as its default IP format and not IPv6.
- If the Internet proxy server uses TLS and requires an HTTPS connection with its clients, you must import the server certificate by using one of the following commands, prior to setting the proxy configuration.

- `vraccli certificate proxy --set path_to_proxy_certificate.pem`
- `vraccli certificate proxy --set stdin`

Use the `stdin` parameter for interactive input.

Procedure

- 1 Create a proxy configuration for the pods or containers that are used by Kubernetes. In this example, the proxy server is accessed by using the HTTP scheme.

```
vraccli proxy set --host http://proxy.vmware.com:3128
```

- 2 Show the proxy configuration.

```
vraccli proxy show
```

The result will be similar to:

```
{
  "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\n acl 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"
}
```

Note If you have configured an Internet proxy server for your organization, then "internal.proxy.config.type": "non-default" appears in the above example instead of 'default'. For security, the password is not shown.

Note If you use the `-proxy-exclude` parameter, you must edit the default values. For example, if you want to add `acme.com` as a domain that cannot be accessed by using the Internet proxy server, use the following steps:

- a Enter `vracli proxy default-no-proxy` to obtain the default proxy-exclude settings. This is a list of automatically generated domains and networks.
 - b Edit the value to add `.acme.com`.
 - c Enter `vracli proxy set --proxy-exclude ...` to update the configuration settings.
 - d Run the `/opt/scripts/deploy.sh` command to redeploy the environment.
-

- 3 (Optional) Exclude DNS domains, FQDNs, and IP addresses from being accessed by the Internet proxy server.

Always modify the default values of the `proxy-exclude` variable using parameter `--proxy-exclude`. To add the domain `exclude.vmware.com`, first use the `vrali proxy show` command, then copy the `proxy-exclude` variable, and add the domain value using the `vracli proxy set ...` command as below:

```
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"
```

Note Add elements to `proxy-exclude` instead of replacing values. If you delete `proxy-exclude` default values, vRealize Automation does not function properly. If this happens, delete the proxy configuration and start over.

- 4 After you set the Internet proxy server with `vracli proxy set ...` command, you can use the `vracli proxy apply` command to update the Internet proxy server configuration and make the latest proxy settings active.

- 5 If you have not already done so, activate the script changes by running the following command:

```
/opt/scripts/deploy.sh
```

- 6 (Optional) If needed, configure the proxy server to support external access on port 22.

To support integrations such as Puppet and Ansible, the proxy server must allow port 22 to access the relevant hosts.

Example: Sample Squid configuration

Relative to step 1, if you are setting up a Squid proxy, you can tune your configuration in `/etc/squid/squid.conf` by adapting it to the following sample:

```
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

```

What can I do with NSX-T mapping to multiple vCenters in vRealize Automation

You can associate an NSX-T cloud account to one or more vCenter cloud accounts to support various deployment objectives.

You can associate the same existing NSX-T network to network profiles for different vCenters and provision a deployment in either vCenter based on constraints. Several examples are listed below:

- Cloud templates that contain a single machine with multiple NICs that use the same network profile, where that network profile contains an NSX-T network that spans multiple vCenters.
- Cloud templates that contain a machine on a *private* network that uses a network profile with subnet-based isolation and that uses an NSX-T *existing* network that spans multiple vCenters.
- Cloud templates that contain a single machine on a *private* network that uses a network profile with security group-based isolation and that uses an NSX-T network that spans vCenters.
- Cloud templates that contain a single machine on a *routed* network that uses a network profile that contains an NSX-T network that spans multiple vCenters.
- Cloud templates that contain an on-demand load balancer that is defined in a network profile where the load balancer is applied to all the vCenter machines on the network.
- Cloud templates that contain an on-demand network that is defined in a network profile where the on-demand network is used by all the vCenters that use the network profile.
- Cloud templates that contain an on-demand security group that optionally contains firewall rules and where the security group is associated to all the vCenters on the network.

You can configure vRealize Automation internal or external IPAM on the NSX-T network and share the same IP address for machines that are provisioned in different vCenters.

If no network profile is defined in your system, you can provision a cloud template that contains multiple machines on different vCenters that share a single *existing* NSX-T network.

What happens if I remove an NSX cloud account association in vRealize Automation

If you remove an association between an NSX cloud account and a vCenter cloud account, you also need to update the related network profiles to remove the associated NSX objects.

If you remove an association between an NSX cloud account and a vCenter cloud account, the infrastructure elements are not updated automatically by vRealize Automation. You must update your existing network profiles to remove the associated NSX objects.

The user interface provides information to help highlight the impacted network profile elements as follows:

- If the network profile has an NSX existing network selected:
 - The object is marked as *invalid* and the message "*Some network objects are missing or invalid.*" is displayed.
 - The objects are removed when you save the network profile.
- If the network profile has app isolation configured, you must update the Isolation policy settings before the network profile can be saved.
- If the network profile has security groups or load balancers selected, the objects are removed when you save the network profile.

Existing deployments continue to work as designed for existing components, but will fail when creating new components, for example in a scale-out operation.

If you re-establish the association, the network profile is repopulated and existing deployments work as designed.

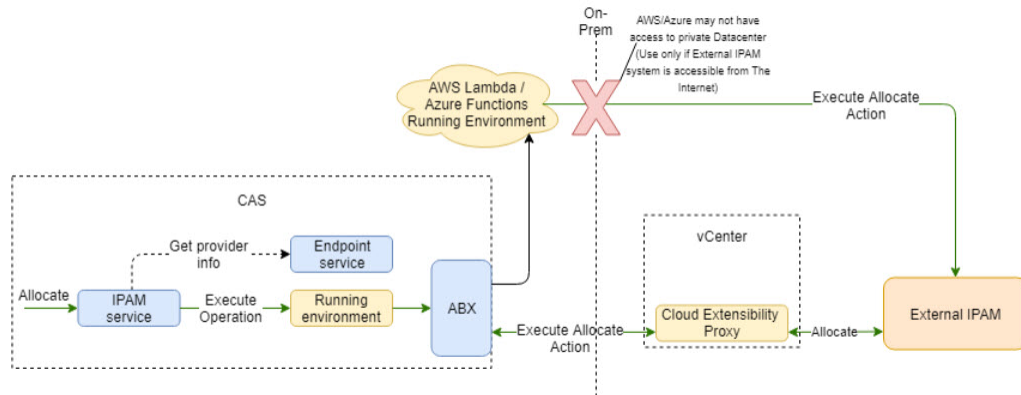
If you remove the NSX cloud account, the above behavior is the same, but network objects are marked as *missing* rather than *invalid*.

How do I use the IPAM SDK to create a provider-specific external IPAM integration package for vRealize Automation

External IPAM vendors and partners can download and use the IPAM SDK to create an IPAM integration package that enables vRealize Automation to support their provider-specific IPAM solution.

The process for building and deploying a custom IPAM integration package for vRealize Automation by using the supplied IPAM SDK is described in the [Creating and Deploying a Provider-specific IPAM Integration Package for VMware Cloud Assembly](#) document. As described in the document, you can download the most recent *VMware vRealize Automation Third-Party IPAM SDK* from the [VMware code](#) site. The following IPAM SDK packages are available:

- [VMware vRealize Automation Third-Party IPAM SDK 1.1.0](#)
- [VMware vRealize Automation Third-Party IPAM SDK 1.0.0](#)



Before taking the time to create a vendor-specific IPAM integration package by using the IPAM SDK, check to see if one already exists for vRealize Automation. You can check for a provider-specific IPAM integration package on the IPAM provider's website, in the [VMware Marketplace](#) and from the vRealize Automation **Marketplace** tab.

While the [Tutorial: Configuring a provider-specific external IPAM integration for vRealize Automation](#) example is vendor-specific, it also contains helpful reference information.

Building your vRealize Automation Cloud Assembly resource infrastructure

4

vRealize Automation Cloud Assembly resource infrastructure is where you define cloud account regions as zones into which cloud templates and their workloads can be deployed.

In addition, resource infrastructure involves creation of common mappings of images and machine sizes, and profiles that define network and storage capabilities across cloud account regions or data centers.

This chapter includes the following topics:

- [How to add cloud zones that define vRealize Automation Cloud Assembly target placement regions or data centers](#)
- [How to add flavor mappings in vRealize Automation to specify common machine sizings](#)
- [How to add image mapping in vRealize Automation to access common operating systems](#)
- [How to add network profiles in vRealize Automation](#)
- [How to add vRealize Automation Cloud Assembly storage profiles that account for different requirements](#)
- [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments](#)
- [How to work with resources in vRealize Automation](#)
- [Configuring Multi-provider tenant resources with vRealize Automation](#)

How to add cloud zones that define vRealize Automation Cloud Assembly target placement regions or data centers

A vRealize Automation Cloud Assembly cloud zone is a set of resources within a cloud account type such as AWS or vSphere.

Cloud zones in a specific account region are where your cloud templates deploy workloads. Each cloud zone is associated with a vRealize Automation Cloud Assembly project.

Select **Infrastructure > Configure > Cloud Zones** and click **Add New Zone**.

Learn more about vRealize Automation Cloud Assembly cloud zones

vRealize Automation Cloud Assembly cloud zones are sections of compute resources that are specific to your cloud account type such as AWS or vSphere.

Cloud zones are specific to a region, you must assign them to a project. There is a many to many relationship between cloud zones and projects. vRealize Automation Cloud Assembly supports deployment to the most popular public clouds including Azure, AWS and GCP as well as to vSphere. See [Adding cloud accounts to vRealize Automation Cloud Assembly](#).

Additional placement controls include placement policy options, capability tags, and compute tags.

■ Placement policy

Placement policy drives host selection for deployments within the specified cloud zone.

- default - Distributes compute resources across clusters and hosts randomly. This option works at an individual machine level. For example, all machines in a particular deployment are distributed randomly across the available clusters and hosts that satisfy the requirements.
- binpack - Places compute resources on the most loaded host that has enough available resources to run the given compute.
- spread - Provisions compute resources, at a deployment level, to the cluster or host with the least number of virtual machines. For vSphere, Distributed Resource Scheduler (DRS) distributes the virtual machines across the hosts. For example, all requested machines in a deployment are placed on the same cluster, but the next deployment may choose another vSphere cluster depending on the current load.

For example, let's assume you have the following configuration:

- DRS cluster 1 with 5 virtual machines
- DRS cluster 2 with 9 virtual machines
- DRS cluster 3 with 6 virtual machines

If you request a cluster of 3 virtual machines and you select a Spread policy, they should all be placed on cluster 1. The updated loads become 8 virtual machines for cluster 1, while the loads for clusters 2 and 3 remain the same at 9 and 6.

Then, if you request an additional 2 virtual machines, they are placed on DRS cluster 3, which will now have 8 virtual machines. The load for clusters 1 and 3 remain the same at 8 and 9.

If two cloud zones both match all the criterias needed for provisioning, then the placement logic selects the one with higher priority.

■ Capability tags

Blueprints contain constraint tags to help determine deployment placement. During deployment, blueprint constraint tags are mapped to matching capability tags in cloud zones to determine which cloud zones are available for compute resource placement.

■ Computes

You can view and manage the compute resources that are available to provision workloads, such as AWS availability zones and vCenter clusters, to this cloud zone.

If a vCenter compute cluster is DRS-enabled, the cloud zone only displays the cluster in the list of computes and it does not display the child hosts. If a vCenter compute cluster is not DRS-enabled, the cloud zone only displays standalone ESXi hosts, if present.

Add compute resources as appropriate for the cloud zone. Initially, the filter selection is Include all Compute and the list below shows all available compute resources, and they are allocated to the applicable zone. You have two additional options for adding compute resources to a cloud zone.

- Manually select compute - Select this option if you want to manually select compute resources from the list below. After you select them, click Add Compute to add the resources to the zone.
- Dynamically include compute by tags - Select this option if you want to select compute resource to be added to the zone based on tags. All compute resources are shown until you add appropriate tags. You can select or enter one or more tags in the Include compute with these tags option.

For either compute option, you can remove one or more of the compute resources shown on the page by selecting the box to the right and clicking Remove.

Compute tags help to further control placement. You can use tags to filter available compute resources to only those that match one or more tags, as shown in the following examples.

- Computes contain no tags and no filtering is used.

New Cloud Zone

Summary **Compute** Projects

All compute resources listed apply to this cloud zone. Use the filter to add or remove resources from the list.

Filter tags Enter tags to filter resources ⓘ

⌵ TAGS

<input type="checkbox"/>	Name	Account / region	Type	Tags
<input type="checkbox"/>	us-east-1a	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1b	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1c	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1d	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1e	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1f	Amazon / us-east-1	Availability Zone	

6 computes

- Two computes contain the same tag but no filtering is used.

New Cloud Zone

Summary Compute Projects

All compute resources listed apply to this cloud zone. Use the filter to add or remove resources from the list.

Filter tags ⓘ

⌵ TAGS

<input type="checkbox"/>	Name	Account / region	Type	Tags
<input type="checkbox"/>	us-east-1a	Amazon / us-east-1	Availability Zone	test.case42
<input type="checkbox"/>	us-east-1b	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1c	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1d	Amazon / us-east-1	Availability Zone	test.case42
<input type="checkbox"/>	us-east-1e	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1f	Amazon / us-east-1	Availability Zone	

6 computes

- Two computes contain the same tag and the tag filter matches the tag used on the two computes.

New Cloud Zone

Summary Compute Projects

All compute resources listed apply to this cloud zone. Use the filter to add or remove resources from the list.

Filter tags ⓘ

⌵ TAGS

<input type="checkbox"/>	Name	Account / region	Type	Tags
<input type="checkbox"/>	us-east-1a	Amazon / us-east-1	Availability Zone	test.case42
<input type="checkbox"/>	us-east-1d	Amazon / us-east-1	Availability Zone	test.case42

2 computes

Projects

You can view which projects have been configured to support workload provisioning to this cloud zone.

After you create a cloud zone, you can validate its configuration.

How to add flavor mappings in vRealize Automation to specify common machine sizings

A vRealize Automation flavor map is where you use natural language to define target deployment sizes for a specific cloud account/region.

Flavor maps express the deployment sizes that make sense for your environment. One example might be *small* for 1 CPU and 2 GB memory and *large* for 2 CPUs and 8 GB memory for a vCenter account in a named data center and t2.nano for an Amazon Web Services account in a named region.

Select **Infrastructure > Configure > Flavor Mappings** and click **New Flavor Mapping**.

Learn more about flavor mappings in vRealize Automation

A flavor mapping groups a set of target deployment sizings for a specific cloud account/region in vRealize Automation using natural language naming.

Flavor mapping lets you create a named mapping that contains similar flavor sizings across your account regions. For example, a flavor map named `standard_small` might contain a similar flavor sizing (such as 1 CPU, 2 GB RAM) for some or all available account/regions in your project. When you build a cloud template, you pick an available flavor that fits your needs.

Organize flavor mappings for your project by deployment intent.

To simplify cloud template creation, you can select a pre-configuration option when you add a new cloud account. When you select the pre-configuration option, your organization's most popular flavor mapping and image mapping for the specified region are selected.

With regard to image mapping in cloud templates that contain vSphere resources, if there are no flavor mappings defined for a vSphere cloud zone, you can configure unlimited memory and CPU by using vSphere-specific settings in the cloud template. If there are flavor mappings defined for a vSphere cloud zone, the flavor mapping serves as a limit for vSphere-specific configurations in the cloud template.

How to add image mapping in vRealize Automation to access common operating systems

A vRealize Automation image map is where you use natural language to define target deployment operating systems for a specific cloud account/region.

Select **Infrastructure > Configure > Image Mappings** and click **New Image Mapping**.

Learn more about image mappings in vRealize Automation

An image mapping groups a set of predefined target OS specifications for a specific cloud account/region in vRealize Automation by using natural language naming.

Cloud vendor accounts such as Microsoft Azure and Amazon Web Services use images to group a set of target deployment conditions together, including OS and related configuration settings. vCenter and NSX-based environments, including VMware Cloud on AWS, use a similar grouping mechanism to define a set of OS deployment conditions. When you build and eventually deploy and iterate a cloud template, you pick an available image that best fits your needs.

Organize image mappings for a project by similar operating system settings, tagging strategy, and functional deployment intent.

To simplify cloud template creation, you can select a pre-configuration option when you add a new cloud account. When you select the pre-configuration option, your organization's most popular flavor mapping and image mapping for the specified region are selected.

When you add image information to a cloud template, you use either the `image` or `imageRef` entry in the `properties` section of a machine component. For example, if you want to clone from a snapshot, use the `imageRef` property.

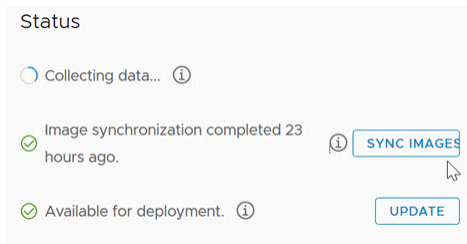
For examples of `image` and `imageRef` entries in cloud template code, see [Chapter 6 Designing your vRealize Automation Cloud Assembly deployments](#).

To assign a permission on a content library, an administrator must grant the permission to the user as a global permission. For related information, see [Hierarchical Inheritance of Permissions for Content Libraries](#) in *vSphere Virtual Machine Administration* at [VMware vSphere Documentation](#).

Synchronizing images for the cloud account/region

You can run image synchronization to ensure that the images you are adding or removing for a given cloud account/region on the **Infrastructure > Configure > Image Mapping** page are current.

- 1 Open the associated **Cloud Account/Region** by selecting **Infrastructure > Connections > Cloud accounts**. Select the existing cloud account/region.
- 2 Click the **Sync Images** button and let the action complete.



- 3 When the action is complete, click **Infrastructure > Configure > Image Mapping**. Define a new or edit an existing image mapping and select the cloud account/region from step 1.
- 4 Click the image synchronization icon on the **Image Mapping** page.



- 5 Configure image mappings settings for the specified cloud account/region on the **Image Mapping** page.

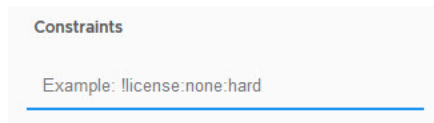
Viewing OVF details

You can include OVF specifications in vRealize Automation Cloud Assembly cloud template objects, such as vCenter machine components and image maps. If your image contains an OVF file, you can discover its content without opening the file. Hover over the OVF to display OVF details, including its name and location. For more information about the OVF file format, see [vcenter ovf: property](#).



Using constraints and tags to refine image selection

To further refine image selection in a cloud template, you can add one or more constraints to specify tag-based restrictions on the type of image that can be deployed. The supplied **Constraints** example that is displayed when you are creating or editing an image mapping configuration is `!license:none:hard`. The example illustrates a tag-based restriction where the image can only be used if the `license:none` tag is *not* present in the cloud template. If you add tags such as `license:88` and `license:92`, the specified image can be used only if the `license:88` and the `license:92` tags *are* present in the cloud template.



Using a cloud configuration script to control deployment

You can use a cloud configuration script in an image map, cloud template, or both to define custom OS characteristics to be used in a vRealize Automation Cloud Assembly deployment. For example, based on whether you are deploying a cloud template to a public or private cloud, you can apply specific user permissions, OS permissions, or other conditions to the image. A cloud configuration script adheres to a `cloud-init` format for Linux-based images or a `cloudbase-init` format for Windows-based images. vRealize Automation Cloud Assembly supports the `cloud-init` tool for Linux systems and the `cloudbase-init` tool for Windows.

For Windows machines, you can use any cloud configuration script format that is supported by `cloudbase-init`.

The machine resource in the following sample cloud template code uses an image that contains a cloud configuration script, the content of which is seen in the `image` entry.

```
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}

```

What happens when an image mapping and a cloud template contain a cloud configuration script

When a cloud template that contains a cloud configuration script uses an image mapping that contains a cloud configuration script, both scripts are combined. The merge action processes the contents of the image mapping script first and the contents of the cloud template script second, with consideration being given to whether the scripts are in `#cloud-config` format or not.

- For scripts that are in the `#cloud-config` format, the merge combines the contents of each module (for example `runcmd`, `users`, and `write_files`) as follows:
 - For modules where the contents are a list, the lists of commands from the image mapping and from the cloud template are merged, excluding commands that are identical in both lists.
 - For modules where the contents are a dictionary, the commands are merged and the result is a combination of both dictionaries. If the same key exists in both dictionaries, the key from the image mapping script dictionary is preserved and the key from the cloud template script dictionary is ignored.
 - For modules where the contents are a string, the content values from the image mapping script are kept and the content values from the cloud template script are ignored.
- For scripts that are in a format other than `#cloud-config` or when one script is in `#cloud-config` format and the other is not, both scripts are combined in a way that the image mapping script is run first and the cloud template script is run when the image mapping script is finished.

For related information, see [Merging user-data sections](#).

More information about configuring and using cloud configuration scripts

For more information about working with cloud configuration scripts, see [How to automatically initialize a machine in a vRealize Automation Cloud Assembly template](#).

Also see VMware blogger articles [vSphere Customization with Cloud-init While Using vRealize Automation 8 or Cloud](#) and [Customizing Cloud Assembly Deployments with Cloud-Init](#).

How to add network profiles in vRealize Automation

A vRealize Automation network profile describes the behavior of the network to be deployed.

For example, a network might need to be Internet-facing rather than internal-only.

Networks and network profiles are cloud-specific.

Select **Infrastructure > Configure > Network Profiles** and click **New Network Profile**.

Learn more about network profiles in vRealize Automation

A network profile defines a group of networks and network settings that are available for a cloud account in a particular region or data center in vRealize Automation.

You typically define network profiles to support a target deployment environment, for example a small test environment where an existing network has outbound access only or a large load-balanced production environment that needs a set of security policies. Think of a network profile as a collection of workload-specific network characteristics.

What's in a network profile

A network profile contains specific information for a named cloud account type and region in vRealize Automation, including the following settings:

- Named cloud account/region and optional capability tags for the network profile.
- Named existing networks and their settings.
- Network policies that define on-demand and other aspects of the network profile.
- Optional inclusion of existing load balancers.
- Optional inclusion of existing security groups.

You determine the network IP management functionality based on the network profile.

Network profile capability tags are matched with constraint tags in cloud templates to help control network selection. Further, all tags that are assigned to the networks that are collected by the network profile are also matched with tags in the cloud template to help control network selection when the cloud template is deployed.

Capability tags are optional. Capability tags are applied to all networks in the network profile, but only when the networks are used as part of that network profile. For network profiles that do not contain capability tags, tag matching occurs on the network tags only. The network and security settings that are defined in the matched network profile are applied when the cloud template is deployed.

When using static IP, the address range is managed by vRealize Automation. For DHCP, the IP start and end addresses are managed by the independent DHCP server, not by vRealize Automation. When using DHCP or mixed network address allocation, the network utilization value is set to zero. An on-demand network allocated range is based on the CIDR and subnet size that is specified in the network profile. To support both static and dynamic assignment in the deployment, the allocated range is divided into two ranges - one for static allocation and another for dynamic allocation.

Networks

Networks, also referred to as subnets, are logical subdivisions of an IP network. A network groups a cloud account, IP address or range, and network tags to control how and where to provision a cloud template deployment. Network parameters in the profile define how machines in the deployment can communicate with one another over IP layer 3. Networks can have tags.

You can add networks to the network profile, edit aspects of networks that are used by the network profile, and remove networks from the network profile.

Note For a VMware Cloud Foundation (VCF) cloud account type, you can only add NSX networks to the network profile, not vSphere networks. The NSX network segments are created locally on the NSX-T network and are not created as global networks.

■ Network domain or Transport zone

A network domain or transport zone is the distributed virtual switch (dvSwitch) for the vSphere vNetwork Distributed PortGroups (dvPortGroup). A *transport zone* is an existing NSX concept that is similar to terms like *dvSwitch* or *dvPortGroup*.

When using an NSX cloud account, the element name on the page is **Transport zone**, otherwise it is **Network domain**.

For standard switches, the network domain or transport zone is the same as the switch itself. The network domain or transport zone defines the boundaries of the subnets within vCenter.

A transport zone controls which hosts an NSX logical switch can reach to. It can span one or more vSphere clusters. Transport zones control which clusters and which virtual machines can participate in the use of a particular network. Subnets that belong to the same NSX transport zone can be used for the same machine hosts.

■ Domain

Represents the vCenter single sign-on domain for a target virtual machine. Domains are configured by a vCenter administrator during vSphere configuration. The domain determines the local authentication space in vCenter.

■ IPv4 CIDR and IPv4 default gateway

vSphere cloud accounts, and vSphere machine components in the cloud template, support dual IPv6 and IPv4 internet protocol methods. For example, 192.168.100.14/24 represents the IPv4 address 192.168.100.14 and its associated routing prefix 192.168.100.0, or equivalently, its subnet mask 255.255.255.0, which has 24 leading 1-bits. The IPv4 block 192.168.100.0/22 represents the 1024 IP addresses from 192.168.100.0 to 192.168.103.255.

■ IPv6 CIDR and IPv6 default gateway

vSphere cloud accounts, and vSphere machine components in the cloud template, support dual IPv6 and IPv4 internet protocol methods. For example, 2001:db8::/48 represents the block of IPv6 addresses from 2001:db8:0:0:0:0:0:0 to 2001:db8:0:ffff:ffff:ffff:ffff:ffff.

The IPv6 format is not supported for on-demand networks.

- **DNS servers and DNS search domains**

- **Support public IP**

Select this option to flag the network as public. Network components in a cloud template that have a `network type: public` property are matched to networks that are flagged as public. Further matching occurs during cloud template deployment to determine network selection.

- **Default for zone**

Select this option to flag the network as a default for the cloud zone. During cloud template deployment, default networks are preferred over other networks.

- **Origin**

Identifies the network source.

- **Tags**

Specifies one or more tags assigned to the network. Tags are optional. Tag matching affect which networks are available for your cloud template deployments.

Network tags exist on the network item itself, irrespective of the network profile. Network tags apply to every occurrence of the network they have been added to and to all network profiles that contain that network. Networks can be instantiated into any number of network profiles. Regardless of network profile residency, a network tag is associated with that network wherever the network is used.

When you deploy a cloud template, constraint tags in a cloud template's network components are matched to network tags, including network profile capability tags. For network profiles that contain capability tags, the capability tags are applied to all the networks that are available for that network profile. The network and security settings that are defined in the matched network profile are applied when the cloud template is deployed.

Network Policies

By using network profiles, you can define subnets for existing network domains that contain static, DHCP, or a mixture of static and DHCP IP address settings. You can define subnets and specify IP address settings by using the **Network Policies** tab.

When using NSX-V, NSX-T, or VMware Cloud on AWS, network policy settings are used when a cloud template requires the `networkType: outbound` or `networkType: private` or when an NSX network requires `networkType: routed`.

Depending on the associated cloud account, you can use network policies to define settings for the `outbound`, `private`, and `routed` network types and for on-demand security groups. You can also use network policies to control `existing` networks when there is a load balancer associated with that network.

Outbound networks allow one way access to upstream networks. Private networks do not allow any outside access. Routed networks allow East/West traffic between the routed networks. The existing and public networks in the profile are used as the underlying or upstream networks.

Options for the following on-demand selections are described in the **Network Profiles** on-screen help and summarized below.

- **Do not create an on-demand network or on-demand security group**

You can use this option when specifying an `existing` or `public` network type. cloud templates that require an `outbound`, `private`, or `routed` network are not matched to this profile.

- **Create an on-demand network**

You can use this option when specifying an `outbound`, `private`, or `routed` network type.

Amazon Web Services, Microsoft Azure, NSX, vSphere, and VMware Cloud on AWS support this option.

- **Create an on-demand security group**

You can use this option when specifying an `outbound` or `private` network type.

A new security group is created for matched cloud templates if the network type is `outbound` or `private`.

Amazon Web Services, Microsoft Azure, NSX, and VMware Cloud on AWS support this option.

Network policy settings can be cloud account type-specific. These settings are described in the on-screen signpost help and summarized below:

- **Network domain or Transport zone**

A network domain or transport zone is the distributed virtual switch (dvSwitch) for the vSphere vNetwork Distributed PortGroups (dvPortGroup). A *transport zone* is an existing NSX concept that is similar to terms like *dvSwitch* or *dvPortGroup*.

When using an NSX cloud account, the element name on the page is **Transport zone**, otherwise it is **Network domain**.

For standard switches, the network domain or transport zone is the same as the switch itself. The network domain or transport zone defines the boundaries of the subnets within vCenter.

A transport zone controls which hosts an NSX logical switch can reach to. It can span one or more vSphere clusters. Transport zones control which clusters and which virtual machines can participate in the use of a particular network. Subnets that belong to the same NSX transport zone can be used for the same machine hosts.

- **External subnet**

An on-demand network with outbound access requires an external subnet that has outbound access. The external subnet is used to provide outbound access if requested in the cloud template - it does not control network placement. For example, the external subnet does not affect the placing of a private network.

- **CIDR**

CIDR notation is a compact representation of an IP address and its associated routing prefix. The CIDR value specifies the network address range to be used during provisioning to create subnets. This CIDR setting on the **Network Policies** tab accepts IPv4 notation ending in /nn and containing values between 0 - 32.

- **Subnet size**

This option specifies the on-demand network size, using IPv4 notation, for each isolated network in a deployment that uses this network profile. The subnet size setting is available for internal or external IP address management.

The IPv6 format is not supported for on-demand networks.

- **Distributed logical router**

For an on-demand routed network, you must specify a distributed logical network when using an NSX-V cloud account.

A distributed logical router (DLR) is used to route east/west traffic between on-demand routed networks on NSX-V. This option is only visible if the account/region value for the network profile is associated to an NSX-V cloud account.

- **IP range assignment**

The option is available for cloud accounts that support NSX or VMware Cloud on AWS, including vSphere.

The IP range setting is available when using an existing network with an external IPAM integration point.

You can select one of the following three options to specify an IP range assignment type for the deployment network:

- **Static and DHCP**

Default and recommended. This mixed option uses the allocated **CIDR** and **Subnet range** settings to configure the DHCP server pool to support half of the address space allocation using the DHCP (dynamic) method and half of the IP address space allocation using the Static method. Use this option when some of the machines that are connected to an on-demand network require assigned static IP addresses and some require dynamic IP addresses. Two IP ranges are created.

This option is most effective in deployments with machines that are connected to an on-demand network, where some of the machines are assigned static IPs and other machines have IPs dynamically assigned by an NSX DHCP server and deployments where the load balancer VIP is static.

- **DHCP (dynamic)**

This option uses the allocated CIDR to configure an IP pool on a DHCP server. All the IP addresses for this network are dynamically assigned. A single IP range is created for each allocated CIDR.

- **Static**

This option uses the allocated CIDR to statically allocate IP addresses. Use this option when a DHCP server is not required to be configured for this network. A single IP range is created for each allocated CIDR.

■ **IP blocks**

The IP blocks setting is available when using an on-demand network with an external IPAM integration point.

Using the IP block setting, you can add a named IP block, or range, to the network profile from your integrated external IPAM provider. You can also remove an added IP block from the network profile. For information about how to create an external IPAM integration, see [Add an external IPAM integration for Infoblox in vRealize Automation](#).

External IPAM is available for the following cloud account/region types:

- vSphere
- vSphere with NSX-T
- vSphere with NSX-V

■ **Network Resources - External network**

External networks are also referred to as existing networks. These networks are data-collected and made available for selection.

■ **Network Resources - Tier-0 logical router**

NSX-T uses the tier-0 logical router as a gateway to networks that are external to the NSX deployment. The tier-0 logical router configures outbound access for on-demand networks.

■ **Network Resources - Edge cluster**

The specified edge cluster provides routing services. The edge cluster is used to configure outbound access for on-demand networks and load balancers. It identifies the edge cluster, or resource pool, where the edge appliance is to be deployed.

■ **Network Resources - Edge datastore**

The specified edge datastore is used to provision the edge appliance. This setting applies to NSX-V only.

Tags can be used to specify which networks are available to the cloud template.

Load Balancers

You can add load balancers to the network profile. Listed load balancers are available based on information that is data-collected from the source cloud account.

If a tag on any of the load balancers in the network profile matches a tag in a load balancer component in the cloud template, the load balancer is considered during deployment. Load balancers in a matched network profile are used when a cloud template is deployed.

For more information, see [Using load balancer settings in network profiles in vRealize Automation Cloud Assembly](#) and [Network, security, and load balancer examples in vRealize Automation cloud templates](#).

Security Groups

When a cloud template is deployed, the security groups in its network profile are applied to the machines NICs that are provisioned. For an Amazon Web Services-specific network profile, the security groups in the network profile are available in the same network domain (VPC) as the networks that are listed on the Networks tab. If the network profile has no networks listed on its Networks tab, all available security groups are displayed.

You can use a security group to further define the isolation settings for an on-demand `private` or `outbound` network. Security groups are also applied to `existing` networks.

Listed security groups are available based on information that is data-collected from the source cloud account or added as an on-demand security group in a project cloud template. For more information, see [Security resources in vRealize Automation](#).

Security groups are applied to all the machines in the deployment that are connected to the network that matches the network profile. As there might be multiple networks in a cloud template, each matching a different network profile, you can use different security groups for different networks.

Adding a tag to an existing security group allows you to use the security group in a cloud template `Cloud.SecurityGroup` component. A security group must have at least one tag or it cannot be used in a cloud template. For more information, see [Security resources in vRealize Automation](#) and [Network, security, and load balancer examples in vRealize Automation cloud templates](#).

More information about network profiles, networks, cloud templates, and tags

For more information about networks, see [Network resources in vRealize Automation](#).

For examples of sample network component code in a cloud template, see [Network, security, and load balancer examples in vRealize Automation cloud templates](#).

For sample network automation workflows, see [Network Automation with Cloud Assembly and NSX](#).

For more information about tags and tag strategy, see [How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments](#).

Using network settings in network profiles and cloud templates in vRealize Automation

You use networks and network profiles in vRealize Automation to help define the behavior of network provisioning for your deployments.

In vRealize Automation, you can define cloud-specific network profiles. See [Learn more about network profiles in vRealize Automation](#).

Using network and network profile settings, you can control how network IP addresses are used in vRealize Automation cloud templates and deployments.

IPv4 and IPv6 support in vRealize Automation networks

vRealize Automation networks support pure IPv4 or dual stack IPv4 and IPv6. Pure IPv6 is not currently supported.

While pure IPv4 is supported for all cloud account and integration types, dual stack IPv4 and IPv6 is supported only for vSphere cloud accounts and their endpoints.

IPv6 is currently not supported for use with load balancers, NSX on-demand networks, or external third-party IPAM providers.

External IPAM provider support

In addition to the supplied internal IPAM support, you can use an external IPAM provider to dynamically or statically allocate IP address for networks - as IP ranges for existing networks in your cloud template designs and deployments and IP blocks for on-demand networks in your cloud template designs and deployments.

Support for external IPAM providers, such as Infoblox, is available for vendor-specific IPAM integration points that you create by using the **Infrastructure > Connections > Add Integration > IPAM** menu sequence.

Options for defining external IPAM provider address information is available by using the **Add IPAM IP Range** option on the **Network Policies > Add IPAM IP Range** page.

For information about how to create an external IPAM integration point, see [How to configure an external IPAM integration in vRealize Automation](#) . For an example of how to create an IPAM integration point for a specific IPAM vendor, see [Tutorial: Configuring a provider-specific external IPAM integration for vRealize Automation](#) .

Network types

A network component in a cloud template is defined as one of the following `networkType` types.

Network type	Definition
<code>existing</code>	<p>Selects an existing network that is configured on the underlying cloud provider, such as vCenter, Amazon Web Services, and Microsoft Azure. An existing network is required by the <code>outbound</code> on-demand network.</p> <p>You can define a range of static IP addresses on an existing network.</p>
<code>public</code>	<p>Machines on a public network are accessible from the Internet. An IT administrator defines these networks. The definition of a <code>public</code> network is identical to that of an <code>existing</code> network for networks that allow network traffic to occur along public networks.</p>

Network type	Definition
private	<p>An on-demand network type.</p> <p>Limits network traffic to occur only between resources on the deployed network. It prevents inbound and outbound traffic. In NSX, it can be equated to on-demand NAT one-to-many.</p>
outbound	<p>An on-demand network type.</p> <p>Limits network traffic to occur between the compute resources in the deployment but also allows one-way outbound network traffic. In NSX, it can be equated to on-demand NAT one-to-many with external IP.</p>
routed	<p>An on-demand network type.</p> <p>Routed networks contain a routable IP space divided across available subnets that are linked together. The virtual machines that are provisioned with routed networks, and that have the same routed network profile, can communicate with each other and with an existing network.</p> <p>Routed networks are an on-demand network type that is available for NSX-V and NSX-T networks. Microsoft Azure and Amazon Web Services provides this connectivity by default.</p> <p>A <code>routed</code> network is only available for cloud template specification in a <code>Cloud.NSX.Network</code> network component.</p>

For examples of populated cloud templates that contain network component data, see [Network, security, and load balancer examples in vRealize Automation cloud templates](#).

Networking scenarios

You can expect the following behavior when you deploy a cloud template that uses the following network profile configuration.

Network type or scenario	No network profiles available for cloud zone	Network profiles available for cloud zone
No network	<p>If no network is specified in the cloud template, a random network is selected from the same provisioning region as the compute.</p> <p>Preference is given to networks that are labeled as default.</p> <p>If no networks exist in an available provisioning region, provisioning fails.</p>	<p>A network is selected from a matched network profile.</p> <p>Preference is given to networks that are labeled as default.</p> <p>If none of the network profiles meet the criteria, provisioning fails.</p>
Existing network	<p>If the network component in the cloud template contains constraint tags, those constraints are used to filter the list of available networks. Constraint tags in the cloud template's network component are matched to network tags and, if available, network profile constraint tags.</p> <p>From the filtered list of networks, a single network is selected from the same provisioning region as the compute.</p> <p>Preference is given to networks that are labeled as default.</p> <p>If after filtering based on constraints there are no networks in the provisioning region, provisioning fails.</p>	<p>A network is selected from a matching network profile.</p> <p>Preference is given to networks that are labeled as default.</p> <p>If none of the network profiles meet the criteria, provisioning fails.</p> <p>Network constraints can be used to filter existing networks in the profile based on their pre-assigned tags.</p>
Public network	<p>If the network has constraints, those constraints are used to filter the list of available networks that have the <code>supports public IP</code> attribute set.</p> <p>From the filtered list of networks, a random network is selected from the same provisioning region as the compute.</p> <p>Preference is given to networks that are labeled as default.</p> <p>If after filtering based on constraints there are no public networks in the provisioning region, provisioning fails.</p>	<p>A network with the <code>supports public IP</code> attribute is selected from a matching network profile.</p> <p>Preference is given to networks that are labeled as default.</p> <p>Network constraints can be used to filter existing public networks in the profile based on their pre-assigned tags.</p>
Private network	<p>Provisioning fails because private networks require information from a network profile.</p>	<p>A new network or new security group is created based on settings in the matched network profile.</p> <p>Network constraint tags can be used to filter network profiles and networks.</p>

Network type or scenario	No network profiles available for cloud zone	Network profiles available for cloud zone
Outbound network	Provisioning fails because outbound networks require information from a network profile.	A new network or new security group is created based on settings in the matched network profile. Network constraint tags can be used to filter network profiles and networks.
On-demand routed network	Provisioning fails because routed networks require information from a network profile.	For NSX-V we need DLR (Distributed Logical Router) selection. For NSX-T and VMware Cloud on AWS, we require similar on-demand settings as private and outbound.
Example Wordpress use case with existing or public networks	Provisioning occurs as described for an existing network or public network.	See above descriptions for existing network and public network behavior. See Tutorial: Setting up and testing multi-cloud infrastructure and deployments in vRealize Automation Cloud Assembly.
Example Wordpress use case with existing or public networks and private or outbound networks	Provisioning fails because the network requires information from a network profile.	See above descriptions for a private network and an outbound network. See Tutorial: Setting up and testing multi-cloud infrastructure and deployments in vRealize Automation Cloud Assembly.
Example Wordpress use case with load balancer	Provisioning fails because a load balancer requires information from a network profile. Provisioning can occur when existing load balancers are present.	A new load balancer is created based on the network profile configuration. You can specify an existing load balancer that has been enabled in the network profile. Provisioning fails if you request an existing load balancer, but none meet the constraints in the network profile. See Tutorial: Setting up and testing multi-cloud infrastructure and deployments in vRealize Automation Cloud Assembly.

Using security group settings in network profiles and cloud template designs in vRealize Automation Cloud Assembly

You can define and change security group settings in network profiles and in cloud template designs.

You can use security group capabilities in several ways:

- Existing security group specified in a network profile

You can add an existing security group to a network profile. When a cloud template design uses that network profile, its machines are grouped together as members of the security group. This method does not require that you add a security group resource to a cloud template design. You can also use a load balancer in this configuration. For related information, see [Using a load balancer resource in a vRealize Automation cloud template](#).

- Security group component associated to machine resource in a cloud template design

You can drag and drop a security group resource on to a cloud template design and bind the security group resource to a machine NIC by using constraint tags on the existing security group resource in the cloud template design and on the existing security group in the data-collected resource. You can also make this association by connecting the objects together with a connection line on the cloud template design canvas, similar to how you associate networks to machines on the design canvas.

When you drag and drop a security group resource onto the cloud template design canvas, it can be of type `existing` or `new`. If it's an `existing` security group type, you should add a tag constraint value as prompted. If it's a `new` security group type, you can configure firewall rules.

- An existing security group allocated with tag constraints and associated with a machine NIC in the cloud template

For example, you can associate a security group resource with a machine NIC (in a machine resource) in the cloud template design by matching tags between the two resources.

As an example for NSX-T when tags are specified in the source endpoint, you can use NSX-T tags specified in your NSX-T application. You can then use an NSX-T tag, specified as a constraint on a network resource in a cloud template design, where the network resource is connected to a machine NIC in the cloud template design. NSX-T tags enable you to dynamically group machines by using a pre-defined NSX-T tag that is data-collected from the NSX-T source endpoint. Use a logical port when you create the NSX-T tag in NSX-T.

- Firewall rules in an on-demand security group resource in a cloud template design

You can add firewall rules to an on-demand security group in the cloud template design.

For information about available firewall rules, see [Using a security group resource in a vRealize Automation cloud template](#).

Learn more

For information about defining security groups in network profiles, see [Learn more about network profiles in vRealize Automation](#).

For information about viewing and changing security groups settings in infrastructure resource pages, see [Security resources in vRealize Automation](#).

For information about defining security groups in cloud template designs, see [Using a security group resource in a vRealize Automation cloud template](#).

For examples of security group resources in cloud template designs, see [Network, security, and load balancer examples in vRealize Automation cloud templates](#).

Using load balancer settings in network profiles in vRealize Automation Cloud Assembly

You can configure load balancer settings in your network profile configuration.

You can add an existing load balancer to a network profile by using the **Load Balancer** tab.

You can add a load balancer to a cloud template design by associating it to a network profile that contains one or more load balancers or directly by using a load balancer resource in the cloud template design canvas or code.

Examples for including a load balancer VIP based on security group use in a network profile

There are two types of security groups that you can use in a network profile – an existing security group that you select from the **Security Groups** tab and an on-demand security group that you create by using an isolation policy on the **Network Policies** tab.

When a load balancer VIP is associated to a security group based on network profile settings, the security group configuration is supplied by the network profile.

The following table illustrates some sample scenarios.

Cloud template design topology - associated resources	Network profile configuration	Security group membership
One-armed load balancer with VIP on private network, and a machine on the same private network.	The selected network profile uses isolation policy defined as an on-demand security group.	The machine NIC and the load balancer VIP are added to the isolation security group.
One-armed load balancer with VIP on private network, and a machine on the same private network.	The selected network profile uses an existing security group and uses isolation policy defined as an on-demand security group.	The machine NIC and the load balancer VIP are added to the isolation security group and the existing security group.
Two-armed load balancer with VIP on a public network and machine on a private network.	The selected network profile uses an existing security group and uses isolation policy defined as an on-demand security group.	The machine NIC and the load balancer VIP are added to the isolation security group and the existing security group.
Two-armed load balancer with VIP on a public network and a machine on a private network.	The selected network profile uses an existing security group.	The machine NIC and the load balancer VIP are added to the existing security group.
Two-armed load balancer, VIP is on network 1 and the machine is on network 2.	Two network profiles: <ul style="list-style-type: none"> ■ Network profile 1: Uses an existing security group 1. ■ Network profile 2: Uses an existing security group 2. 	<p>The load balancer lands on network profile 1 and the machine lands on network profile 2.</p> <p>The load balancer VIP is added to security group 1 and the machine NIC is added to security group 2.</p>

Learn more

For information about adding load balancer resources to a cloud template design, see [Using a load balancer resource in a vRealize Automation cloud template](#).

For examples of cloud template designs that include load balancers, see [Network, security, and load balancer examples in vRealize Automation cloud templates](#).

How do I configure a network profile to support an on-demand network for an external IPAM integration in vRealize Automation

You can configure a network profile to support blocks of IP addresses for an on-demand network when that network profile is used in a vRealize Automation cloud template that uses external IPAM integration.

Using an existing integration for a particular external IPAM provider, you can provision on-demand network to create of a new network in the external IPAM system.

Using this process, you configure a block of IP addresses instead of supplying a parent CIDR (as is done when using vRealize Automation's internal IPAM). The IP address block is used during on-demand network provisioning to segment the new network. The IP blocks are data-collected from the external IPAM provider, provided the integration supports on-demand networking. For example, when using an Infoblox IPAM integration, IP blocks represent Infoblox network containers.

When you use an on-demand network profile and an external IPAM integration in a cloud template, the following events occur when the cloud template is deployed:

- A network is created in the external IPAM provider.
- A network is also created in vRealize Automation, reflecting the new network configuration from the IPAM provider, including settings such as CIDR and gateway properties.
- The IP address for the deployed virtual machine is fetched from the newly created network.

In this on-demand networking example, you configure a network profile to allow a cloud template deployment to provision a machine to an on-demand network in vSphere by using Infoblox as the external IPAM provider.

For related information, see [How do I configure a network profile to support an existing network for an external IPAM integration in vRealize Automation](#). Both network configuration examples fit within the overall vendor-specific workflow for external IPAM integration at [Tutorial: Configuring VMware Cloud on AWS for vRealize Automation](#).

Prerequisites

While the following prerequisites apply to the person who creates or edits the network profile, the network profile itself would be applicable when used by a cloud template deployment that contains an IPAM integration. To learn about vendor-specific IPAM integration points, see [How to configure an external IPAM integration in vRealize Automation](#).

This sequence of steps is shown in the context of an IPAM provider integration workflow. See [Tutorial: Configuring a provider-specific external IPAM integration for vRealize Automation](#).

- Verify that you have cloud administrator credentials. See [Credentials required for working with cloud accounts in vRealize Automation](#).

- Verify that you have the cloud administrator user role. See [What are the vRealize Automation user roles](#).
- Verify that you have an account with the external IPAM provider, for example [Infoblox](#) or [Bluecat](#), and that you have the correct access credentials to your organization's account with the IPAM provider. In this example workflow, the IPAM provider is Infoblox.
- Verify that you have an IPAM integration point for the IPAM provider and that the IPAM package used to create the IPAM integration supports on-demand networks. See [Add an external IPAM integration for Infoblox in vRealize Automation](#).

While the Infoblox IPAM package supports on-demand networks, if you are using an external IPAM integration for a different provider, verify that their IPAM integration package supports on-demand networks.

Procedure

- 1 To configure a network profile, click **Infrastructure > Configure > Network Profiles**.
- 2 Click **New Network Profile**.
- 3 Click the **Summary** tab and specify the following sample settings:

- Specify a vSphere cloud account/region, for example **vSphere-IPAM-OnDemandA/Datacenter**.

This example assumes use of a vSphere cloud account that is not associated with an NSX cloud account.

- Name the network profile, for example **Infoblox-OnDemandNP**.
- Add a capability tag for the network profile, for example **infoblox_ondemandA**.

Make note of the capability tag value, as you must also use it as a cloud template constraint tag to make the network profile association to be used when provisioning the cloud template.

- 4 Click the **Network Policies** tab and specify the following sample settings:

- From the **Isolation policy** drop-down menu, select **On-demand network**.

This option allows you to use external IPAM IP blocks. Depending on the cloud account, new options appear. For example, the following options appear when using a vSphere cloud account that is associated to an NSX cloud account:

- Transport zone
- Tier-0 logical router
- Edge cluster

For this example, the vSphere cloud account is not associated to NSX, so the **Network domain** menu option appears.

- Leave the **Network domain** option blank.

- 5 Click **External** as the address management **Source**.
- 6 Click **Add IP Block**, which opens the **Add IPAM IP Block** page.
- 7 From the **Provider** menu on the **Add IPAM IP Block** page, select an existing external IPAM integration. For example, select the *Infoblox_Integration* integration point from [Add an external IPAM integration for Infoblox in vRealize Automation](#) in the example workflow.
- 8 From the **Address spaces** menu, select one of the available and listed IP blocks, for example **10.23.118.0/24** and add it.

If the IPAM provider supports address spaces, the **Address spaces** menu appears. For an Infoblox integration, address spaces are represented by Infoblox network views.

- 9 Select a **Subnet size**, such as **/29 (-6 IP addresses)**.
- 10 Click **Create**.

Results

A network profile is created that can be used to provision an on-demand network using the specified external IPAM integration. The following sample cloud template shows a single machine to be deployed to a network that is defined by this new network profile.

```
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
```

Note When the cloud template is deployed, the first available network in the specified IP block is fetched and considered to be the network CIDR. If you are using an NSX network in the cloud template, you can instead set the CIDR of the network manually by using the network property `networkCidr`, as shown below, to manually set a CIDR and override the settings for IP blocks and subnet size that are specified in the associated network profile.

```
Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkCidr: 10.10.0.0/16
```

How do I configure a network profile to support an existing network for an external IPAM integration in vRealize Automation

You can configure a network profile to support IP address ranges for an existing network when that network profile is used in a vRealize Automation blueprint that uses external IPAM integration.

An example is provided within the context of a vendor-specific sample workflow at [Configure a network and network profile to use external IPAM for an existing network in vRealize Automation](#) . The overall vendor-specific workflow for external IPAM integration is at [Tutorial: Configuring VMware Cloud on AWS for vRealize Automation](#).

For related information, see [How do I configure a network profile to support an on-demand network for an external IPAM integration in vRealize Automation](#).

How to add vRealize Automation Cloud Assembly storage profiles that account for different requirements

A vRealize Automation Cloud Assembly storage profile describes the kind of storage to be deployed.

Storage is usually profiled according to characteristics such as service level or cost, performance, or purpose, such as backup.

Select **Infrastructure > Configure > Storage Profiles** and click **New Storage Profile**.

Learn more about storage profiles in vRealize Automation

A cloud account region contains storage profiles that let the cloud administrator define storage for the region in vRealize Automation.

Storage profiles include disk customizations, and a means to identify the type of storage by capability tags. Tags are then matched against provisioning service request constraints to create the desired storage at deployment time.

Storage profiles are organized under cloud-specific regions. One cloud account might have multiple regions, with multiple storage profiles under each.

Vendor-independent placement is possible. For example, visualize three different vendor accounts and a region in each. Each region includes a storage profile that is capability tagged as *fast*. At provisioning time, a request containing a hard *fast* constraint tag looks for a matching *fast* capability, regardless of which vendor cloud is supplying the resources. A match then applies the settings from the associated storage profile during creation of the deployed storage item.

Note Different cloud storage might have different performance characteristics but still be considered the *fast* offering by the administrator who tagged it.

Capability tags that you add to storage profiles should not identify actual resource targets. Instead, they describe types of storage. For more about actual resources, see [Storage resources in vRealize Automation](#).

You can create a storage profile to support either first class disk (FCD) storage or standard disk storage by using the **Disk type** option on the storage profile page or by using the vRealize Automation API. When you select the first class disk (FCD) option, you effectively create a vSphere storage profile.

- First class disk

A first class disk can be created and managed independently of a vSphere VM. An FCD has life-cycle management capabilities that also operate independently from a VM. FCD is available for use with vSphere version 6.7 Update 2 and greater and is currently implemented in vRealize Automation as an API-only feature.

For information about first class disk (FCD) storage, including the capabilities that are available by using the vRealize Automation API and links to the API documentation itself, see [What can I do with first class disk storage in vRealize Automation](#).

- Standard disk

Standard disk storage is created and managed as an integrated component of a VM.

For information about standard disk storage, see [What can I do with standard disk storage in vRealize Automation](#) and [What can I do with persistent disk storage in vRealize Automation](#).

How do I use tags to manage vRealize Automation Cloud Assembly resources and deployments

Tags are a critical component of vRealize Automation Cloud Assembly that drive the placement of deployments through matching of capabilities and constraints. You must understand and implement tags effectively to make optimal use of vRealize Automation Cloud Assembly.

Fundamentally, tags are labels that you add to vRealize Automation Cloud Assembly items. You can create any tags that are appropriate for your organization and implementation. Tags function as much more than labels though, because they control how and where vRealize Automation Cloud Assembly uses resources and infrastructure to build deployable services. Tags also support governance within Cloud Assembly.

Tag structure

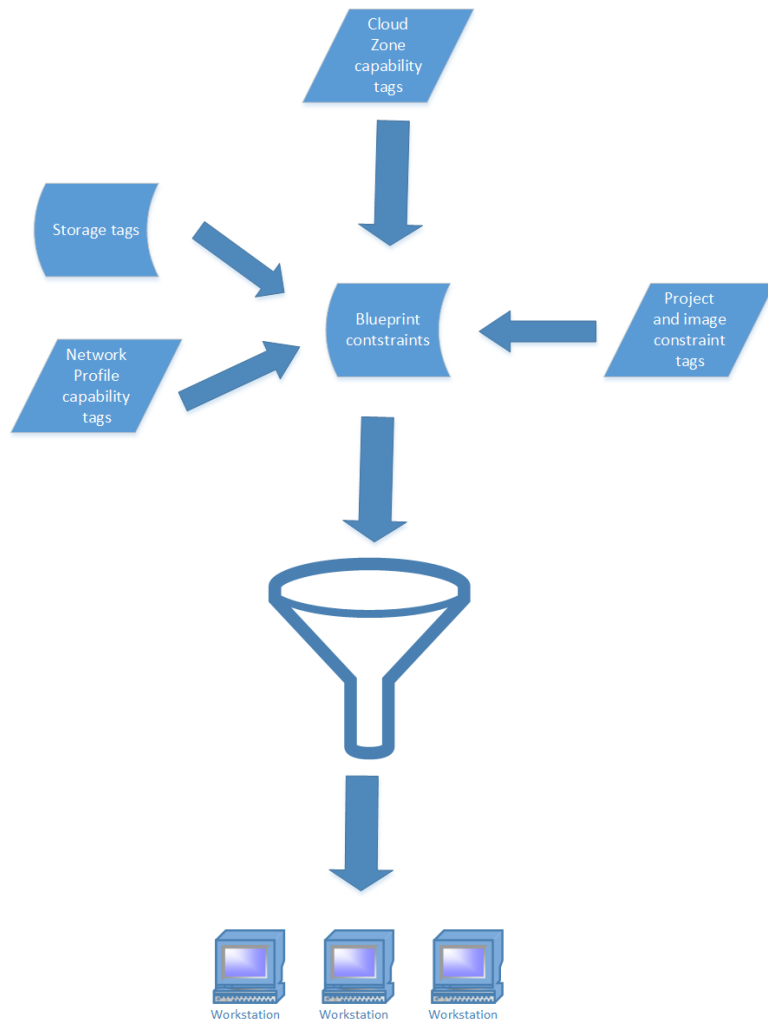
Structurally, tags must follow the `name:value` pair convention, but otherwise their construction is largely free form. Throughout vRealize Automation Cloud Assembly, all tags appear the same, and tag functionality is determined by context.

For example, tags on infrastructure resources function primarily as capability tags because vRealize Automation Cloud Assembly uses them to match resources with deployments. Secondly, they also identify the resources.

Tag function

The primary function of tags is to express capabilities and constraints that vRealize Automation Cloud Assembly uses to define deployments. Context determines the function of tags. Tags placed on cloud zones, network and storage profiles, and individual infrastructure resources function as capability tags and define desired capabilities for infrastructure used in deployments. Tags placed on cloud templates function as constraints that define resources for deployments. Also, cloud administrators can place constraint tags on projects to exercise a form of governance over those projects. These constraint tags are added to other constraints expressed in cloud templates.

During provisioning, vRealize Automation Cloud Assembly matches these capabilities with constraints, also expressed as tags, in cloud templates to define deployment configuration. This tag-based capability and constraint functionality serves as the foundation for deployment configuration in vRealize Automation Cloud Assembly. For instance, you can use tags to make infrastructure available only on PCI resources in a particular region.



On a secondary level, tags also facilitate search and identification of storage and network items and other infrastructure resources.

For example, assume that you are setting up cloud zones and you have many compute resources available. If you have tagged your compute resources appropriately, you can use the search function on the Compute tab of the Cloud Zone page to filter the resources that are associated with that particular cloud zone.

Also, the Manage Tags page and resource configuration pages contain search functions that enable you to locate items by tag names. Using logical and human readable tags for these items is key to facilitating this search and identification function.

Take a look at the following Youtube video for more information and examples of tag usage:
<https://youtu.be/4zNQ33RyQio>

External tags

vRealize Automation Cloud Assembly might also contain external tags. These tags are imported automatically from cloud accounts that you associate with a vRealize Automation Cloud Assembly instance. These tags might be imported from vSphere, AWS, Azure or other external software products. When imported, these tags are available for use in the same manner as user created tags.

Managing tags

You can use the Manage Tags page in vRealize Automation Cloud Assembly to monitor and manage your tags library. You can also create tags on this page. In addition, the Manage Tags page is the only page on which you can view and identify external tags.

The screenshot displays the 'Tag Management' page in vRealize Automation Cloud Assembly. The interface includes a sidebar with navigation options: Configure, Projects, Cloud Zones, Flavor Mappings, Image Mappings, Network Profiles, Storage Profiles, Tags, Configuration Properties, Resources, Compute, Network, Storage, Machines, Volumes, Activity, Requests, and Events. The main panel is titled 'Tag Management' and contains a table of tags. The table has two columns: 'Key' and 'Value'. The table lists various tags, including 'a', 'AAA', 'aktag1', 'alex', 'AppID', 'applicationtier', 'Application Tier', 'astoyanov-rp', 'Atos-Tagging-Category', and 'AutomaticCleanExpirationTime'. The 'AutomaticCleanExpirationTime' tag has a value of '2019-01-08T08:45:33.127Z'. The table also shows a 'Filter...' button and a '+ NEW TAG' button. The bottom right corner of the table indicates '215 tags'.

Key	Value
a	
AAA	sofiaaaa
aktag1	val1
alex	kris
AppID	ABC
AppID	XYZ
applicationtier	tango-machine
Application Tier	tango-machine
Application Tier	
astoyanov-rp	
Atos-Tagging-Category	Atos-Storage-Tag
AutomaticCleanExpirationTime	2019-01-08T08:45:33.127Z

Tag strategy

To minimize confusion, before creating tags in vRealize Automation Cloud Assembly, devise an appropriate tag strategy and tagging conventions, so that all users who create and use tags understand what they mean and how they should be used. See [Creating a tagging strategy](#).

Creating a tagging strategy

You must carefully plan and implement an appropriate tagging strategy based on your organization's IT structure and goals to maximize Cloud Assembly functionality and minimize potential confusion.

While tagging serves several common purposes, your tagging strategy must be tailored to your deployment needs, structure, and goals.

Best practices for tagging

Some general characteristics of an effective tag strategy:

- Design and implement a coherent strategy for tagging that relates to the structure of your business and communicate this plan to all applicable users. A strategy must support your deployment needs, use clear human readable language, and be understandable to all applicable users.
- Use simple, clear, and meaningful names and values for tags. For instance, tag names for storage and network items should be clear and coherent so that users can readily understand what they are selecting or reviewing tag assignments for a deployed resource.
- Though you can create tags using a name with no value, as a best practice, it is more appropriate to create an applicable value for each tag name, as this makes the tag usage clear to other users.
- Avoid creating duplicate or extraneous tags. For example, only create tags on storage items that relate to storage issues.

Tagging implementation

Map out your primary considerations for a basic tagging strategy. The following list shows typical considerations to consider when mapping your strategy. Be aware that these considerations are representative rather than definitive. You might have other considerations that are highly relevant to your use cases. Your specific strategy must be appropriate for your specific use cases.

- How many different environments do you deploy to. Typically, you will create tags that represent each environment.
- How are your compute resources structured and used to support deployments.
- How many different regions or locations do you deploy to. Typically, you will create tags, at the profile level, that represents each of these different regions or locations.
- How many different storage options are available for deployments, and how do you want to characterize them. These options should be represented by tags.
- Categorize your networking options and create tags to accommodate all applicable options.
- Typical deployment variables. For example, how many different environments do you deploy to. Typically, many organizations have Test, Dev, and Production environments at a minimum. You will want to create and coordinate constraint tags and cloud zone capability tags that match so that you can easily set up deployments to one or more of these environments.
- Coordinate tags on network and storage resources so that they make logical sense in context of the network and storage profiles in which they are used. The resource tags can serve as a finer level of control over the resource deployment.
- Coordinate cloud zone and network profile capability tags, and other capability tags, with constraint tags. In general, your administrator will create capability tags for cloud zones and network profiles first, and then other users can design s with constraints that match these capability tags.

After you understand the important considerations for your organization, you can plan appropriate tag names that address these considerations in a logical manner. Then, create an outline of your strategy and make it available to all users with privileges to create or edit tags.

As a useful implementation approach, you can begin by tagging all of your compute infrastructure resources individually. As noted, use logical categories for tag names that relate to the specific resource. For instance, you might tag storage resources as tier1, tier2, etc. Also, you might tag compute resources based on their operating system, such as Windows, Linux, etc.

After you tag resources, you can then consider the approach to creating tags for cloud zone and storage and network profiles that best suits your needs.

Using capability tags in vRealize Automation Cloud Assembly

In vRealize Automation Cloud Assembly, capability tags enable you to define deployment capabilities for infrastructure components. Along with constraints, they function as the basis of placement logic in vRealize Automation.

You can create capability tags on compute resources, cloud zones, images and image maps, and networks and network profiles. The pages for creating these resources contain options for creating capability tags. Alternatively, you can use the Tag Management page in vRealize Automation Cloud Assembly to create capability tags. Capability tags on cloud zones and network profiles affect all resources within those zones or profiles. Capability tags on storage or network components affect only the components on which they are applied.

Typically, capability tags might define characteristics such as location for a compute resource, adapter type for a network, or tier level for a storage resource. They can also define environment location or type and any other business considerations. As with your overall tagging strategy, you should organize your capability tags in a logical manner for your business needs.

vRealize Automation Cloud Assembly matches capability tags from cloud zones with constraints on cloud templates at deployment time. So, when creating and using capability tags, you must understand and plan to create appropriate cloud template constraints so that matching will occur as expected.

For example, the Add Cloud Zone section of topic in the [Tutorial: Setting up and testing multi-cloud infrastructure and deployments in vRealize Automation Cloud Assembly](#) included with the documentation describes how to create dev and test tags for the OurCo-AWS-US-East and OurCo-AWS-US-West cloud zones. In this tutorial, these tags indicate that the OurCo-AWS-US-East zone is a development environment, and the OurCo-AWS-US_West zone is a test environment. If you create analogous constraint tags in cloud templates, these capability tags enable you to direct deployments to the desired environments.

Using constraint tags in vRealize Automation Cloud Assembly

Tags added to projects and cloud templates function as constraint tags when they are used to match capability tags on infrastructure resources, profiles and cloud zones. In the case of cloud templates, vRealize Automation Cloud Assembly uses this matching functionality to allocate resources for deployments.

vRealize Automation Cloud Assembly enables you to use constraint tags in two primary ways. The first way is when configuring projects and images. You can use tags as constraints to associate resources with the project or image. The second is in cloud templates where tags specified as constraints are used to select resources for deployments. Constraints applied in both of these ways are merged in cloud templates to form a set of deployment requirements that define resources available for a deployment.

How constraint tags work on projects

When configuring vRealize Automation Cloud Assembly resources, cloud administrators can apply constraint tags on projects. In this way, administrators can apply governance constraints directly at the project level. All constraints added at this level are applied to every cloud template requested for the applicable project, and these constraint tags take precedence over other tags.

If constraint tags on the project conflict with constraint tags on the cloud template, the project tags take precedence, thus allowing the cloud administrator to enforce governance rules. For example, if the cloud administrators creates a `location:london` tag on the project, but a developer places a `location:boston` tag on the cloud template, the former will take precedence and the resource is deployed to infrastructure containing the `location:london` tag.

You can apply up to three constraints on projects. Project constraints can be hard or soft. By default they are hard. Hard constraints allow you to rigidly enforce deployment restrictions. If one or more hard constraints are not met, the deployment will fail. Soft constraints offer a way to express preferences that will be selected if available, but the deployment won't fail if soft constraints are not met.

How constraint tags work in cloud templates

In cloud templates, you add constraint tags to resources as YAML code to match the appropriate capability tags that your cloud administrator created on resources, cloud zones and storage and network profiles. In addition, there are other more complex options for implementing constraint tags. For example, you can use a variable to populate one or more tags on a request. This enables you to specify one or more of the tags at request time.

Create constraint tags by using the `tag` label under a constraint heading in the cloud template YAML code. Constraint tags from projects are added to the constraint tags created in cloud templates.

vRealize Automation Cloud Assembly supports a simple string formatting to make using constraints easier in YAML files:

```
[!]tag_key[:tag_value][:hard|:soft]
```

By default vRealize Automation Cloud Assembly creates a positive constraint with hard enforcement. The tag value is optional, though recommended, as in the rest of the application.

The following WordPress with MySQL example shows YAML constraint tags that specific location information for compute resources.

```
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 ...
```

For more information about how to work with cloud templates, see [Part 3: Design and deploy the example vRealize Automation Cloud Assembly template](#).

How hard and soft constraints work in projects and cloud templates

Constraints in both projects and cloud templates can be hard or soft. The preceding code snippet shows examples of hard and soft constraints. By default all constraints are hard. Hard constraints allow you to rigidly enforce deployment restrictions. If one or more hard constraints are not met, the deployment will fail. Soft constraints express preferences that apply if available, but they won't cause a deployment to fail if not met.

If you have a series of hard and soft constraints on a specific resource type, the soft constraints can also serve as tie breakers. That is, if multiple resources meet a hard constraint, the soft constraints are used to select the actual resource used in the deployment.

For example you can specify up to three constraints on a project in any combination of network, storage and extensibility items. Also, you can select whether each constraint is hard or soft. Let's say that you create a hard storage constraint with a tag of `location:boston`. If no storage in the project matches this constraint, any related deployment will fail.

Standard tags

vRealize Automation Cloud Assembly applies standard tags to some deployments to support analysis, monitoring, and grouping of deployed resources.

Standard tags are unique within vRealize Automation Cloud Assembly. Unlike other tags, users do not work with them during deployment configuration, and no constraints are applied. These tags are applied automatically during provisioning on AWS, Azure, and vSphere deployments. These tags are stored as system custom properties, and they are added to deployments after provisioning.

The list of standard tags appears below.

Table 4-1. Standard tags

Description	Tag
Organization	org:orgID
Project	project:projectID
Requester	requester:username
Deployment	deployment:deploymentID
Cloud template reference (if applicable)	blueprint:blueprintID
Component name in blueprint	blueprintResourceName:CloudMachine_1
Placement Constraints: applied in blueprint, request parameters, or via IT policy	constraints:key:value:soft
Cloud Account	cloudAccount:accountID
Zone or profile, if applicable	zone:zoneID, networkProfile:profileID, storageProfile:profileID

How vRealize Automation Cloud Assembly processes tags

In vRealize Automation Cloud Assembly, tags express capabilities and constraints that determine how and where resources are allocated to provisioned deployments during the provisioning process.

vRealize Automation Cloud Assembly uses a specific order and hierarchy of operations in resolving tags to create provisioned deployments. Understanding the basics of this process will help you to implement tags efficiently to create predictable deployments.

The following list summarizes the high level operations and sequence that Cloud Assembly uses to resolve tags and define a deployment:

- Cloud zones are filtered by several criteria, including availability and profiles; tags in profiles for the region the zone belongs to are matched at this point.
- Zone and compute capability tags are used to filter the remaining cloud zones by hard constraints.
- Out of the filtered zones, priority is used to select a cloud zone. If there are several cloud zones with the same priority, they are sorted by matching soft constraints, using a combination of the cloud zone and compute capabilities.

- After a cloud zone is selected, a host is selected by matching a series of filters, including hard & soft constraints as expressed in cloud templates.

How do I set up a simple tagging structure

This topic describes a basic approach and options for a logical vRealize Automation Cloud Assembly tagging strategy. You can use these examples as a starting point for an actual deployment, or you can devise a different strategy that better suits your needs.

Typically, the cloud administrator is the primary individual responsible for creating and maintaining tags.

This topic refers to the WordPress use case described elsewhere in the vRealize Automation Cloud Assembly documentation to illustrate how tags can be added to some key items. It also describes possible alternatives and extensions to the tagging examples that appear in the WordPress use case.

See [Tutorial: Setting up and testing multi-cloud infrastructure and deployments in vRealize Automation Cloud Assembly](#) for more information about the WordPress use case.

The WordPress use case describes how to place tags on cloud zones and storage and network profiles. These profiles are like organized packages of resources. Tags placed on profiles apply to all items within the profile. You can also create and place tags on storage resources and individual network items as well as on compute resources, but these tags apply only to the specific resources on which they are placed. When setting up tags, it is usually best to begin by tagging compute resources, and then you can add tags to profiles and cloud zones later. Also, you use these tags to filter the list of compute resources for a cloud zone.

For example, while you can place tags on storage profiles as shown in this use case, you can also place tags on individual storage policies, data stores, and storage accounts. Tags on these resources enable you to exercise finer control over how storage resources are deployed. During processing in preparation for deployment, these tags are resolved as a next level of processing after the profile tags.

As an example of how you might configure a typical customer scenario, you could place a tag of `region: eastern` on a network profile. This tag would apply to all resources within that profile. Then you could place a tag of `networktype:pci` on a pci network resource within the profile. A cloud template with constraints of eastern and pci would create deployments that use this pci network for the eastern region.

Procedure

1 Tag your compute infrastructure resources in a logical and appropriate manner.

It is particularly important that you tag compute resources in a logical manner so that you can find them using the search function on the Compute tab of the Create Cloud Zone page. Using this search function, you can quickly filter the compute resources associated with a cloud zone. If you tag Storage and Networks at the profile level, you may not need to tag individual storage and network resources.

- a Select **Resources > Compute** to view the compute resources that have been imported for your vRealize Automation Cloud Assembly instance.
- b Select each compute resource as appropriate and click **Tags** to add a tag to the resource. You can add more than one tag to each resource if appropriate.
- c Repeat the previous step for storage and network resources as appropriate.

2 Create cloud zone and network profile capability tags.

You can use the same tags for both cloud zones and network profiles, or you can create unique tags for each item if that makes more sense for your implementation.

In network profiles, you can place tags on the entire profile as well as on subnets within the profile. Tags applied at the profile level apply to all components, such as subnets, within that profile. Tags on subnets apply only to the specific subnet on which they are placed. During tag processing, the profile level tags take precedence over the subnet level tags.

In this example we create three simple tags that appear throughout the use case documentation for vRealize Automation Cloud Assembly cloud zone and network profile tags. These tags identify the environment for the profile components.

- `zone:test`
- `zone:dev`
- `zone:prod`

3 Create storage profile tags for your storage components.

Typically, storage tags identify the performance level of storage items, such as tier1 or tier2, or they identify the nature of storage items, such as pci.

See [6. Add storage profiles](#) for information about adding tags to storage profiles.

- `usage:general`
- `usage:fast`

Results

After you create a basic tagging structure, you can begin working with it and add or edit tags as appropriate to refine and extend your tagging capabilities.

How to work with resources in vRealize Automation

A cloud administrator can review vRealize Automation resources that are exposed through data collection.

The cloud administrator can label resources with capability tags to affect where vRealize Automation cloud templates are deployed.

Compute resources in vRealize Automation

A cloud administrator can review compute resources that are exposed through data collection.

The cloud administrator might choose to apply tags directly to the resources to label capabilities for matching purposes in vRealize Automation provisioning.

Network resources in vRealize Automation

In vRealize Automation, cloud administrators can view and edit the network resources that have been data-collected from the cloud accounts and integrations that are mapped to your project.

After you add a cloud account to your vRealize Automation Cloud Assembly infrastructure, for example by using the **Infrastructure > Connections > Cloud Accounts** menu sequence, data collection discovers the cloud account's network and security information. That information is then available for to use in networks, network profiles, and other definitions.

Networks are the IP-specific components of an available network domain or transport zone. If you're an Amazon Web Services or Microsoft Azure user, think of networks as subnets.

You can display information about the networks in your project by using the **Infrastructure > Resources > Networks** page.

The vRealize Automation Cloud Assembly **Networks** page contains information such as:

- Networks and load balancers that are defined externally in the network domain of your cloud account, for example in vCenter, NSX-V, or Amazon Web Services.
- Networks and load balancers that have been deployed by the cloud administrator.
- IP ranges and other network characteristics that have been defined or modified by your cloud administrator.
- External IPAM provider IP ranges for a particular address space in an provider-specific external IPAM integration.

For more information about networks, see the following information, signpost help for various settings on the **Networks** page, and [Learn more about network profiles in vRealize Automation](#).

Networks

You can view and edit networks and their characteristics, for example to add tags or remove support for public IP access. You can also manage network settings such as DNS, CIDR, gateway, and tag values. You can also define new, and manage existing, IP ranges within a network.

For existing networks you can change the IP range and tag settings by selecting the network's checkbox and selecting either **Manage IP Ranges** or **Tags**. Otherwise you can select the network itself to edit its information.

Tags provide a means for matching appropriate networks, and optionally network profiles, to network components in cloud templates. Network tags are applied to every instance of that network, regardless of any network profiles in which the network may reside. Networks can be instanced into any number of network profiles. Regardless of network profile residency, a network tag is associated with that network wherever the network is used. Network tag matching occurs with other components in the cloud template after the cloud template has been matched with one or more network profiles.

IP Ranges

Use an IP range to define or make changes to the start and end IP address for a particular network in your organization. You can display and manage IP ranges for listed networks. If the network is managed by an external IPAM provider, you can manage IP ranges in connection with the associated IPAM integration point.

Click **New IP Range** to add an additional IP range to the network. You can specify an **internal IP range**, or if there is a valid IPAM integration available you can specify an **External IP range**.

You cannot include the default gateway in an IP range. The subnet IP range cannot include the subnet gateway value.

If you are using an external IPAM integration for a particular IPAM provider, you can use the **External IP range** to select an IP range from an available external IPAM integration point. This process is described within the context of an overall external IPAM integration workflow at [Configure a network and network profile to use external IPAM for an existing network in vRealize Automation](#).

IP Addresses

You can see the IP addresses that are currently used by your organization and display their status, for example `available` or `allocated`. The IP addresses that are displayed are either IP addresses that are managed internally by vRealize Automation or IP addresses that are designated for deployments that contain an external IPAM provider integration. External IPAM providers manage their own IP address allocation.

If the network is managed internally by vRealize Automation, and not by an external IPAM provider, you can also release IP addresses.

When using internal IPAM and releasing IP addresses, for example after deleting a machine that had been using the IP addresses, there is a 30 minute wait period between when the addresses are released and when you can reuse them. The wait period allows for the DNS cache to clear. The IP addresses can then be allocated to a new machine. For example, you can then provision a machine with the same IP addresses as the previously deleted machine.

Load Balancers

You can manage information about available load balancers for the account/region cloud accounts in your organization. You can open and display the configured settings for each available load balancer. You can also add and remove tags for a load balancer.

Network Domains

The network domains list contains related and non-overlapping networks.

Security resources in vRealize Automation

After you add a cloud account in vRealize Automation Cloud Assembly, data collection discovers the cloud account's network and security information and makes that information available for use in network profiles and other options.

Security groups and firewall rules support network isolation. Security groups are data-collected. Firewall rules are not data-collected.

Security groups

Using the **Infrastructure > Resources > Security** menu sequence, you can view on-demand security groups that have been created in vRealize Automation Cloud Assembly cloud template designs and existing security groups that were created in source applications, such as NSX-T and Amazon Web Services. Available security groups are exposed by the data collection process.

You can view the available security groups and add or remove tags for selected security groups. A cloud template author can assign one or more security groups to a machine NIC to control security for the deployment.

In the cloud template design the `securityGroupType` parameter in the security group resource is specified as `existing` for an existing security group or `new` for an on-demand security group.

Existing security groups from the underlying cloud account endpoint, such as NSX-V, NSX-T, or Amazon Web Services applications, are available for use. On-demand security groups that were created in your organization's cloud template designs are also data-collected. On-demand security groups are currently available for NSX-V and NSX-T only.

Existing security groups are displayed and classified in the **Origin** column as `Discovered`. On-demand security groups that you create in vRealize Automation Cloud Assembly, either in a cloud template or in a network profile, are displayed and classified in the **Origin** column as `Managed by Cloud Assembly`. On-demand security groups that you create as part of a network profile are internally classified as an isolation security group with pre-configured firewall rules and are not added to a cloud template design as a security group resource. On-demand security groups that you create in a cloud template design, and that can contain express firewall rules, are added as part of a security group resource that is classified as `new`.

If you edit an existing security group directly in the source application, such as in the source NSX application rather than in vRealize Automation Cloud Assembly, the updates are not visible in vRealize Automation Cloud Assembly until you data collection runs and data collects the associated cloud account or integration point from within vRealize Automation Cloud Assembly. Data collection runs automatically every 10 minutes.

A cloud administrator can assign one or more tags to an existing security group to allow it to be used in a cloud template. A cloud template author can use a `Cloud.SecurityGroup` resource in a cloud template design to allocate an existing security group by using tag constraints. An existing security group requires at least one constraint tag be specified in the security resource in the cloud template design.

Using firewall rules in security groups

You can create firewall rules for on-demand security groups for NSX-V and NSX-T directly in a security group resource in cloud template design code.

The **Applied To** column does not contain security groups that are classified or managed by an NSX Distributed Firewall (DFW). Firewall rules that apply to applications are for east/west DFW traffic.

Some firewall rules can only be managed in the source application and cannot be edited in vRealize Automation Cloud Assembly. For example, ethernet, emergency, infrastructure, and environment rules are managed in NSX-T.

Learn more

For more information about using security groups in network profiles, see [Learn more about network profiles in vRealize Automation](#).

For information about defining firewall rules, see [Using security group settings in network profiles and cloud template designs in vRealize Automation Cloud Assembly](#) and [Using a security group resource in a vRealize Automation cloud template](#).

For cloud template design code samples that contain security groups, see [Network, security, and load balancer examples in vRealize Automation cloud templates](#).

Storage resources in vRealize Automation

A cloud administrator can work with storage resources and their capabilities, which are discovered through vRealize Automation data collection from associated cloud accounts.

Storage resource capabilities are exposed through tags that typically originate at the source cloud account. A cloud administrator can choose to apply additional tags directly to storage resources though, using vRealize Automation Cloud Assembly. The additional tags might label a specific capability for matching purposes at provisioning time.

vRealize Automation supports standard disk and first class disk capabilities. First class disk is available for vSphere only.

- [What can I do with standard disk storage in vRealize Automation](#)

■ [What can I do with first class disk storage in vRealize Automation](#)

Capabilities on storage resources become visible as part of the definition of a vRealize Automation Cloud Assembly storage profile. See [Learn more about storage profiles in vRealize Automation](#).

First class disks that have been data-collected appear on the **Volumes** resource page. See [Volume resources in vRealize Automation](#).

Machine resources in vRealize Automation

In vRealize Automation, all users can review machine resources that are exposed through data collection.

All the machines in your projects are listed. You can list only your machines or specify filters to control the display of listed machines.

Unmanaged machines that are associated to cloud accounts in your projects appear in this list, as do managed machines. The Origin column indicates the machine status.

- Discovered - machines that have not yet been onboarded.
- Deployed - machines that have been onboarded or provisioned from vRealize Automation and are considered to be managed machines.

You can use a workload onboarding plan to bring unmanaged machines into vRealize Automation management.

Disconnected machine NICs are not listed because vRealize Automation requires the presence of the network switch or subnet information to enumerate the ethernet card. For example, if you have removed a machine NIC from a deployment, the NIC is not listed.

For information about using onboarding plans to bring unmanaged machines into vRealize Automation management, see [What are onboarding plans in vRealize Automation Cloud Assembly](#).

Volume resources in vRealize Automation

In vRealize Automation, all users can review volume resources.

vRealize Automation Cloud Assembly displays volumes or logical drives that originate from two sources:

- Volumes discovered through data collection of source cloud accounts
- Volumes associated with workloads provisioned by vRealize Automation Cloud Assembly

You can review capacity and capabilities according to volume or logical drive. The list also exposes capability tags that originated at the source cloud account or were added in vRealize Automation Cloud Assembly itself. The volume's status as a first class disk is also noted. For information about first class disk storage volumes, see [What can I do with first class disk storage in vRealize Automation](#).

Learn more about resources in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly can expose additional information around data-collected resources, such as pricing cards.

How does data collection work in vRealize Automation

After initial data collection, resource data collection occurs automatically every 10 minutes. The data collection interval is not configurable and you cannot manually initiate data collection.

You can discover information about resource data collection and image synchronization for an existing cloud account in the Status section of its page. Do so by selecting **Infrastructure > Connections > Cloud Accounts** and then clicking **Open** on the existing cloud account of your choice.

You can open an existing cloud account and see its associated endpoint version in the **Status** section of its page. If the associated endpoint has been upgraded, the new endpoint version is discovered during data collection and reflected in the **Status** section on the cloud account's page.

Resource data collection

Data collection occurs every 10 minutes. Each cloud account displays when its data collection last completed.

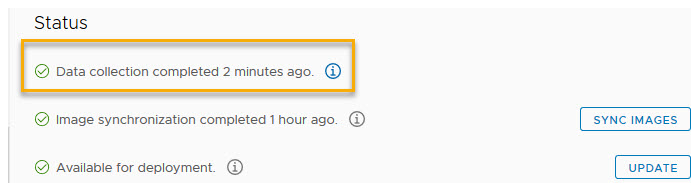
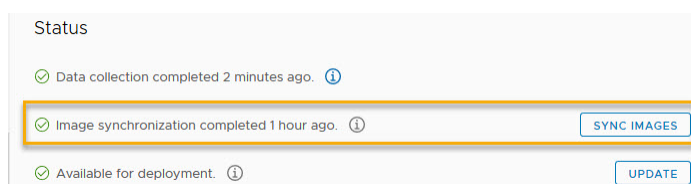


Image data collection

Image synchronization occurs every 24 hours. You can initiate image synchronization for some cloud account types. To initiate image synchronization, open the cloud account (**Infrastructure > Cloud Accounts** then select and open the existing cloud account) and click the **Sync Images** button. There is no image synchronization option for NSX cloud accounts.

Note Images are internally classified as either public or private. Public images are shared and are not specific to a particular cloud subscription or organization. Private images are not shared and are specific to a specific subscription. Public and private images are automatically synchronized every 24 hours. An option on the cloud account page allows you to trigger synchronization for private images.

The cloud account page displays when image synchronization was last completed.



To facilitate fault tolerance and high availability in deployments, each NSX-T data center endpoint represents a cluster of three NSX managers. For related information, see [Create an NSX-T cloud account in vRealize Automation](#).

Cloud accounts and onboarding plans

When you create a cloud account, all machines that are associated to it are data-collected and then displayed on the **Infrastructure > Resources > Machines** page. If the cloud account has machines that were deployed outside of vRealize Automation Cloud Assembly, you can use an onboarding plan to allow vRealize Automation Cloud Assembly to manage the machine deployments.

For information about adding cloud accounts, see [Adding cloud accounts to vRealize Automation Cloud Assembly](#).

For information about onboarding unmanaged machines, see [What are onboarding plans in vRealize Automation Cloud Assembly](#).

What can I do with standard disk storage in vRealize Automation

Standard disks can be persistent or non-persistent.

vRealize Automation supports two categories of storage – standard disk and first class disk. First class disk is only available for vSphere.

■ vSphere

vSphere supports dependent (default), independent persistent, and independent non-persistent standard disks. For related information, see [What can I do with persistent disk storage in vRealize Automation](#).

When you delete a virtual machine, its dependent and independent non-persistent disks are also deleted.

When you delete a virtual machine, its independent persistent disks are not deleted.

You can create a snapshot of dependent and independent non-persistent disks. You cannot create a snapshot of an independent persistent disk.

■ Amazon Web Services (AWS) EBS

You can attach an EBS volume to an AWS compute instance or detach an EBS volume from an AWS compute instance.

When you delete a virtual machine, its attached EBS volume is detached but not deleted.

■ Microsoft Azure VHD

Attached disks are always persistent.

When you delete a virtual machine, you specify whether to remove its attached storage disks.

■ Google Cloud Platform (GCP)

Attached disks are always persistent.

Persistent disks are located independently from your virtual machine instances, so you can detach or move persistent disks to keep your data even after you delete your instances.

When you delete a virtual machine, its attached disk is detached but not deleted.

For related information, see [Learn more about storage profiles in vRealize Automation](#).

What can I do with first class disk storage in vRealize Automation

A first class disk (FCD) provides storage life-cycle management on virtual disks as a disk-as-a service or as EBS-like disk storage that allows you to create and manage disks independently of vSphere virtual machines.

vRealize Automation supports two categories of storage disks – standard disk and first class disk. First class disk functionality is supported for vSphere only. vRealize Automation currently provides first class disk functionality as an API-only capability.

A first class disk has its own life-cycle management capabilities that operate independently from a VM. One way that a first class disk differs from an independent persistent disk, is that you can use a first class disk to create and manage snapshots independent of a VM.

You can create a new vRealize Automation storage profile to support either first class disk capabilities or standard disk capabilities. See [Learn more about storage profiles in vRealize Automation](#) and [Storage resources in vRealize Automation](#).

You can also add a `Cloud.vSphere.Disk` first class disk element in your vRealize Automation cloud templates and deployments to support vSphere first class disks. First class disks that have been data-collected appear on the **Volumes** resource page. See [Volume resources in vRealize Automation](#).

In vCenter, first class disks are also referred to as *Improved Virtual Disks (IVD)* or *managed virtual disks*.

Capabilities

Using vRealize Automation API capabilities, you can:

- Create, list, and delete a first class disk.
- Resize a first class disk.
- Attach and detach a first class disk.
- Create and manage first class disk snapshots.
- Convert an existing standard disk to first class disk

Related API information about creating and managing first class disk (FCD) storage by using the vRealize Automation API, including how to define a storage profile to use first class disk capabilities, is available at code.vmware.com at [What are the vRealize Automation Cloud APIs and how do I use them](#) or by navigating from the following locations:

- API documentation for FCD is available in the [First Class Disk \(FCD\)](#) section of the [Virtual Disk Development Kit Programming Guide](#).

- Links to API use case documentation for FCD in vRealize Automation are available on the [vRealize Automation API Documentation page](#) for your vRealize Automation release.

Considerations and limitations

First class disk considerations and limitations currently include:

- First class disk is available for vSphere VMs only.
- vSphere 6.7 Update 2 or later is required to use first class disks.
- Provisioning first class disks on datastore clusters is not supported.
- Volume multi-attach is not supported for first class disks.
- First class disks with snapshots cannot be resized.
- First class disks with snapshots cannot be deleted.
- First class disk snapshot hierarchy can only be constructed by using the `createdAt` API option.
- The minimum VM hardware version required to attach a first class disk is vmx-13 (ESX 6.5 compatible).

What can I do with persistent disk storage in vRealize Automation

Persistent disks preserve valuable data from accidental deletion.

In a cloud template, under a volume, you can add the `persistent: true` property to have the disk survive vRealize Automation Cloud Assembly or vRealize Automation Service Broker deletions. Persistent disks aren't removed during deployment deletion nor Day 2 delete or remove disk operations.

Because of that, persistent disks can remain in your infrastructure even after a deployment deletion or disk deletion. To remove them, you can use the following techniques.

- Explicitly pass the purge flag as a query parameter using the DELETE API.
- Delete them directly from your cloud endpoint.

Note that there is no vRealize Automation Cloud Assembly or vRealize Automation Service Broker user interface for removing them.

What are Pricing Cards

vRealize Automation Cloud Assembly pricing cards help cloud administrators define and assign the pricing policy for the monetary impact of your individual deployments to help you manage resources.

Before you can create or assign pricing cards, you must configure and enable pricing in vRealize Operations Manager to work with vRealize Automation . When configuring vRealize Operations Manager with vRealize Automation , ensure that both applications are set to the same timezone. To configure the timezone in vRealize Operations, enable SSH and log in to each vRealize Operations Manager node, edit the `$ALIVE_Base/user/conf/analytics/advanced.properties` file, and add `timeZoneUseInMeteringCalculation = <time zone>`.

Note For pricing to work on multi-tenant environments, you must have a separate vRealize Operations Manager instance for each vRealize Automation tenant.

Pricing cards define the rates for a pricing policy. The pricing policy can then be assigned to specific projects to define a total price. After creating a vRealize Operations Manager endpoint, a predefined Default Rate Card is available with a cost equal to price configuration on the **Infrastructure > Pricing Cards** tab. You can create pricing cards that apply to projects only or cloud zones. By default, all new pricing cards are applied to projects.

Note If you change the **All pricing cards are applied to** setting, all existing pricing card assignments are deleted. Also, if the vRealize Operations Manager endpoint is deleted from Cloud Assembly, all pricing cards and assignments are also deleted.

The price of a deployment over time appears on the deployment card as the month-to-date price, which resets to zero at the beginning of each month. The component cost breakdowns are available in the deployment details. Providing this information at the deployment level informs the cloud administrator, but it also helps the members understand the impact their work might have on budgets and long-term development.

You can choose to display pricing information from users in Cloud Assembly and Service Broker by selecting the Display pricing information button. If left disabled, the pricing information is hidden from Cloud Assembly and Service Broker users.

How is price calculated

The initial price that you see at the deployment level for your compute and storage resources are based on industry standard benchmark rates, and then calculated over time. The rate is applied to hosts and the service calculates the CPU and memory rates. The server recalculates the price every 24-hours.

New policies, assignments, and upfront pricing are priced during the next occurring vROPs data collection cycle. By default, the data collection cycle is run every 5 minutes. It can take up to 24-hours for new policies or changes to be updated in projects and deployments.

You can also manually refresh the price server at any time on the vROPs Endpoint page, **Infrastructure > Integrations > vROPs Endpoint >** . In the vCenter servers section, click **Sync**. When manually refreshing the price server using the **Sync** option, the price is recalculated for all projects in the organization. Depending on how many projects your organization has this process might be intensive and take time.

For a list of supported resources, see [List of costed component types in vRealize Automation Cloud Assembly](#).

List of costed component types in vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly provides benchmark cost information for the following blueprint component types.

Table 4-2. Costed Component Types

Blueprint Component Type	Service Name/Object Type	Blueprint Resource Type	Comments
Cloud Agnostic	Machine	Cloud.Machine	If an agnostic machine is configured with vSphere, you can view deployment cost.
	Disk	Cloud.Volume	If an agnostic disk is attached to a virtual machine that is configured with vSphere, you can view deployment cost.
vSphere	vSphere machine	Cloud.vSphere.Machine	Deployed using a cloud-specific blueprint.
	vSphere disk	Cloud.vSphere.Disk	Deployed using a cloud-specific blueprint attached to a virtual machine.
VMware Managed Cloud (VMC)	vSphere machine	Cloud.vSphere.Machine	VMC only supports rate-based pricing cards (cost based pricing cards are not supported).
	vSphere disk	Cloud.vSphere.Disk	

How to create a pricing card in Cloud Assembly

You can create and assign a pricing card to projects or cloud zones, depending on the pricing strategy determined by the cloud administrator.

Pricing cards are customizable based on user-selected parameters. After configuring a pricing card, you can assign it to one or more projects and cloud zones determined by the pricing strategy.

Prerequisites

Before you can create or assign pricing cards, you must configure and enable pricing and configure currency in vRealize Operations to work with vRealize Automation . When configuring vRealize Operations with vRealize Automation , ensure that both applications are set to the same timezone. To configure the timezone in vRealize Operations, enable SSH and log in to each vRealize Operations node, edit the `$ALIVE_Base/user/conf/analytics/advanced.properties` file, and add `timeZoneUseInMeteringCalculation = <time zone>`.

You must configure a vRealize Operations endpoint before you can configure pricing cards. To configure the vRealize Operations endpoint navigate to **Infrastructure > Connections > Integrations > Add Integration**.

Note When multiple vRealize Operations endpoints are added they must not monitor the same vCenter.

Procedure

- 1 Navigate to **Infrastructure > Pricing Cards > New Pricing Card**.
- 2 On the Summary tab, enter a name and description for the pricing card. Once the policy is defined on the pricing tab, the Overview table is populated with pricing card rates.

Note The currency unit is determined by the valued selected in vRealize Operations.

- 3 Optional. Select the **Default for unassigned projects?** check box to assign this pricing card to all unassigned projects by default.

4 Click **Pricing**, and configure the details of your pricing policy.

Table 4-3. Pricing Policy Configuration

Parameter	Description
Basic Charges	<p>Enter a name and description for your policy. Select cost or rate based.</p> <ul style="list-style-type: none"> ■ Cost - The cost is defined in vRealize Operations. If selected, a multiplication factor is required. For example, if you select 1.1 as a factor, the cost is multiplied by 1.1 resulting in a 10% increase to the calculated cost. The price equation using cost is: $\text{<cost>} \times \text{<multiplication factor>} = \text{Price}$ ■ Rate - If selected, you must use absolute values to determine the cost. The price equation using rate is: $\text{<Rate>} = \text{Price}$. Select a rate interval from the drop down list to specify how this rate is charged. <p>In the basic charges section, you define the cost or rate for CPU, memory, storage, and additional miscellaneous costs.</p>
Guest OSes	<p>You can define a Guest OS charge by clicking Add Charge.</p> <p>Enter the guest OS name and define the charging method and base rate.</p> <ul style="list-style-type: none"> ■ Recurring - enter a base rate and define recurring interval as the charge period. The absolute rate value is required and it is added to the overall price. ■ One time - define the one-time base rate charge. The absolute value is required and it is added as a one time price. ■ Rate Factor - A multiplication factor is required that is applied to the select charge category. For example, if you select CPU Charge and a rate factor of 2. The Guest OS CPU is charged as 2 times the standard cost value. <p>You can add multiple Guest Oses with different rates by clicking Add Charge and configuring an additional charge policy.</p> <hr/> <p>Note Upfront charges for Guest Oses are not shown on the summary page, even though they are part of the policy.</p>

Table 4-3. Pricing Policy Configuration (continued)

Parameter	Description
Tags	<p>You can define a Tag charge by clicking Add Charge. Select the Tag name and define the charging method and base rate.</p> <ul style="list-style-type: none"> ■ Recurring - enter a base rate and define recurring interval as the charge period. The absolute rate value is required and it is added to the overall price. ■ One time - define the one-time base rate charge. The absolute value is required and it is added as a one time price. ■ Rate Factor - A multiplication factor is required that is applied to the select charge category. <p>Select how to charge the Tag based on powered on state.</p> <p>You can add multiple Tags with different rates by clicking Add Charge and configuring an additional charge policy.</p> <hr/> <p>Note Additional charges in the calculated final price include on tags on VMs and does not include tags on disks and networks.</p>
Custom Properties	<p>You can define a Custom Property charge by clicking Add Charge.</p> <p>Enter the property name and value, and define the charging method and base rate.</p> <ul style="list-style-type: none"> ■ Recurring - enter a base rate and define recurring interval as the charge period. The absolute rate value is required and it is added to the overall price. ■ One time - define the one-time base rate charge. The absolute value is required and it is added as a one time price. ■ Rate Factor - A multiplication factor is required that is applied to the select charge category. <p>Select how to charge the custom property based on powered on state.</p> <p>You can add multiple custom properties with different rates by clicking Add Charge and configuring an additional charge policy.</p>
Overall Charges	<p>Define any additional charge you would like to add to the pricing policy. You can add both one time and recurring charges.</p>

Note One time charges are not shown in the price estimate of a catalog item or on the summary tab. Only the daily price estimate for a given catalog item is shown.

- Click the **Assignments** tab and click **Assign Projects**. Select one or more projects to assign the pricing card to.

Note By default pricing cards are applied to projects. On the **Infrastructure > Pricing Cards** tab, you can select to apply pricing cards to cloud zones. If cloud zones were selected, you would click **Assign Cloud Zones** on the Assignments tab.





- Click **Create** to save and create your pricing policy.

Results

Your new pricing policy appears on the Pricing Cards page. To view or edit the policy details and configuration click **Open**.

How do I estimate the price of a deployment

Before deploying a catalog item, you can use the upfront price as a price estimate for your deployment.

Daily Price Estimate		×
<div>  Guest OS and one time prices are excluded in this estimate. </div>		
	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
<div>CLOSE</div>		

For an upfront price estimation, the size of boot disk per VM is always 8 GB.

The upfront price of a deployment is a daily price estimate, based on the allocation of a resource, for a given catalog item before it is deployed. After a catalog item is deployed, you can view the month-to-date price as an aggregate of the upfront price on the **Deployment** and **Infrastructure > Projects** tabs. Upfront pricing is supported for private cloud resources such as vSphere Machine and vSphere Disk, Cloud Assembly catalog items, and cloud agnostic items with vCenter configured for private cloud.

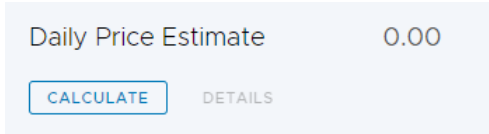
Note Upfront pricing is not supported for public cloud resources, or non-vSphere Machine or Disk private cloud resources.

Prerequisites

To view the price in vRealize Automation Cloud Assembly, you must have a vRealize Operations integration endpoint configured with pricing enabled and currency preset.

Procedure

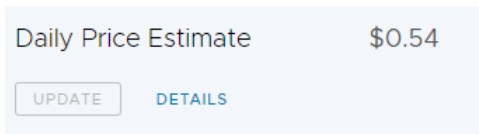
- 1 From the Catalog, select a catalog item and click **Request**.



Daily Price Estimate 0.00

CALCULATE DETAILS

- 2 Enter the details for your catalog item request and click **Calculate**.



Daily Price Estimate \$0.54

UPDATE **DETAILS**

- 3 (Optional) Click **Details** to view the price breakdown in the Daily price Estimate window.

What to do next

If the daily price estimate is acceptable, click **Submit** to continue the deployment request.

How do I estimate the price of all my projects

As a cloud administrator you might want to estimate the total price of all your projects.

For showback purposes, you can use project pricing cards to estimate the total price of all your projects.

Procedure

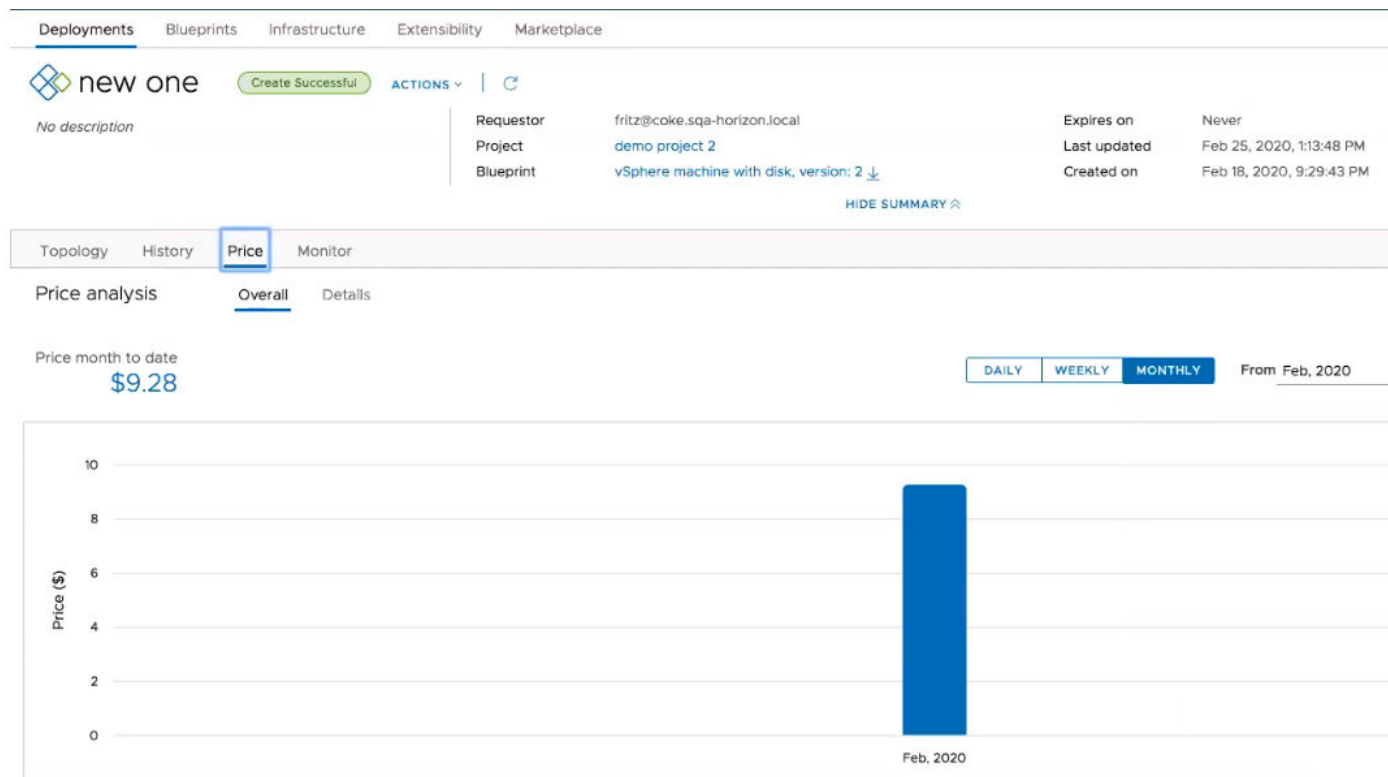
- 1 On the **Infrastructure > Pricing Card** page, next to **All pricing cards are applied to:** click **Edit** and select **Projects**.

Note If you change the **All pricing cards are applied to** setting, all existing pricing card assignments are deleted.

- 2 Create pricing cards and assignments using a cost-based approach. See [How to create a pricing card in Cloud Assembly](#).

How do I view the price history of my deployment

After defining and assigning a pricing card to a project, you can view the price history of an individual deployment over time.



To view the price history, navigate to your deployment and click **Price**. The price analysis provides an overview and detailed view of the deployment price along with the price month-to-date value. You can change the graphical representation to display the deployment price as daily, weekly, or monthly values. Also, you can specify an exact date range or month for the price history.

To view the price breakdown by cost component, click **Details**.

The screenshot displays the vRealize Automation Cloud Assembly interface. At the top, there are tabs for Deployments, Blueprints, Infrastructure, Extensibility, and Marketplace. The 'Deployments' tab is active, showing a deployment named 'new one' with a 'Create Successful' status. Below this, there is a table with deployment details: Requestor (fritz@coke.sqa-horizon.local), Project (demo project 2), and Blueprint (vSphere machine with disk, version: 2). To the right, there are fields for Expires on (Never), Last updated (Feb 25, 2020, 1:13:48 PM), and Created on (Feb 18, 2020, 9:29:43 PM). A 'HIDE SUMMARY' link is also present.

Below the deployment details, there are tabs for Topology, History, Price, and Monitor. The 'Price' tab is active, showing a 'Price analysis' section. Under 'Price analysis', there are two sub-tabs: Overall and Details. The 'Details' sub-tab is selected, showing a price analysis for 'Cloud_vSphere_Machine_1' with a price of \$9.28. A note indicates that the cost of disk is accommodated in the VM's storage cost. A diagram on the right shows two 'Cloud_vSphere' components connected by a line, with a price tag of \$9.28.

Configuring Multi-provider tenant resources with vRealize Automation

In multi-tenancy environments, customers can manage allocation of resources on a per-tenant basis using Virtual Private Zones (VPZs).

In vRealize Automation 8.x, customers can configure multi-tenancy environments using VMware Life Cycle Manager and Workspace ONE Access. These tools enable users to set up multi-tenancy and create and configure tenants. After tenants are configured, provider administrators can create Virtual Private Zones in vRealize Automation Cloud Assembly and then they can assign Zones to tenants using the vRealize Automation Cloud Assembly Manage Tenants functionality.

Multi-tenancy relies on coordination and configuration of three different VMware products as outlined below:

- Workspace ONE Access - This product provides the infrastructure support for multi-tenancy and the Active Directory domain connections that provide user and group management within tenant organizations.
- vRealize Suite Lifecycle Manager - This product supports the creation and configuration of tenants for supported products, such as vRealize Automation. In addition, it provides some certificate management capabilities.
- vRealize Automation - Providers and users log in to vRealize Automation to access tenants in which they create and manage deployments.

When configuring multi-tenancy, users should be familiar with all three of these products and their associated documentation.

For more information about working with Lifecycle Manager and Workspace ONE Access, see [User Management with VMware Identity Manager](#) and [Managing Users and Groups](#).

How do I create a Virtual Private Zone for vRealize Automation

Provider administrators can create a Virtual Private Zone (VPZ) to allocate infrastructure resources to tenants in a multi-organization vRealize Automation environment. Administrators can also use VPZ's to control resource allocation in single tenant deployments.

You can use VPZ's to allocate resources such as images, networks, and storage resources. They function much as cloud zone on a per tenant basis but they are designed specifically for use with multi tenant deployments. For any given project, you can use either cloud zones or VPZ's but not both. Also, there is a one to one relationship between VPZ's and tenants. That is, a VPZ can be assigned to only one tenant at a time.

You can create a VPZ with or without NSX. If you create a zone without NSX, there are limits regarding NSX-related functionality on vSphere endpoints.

- Security (groups, firewall)
- Network components (NAT)

Prerequisites

- Enable and configure multi-tenancy on your vRealize Automation deployment using VMware Life Cycle Manager and VMware Workspace ONE Access.
- Create tenant administrators as appropriate for your tenant configuration.
- If you want to use NSX, you must create an appropriate NSX cloud account in your provider organization.

Procedure

1 Select **Infrastructure > Configure > Virtual Private Zones**

The VPZ page shows all existing zones and enables you to create zones.

2 Click **New Virtual Private Zone**.

There are six selections on the left side of the page that you can use to configure summary information and infrastructure components for the zone.

3 Enter Summary information for the new zone.

- a Add a Name and Description.
- b Select an Account to which the zone applies.
- c Select the Placement Policy.

Placement policy drives host selection for deployments within the specified cloud zone.

- Default - Distributes compute resources across clusters and hosts randomly. This selection works at an individual machine level. For example, all machines in a particular deployment are distributed randomly across the available clusters and hosts that satisfy the requirements.
- binpack - Places compute resources on the most loaded host that has enough available resources to run the given compute.
- spread - Provisions deployment compute resources to the cluster or host with the least number of virtual machines. For vSphere, Distributed Resource Scheduler (DRS) distributes the virtual machines across the hosts. For example, all requested machines in a deployment are placed on the same cluster, but the next deployment might select another vSphere cluster depending on the current load.

4 Select the Compute resource for the zone.

Add compute resources as appropriate for the cloud zone. Initially, the filter selection is Include all Compute and the following list shows all available compute resources, and they are allocated to the applicable zone. You have two additional options for adding compute resources to a cloud zone.

- Manually select compute - Select this menu item if you want to select compute resources manually from the list below. After you select them, click Add Compute to add the resources to the zone.
- Dynamically include compute by tags - Select this menu item if you want to select compute resource to be added to the zone based on tags. All compute resources are shown until you add appropriate tags. You can select or enter one or more tags in the Include compute with these tags option.

For either compute selection, you can remove one or more of the compute resources shown on the page by selecting the box to the right and clicking Remove.

5 Enter or select tags as appropriate.

6 Select Flavors on the left menu and define one or more flavors for the zone. Flavors define target deployment sizes for a specific cloud account/region.

7 Select Image on the left menu and define one or more images for the zone. Images are machine templates that define OS specifications which are available for the zone.

8 Select Storage on the left menu and select the Storage policy and other storage configurations for the zone.

- 9 On the left menu, select **Network** and define the networks and, optionally, a network policy to use with this zone. You can also configure load balancers and security groups for selected network policies.

Network	<ul style="list-style-type: none"> ■ All existing networks associated with this VPZ appear in the table on the Networks tab. ■ Click Add Network to see all networks associated with the selected region. add a network for use with this zone. ■ Select a network and click Tags to add one or more tags to the specified network. ■ Select Manage IP Ranges to specify the IP Range through which users can access this network. ■ If applicable, click the Network Policies tab and select an isolation policy.
Network policies	<p>If configured, select a network policy to use with this zone to enforce an isolation policy for outbound and private networks.</p> <ul style="list-style-type: none"> ■ Select an isolation policy if desired. ■ Select a Tier-0 logical router and an Edge cluster if desired.
Load Balancers	Click Add Load Balancer to configure load balancers for the account/region cloud accounts.
Security Groups	Click Add Security Group to use security groups to apply firewall rules to provisioned machines.

Results

The Virtual Private Zone is created with the specified resource allocations.

What to do next

Cloud administrators can associate the VPZ with a project.

- 1 In Cloud Assembly, select **Administration > Projects**
- 2 Select the **Provisioning** tab.
- 3 Click **Add Zone** and choose **Add Virtual Private Zone**.
- 4 Select the desired VPZ from the list.
- 5 You can set the provision priority and limits on the number of instances, the amount of memory available and the number of CPUs available.
- 6 Click **Add**.

Manage VPZ configuration for vRealize Automation tenants

Provider administrators can manage Virtual Private Zones (VPZs) within vRealize Automation Cloud Assembly to control infrastructure resource allocation on a per tenant basis. Using the

Tenant Management page, administrators can view tenants and VPZ zones and enable or disable VPZs for tenants.

By default, VPZs are not allocated to any tenants. You must allocate VPZ's on this page in order to use them with your tenants.

When initially created, VPZ's are enabled by default. An enabled VPZ is ready to be allocated and used with the specified tenant. When VPZ's are disabled, they cannot be used for provisioning or allocated to a tenant. A VPZ can be disabled but still allocated for a tenant.

When a provider administrator navigates to the Tenant Management page, the page shows all available tenants and the administrator can select one. After a tenant is selected, the page shows VPZs currently allocated for that tenant, if any. The administrator can use this page to allocate VPZs to the selected tenant.

When a VPZ is allocated, tenant administrators can add it to their projects, and it becomes available for provisioning by tenant users. After a VPZ is allocated to one tenant, it can be allocated to another tenant.

After a VPZ is enabled, it is ready for use within the specified tenant. Provider administrators can disable VPZ's to facilitate maintenance or tenant re-configuration, and they can provide notification to users of the disablement. If you want to make a VPZ unavailable to a tenant on a more permanent basis, you can de-allocate it. If an existing VPZ is de-allocated from a tenant for some reason, it cannot be used to create deployments from that tenant.

Prerequisites

- Set up multi-tenancy and create VPZs as appropriate for your deployment.

Procedure

- 1 In vRealize Automation Cloud Assembly select Manage Tenants.

The Tenant Management page shows all tenants configured for the administrator's organization in a card view.

- 2 Click on a tenant to select it.
- 3 Click the infrastructure management tab to see all allocated VPZ's for the tenant
- 4 Select **Allocate Virtual Private Zone** to open a dialog that shows all zones not currently allocated to tenants. allocate the zone to a tenant.
- 5 Select one or more zones on the dialog and click **Allocate To Tenant**.

What to do next

After VPZs are allocated, tenant administrators can assign them to projects.

Provider administrators can use the card view of tenants to monitor and manager status of VPZs.

- If you want to disable a tenant, click **Disable** on the card for the tenant.
- To enable a tenant, click **Enable** on the card for the tenant.

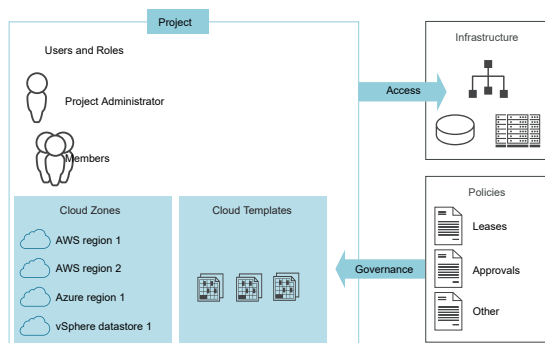
- If you want to de-allocate a tenant, click **Deallocate** on the card for that tenant.

Adding and managing vRealize Automation Cloud Assembly projects

5

Projects control who has access to vRealize Automation Cloud Assembly cloud templates and where the templates are deployed. You use projects to organize and govern what your users can do and to what cloud zones they can deploy cloud templates in your cloud infrastructure.

Cloud administrators set up the projects, to which they can add users and cloud zones. Anyone who creates and deploys cloud templates must be a member of at least one project.



This chapter includes the following topics:

- [How do I add a project for my vRealize Automation Cloud Assembly development team](#)
- [Learn more about vRealize Automation Cloud Assembly projects](#)

How do I add a project for my vRealize Automation Cloud Assembly development team

You create a project to which you add members and cloud zones so that the project members can deploy their cloud templates to the associated zones. As the vRealize Automation Cloud Assembly administrator, you create a project for a development team. You can then assign a project administrator or you can operate as the project administrator.

When you create a cloud template, you first select the project to associate it with. The project must exist before you can create the cloud template.

Ensure that your projects support the business needs of the development team.

- Does the project provide the resources that support the team's goals. For an example of how the infrastructure resources and a project support a cloud template, see [Tutorial: Setting up and testing multi-cloud infrastructure and deployments in vRealize Automation Cloud Assembly](#).
- Do your project members require or expect their deployments to be shared or private. Shared deployments are available to all the project members on the Deployments tab, not only the deploying member. You can change the deployment sharing state at anytime.

When you share the deployment with project members, the members can run the same day 2 action. To manage the ability of members to run day 2 actions, you can create day 2 policies in vRealize Automation Service Broker. The policies apply to vRealize Automation Cloud Assembly and vRealize Automation Service Broker deployments.

To learn more about the day 2 policies, see [How do I entitle deployment users to day 2 actions using policies](#).

This procedure is based on creating an initial project that includes only the basic configurations. As your development team creates and deploys their cloud templates, you might modify to the project. You can add constraints, custom properties, and other options to improve deployment efficiencies. See the articles available in [Learn more about vRealize Automation Cloud Assembly projects](#).

Prerequisites

- Verify that you configured the cloud zones. See [Chapter 4 Building your vRealize Automation Cloud Assembly resource infrastructure](#).
- Verify that you configured the mappings and profiles for the regions that include as cloud zones for this project. See [Chapter 4 Building your vRealize Automation Cloud Assembly resource infrastructure](#).
- Verify that you have the necessary permissions to perform this task. See [What are the vRealize Automation user roles](#).
- Determine who you are designating as the project administrator. To understand what the project administrator can do in vRealize Automation Cloud Assembly, see [What are the vRealize Automation user roles](#).
- If you are adding Active Directory groups to projects, verify that you configured Active Directory groups for your organization. See [Edit group role assignments in vRealize Automation](#) in *Administering vRealize Automation*. If the groups are not synchronized, they are not available when you try to add them to a project.

Procedure

- 1 Select **Infrastructure > Administration > Projects**, and click **New Project**.
- 2 Enter the project name.

3 Click the **Users** tab.

- a To make deployments by project members accessible only to the requesting user, turn off **Deployment sharing**. To ensure that you can assign the ownership of a deployment to another member of the project, verify that the **Deployment sharing** is turned on.
- b Add users with assigned roles.

4 Click the **Provisioning** tab and add one or more cloud zones.

Add any cloud zones and virtual private zones that contain the resources that support the cloud templates deployed by the project users.

For each zone, you can set a zone priority and you can limit the amount of resources that the project can utilize. The possible limits include the number of instances, memory, and CPUs. For vSphere cloud zones only, you can configure storage limits.

As you add each zone and apply limits, don't limit the project resources so much that the members cannot deploy their cloud templates.

When your users submit a deployment request, the zones are evaluated to determine which zones have the resources to support the deployment. If more than one zone supports the deployment, then the priority is evaluated and the workload is placed on the one with the higher priority, which is the lowest integer.

5 Click **Create**.**6** To test your project with the project cloud zones, click **Test Configuration** on the Projects page.

The simulation runs a standardized hypothetical deployment test against the project cloud zone resources. If it fails, you can review the details and correct your resource configuration.

What to do next

Get started with cloud templates. See [Chapter 6 Designing your vRealize Automation Cloud Assembly deployments](#).

Learn more about vRealize Automation Cloud Assembly projects

Projects are the connector between cloud templates and resources. The more you understand about how they work and how you can make them work for you, the more effective your vRealize Automation Cloud Assembly development and deployment process will be.

Using vRealize Automation Cloud Assembly project tags and custom properties

As an administrator, you can add project-level governance constraints or custom properties when the requirements of the project are different from the vRealize Automation Cloud Assembly cloud

templates. In addition to constraint tags, you can add resource tags that are added to deployed resources during the provisioning process so that you can manage the resources.

What are project resource tags

A project resource tag operates as an standardized identifying tag that you can use to manage the deployed resources and ensure compliance.

The resource tags defined in a project are added to all component resources deployed as part of that project. You can then use the standard tagging to manage the resources using other applications.

For example, as a cloud administrator, you want to use an application like CloudHealth to manage costs. You add the `costCenter:eu-cc-1234` tag to a project dedicated to developing a European Union human resources tool. When the project team deploys from this project, the tag is added to the deployed resources. You then configure the costing tool to identify and manage the resources that include this tag. Other projects with other cost centers would have alternative values to go with the key.

What are project constraint tags

A project constraint operates as a governance definition. It is a `key:value` tag that defines what resources the deployment request consumes or avoids in the project cloud zones.

The deployment process looks for tags for the networks and storage that match the project constraints, and deploys based on matching tags.

The extensibility constraint is used to specify which vRealize Orchestrator integrated instance to use for extensibility workflows.

Consider the following formats when you configure project constraints.

- **key:value** and **key:value:hard**. Use this tag, in either format, when the cloud template must be provisioned on resources with the matching capability tag. The deployment process fails when no matching tag is found. For example, a cloud template deployed by the members of a project must be provisioned on a PCI-compliant network. You use `security:pci`. If no networks are found in the project cloud zones, the deployment fails, ensuring no insecure deployments.
- **key:value:soft**. Use this tag when you prefer a matching resource, but you want the deployment process to proceed without failing and can accept resources where the tag does not match. For example, you prefer that the project members deploy their cloud templates to a less expensive storage, but you do not want storage availability to interfere with their ability to deploy. You use `tier:silver:soft`. If there is no storage tagged `tier:silver` in the project cloud zones, the cloud template still deploys on other storage resources.
- **!key:value**. Use this tag, with hard or soft, when you want to avoid deploying to resources with a matching tag.

Importantly, the project constraint tags have a higher priority than the cloud template constraint tags and override them at deployment time. If you have a cloud template where this must never happen, you can use the `failOnConstraintMergeConflict:true` in the template. For example, if your project has a network `loc:london` constraint, but the cloud template is `loc:mumbai`, but rather than the project location taking precedence, you want the deployment to fail with a constraint conflict message, you add a property similar to the following sample.

```
constraints:
  - tag: 'loc:mumbai'
failOnConstraintMergeConflict:true
```

How might I use project custom properties

You can use a project custom property for reporting, to trigger and populate extensibility actions and workflow, and to override cloud template level properties.

Adding a custom property to a deployment allows you to use the value in the user interface or to retrieve it using the API so that you can generate reports.

Extensibility can also use a custom property for an extensibility subscription.

A cloud template might have a particular property value that you want to change for a project. You can provide an alternative name and value as a custom property.

How do vRealize Automation Cloud Assembly projects work at deployment time

Projects control user access to the cloud zones and user ownership of the provisioned resources. Whether you are a cloud administrator or a cloud template developer, you must understand how the projects work at deployment time so that you can manage your deployments and troubleshoot any problems.

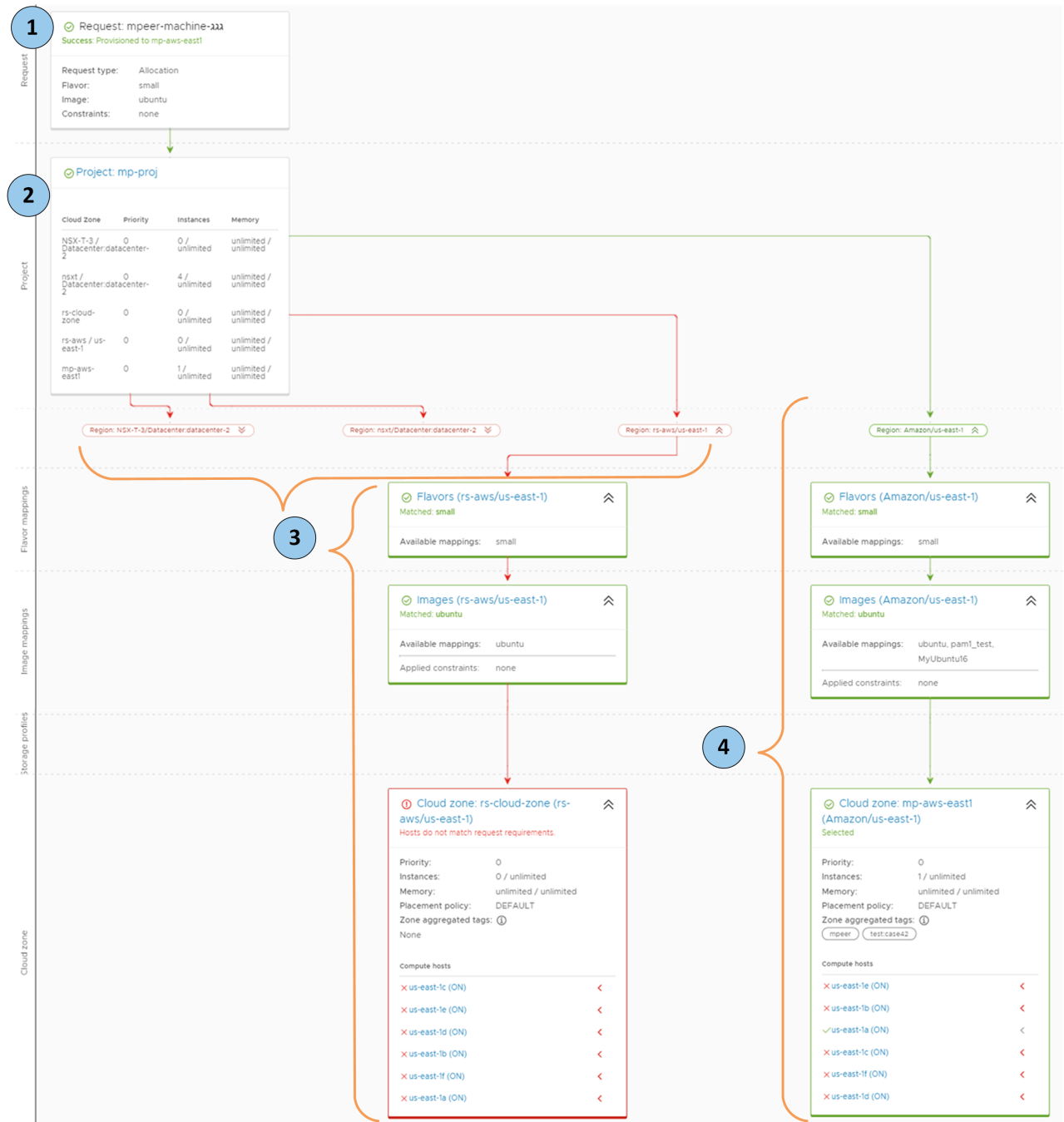
As a cloud administrator who is setting up projects for various teams, you must understand how projects determine where cloud template components are deployed. This understanding helps you create projects that support cloud template developers and to troubleshoot failed deployments.

When you create a cloud template, you first associate it with a project. At deployment time, the cloud template requirements are evaluated against the project cloud zones to find the best deployment location.

The following workflow illustrates the process.

- 1 You submit a cloud template deployment request.
- 2 The project evaluates the template and project requirements, for example, flavor, image, and constraint tags. The requirements are compared to the project cloud zones to locate a zone that supports the requirements.
- 3 These zones did not have the resources to support the request.

- 4 This cloud zone supports the request requirements and the template is deployed to this cloud zone account region.



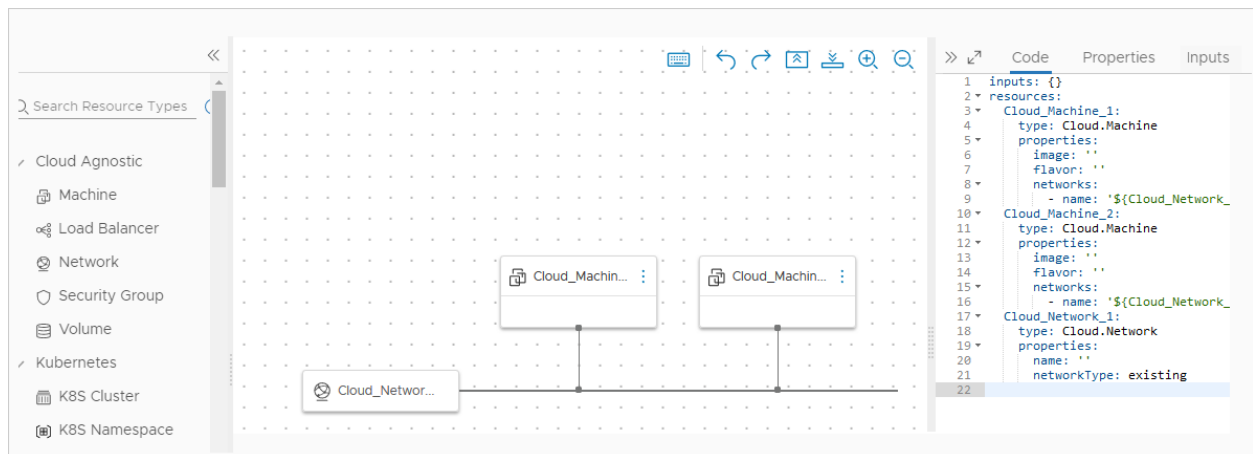
Designing your vRealize Automation Cloud Assembly deployments

6

Deployments begin with cloud templates, formerly called blueprints, which are the specifications that define the machines, applications, and services that you create on cloud resources by way of vRealize Automation Cloud Assembly.

As a cloud template developer, you can design templates that target specific cloud vendors, or make them cloud agnostic. The cloud zones that are assigned to your project determine which approach you might take. Check with your cloud administrator to make sure that you understand what kind of resources make up your cloud zones.

Be aware that vRealize Automation Cloud Assembly template creation is an infrastructure-as-code process. You add and connect resources in the design canvas to get started. Then, you complete the details using the code editor to the right of the canvas. The code editor allows you to type code directly or enter property values into a form.



Before you create a cloud template

You can create a vRealize Automation Cloud Assembly template at any time, but to deploy it you first need to define your cloud resource infrastructure.

- [Chapter 4 Building your vRealize Automation Cloud Assembly resource infrastructure](#)

In addition, you must create a vRealize Automation Cloud Assembly project that includes those infrastructure resources as cloud zones.

- [Chapter 5 Adding and managing vRealize Automation Cloud Assembly projects](#)

This chapter includes the following topics:

- [Ways to create cloud templates](#)
- [How to create a simple vRealize Automation Cloud Assembly template from scratch](#)
- [How to enhance a simple vRealize Automation Cloud Assembly template](#)
- [How to add advanced features to vRealize Automation Cloud Assembly designs](#)
- [What are the vRealize Automation resource properties](#)
- [What are some vRealize Automation Cloud Assembly code examples](#)
- [How to include Terraform configurations in vRealize Automation Cloud Assembly](#)
- [How to use the vRealize Automation Cloud Assembly Marketplace](#)

Ways to create cloud templates

vRealize Automation Cloud Assembly creates and saves cloud templates as code, which allows you to easily design and reuse templates.

You can build a cloud template from a blank canvas or take advantage of existing code.

The vRealize Automation Cloud Assembly design page

To create a cloud template from scratch, go to **Design > Cloud Templates** and click **New from > Blank canvas**. Drag resources to the canvas, connect them, and finish configuring them in the code editor.

The code editor allows you to type, cut, copy, and paste code directly. If you're uncomfortable editing code, you can select a resource in the design canvas, click the code editor **Properties** tab, and enter values there. Property values that you enter appear in the code as if you had typed them directly.

The screenshot displays the vRealize Automation Cloud Assembly interface. On the left, a code editor shows the following YAML code for a 'WebTier' resource:

```
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
```

On the right, the 'Properties' tab is active, showing a form for configuring the resource. The form includes the following fields and sections:

- Count:** Set to `"${input.count}"`.
- Image Type:** Set to `ubuntu`.
- Flavor *:** Set to `${input.size}`.
- Storage:** A section for configuring storage.
- Constraints:** A section for adding constraints, currently showing a 'Tag' constraint.
- Maximum Capacity of the disk in GB:** Set to `1`.
- Size of boot disk in GB:** Set to `1`.
- Networks:** A section for adding networks.

Note that you can copy and paste code from one cloud template to another.

Cloud template cloning

To clone a template, go to **Design**, select a source, and click **Clone**. You clone a cloud template to create a copy based on the source, then assign the clone to a new project or use it as starter code for a new application.

Uploading and downloading

The vRealize Automation Cloud Assembly Marketplace offers finished cloud templates to jumpstart your effort. See [How to use the vRealize Automation Cloud Assembly Marketplace](#).

In addition, you can upload, download, and share cloud template YAML code in any way that makes sense for your site. You can even modify template code using external editors and development environments.

Note A good way to validate shared template code is to inspect it in the vRealize Automation Cloud Assembly code editor on the design page.

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

How to create a simple vRealize Automation Cloud Assembly template from scratch

You use the design page to create vRealize Automation Cloud Assembly template specifications for the machines or applications that you want to provision.

- 1 Locate resources.
- 2 Drag resources to the canvas.
- 3 Connect resources.
- 4 Configure resources by editing the cloud template code.

The screenshot shows the vRealize Automation Cloud Assembly design page. On the left, a sidebar lists resource categories: Cloud Agnostic, Machine, Load Balancer, Network, Security Group, Volume, Kubernetes, K8S Cluster, and K8S Namespace. A search bar is at the top of the sidebar. In the center, a canvas displays a diagram with three resources: 'Cloud_Machine_1', 'Cloud_Machine_2', and 'Cloud_Network_1'. Lines connect these resources, indicating dependencies. On the right, a code editor shows the JSON configuration for these resources. The code defines inputs, resources, and their properties, including image, flavor, and network details. Numbered callouts (1, 2, 3, 4) highlight key steps: 1 points to the 'Machine' resource in the sidebar, 2 points to a resource on the canvas, 3 points to a connection line, and 4 points to the code editor.

```

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

```

From the design page, you can also change the cloud template name, version or revert to versions, clone, or deploy a template.

How to select and add vRealize Automation Cloud Assembly resources to a cloud template

vRealize Automation Cloud Assembly resources are your cloud template building blocks. The design page lets you use cloud agnostic resources, or resources specific to a cloud vendor.

Resources appear for selection on the left side of the design page.

Cloud agnostic resources

You can deploy cloud agnostic resources to any cloud vendor. At provisioning time, the deployment uses cloud specific resources that match. For example, if you expect a cloud template to deploy to both AWS and vSphere cloud zones, use cloud agnostic resources.

Cloud vendor resources

Vendor resources, such as those specific to Amazon Web Services, Microsoft Azure, Google Cloud Platform, or VMware vSphere, can only be deployed to matching AWS, Azure, GCP, or vSphere cloud zones.

You can add cloud agnostic resources to a cloud template that contains cloud specific resources for a particular vendor. Just be aware of what the project cloud zones support in terms of vendor.

Configuration management resources

Configuration management resources depend on your integrated applications. For example, a Puppet resource can monitor and enforce the configuration of the other resources.

How to connect cloud template resources in vRealize Automation Cloud Assembly

Use the vRealize Automation Cloud Assembly graphical design canvas to connect cloud template resources.

You can connect resources when they are compatible for a connection. For example:

- Connecting a load balancer to a cluster of machines.
- Connecting a machine to a network.
- Connecting external storage to a machine.

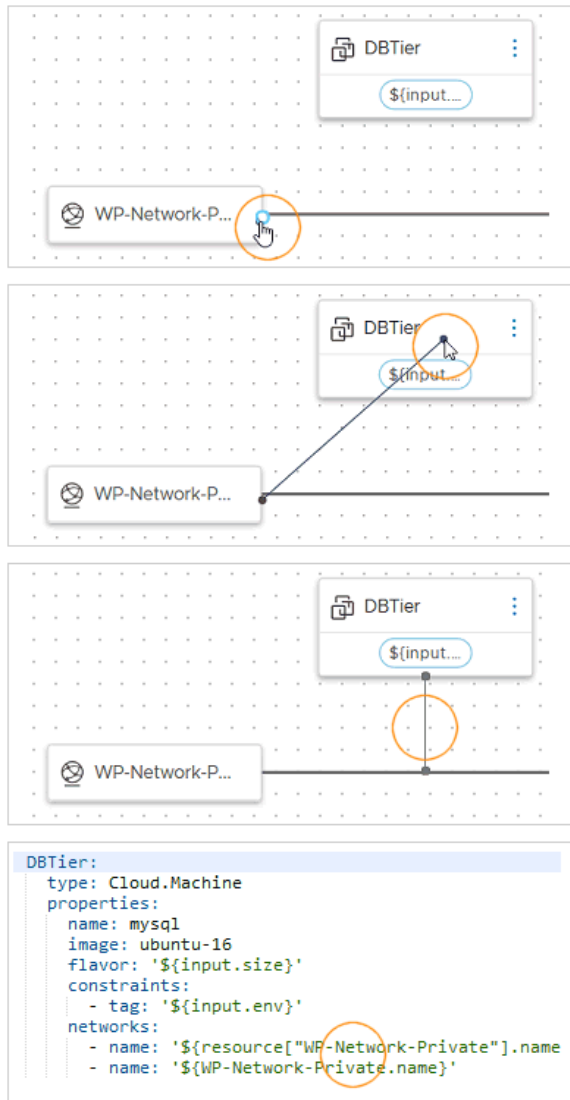
Important A solid line connector requires that the two resources be deployed in the same cloud zone. If you add conflicting constraints to the resources, deployment might fail.

For example, you can't deploy connected resources where constraint tags force the placement of one to a zone in us-west-1, and the other to a zone in us-east-1.

Solid or dashed arrows only indicate a dependency, not a connection. For more about dependencies, see [How to set the resource deployment sequence in vRealize Automation Cloud Assembly](#).

To connect, hover over the edge of a resource to reveal the connection bubble. Then, click and drag the bubble to the target resource and release.

In the code editor, additional code for the source resource appears in the target resource code.

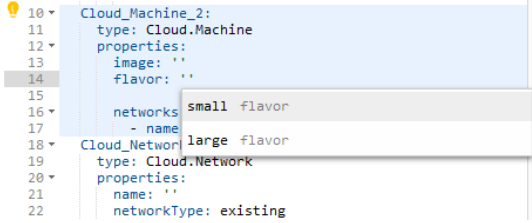
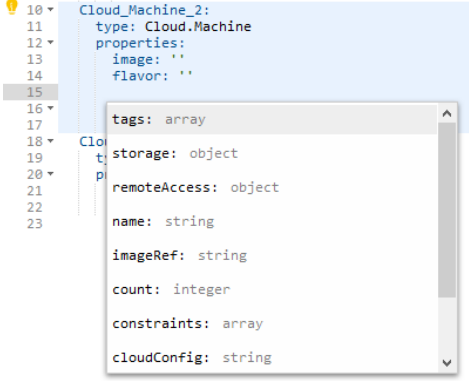
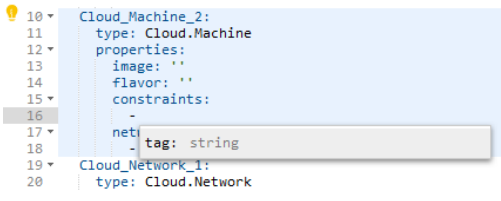
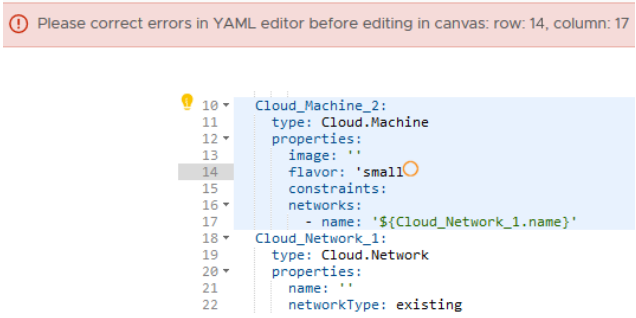
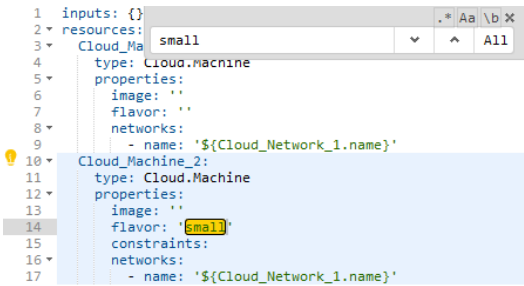


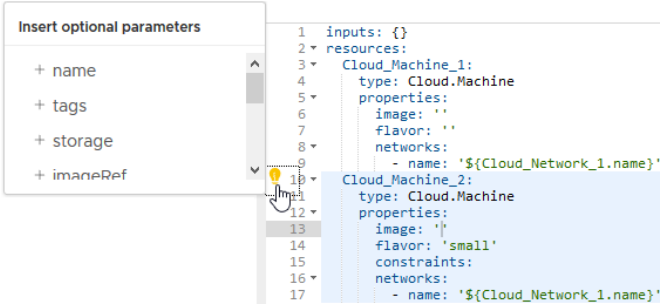
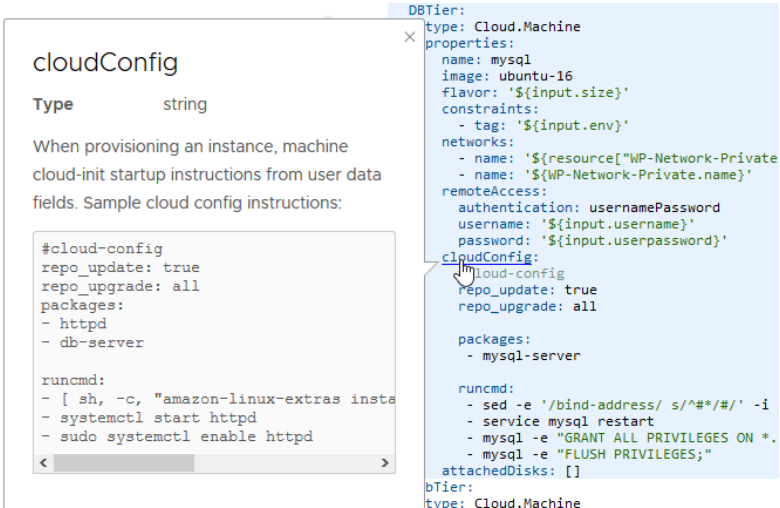
In the figure, the SQL machine and private network are connected, so they must be deployed in the same cloud zone.

How to create valid cloud template code in vRealize Automation Cloud Assembly

Adding vRealize Automation Cloud Assembly resources and connecting them in the canvas only creates starter code. To fully configure them, edit the code.

The code editor allows you to type code directly or enter property values into a form. To help with direct code creation, the vRealize Automation Cloud Assembly editor includes syntax completion and error checking features.

Editor	
Hints	Example
Available values	
Allowed properties	
Child properties	
Syntax errors	
Ctrl+F to search	

Editor Hints	Example
Optional parameter s	 <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>
Schema help	<p>For all of the custom properties, you can also refer to the vRealize Automation Resource Type Schema on VMware {code}.</p>  <pre> DBTier: 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>

How to save different versions using vRealize Automation Cloud Assembly

As a cloud template developer, you can safely capture a snapshot of a working design before risking further changes.

At deployment time, you can select any of your versions to deploy.

Capturing a cloud template version

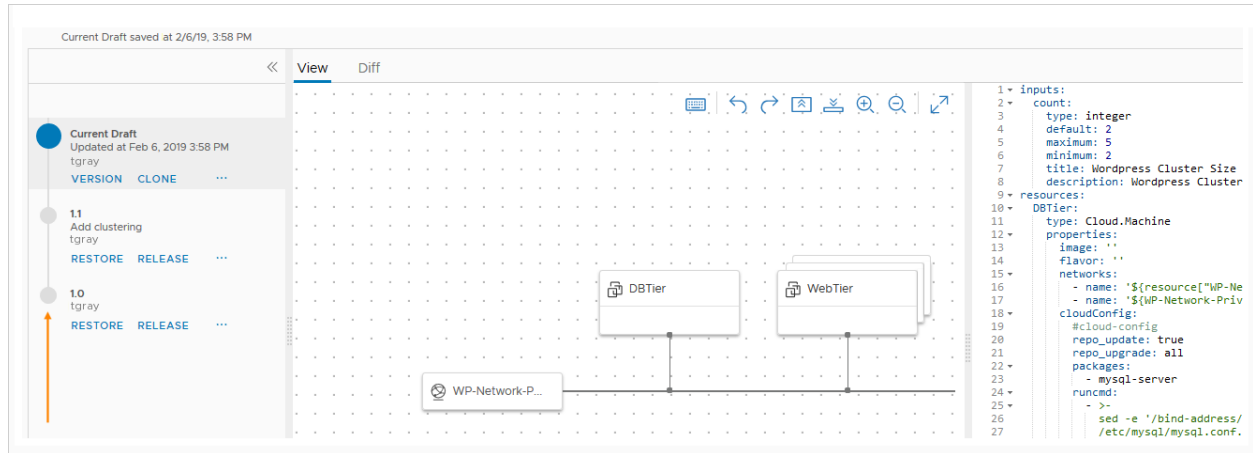
From the design page, click **Version**, and provide a name.

The name must be alphanumeric, with no spaces, and only periods, hyphens, and underscores allowed as special characters.

Restoring an older version

From the design page, click **Version History**.

On the left, select an older version to inspect it in the canvas and code editor. When you find the version that you want, click **Restore**. Restoring overwrites the current draft without removing any named versions.



Releasing a version to vRealize Automation Service Broker

From the design page, click **Version History**.

On the left, select a version and release it.

You can't release a Current Draft until you version it.

Reimporting the version in vRealize Automation Service Broker

To enable the new version for catalog users, reimport it.

In vRealize Automation Service Broker, go to **Content & Policies > Content Sources**.

In the list of sources, click the source for the project that contains the cloud template with the newly released version.

Click **Save & Import**.

Comparing cloud template versions

When changes and versions accumulate, you might want to identify differences among them.

In vRealize Automation Cloud Assembly, from the Version History view, select a version, and click **Diff**. Then, from the **Diff against** drop-down, select another version to compare to.

Note that you can toggle between reviewing code differences or visual topology differences.

Figure 6-1. Code Differences

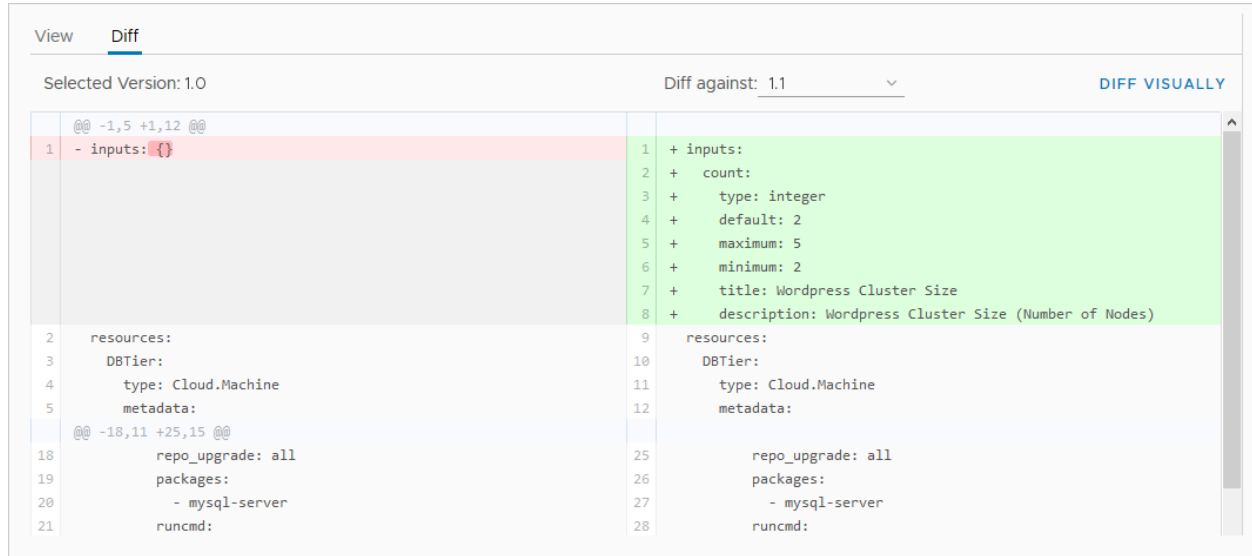
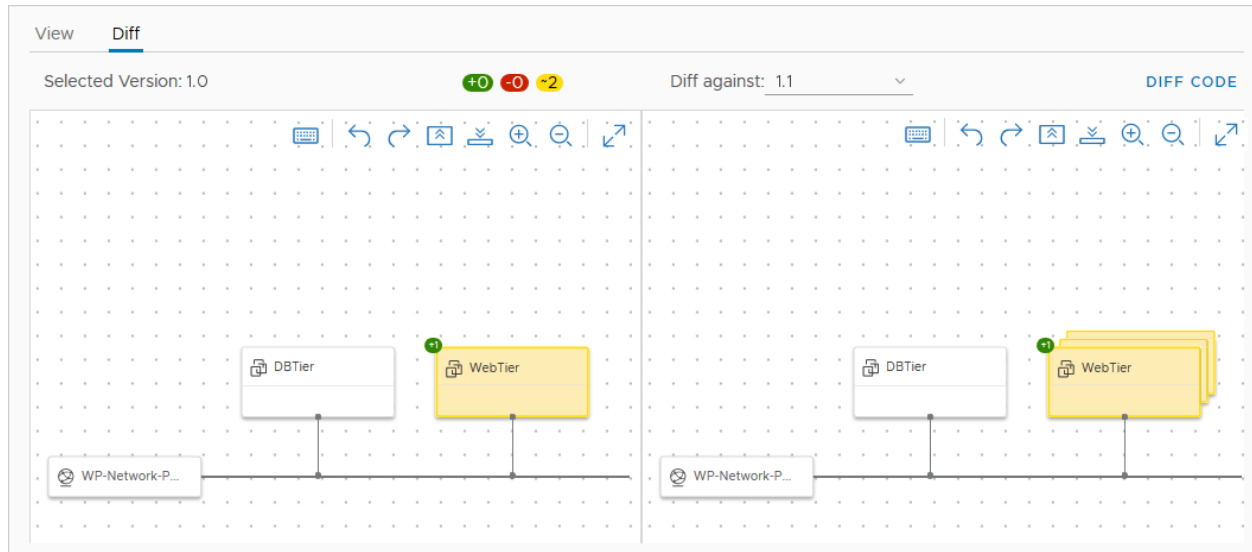


Figure 6-2. Visual Topology Differences



Cloning a cloud template

Although it's not the same as saving a version, from the design page, **Actions > Clone** makes a copy of the current template for alternative development.

How to enhance a simple vRealize Automation Cloud Assembly template

There are vRealize Automation Cloud Assembly template code possibilities that can take a simple template to the next level.

The techniques described here require some comfort with infrastructure code. Fortunately, vRealize Automation Cloud Assembly code is human readable and fairly easy to follow.

How user input can customize a cloud template in vRealize Automation

As a cloud template designer, you use input parameters so that users can make custom selections at request time.

When users supply inputs, you no longer need to save multiple copies of templates that are only slightly different. In addition, inputs can prepare a template for day 2 operations. See [How to use cloud template inputs for vRealize Automation day 2 updates](#) .

The following inputs show how you might create one cloud template for a MySQL database server, where users can deploy that one template to different cloud resource environments and apply different capacity and credentials each time.

The screenshot shows a 'Testing Basic' dialog box with the following fields:

- Environment:** A dropdown menu with 'env:dev' selected.
- Tier Machine Size:** A dropdown menu with 'small' selected.
- Database Username:** A text input field containing 'ouradmin'.
- Database Password:** A password input field containing '.....'.

At the bottom right, there are two buttons: 'CANCEL' and 'TEST'.

How to define cloud template input parameters

Add an `inputs` section to your template code, where you set the selectable values.

In the following example, machine size, operating system, and number of clustered servers are selectable.

```
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)

```

If you're uncomfortable editing code, you can click the code editor **Inputs** tab, and enter settings there. The following example shows some inputs for the MySQL database mentioned earlier.

The screenshot shows the 'Inputs' tab in the vRealize Automation Cloud Assembly interface. The main window displays a table of cloud template inputs. Below the table, an 'Edit Cloud Template Input' dialog is open for the 'size' input.

<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

Edit Cloud Template Input: size

Name *

Title

Description

Type

Encrypted ☐

How to reference cloud template input parameters

Next, in the `resources` section, you reference an input parameter using `${input.property-name}` syntax.

If a property name includes a space, delimit with square brackets and double quotes instead of using dot notation: `${input["property name"]}`

Important In cloud template code, you cannot use the word `input` except to indicate an input parameter.

```
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      flavor: '${input.wp-size}'
      image: '${input.wp-image}'
      count: '${input.wp-count}'
```

List of input properties

Property	Description
const	Used with oneOf. The real value associated with the friendly title.
default	Prepopulated value for the input. The default must be of the correct type. Do not enter a word as the default for an integer.
description	User help text for the input.
encrypted	Whether to encrypt the input that the user enters, true or false. Passwords are usually encrypted.
enum	A drop-down menu of allowed values. Use the following example as a format guide. <div> <pre>enum: - value 1 - value 2</pre> </div>
format	Sets the expected format for the input. For example, (25/04/19) supports date-time. Allows the use of the date picker in vRealize Automation Service Broker custom forms.
items	Declares items within an array. Supports number, integer, string, Boolean, or object.
maxItems	Maximum number of selectable items within an array.
maxLength	Maximum number of characters allowed for a string. For example, to limit a field to 25 characters, enter <code>maxLength: 25</code> .
maximum	Largest allowed value for a number or integer.

Property	Description
minItems	Minimum number of selectable items within an array.
minLength	Minimum number of characters allowed for a string.
minimum	Smallest allowed value for a number or integer.
oneOf	Allows the user input form to display a friendly name (title) for a less friendly value (const). If setting a default value, set the const, not the title. Valid for use with types string, integer, and number.
pattern	Allowable characters for string inputs, in regular expression syntax. For example, '[a-z]+' or '[a-z0-9A-Z@#]+\$'
properties	Declares the key:value properties block for objects.
readOnly	Used to provide a form label only.
title	Used with oneOf. The friendly name for a const value. The title appears on the user input form at deployment time.
type	Data type of number, integer, string, Boolean, or object.
writeOnly	Hides keystrokes behind asterisks in the form. Cannot be used with enum. Appears as a password field in vRealize Automation Service Broker custom forms.

Additional examples

String with 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

```

Integer with minimum and maximum

```
count:
  type: integer
  title: Machine Count
  description: The number of machines that you want to deploy.
  maximum: 5
  minimum: 1
  default: 1
```

Array of objects

```
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
```

String with friendly names

```
platform:
  type: string
  oneOf:
    - title: AWS
      const: platform:aws
    - title: Azure
      const: platform:azure
    - title: vSphere
      const: platform:vsphere
  default: platform:aws
```

String with pattern validation

```
username:
  type: string
  title: Username
  description: The name for the user that will be created when the machine is provisioned.
  pattern: ^[a-zA-Z]+$
```

String as password

```
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
```

String as text area

```
ssh_public_key:
  type: string
  title: SSH public key
  maxLength: 256
```

Boolean

```
public_ip:
  type: boolean
  title: Assign public IP address
  description: Choose whether your machine should be internet facing.
  default: false
```

Date and time calendar selector

```
leaseDate:
  type: string
  title: Lease Date
  format: date-time
```

How vRealize Automation Cloud Assembly resource flags can customize a request

vRealize Automation Cloud Assembly includes several cloud template settings that adjust how a resource is handled at request time.

Resource flag settings aren't part of the resource object properties schema. For a given resource, you add the flag settings outside of the properties section as shown.

```
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
```

Resource Flag	Description
createBeforeDelete	<p>Some update actions require that the existing resource be removed and a new one be created. By default, removal is first, which can lead to conditions where the old resource is gone but the new one wasn't created successfully for some reason.</p> <p>Set this flag to true if you need to make sure that the new resource is successfully created before deleting the previous one.</p>
createTimeout	<p>The vRealize Automation Cloud Assembly default timeout for resource allocate, create, and plan requests is 2 hours (2h). In addition, a project administrator can set a custom default timeout for these requests, applicable throughout the project.</p> <p>This flag lets you override any defaults and set the individual timeout for a specific resource operation. See also <code>updateTimeout</code> and <code>deleteTimeout</code>.</p>
deleteTimeout	<p>The vRealize Automation Cloud Assembly default timeout for delete requests is 2 hours (2h). In addition, a project administrator can set a different default timeout for delete requests, applicable throughout the project.</p> <p>This flag lets you override any defaults and set the individual timeout for a specific resource delete operation. See also <code>updateTimeout</code> and <code>createTimeout</code>.</p>
dependsOn	<p>This flag identifies an explicit dependency between resources, where one resource must exist before creating the next one. For more information, see How to set the resource deployment sequence in vRealize Automation Cloud Assembly.</p>
dependsOnPreviousInstances	<p>When set to true, create cluster resources sequentially. The default is false, which simultaneously creates all resources in a cluster.</p> <p>For example, sequential creation is useful for database clusters where primary and secondary nodes must be created, but secondary node creation needs configuration settings that connect the node to an existing, primary node.</p>
forceRecreate	<p>Not all update actions require that the existing resource be removed and a new one be created. If you want an update to remove the old resource and create a new one, independent of whether the update would have done so by default, set this flag to true.</p>

Resource Flag	Description
ignoreChanges	<p>Users of a resource might reconfigure it, changing the resource from its deployed state.</p> <p>If you want to perform a deployment update but not overwrite the changed resource with the configuration from the cloud template, set this flag to true.</p>
preventDelete	<p>If you need to protect a resource from subsequent delete requests, set this flag to true.</p>
updateTimeout	<p>The vRealize Automation Cloud Assembly default timeout for update requests is 2 hours (2h). In addition, a project administrator can set a different default timeout for update requests, applicable throughout the project.</p> <p>This flag lets you override any defaults and set the individual timeout for a specific resource update operation. See also <code>deleteTimeout</code> and <code>createTimeout</code>.</p>

How to set the resource deployment sequence in vRealize Automation Cloud Assembly

When you deploy a vRealize Automation Cloud Assembly template, one resource might need another resource to be available first.

Important Solid or dashed arrows only indicate a dependency, not a connection. To connect resources so that they communicate, see [How to connect cloud template resources in vRealize Automation Cloud Assembly](#).

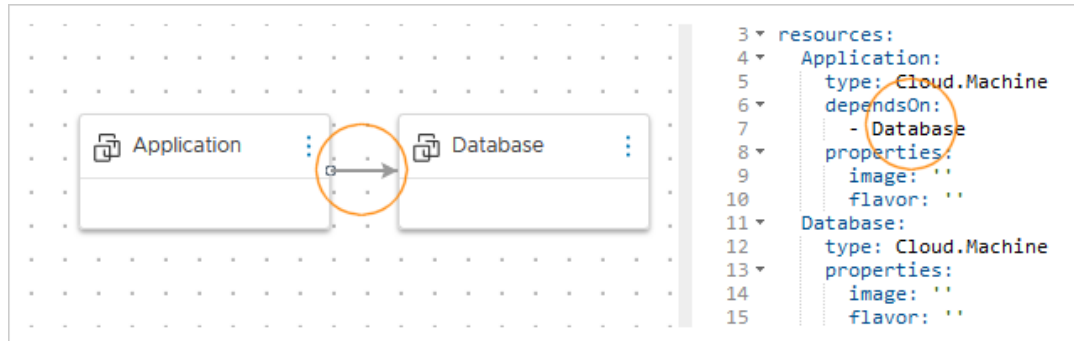
How to create an explicit dependency

Sometimes, a resource needs another to be deployed first. For example, a database server might need to exist first, before an application server can be created and configured to access it.

An explicit dependency sets the build order at deployment time, or for scale in or scale out actions. You can add an explicit dependency using the graphical design canvas or the code editor.

- Design canvas option—draw a connection starting at the dependent resource and ending at the resource to be deployed first.
- Code editor option—add a `dependsOn` property to the dependent resource, and identify the resource to be deployed first.

An explicit dependency creates a solid arrow in the canvas.



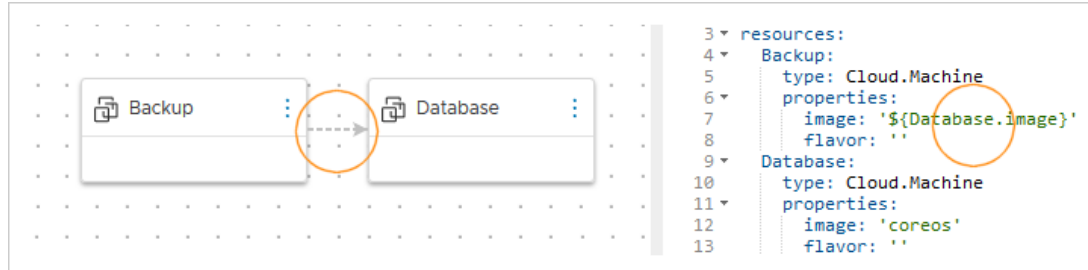
How to create an implicit dependency or property binding

Sometimes, a resource property needs a value found in a property of another resource. For example, a backup server might need the operating system image of the database server that is being backed up, so the database server must exist first.

Also called a property binding, an implicit dependency controls build order by waiting until the needed property is available before deploying the dependent resource. You add an implicit dependency using the code editor.

- Edit the dependent resource, adding a property that identifies the resource and property that must exist first.

An implicit dependency or property binding creates a dashed arrow in the canvas.



How to use expressions to make cloud template code more versatile in vRealize Automation Cloud Assembly

For increased flexibility, you can add expressions to cloud template code in vRealize Automation Cloud Assembly.

Expressions use the `${expression}` construct, as shown in the following examples.

The examples are pruned to show only the important lines. The entire, unedited cloud template appears at the end.

Examples

At deployment time, allow the user to paste in the encrypted key needed for remote access:

```
inputs:
  sshKey:
    type: string
    maxLength: 500
resources:
  frontend:
    type: Cloud.Machine
    properties:
      remoteAccess:
        authentication: publicPrivateKey
        sshKey: '${input.sshKey}'
```

For deploying to VMware Cloud on AWS, set the folder name to the required name of *Workload*:

```
inputs:
  environment:
    type: string
    enum:
      - AWS
      - vSphere
      - Azure
      - VMC
      - GCP
    default: vSphere
resources:
  frontend:
    type: Cloud.Machine
    properties:
      folderName: '${input.environment == "VMC" ? "Workload" : ""}'
```

At deployment time, tag the machine with an all-lowercase *env* tag that matches the selected environment:

```
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)}'
```


Set the number of machines in the front-end cluster to one (small) or two (large). Note that the large cluster is set by process of elimination:

```
inputs:
  envsize:
    type: string
    enum:
      - Small
      - Large
resources:
  frontend:
    type: Cloud.Machine
    properties:
      count: '${input.envsize == "Small" ? 1 : 2}'
```

Attach machines to the same *Default* network by binding to the property found in the network resource:

```
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
```

Encrypt access credentials submitted to the API:

```
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
```

Discover the address of the API machine:

```
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}'

```

Complete cloud template

```

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)}'

```

Cloud template expression syntax in vRealize Automation Cloud Assembly

The expression syntax exposes all of the available capabilities of expressions in vRealize Automation Cloud Assembly templates.

The syntax is only partly represented in the examples shown in [How to use expressions to make cloud template code more versatile in vRealize Automation Cloud Assembly](#).

Literals

The following literals are supported:

- Boolean (true or false)
- Integer
- Floating point
- String

Backslash escapes double quote, single quote, and backslash itself:

" is escaped as \"

' is escaped as \'

\ is escaped as \\

Quotes only need to be escaped inside a string enclosed with the same type of quote, as shown in the following example.

```
"I am a \"double quoted\" string inside \"double quotes\"."
```

- Null

Environment variables

Environment names:

- orgId
- projectId
- projectName
- deploymentId
- deploymentName
- blueprintId
- blueprintVersion
- blueprintName
- requestedBy (user)
- requestedAt (time)

Syntax:

```
env.ENV_NAME
```

Example:

```
${env.blueprintId}
```

Resource variables

Resource variables let you bind to resource properties from other resources.

Syntax:

```
resource.RESOURCE_NAME.PROPERTY_NAME
```

Examples:

- `${resource.db.id}`
- `${resource.db.networks[0].address}`
- `${resource.app.id}` (Return the string for non-clustered resources, where count isn't specified. Return the array for clustered resources.)
- `${resource.app[0].id}` (Return the first entry for clustered resources.)

Resource self variables

Resource self variables are allowed only for resources supporting the allocation phase. Resource self variables are only available (or only have a value set) after the allocation phase is complete.

Syntax:

`self.property_name`

Example:

`${self.address}` (Return the address assigned during the allocation phase.)

Note that for a resource named `resource_x`, `self.property_name` and `resource.resource_x.property_name` are the same and are both considered self-references.

Cluster count index

Syntax:

`count.index`

Example:

`${count.index == 0 ? "primary" : "secondary"}` (Return the node type for clustered resources.)

Limitations:

Use of `count.index` for resource allocation is not supported. For example, the following capacity expression fails when it references the position within an array of disks created at input time.

```
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)}'
```

Conditions

Syntax:

- Equality operators are `==` and `!=`.
- Relational operators are `<` `>` `<=` and `>=`.
- Logical operators are `&&` `||` and `!`.
- Conditionals use the pattern:

condition-expression ? true-expression : false-expression

Examples:

```
${input.count < 5 && input.size == 'small'}
```

```
${input.count < 2 ? "small" : "large"}
```

Arithmetic operators

Syntax:

Operators are + - / * and %.

Example:

```
${(input.count + 5) * 2}
```

String concatenation

Syntax:

`${'ABC' + 'DEF'}` evaluates to ABCDEF.

Operators [] and .

The expression follows ECMAScript in unifying the treatment of the [] and . operators.

So, `expr.identifier` is equivalent to `expr["identifier"]`. The identifier is used to construct a literal whose value is the identifier, and then the [] operator is used with that value.

Example:

```
${resource.app.networks[0].address}
```

In addition, when a property includes a space, delimit with square brackets and double quotes instead of using dot notation.

Incorrect:

```
input.operating system
```

Correct:

```
input["operating system"]
```

Construction of map

Syntax:

```
${{'key1':'value1', 'key2':input.key2}}
```

Construction of array

Syntax:

```
${['key1','key2']}
```

Example:

```
${ [1, 2, 3] }
```

Functions

Syntax:

```
${function(arguments...)}
```

Example:

```
${to_lower(resource.app.name) }
```

Table 6-1. Functions

Function	Description
<code>abs(number)</code>	Absolute number value
<code>floor(number)</code>	Returns the largest (closest to positive infinity) value that is less than or equal to the argument and is equal to a mathematical integer
<code>ceil(number)</code>	Returns the smallest (closest to negative infinity) value that is greater than or equal to the argument and is equal to a mathematical integer
<code>to_lower(str)</code>	Convert string to lower case
<code>to_upper(str)</code>	Convert string to upper case
<code>contains(array, value)</code>	Check if array contains a value
<code>contains(string, value)</code>	Check if string contains a value
<code>join(array, delim)</code>	Join array of strings with a delimiter and return a string
<code>split(string, delim)</code>	Split string with a delimiter and return array of strings
<code>slice(array, begin, end)</code>	Return slice of array from begin index to end index
<code>reverse(array)</code>	Reverse entries of array
<code>starts_with(subject, prefix)</code>	Check if subject string starts with prefix string
<code>ends_with(subject, suffix)</code>	Check if subject string ends with suffix string
<code>replace(string, target, replacement)</code>	Replace string containing target string with target string
<code>substring(string, begin, end)</code>	Return substring of string from begin index until end index
<code>format(format, values...)</code>	Return a formatted string using Java Class Formatter format and values.
<code>keys(map)</code>	Return keys of map
<code>values(map)</code>	Return values of map
<code>merge(map, map)</code>	Return a merged map
<code>length(string)</code>	Return string length

Table 6-1. Functions (continued)

Function	Description
length(array)	Return array length
max(array)	Return maximum value from array of numbers
min(array)	Return minimum value from array of numbers
sum(array)	Return sum of all values from array of numbers
avg(array)	Return average of all values from array of numbers
digest(value, type)	Return digest of value using supported type (md5, sha1, sha256, sha384, sha512)
to_string(value)	Return string representation of the value
to_number(string)	Parse string as number
not_null(array)	Return the first entry which is not null
base64_encode(string)	Return base64 encoded value
base64_decode(string)	Return decoded base64 value
now()	Return current time in ISO-8601 format
uuid()	Return randomly generated UUID
from_json(string)	Parse json string
to_json(value)	Serialize value as json string
json_path(value, path)	Evaluate path against value using XPath for JSON .
matches(string, regex)	Check if string matches a regex expression
url_encode(string)	Encode string using url encoding specification
trim(string)	Remove leading and trailing spaces

How to enable remote access in vRealize Automation Cloud Assembly templates

To remotely access a machine that vRealize Automation Cloud Assembly has deployed, you add properties, before deployment, to the cloud template for that machine.

For remote access, you can configure one of the following authentication options.

Note In cases where keys need to be copied, you might also create a cloudConfig section in the cloud template, to automatically copy the keys upon provisioning. The specifics aren't documented here, but [How to automatically initialize a machine in a vRealize Automation Cloud Assembly template](#) provides general information about cloudConfig.

Generate a key pair at vRealize Automation Cloud Assembly provisioning time

If you don't have your own public-private key pair for remote access authentication, you can have vRealize Automation Cloud Assembly generate a key pair.

Use the following code as a guideline.

- 1 In vRealize Automation Cloud Assembly, before provisioning, add `remoteAccess` properties to the cloud template as shown in the example.

The username is optional. If you omit it, the system generates a random ID as the username.

Example:

```
type: Cloud.Machine
properties:
  name: our-vm2
  image: Linux18
  flavor: small
  remoteAccess:
    authentication: generatedPublicPrivateKey
    username: testuser
```

- 2 In vRealize Automation Cloud Assembly, provision the machine from its cloud template, and bring it to a started-up state.

The provisioning process generates the keys.

- 3 Locate the key name in the **Deployments > Topology** properties.
- 4 Use the cloud provider interface, such as the vSphere client, to access the provisioned machine command line.
- 5 Grant read permission to the private key.

```
chmod 600 key-name
```

- 6 Go to the vRealize Automation Cloud Assembly deployment, select the machine, and click **Actions > Get Private Key**.

- 7 Copy the private key file to your local machine.

A typical local file path is `/home/username/.ssh/key-name`.

- 8 Open a remote SSH session, and connect to the provisioned machine.

```
ssh -i key-name user-name@machine-ip
```

Supply your own public-private key pair to vRealize Automation Cloud Assembly

Many enterprises create and distribute their own public-private key pairs for authentication.

Use the following code as a guideline.

- 1 In your local environment, obtain or generate your public-private key pair.

For now, just generate and save the keys locally.

- 2 In vRealize Automation Cloud Assembly, before provisioning, add `remoteAccess` properties to the cloud template as shown in the example.

The `sshKey` includes the long alphanumeric found within the public key file *key-name.pub*.

The username is optional and gets created for you to log in with. If you omit it, the system generates a random ID as the username.

Example:

```
type: Cloud.Machine
properties:
  name: our-vm1
  image: Linux18
  flavor: small
  remoteAccess:
    authentication: publicPrivateKey
    sshKey: ssh-rsa Iq+5aQgBP3ZNT4o1baP5Ii+dstIcowRRkyobbfpA1mj9ts1f
    qGxvU66PX9IeZax5hZvNWFgjw6ag+Z1zndOLhVdVoW49f274/mIRi1d7Uuw...
    username: testuser
```

- 3 In vRealize Automation Cloud Assembly, provision the machine from its cloud template, and bring it to a started-up state.
- 4 Using the cloud vendor client, access the provisioned machine.
- 5 Add the public key file to the home folder on the machine. Use the key that you specified in `remoteAccess.sshKey`.
- 6 Verify that the private key file counterpart is present on your local machine.

The key is typically `/home/username/.ssh/key-name` with no `.pub` extension.

- 7 Open a remote SSH session, and connect to the provisioned machine.

```
ssh -i key-name user-name@machine-ip
```

Supply an AWS key pair to vRealize Automation Cloud Assembly

By adding an AWS key pair name to the cloud template, you can remotely access a machine that vRealize Automation Cloud Assembly deploys to AWS.

Be aware that AWS key pairs are region specific. If you provision workloads into `us-east-1`, the key pair must exist in `us-east-1`.

Use the following code as a guideline. This option works for AWS cloud zones only.

```
type: Cloud.Machine
properties:
  image: Ubuntu
  flavor: small
  remoteAccess:
```

```

authentication: keyPairName
keyPair: cas-test
constraints:
  - tag: 'cloud:aws'

```

Supply a username and password to vRealize Automation Cloud Assembly

By adding a username and password to the cloud template, you can have simple remote access to a machine that vRealize Automation Cloud Assembly deploys.

Although it is less secure, logging in remotely with a username and password might be all that your situation requires. Be aware that some cloud vendors or configurations might not support this less secure option.

- 1 In vRealize Automation Cloud Assembly, before provisioning, add `remoteAccess` properties to the cloud template as shown in the example.

Set the username and password to the account that you expect to log in with.

Example:

```

type: Cloud.Machine
properties:
  name: our-vm3
  image: Linux18
  flavor: small
  remoteAccess:
    authentication: usernamePassword
    username: testuser
    password: admin123

```

- 2 In vRealize Automation Cloud Assembly, provision the machine from its cloud template, and bring it to a started-up state.
- 3 Go to your cloud vendor's interface, and access the provisioned machine.
- 4 On the provisioned machine, create or enable the account.
- 5 From your local machine, open a remote session to the provisioned machine IP address or FQDN, and log in with the username and password as usual.

How to add advanced features to vRealize Automation Cloud Assembly designs

There are advanced infrastructure-as-code techniques and vRealize Automation Cloud Assembly features that increase the enterprise readiness of your designs.

Some features described here expand the design capabilities of vRealize Automation Cloud Assembly while others apply directly to cloud template coding practices.

How to customize the names of deployed resources using vRealize Automation Cloud Assembly

As a cloud or project administrator, you have a prescribed naming convention for resources in your environment, and you want the deployed resource to follow those conventions without user interaction. You can create a naming template for all deployments from a vRealize Automation Cloud Assembly project.

For example, your host naming convention is to prefix a resource as *projectname-sitecode-costcenter-whereDeployed-identifier*. You configure the custom naming template for the machines for each project. Some of the template variables are pulled from the system as it is deployed, other are based on project custom properties. The custom naming template for the above prefix looks similar to the following example.

```
${project.name}-${resource.siteCode}-${resource.costCenter}-${endpoint.name}-${#####}
```

The identifier, provided in the template as `${#####}`, shows a six digit identifier. The identifier is a counter that ensures uniqueness. The counter is global for the organization and increments across all projects, not only the current project. When you have multiple projects, do not expect a sequence from 000123 to 000124 for deployments in you current project. You can expect an increment from 000123 to 000127.

All resource names must be unique. Use the incremental number property to ensure uniqueness. The numbers increment for all deployments, including those that are named by vRealize Automation Cloud Assembly. As your system becomes more robust, and because the custom naming is applied to many resources, including virtual machines, load balancers, security groups, NATs, gateways, resource groups, and disks, the numbering might appear random, but the values still ensure uniqueness. The numbers also increment when you run a test deployment.

In addition to the examples provided here, you can also add the user name, the image that is used, other built-in options, and simple strings. As you build the template, hints regarding possible options are provided.

Remember that some of the values you see are only use case examples. You won't be able to use them letter-by-letter in your environment. Think about where you would make your own substitutions, or extrapolate from the example values, in order to fit your own cloud infrastructure and deployment management needs.

Prerequisites

- Verify that you know the naming convention that you want to use for deployments from a project.
- This procedure assumes you have or can create a simple cloud template that you use to test your custom host prefix naming.

Procedure

- 1 Select **Infrastructure > Projects**.

- 2 Select an existing project or create a new one.
- 3 On the **Provisioning** tab, locate the Custom Properties section and create the properties for the site code and cost center values.

This is where you replace the values you see here with ones pertinent to your environment.

Custom Properties

Specify the custom properties that should be added to all requests in this project. ⓘ

Define custom properties	Name	Value
	siteCode	BGL
	costCenter	IT-research

Custom Naming (Beta)

Specify the naming template to be used for machines provisioned in this project.

Template `${project.name}-${resource.siteCode}-${resource.costCenter}-${endpoint.name}-${#####}` ⓘ

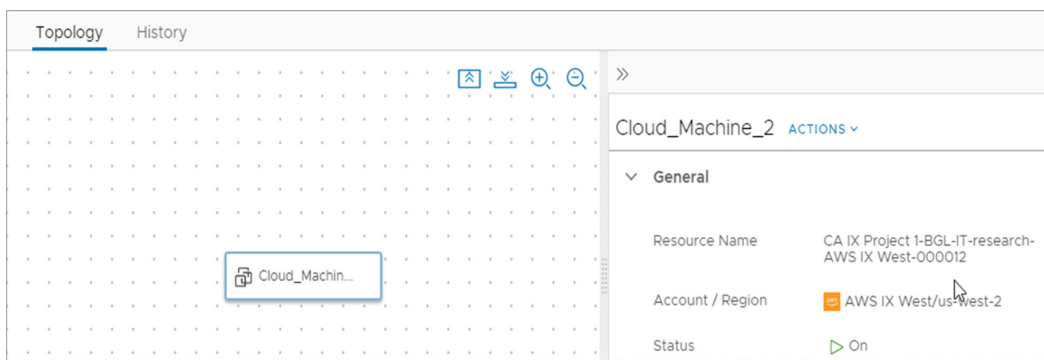
- a Create a custom property with the name **siteCode** and the value **BGL**.
- b Add another custom property with the name **costCenter** and the value **IT-research**.
- 4 Locate the Custom Naming section and add the following template.

```
${project.name}-${resource.siteCode}-${resource.costCenter}-${endpoint.name}-${#####}
```

You can copy in the string, but if this is your first naming template, consider using the hint text and quick select as you build the template.

- 5 Deploy a cloud template associated with the project to verify that the custom name is applied to the resource.
 - a Click the **Design** tab, and then click a cloud template associated with the project.
 - b Deploy the cloud template.

The **Deployments** tab opens, showing your deployment in process.
 - c When deployment is completed, click the deployment name.
 - d On the **Topology** tab, notice that your custom name is the resource name in the right pane.



- 6 If you deployed a test cloud template to verify the naming convention, you can delete the deployment.

What to do next

Create custom naming templates for your other projects.

How to automatically initialize a machine in a vRealize Automation Cloud Assembly template

You can apply machine initialization in vRealize Automation Cloud Assembly by running commands directly or, if deploying to vSphere based cloud zones, through customization specifications.

- **Commands**—a `cloudConfig` section in your cloud template code holds the commands that you want to run.
- **Customization specifications**—a property in your cloud template code references a vSphere customization specification by name.

Commands and customization specifications might not mix

When deploying to vSphere, proceed carefully if you attempt to combine `cloudConfig` and customization specification initialization. They aren't formally compatible and might produce inconsistent or unwanted results when used together.

For an example of how commands and customization specifications interact, see [vSphere static IP address assignment in vRealize Automation Cloud Assembly cloud templates](#).

vSphere customization specifications in vRealize Automation Cloud Assembly templates

When deploying to vSphere based cloud zones, customization specifications can apply guest operating system settings at deployment time.

How to enable the customization specification

The customization specification must exist in vSphere, at the target that you deploy to.

Edit the cloud template code directly. The following example points to a `cloud-assembly-linux` customization specification for a WordPress host on 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'
```

Whether to use customization specifications or cloudConfig commands

If you want the provisioning experience to match what you are currently doing in vSphere, continuing to use customization specifications might be the best approach. However, to expand to hybrid or multiple cloud provisioning, a more neutral approach is cloudConfig initialization commands.

For more about cloudConfig sections in cloud templates, see [Configuration commands in vRealize Automation Cloud Assembly templates](#).

Commands and customization specifications might not mix

When deploying to vSphere, proceed carefully if you attempt to combine embedded cloudConfig command and customization specification initialization. They aren't formally compatible and might produce inconsistent or unwanted results when used together.

For an example of how commands and customization specifications interact, see [vSphere static IP address assignment in vRealize Automation Cloud Assembly cloud templates](#).

Configuration commands in vRealize Automation Cloud Assembly templates

You can add a cloudConfig section to vRealize Automation Cloud Assembly template code, in which you add machine initialization commands that run at deployment time.

How cloudConfig commands are formed

- Linux—initialization commands follow the open [cloud-init](#) standard.
- Windows—initialization commands use [Cloudbase-init](#).

Linux [cloud-init](#) and Windows [Cloudbase-init](#) don't share the same syntax. A cloudConfig section for one operating system won't work in a machine image of the other operating system.

What cloudConfig commands can do

You use initialization commands to automate the application of data or settings at instance creation time, which can customize users, permissions, installations, or any other command-based operations. Examples include:

- Setting a hostname
- Generating and setting up SSH private keys
- Installing packages

Where cloudConfig commands can be added

You can add a cloudConfig section to cloud template code, but you can also add one to a machine image in advance, when configuring infrastructure. Then, all cloud templates that reference the source image get the same initialization.

You might have an image map and a cloud template where both contain initialization commands. At deployment time, the commands merge, and vRealize Automation Cloud Assembly runs the consolidated commands.

When the same command appears in both places but includes different parameters, only the image map command is run.

See [Learn more about image mappings in vRealize Automation](#) for additional details.

Example cloudConfig commands

The following example cloudConfig section is taken from [Create a basic cloud template](#) cloud template code for the Linux-based MySQL server.

Note To ensure correct interpretation of commands, always include the pipe character cloudConfig: | as shown.

```
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
```

If a cloud-init script behaves unexpectedly, check the captured console output in `/var/log/cloud-init-output.log` when troubleshooting. For more about cloud-init, [see the cloud-init documentation](#).

Commands and customization specifications might not mix

When deploying to vSphere, proceed carefully if you attempt to combine embedded cloudConfig command and customization specification initialization. They aren't formally compatible and might produce inconsistent or unwanted results when used together.

For an example of how commands and customization specifications interact, see [vSphere static IP address assignment in vRealize Automation Cloud Assembly cloud templates](#).

vSphere static IP address assignment in vRealize Automation Cloud Assembly cloud templates

When deploying to vSphere, you can assign a static IP address but must take care not to introduce conflicts between cloudConfig initialization commands and customization specifications.

Sample designs

The following designs safely apply a static IP address without any conflict between cloud template initialization commands and customization specifications. All contain the `assignment: static` network setting.

Design	Sample Cloud Template Code
<p>Assign a static IP address to a Linux machine that has no cloud-init code</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>Assign a static IP address to a Linux machine with cloud-init code that doesn't contain network assignment commands.</p> <p>NOTE: The vSphere customization spec is applied whether you set the <code>customizeGuestOs</code> property to <code>true</code> or omit the <code>customizeGuestOs</code> property.</p>	<p>Ubuntu sample</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 sample</p> <pre>resources: wpnet: type: Cloud.Network properties:</pre>

Design**Sample Cloud Template Code**

```
    name: wpnet
    networkType: public
    constraints:
      - tag: sqs
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	Sample Cloud Template Code
<p>Assign a static IP address to a Linux machine with cloud-init code that contains network assignment commands.</p> <p>The <code>customizeGuestOs</code> property must be <code>false</code>.</p>	<p>Ubuntu sample</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 sample</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**Sample Cloud Template Code**

```

    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}'

```

When basing the deployment on a referenced image, assign a static IP address to a Linux machine with cloud-init code that contains network assignment commands.

The `customizeGuestOs` property must be false.

In addition, the cloud template must not include the `ovfProperties` property, which blocks customization.

```

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	Sample Cloud Template Code
	<pre> 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}' </pre>

Designs that won't work or might produce unwanted results

- The cloud-init code doesn't contain network assignment commands, and the `customizeGuestOs` property is false.
Neither initialization commands nor customization spec are present to configure network settings.
- The cloud-init code doesn't contain network assignment commands, and the `ovfProperties` property is set.
Initialization commands aren't present, but `ovfProperties` blocked the customization spec.
- The cloud-init code contains network assignment commands, and the `customizeGuestOs` property is missing or set to true.
Application of the customization spec conflicts with initialization commands.

Other workarounds for cloud-init and customization specs

When deploying to vSphere, you can also customize an image to work around cloud-init and customization spec conflicts. See the following external repository for more information.

- [vSphere Image Preparation Scripts](#)

How to make a vRealize Automation Cloud Assembly deployment wait for initialization

Sometimes, a virtual machine needs to be fully started before proceeding with vRealize Automation Cloud Assembly deployment.

For example, deploying a machine that is still installing packages and starting a web server might lead to conditions where a fast user tries to reach the application before it's available.

Be aware of the following considerations when using this feature.

- The feature uses the [cloud-init](#) phone_home module and is available when deploying Linux machines.
- Phone home isn't available for Windows because of [Cloudbase-init](#) limitations.
- Phone home can affect deployment order like an explicit dependency, but has more flexibility around timing and processing options.

See [How to set the resource deployment sequence in vRealize Automation Cloud Assembly](#).

- Phone home requires a cloudConfig section in the cloud template.
- Your creativity is a factor. Initialization commands might include embedded wait time between operations, which can be used in concert with phone home.
- Cloud template-based phone home won't work if the machine template already contains phone_home module settings.
- The machine must have outbound communication access back to vRealize Automation Cloud Assembly.

To wait for machine initialization by using phone home in vRealize Automation Cloud Assembly, add a `cloudConfigSettings` section to the cloud template:

```
cloudConfigSettings:
  phoneHomeShouldWait: true
  phoneHomeTimeoutSeconds: 600
  phoneHomeFailOnTimeout: true
```

Property	Description
phoneHomeShouldWait	Whether to wait for initialization, true or false.
phoneHomeTimeoutSeconds	When to decide whether to proceed with deployment even though initialization is still running. Default is 10 minutes.
phoneHomeFailOnTimeout	Whether to proceed with deployment after timing out, true or false. Note that even when proceeding, deployment might still fail for separate reasons.

How to perform Windows guest customization

To have vRealize Automation Cloud Assembly automatically initialize a Windows machine at deployment, prepare an image that supports Cloudbase-Init, then a cloud template that contains the appropriate commands.

The image creation process varies depending on cloud vendor. The example shown here is for vSphere.

How to create an initializable Windows image for vSphere

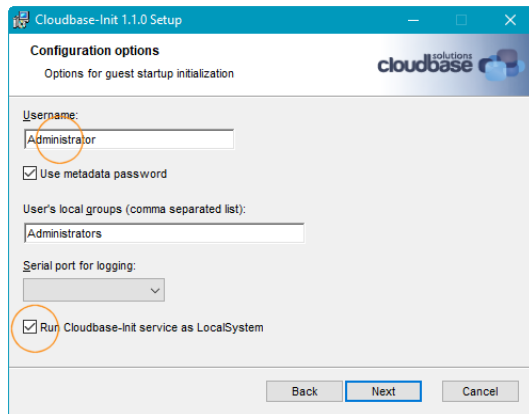
For vRealize Automation Cloud Assembly to initialize a Windows machine deployed to vSphere, it needs to be based on a template with Cloudbase-Init installed and configured.

- 1 Use vSphere to make and power on a Windows virtual machine.
- 2 On the virtual machine, log in to Windows.
- 3 Download Cloudbase-Init.

<https://cloudbase.it/cloudbase-init/#download>

- 4 Start the Cloudbase-Init setup .msi file.

During installation, enter **Administrator** as the username, and select the option to run as LocalSystem.



Other setup selections can remain as default values.

- 5 Allow the installation to run, but do not close the final Completed page of the setup wizard.

Important Do not close the final page of the setup wizard.

- 6 With the Completed page of the setup wizard still open, use Windows to navigate to the Cloudbase-Init installation path, and open the following file in a text editor.

```
conf\cloudbase-init-unattend.conf
```

- 7 Set `metadata_services` to `OvfService` as shown.

```
metadata_services=cloudbaseinit.metadata.services.ovfservice.OvfService
```


- 8 Save and close `cloudbase-init-unattend.conf`.
- 9 In the same folder, open the following file in a text editor.

```
conf\cloudbase-init.conf
```

- 10 Set `first_logon_behaviour`, `metadata_services`, and `plugins` as shown.

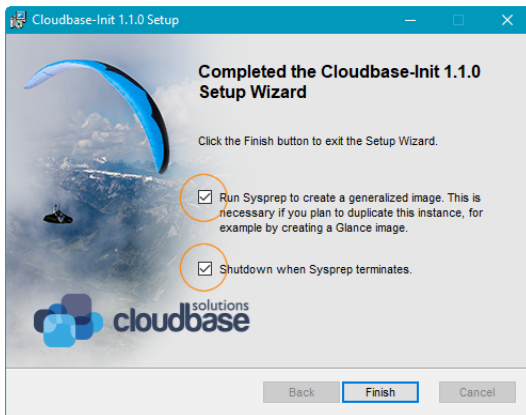
```
first_logon_behaviour=always
. . .
metadata_services=cloudbaseinit.metadata.services.ovfservice.OvfService
. . .
plugins=cloudbaseinit.plugins.windows.createuser.CreateUserPlugin,cloudbaseinit.plugins.win
dows.setuserpassword.SetUserPasswordPlugin,cloudbaseinit.plugins.common.sshpublickeys.SetUs
erSSHPublicKeysPlugin,cloudbaseinit.plugins.common.userdata.UserDataPlugin
. . .
```

- 11 Save and close `cloudbase-init.conf`.
- 12 On the Completed page of the setup wizard, select the options to run Sysprep and to shut down after Sysprep, then click **Finish**.

Note VMware has seen cases where running Sysprep prevents deployments of the image from working.

When deploying, vRealize Automation Cloud Assembly applies a dynamically generated customization specification, which disconnects the network interface. The pending Sysprep state in the image might cause the customization specification to fail and leave the deployment disconnected.

If you suspect that this is happening in your environment, try leaving the Sysprep options deactivated when creating the image.



- 13 After the virtual machine shuts down, use vSphere to turn it into a template.

Additional details

The following table expands upon the configuration entries made during setup.

Configuration Setting	Purpose
Username, CreateUserPlugin, and SetUserPasswordPlugin	After Sysprep, first boot uses CreateUserPlugin to create the username Administrator account with a blank password. SetUserPasswordPlugin allows Cloudbase-Init to change the blank password to the remote access password that will be included in the cloud template.
First Logon Behavior	This setting prompts the user to change the password upon first login.
Metadata services	By listing only OvfService, Cloudbase-Init won't try to find other metadata services that aren't supported in vCenter. This results in cleaner log files, because the logs would otherwise fill with entries about failing to find those other services.
Plugins	By listing only plugins with capabilities supported by OvfService, logs are again cleaner. Cloudbase-Init runs plugins in the order specified.
Run as LocalSystem	This setting supports any advanced initialization commands that might require Cloudbase-Init to run under a dedicated administrator account.

How to include Cloudbase-Init commands in a cloud template

To initialize a Windows machine, create infrastructure and cloud templates in vRealize Automation Cloud Assembly so that the initializable Windows image runs the commands that you want.

The example shown here is based on vSphere, but other cloud vendors should be similar.

Prerequisites

- Create infrastructure. In vRealize Automation Cloud Assembly, add your vSphere cloud account and an associated cloud zone.
- Add flavor and image mappings, and add network and storage profiles.
 In your infrastructure, an image mapping must point to the Windows template you created to support Cloudbase-Init. See [How to create an initializable Windows image for vSphere](#) .
 If the template isn't listed, go to Cloud Accounts, and synchronize images. Otherwise, automatic synchronization runs every 24 hours.
- Add a project, add users, and make sure the users can provision to your cloud zone.

For more about creating infrastructure and projects, see the examples in the [Tutorial: Setting up and testing multi-cloud infrastructure and deployments in vRealize Automation Cloud Assembly](#).

Procedure

- 1 In vRealize Automation Cloud Assembly, go to the **Design** tab, and create a new cloud template.
- 2 Add a `cloudConfig` section with the Cloudbase-init commands that you want.

The following command examples create a new file at the Windows c: drive and set the host name.

```
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
```

For more information, see the [Cloudbase-init documentation](#).

- 3 Add `remoteAccess` properties so that you configure the machine for initial login to Windows.

As mentioned when you created the template, the metadata service picks up the login credentials and exposes them to `CreateUserPlugin` and `SetUserPasswordPlugin`. Note that the password must meet Windows password requirements.

- 4 From vRealize Automation Cloud Assembly, test and deploy the cloud template.
- 5 After deploying, use Windows RDP and the credentials in the template to log in to the new Windows machine and verify the customization.

In the example above, you would look for the `C:\test.txt` file, and check the system properties for the host name.

How to create custom resource types to use in vRealize Automation Cloud Assembly cloud templates

When you create a cloud template in vRealize Automation Cloud Assembly, the resource type palette includes resource types for the supported cloud account and integration endpoints. You might have use cases where you want to create cloud templates based on an expanded list of resource types. You can create custom resources, add them to the design canvas, and create cloud templates that support your design and deployment needs.

Use vRealize Orchestrator to create custom resources

Each custom resource is based on a vRealize Orchestrator SDK inventory type and is created by a vRealize Orchestrator workflow that has an output which is an instance of your desired SDK type. Primitive types, such as `Properties`, `Date`, `string`, and `number` are not supported for the creation of custom resources.

Note SDK object types can be differentiated from other property types by the colon (":") used to separate the plug-in name and the type name. For example, `AD:UserGroup` is a SDK object type used to manage Active Directory user groups.

You can use the built-in workflows in vRealize Orchestrator, or you can create your own. Using vRealize Orchestrator to create anything-as-a-service/XaaS workflows means that you can create a cloud template that adds an Active Directory user to machines at deployment time, or add a custom F5 load balancer to a deployment.

Custom resource name and resource type

The custom resource name identifies your custom resource inside the cloud template resource type palette.

The resource type of a custom resource must begin with **Custom.** and each resource type must be unique. For example, you might set `Custom.ADUser` as a resource type for a custom resource that adds Active Directory users. Although the inclusion of **Custom.** is not validated in the text box, the string is automatically added if you remove it.

External type

The external type property defines the type of your custom resource. When you select a Create workflow in your custom resource in vRealize Automation Cloud Assembly, the external type drop-down appears underneath it. The drop-down includes external type properties, that are selected from the output parameters of the vRealize Orchestrator workflow. The selected workflow output properties included in the drop-down must be non-array SDK object types such as `VC:VirtualMachine` or `AD:UserGroup`.

Note When creating custom workflows that use the dynamic type plug-in, verify that their variables are created by using the `DynamicTypesManager.getObject()` method.

When you define your custom resources, you also define the scope of the availability of the select external type. The selected external type can be:

- Shared across projects.
- Available only for the selected project.

You can only have one external type per defined scope. For example, if you create a custom resource in your project, that uses `VC:VirtualMachine` as an external type, you cannot create another custom resource for the same project that uses the same external type. You also cannot create two shared custom resources that use the same external type.

Workflow input/output validation

When you add Create, Delete, and Update workflows as lifecycle actions to your custom resource, vRealize Automation Cloud Assembly validates that the selected workflows have correct input and output property definitions.

- The Create workflow must have an output parameter that is an SDK object type, such as `SSH:Host` or `SQL:Database`. If the selected workflow does not pass the validation, you cannot add Update or Delete workflows, or save your changes to the custom resource.
- The Delete workflow must have an input parameter that is an SDK object type that matches the external type of the custom resource.
- The Update workflow must have both an input and output parameter that is an SDK object type that matches the external type of the custom resource.

Custom resource property schema

When you add vRealize Orchestrator workflows to your custom resource, their input and output parameters are added as properties. You can view the custom resource properties schema by selecting the **Properties** tab. The schema includes the name, data type, property type, and, if it is available, the description of a given property. The schema also defines if a given property is required or optional.

How do I create a cloud template in vRealize Automation Cloud Assembly that adds users to Active Directory

In addition to the vRealize Automation Cloud Assembly cloud template resources that you use when you create cloud templates, you can also create your own custom resources.

Custom resources are vRealize Orchestrator objects that you manage through vRealize Automation with the defined main resource operation workflows. The cloud template service automatically call up the appropriate vRealize Orchestrator workflows when a create or delete operation is triggered. You can extend the functionality of the resource type by also selecting vRealize Orchestrator workflows that can be used as day 2 operations.

This use case uses built-in workflows that are provided in the vRealize Orchestrator library. It includes prescriptive values or strings to demonstrate how to perform the process. You can modify them to suit your environment.

For reference purposes, this use case uses a project named **DevOpsTesting**. You can replace this sample project with any project in your environment.

Prerequisites

- Verify that you configured a vRealize Orchestrator integration. See [Configure vRealize Orchestrator integration in Cloud Assembly](#).
- Verify that the workflows that you are using for the create, update, destroy, and day 2 actions exist in vRealize Orchestrator and run successfully from there.

- In vRealize Orchestrator, locate the resource type used by the workflows. The workflows included in this custom resource must all use the same resource type. In this use case, the resource type is `AD:User`. For more information on resource type validation, see [How to create custom resource types to use in vRealize Automation Cloud Assembly cloud templates](#).
- By using the built-in Active Directory workflows in your vRealize Orchestrator integration, configure an Active Directory server.
- Verify that you know how to configure and deploy a machine cloud template.

Procedure

- 1 Create an Active Directory custom resource for adding a user in a group.

This step adds the custom resource to the cloud template design canvas as a resources type.

- a In vRealize Automation Cloud Assembly, select **Design > Custom Resources**, and click **New Custom Resource**.
- b Provide the following values.

Remember, except for the workflow names, these are sample values.

Setting	Sample Value
Name	AD user This is the name that appears in the cloud template resource type palette.
Resource Type	Custom.ADUser The resource type must begin with Custom. and each resource type must be unique. Although the inclusion of Custom. is not validated in the text box, the string is automatically added if you remove it. This resource type is added to the resource type palette so that you can use it in the cloud template.

- c To enable this resource type in the cloud template resource type list, verify that **Activate** option is toggled on.
- d Select the **Scope** setting that makes the resource type available to any project.

- e Select the workflows that define the resource and the day 2 actions.

Note The selected day 2 workflows must have an input parameter that is of the same type as the external type. The external type input is not displayed in the day 2 custom form requested by the user, as it is automatically bound to the custom resource.

Setting	Sample Value
Lifecycle Actions - Create	<p>Select the Create a user with a password in an organizational unit workflow.</p> <p>If you have multiple vRealize Orchestrator integrations, select the workflow on the integration instance you use to run these custom resources.</p> <p>After selecting the workflow, the external type drop-down menu becomes available and is automatically set to <code>AD:User</code>.</p> <p>Note An external source type can be used only once if shared and once per project. In this use case, you are providing the same custom resource for all the projects. It does mean that you cannot use <code>AD:User</code> for any other resource types for all projects. If you have other workflows that require the <code>AD:User</code> type, you must create individual custom resources for each project.</p>
Lifecycle Actions - Destroy	Select the Destroy a user workflow.
Additional Actions	<p>Select the Change a user password workflow.</p> <p>To modify the action request form that the user responds to when they request the action, click the icon in the Request Parameters column.</p> <p>Note For additional action workflows, verify that the workflow has a input parameter that is of the same type as the external type.</p>

In this example, there is no appropriate application of an update workflow. A common example of an update workflow, which makes changes to the provisioned custom resource, is scaling in or scaling out a deployment.

- f Review the schema key and type values in the **Properties** tab so that you understand the workflow inputs so that you can configure the inputs in the cloud template.

The schema lists the required and optional input values defined in the workflow. The required input values are included in the cloud template YAML.

In the Create a user workflow, `accountName`, `displayName`, and `ouContainer` are required input values. The other schema properties are not required. You can also use the schema to determine where you want to create bindings to other field values, workflows, or actions. Bindings are not included in this use case.

- g To finish creating your custom resource, click **Create**.

- 2 Create a cloud template that adds the user to a machine when you deploy it.
 - a Select **Design > Cloud Templates**, and click **New from > Blank canvas**.
 - b Name the cloud template **Machine with an AD user**.
 - c Select the **DevOpsTesting** project, and click **Create**.
 - d Add and configure a vSphere machine.
 - e From the custom resource list on the left of the cloud template design page, drag the **AD user** resource type onto the canvas.

Note You can select the custom resource by either scrolling down and selecting it from the left pane, or searching for it in the **Search Resource Types** text box. If the custom resource does not appear, click the refresh button next to the **Search Resource Types** text box.

- f On the right, edit the YAML code to add the mandatory input values and the password.

Add an `inputs` section in the code so that users can provide the name of the users that they are adding. In the following example, some of these values are sample data. Your values might be different.

```
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 In the `resources` section, add `${input.input-name}` code to prompt for the user selection.

```
resources:
  Custom_ADUser_1:
    type: Custom.ADUser
    properties:
      accountName: '${input.accountName}'
      displayName: '${input.displayName}'
      ouContainer: '${input.ouContainer}'
      password: '${input.password}'
      confirmPassword: '${input.confirmPassword}'
```

3 Deploy the cloud template.

- a On the cloud template designer page, click **Deploy**.
- b Enter the **Deployment Name AD User Scott**.
- c Select the **Cloud Template Version** and click **Next**.

- d Complete the deployment inputs.
 - e Click **Deploy**.
- 4 Monitor the provisioning process to ensure that the user is added to Active Directory.
- a Click **Deployments** and locate your **AD User Scott** deployment.
 - b Monitor the status of the request and verify the successful deployment.
 - c Verify that the change password action is available and working.

What to do next

When your tested cloud template is working, you can then begin using the **AD user** custom resource with other cloud templates.

How do I create a cloud template in Cloud Assembly that includes SSH

You can create custom resources that you can use to build cloud templates using vRealize Orchestrator workflows. In this use case, you add a custom resource that adds an SSH host. You can then include the resource in cloud templates. This procedure also adds an update workflow so that users change the SSH configuration after deployment rather than perform individual day 2 actions.

Custom resources are vRealize Orchestrator objects that you manage through vRealize Automation with the defined main resource operation workflows. The cloud template service automatically call up the appropriate vRealize Orchestrator workflows when a create or delete operation is triggered. You can extend the functionality of the resource type by also selecting vRealize Orchestrator workflows that can be used as day 2 operations.

This use case uses built-in workflows provided in the vRealize Orchestrator library. It includes prescriptive values or strings to demonstrate how to perform the process. You can modify them to suit your environment.

For reference purposes, this use case uses a project named **DevOpsTesting**. You can replace the project with one that you already have.

Prerequisites

- Verify that you configured a vRealize Orchestrator integration. See [Configure vRealize Orchestrator integration in Cloud Assembly](#).
- Verify that the workflows that you are using for the create, update, destroy, and day 2 actions exist in vRealize Orchestrator and run successfully from there.
- In vRealize Orchestrator, locate the resource type used by the workflows. The workflows included in this custom resource must all use the same resource type. In this use case, the resource type is `SSH:Host`. For more information on resource type validation, see [How to create custom resource types to use in vRealize Automation Cloud Assembly cloud templates](#).
- Verify that you know how to configure and deploy a machine cloud template.

Procedure

- 1 Create an SSH host custom resource for adding SSH to a cloud template.

This step adds the custom resource to the cloud template design canvas as a resource type.

- a In vRealize Automation Cloud Assembly, select **Design > Custom Resources**, and click **New Custom Resource**.
- b Provide the following values.

Remember, except for the workflow names, these are sample values.

Table 6-2.

Setting	Sample Value
Name	SSH Host - DevOpsTesting Project This is the name that appears in the cloud template resource type palette.
Resource Type	Custom.SSHHost The resource type must begin Custom. and each resource type must be unique. Although the inclusion of Custom. is not validated in the text box, the string is automatically added if you remove it. This resource type is added to the design canvas so that you can use it in the cloud template.

- c To enable this resource type in the cloud template resource type list, verify that **Activate** option is toggled on.
- d Select the **Scope** setting that makes the resource type available to the **DevOpsTesting** project.
- e Select the workflows that define the resource.

Setting	Setting
Lifecycle Actions - Create	Select the Add SSH Host workflow. If you have multiple vRealize Orchestrator integrations, select the workflow on the integration instance you use to run these custom resources. After select the workflow, the external type drop-down menu becomes available and is automatically set to SSH:Host . An external source type can be used only once if share and once per project. In this use case, you are providing the custom resource for only the DevOpsTesting project. If you had other workflows that require the SSH:Host type, you must create individual custom resources for each project.
Lifecycle Actions - Update	Select the Update SSH Host workflow.
Lifecycle Actions - Destroy	Select the Remove SSH Host workflow.

- f Review the schema key and type values in the **Properties** tab so that you understand the workflow inputs so that you can configure the inputs in the cloud template.

The schema lists the required and optional input values defined in the workflow. The required input values are included in the cloud template YAML.

In the **Add SSH Host** workflow, `hostname`, `port`, and `username` are required input values. The other schema properties are not required. You can also use the schema to determine where you want to create bindings to other field values, workflows, or actions. Bindings are not included in this use case.

- g To finish creating your custom resource, click **Create**.

2 Create a cloud template that adds the SSH host when you deploy it.

- a Select **Design > Cloud Templates**, and click **New from > Blank canvas**.
- b Name the cloud template **Machine with SSH Host**.
- c Select the **DevOpsTesting** project, and click **Create**.
- d Add and configure a vSphere machine.
- e From the custom resource list on the left of the cloud template design page, drag the **SSH Host - DevOpsTesting Project** resource type onto the canvas.

Note You can select the custom resource by either scrolling down and selecting it from the left pane, or searching for it in the **Search Resource Types** text box. If the custom resource does not appear, click the refresh button next to the **Search Resource Types** text box.

A reminder that the resource type is available because it was configured for the project. If you were creating a cloud template for another project, you cannot see the resource type.

- f On the right, edit the YAML code to add the mandatory input values.

Add an `inputs` section in the code so that users can provide the user name and the host name at deployment time. In this example, the port default is 22. In the following example, some of these values are sample data. Your values might be different.

```
inputs:
  hostname:
    type: string
    title: The hostname of the SSH Host
  username:
    type: string
    title: Username
```

- g In the `resources` section, add `${input.input-name}` code to prompt for the user selection.

```
resources:
  Custom_SSHTest_1:
    type: Custom.SSHTest
    properties:
      port: 22
      hostname: '${input.hostname}'
      username: '${input.username}'
```

- 3 Deploy the cloud template.
 - a On the cloud template designer page, click **Deploy**.
 - b Enter the **Deployment Name SSH Host Test**.
 - c Select the **Cloud Template Version** and click **Next**.
 - d Complete the deployment inputs.
 - e Click **Deploy**.
- 4 Monitor the provisioning process to ensure that the SSH host is included in the deployment.
 - a Click **Deployments** and locate your **SSH Host Test** deployment.
 - b Monitor the status of the request and verify the successful deployment.

What to do next

When your tested cloud template is working, you can then begin using the `SSH Host` custom resource with other cloud templates.

How to design in vRealize Automation Cloud Assembly to prepare for day 2 changes

In addition to the day 2 actions already associated with vRealize Automation Cloud Assembly resource types, you have design options that let you prepare in advance for custom updates that users might need to make.

Caution To change a deployment, you can edit its cloud template and reapply it, or you can use day 2 actions. However, in most cases you should avoid mixing the two approaches.

Lifecycle day 2 changes such as power on/off are usually safe, but others require caution, such as when adding disks.

For example, if you add disks with a day 2 action, and then take a mixed approach by reapplying the cloud template, the cloud template could overwrite the day 2 change, which might remove disks and cause data loss.

Day 2 preparation can involve either direct use of cloud template code, or the vRealize Automation Cloud Assembly design interface.

- You can use inputs in cloud template code so that, when you update the deployment or deployed resource, the interface prompts for fresh values.
- You can use vRealize Automation Cloud Assembly to design a custom action based on a vRealize Orchestrator workflow or action. Running the custom action results in vRealize Orchestrator making changes to the deployment or deployed resource.

How to use cloud template inputs for vRealize Automation day 2 updates

When designing cloud templates, vRealize Automation input parameters allow day 2 users to re-enter selections from the initial deployment request.

Caution Some property changes cause a resource to be re-created. For example, changing the `connection_string.name` under a `Cloud.Service.Azure.App.Service` deletes the existing resource and creates a new one.

When designing inputs to support day 2 changes, decide whether to allow inputs that delete and re-create resources. To learn which properties re-create a resource, follow the schema link at [What are the vRealize Automation resource properties](#) .

For information on how to create inputs, see [How user input can customize a cloud template in vRealize Automation](#).

For a specific day 2 example, see the following section.

How to move a deployed machine to another network

While maintaining deployments and networks, you might need the ability to relocate machines that you deployed with vRealize Automation Cloud Assembly.

For example, you might deploy to a test network first, then move to a production network. The technique described here lets you design a cloud template in advance to prepare for such day 2 actions. Note that the machine is moved. It isn't deleted and redeployed.

This procedure only applies to **Cloud.vSphere.Machine** resources. It won't work for cloud agnostic machines deployed to vSphere.

Prerequisites

- The vRealize Automation Cloud Assembly network profile must include all subnets that the machine will connect to. In vRealize Automation Cloud Assembly, you can check networks by going to **Infrastructure > Configure > Network Profiles**.

The network profile must be in an account and region that are part of the appropriate vRealize Automation Cloud Assembly project for your users.

- Tag the two subnets with different tags. The example that follows assumes that **test** and **prod** are the tag names.
- The deployed machine must keep the same IP assignment type. It can't change from static to DHCP, or vice versa, while moving to another network.

Procedure

- 1 In vRealize Automation Cloud Assembly, go to **Design**, and create a cloud template for the deployment.
- 2 In the inputs section of the code, add an entry that lets the user select a network.

```
inputs:
  net-tagging:
    type: string
    enum:
      - test
      - prod
    title: Select a network
```

- 3 In the resources section of the code, add the **Cloud.Network** and connect the vSphere machine to it.
- 4 Under the **Cloud.Network**, create a constraint that references the selection from the inputs.

```
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 Continue with your design, and deploy it as you normally would. At deployment, the interface prompts you to select the **test** or **prod** network.
- 6 When you need to make a day 2 change, go to **Deployments**, and locate the deployment associated with the cloud template.
- 7 To the right of the deployment, click **Actions > Update**.
- 8 In the Update panel, the interface prompts you the same way, to select the **test** or **prod** network.
- 9 To change networks, make your selection, click **Next**, and click **Submit**.

How to create a vRealize Automation Cloud Assembly custom action to vMotion a virtual machine

After you deploy a cloud template, you can run day 2 actions that change the deployment. vRealize Automation Cloud Assembly includes many day 2 actions, but you might want to provide others. You can create custom resource actions and make them available to users as day 2 actions.

The custom resource actions are based on vRealize Orchestrator workflows.

This example of a custom day 2 action is meant to introduce you to the creation process. To use custom actions effectively, you must be able to create vRealize Orchestrator workflows and actions that run the tasks you need.

Prerequisites

- Verify that you configured a vRealize Orchestrator integration. See [Configure vRealize Orchestrator integration in Cloud Assembly](#).
- Verify that the workflow that you are using for the day 2 action exists in vRealize Orchestrator and runs successfully there.

Procedure

- 1 Create a custom resource action that uses vMotion to move a vSphere virtual machine from one host to another.
 - a In vRealize Automation Cloud Assembly, select **Design > Resource Actions**, and click **New Resource Action**.
 - b Provide the following values.

Remember, except for the workflow names, these are sample values.

Setting	Sample Value
Name	vSphere_VM_vMotion This is the name that appears in the resource actions list.
Display name	Move VM This is the name that users see in the deployment actions menu.

- c Click the **Activate** option to enable this action in the day 2 actions menu for resources that matches the resource type.
 - d Select the resource type and workflow that define the day 2 action.

Setting	Sample Value
Resource Type	Select the Cloud.vSphere.Machine resource type. This is the resource type that is deployed as a cloud template component, not necessarily what is in the cloud template. For example, you might have a cloud agnostic machine in your cloud template, but when it is deployed on a vCenter Server, the machine is Cloud.vSphere.Machine . Because the action applies to the deployed type, do not use cloud agnostic types when you define your custom actions. In this example, vMotion only works for vSphere machines, but you might have other actions that you want to run on multiple resource types. You must create an action for each resource type.
Workflow	Select the Migrate virtual machine with vMotion workflow. If you have multiple vRealize Orchestrator integrations, select the workflow on the integration instance you use to run these custom resource actions.

- 2 Create a binding for the vRealize Orchestrator properties to the vRealize Automation Cloud Assembly schema properties. vRealize Automation Cloud Assembly day 2 actions support three types of bindings.

Binding type	Description
in request	The default value binding type. When selected, the input property is displayed in the request form and its value must be provided by the user at the request time.
with binding action	<p>This option is available only for reference type inputs such as:</p> <ul style="list-style-type: none"> ■ VC:VirtualMachine ■ VC:Folder <p>The user selects an action that performs the binding. The selected action must return the same type as the input parameter. The correct property definition is <code>{properties.someProperty}</code>.</p>
direct	This option is available for input properties that use primitive data types. When selected, the property, with the suitable type, is mapped directly from the schema of the input property. The user selects the property from the schema tree. Properties with different types are disabled.

In this use case, the binding is a vRealize Orchestrator action that makes the connection between vRealize Orchestrator `VC:VirtualMachine` input type used in the workflow and the vRealize Automation Cloud Assembly `Cloud.vSphere.Machine` resource type. By setting up the binding, you make the day 2 action seamless for the user requesting the vMotion action on a vSphere VM machine. The system provides the name in the workflow so that the user does not have to do it.

- a After selecting the **Migrate virtual machine with vMotion** workflow, navigate to the **Property Binding** pane.
 - b Select the binding of the `vm` input property.
 - c Under **Binding**, select **with binding action**.

The **findVcVmByVcAndVmUuid** action is automatically selected. This action comes preconfigured with your vRealize Orchestrator integration in vRealize Automation Cloud Assembly.
 - d Click **Save**.
- 3 To save the changes to your day 2 action, click **Create**.

- 4 To account for the other input parameters in the workflow, you can customize the request form that users see when they request the action.

- a From **Resource Actions**, select your recently created day 2 action.
- b Click **Edit Request Parameters**.

You can customize how the request page is presented to users.

Default Field Name	Appearance	Values	Constraints
Destination resource pool for the virtual machine. Default is the current resource pool.	<ul style="list-style-type: none"> Label = Target resource pool Display type = Value Picker 		
Destination host to which to migrate the virtual machine	<ul style="list-style-type: none"> Label = Target host Display type = Value Picker 		Required = Yes
Priority of the migration task	Label = Priority of the task	Value options <ul style="list-style-type: none"> Value source = Constant In the text box, enter a comma-separated list. <div> lowPriority Low,defaultPriority Default,highPriority High </div>	Required = Yes
(Optional) Only migrate the virtual machine if its power on state matches the specified state	Delete this text box. vMotion can move machines in any power state.		

- c Click **Save**.
- 5 To limit when the action is available, you can configure the conditions.

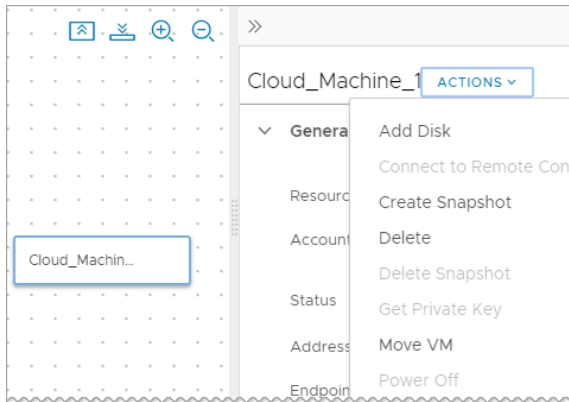
For example, you only want the vMotion action to be available when the machine has four or fewer CPUs.

- a Toggle on **Requires condition**.
- b Enter the condition.

Key	Operator	Value
\${properties.cpuCount}	lessThan	4

- c Click **Update**.

- 6 Verify that the Move VM action is available for deployed machines that match the criteria.
 - a Select **Deployments**.
 - b Locate a deployment that includes a deployed machine that matches the defined criteria.
 - c Open the deployment and select the machine.
 - d Click actions in the right pane and verify that the `Move VM` action exists.



- e Run the action.

How to extend and automate application life cycles with extensibility

You can extend your application life cycles by using either extensibility actions or vRealize Orchestrator workflows with extensibility subscriptions.

With vRealize Automation Cloud Assembly Extensibility, you can assign an extensibility action or vRealize Orchestrator workflow to an event by using subscriptions. When the specified event occurs, the subscription initiates the action or workflow to run, and all subscribers are notified.

Extensibility Actions

Extensibility actions are small, lightweight scripts of code used to specify an action and how that action is to perform. You can import extensibility actions from pre-defined vRealize Automation Cloud Assembly action templates or from a ZIP file. You can also use the action editor to create custom scripts for your extensibility actions. When multiple action scripts are linked together in one script, you create an action flow. By using action flows, you can create a sequence of actions. For information on using action flows, see [What is an action flow](#).

vRealize Orchestrator Workflows

By integrating vRealize Automation Cloud Assembly with your existing vRealize Orchestrator environment, you can use workflows in your extensibility subscriptions.

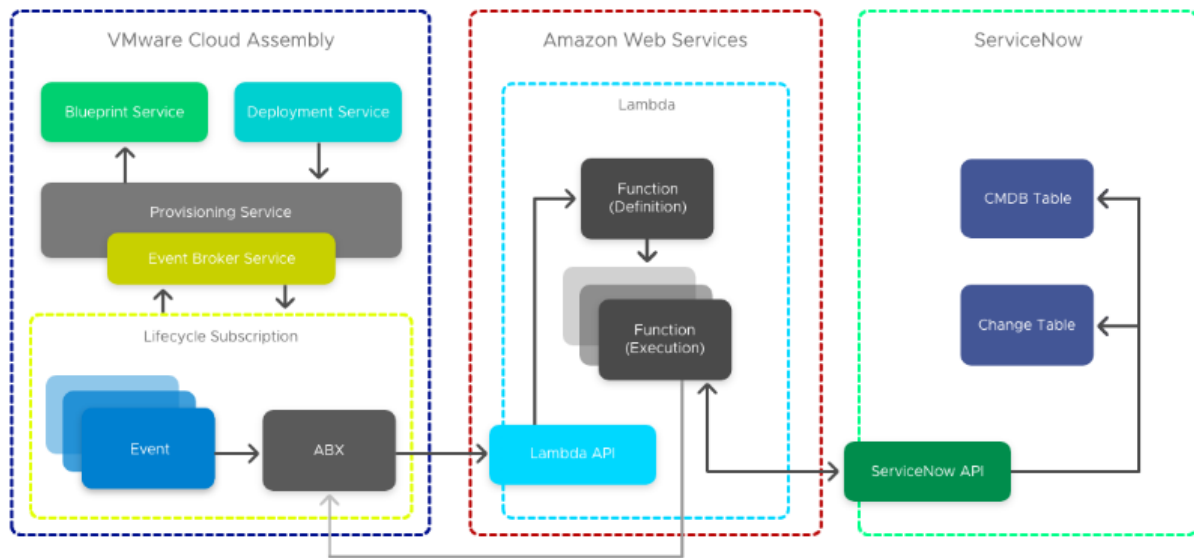
Extensibility action subscriptions

You can assign an extensibility action to a vRealize Automation Cloud Assembly subscription to extend your application life cycle.

Note The following subscriptions are use case examples and do not cover all extensibility action functionality.

How do I integrate Cloud Assembly with ServiceNow using extensibility actions

Using extensibility actions you can integrate vRealize Automation Cloud Assembly with an Enterprise ITSM, like ServiceNow.

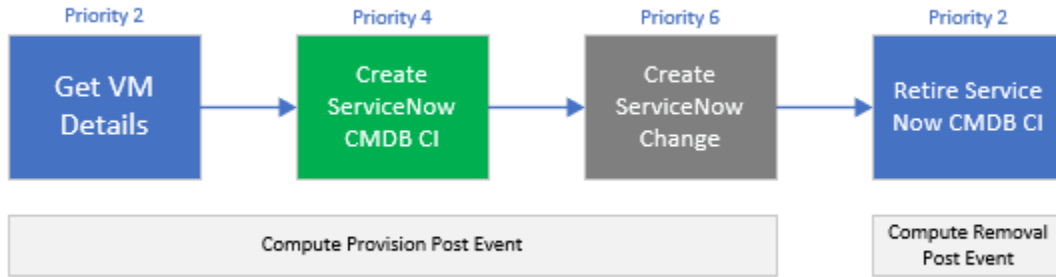


Enterprise users commonly integrate their Cloud Management Platform with an IT Service Management (ITSM) and Configuration Management Database (CMDB) platform for compliance. Following this example, you can integrate vRealize Automation Cloud Assembly with ServiceNow for CMDB and ITSM by using extensibility action scripts.

Note You can also integrate ServiceNow with vRealize Automation Cloud Assembly by using vRealize Orchestrator workflows. For information about integrating ServiceNow by using workflows, see [How do I integrate Cloud Assembly for ITSM with ServiceNow using vRealize Orchestrator workflows](#).

To create this integration, you use four extensibility action scripts. The first three scripts are initiated in sequence during provisioning, at the compute provision post event. The fourth script triggers at the compute removal post event.

For more information on event topics, refer to [Event topics provided with vRealize Automation Cloud Assembly](#).



Get VM Details

The Get VM details script acquires additional payload details required for CI creation and an identity token that is stored in Amazon Web Services Systems Manager Parameter Store (SSM). Also, this script updates `customProperties` with additional properties for later use.

Create ServiceNow CMDB CI

The Create ServiceNow CMDB CI script passes the ServiceNow instance URL as an input and stores the instance in SSM to meet security requirements. This script also reads the ServiceNow CMDB unique record identifier response (`sys_id`). It passes it as an output and writes the custom property `serviceNowSysId` during creation. This value is used to mark the CI as retired when the instance is destroyed.

Note Additional permissions might need to be allocated to your vRealize Automation services Amazon Web Services role to allow Lambda to access the SSM Parameter Store.

Create ServiceNow Change

This script finishes the ITSM integration by passing the ServiceNow instance URL as an input and storing the ServiceNow credentials as SSM to meet security requirements.

Create ServiceNow Change

The retire ServiceNow CMDB CI script prompts the ServiceNow to stop and marks the CI as retired based on the custom property `serviceNowSysId` that was created in the creation script.

Prerequisites

- Before configuring this integration, filter all event subscriptions with the conditional cloud template property: `event.data["customProperties"]["enable_servicenow"] === "true"`

Note This property exists on cloud templates that require a ServiceNow integration.

- Download and install Python.

For more information on filtering subscriptions, see [.Create an extensibility subscription.](#)

Procedure

- 1 Open a command-line prompt from your Virtual Machine.
- 2 Run the Get VM details script.

```

from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):
    baseUri = inputs['url']
    casToken = client.get_parameter(Name="casToken",WithDecryption=True)

    url = baseUri + "/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 = baseUri + "/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 Run the CMDB configuration item creation action.

```

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 Run the Creation action script.

```

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)

```

Results

vRealize Automation Cloud Assembly is successfully integrated with ITSM ServiceNow.

What to do next

When desired, you can retire your CI by using the CMDB configuration item retire action:

```

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)

```

For more information on how you can use extensibility actions to integrate ServiceNow in vRealize Automation Cloud Assembly, see [Extending Cloud Assembly with Action Based Extensibility for ServiceNow Integration](#).

How do I tag virtual machines during provisioning by using extensibility actions

You can use extensibility actions along with subscriptions to automate and simplify tagging VMs.

As a cloud administrator, you can create deployments that are automatically tagged with specified inputs and outputs by using extensibility actions and extensibility subscriptions. When a new deployment is created against the project containing the tag VM subscription, the deployment event triggers the Tag VM script to run and the tags are automatically applied. This saves time and promotes efficiency while allowing for easier deployment management.

Prerequisites

- Access to cloud administrator credentials.
- Amazon Web Services role for Lambda functions.

Procedure

- 1 Navigate to **Extensibility > Library > Actions > New Action** and create an action with the following parameters.

Parameter	Description
Action Name	Extensibility action name, preferably with TagVM as a prefix or suffix.
Project	Project to test the extensibility action against.
Action Template	Tag VM
Runtime	Python
Script Source	Write Script

- 2 Enter **Handler** as the **Main function**.
- 3 Add tagging inputs for testing the extensibility action.
For example, `resourceNames = ["DB_VM"]` and `target = world`.
- 4 To save your action, click **Save**.
- 5 To test your action, click **Test**.
- 6 To exit the action editor, click **Close**.
- 7 Navigate to **Extensibility > Subscriptions**.
- 8 Click **New Subscription**.

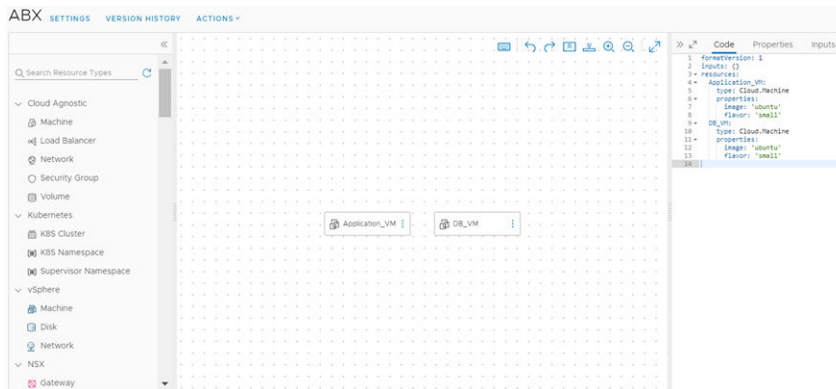
9 Enter the following subscription details.

Detail	Setting
Event Topic	Select an event topic related to the tagging phase of the VM. For example, Compute Allocation. Note Tags must be part of the event parameters of the selected event topic.
Blocking	Set the timeout for the subscription to 1 minute.
Action/Workflow	Select an extensibility action runnable type, and select your custom extensibility action.

10 To save your custom extensibility action subscription, click **Save**.

11 Navigate to **Design > Cloud Templates**, and create a cloud template from a blank canvas.

12 Add two virtual machines to the cloud template: `Application_VM` and `DB_VM`.



13 To deploy the VMs, click **Deploy**.

14 During deployment, verify that the event is initiated and the extensibility action is run.

15 To verify that the tags were applied correctly, navigate to **Infrastructure > Resources > Machines**.

Learn more about extensibility actions

Action-based extensibility uses streamlined scripts of code within vRealize Automation Cloud Assembly to automate extensibility actions.

Action-based extensibility provides a lightweight and flexible run-time engine interface where you can define small scriptable actions and configure them to initiate when events specified in extensibility subscriptions occur.

You can create these extensibility action scripts of code within vRealize Automation Cloud Assembly, or on your local environment, and assign them to subscriptions. Extensibility action scripts are used for more lightweight and simple automation of tasks and steps. For more information on integrating vRealize Automation Cloud Assembly with a vRealize Orchestrator server, see [Configure vRealize Orchestrator integration in Cloud Assembly](#).

Action-based extensibility provides:

- An alternative to vRealize Orchestrator workflows, using small and reusable scriptable actions, for lightweight integrations and customizations.
- A way to reuse action templates, which contain reusable parameterized actions.

You can create extensibility actions by either writing a user-defined action script code or importing a predefined script code as a .ZIP package. Action-based extensibility supports Node.js, Python, and PowerShell run-time environments. The Node.js and Python run-times rely on Amazon Web Services Lambda. Therefore, you must have an active subscription with Amazon Web Services Identity and Access Management (IAM), and configure Amazon Web Services as an endpoint in vRealize Automation Cloud Assembly. For information on getting started with Amazon Web Services Lambda, see [ABX: Serverless Extensibility of Cloud Assembly Services](#).

Note Extensibility actions are project-specific.

How do I create extensibility actions

With vRealize Automation Cloud Assembly, you can create extensibility actions for use in extensibility subscriptions.

Extensibility actions are highly customizable, lightweight, and flexible ways to extend application life cycles by using user-defined script code and action templates. Action templates contain predefined parameters that help set up the foundation of your extensibility action.

There are two methods of creating an extensibility action:

- Writing user-defined code for an extensibility action script.

Note Writing user-defined code in the extensibility action editor might require an active Internet connection.

- Importing a deployment package as a ZIP package for an extensibility action. For information on creating a ZIP package for extensibility actions, see [Create a ZIP package for Python runtime extensibility actions](#), [Create a ZIP package for Node.js runtime extensibility actions](#), or [Create a ZIP package for PowerShell runtime extensibility actions](#).

The following steps describe the procedure for creating an extensibility action that uses Amazon Web Services as a FaaS provider.

Prerequisites

- Membership in an active and valid project.
- Configured Amazon Web Services role for Lambda functions. For example, `AWSLambdaBasicExecutionRole`.
- Cloud administrator role or `iam:PassRole` permissions enabled.

Procedure

- 1 Select **Extensibility > Library > Actions**.

- 2 Click **New Action**.
- 3 Enter a name for your action and select a project.
- 4 Click **Next**.
- 5 Search and select an action template.

Note To create a custom action without using an action template, select **Custom Script**.

New configurable parameters appear.

- 6 Select **Write script** or **Import package**.
- 7 Select the action runtime.
- 8 Enter an **Main function** name for the action's entry point.

Note For actions imported from a ZIP package, the main function must also include the name of the script file that contains the entry point. For example, if your main script file is titled `main.py` and your entry point is `handler (context, inputs)`, the name of the main function must be *main.handler*.

- 9 Define the **Input** and **Output** parameters of the action.
- 10 (Optional) Add application dependencies to the action.

Note For PowerShell scripts, you can define your application dependencies so they are resolved against the PowerShell Gallery repository. To define your application dependencies so, they are resolvable from the public repository use the following format:

```
@{  
    Name = 'Version'  
}  
  
e.g.  
  
@{  
    Pester = '4.3.1'  
}
```

Note For actions imported from a ZIP package, application dependencies are added automatically.

- 11 To define timeout and memory limits, enable the **Set custom timeout and limits** option.
- 12 To test your action, click **Save** and then **Test**.

What to do next

After your extensibility action is created and verified, you can assign it to a subscription.

Note Extensibility subscriptions use the latest released version of an extensibility action. After creating a new version of an action, click **Versions** on the top-right of the editor window. To release the version of the action you want to use in your subscription, click **Release**.

Create a ZIP package for Python runtime extensibility actions

You can create a ZIP package that contains the Python script and dependencies used by your vRealize Automation Cloud Assembly extensibility actions.

There are two methods of building the script for your extensibility actions:

- Writing your script directly in the extensibility action editor in vRealize Automation Cloud Assembly.
- Creating your script on your local environment and adding it, with any relevant dependencies, to a ZIP package.

By using a ZIP package, you can create a custom preconfigured template of action scripts and dependencies that you can import to vRealize Automation Cloud Assembly for use in extensibility actions.

Furthermore, you can use a ZIP package in scenarios where modules associated with dependencies in your action script cannot be resolved by the vRealize Automation Cloud Assembly service, such as when your environment lacks Internet access.

You can also use a ZIP package to create extensibility actions that contain multiple Python script files. Using multiple script files can be useful for organizing the structure of your extensibility action code.

Prerequisites

If you are using Python 3.3 or earlier, download and configure the PIP package installer. See [Python Package Index](#).

Procedure

- 1 On your local machine, create a folder for your action script and dependencies.
For example, `/home/user1/zip-action`.
- 2 Add your main Python action script or scripts to the folder.
For example, `/home/user1/zip-action/main.py`.

3 (Optional) Add any dependencies for your Python script to the folder.

- a Create a `requirements.txt` file that contains your dependencies. See [Requirements Files](#).
- b Open a Linux shell.

Note The runtime of action-based extensibility in vRealize Automation Cloud Assembly is Linux-based. Therefore, any Python dependencies compiled in a Windows environment might make the generated ZIP package unusable for the creation of extensibility actions. Therefore, you must use a Linux shell.

- c Install your `requirements.txt` file in the script folder by running the following command:

```
pip install -r requirements.txt --target=home/user1/zip-action
```

4 In the assigned folder, select your script elements and, if applicable, your `requirements.txt` file and compress them to a ZIP package.

Note Both your script and dependency elements must be stored at the root level of the ZIP package. When creating the ZIP package in a Linux environment, you might encounter a problem where the package content is not stored at the root level. If you encounter this problem, create the package by running the `zip -r` command in your command-line shell.

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

What to do next

Use the ZIP package to create an extensibility action script. See [How do I create extensibility actions](#).

Create a ZIP package for Node.js runtime extensibility actions

You can create a ZIP package that contains the Node.js script and dependencies used by your vRealize Automation Cloud Assembly extensibility actions.

There are two methods of building the script for your extensibility actions:

- Writing your script directly in the extensibility action editor in vRealize Automation Cloud Assembly.
- Creating your script in your local environment and adding it, with any relevant dependencies, to a ZIP package.

By using a ZIP package, you can create a custom preconfigured template of action scripts and dependencies that you can import to vRealize Automation Cloud Assembly for use in extensibility actions.

Furthermore, you can use a ZIP package in scenarios where modules associated with dependencies in your action script cannot be resolved by the vRealize Automation Cloud Assembly service, such as when your environment lacks Internet access.

Also, you can use packages to create extensibility actions that contain multiple Node.js script files. Using multiple script files can be useful for organizing the structure of your extensibility action code.

Procedure

- 1 On your local machine, create a folder for your action script and dependencies.

For example, `/home/user1/zip-action`.

- 2 Add your main Node.js action script or scripts to the folder.

For example, `/home/user1/zip-action/main.js`.

- 3 (Optional) Add any dependencies for your Node.js script to the folder.

- a Create a `package.json` file with dependencies in your script folder. See [Creating a package.json file](#) and [Specifying dependencies and devDependencies in a package.json file](#).
- b Open a command-line shell.
- c Navigate to the folder that you created for the action script and dependencies.

```
cd /home/user1/zip-action
```

- d Install your `package.json` file in the script folder by running the following command:

```
npm install --production
```

Note This command creates a `node_modules` directory in your folder.

- 4 In the assigned folder, select your script elements and, if applicable, your `node_modules` directory and compress them to a ZIP package.

Note Both your script and dependency elements must be stored at the root level of the ZIP package. When creating the ZIP package in a Linux environment, you might encounter a problem where the package content is not stored at the root level. If you encounter this problem, create the package by running the `zip -r` command in your command-line shell.

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

What to do next

Use the ZIP package to create an extensibility action script. See [How do I create extensibility actions](#).

Create a ZIP package for PowerShell runtime extensibility actions

You can create a ZIP package that contains your PowerShell script and dependency modules for use in extensibility actions.

There are two methods of building the script for your extensibility actions:

- Writing your script directly in the extensibility action editor in vRealize Automation Cloud Assembly.
- Creating your script on your local environment and adding it, with any relevant dependencies, to a ZIP package.

By using a ZIP package, you can create a custom preconfigured template of action scripts and dependencies that you can import to vRealize Automation Cloud Assembly for use in extensibility actions.

Note You do not need to define PowerCLI cmdlets as dependencies or bundle them into a ZIP package. PowerCLI cmdlets come preconfigured with the PowerShell runtime of your vRealize Automation Cloud Assembly service.

Furthermore, you can use a ZIP package in scenarios where modules associated with dependencies in your action script cannot be resolved by the vRealize Automation Cloud Assembly service, such as when your environment lacks Internet access.

You can also use a ZIP package to create extensibility actions that contain multiple PowerShell script files. Using multiple script files can be useful for organizing the structure of your extensibility action code.

Prerequisites

Verify that you are familiar with PowerShell and PowerCLI. You can find a Docker image with PowerShell Core, PowerCLI 10, PowerNSX, and several community modules and script examples at [Docker Hub](#).

Procedure

- 1 On your local machine, create a folder for your action script and dependencies.

For example, `/home/user1/zip-action`.

- 2 Add your main PowerShell script with a `.psm1` extension to the folder.

The following script presents a simple PowerShell function called `main.psm1`:

```
function handler($context, $payload) {  
  
    Write-Host "Hello " $payload.target
```

```
return $payload
```

Note The output of a PowerShell extensibility action is based on the last variable displayed in the body of the function. All other variables in the included function are discarded.

- 3 (Optional) Add a proxy configuration to your main PowerShell script by using `context` parameters. See [Using context parameters to add a proxy configuration in your PowerShell script](#).
- 4 (Optional) Add any dependencies for your PowerShell script.

Note Your PowerShell dependency script must use the `.psm1` extension. Use the same name for the script and the subfolder where the script is saved.

- a Log in to a Linux PowerShell shell.

Note The runtime of action-based extensibility in vRealize Automation Cloud Assembly is Linux-based. Any PowerShell dependencies compiled in a Windows environment might make the generated ZIP package unusable. Any installed third-party dependencies must be compatible with the VMware Photon OS as PowerShell scripts run on Photon OS.

- b Navigate to the `/home/user1/zip-action` folder.
- c Download and save the PowerShell module containing your dependencies, by running the `Save-Module` cmdlet.

```
Save-Module -Name <module name> -Path ./
```

- d Repeat the previous substep for any additional dependency modules.

Important Verify that each dependency module is located in a separate subfolder. For more information on writing and managing PowerShell modules, see [How to Write a PowerShell Script Module](#).

- 5 In the assigned folder, select your script elements and, if applicable, your dependency module subfolders and compress them to a ZIP package.

Note Both your script and dependency module subfolders must be stored at the root level of the ZIP package. When creating the ZIP package in a Linux environment, you might encounter a problem where the package content is not stored at the root level. If you encounter this problem, create the package by running the `zip -r` command in your command-line shell.

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

What to do next

Use the ZIP package to create an extensibility action script. See [How do I create extensibility actions](#).

Using context parameters to add a proxy configuration in your PowerShell script

You can enable network proxy communication in your PowerShell script by using `context` parameters.

Certain PowerShell cmdlets might require that you set a network proxy as an environment variable in your PowerShell function. Proxy configurations are provided to the PowerShell function with the `$context.proxy.host` and `$context.proxy.port` parameters.

You can add these `context` parameters in the beginning of your PowerShell script.

```
$proxyString = "http://" + $context.proxy.host + ":" + $context.proxy.port
$Env:HTTP_PROXY = $proxyString
$Env:HTTPS_PROXY = $proxyString
```

If the cmdlets support the `-Proxy` parameter, you can also pass the proxy value directly to the specific PowerShell cmdlets.

Configure cloud-specific extensibility actions

You can configure extensibility actions to work with your cloud accounts.

When creating an extensibility action, you can configure and link it to various cloud-based accounts:

- Microsoft Azure
- Amazon Web Services

Prerequisites

A valid cloud account is required.

Procedure

- 1 Select **Extensibility > Library > Action**.
- 2 Click **New Action**.
- 3 Enter the action parameters as necessary.
- 4 In the **FaaS provider** drop-down menu, select your cloud account provider or select **Auto**.

Note If you select **Auto**, the action automatically defines the FaaS provider.

- 5 Click **Save**.

Results

Your extensibility action is linked for use with the configured cloud account.

Configure on-premises extensibility actions

You can configure your extensibility actions to use an on-premises FaaS provider instead of an Amazon Web Services or Microsoft Azure cloud account.

By using an on-premises FaaS provider for your extensibility actions, you can use on-premises services like LDAP, CMDB, or vCenter data centers in your vRealize Automation Cloud Assembly extensibility subscriptions.

Procedure

- 1 Select **Extensibility > Library > Actions**.
- 2 Click **New Action**.
- 3 Enter a name and project for the extensibility action.
- 4 (Optional) Enter a description for the extensibility action.
- 5 Click **Next**.
- 6 Create or import your extensibility action script.
- 7 Click the **FaaS provider** drop-down menu and select **On Prem**.
- 8 To save the new extensibility action, click **Save**.

What to do next

Use the created extensibility action in your vRealize Automation Cloud Assembly extensibility subscriptions.

Create shared extensibility actions

As a vRealize Automation Cloud Assembly administrator, you create extensibility actions that can be shared across projects without exporting and importing the action.

For information on exporting and importing extensibility actions, see [Export and import extensibility actions](#).

Prerequisites

Create two or more projects in your vRealize Automation Cloud Assembly organization.

Procedure

- 1 Select **Extensibility > Library > Actions**.
- 2 Click **New Action**.
- 3 Enter a name for your extensibility action.
- 4 (Optional) Enter a description for your extensibility action.
- 5 Select a project in which your extensibility action is created.
- 6 Tick the **Share with all projects in this organization** checkbox.
- 7 Click **Next**.

- 8 Create or import your action script, and save your extensibility action.

Note You can enable or disable sharing from **Settings**. If the extensibility action is used in subscriptions, you cannot disable sharing. To disable sharing, you must remove the extensibility action from your subscriptions.

- 9 Create an extensibility subscription, add the shared extensibility action, and set the subscription scope to **Any Project**.

Note For more information on creating extensibility subscriptions, see [Create an extensibility subscription](#).

The extensibility subscription is triggered by matching events in any of your projects.

What to do next

You can also import shared extensibility actions as a content source in the vRealize Automation Service Broker catalog. When you select the source project, enter the project that the extensibility action was created in. For more information on adding extensibility actions to vRealize Automation Service Broker, see [Add extensibility actions to the Service Broker catalog](#).

Export and import extensibility actions

With vRealize Automation Cloud Assembly, you can export and import extensibility actions for use in different projects.

Prerequisites

An existing extensibility action.

Procedure

- 1 Export an extensibility action.

- a Navigate to **Extensibility > Library > Actions**.
- b Select an extensibility action and click **Export**.

The action script and its dependencies are saved on your local environment as a ZIP file.

- 2 Import an extensibility action.

- a Navigate to **Extensibility > Library > Actions**.
- b Click **Import**.
- c Select the exported extensibility action and assign it to a project.
- d Click **Import**.

Note If the imported extensibility action is already assigned to the specified project, you are prompted to select a conflict resolution policy.

Alternate You can also import action scripts by selecting the **Import package** option directly from the action editor.

What is an action flow

Action flows are a set of extensibility action scripts that are used to extend life cycles and automation further.

All action flows begin with `flow_start` and end with `flow_end`. You can link several extensibility action scripts together, by using the following action flow elements:

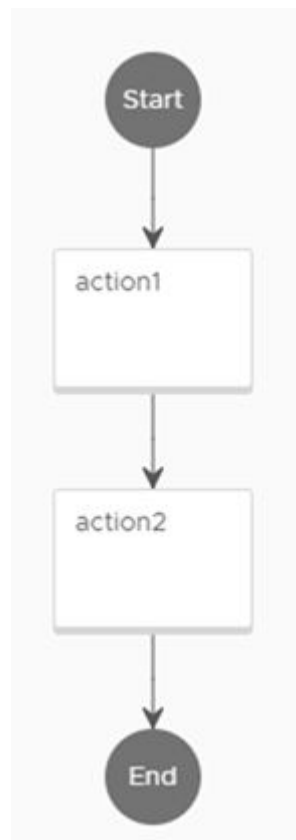
- **Sequential action flows** - Multiple extensibility action scripts running sequentially.
- **Fork action flows** - Multiple extensibility action scripts or flows that split pathways to contribute to the same output.
- **Join action flows** - Multiple extensibility action scripts or flows that join together and contribute to the same output.
- **Conditional action flows** - Multiple extensibility action scripts or flows that run after a condition is satisfied.

Sequential action flows

Multiple extensibility action scripts running sequentially.

```
version: "1"
flow:
  flow_start:
    next: action1
  action1:
    action: <action_name>
    next: action2
  action2:
    action: <action_name>
    next: flow_end
```

Note You can loop back to a previous action by assigning it as the `next: action`. For instance, in this example, instead of `next: flow_end`, you can enter `next: action1` to rerun action1 and restart the sequence of actions.



Fork action flows

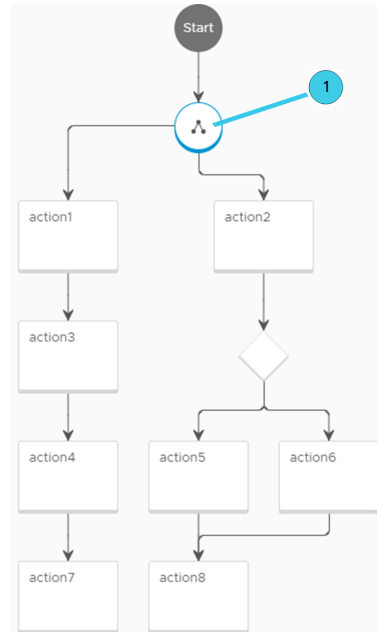
Multiple extensibility action scripts or flows that split pathways to contribute to the same output.

```

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>

```

Note You can loop back to a previous action by assigning it as the `next: action`. For example, instead of `next: flow_end` to end your action flow, you can enter `next: action1` to rerun action1 and restart the sequence of actions.



1 Fork Element

Join action flows

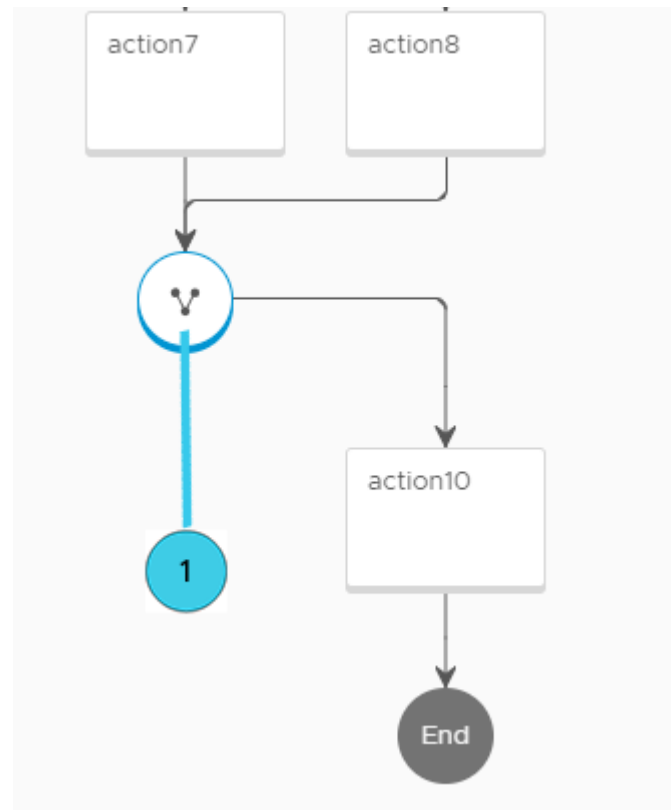
Multiple extensibility action scripts or flows that join pathways together and contribute to the same output.

```

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

```

Note You can loop back to a previous action by assigning it as the `next: action`. For instance, in this example, instead of `next: flow_end`, you can enter `next: action1` to rerun action1 and restart the sequence of actions.



1 Join Element

Conditional action flows

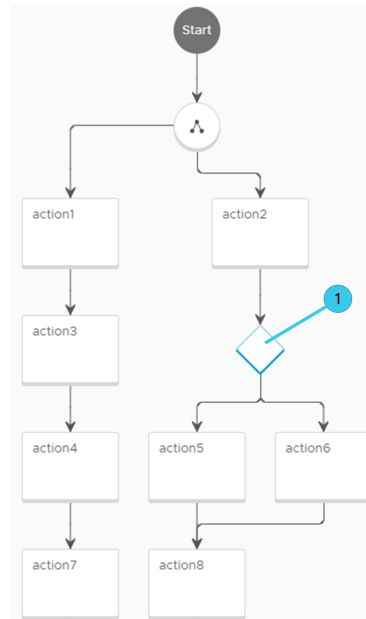
Multiple extensibility action scripts or flows that run when a condition is satisfied using a switch element.

In some cases, the condition must be equal to `true` in order for the action to run. Other cases, as seen in this example, require parameter values to be met before an action can run. If none of the conditions are met the action flow fails.


```

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

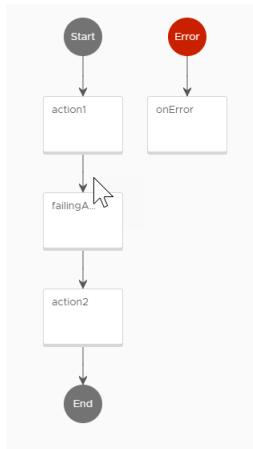
Note You can loop back to a previous action by assigning it as the `next: action`. For example, instead of `next: flow_end` to end your action flow, you can enter `next: action1` to rerun action1 and restart the sequence of actions.

How do I use an error handler with action flows

You can configure your action flow to issue an error at specified stages of the flow by using an error handler element.

An error handler element requires two inputs:

- Specified error message of the failed action.
- Action flow inputs.



If an action in your flow fails and the action flow contains an error handler element, an error message is issued alerting you of the action failure. The error handler is an action on its own. The following script is an example of an error handler that can be used in an action flow.

```
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
```

You can view the successful and failed runs on the Action Runs window.

Status	Run ID	Action
Completed	8a76996b6839fe3c01684...	error-handler
Failed	8a76996b6839fe3c01684...	failing-action
Completed	8a76996b6839fe3c01684...	simple-hello
Completed	8a76996b6839fe3c01684...	flow-with-handler

In this example, the flow-with-handler action flow, which contains an error handler element, was run successfully. However, one of the actions in the flow failed, which then initiated the error handler to issue an error.

How do I track action runs

The action runs tab shows you a log of subscription triggered extensibility actions and their status.

You can view the log of action runs using **Extensibility > Activity > Action Runs**. Also, you can filter the list of action runs by one or more properties at once. To view additional details of an individual action run, click the Run ID.

Troubleshooting failed extensibility action runs

If your extensibility action run fails, you can perform troubleshooting steps to correct it.

When an action run fails you might receive an error message, a failed status, and a failed log. If your action run fails, it is either due to a deployment or code failure.

Problem	Solution
Deployment Failure	These failures are a result of problems related to the cloud account configuration, action deployment, or other dependencies that can prevent the action from deploying. Ensure that the project you used is defined within the configured cloud account and granted permissions to run functions. Before initiating the action again, you can test the action against a specific project within the action's details page.
Code Failure	These failures are a result of invalid scripts or code. Use the Action run logs to troubleshoot and correct the invalid scripts.

Extensibility workflow subscriptions

You can use your vRealize Orchestrator hosted workflows with vRealize Automation Cloud Assembly to extend application lifecycle.

How do I modify virtual machine properties using a vRealize Orchestrator workflow subscription

You can use an existing vRealize Orchestrator workflow to modify virtual machine properties and add virtual machines to the active directory.

The event topic parameters define the format of the payload for Event Broker Service (EBS) messages. To receive and use EBS message payload inside a workflow, you must define the `inputProperties` workflow input parameters.

Prerequisites

- Cloud administrator user role
- Existing vRealize Orchestrator on-premises workflows.
- Successful integration and connection to the vRealize Orchestrator client server.

Procedure

- 1 Select **Extensibility > Subscriptions**.
- 2 Click **New Subscription**.

3 Create a subscription with the following parameters:

Parameter	Value
Name	RenameVM
Event topic	Select an event topic suitable for the desired vRealize Orchestrator integration. For example, compute allocation.
Blocking/Non-blocking	Non-blocking
Action/workflow	Select a vRealize Orchestrator runnable type. Select the desired workflow. For example, Set VM name.

4 To save your subscription, click **Save**.

5 Assign and activate your subscription by creating a cloud template or deploying an existing cloud template.

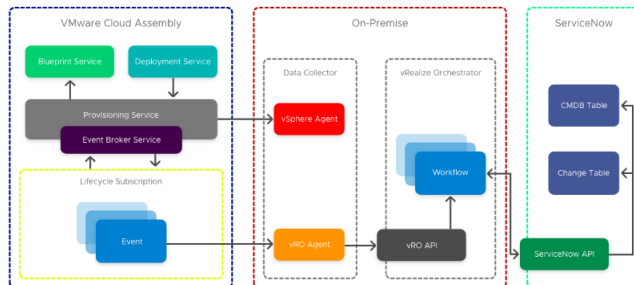
What to do next

Verify that the workflow initiated successfully by one of the following methods:

- Verify the workflow runs log, **Extensibility > Activity > Workflow Runs**.
- Open the vRealize Orchestrator client and check workflow status by navigating to the workflow and verifying the status or by opening the specific logs tab.

How do I integrate Cloud Assembly for ITSM with ServiceNow using vRealize Orchestrator workflows

Using vRealize Orchestrator hosted workflows, you can integrate vRealize Automation Cloud Assembly with ServiceNow for ITSM compliance.



Enterprise users commonly integrate their Cloud Management Platform with an IT Service Management (ITSM) and Configuration Management Database (CMDB) platform for compliance. Following this example, you can integrate vRealize Automation Cloud Assembly with ServiceNow for CMDB and ITSM using vRealize Orchestrator hosted workflows. When using vRealize Orchestrator integrations and workflows, capability tags are especially useful if you have multiple instances for different environments. For more information on capability tags, See [Using capability tags in vRealize Automation Cloud Assembly](#).

Note You can also integrate ServiceNow with vRealize Automation Cloud Assembly using extensibility action scripts. For information about integrating ServiceNow using extensibility action scripts, see [How do I integrate Cloud Assembly with ServiceNow using extensibility actions](#).

In this example, the ServiceNow integration is composed of three top-level workflows. Each workflow has their own subscriptions so that you can update and iterate each component individually.

- Event subscription entry point - Basic logging, identifies the requesting user and vCenter VM, if applicable.
- Integration workflow - Separates objects and feeds inputs into the technical workflow, handles logging, property, and output updates.
- Technical workflow - Downstream system integration for ServiceNow API to create the CMDB CI, CR, and vRealize Automation Cloud Assembly IaaS API with additional virtual machine properties outside of the payload.

Prerequisites

- A standalone or clustered vRealize Orchestrator environment.
- A vRealize Orchestrator integration in vRealize Automation Cloud Assembly. For information on integrating a standalone vRealize Orchestrator with vRealize Automation Cloud Assembly, see [Configure vRealize Orchestrator integration in Cloud Assembly](#).

Procedure

- 1 Create and save a configuration file in vRealize Orchestrator that contains common configuration used in multiple workflows.
- 2 Save your vRealize Automation Cloud Assembly API token in the same location, as the configuration file from Step 1.

Note The vRealize Automation Cloud Assembly API token has an expiration.

- 3 Create a workflow in vRealize Orchestrator with the provided script element. This script references and locates a REST Host. It also standardizes REST actions that use an optional parameter of a token, which is added as an extra authorization header.

```
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"];

```

This script sends the output `cpuCount` and `memoryMB` to the parent workflow and updates the existing `customProperties` properties. These values can be used in subsequent workflows when creating the CMDB.

- 4 Add the ServiceNow CMDB Create CI script element to your workflow. This element locates the ServiceNow REST Host using the configuration item, creates a REST operation for the `cmdb_ci_vmware_instance` table, creates a string of content object based on workflow inputs for post data, and outputs the returned `sys_id`.

```

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,attribute
Name)

//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 Using the output from the child workflow, create a properties object using the existing `customProperties` and overwrite the `serviceNowSysId` property with the value from ServiceNow. This unique id is used in the CMDB to mark an instance as retired on destroy.

Results

vRealize Automation Cloud Assembly is successfully integrated with ITSM ServiceNow. For more information on how you can use workflows to integrate ServiceNow in vRealize Automation Cloud Assembly, see [Extending Cloud Assembly with vRealize Orchestrator for ServiceNow Integration](#).

Learn more about workflow subscriptions

By using an vRealize Orchestrator integration with vRealize Automation Cloud Assembly, you can extend the life cycles of applications with workflows.

vRealize Automation includes an embedded vRealize Orchestrator deployment. You can use the workflow library of the embedded vRealize Orchestrator deployment in your subscriptions. You can create, modify, and delete workflows by using the vRealize Orchestrator client.

You can also integrate an external vRealize Orchestrator deployment in vRealize Automation Cloud Assembly. See *How do I integrate an external vRealize Orchestrator Client* in *Using the Embedded vRealize Orchestrator Client*.

Best practices for creating vRealize Orchestrator workflows

A workflow subscription is based on a specific event topic and the event parameters of that topic. To ensure that the subscriptions initiate the vRealize Orchestrator workflows, you must configure them with the correct input parameters so that they work with the event data.

Workflow Input Parameters

Your custom workflow can include all the parameters or a single parameter that consumes all the data in the payload.

To use a single parameter, configure one parameter with a type of `Properties` and name `inputProperties`.

Workflow Output Parameters

Your custom workflow can include output parameters that are relevant to subsequent events necessary for a reply event topic type.

If an event topic expects a reply, the workflow output parameters must match the parameters of the reply schema.

How do I track workflow runs

The **Workflow Runs** window displays the logs of the subscription triggered workflows and their status.

You can view the logs of your workflow runs by navigating to **Extensibility > Activity > Workflow Runs**.

Troubleshooting failed workflow subscriptions

If your workflow subscription fails, you can perform troubleshooting steps to correct it.

Failed workflow runs can cause your workflow subscription not to start or complete successfully. Workflow run failure can result from several common problems.

Problem	Cause	Solution
Your vRealize Orchestrator workflow subscription did not start or complete successfully.	You configured a workflow subscription to run a custom workflow when the event message is received, but the workflow does not run or complete successfully.	<ol style="list-style-type: none"> 1 Verify that the workflow subscription is saved correctly. 2 Verify that the workflow subscription conditions are configured correctly. 3 Verify that vRealize Orchestrator contains the specified workflow. 4 Verify that the workflow is configured correctly within vRealize Orchestrator.
Your approval request vRealize Orchestrator workflow subscription did not run.	You configured a pre-approval or post-approval workflow subscription to run a vRealize Orchestrator workflow. The workflow does not run when a machine that matches the defined criteria is requested in the service catalog.	<p>To successfully run an approval workflow subscription, you must verify that all the components are configured correctly.</p> <ol style="list-style-type: none"> 1 Verify that the approval policy is active and correctly applied. 2 Verify that your workflow subscription is correctly configured and saved. 3 Review the event logs for messages related to approvals.
Your approval request vRealize Orchestrator workflow subscription was rejected.	<p>You configured a pre-approval or post-approval workflow subscription that runs a specified vRealize Orchestrator workflow, but the request is rejected on the external approval level.</p> <p>One possible cause is an internal workflow run error in vRealize Orchestrator. For example, the workflow is missing or the vRealize Orchestrator server is not running.</p>	<ol style="list-style-type: none"> 1 Review the logs for messages related to approvals. 2 Verify that the vRealize Orchestrator server is running. 3 Verify that vRealize Orchestrator contains the specified workflow.

Learn more about extensibility subscriptions

You can extend your application life cycles by using either extensibility actions or vRealize Orchestrator hosted workflows with extensibility subscriptions.

When a triggering event occurs in your environment, the subscription is initiated and the specified workflow or extensibility action is run. You can view system events on the event log, workflow runs in the workflow runs window, and action runs in the action run window. Subscriptions are project-specific, meaning they are linked to cloud templates and deployments through the specified project.

Extensibility terminology

As you work with extensibility subscriptions within vRealize Automation Cloud Assembly, you might encounter some terminology that is specific to the subscriptions and event broker service.

Table 6-3. Extensibility Terminology

Term	Description
Event Topic	Describes a set of events that have the same logical intent and the same structure. Every event is an instance of an event topic. You can assign blocking parameters to certain event topics. For more information, see Blocking event topics .
Event	Indicates a change in the state in the producer or any of the entities managed by it. The event is the entity that records information about the event occurrence.
Event Broker Service	The service that dispatches messages published by a producer to the subscribed consumers.
Payload	The event data that contains all the relevant properties related to that Event Topic.
Subscription	Indicates that a subscriber is interested in being notified about an event by subscribing to an event topic and defining the criteria that triggers the notification. Subscriptions link either extensibility actions or workflows to triggering events used to automate parts of the applications life cycle.
Subscriber	The users notified by the events published to the event broker service based on the subscription definition. The subscriber can also be called a consumer.
System Administrator	A user with privileges to create, read, update, and delete tenant workflow subscriptions and system workflow subscriptions using vRealize Automation Cloud Assembly.
Workflow Subscription	Specifies the event topic and conditions that trigger a vRealize Orchestrator workflow.
Action Subscription	Specifies the event topic and conditions that trigger an extensibility action to run.

Table 6-3. Extensibility Terminology (continued)

Term	Description
Workflow	A vRealize Orchestrator workflow that is integrated within vRealize Automation Cloud Assembly. You can link these workflows to events within subscriptions.
Extensibility Action	A streamlined script of code that can run after an event is triggered in a subscription. Extensibility actions are similar to workflows, but are more lightweight. Extensibility actions can be customized from within vRealize Automation Cloud Assembly.
Action Runs	Accessible through the Action Runs tab. An action run is a detailed log of extensibility actions that have run in response to triggering events.

Blocking event topics

Some event topics support blocking events. The behavior of an extensibility subscription depends on whether the topic supports these event types and how you configure the subscription.

vRealize Automation Cloud Assembly extensibility subscriptions can use two broad types of event topics: non-blocking and blocking event topics. The event topic type defines the behavior of the extensibility subscription.

Non-Blocking Event Topics

Non-blocking event topics only allow you to create non-blocking subscriptions. Non-blocking subscriptions are triggered asynchronously and you cannot rely on the order that the subscriptions are triggered in.

Blocking Event Topics

Some event topics support blocking. If a subscription is marked as blocking, all messages that meet the set conditions are not received by any other subscriptions with matching conditions until the runnable item of the blocking subscription is run.

Blocking subscriptions run in priority order. The highest priority value is 0 (zero). If you have more than one blocking subscription for the same event topic with the same priority level, the subscriptions run in a reverse alphabetical order based on the name of the subscription. After all blocking subscriptions are processed, the message is sent to all the non-blocking subscriptions at the same time. Because the blocking subscriptions run synchronously, the changed event payload includes the updated event when the subsequent subscriptions are notified.

You can use blocking event topics to manage multiple subscriptions that are dependent on each other.

For example, you can have two provisioning workflow subscriptions where the second subscription depends on the results of the first subscription. The first subscription changes a property during provisioning, and the second subscription records the new property, such as a machine name, in a file system. The ChangeProperty subscription is prioritized as 0 and the RecordProperty is prioritized as 1 because the second subscription uses the results of the first subscription. When a machine is provisioned, the ChangeProperty subscription begins running.

Because the RecordProperty subscription conditions are based on a post-provisioning condition, an event triggers the RecordProperty subscription. However, because the ChangeProperty workflow is a blocking workflow, the event is not received until it is finished. When the machine name is changed and the first workflow subscription is finished, the second workflow subscription runs and records the machine name in the file system.

Recovery Runnable Item

For blocking event topics, you can add a recovery runnable item to the subscription. The recovery runnable item in a subscription runs if the primary runnable item fails. For example, you can create a workflow subscription where the primary runnable item is a workflow that creates records in a CMDB system such as ServiceNow. Even if the workflow subscription fails, some records might be created in the CMDB system. In this scenario, a recovery runnable item can be used to clean up the records left in the CMDB system by the failed runnable item.

For use cases that include multiple subscriptions that are dependent on each other, you can add a `ebs.recover.continuation` property to the recovery runnable item. With this property, you can direct if the Extensibility service must continue with the next subscription in your chain, if the current subscription fails.

Event topics provided with vRealize Automation Cloud Assembly

vRealize Automation Cloud Assembly includes predefined event topics.

Event Topics

Event topics are the categories that group similar events together. When assigned to a subscription, event topics define which event triggers the subscription. The following event topics are provided by default with vRealize Automation Cloud Assembly. All topics can be used to add or update custom properties or tags of the resource. If a vRealize Orchestrator workflow or extensibility action fails, the corresponding task fails as well.

Table 6-4. Cloud Assembly Event Topics

Event Topic	Blockable	Description
Cloud template configuration	No	Issued when a cloud template configuration event, such as the creation or deletion of a cloud template, occurs. This event topic can be useful for notifying external systems of such events.
Cloud template version configuration	No	Issued when a new cloud template versioning event occurs, such as the creation, release, de-release, or restoration of a version. This event topic can be useful with integrations of third-party version control systems.

Table 6-4. Cloud Assembly Event Topics (continued)

Event Topic	Blockable	Description
Compute allocation	Yes	Issued before the allocation of <code>resourcenames</code> and <code>hostselections</code> . Both of these properties can be modified at this stage.
Compute post provision	Yes	Issued after a resource was provisioned successfully.
Compute post removal	Yes	issued after a compute resource was removed.
Compute provision	Yes	Issued before the resource is provisioned at the hypervisor layer. Note You can change the allocated IP address.
Compute removal	Yes	Issued before the resource is removed.
Compute reservation	Yes	Issued at the time of reservation. Note You can change the placement order.
Deployment action completed	Yes	Issued after a deployment action is finished.
Deployment action requested	Yes	Issued before a deployment action is finished.
Deployment completed	Yes	Issued after the deployment of a cloud template or catalog request.
Deployment onboarded	No	Issued when a new deployment is onboarded.
Deployment requested	Yes	Issued before the deployment of a cloud template or catalog request.
Deployment resource action completed	Yes	Issued after the deployment of a resource action.
Deployment resource action requested	Yes	Issued before the deployment of a resource action.
Deployment resource completed	Yes	Issued after the provisioning of a deployment resource.
Deployment resource requested	Yes	Issued before the provisioning of a deployment resource.
Disk allocation	Yes	Issued for the preallocation of disk resources.

Table 6-4. Cloud Assembly Event Topics (continued)

Event Topic	Blockable	Description
Disk attach	Yes	<p>Issued before a disk is attached to a machine. <code>Disk attach</code> is a read and write event. Disk properties supported for write-back are:</p> <ul style="list-style-type: none"> ■ <code>diskFullPaths</code> ■ <code>diskDatastoreNames</code> ■ <code>diskParentDirs</code> <p>All three vSphere specific disk properties are required for updates. All other properties are read-only.</p> <p>Note Write-back is optional for vSphere First Class Disks.</p>
Disk detach	Yes	Issued after a disk is detached from a machine. <code>Disk detach</code> is a read-only event.
Disk post removal	Yes	Issued after a disk resource is deleted.
Disk post resize	Yes	Issued after a disk resource is resized.
EventLog	Yes	Issued for logging related events.
Kubernetes cluster allocation	Yes	Issued for the preallocation of resources for a Kubernetes cluster.
Kubernetes cluster post provision	Yes	Issued after a Kubernetes cluster is provisioned.
Kubernetes cluster post removal	Yes	Issued after a Kubernetes cluster is deleted.
Kubernetes cluster provision	Yes	Issued before a Kubernetes cluster is provisioned.
Kubernetes cluster removal	Yes	Issued before the process of deleting a Kubernetes cluster is initiated.
Load balancer post provision	Yes	Issued after the provisioning of a load balancer.
Load balancer post removal	Yes	Issued after the removal of a load balancer.
Load balancer provision	Yes	Issued before provisioning a load balancer
Load balancer removal	Yes	Issued before removing a load balancer.
Network Configure	Yes	<p>Issued when the network is configured during compute allocation.</p> <p>Note The Network Configure topic supports multiple IP addresses/NICs.</p>

Table 6-4. Cloud Assembly Event Topics (continued)

Event Topic	Blockable	Description
Network post provisioning	Yes	Issued after a network resource is provisioned.
Network post removal	Yes	Issued after a network resource is removed.
Network provisioning	Yes	Issued before a network resource is provisioned.
Network removal	Yes	Issued before a network resource is removed.
Security group post provisioning	Yes	Issued after a security group is provisioned.
Security group post removal	Yes	Issued after a security group is removed.
Security group provisioning	Yes	Issued before a security group is provisioned.
Security group removal	Yes	Issued before a security group is removed.
Project Lifecycle	No	Events issued when a project is created, updated, or deleted.

Event Parameters

After you add an event topic, you can view the parameters of that event topic. These event parameters define the structure of the event's payload, or `inputProperties`. Certain event parameters cannot be modified and are marked as read-only. You can identify these read-only parameters by clicking the info icon to the right of the parameter.

Extensibility event log

The extensibility events page displays a list of all events that have occurred within your environment.

You can view the extensibility event logs by navigating to **Extensibility > Events**. You can also filter the list of events by one or more properties. To view additional details of an individual event, select the event's ID.

ID	Timestamp	Event Topic	User Name	Target ID	Description
cbaf56ce-a324-f5ae-5dd1-66d1e5911a65	04/28/20, 1:10 PM	N/A	N/A	endpoints	CREATE
ef621151-2906-dce2-14ab-68c17132d756	03/25/20, 4:22 PM	N/A	N/A	endpoints	CREATE
468a8b55-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

Create an extensibility subscription

By using a vRealize Orchestrator integration, or extensibility actions with vRealize Automation Cloud Assembly, you can create subscriptions to extend your applications.

Extensibility subscriptions allow you to extend your applications by triggering workflows or actions at specific life-cycle events. You can also apply filters to your subscriptions to set boolean conditions for the specified event. For example, the event and workflow or action only triggers if the boolean expression is `'true'`. This is helpful for scenarios where you want to control when events, actions, or workflows are triggered.

Prerequisites

- Cloud administrator user role
- If you are using vRealize Orchestrator workflows:
 - The library of the embedded vRealize Orchestrator Client or the library of any integrated external vRealize Orchestrator instance.
- If you are using extensibility actions:
 - Existing extensibility action scripts. For more information, see [How do I create extensibility actions](#).

Procedure

- 1 Select **Extensibility > Subscriptions**.
- 2 Click **New Subscription**.
- 3 Enter the details of your subscription.
- 4 Select an **Event Topic**.
- 5 (Optional) Set conditions for the event topic.

Note Conditions can be created by using a javascript syntax expression. This expression can include boolean operators, such as `"&&"` (AND), `"||"` (OR), `"^"` (XOR), and `"!"` (NOT). You can also use arithmetic operators, such as `"=="` (equal to), `"!="` (not equal to), `">="` (greater than or equal), `"<="` (less than or equal), `">"` (greater than), and `"<"` (lesser than). More complex boolean expressions can be built out of simpler expressions. To access the event's payload (data) according to the specified topic parameters, use `'event.data'` or any of the event's header properties: `sourceType`, `sourceIdentity`, `timeStamp`, `eventType`, `eventTopicId`, `correlationType`, `correlationId`, `description`, `targetType`, `targetId`, `userName`, and `orgId`.

- 6 Under **Action/workflow**, select a runnable item for your extensibility subscription.
- 7 (Optional) If applicable, configure the blocking behavior for the event topic.
- 8 (Optional) To define the project scope of the extensibility subscription, disable **Any Project**, and click **Add Projects**.

9 To save your subscription, click **Save**.

Results

Your subscription is created. When an event, categorized by the selected event topic, occurs the linked vRealize Orchestrator workflow or extensibility action is initiated and all subscribers are notified.

What to do next

After creating your subscription, you can create or deploy a cloud template to link and use the subscription. You can also verify the status of the workflow run in the **Extensibility** tab within vRealize Automation Cloud Assembly. For subscriptions containing vRealize Orchestrator workflows, you can also monitor runs and workflow status from the vRealize Orchestrator client.

Troubleshooting an extensibility subscription

Troubleshoot extensibility subscription failures.

When your subscription fails, it is commonly a result of errors with your workflow or extensibility action script.

View topic parameters and payload

You can use a dump subscription topic parameters script to view the specific parameters and payload of your virtual machine at any given event stage.

Primarily, this script is useful for debugging and verifying available inputs for your vRealize Orchestrator workflow. To view all parameters of your virtual machine, use the following script with your 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")
```

Subscription version history

If your subscription fails, you can view the version history.

Viewing Subscription Version History

The version history tab can show you the change history of your subscription with the user and date of the change. If your subscription fails or is running incorrectly, the version history can help identify the cause.

The screenshot shows the vRealize Automation Cloud Assembly interface. The top navigation bar includes 'Infrastructure', 'Blueprints', 'Deployments', 'Extensibility [Beta]', and 'Marketplace'. The left sidebar has a search icon and a list of items: 'Events', 'Subscriptions' (highlighted with a blue circle and the number 1), 'Library', and 'Runs'. The 'Subscriptions' section is expanded, showing 'Event Topics', 'Actions', 'Workflows', 'Action Runs', and 'Workflow Runs'. The main content area is titled 'Test subscription' with a 'DELETE' button. Below the title, there are fields for 'Name' (Test subscription) and 'Description'. The 'On Event', 'Run Item', and 'Version History' tabs are visible, with 'Version History' selected (highlighted with a blue circle and the number 2). The 'Version History' tab displays a list of entries with timestamps and user information (highlighted with a blue circle and the number 3). The entries are as follows:

Timestamp	User
11/26/18, 7:55 AM - current	xxxx@vmware.com
11/26/18, 7:52 AM	xxxx@vmware.com
11/12/18, 5:38 AM	xxxx@vmware.com
11/12/18, 5:35 AM	xxxx@vmware.com
11/6/18, 6:04 AM	xxxx@vmware.com
11/2/18, 11:26 AM	xxxx@vmware.com
11/2/18, 10:26 AM	xxxx@vmware.com

On the right side of the 'Version History' tab, a JSON object is displayed, representing the subscription configuration:

```
{
  "id": "sub_1541168801838",
  "type": "RUNNABLE",
  "eventTopicId": "compute.allocation.pre",
  "name": "Test subscription",
  "orgId": "b99d05f4-6ce4-4e45-a5dc-c01e5ad4587a",
  "ownerId": "albena@vmware.com",
  "subscriberId": "abx-svc",
  "blocking": false,
  "description": "Let's have something long for this subscription.\nMake it multiline\nAnd very long",
  "criteria": "event.userName == \"mvaleva@vmware.com\"",
  "timeout": 0,
  "broadcast": false,
  "priority": 10,
  "runnableType": "extensibility.abx",
  "runnableId": "8a76836f73c2c7e01674f9738090055"
}
```

1 Open your subscription from the **Subscriptions** tab.

2 To view the version history, click **Version History**.

3 You can click each change entry to view the corresponding subscription code associated with the change.

What are the vRealize Automation resource properties

The vRealize Automation infrastructure-as-code editor lets you click or hover for syntax and code completion help. To view the complete set of cloud template resource properties though, sometimes called custom properties, refer to the consolidated resource schema.

The schema is available from the VMware {code} site. Follow the link, and click **Models** to list the resource objects that are available for cloud templates, formerly called blueprints.

- [vRealize Automation Resource Type Schema on VMware {code}](#)

What are some vRealize Automation Cloud Assembly code examples

Cloud template code in vRealize Automation Cloud Assembly can be almost limitless in combination and application.

Often, an example of successful code is your best starting point for further development. When following an example, make substitutions in order to apply your site settings in terms of resource names, values, and so on.

vSphere resource examples in vRealize Automation Cloud Assembly cloud templates

These code examples illustrate vSphere machine resources within vRealize Automation Cloud Assembly cloud templates.

Resource	Example Cloud Template
vSphere virtual machine with CPU, memory, and operating system	<pre>resources: demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine cpuCount: 1 totalMemoryMB: 1024 image: ubuntu</pre>
vSphere machine with a datastore resource	<pre>resources: demo-vsphere-disk-001: type: Cloud.vSphere.Disk properties: name: DISK_001 type: 'HDD' capacityGb: 10 datastore: 'datastore-01' provisioningType: thick</pre>

Resource	Example Cloud Template
vSphere machine with an attached disk	<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 machine with a dynamic number of disks	<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 machine from a snapshot image. Append a forward slash and the snapshot name. The snapshot image can be a linked clone.	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: imageRef: 'demo-machine/snapshot-01' cpuCount: 1 totalMemoryMB: 1024 </pre>

Resource	Example Cloud Template
vSphere machine in a specific folder in vCenter	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine cpuCount: 2 totalMemoryMB: 1024 imageRef: ubuntu resourceGroupName: 'myFolder' </pre>
vSphere machine with multiple NICs	<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 machine with an attached tag in vCenter	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu tags: - key: env value: demo </pre>

Resource	Example Cloud Template
vSphere machine with a customization spec	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine image: ubuntu flavor: small customizationSpec: Linux </pre>
vSphere machine with remote access	<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>

Documented vRealize Automation Cloud Assembly template example

By including a thorough set of comments, this example lets you review the structure and purpose of the sections in a vRealize Automation Cloud Assembly template, formerly called a blueprint.

```

# *****
#
# 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 extensiblity 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: '${env.requestedBy}'
#
# -----
# You are free to add custom properties, which might be used to initiate
# an extensibility subscription, for example.
# -----
#   ABC-Company-ID: 9393
#
# -----
# Tag the web server to deploy to the cloud vendor chosen from the
# user input. Tags are case-sensitive, so 'to_lower' forces the tag to
# lowercase to ensure a match with your site's tagging convention. It's
# important if platform input were to contain any upper case characters.
# -----
#   constraints:
#     - tag: '${"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
#
# *****

```

Network, security, and load balancer examples in vRealize Automation cloud templates

You can use networking, security, and load balancer resources and settings in cloud template designs and deployments.

For a summary of cloud template design code options, see [vRealize Automation Resource Type Schema](#).

For related information, see:

- [Using a network resource in a vRealize Automation cloud template](#)
- [Using a security group resource in a vRealize Automation cloud template](#)
- [Using a load balancer resource in a vRealize Automation cloud template](#)

These examples illustrate sample network, security group, and load balancer resources within basic cloud template designs.

Resource scenario	Example cloud template design code
vSphere machine with multiple NICs associated to an NSX network resource.	<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>
Enable NAT port forwarding by using a Cloud.NSX.Gateway cloud template resource on an outbound network.	<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>

Resource scenario	Example cloud template design code
Specify a load balance logging level, algorithm, and size.	<p>Sample NSX load balancer showing use of logging level, algorithm, and size:</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>
Associate a load balancer with a named machine or a named machine NIC. You can specify either machine ID or machine network ID to add the machine to the load balancer pool. The instances property supports both machines (machine by ID) and NICs (machine by network ID).	<p>You can use the instances property to define a machine ID or a machine network ID:</p> <p>■ Machine ID</p> <pre> Cloud_LoadBalancer_1: type: Cloud.LoadBalancer properties: network: '\${resource.Cloud_Network_1.id}' instances: '\$ {resource.Cloud_Machine_1.id}' </pre> <p>■ Machine network ID</p> <pre> Cloud_LoadBalancer_1: type: Cloud.LoadBalancer properties: network: '\${resource.Cloud_Network_1.id}' instances: '\$ {resource.Cloud_Machine_1.networks[0].id}' </pre> <p>■ One machine specified for load balancer inclusion and another machine NIC specified for load balancer inclusion:</p> <pre> instances: - resource.Cloud_Machine_1.id - resource.Cloud_Machine_2.networks[2].id </pre>
Public cloud machine to use an internal IP instead of a public IP. This example uses a specific network ID.	<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>
Note: The network: option is used in the networks: setting to specify a target network ID. The name: option in the networks: setting has been deprecated and should not be used.	

Resource scenario	Example cloud template design code
Routed network for NSX-V or NSX-T using the NSX network resource type.	<pre>Cloud_NSX_Network_1: type: Cloud.NSX.Network properties: networkType: routed</pre>
Add a tag to a machine NIC resource in the cloud template.	<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>
<p>Tag NSX-T logical switches for an outbound network.</p> <p>Tagging is supported for NSX-T and VMware Cloud on AWS. For more information on this scenario, see community blog post Creating Tags in NSX with Cloud Assembly.</p>	<pre>Cloud_NSX_Network_1: type: Cloud.NSX.Network properties: networkType: outbound tags: - key: app value: opencart</pre>

Resource scenario	Example cloud template design code
<p>Existing security group with a constraint tag applied to a machine NIC.</p> <p>To use an existing security group, enter <i>existing</i> for the <code>securityGroupType</code> property.</p> <p>You can assign tags to a <code>Cloud.SecurityGroup</code> resource to allocate existing security groups by using tag constraints. Security groups that do not contain tags cannot be used in the cloud template design.</p> <p>Constraint tags must be set for <code>securityGroupType: existing</code> security group resources. Those constraints must match the tags set on the existing security groups. Constraint tags cannot be set for <code>securityGroupType: new</code> security group resources.</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>

Resource scenario	Example cloud template design code
On-demand security group with two firewall rules illustrating the Allow and Deny access options.	<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>

Resource scenario	Example cloud template design code
<p>Complex cloud template with 2 security groups, including:</p> <ul style="list-style-type: none"> ■ 1 existing security group ■ 1 on-demand security group with multiple firewall rule examples ■ 1 vSphere machine ■ 1 existing network <p>This sample illustrates different combinations of protocols and ports, services, IP CIDR as source and destination, IP range as source or destination, and the options for any, IPv6, and (::/0).</p> <p>For machine NICs, you can specify the connected network, and security group(s). You can also specify the NIC index or an IP address.</p>	<pre> formatVersion: 1 inputs: {} resources: DEMO_ESG : <i>existing security group - security group 1</i>) type: Cloud.SecurityGroup properties: constraints: - tag: BlockAll securityGroupType: existing (<i>designation of existing for security group 1</i>) DEMO_ODSG: (<i>on-demand security group - security group 2</i>) type: Cloud.SecurityGroup properties: rules: (<i>multiple firewall rules in this section</i>) - name: IN-ANY (<i>rule 1</i>) source: any service: any direction: inbound access: Deny - name: IN-SSH (<i>rule 2</i>) source: any service: SSH direction: inbound access: Allow - name: IN-SSH-IP (<i>rule 3</i>) source: 33.33.33.1-33.33.33.250 protocol: TCP ports: 223 direction: inbound access: Allow - name: IPv-6-ANY-SOURCE (<i>rule 4</i>) source: ':::/0' protocol: TCP ports: 223 direction: inbound access: Allow - name: IN-SSH-IP (<i>rule 5</i>) source: 44.44.44.1/24 protocol: UDP ports: 22-25 direction: inbound access: Allow - name: IN-EXISTING-SG (<i>rule 6</i>) source: '\${resource["DEMO_ESG"].id}' protocol: ICMPv6 direction: inbound access: Allow - name: OUT-ANY (<i>rule 7</i>) destination: any service: any direction: outbound access: Deny - name: OUT-TCP-IPv6 (<i>rule 8</i>) destination: '2001:0db8:85a3::8a2e:0370:7334/64' protocol: TCP ports: 22 direction: outbound access: Allow </pre>

Resource scenario	Example cloud template design code
	<pre> - 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 </pre>

Resource scenario	Example cloud template design code
On-demand network with a 1-arm load balancer.	<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>
Existing network with a load balancer.	<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>

Resource scenario	Example cloud template design code
	<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>

Learn more

For network and security implementation scenarios, see VMware blogs such as these:

- [vRealize Automation Cloud Assembly Load Balancer with NSX-T Deep Dive](#)
- [Network Automation with Cloud Assembly and NSX – Part 1](#) (includes use of NSX-T and vCenter cloud accounts and network CIDR)
- [Network Automation with Cloud Assembly and NSX – Part 2](#) (includes use of existing and outbound network types)
- [Network Automation with Cloud Assembly and NSX – Part 3](#) (includes use of existing and on-demand security groups)
- [Network Automation with Cloud Assembly and NSX – Part 4](#) (includes use of existing and on-demand load balancers)

Using a network resource in a vRealize Automation cloud template

As you create or edit your vRealize Automation cloud template designs, use the most appropriate network resources for your objectives. Learn about the NSX and cloud-agnostic network options that are available in the cloud template.

Select one of the available network resource types based on machine and related conditions in your vRealize Automation cloud template.

Cloud agnostic network resource

You add a cloud agnostic network by using the **Cloud Agnostic > Network** resource on the cloud template **Design** page. The resource displays in the cloud template code as a `Cloud.Network` resource type. The default resource displays as:

```
Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkType: existing
```

Use a cloud agnostic network when you want to specify networking characteristics for a target machine type that is not, or might not, be connected to an NSX network.

The cloud agnostic network resource is available for these resource types:

- Cloud agnostic machine
- vSphere
- Google Cloud Platform (GCP)
- Amazon Web Services (AWS)
- Microsoft Azure
- VMware Cloud on AWS (VMC)

The cloud agnostic network resource is available for these network type (`networkType`) settings:

- public
- private
- outbound
- existing

vSphere network resource

You add a vSphere network by using the **vSphere > Network** resource on the cloud template **Design** page. The resource displays in the cloud template code as a `Cloud.vSphere.Network` resource type. The default resource displays as:

```
Cloud_vSphere_Network_1:
  type: Cloud.vSphere.Network
  properties:
    networkType: existing
```

Use a vSphere network when you want to specify networking characteristics for a vSphere machine type (`Cloud.vSphere.Machine`).

The vSphere network resource is only available for a `Cloud.vSphere.Machine` machine type.

The vSphere resource is available for these network type (`networkType`) settings:

- public

- private
- existing

For more information about network types, see [Using network settings in network profiles and cloud templates in vRealize Automation](#).

NSX network resource

You add an NSX network by using the **NSX > Network** resource on the cloud template **Design** page. The resource displays in the cloud template code as a `Cloud.NSX.Network` resource type. The default resource displays as:

```
Cloud_NSX_Network_1:
  type: Cloud.NSX.Network
  properties:
    networkType: existing
```

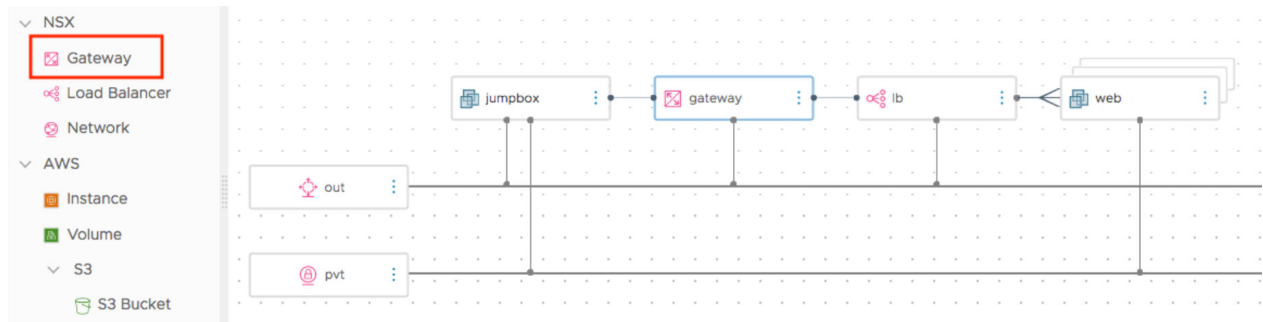
Use an NSX network when you want to attach a network resource to one or more machines that have been associated to an NSX-V or NSX-T cloud account. The NSX network resource allows you to specify NSX networking characteristics for a vSphere machine resource that is associated to an NSX-V or NSX-T cloud account.

The `Cloud.NSX.Network` resource is available for these network type (`networkType`) settings:

- public
- private
- outbound
- existing
- routed - Routed networks are only available for NSX-V and NSX-T.

Each on-demand NSX-T network creates a new Tier-1 logical router. Each on-demand NSX-V network creates a new Edge.

To support NAT rules and NAT port forwarding, you can add a `Cloud.NSX.Gateway` cloud template resource to allow DNAT rules to be specified for the gateway/router that is connected to an outbound NSX-V or NSX-T network. The gateway must be attached to a single outbound network and can be connected to multiple machines or load balancers that are connected to the same outbound network. DNAT rules specified within the gateway reference these machines or load balancers as their target. NAT rules cannot be specified for clustered machines, however as a Day 2 operation they can be specified for individual machines within the cluster.



For related i

[Network, security, and load balancer examples in vRealize Automation cloud templates.](#)

External IPAM integration options

For information about properties that are available for use with your Infoblox IPAM integrations in cloud template designs and deployments, see [Using Infoblox-specific properties and extensible attributes for IPAM integrations in vRealize Automation.](#)

Available day 2 operations

For a list of common day 2 operations that are available for cloud template and deployment resources, see [What actions can I run on vRealize Automation Cloud Assembly deployments.](#)

For an example of how to move from one network to another, see [How to move a deployed machine to another network.](#)

Learn more

For information about defining network resources, see [Network resources in vRealize Automation.](#)

For information about defining network profiles, see [Learn more about network profiles in vRealize Automation.](#)

For examples of cloud template designs that illustrate sample network resources and settings, see [Network, security, and load balancer examples in vRealize Automation cloud templates.](#)

Using a security group resource in a vRealize Automation cloud template

As you create or edit your vRealize Automation cloud template, use the most appropriate security group resources for your objectives. Learn about the security group options that are available in the cloud template.

Cloud agnostic security group resource

There is currently only one type of security group resource. You add a security group resource by using the **Cloud Agnostic > Security Group** resource on the cloud template Design page. The resource displays in the cloud template code as a `Cloud.SecurityGroup` resource type. The default resource displays as:

```
Cloud_SecurityGroup_1:
  type: Cloud.SecurityGroup
  properties:
    constraints: []
    securityGroupType: existing
```

You specify a security group resource in a cloud template design as either existing (`securityGroupType: existing`) or on-demand (`securityGroupType: new`).

You can add an existing security group directly to your cloud template design or you can use an existing security group that has been added to a network profile. Existing security groups are supported for various cloud account types.

For NSX-V and NSX-T, you can add an existing security group or define a new security group as you design or modify your cloud template. On-demand security groups are only supported for NSX-T and NSX-V.

For all cloud account types except Microsoft Azure, you can associate one or more security groups to a machine NIC. A Microsoft Azure virtual machine NIC (*machineName*) can only be associated to one security group.

By default, the security group property `securityGroupType` is set to `existing`. To create an on-demand security group, enter `new` for the `securityGroupType` property. To specify firewall rules for an on-demand security group, use the `rules` property in the `Cloud.SecurityGroup` section of the security group resource.

Existing security groups

Existing security groups are created in a source cloud account resource such as NSX-T or Amazon Web Services. They are data collected by vRealize Automation from the source. You can select an existing security group from a list of available resources as part of a vRealize Automation network profile. In a cloud template design, you can specify an existing security group either inherently by its membership in a specified network profile or specifically by name using the `securityGroupType: existing` setting in a security group resource. If you add a security group to a network profile, add at least one capability tag to the network profile. On-demand security group resources require a constraint tag when used in a cloud template design.

You can associate a security group resource in your cloud template design to one or more machine resources.

Note If you intend to use a machine resource in your cloud template design to provision to a Microsoft Azure virtual machine NIC (*machineName*), you should only associate the machine resource to a single security group.

On-demand NSX-V and NSX-T security groups

You can define on-demand security groups as you define or modify a cloud template design by using the `securityGroupType: new` setting in the security group resource code.

You can use an on-demand NSX-V or NSX-T security group to apply a specific set of firewall rules to a networked machine resource or set of grouped resources. Each security group can contain multiple named firewall rules. You can use an on-demand security group to specify services or protocols and ports. Note that you can specify either a service or a protocol but not both. You can specify a port in addition to a protocol. You cannot specify a port if you specify a service. If the rule contains neither a service or a protocol, the default service value is Any.

You can also specify IP addresses and IP ranges in firewall rules. Some firewall rule examples are shown in [Network, security, and load balancer examples in vRealize Automation cloud templates](#).

When you create firewall rules in an NSX-V or NSX-T on-demand security group, the default is to allow the specified network traffic but to also allow other network traffic. To control network traffic, you must specify an access type for each rule. The rule access types are:

- Allow (default) - Allows the network traffic that is specified in this firewall rule.
- Deny - Blocks the network traffic that is specified in this firewall rule. Actively tells the client that the connection is rejected.
- Drop - Rejects the network traffic that is specified in this firewall rule. Silently drops the packet as if the listener is not online.

For an example design that uses an `access: Allow` and an `access: Deny` firewall rule, see [Network, security, and load balancer examples in vRealize Automation cloud templates](#).

Note A cloud administrator can create a cloud template design that contains only an NSX on-demand security group and can deploy that design to create a reusable existing security group resource that members of the organization can add to network profiles and cloud template designs as an existing security group.

Firewall rules support either IPv4 or IPv6 format CIDR values for source and destination IP addresses. For an example design that uses IPv6 CIDR values in a firewall rule, see [Network, security, and load balancer examples in vRealize Automation cloud templates](#).

Using app isolation policies in on-demand security group firewall rules

You can use an app isolation policy to only allow internal traffic between the resources that are provisioned by the cloud template. With app isolation, the machines provisioned by the cloud template can communicate with each other but cannot connect outside the firewall. You can create an app isolation policy in the network profile. You can also specify app isolation in a cloud template design by using an on-demand security group with a Deny firewall rule or a private or outbound network.

An app isolation policy is created with a lower precedence. If you apply multiple policies, the policies with the higher weight will take precedence.

When you create an app isolation policy, the policy is assigned an auto-generated policy name. The policy is also made available for reuse in other cloud template designs and design iterations specific to the associated resource endpoint and project. The app isolation policy name is not visible in the cloud template design code but it is visible as a custom property on the project page (**Infrastructure > Administration > Projects**) after the cloud template design is deployed.

For the same associated endpoint in a project, any deployment that requires an on-demand security group for app isolation can use the same app isolation policy. Once the policy is created, it is not deleted. When you specify an app isolation policy, vRealize Automation searches for the policy within the project and relative to the associated endpoint - If it finds the policy it reuses it, if it does not find the policy, it creates it. The app isolation policy name is only visible after its initial deployment in the project's custom properties listing.

Using security groups in iterative cloud template development

When changing security group constraints during iterative development, where the security group is not associated to a machine in the cloud template, the security group is updated in the iteration as specified. However, when the security group is already associated to a machine, redeployment fails. You must detach existing security groups and/or `securityGroupType` resource properties from associated machines during iterative cloud template development and reassociate between each redeployment. The needed workflow is as follows, assuming that you have initially deployed the cloud template:

- 1 In the Cloud Assembly template designer, detach the security group from all its associated machines in the cloud template.
- 2 Redeploy the template by clicking **Update an existing deployment**.
- 3 Remove the existing security group constraint tags and/or `securityGroupType` properties in the template.
- 4 Add new security group constraint tags and/or `securityGroupType` properties in the template.
- 5 Associate the new security group constraint tags and/or `securityGroupType` property instances to the machines in the template.
- 6 Redeploy the template by clicking **Update an existing deployment**.

Available day 2 operations

For a list of common day 2 operations that are available for cloud template and deployment resources, see [What actions can I run on vRealize Automation Cloud Assembly deployments](#).

Learn more

For related information about using a security group for network isolation, see [Security resources in vRealize Automation](#).

For information about using security group settings in a network profile, see [Learn more about network profiles in vRealize Automation](#) and [Using security group settings in network profiles and cloud template designs in vRealize Automation Cloud Assembly](#).

For examples of cloud template designs that illustrate sample security resources and settings, see [Network, security, and load balancer examples in vRealize Automation cloud templates](#).

Using a load balancer resource in a vRealize Automation cloud template

As you create or edit your vRealize Automation cloud templates, use the most appropriate load balancer resources for your objectives.

You can use NSX and cloud-agnostic load balancer resources in a cloud template to control load balancing in a deployment.

The cloud-agnostic load balancer can be deployed across multiple clouds. A cloud-specific load balancer can specify advanced settings and features that are available only to a specific cloud/topology. Cloud-specific properties are available in the NSX load balancer (Cloud.NSX.LoadBalancer) resource type. If you add these properties on a cloud-agnostic load balancer (Cloud.LoadBalancer), they are ignored if, for example, an Amazon Web Services or Microsoft Azure load balancer is provisioned, but are respected if an NSX-V or NSX-T load balancer is provisioned. Choose one of the available load balancer resource types based on conditions in your vRealize Automation cloud template.

You cannot connect a load balancer resource directly to a security group resource in the design canvas.

Cloud agnostic load balancer resource

Use a cloud agnostic load balancer when you want to specify networking characteristics for any type of target machine.

You add a cloud agnostic load balancer by using the **Cloud Agnostic > Load Balancer** resource on the cloud template design page. The resource displays in the cloud template code as a `Cloud.LoadBalancer` resource type. The default resource displays as:

```
Cloud_LoadBalancer_1:
  type: Cloud.LoadBalancer
  properties:
    routes: []
    network: ''
    instances: []
    internetFacing: false
```

NSX load balancer resource

Use an NSX load balancer when your cloud template contains characteristics that are specific to NSX-V or NSX-T (either Policy API or Manager API methods). You can attach one or more load balancers to an NSX-V or NSX-T network or to machines that are associated to an NSX-V or NSX-T network.

You add an NSX load balancer by using the **NSX > Load Balancer** resource. The resource displays in the cloud template code as a `Cloud.NSX.LoadBalancer` resource type. The default resource displays as:

```
Cloud_NSX_LoadBalancer_1:
  type: Cloud.NSX.LoadBalancer
  properties:
    routes: []
    network: ''
    instances: []
```

Load balancer options in cloud template code

Adding one or more load balancer resources to your cloud template allows you to specify the following settings. Some examples are available at [Network, security, and load balancer examples in vRealize Automation cloud templates](#).

- Machine specification

You can specify named machine resources to participate in a load balancing pool. Alternatively you can specify that a specific machine NIC participate in the load balancer pool.

This option is available for the **NSX** load balancer resource (`Cloud.NSX.LoadBalancer`) only.

This option is available for `existing` and `public` network types. On-demand `private`, `routed`, and `outbound` network types are also supported.

- `resource.Cloud_Machine_1.id`

Specifies that the load balancer include the machine identified in the cloud template code as `Cloud_Machine_1`.

- `resource.Cloud_Machine_2.networks[2].id`

Specifies that the load balancer only include the machine identified in the cloud template code as `Cloud_Machine_2` when it is deployed to machine NIC `Cloud_Machine_2.networks[2]`.

- Logging level

The logging level value specifies a severity level for the error log. The options are NONE, EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, INFO, DEBUG, and NOTICE. The logging level value applies to all load balancers in the cloud template. This option is specific to NSX. For load balancers that have a parent, the parent logging level setting overrides any logging level setting in its children.

For related information, see topics such as [Add Load Balancers](#) in NSX product documentation.

- Type

Use a load balancer type to specify a scaling size. The default is small. This option is specific to NSX. For load balancers that have a parent, the parent type setting overrides any type setting in its children.

- Small

Correlates to compact in NSX-V and small in NSX-T.

- Medium

Correlates to large in NSX-V and medium in NSX-T.

- Large

Correlates to quad-large in NSX-V and large in NSX-T.

- Extra Large

Correlates to xlarge in NSX-V and large in NSX-T.

For related information, see topics such as [Scaling Load Balancer Resources](#) in NSX product documentation.

This option is only available for the **NSX** load balancer resource (`Cloud.NSX.LoadBalancer`).

- Algorithm (server pool)

Use an algorithm balancing method to control how incoming connections are distributed among the server pool members. The algorithm can be used on a server pool or directly on a server. All load balancing algorithms skip servers that meet any of the following conditions:

- The Admin state is set to DISABLED.
- The Admin state is set to GRACEFUL_DISABLED and there is no matching persistence entry.
- The active or passive health check state is DOWN.
- The connection limit for the maximum server pool concurrent connections is reached.

This option is specific to NSX.

- IP_HASH

Selects a server based on a hash of the source IP address and the total weight of all the running servers.

Correlates to IP-HASH in NSX-V and NSX-T.

- LEAST_CONNECTION

Distributes client requests to multiple servers based on the number of connections already on the server. New connections are sent to the server with the fewest connections. Ignores the server pool member weights even if they are configured.

Correlates to LEASTCONN in NSX-V and LEAST_CONNECTION in NSX-T.

- ROUND_ROBIN

Incoming client requests are cycled through a list of available servers capable of handling the request. Ignores the server pool member weights even if they are configured. Default.

Correlates to ROUND_ROBIN in NSX-V and NSX-T.

- **WEIGHTED_LEAST_CONNECTION**

Each server is assigned a weight value that signifies how that server performs relative to other servers in the pool. The value determines how many client requests are sent to a server compared to other servers in the pool. This load balancing algorithm focuses on using the weight value to distribute the load among the available server resources fairly. By default, the weight value is 1 if the value is not configured and slow start is enabled.

Correlates to WEIGHTED_LEAST_CONNECTION in NSX-T. There is no correlation in NSX-V.

- **WEIGHTED_ROUND_ROBIN**

Each server is assigned a weight value that signifies how that server performs relative to other servers in the pool. The value determines how many client requests are sent to a server compared to other servers in the pool. This load balancing algorithm focuses on fairly distributing the load among the available server resources.

Correlates to WEIGHTED_ROUND_ROBIN in NSX-T. There is no correlation in NSX-V.

- **URI**

The left part of the URI is hashed and divided by the total weight of the running servers. The result designates which server receives the request. This ensures that a URI is always directed to the same server if no server goes up or down. The URI algorithm parameter has two options `uriLength=<len>` and `uriDepth=<dep>`. The length parameter range should be $1 \leq \text{len} < 256$. The depth parameter range should be $1 \leq \text{dep} < 10$. Length and depth parameters are followed by a positive integer number. These options can balance servers based on the beginning of the URI only. The length parameter indicates that the algorithm should only consider the defined characters at the beginning of the URI to compute the hash. The depth parameter indicates the maximum directory depth to be used to compute the hash. One level is counted for each slash in the request. If both parameters are specified, the evaluation stops when either is reached.

Correlates to URI in NSX-V. There is no correlation in NSX-T.

- **HTTPHEADER**

HTTP header name is looked up in each HTTP request. The header name in parentheses is not case-sensitive. If the header is absent or does not contain any value, the round robin algorithm is applied. The HTTPHEADER algorithm parameter has one option `headerName=<name>`.

Correlates to HTTPHEADER in NSX-V. There is no correlation in NSX-T.

- **URL**

URL parameter specified in the argument is looked up in the query string of each HTTP GET request. If the parameter is followed by an equal sign = and a value, then the value is hashed and divided by the total weight of the running servers. The result designates which server receives the request. This process is used to track user identifiers in requests and ensure that a same user ID is always sent to the same server as long as no server goes up or down. If no value or parameter is found, then a round robin algorithm is applied. The URL algorithm parameter has one option `urlParam=<url>`.

Correlates to URL in NSX-V. There is no correlation in NSX-T.

For related information, see topics such as [Add a Server Pool for Load Balancing](#) in NSX product documentation.

NSX-V and NSX-T networks and load balancer options

Load balancer options depend on the network that the load balancer resource is associated to in the cloud template. You can configure a load balancer relative to the network type and network conditions.

- On-demand outbound network

If the load balancer computes are attached to an on-demand `outbound` network, a load balancer is created for the Tier-1 router of the on-demand network.

- On-demand private network

If the load balancer computes are attached to an on-demand `private` network, a new Tier-1 router is created and attached to the Tier-0 router specified in the network profile. The load balancer is then attached to the Tier-1 router. The Tier-1 router VIP advertisement is enabled if the VIP is on an `existing` network. If a `private` network is configured for DHCP, the private network and load balancer share the Tier-1 router.

- Existing network

If the load balancer is attached to an `existing` network, the load balancer is created with the Tier-1 router of the existing network. A new load balancer is created if there is no load balancer attached to the Tier-1 router. If the load balancer already exists, new virtual servers are attached to it. If the `existing` network is not attached to a Tier-1 router, a new Tier-1 router is created and attached to a Tier-0 router defined in the network profile, the Tier-1 router VIP advertisement is not enabled.

- Network isolation defined in the network profile

For network types of `outbound` or `private`, you can specify network isolation settings in a network profile to emulate a new security group. Because machines are attached to an existing network and isolation settings are defined in the profile, this option is similar to a load balancer created on an existing network. The difference is that to enable the data path, the Tier-1 uplink port IP is added to the isolation security group.

You can specify load balancer settings for NSX-associated networks by using an NSX load balancer resource in the cloud template design.

To learn more, see VMware blog post [vRA Cloud Assembly Load Balancer with NSX-T Deep Dive](#).

Reconfiguring logging level or type settings when multiple load balancers share an NSX-T Tier 1 or NSX-V Edge

When using a cloud template that contains multiple load balancers which share a Tier-1 router in the NSX-T endpoint or an Edge router in the NSX-V endpoint, reconfiguring the logging level or type settings in one of the load balancer resources does not update the settings for the other load balancers. Mismatched settings cause inconsistencies in NSX. To avoid inconsistencies when reconfiguring these logging level and/or type settings, use the same reconfiguration values for all the load balancer resources in the cloud template which share a Tier 1 or Edge in their associated NSX endpoint.

Available day 2 operations

When you scale in or scale out a deployment that contains a load balancer, the load balancer is configured to include newly added machines or to stop load balancing machines that are targeted for tear down.

For a list of common day 2 operations that are available for cloud templates and deployments, see [What actions can I run on vRealize Automation Cloud Assembly deployments](#).

Learn more

For information about defining load balancer settings in a network profile, see [Learn more about network profiles in vRealize Automation](#)

For examples of cloud template designs that include load balancers, see [Network, security, and load balancer examples in vRealize Automation cloud templates](#).

Puppet-enabled cloud template with username and password access

In this example, you add Puppet configuration management to a cloud template deployed on a vCenter compute resource with username and password access.

This procedure shows an example of how you might create a Puppet enabled deployable resource that requires username and password authentication. Username and password access means that the user must manually log in from the compute resource to the Puppet primary machine in order to invoke Puppet configuration management.

Optionally, you can configure remote access authentication which sets up configuration management in a cloud template so that the compute resource handles authentication with the Puppet primary machine. With remote access enabled, the compute resource automatically generates a key to satisfy password authentication. A valid username is still required.

See [AWS Puppet configuration management cloud template examples](#) and [vCenter Puppet configuration cloud template examples](#) for more examples of how you can configure different Puppet scenarios in vRealize Automation Cloud Assembly blueprints.

Prerequisites

- Set up a Puppet Enterprise instance on a valid network.

- Add your Puppet Enterprise instance to vRealize Automation Cloud Assembly using the Integrations feature. See [Configure Puppet Enterprise integration in vRealize Automation Cloud Assembly](#)
- Set up a vSphere account and a vCenter compute resource.

Procedure

- 1 Add a Puppet configuration management component to a vSphere compute resource on the canvas for the desired cloud template.
 - a Select **Infrastructure > Manage > Integrations**.
 - b Click **Add Integration** and select Puppet.
 - c Enter the appropriate information on the Puppet configuration page.

Configuration	Description	Example Value
Hostname	Host name or IP address of the Puppet primary machine	Puppet-Ubuntu
SSH Port	SSH port for communication between vRealize Automation Cloud Assembly and Puppet primary machine. (Optional)	NA
Autosign secret	The shared secret configured on the Puppet primary machine that nodes should provide to support autosign certificate requests.	User specific
Location	Indicate whether the Puppet primary machine is on a private or public cloud. Note Cross cloud deployment is supported only if there is connectivity between the deployment compute resource and the Puppet primary machine.	
Cloud proxy	Not required for public cloud accounts, such as Microsoft Azure or Amazon Web Services. If you are using a vCenter based cloud account, select the appropriate cloud proxy for your account.	NA
Username	SSH and RBAC user name for Puppet primary machine.	User specific. YAML value is '\$ {input.username}'
Password	SSH and RBAC password for Puppet primary machine.	User specific YAML value is '\$ {input.password}'
Use sudo commands for this user	Select to use sudo commands for the procidd.	true
Name	Puppet primary machine name.	PEMasterOnPrem
Description		

- 2 Add the username and password properties to the Puppet YAML as shown in the following example.
- 3 Ensure that the value for the remoteAccess property to the Puppet cloud template YAML is set to authentication: username and password as shown in the example below.

Example: vCenter username and password YAML code

The following example shows the representative YAML code for adding username and password authentication on a vCenter compute resource.

```
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}'
```

AWS Puppet configuration management cloud template examples

There are several options for configuring cloud templates to support Puppet based configuration management on AWS compute resources.

Puppet management on AWS with username and password

Example of...	Sample Blueprint YAML
authentication of cloud configuration on any supported Amazon Machine Image.	<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: PEOAWS environment: production role: 'role::linux_webserver' host: '\${Webserver.*}' osType: linux username: '\${input.username}' password: '\${input.password}' useSudo: true </pre>
Authentication of cloud configuration on a custom Amazon Machine Image with an existing user.	<pre> inputs: username: type: string title: Username default: puppet password: type: string title: Password encrypted: true default: VMware@123 </pre>

Example of...	Sample 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 management on AWS with generated PublicPrivateKey

Example of...	Sample Blueprint YAML
remoteAccess.authentication authentication on AWS with generatedPublicPrivateKey access.	<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>

vCenter Puppet configuration cloud template examples

There are several options for configuring cloud templates to support Puppet based configuration management on vCenter compute resources.

Puppet on vSphere with username and password authentication

The following example shows example YAML code for Puppet on a vSphere OVA with username and password authentication.

Table 6-5.

Example of...	Sample Blueprint YAML
YAML code for Puppet on a vSphere OVA with username and password authentication.	<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>
YAML code for Puppet on a vSphere OVA with username and password authentication on the compute resource.	<pre> inputs: username: type: string title: Username default: puppet </pre>

Table 6-5. (continued)

Example of...	Sample Blueprint YAML
	<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>
<p>YAML code for Puppet on a vCenter with remote access enabled password authentication on the compute resource.</p>	<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>

Table 6-5. (continued)

Example of...	Sample 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 on vSphere with generated PublicPrivateKey authentication

Table 6-6.

Example of...	Sample Blueprint YAML
YAML code for Puppet on a vSphere OVA with generated PublicPrivateKey authentication on the compute resource.	<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>

How to include Terraform configurations in vRealize Automation Cloud Assembly

You can embed Terraform configurations as a resource in cloud templates in vRealize Automation Cloud Assembly.

Preparing a vRealize Automation Cloud Assembly Terraform runtime environment

Designs that include Terraform configurations require access to a Terraform runtime environment that you integrate with the vRealize Automation Cloud Assembly on-premises product.

How to add a Terraform runtime

The runtime environment consists of a Kubernetes cluster that runs Terraform CLI commands to perform requested operations. In addition, the runtime collects logs and returns the results from Terraform CLI commands.


The vRealize Automation on-premises product requires users to configure their own Terraform runtime Kubernetes cluster. Only one Terraform runtime per organization is supported. All Terraform deployments for that organization use the same runtime.

- 1 Verify that you have a Kubernetes cluster on which to run the Terraform CLI.
 - All users can supply a kubeconfig file to run the Terraform CLI on an unmanaged Kubernetes cluster.
 - Enterprise license users have the option to run the Terraform CLI on a Kubernetes cluster managed by vRealize Automation.

In vRealize Automation Cloud Assembly, go to **Infrastructure > Resources > Kubernetes**, and verify that you have a Kubernetes cluster. See [How do I work with Kubernetes in vRealize Automation Cloud Assembly](#) if you need to add one.
- 2 If the Kubernetes cluster is newly added or modified, wait for its data collection to complete.

Data collection retrieves the list of namespaces and other information, and might take up to 5 minutes depending on provider.
- 3 After data collection completes, go to **Infrastructure > Integrations > Add Integration**, and select the **Terraform Runtime** card.
- 4 Enter settings.

Figure 6-3. Example Terraform runtime integration



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)

Setting	Description
Name	Give the runtime integration a unique name.
Description	Explain what the integration is for.
Terraform Runtime Integration:	
Runtime type (Enterprise only)	Enterprise license users may select whether to run the Terraform CLI on a Kubernetes cluster managed by vRealize Automation or an unmanaged one.
Kubernetes kubeconfig (all users)	<p>For an unmanaged Kubernetes cluster, paste in the entire contents of the kubeconfig file for the external cluster.</p> <p>To use an external Kubernetes runtime with a proxy server, see How to add proxy support.</p> <p>This option is available for all users.</p>
Kubernetes cluster (Enterprise only)	<p>For Kubernetes managed by vRealize Automation, select the cluster in which to run the Terraform CLI.</p> <p>The cluster and its kubeconfig file must be reachable. You can validate access to kubeconfig with a GET on <code>/cmx/api/resources/k8s/clusters/{clusterId}/kube-config</code>.</p> <p>This option is only available for Enterprise licenses.</p>
Kubernetes namespace	Select the namespace to use within the cluster, for creating pods that run the Terraform CLI.
Runtime Container Settings:	

Setting	Description
Image	Enter the path to the container image of the Terraform version that you want to run. Note The VALIDATE button doesn't check for the container image.
CPU request	Enter the amount of CPU for running containers. Default is to 250 millicores.
CPU limit	Enter the maximum allowable CPU for running containers. Default is to 250 millicores.
Memory request	Enter the amount of memory for running containers. Default is 512 MB.
Memory limit	Enter the maximum allowable memory for running containers. Default is 512 MB.

5 Click **VALIDATE** and adjust settings as needed.

6 Click **ADD**.

Settings are cached. After adding the integration, you can modify settings such as the cluster or namespace, but it might take up to 5 minutes for a change to be detected and for the Terraform CLI to run under the new settings.

Troubleshooting the Terraform runtime

Some Terraform configuration deployment problems might be related to the runtime integration.

Problem	Cause	Resolution
Validation fails with an error stating that the namespace is invalid.	You modified the cluster but left the previous namespace in the UI.	Always reselect a namespace after modifying the cluster selection.
The namespace drop down is empty or doesn't list newly added namespaces.	Data collection for the cluster has not completed. Data collection takes up to 5 minutes after entering or modifying the cluster and up to 10 minutes when entering or modifying the namespace.	For a new cluster with existing namespaces, wait up to 5 minutes for data collection to complete. For a new namespace in an existing cluster, wait up to 10 minutes for data collection to complete. If the problem continues, remove the cluster and re-add it under Infrastructure > Resources > Kubernetes .

Problem	Cause	Resolution
Terraform CLI containers are created in a previous cluster, previous namespace, or with previous runtime settings, even after the integration account was updated.	The Kubernetes API client used by vRealize Automation is cached for 5 minutes.	Changes might need up to 5 minutes to take effect.
Validation or a Terraform deployment operation fails with an error stating that kubeconfig is not available.	Sometimes these errors occur because the cluster isn't reachable from vRealize Automation. In other cases, user credentials, tokens, or certificates are invalid.	The kubeconfig error can occur for a number of reasons and might require engagement with technical support for troubleshooting.

How to add proxy support

To have your external Kubernetes runtime cluster connect through a proxy server, follow these steps.

- 1 Log in to your Kubernetes cluster server.
- 2 Create an empty folder.
- 3 In the new folder, add the following lines to a new file named Dockerfile.

```
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 Modify the placeholder values so that the `https_proxy` and `http_proxy` environment variables include the proxy server settings that you use to access the internet.

The *protocol* will be http or https according to what your proxy server uses, which might not match the environment variable name of `https_proxy` or `http_proxy`.

- 5 Save and close Dockerfile.
- 6 From the empty folder, run the following command. Depending on your account privileges, you might need to run the command in sudo mode.

```
docker build --file Dockerfile --tag custom-terraform-runtime:1.0 .
```

The command creates a local custom-terraform-runtime:1.0 Docker image.

- 7 In vRealize Automation Cloud Assembly, under **Infrastructure > Connections > Integrations**, go to your Terraform runtime integration.
- 8 Create or edit the runtime container settings to use the custom-terraform-runtime:1.0 image:

Runtime Container Settings

Image

custom-terraform-runtime:1.0

ⓘ

vRealize Automation Cloud Assembly Terraform runtime with no internet access

vRealize Automation Cloud Assembly users who need to design and run Terraform integrations while disconnected from the internet can set up their runtime environment by following this example.

Note You must temporarily connect to the internet during setup.

This process assumes that you have [your own Docker registry](#) and can access its repositories without an internet connection.

Create the custom container image

- 1 Build a custom container image that includes the Terraform provider plug-in binaries.

The following Dockerfile shows an example of creating a custom image with the Terraform GCP provider.

The base image `projects.registry.vmware.com/vra/terraform:latest` download in the Dockerfile requires temporary internet access to the VMware Harbor registry at `projects.registry.vmware.com`.

Firewall settings or proxy settings can cause the image build to fail. You might need to enable temporary access to `releases.hashicorp.com` to download the Terraform provider plug-in binaries. However, you may use your private registry to supply the plug-in binaries as an option.

```
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 Build, tag, and push the custom container image to your own Docker repository.
- 3 In vRealize Automation Cloud Assembly, under **Infrastructure > Connections > Integrations**, go to your Terraform runtime integration.
- 4 Create or edit the runtime container settings to add your repository for the custom container image. The example built custom container image name is `registry.ourcompany.com/project1/image1:latest`.

Runtime Container Settings	
Image	<u>registry.ourcompany.com/project1/image1:latest</u> ⓘ

Host the Terraform CLI locally

- 1 Download the Terraform CLI binaries.
- 2 Upload the Terraform CLI binaries to your local web server.
- 3 In vRealize Automation Cloud Assembly, go to **Infrastructure > Configure > Terraform Versions**.
- 4 Create or edit the Terraform version so that it includes the URL to the Terraform CLI binaries hosted on your local web server.

0.12.29 DELETE	
Version *	<u>0.12.29</u> ⓘ
Description	<div></div>
Enabled	<input checked="" type="checkbox"/> ⓘ
URL *	<u>http://host1.ourcompany.com:8080/tf/0.12.29/terraform_0.12.29_linux_amd64.zip</u> ⓘ
SHA256 Checksum *	<u>872245d9c6302b24dc0d98a1e010aef1e4ef60865a2d1f60102c8ad03e9d5a1d</u> ⓘ

Design and deploy Terraform configurations

With the runtime in place, you can add Terraform configuration files to git, design cloud templates for them, and deploy.

To get started, see [Preparing for Terraform configurations in vRealize Automation Cloud Assembly](#).

Troubleshooting

When deploying, open the deployment in vRealize Automation Cloud Assembly. Under the History tab, look for Terraform events, and click **Show Logs** to the right. When your local Terraform provider is working, the following messages appear in the log.

```
Initializing provider plugins
```

```
Terraform has been successfully initialized
```


For a more robust log, you can manually edit the cloud template code to add `TF_LOG: DEBUG` as shown in the following example.

```
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
```

Preparing for Terraform configurations in vRealize Automation Cloud Assembly

Before you add a Terraform configuration to a vRealize Automation Cloud Assembly template, set up and integrate your version control repository.

- 1 [Prerequisites](#)
- 2 [Store Terraform configuration files in a version control repository](#)
- 3 [Enable cloud zone mapping](#)
- 4 [Integrate your repository with vRealize Automation Cloud Assembly](#)

Prerequisites

For the vRealize Automation on-premises product to run Terraform operations, you need the Terraform runtime integration. See [Preparing a vRealize Automation Cloud Assembly Terraform runtime environment](#).

Store Terraform configuration files in a version control repository

vRealize Automation Cloud Assembly supports the following version control repositories for Terraform configurations.

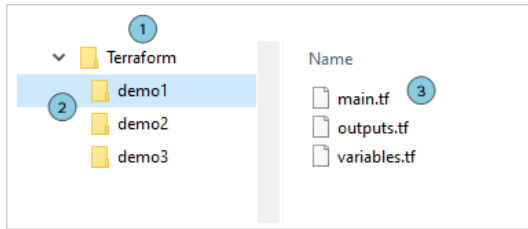
- GitHub cloud, GitHub Enterprise on-premises
- GitLab cloud
- Bitbucket on-premises

In your version control repository, create a default directory with one layer of subdirectories, each with Terraform configuration files. Create one subdirectory per Terraform configuration.

- 1 [Default directory](#)

- 2 Single subdirectory layer
- 3 Deployment-ready Terraform configuration files

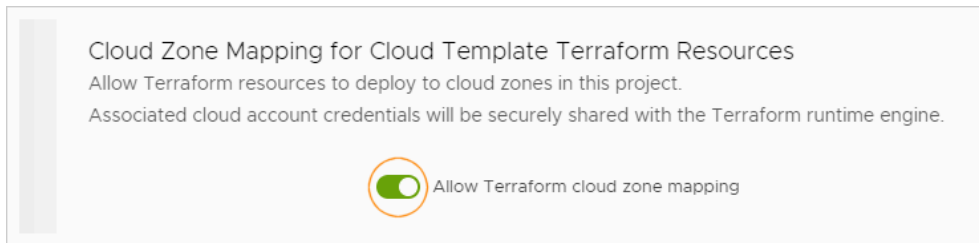
Don't include a Terraform state file with configuration files. If `terraform.tfstate` is present, errors occur during deployment.



Enable cloud zone mapping

If you expect to deploy to a cloud account, the Terraform runtime engine needs those cloud zone credentials.

In the project **Provisioning** tab, enable **Allow Terraform cloud zone mapping**.



Even though credentials are securely transmitted, for additional security, you should leave the option deactivated if project users don't need to deploy to a cloud account.

Integrate your repository with vRealize Automation Cloud Assembly

In vRealize Automation Cloud Assembly, go to **Infrastructure > Connections > Integrations**.

Add an integration to the repository offering type where you stored the Terraform configurations: GitHub, GitLab, or Bitbucket.

When you add your project to the integration, select the **Terraform Configurations** type, and identify the repository and branch.

Folder is the default directory of your earlier structure.

Add Repository: testProject

Configure a repository to be used for this project.

Type *	Terraform Configurations	▼ ⓘ
Repository *	parnassusdemo/repository1	ⓘ
Branch *	master	
Folder	/Terraform	

Designing for Terraform configurations in vRealize Automation Cloud Assembly

With your repository and Terraform configuration files in place, you can design a vRealize Automation Cloud Assembly template for them.

- 1 [Prerequisites](#)
- 2 [Enable Terraform runtime versions](#)
- 3 [Add Terraform resources to the design](#)
- 4 [Deploy the cloud template](#)

Prerequisites

Set up and integrate your version control repository. See [Preparing for Terraform configurations in vRealize Automation Cloud Assembly](#).

Enable Terraform runtime versions

You can define the Terraform runtime versions available to users when deploying Terraform configurations. Note that Terraform configurations might also include internally coded version constraints.

To create the list of allowable versions, go to **Infrastructure > Configure > Terraform Versions**. Only versions 0.12.x are supported.

Add Terraform resources to the design

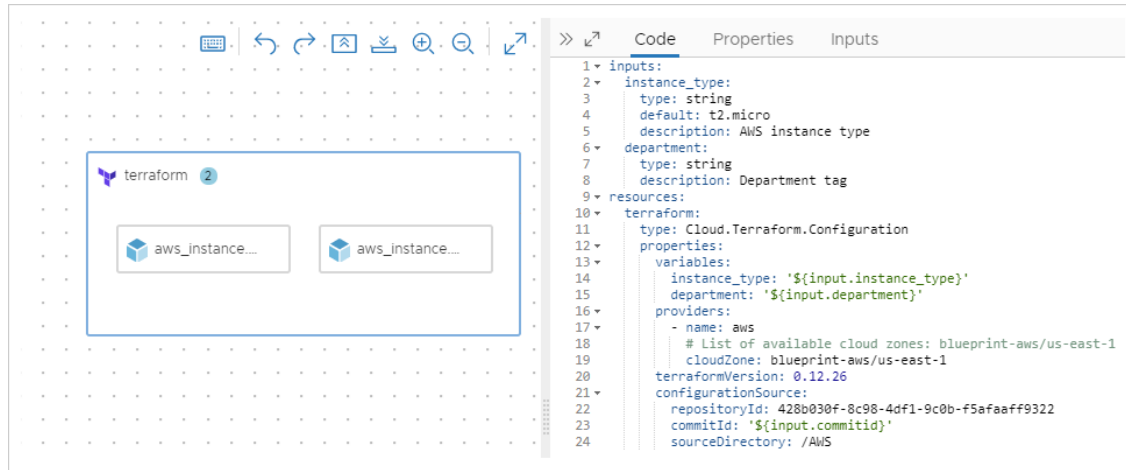
Create your cloud template that includes Terraform configurations.

- 1 In vRealize Automation Cloud Assembly, go to **Design > Cloud Templates** and click **New from > Terraform**.
The Terraform configuration wizard appears.
- 2 Follow the prompts.

Wizard Page	Setting	Value
New Cloud Template	Name	Give the design an identifying name.
	Description	Explain what the design is for.
	Project	Select the project that includes the repository integration where the Terraform configuration is stored.
Configuration Source	Repository	Select the integrated repository where you stored the Terraform configuration.
	Commit	Select a repository commit, or leave the entry blank to use the Terraform configuration from the repository head. Bitbucket Limitation—The number of selectable commits might be truncated because of the Bitbucket repository server configuration.
	Source directory	Select a subdirectory from the repository structure that you created. The example subdirectories shown in the earlier setup were demo1, demo2, and demo3.
Finalize Configuration	Repository	Verify the correct repository selection.
	Source directory	Verify the correct directory selection.
	Terraform version	Select the Terraform runtime version to run when deploying the Terraform configuration.
	Providers	If the Terraform configuration included a provider block, verify the provider and cloud zone that this cloud template will deploy to. Having no provider isn't a problem. After finishing the wizard, just edit the provider and cloud zone in the template properties to add or change the deployment target.
	Variables	Select sensitive values for encryption, such as passwords.
	Outputs	Verify the outputs from the Terraform configuration, which convert to expressions that your design code can further reference.

3 Click **Create**.

The Terraform resource appears on the cloud template canvas, with vRealize Automation Cloud Assembly code that reflects the Terraform configuration to deploy.



If desired, you can add other vRealize Automation Cloud Assembly resources to the cloud template, to combine Terraform and non-Terraform code into a hybrid design.

Note Updating Terraform configurations in the repository doesn't synchronize the changes into your cloud template. Automatic synchronization can introduce security risks, such as newly added sensitive variables.

To capture Terraform configuration changes, rerun the wizard, choose the new commit, and identify any new sensitive variables.

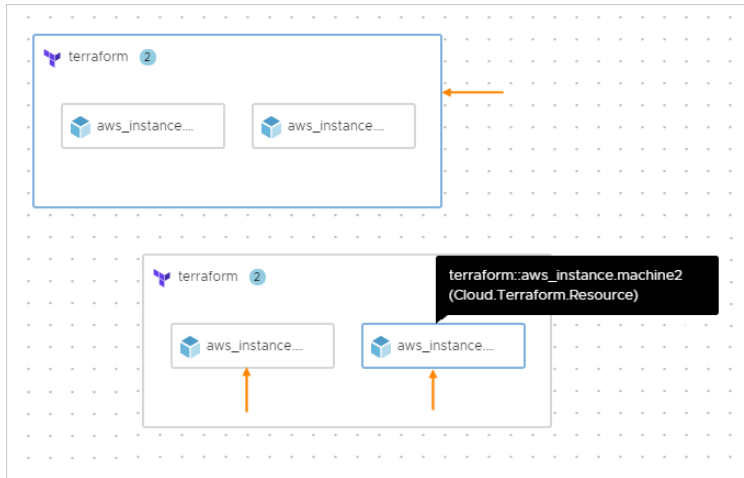
Deploy the cloud template

When you deploy the cloud template, the deployment **History** tab lets you expand an event such as an allocate or create phase, to inspect a log of messages from the Terraform CLI.

Approvals—In addition to the expected Terraform phases such as PLAN, ALLOCATE, or CREATE, vRealize Automation Cloud Assembly introduces governance by means of an approval phase. See [How do I configure Service Broker approval policies](#) for more information about request approvals.

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...			

After deploying, you see an outer resource that represents the overall Terraform component, with child resources inside for the separate components that Terraform created. The parent Terraform resource controls the lifecycle of the child resources.



Learn more about Terraform configurations in vRealize Automation

Be aware of certain limitations and troubleshooting when you embed Terraform configurations as a resource in vRealize Automation.

Limitations for Terraform configurations

- When validating a design with Terraform configurations, the TEST button checks vRealize Automation Cloud Assembly syntax but not the native Terraform code syntax.

In addition, the TEST button doesn't validate commit IDs associated with Terraform configurations.

- For a cloud template that includes Terraform configurations, cloning the template to a different project requires the following workaround.
 - In the new project, under the **Integrations** tab, copy the `repositoryId` for your integration.
 - Open the clone template. In the code editor, replace the `repositoryId` with the one you copied.
- In the version control repository, don't include a Terraform state file with configuration files. If `terraform.tfstate` is present, errors occur during deployment.

Supported day 2 actions for the parent Terraform resource

For the parent Terraform resource, you can view or refresh the Terraform state file. For more about the state file actions, see the comprehensive list of actions at [What actions can I run on vRealize Automation Cloud Assembly deployments](#).

Supported day 2 actions for child resources

After deploying Terraform configurations, it might take up to 20 minutes for a day 2 action to become available on child resources.

For child resources in a Terraform configuration, only the following subset of day 2 actions are supported. For details about the actions, look them up in the comprehensive list of actions at [What actions can I run on vRealize Automation Cloud Assembly deployments.](#)

Provider	Terraform Resource Type	Supported Day 2 Actions
AWS	aws_instance	Power On
		Power Off
		Reboot
		Reset
Azure	azurerm_virtual_machine	Power On
		Power Off
		Restart
		Suspend
vSphere	vsphere_virtual_machine	Power On
		Power Off
		Reboot
		Reset
		Shutdown
		Suspend
		Create Snapshot
		Delete Snapshot
		Revert Snapshot
GCP	google_compute_instance	Power On
		Power Off
		Create Snapshot
		Delete Snapshot

Troubleshooting day 2 action availability

Out-of-the-box (OOTB) day 2 actions that are missing or deactivated might need troubleshooting.

Problem	Cause	Resolution
A Terraform resource does not have an expected OOTB day 2 action on the Actions menu.	The action might not be supported for the provider and resource type as mentioned in the previous list. Alternatively, the action might need up to 20 minutes to appear due to the timing of resource discovery and resource caching.	Check the provider and resource type in the design. Wait up to 20 minutes for data collection to complete.
A Terraform resource does not have an expected day 2 action even after the 20 minutes to account for data collection.	A resource discovery problem is preventing the action from appearing. One way that happens is when the resource is accidentally created on an out-of-project cloud zone. For example, your project only includes a cloud account and region us-east-1 cloud zone, but the Terraform configuration includes a provider block for us-west-1, and you didn't change it at design time. Another possibility is that data collection isn't working.	Check the project cloud zones against the cloud zones in the design. Go to Infrastructure > Connections > Cloud Accounts and check the data collection status and last successful collection time for the cloud account.
Even though there are no obvious problems with the resource state and data collection, a day 2 action is deactivated (gray).	Occasional, intermittent timing issues and data collection failures are known to occur.	The problem should resolve itself within 20 minutes.
The wrong day 2 action is deactivated, one that should be active based on the resource state. For example, Power Off is enabled, and Power On is deactivated, even though the resource was powered off using the provider interface.	Data collection timing can cause a temporary mismatch. If you change the power state from outside vRealize Automation, it takes time to correctly reflect the change.	Wait up to 20 minutes.

Using custom Terraform providers in vRealize Automation

If you have created and want to use a custom Terraform provider, take the following steps.

- 1 Under the default Terraform directory in your git version control repository, add the following subdirectory structure.

```
terraform.d/plugins/linux_amd64
```

- 2 Add your custom Terraform provider Go binaries to the `linux_amd64` directory.

By default, `terraform init` will search that directory for custom provider plug-ins.

Note VMware has seen cases where a custom Terraform provider fails to run and posts a `no such file or directory` message.

If that happens, try recompiling your custom provider Go binaries with CGO deactivated (set to zero). CGO is for Go packages that call C code.

How to use the vRealize Automation Cloud Assembly Marketplace

To jumpstart your resource library, download files from the vRealize Automation Cloud Assembly Marketplace. The Marketplace provides finished cloud templates and open virtualization images.

How to access the Marketplace

In vRealize Automation Cloud Assembly, select **Infrastructure > Connections > Integrations**. Click **Add Integration**, click **My VMware**, and provide your My VMware account credentials.

How to download and use Marketplace cloud template files

In the **Marketplace** tab, click **Get**, and accept the cloud template EULA. Then, you can add the template to a vRealize Automation Cloud Assembly project, or simply download it. You can upload a cloud template in the **Design** tab.

For a project-based example, imagine that you are a project administrator for a Big Data effort. To assist your team, you locate a Marketplace Hadoop template that you add to the team project. You then customize the cloud template for your resource environment, and release it. Then, you import the template into the vRealize Automation Service Broker catalog so that your team can deploy it.

How to download and use Marketplace image files

In the **Marketplace** tab, click **Get**, and accept the OVF or OVA image EULA. Afterward, you can download the OVF or OVA image and reference it in cloud template code.

Continuing with the previous example, your team might need access to a version of Hadoop itself. You download a Hadoop OVF and add it to cloud account resources such as a vCenter Server Content Library. You then update any template code that needs to point to the OVF image.

Managing vRealize Automation Cloud Assembly deployments

7

As a vRealize Automation Cloud Assembly cloud template developer, you use the Deployment tab to manage your deployments. You can troubleshoot failed provisioning processes, make changes, and destroy unused deployments.

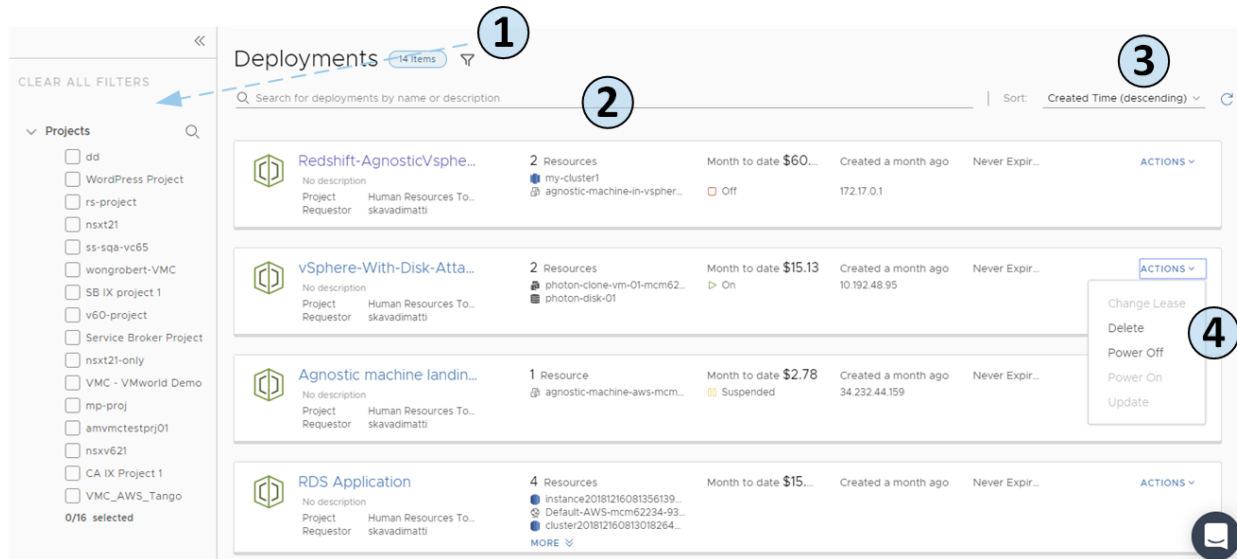
Deployments are the provisioned instances of cloud templates. The Deployments tab displays your successful and failed deployments. You use the page to manage your successful deployments or to begin troubleshooting any failed requests.

Working with deployment cards

You can locate and manage your deployments using the card list. You can filter or search for specific deployments, and then run actions on those deployments.

- 1 Filter your requests based on attributes.
- 2 Search for deployments based on keywords or requestor.
- 3 Sort the list to order by time or name.
- 4 Run deployment-level actions on the deployment, including deleting unused deployments to reclaim resources.

You can also see deployment costs, expiration dates, and status.



This chapter includes the following topics:

- How do I monitor deployments in vRealize Automation Cloud Assembly
- What can I do if a vRealize Automation Cloud Assembly deployment fails
- How do I manage the life cycle of a completed vRealize Automation Cloud Assembly deployment
- What actions can I run on vRealize Automation Cloud Assembly deployments

How do I monitor deployments in vRealize Automation Cloud Assembly

After you deploy a vRealize Automation Cloud Assembly cloud template, you can monitor your request to ensure that the resources are provisioned and running. Beginning with the deployment card, you can verify the provisioning of your resources. Next, you can examine the deployment details. Finally, you can view deleted deployments.

Procedure

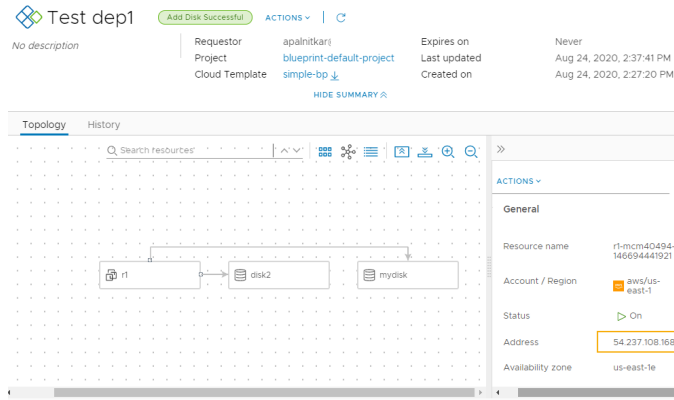
- 1 Click **Deployments** and locate your in-process deployment card using the filter and search, if needed.
- 2 Review the card status.

If the deployment is in progress, the process bar indicates the number of tasks remaining. If the deployment completed successfully, the card displays the basic details about the



- 3 To determine where your resources were deployed, click the deployment name and review the details on the Topology page.

You will likely need the IP address for the primary component. As you click on each component, notice the information provided that is specific to the component. In this example, the IP address is highlighted.



The availability of the external link depends on the cloud provider. Where it is available, you must have the credential on that provider to access the component.

What to do next

- You can make changes to your deployment. See [How do I manage the life cycle of a completed vRealize Automation Cloud Assembly deployment.](#)
- If your deployment fails, see [What can I do if a vRealize Automation Cloud Assembly deployment fails.](#)

What can I do if a vRealize Automation Cloud Assembly deployment fails

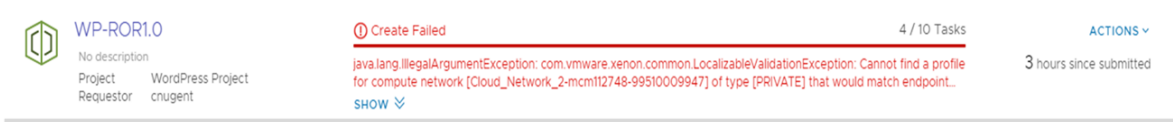
Your deployment request might fail for many reasons. It might be due to network traffic, a lack of resources on the target cloud provider, or a flawed deployment specification. Or, the deployment succeeded, but it does not appear to be working. You can use vRealize Automation Cloud Assembly to examine your deployment, review any error messages, and determine whether the problem is the environment, the requested workload specification, or something else.

You use this workflow to begin your investigation. The process might reveal that the failure was due to a transient environmental problem. Redeploying the request after verifying the conditions have improved resolves this type of problem. In other cases, your investigation might require you to examine other areas in detail.

As a project member, you can review the request details in vRealize Automation Cloud Assembly.

Procedure

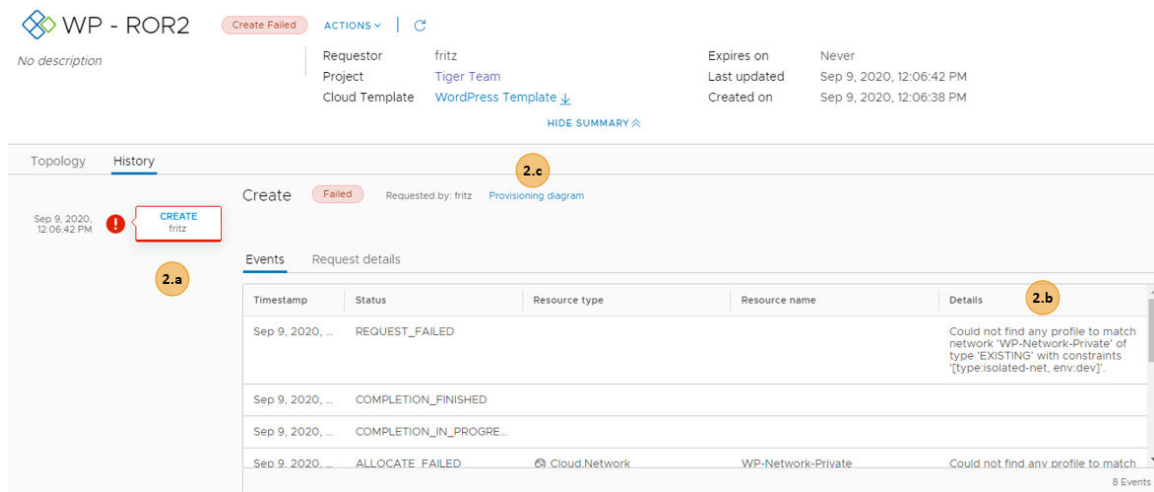
- 1 To determine if a request failed, click the **Deployments** tab and locate the deployment card.



Failed deployments are indicated on the card.

- a Review the error message.
- b For more information, click the deployment name for the deployment details.

- 2 On the deployment details page, click the **History** tab.



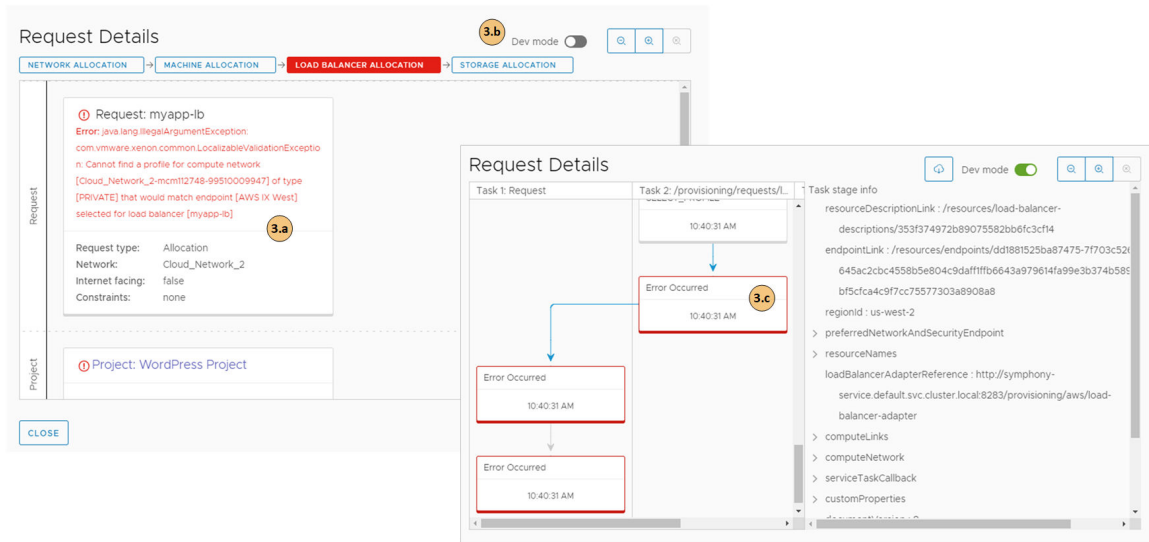
- a Review the event tree to see where the provisioning process failed. This tree is useful when you modify a deployment, but the change fails.

The tree also shows when you run deployment actions. You can use the tree to troubleshoot failed changes.

- b The **Details** provides a more verbose version of the error message.
- c If the requested item was a vRealize Automation Cloud Assembly cloud template, the link to the right of the message opens vRealize Automation Cloud Assembly so that you can see the **Request Details**.

- 3 The **Request Details** provides the provisioning workflow for failed components so that you can research the problem.

The request history is retained for one week.

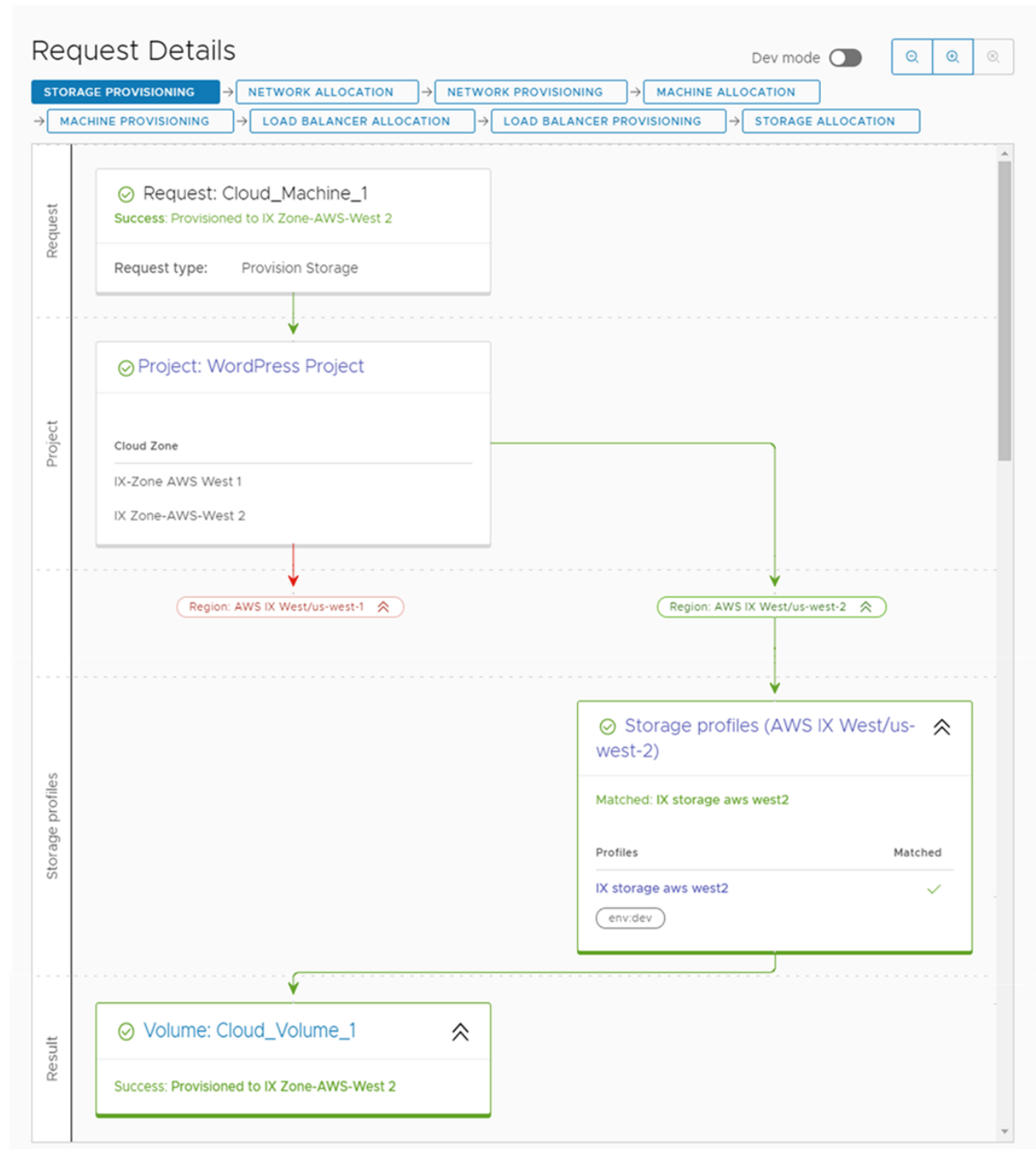


- a Review the error message.
 - b You can turn on the **Dev mode** to switch between the simple provisioning workflow and a more detailed flowchart.
 - c Click the card to review the deployment script.
- 4 Resolve the errors and redeploy the cloud template.

The errors might be in the template construction or they might be related to how your infrastructure is configured.

What to do next

When the errors are resolved and the cloud template is deployed, you can see information similar to the following example in the Request Details. To see the request details, select **Infrastructure > Activity > Requests**.



How do I manage the life cycle of a completed vRealize Automation Cloud Assembly deployment

After a deployment is provisioned and running, you have several actions that you can run to manage the deployment. The life cycle management can include powering on or off, resizing, and deleting a deployment. You can also run various actions on individual components to manage them.

Procedure

- 1 Click **Deployments** and locate your deployment.
- 2 To access the deployment details, click the deployment name.

You can use the Topology tab to visualize the deployment structure and resources.

The History tab includes all the provisioning events and any events related to actions that you run after the requested item is deployed. If there are any problems with the provisioning process, the History tab events will help you with troubleshooting the failures.

The Cost tab provides the current cost of some components since they were deployed.

The first screenshot shows the **Topology** tab. It displays a diagram with two components: **Cloud_AWS_Vo...** and **Cloud_AWS_EC...**. The right sidebar shows details for **Cloud_AWS_Volume_1**, including Resource Name (attached-ebs-disk), CapacityGB (1), and Type (HDD).

The second screenshot shows the **History** tab. It displays a table of events for all requests. The table has columns for Timestamp, Status, Resource Type, Resource Name, and Details. The events listed are:

Timestamp	Status	Resource Type	Resource Name	Details
Dec 20, 2018, 4:35:46 AM	REQUEST_FINISH			
Dec 20, 2018, 4:35:45 AM	CREATE_FINISH	Cloud AWS E C2 Instance	Cloud_AWS_EC_2_Instance_1	Provisioning diagram
Dec 20, 2018, 4:35:45 AM	CREATE_IN_PROGRESS	Cloud AWS E C2 Instance	Cloud_AWS_EC_2_Instance_1	

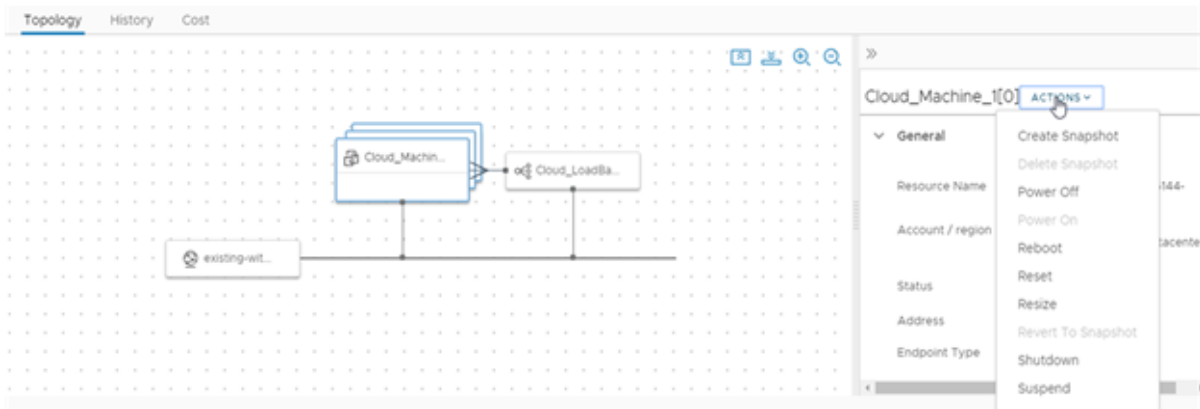
The third screenshot shows the **Cost** tab. It displays a **Cost Analysis** table with the following data:

Component	Cost
Cloud_AWS_Volume_1	\$0.04
Storage	\$0.04
Cloud_AWS_EC2_Instance_1	\$2.78
Total	\$2.82

The total cost is \$2.82, labeled as 'COST MONTH TO DATE'. The right sidebar shows a diagram with the same two components as the Topology tab, with cost labels: \$0.04 for **Cloud_AWS_Vo...** and \$2.78 for **Cloud_AWS_EC...**.

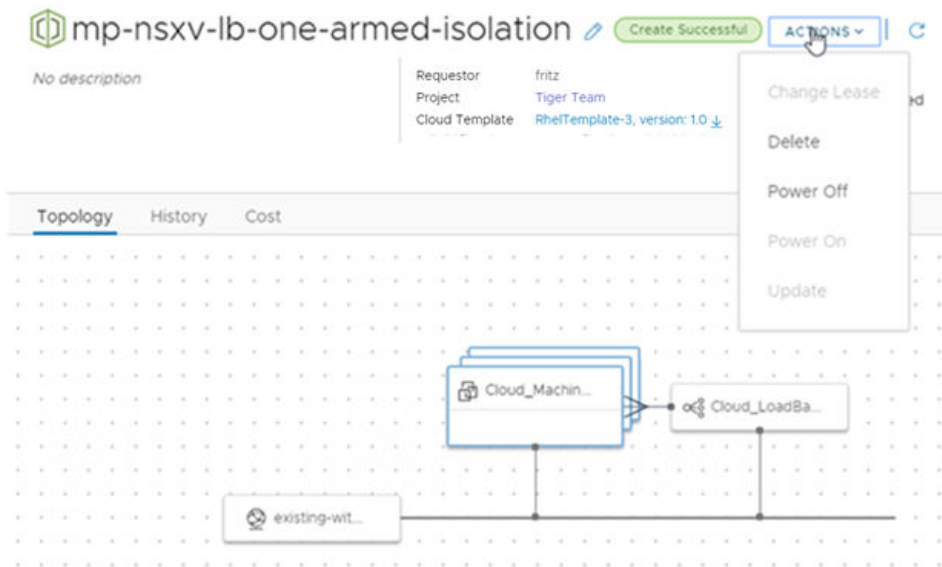
- 3 If you determine that a deployment is too costly in its current configuration and you want to resize a component, select the component on the topology page and then select **Actions > Resize** on the component page.

The available actions depend on the component, the cloud account, and your permissions.



- 4 As part of your development life cycle, one of your deployments is no longer needed. To remove the deployment and reclaim resources, select **Actions > Delete**.

The available actions depend on the state of the deployment.



What to do next

To learn more about possible actions, see [What actions can I run on vRealize Automation Cloud Assembly deployments](#).

What actions can I run on vRealize Automation Cloud Assembly deployments

After you deploy cloud templates, you can run actions in vRealize Automation Cloud Assembly to manage the resources. The available actions depend on the resource type and whether the actions are supported on a particular cloud account or integration platform.

The available actions also depend on what your administrator entitled you to run.

As an administrator or project administrator, you can set up Day 2 Actions policies in vRealize Automation Service Broker. See [How do I entitle consumers to Service Broker day 2 action policies](#)

You might also see actions that are not included in the list. These are likely custom actions added by your administrator. For example, a [How to create a vRealize Automation Cloud Assembly custom action to vMotion a virtual machine](#).

Table 7-1. List of possible actions

Action	Applies to these resource types	For these cloud accounts or integrations	Description
Add Disk	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	Add additional disks to existing virtual machines.
Change Lease	Deployments	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	<p>Change the lease expiration date and time.</p> <p>When a lease expires, the deployment is destroyed and the resources are reclaimed.</p> <p>Lease policies are set in vRealize Automation Service Broker.</p>
Change Security Groups	Machines	<ul style="list-style-type: none"> ■ VMware vSphere 	<p>You can associate and dissociate security groups with machine networks in a deployment. The change action applies to existing and on-demand security groups for NSX-V and NSX-T. This action is available only for single machines, not machine clusters.</p> <p>To associate a security group with the machine network, the security group must be present in the deployment.</p> <p>Dissociating a security group from all networks of all machines in a deployment does not remove the security group from the deployment.</p> <p>These changes do not affect security groups applied as part of the network profiles.</p> <p>This action changes the machine's security group configuration without recreating the machine. This is a non-destructive change.</p> <p>Change security groups on a machine</p> <ul style="list-style-type: none"> ■ To change the machine's security group configuration, select the machine in the topology pane, then click the Action menu in the right pane and select Change Security Groups. You can now add or remove the association on the security groups with the machine networks.
Connect to Remote Console	Machines	<ul style="list-style-type: none"> ■ VMware vSphere 	<p>Open a remote session on the selected machine.</p> <p>Review the following requirements for a successful connection.</p> <ul style="list-style-type: none"> ■ As a deployment consumer, verify that the provisioned machine is powered on.

Table 7-1. List of possible actions (continued)

Action	Applies to these resource types	For these cloud accounts or integrations	Description
Create Snapshot	Machines	<ul style="list-style-type: none"> ■ Google Cloud Platform ■ VMware vSphere 	<p>Create a snapshot of the virtual machine.</p> <p>If you are allowed only two snapshots in vSphere and you already have them, this command is not available until you delete a snapshot.</p>
Delete	Deployments	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<p>Destroy a deployment.</p> <p>All the resources are deleted and the reclaimed.</p> <p>If a delete fails, you can run the delete action on a deployment a second time. During the second attempt, you can select Ignore Delete Failures. If you select this option, the deployment is deleted, but the resources might not be reclaimed. You should check the systems on which the deployment was provisioned to ensure that all resources are removed. If they are not, you must manually delete the residual resources on those systems.</p>
	NSX Gateway	<ul style="list-style-type: none"> ■ NSX 	Delete the NAT port forwarding rules from an NSX-T or NSX-V gateway.
	Machines and load balancers	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere ■ VMware NSX 	Delete a machine or load balancer from a deployment. This action might result in an unusable deployment.
	Security groups	<ul style="list-style-type: none"> ■ NSX-T ■ NSX-V 	<p>If the security is not associated with any machine in the deployment, the process removes the security group from the deployment.</p> <ul style="list-style-type: none"> ■ If the security group is on-demand, then it is destroyed on the endpoint. ■ If the security group is shared, the action fails.
Delete Snapshot	Machines	<ul style="list-style-type: none"> ■ VMware vSphere ■ Google Cloud Platform 	Delete a snapshot of the virtual machine.
Edit Tags	Deployments	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	Add or modify resource tags that are applied to individual deployment resources.

Table 7-1. List of possible actions (continued)

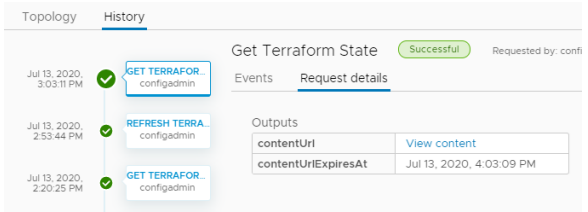
Action	Applies to these resource types	For these cloud accounts or integrations	Description
Get Terraform State	Terraform Configuration	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<p>Display the Terraform state file.</p> <p>To view any changes that were made to the Terraform machines on the cloud platforms that they were deployed on and update the deployment, you first run the Refresh Terraform State action, and then run this Get Terraform State action.</p> <p>When the file is displayed in a dialog box. The file is available for approximately 1 hour before you need to run a new refresh action. You can copy it if you need it for later. You can also view the file on the deployment History tab. Select the Get Terraform State event on the Events tab, and then click Request Details. If the file is not expired, click View content. If the file is expired, run the Refresh and Get actions again.</p> 
Power Off	Deployments	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	Power off the deployment without shutting down the guest operating systems.
	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	Power off the machine without shutting down the guest operating systems.
Power On	Deployments	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	Power on the deployment. If the resources were suspended, normal operation resumes from the point at which they were suspended.
	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	Power on the machine. If the machine was suspended, normal operation resumes from the point at which the machine was suspended.
Reboot	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ VMware vSphere 	Reboot the guest operating system on a virtual machine. For a vSphere machine, VMware Tools must be installed on the machine to use this action.

Table 7-1. List of possible actions (continued)

Action	Applies to these resource types	For these cloud accounts or integrations	Description
Reconfigure	Load Balancers	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware NSX 	Change the load balancer size and logging level. You can also add or remove routes, and change the protocol, port, health configuration, and member pool settings.
	NSX Gateway port forwarding	<ul style="list-style-type: none"> ■ NSX-T ■ NSX-V 	Add, edit, or delete the NAT port forwarding rules from an NSX-T or NSX-V gateway.
Refresh Terraform State	Terraform Configuration	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	Retrieve the latest iteration of the Terraform state file. To retrieve any changes that were made to the Terraform machines on the cloud platforms that they were deployed on and update the deployment, you first run this Refresh Terraform State action. To view the file, run the Get Terraform State action on the configuration. Use the deployment history tab to monitor the refresh process.
Remove Disk	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	Remove disks from existing virtual machines.
Reset	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ VMware vSphere 	Force a virtual machine restart without shutting down the guest operating system.
Resize	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ Google Cloud Platform ■ VMware vSphere 	Increase or decrease the CPU and memory of a virtual machine.
Resize Boot Disk	Machines	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	Increase or decrease the size of your boot disk medium.
Resize Disk	Storage disk	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform 	Increase the capacity of a storage disk.
Restart	Machines	<ul style="list-style-type: none"> ■ Microsoft Azure 	Shut down and restart a running machine.
Revert to Snapshot	Machines	<ul style="list-style-type: none"> ■ Google Cloud Platform ■ VMware vSphere 	Revert to a previous snapshot of the machine. You must have an existing snapshot to use this action.

Table 7-1. List of possible actions (continued)

Action	Applies to these resource types	For these cloud accounts or integrations	Description
Run Puppet Task	Managed resources	<ul style="list-style-type: none"> ■ Puppet Enterprise 	Run the selected task on machines in your deployment. The tasks are defined in your Puppet instance. You must be able to identify the task and provide the input parameters.
Shutdown	Machines	<ul style="list-style-type: none"> ■ VMware vSphere 	Shut down the guest operating system and power off the machine. VMware Tools must be installed on the machine to use this action.
Suspend	Machines	<ul style="list-style-type: none"> ■ Microsoft Azure ■ VMware vSphere 	Pause the machine so that it cannot be used and does not consume any system resources other than the storage it is using.
Update	Deployments	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	Change the deployment based on the input parameters. For an example, see How to move a deployed machine to another network .
Update Tags	Machines and disks	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	Add, modify, or delete a tag that is applied to an individual resource.