

# 使用和管理 vRealize Automation Cloud Assembly

2022 年 10 月

vRealize Automation 8.2

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

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

**威睿信息技术（中国）有  
限公司**  
北京办公室  
北京市  
朝阳区新源南路 8 号  
启皓北京东塔 8 层 801  
[www.vmware.com/cn](http://www.vmware.com/cn)

上海办公室  
上海市  
淮海中路 333 号  
瑞安大厦 804-809 室  
[www.vmware.com/cn](http://www.vmware.com/cn)

广州办公室  
广州市  
天河路 385 号  
太古汇一座 3502 室  
[www.vmware.com/cn](http://www.vmware.com/cn)

版权所有 © 2022 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

# 目录

<b>1</b>	<b>vRealize Automation Cloud Assembly 是什么</b>	<b>7</b>
	vRealize Automation Cloud Assembly 如何工作	8
<b>2</b>	<b>教程</b>	<b>10</b>
	设置和测试 vSphere 基础架构和部署	12
	配置和置备生产工作负载	27
	多云基础架构和部署	34
	第 1 部分：配置示例基础架构	34
	第 2 部分：创建示例项目	40
	第 3 部分：设计并部署示例云模板	41
	配置 VMware Cloud on AWS	56
	配置基本 VMware Cloud on AWS 工作流	57
	在 VMware Cloud on AWS 中配置隔离网络	68
	为 Infoblox 配置外部 IPAM 集成	72
	在部署下载软件包之前，先在 Infoblox 应用程序中添加所需的可扩展属性	73
	下载并部署外部 IPAM 提供程序软件包	74
	为 IPAM 集成点创建运行环境	75
	为 Infoblox 添加外部 IPAM 集成	76
	配置网络和网络配置文件，以对现有网络使用外部 IPAM	79
	定义并部署使用外部 IPAM 提供程序范围分配的云模板	81
	对 IPAM 集成使用特定于 Infoblox 的属性	83
<b>3</b>	<b>为您的组织设置 vRealize Automation Cloud Assembly</b>	<b>86</b>
	vRealize Automation 用户角色是什么	86
	组织和服务用户角色	88
	自定义用户角色	98
	用例：用户角色如何帮助我控制访问权限	101
	添加云帐户	118
	使用云帐户所需的凭据	119
	创建 Microsoft Azure 云帐户	136
	创建 Amazon Web Services 云帐户	137
	创建 Google Cloud Platform 云帐户	138
	创建 vCenter 云帐户	139
	创建 NSX-V 云帐户	140
	创建 NSX-T 云帐户	141
	创建 VMware Cloud on AWS 云帐户	144
	创建 VMware Cloud Foundation 云帐户	145

与其他应用程序集成	146
如何使用 GitLab 和 GitHub 集成	146
如何配置外部 IPAM 集成	151
如何升级到较新的外部 IPAM 集成软件包	153
在 vRealize Automation Cloud Assembly 中配置 My VMware 集成	153
在 Cloud Assembly 中配置 vRealize Orchestrator 集成	154
如何在 vRealize Automation Cloud Assembly 中使用 Kubernetes	156
什么是 vRealize Automation Cloud Assembly 中的配置管理	170
如何在 vRealize Automation Cloud Assembly 中创建 Active Directory 集成	179
配置 VMware SDDC Manager 集成	180
与 vRealize Operations Manager 集成	181
载入计划是什么	188
将选定的计算机载入为单个部署	189
将规则筛选的计算机作为单独部署载入	190
高级配置	195
如何配置 Internet 代理服务器	195
NSX-T 映射到多个 vCenter 有哪些用途	198
如果移除 NSX 云帐户关联，会发生什么情况	199
如何使用 IPAM SDK 创建提供程序特定的外部 IPAM 集成软件包	200

## 4 构建资源基础架构 201

如何添加云区域	201
了解有关云区域的更多信息	201
如何添加特定实例映射	204
了解有关特定实例映射的更多信息	204
如何添加映像映射	204
了解有关映像映射的更多信息	204
如何添加网络配置文件	207
了解有关网络配置文件的更多信息	207
使用网络设置	213
使用安全组设置	215
使用负载均衡器设置	216
如何配置网络配置文件以对外部 IPAM 集成支持按需网络	217
如何配置网络配置文件以对外部 IPAM 集成支持现有网络	220
如何添加存储配置文件	220
了解有关存储配置文件的更多信息	220
如何使用标记	221
创建标记策略	223
在 vRealize Automation Cloud Assembly 中使用功能标记	224
在 vRealize Automation Cloud Assembly 中使用限制标记	225
标准标记	226



vRealize Automation Cloud Assembly 如何处理标记	227
如何设置简单的标记结构	227
如何使用资源	229
计算资源	229
网络资源	229
安全资源	230
存储资源	231
计算机资源	232
卷资源	232
了解有关资源的更多信息	232
使用 vRealize Automation 配置多提供者租户资源	242
如何为 vRealize Automation 创建虚拟专用区域	243
管理 vRealize Automation 租户的 VPZ 配置	245
<b>5 添加和管理项目</b>	<b>247</b>
如何为我的开发团队添加项目	247
了解有关项目的更多信息	249
使用项目标记和自定义属性	249
项目在部署时的工作方式	250
<b>6 设计部署</b>	<b>252</b>
创建云模板的方法	253
如何从头开始创建简单的云模板	254
如何选择资源并将其添加到云模板	255
如何连接云模板资源	255
如何创建有效的云模板代码	257
如何保存不同版本	258
如何增强简单云模板	260
用户输入如何自定义云模板	261
资源标志如何自定义请求	266
如何设置资源部署顺序	267
如何使用表达式使云模板代码更具通用性	268
如何在云模板中启用远程访问	277
如何将高级功能添加到设计中	280
如何自定义已部署资源的名称	280
如何云模板中自动初始化计算机	282
如何创建要在云模板中使用的自定义资源类型	295
如何为实施后更改做准备	303
如何使用可扩展性扩展应用程序生命周期并实现自动化	308
有哪些资源属性	343
有哪些代码示例	343

云模板中的 vSphere 资源示例	344
可查看的云模板	347
云模板中的网络、安全性和负载均衡器示例	354
Puppet 支持的具有用户名和密码访问权限的云模板	372
如何包括 Terraform 配置	381
准备 Terraform 运行时环境	381
准备 Terraform 配置	387
为 Terraform 配置进行设计	388
了解有关 Terraform 配置的更多信息	391
如何使用商城	393

## 7 管理部署 395

如何监控部署	396
vRealize Automation Cloud Assembly 部署失败时可以执行哪些操作	397
如何管理已完成部署的生命周期	399
可以对部署运行哪些操作	401

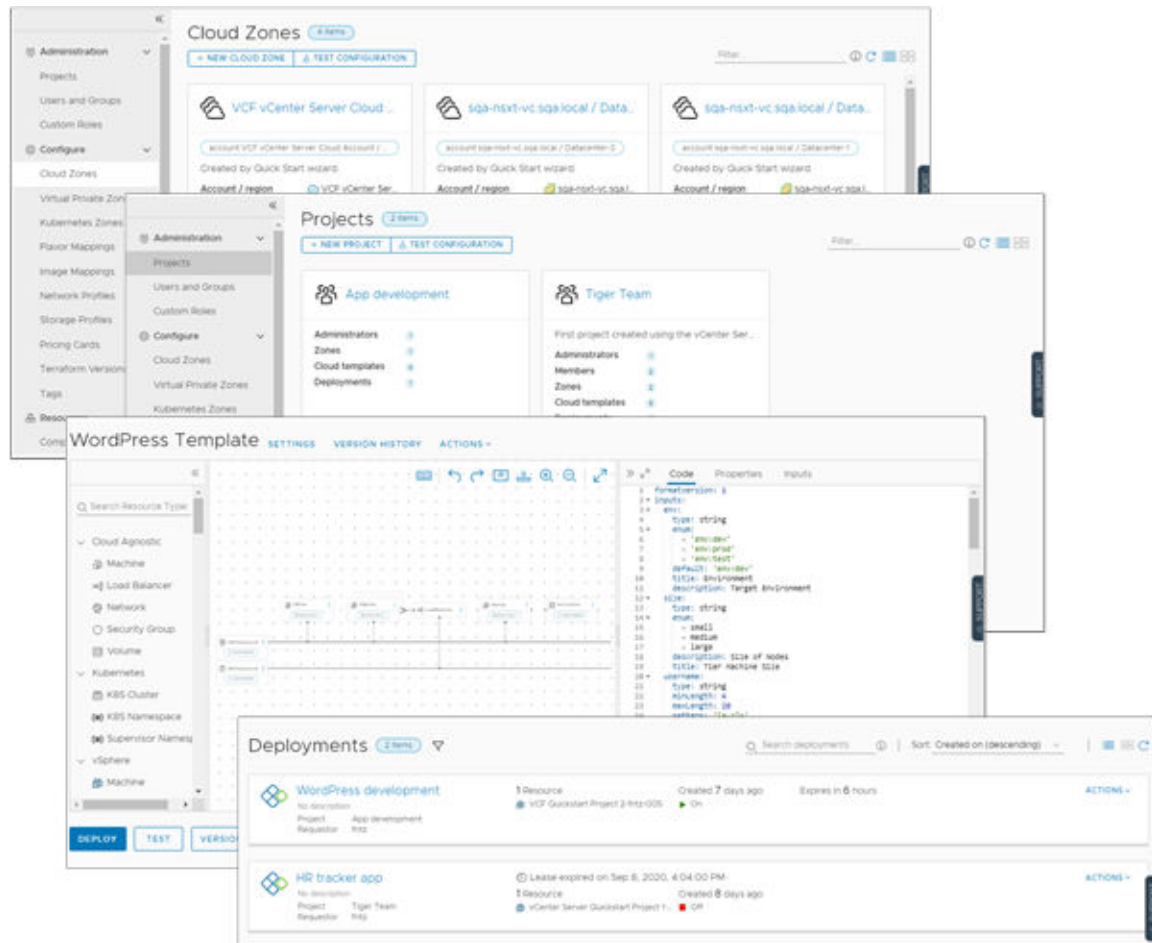
# vRealize Automation Cloud Assembly 是什么

# 1

可以使用 vRealize Automation Cloud Assembly 连接到公有云提供商和私有云提供商，以将创建的计算机、应用程序和服务部署到这些资源。您和您的团队可以在支持迭代式工作流（从开发到测试再到生产）的环境中开发云模板即代码。在置备时，可以部署到一系列云供应商。此服务是一个受管 VMware SaaS 和基于 NaaS 的框架。

vRealize Automation Cloud Assembly 概览包括以下基本功能。

- 在“基础架构”选项卡，可以添加和组织云供应商资源和用户。此选项卡还提供有关已部署的云模板的信息。
- “商城”选项卡提供有助于生成模板库和访问支持 OVA 或 OVF 的 VMware Solution Exchange 云模板和映像。
- “设计”选项卡是主要开发工作区。您可以使用画布和 YAML 编辑器来开发然后部署计算机和应用程序。
- “部署”选项卡显示了已置备资源的当前状态。您可以访问用于管理部署的详细信息和历史记录。



本章讨论了以下主题：

- [vRealize Automation Cloud Assembly 如何工作](#)

## vRealize Automation Cloud Assembly 如何工作

vRealize Automation Cloud Assembly 是一项云模板部署和开发服务。您和您的团队可以使用此服务将计算机、应用程序和服务部署到云供应商资源中。

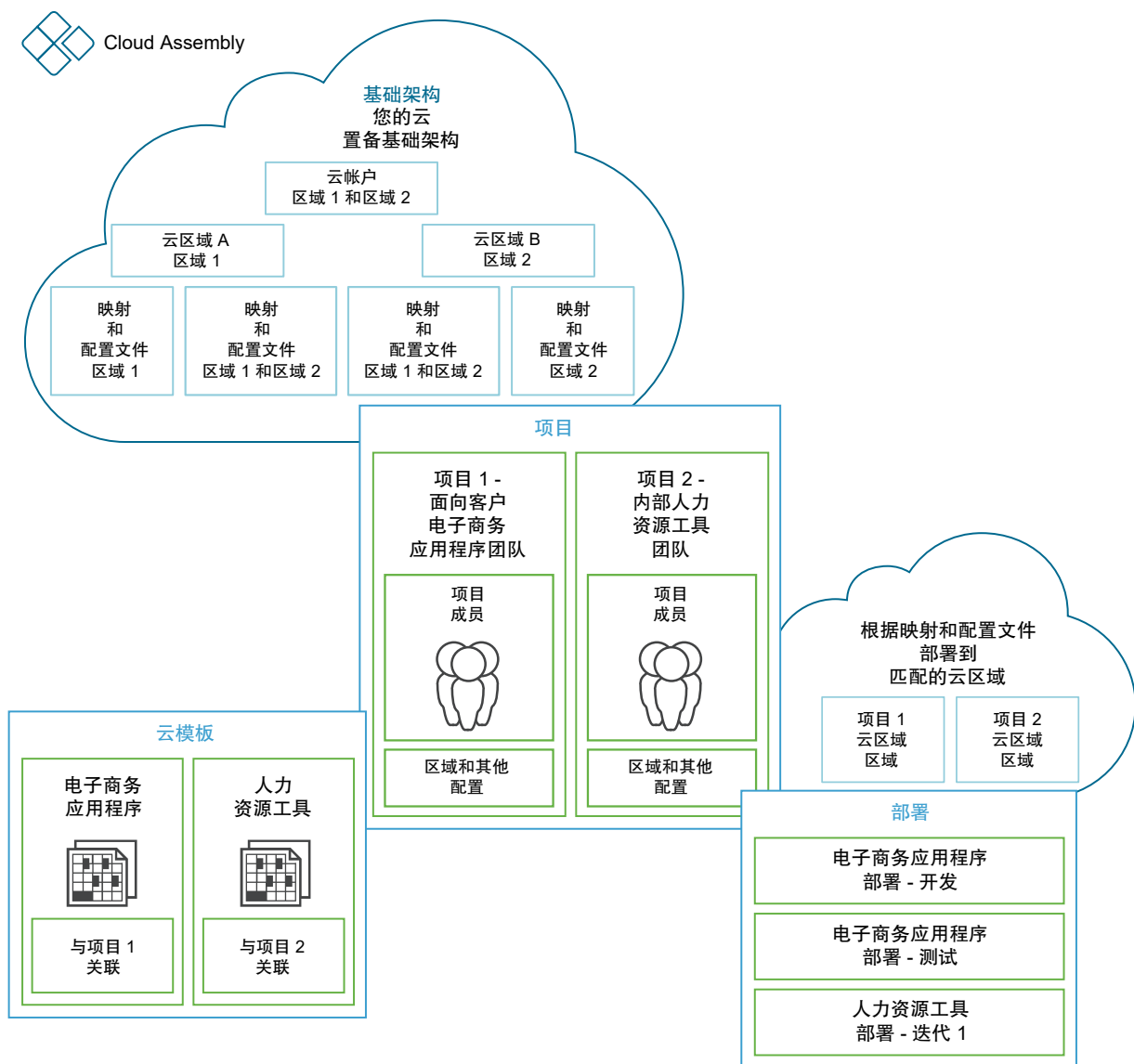
作为 Cloud Assembly 管理员（通常称为云管理员），您可以设置准备基础架构并创建用于对用户和资源进行分组的项目。

- 添加云供应商帐户。请参见[将云帐户添加到 vRealize Automation Cloud Assembly](#)。
- 确定哪些区域或数据存储是您希望开发人员部署到的云区域。请参见[了解有关 vRealize Automation Cloud Assembly 云区域的更多信息](#)。
- 创建策略以定义云区域。请参见第 4 章 [构建您的 vRealize Automation Cloud Assembly 资源基础架构](#)。
- 创建项目以将开发人员与云区域分组到一起。请参见[使用 vRealize Automation Cloud Assembly 项目标记和自定义属性](#)。

作为云模板开发人员，您是一个或多个项目的成员。您可以创建模板并将其部署到与其中一个项目关联的云区域。

- 使用画布为项目开发云模板。项目管理员可以使用商城从 VMware Solution Exchange 下载模板和支持映像。请参见第 6 章 [设计 vRealize Automation Cloud Assembly 部署和如何使用 vRealize Automation Cloud Assembly 商城](#)。
- 根据策略和限制将云模板部署到项目云区域。
- 管理部署，包括删除未使用的应用程序。请参见第 7 章 [管理 vRealize Automation Cloud Assembly 部署](#)。

欢迎使用 vRealize Automation Cloud Assembly。有关如何定义基础架构然后创建并部署云模板的示例，请参见 [教程：在 vRealize Automation Cloud Assembly 中设置和测试多云基础架构和部署](#)。



# Cloud Assembly 教程

# 2

教程介绍如何执行常见任务，以帮助您精通 vRealize Automation Cloud Assembly。

开始时，需注意，除了教程中的步骤外，本指南中还有其他信息。提供了相关主题的连接。

## 访问用户帮助

在整个应用程序中提供用户帮助同样十分重要。用户帮助有助于了解功能，并提供帮助您决定如何填充文本框的信息。外部文档提供更深入信息、代码示例和用例。

帮助类型	如何访问帮助	示例
字段级别的标志帮助	单击字段旁边的信息图标 (i)。	
上下文支持面板帮助	单击您的姓名和组织旁边的“帮助”图标 (?)。	
访问外部文档	单击标记为文档的文章标题，或单击在 VMware Docs 中查看更多。	

本章讨论了以下主题：

- 教程：在 vRealize Automation Cloud Assembly 中设置和测试 vSphere 基础架构和部署
- 教程：配置 vRealize Automation Cloud Assembly 以置备生产工作负载
- 教程：在 vRealize Automation Cloud Assembly 中设置和测试多云基础架构和部署
- 教程：为 vRealize Automation 配置 VMware Cloud on AWS
- 教程：为 vRealize Automation 配置提供程序特定的外部 IPAM 集成

## 教程：在 vRealize Automation Cloud Assembly 中设置和测试 vSphere 基础架构和部署

如果您不熟悉 vRealize Automation 或仅需要进修课程，本教程将指导您完成 vRealize Automation Cloud Assembly 配置过程。添加云 vSphere 帐户端点、定义基础架构、将用户添加到项目，然后基于 vSphere 资源类型使用 VMware Cloud Templates 设计和部署工作负载，学习整个过程。

虽然本教程仅仅是个开端，但您已踏上实现自助服务自动化和迭代开发（适用于多个公有云和私有云）之路。本教程重点介绍 VMware vCenter Server 和 NSX-T。完成此工作流后，可以应用所学知识添加更多类型的云帐户以及交付更完美的云模板。

按照步骤操作时，我们会提供数据示例。请将示例替换为适用于您环境的值。

您将在 vRealize Automation Cloud Assembly 中执行本教程中的所有步骤。

本教程将指导您配置每个所需的组件。

- **步骤 1：添加 vCenter Server 云帐户和 NSX 云帐户。**云帐户是指将 vRealize Automation Cloud Assembly 连接到云供应商端点的凭据。
- **步骤 2：定义云区域计算资源。**云区域是指帐户/区域中的所选计算资源，可以根据项目需求以及合规性和成本管理目标将其分配给不同的项目。
- **步骤 3：配置可用于帐户/区域的可能资源。**基础架构资源是指与云模板中所用帐户/区域相关联的计算资源、存储、网络和其他资源的定义。
- **步骤 4：创建项目。**项目是指您如何根据项目的应用程序开发目标为用户提供对云区域的访问权限。
- **步骤 5：设计并部署基本云模板。**云模板是指以迭代方式开发和部署的应用程序工作负载的定义。

此配置过程是体验 Cloud Assembly 开发过程的基础。在构建基础架构并掌握云模板开发技能时，将重复使用并深入了解此工作流。

### 开始之前

- 确认您具有 Cloud Assembly 管理员角色。请参见 [vRealize Automation 中的组织和服务用户角色](#)。
- 如果尚未在 vRealize Automation 控制台使用 VMware vCenter Server 或 VMware Cloud Foundation 快速入门向导，现在可以使用。

这些向导驱动式工作流包括本教程中的大部分配置，但不包括全部配置。

本教程提供动手体验，可帮助您深入了解如何组合工作基础架构并部署工作负载。

请参见“入门”指南中的[如何设置 Cloud Assembly](#)。

- 如果尚未使用 vRealize Automation Cloud Assembly 中提供的引导式设置，现在可以使用。引导式设置可引导您完成在本教程中执行的大部分过程，但不是全部过程。要打开引导式设置，请单击选项卡栏右侧的[引导式设置](#)。
- 确保您具有 vCenter Server 和 NSX 凭据。有关凭据必须具有的权限的详细信息，请参见在 [vRealize Automation 中使用云帐户所需的凭据](#)。如果您计划将其他用户添加到项目，请确认他们是 vRealize Automation Cloud Assembly 服务的成员。



## 步骤 1: 添加 vCenter Server 云帐户和 NSX 云帐户

这些云帐户提供 vRealize Automation 用于连接到 vCenter Server 和关联 NSX 服务器的凭据。

### 1 添加 vCenter Server 云帐户。

vCenter Server 云帐户提供 vCenter 凭据，vRealize Automation Cloud Assembly 可用于发现资源和部署云模板。

有关 vCenter Server 云帐户的其他信息，请参见在 [vRealize Automation](#) 中创建 vCenter 云帐户。

- a 选择 **基础架构 > 连接 > 云帐户**。
- b 单击 **添加云帐户**，然后选择 **vCenter**。
- c 输入值。

**New Cloud Account**

Name \* vCenter Server Account

Description

vCenter Server Credentials

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

Username \* mgmt@cmbu.local

Password \* .....

VALIDATE ✔ Credentials validated successfully. ✕

Configuration

Allow provisioning to these datacenters \* ☒ wld01-DC

☒ Create a cloud zone for the selected datacenters

NSX cloud account

Capabilities

Capability tags  ⓘ

**ADD** **CANCEL**

请记住，这些值仅为示例而已。您的值将特定于您的环境。

设置	示例值
名称	vCenter Server 帐户
vCenter IP 地址/FQDN	your-dev-vcenter.company.com
用户名和密码	vCenterCredentials@yourCompany.com

- d 要验证凭据，请单击 **验证**。

- e 要允许置备到选定数据中心，请选择一个或多个数据中心。
- f 跳过 NSX 云帐户。稍后将配置此帐户，将 vCenter Server 帐户链接到 NSX 云帐户。
- g 单击添加。

## 2 添加关联的 NSX 云帐户。

NSX-T 云帐户提供 NSX-T 凭据，vRealize Automation Cloud Assembly 可用于发现网络资源并使用云模板部署网络。

有关 NSX-T 云帐户的详细信息，请参见在 [vRealize Automation](#) 中创建 vCenter 云帐户。

- a 选择**基础架构 > 连接 > 云帐户**。
- b 单击**添加云帐户**，然后选择 NSX-T 或 NSX-V。本教程使用 **NSX-T**。
- c 输入值。

**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. X

Associations

vCenter cloud accounts + ADD X 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

这些值仅为示例而已。您的值将特定于您的环境。

设置	示例值
名称	NSX-T 帐户
vCenter IP 地址/FQDN	your-dev-NSX-vcenter.company.com

设置	示例值
用户名和密码	NSXCredentials@yourCompany.com
NSX 模式	不知道该选择哪个？ 这是使用产品内置帮助的好机会。单击字段右侧的信息图标。请注意，字段级别帮助包括可帮助您配置选项的信息。 在此示例中，选择 <b>策略</b> 。

- d 要验证凭据，请单击**验证**。
- e 要关联在上一步中创建的 vCenter 云帐户，请单击**添加**，然后选择 **vCenter 帐户**。  
此 vCenter 云帐户关联可确保网络安全。
- f 在 NSX 云帐户页面上，单击**添加**。

## 步骤 2：定义云区域计算资源


云区域是帐户/区域中的计算资源组，可将其供项目使用。项目成员通过使用分配的云区域中的资源部署云模板。如果希望对部署项目云模板的位置进行更精细的控制，可以创建多个具有不同计算资源的云区域。

帐户/区域是云供应商将资源与隔离区域或数据存储相关联的方式。帐户指示云帐户类型，区域指示区域或数据存储。vCenter Server 使用数据存储，置备资源是选定的集群和资源池。

在本教程中，您必须确保云区域包括支持项目开发团队目标的资源以及您的预算和管理要求。

有关云区域的详细信息，请参见[了解有关 vRealize Automation Cloud Assembly 云区域的更多信息](#)。

- 1 选择**基础架构 > 配置 > 云区域**。
- 2 单击为 vCenter Server 实例添加的云区域，然后输入值。


**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

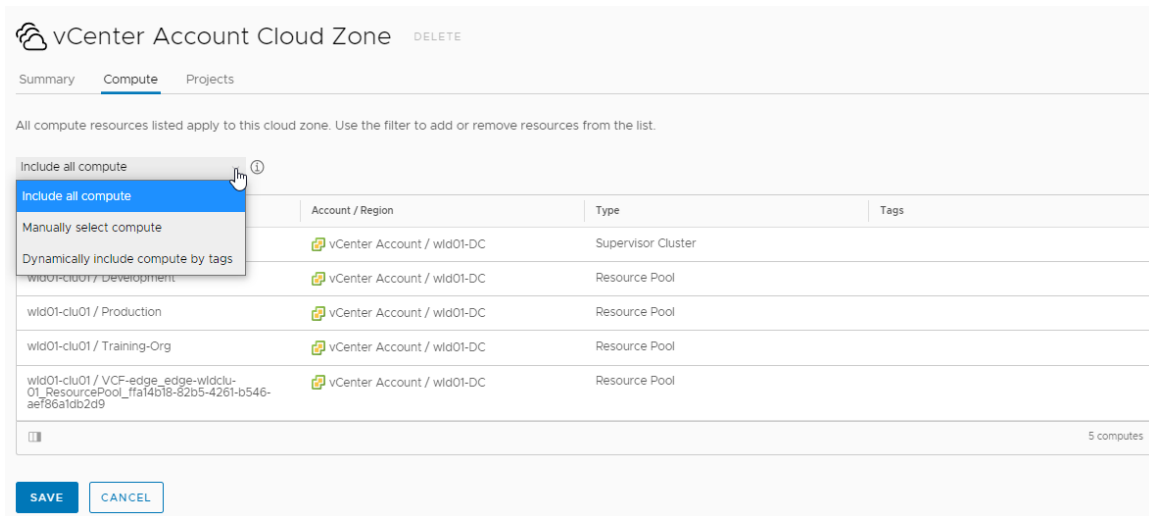
CANCEL

设置	示例值
帐户/区域	vCenter 帐户/数据中心名称
名称	vCenter Server 云区域 此值在创建后将无法更改。如果要为不同的 vCenter Server 配置不同的数据中心，则必须创建一个新的云区域，您可以在其中选择帐户/区域。
说明	All vCenter Server compute resources for development.
策略	默认 如果对字段值有疑问，您可以查阅帮助。

请记住，所有值都仅为示例而已。您的区域详细信息将特定于您的环境。

- 单击**计算资源**选项卡，然后验证计算资源是否全部存在。

如果需要排除一个，请切换到**手动选择计算资源**，然后仅添加要包含在云区域中的计算资源。



4 单击**保存**。

5 对任何其他云区域重复此过程，但必须确保区域名称唯一。

### 步骤 3：配置可用于帐户/区域的可能资源

您已将帐户/区域添加到云区域。现在，可以为云帐户定义可能的计算机大小（特定实例映射）、映像映射、网络配置文件和存储配置文件。部署云模板时，将评估映射和配置文件定义的匹配性，从而确保工作负载包括适当的计算机大小（特定实例）、映像、网络和存储。

1 为帐户/区域配置特定实例映射。

特定实例有时也称为“**T 恤调整大小**”。根据云模板的配置方式，应用的特定实例映射将确定 CPU 数和内存。

有关特定实例映射的详细信息，请参见[了解有关 vRealize Automation 中的特定实例映射的更多信息](#)。

a 选择**基础架构 > 配置 > 特定实例映射**。

b 单击**新建特定实例映射**，然后输入定义小型、中型和大型计算机的值。

请记住，这些是示例值。必须选择相关的帐户/区域并定义大小。

small DELETE

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

Flavor name \* small

Configuration \*

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

GB ▾ - +

设置	示例值
特定实例名称	small
帐户/区域	vCenter 帐户/数据中心
CPU 值	2
内存值	1 GB

- c 单击**创建**。
- d 要创建其他大小，请为帐户/区域配置中型和大型特定实例映射。

设置	示例值
特定实例名称	中型
帐户/区域	vCenter 帐户/数据中心
CPU 值	4
内存值	2 GB
特定实例名称	大型
帐户/区域	vCenter 帐户/数据中心
CPU 值	8
内存值	4 GB

## 2 为帐户/区域配置映像映射。

映像是在云模板中计算机的操作系统。使用 vCenter Server 映像时，需要选择 vCenter 模板。有关映像映射的详细信息，请参见[了解有关 vRealize Automation 中的映像映射的更多信息](#)。

- a 选择**基础架构 > 配置 > 映像映射**。
- b 单击**新建映像映射**，然后搜索帐户/区域的映像。

请记住，这些是示例值。您必须选择在您的帐户/区域中发现的相关映像。

设置	示例值
映像名称	centos
帐户/区域	vCenter 帐户
映像	centos7

c 单击**创建**。

d 重复此过程以创建其他映像映射。例如，帐户/区域的 ubuntu 映射。

### 3 配置网络配置文件。

网络配置文件定义可用于帐户/区域的网络和网络设置。配置文件必须支持目标部署环境。

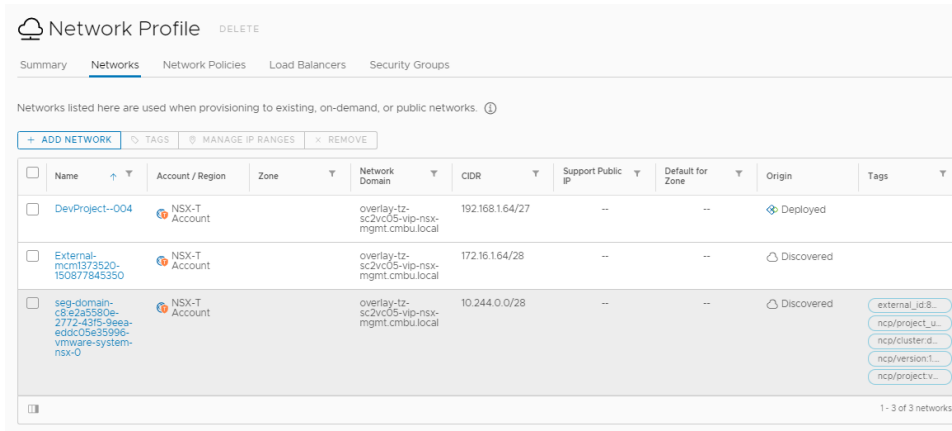
此任务提供最少量配置信息，以确保成功。如果需要有关网络配置文件的详细信息，请从[了解有关 vRealize Automation 中的网络配置文件的更多信息](#)开始。

a 选择**基础架构 > 配置 > 网络配置文件**。

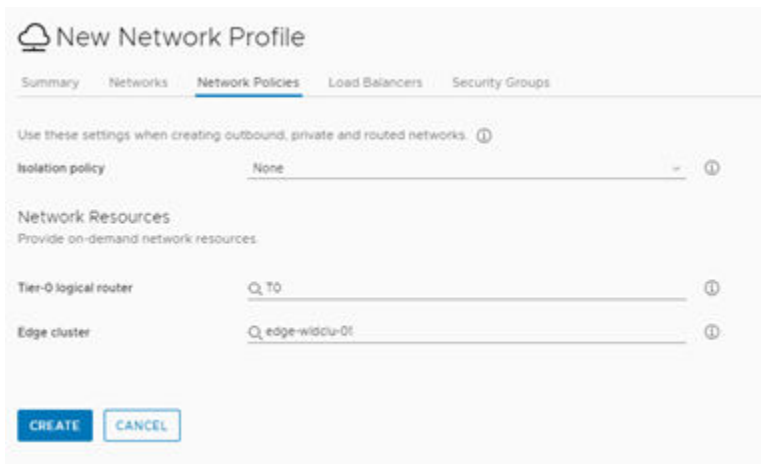
b 单击**新建网络配置文件**，然后创建用于 vCenter 帐户/数据中心帐户/区域的配置文件。

设置	示例值
帐户/区域	vCenter 帐户/数据中心
名称	Network Profile
说明	Networks for development teams.

- c 单击**网络**选项卡，然后单击**添加网络**。



- d 选择要供应用程序开发团队使用的 NSX 网络。
- 在此示例中，我们有一个名为 DevProject-004 的 NSX-T 网络。
- e 单击**网络策略**选项卡，然后创建策略。



设置	示例值
隔离策略	无
第 0 层逻辑路由器	Tier-0-router
边缘集群	EdgeCluster

- f 单击**创建**。

#### 4 配置存储配置文件。

存储配置文件定义帐户/区域的磁盘。配置文件必须支持目标部署环境。

如果需要有关存储配置文件的详细信息，请参见了解有关 vRealize Automation 中的存储配置文件的更多信息。

- a 选择**基础架构 > 配置 > 存储配置文件**。



- b 单击**新建存储配置文件**，然后创建用于 vCenter Server/数据中心帐户/区域的配置文件。  
除非在表中指定，否则保留默认值。

**Storage Profile**

Account / region: vCenter Account / wld01-DC

Name: Storage Profile

Description: [Empty text box]

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

Storage policy: Datastore default ⓘ

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

Provisioning type: Unspecified ⓘ

Shares: Unspecified ⓘ

Limit IOPS: ⓘ

Disk mode: Dependent ⓘ

☐ Supports encryption ⓘ

☒ Preferred storage for this region ⓘ

Capability tags: Enter capability tags ⓘ

**SAVE** **CANCEL**

设置	示例值
帐户/区域	vCenter 帐户/数据中心
名称	Storage Profile
数据存储/集群	已选择具有足够容量且可供所有主机访问的数据存储。
此区域的首选存储	选中该复选框。

- c 单击**创建**。

## 步骤 4：创建项目

可以在此阶段真正开始考虑项目目标。

- 哪些用户需要访问计算资源，以便他们可以创建和部署应用程序云模板？有关不同项目角色可以查看和执行哪些操作的详细信息，请参见 [vRealize Automation 中的组织和服务用户角色](#)。
- 项目成员是否将创建从开发到生产的应用程序？哪些是必要的资源？
- 他们需要哪些云区域？应对项目的每个区域设置何种优先级和限制？

在本教程中，我们将在开发团队创建和扩展内部软件应用程序时为其提供支持。

此任务提供最少量配置信息，以确保成功。如果需要有关项目的详细信息，请从[了解有关 vRealize Automation Cloud Assembly 项目的更多信息](#)开始。

- 1 选择**基础架构 > 管理 > 项目**。
- 2 单击**新建项目**，然后输入名称 **Development Project**。
- 3 单击**用户**选项卡，然后单击**添加用户**。

此时不需要添加用户。但是，如果您希望其他用户使用云模板，这些用户必须是项目的成员。

- 4 输入电子邮件地址以将用户添加为项目成员或管理员，具体取决于您希望每个人拥有的权限。

Add Users

Users alex

Assign role Alex Orlander - alex

CANCEL ADD

- 5 单击**置备**，然后单击**添加区域 > 云区域**。
- 6 添加用户可部署到的云区域。

此外，还可以为项目中的云区域设置资源限制。以后，可以为其他项目设置不同的限制。

Add Cloud Zone

Add a cloud zone that can be used by this project.

Cloud zone vCenter Server Account / wid01-DC

Provisioning priority 1

Instances limit 5

Memory limit (MB) 0

CPU limit 0

Storage limit (GB) 0

CANCEL ADD

项目云区域设置	示例值
云区域	vCenter 帐户云区域
置备优先级	1
实例限制	5

- 7 将任何其他云区域添加到项目。
- 8 单击**创建**。
- 9 要验证是否已将项目添加到云区域，请选择**基础架构 > 配置 > 云区域**，然后打开 vCenter Account Zone 云区域卡视图，以便可以查看**项目**选项卡。您应该会看到 Development Project。

## 步骤 5：设计并部署基本云模板

您可以设计并部署云模板，确保正确配置基础架构以支持模板。以后，可以在创建满足项目需求的应用程序时基于模板构建。

构建云模板的最佳方式是逐个组件构建，验证是否在两次更改之间进行部署。本教程从简单的计算机开始，然后以迭代方式添加更多资源。

此过程中的示例使用 **YAML** 代码编辑器。此方法可更简便地提供代码片段。但是，如果您更喜欢使用对话框驱动式用户界面，请单击**输入**。

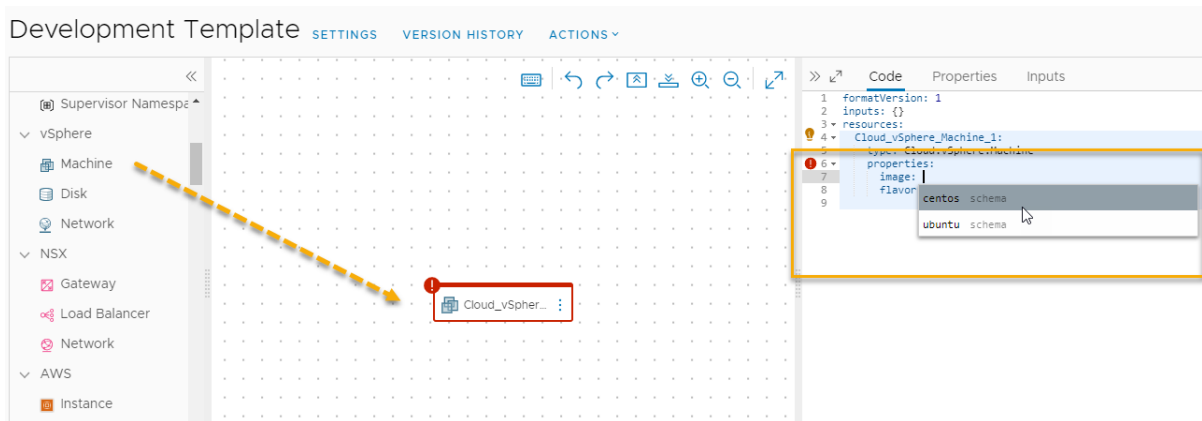
与本教程所提供内容相比，使用云模板可以执行更多操作。如果需要详细信息，请从第 6 章 [设计 vRealize Automation Cloud Assembly 部署](#) 开始。

本教程使用 **vSphere** 和 **NSX** 资源类型。这些资源类型只能在 **vCenter Server** 云帐户端点上部署。您还可以使用云平台无关的资源类型创建可在任何端点上部署的云模板。有关如何为任何端点配置基础架构和设计模板的示例，请参见教程：在 [vRealize Automation Cloud Assembly](#) 中设置和测试多云基础架构和部署。



有关演示此过程中基本步骤的视频，请观看[如何设计和部署基本云模板](#)。

- 1 选择**设计 > 云模板**。
- 2 选择**新建自 > 空白画布**。
- 3 输入名称 **Development Template**，选择项目 **Development Project**，然后单击**创建**。
- 4 将 **vSphere** 计算机添加到设计画布，进行测试并部署。



- a 从资源类型窗格中，将 **vSphere 计算机** 拖动到画布中。

请注意，**代码**窗格将显示计算机的 **YAML**，其中映像以及预定义的 **CPU** 和内存属性的值为空。您将使此模板能够支持灵活的大小调整。

- b 要选择映像值，请将指针放在 **image** 的单引号之间，然后从配置的映像列表中选择 **centos**。

请记住，这些是示例值。如果未配置 **centos** 映像，请选择已配置的映像。

- c 在映像属性下方创建一行，输入或选择 **flavor**，然后从列表中选择 **small**。

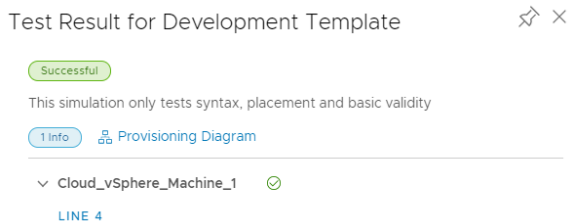
- d 删除 **cpuCount** 和 **totalMemory**。

您的 YAML 应类似于以下示例。

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

- e 单击**测试**。

通过测试，可以验证云模板的语法和布置。测试成功并不意味着部署模板时不出错。



如果测试失败，请单击**置备图**，然后查找故障点。有关使用图表进行故障排除的详细信息，请参见[测试基本云模板](#)。

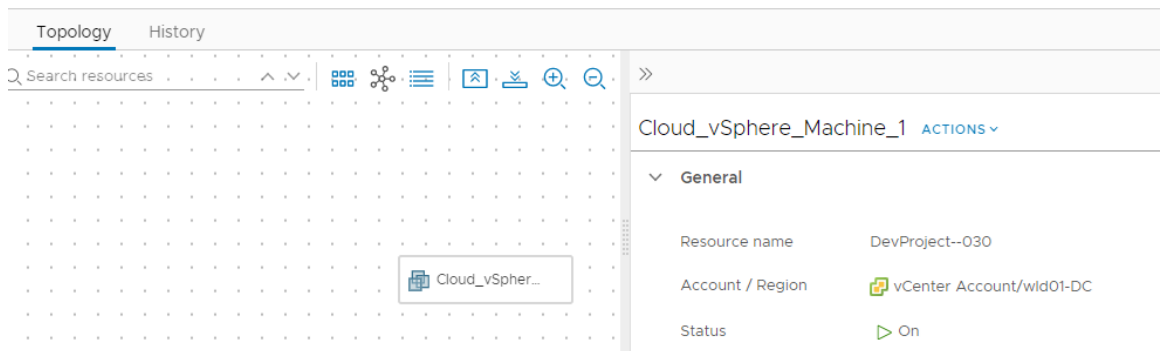
- f 单击**部署**。

- g 输入**部署名称 DevTemplate - machine**，然后单击**部署**。

可以在 DevTemplate 部署详细信息页面或“部署”选项卡上跟踪部署进度。

如果部署失败，可以对问题进行故障排除并修改模板。请参见[vRealize Automation Cloud Assembly 部署失败时可以执行哪些操作](#)。

成功的部署在“部署”选项卡上类似于以下示例。



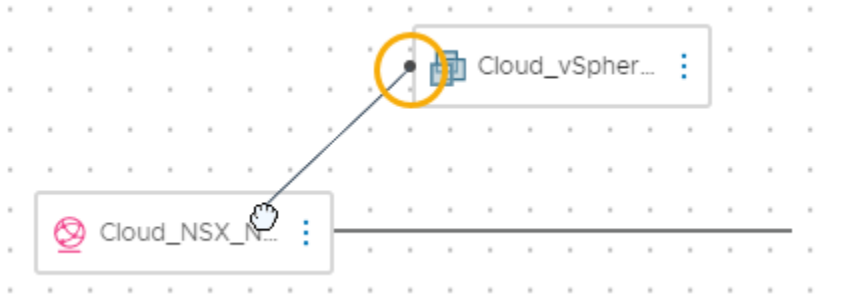
- 5 对模板进行版本控制并添加网络。

要使云模板可在 **Service Broker** 目录中使用，需要对其进行版本控制，但在开发期间拥有一个可以恢复到的优质版本，非常有帮助。

- a 在设计画布中打开模板。

- b 单击**版本**，输入类似于 **Simple deployable machine** 的**描述**，然后单击**创建**。
- c 从“资源类型”窗格中，将 **NSX 网络**资源类型拖动到画布中。
- d 将计算机连接到网络。

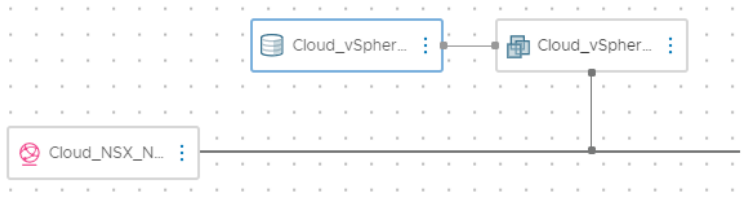
单击计算机组件上的小圆圈，然后将连接拖动到网络。



请注意，YAML 现在类似于以下示例。

```
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 单击**测试**以验证模板。
  - f 单击**部署**。
  - g 输入名称 **DevTemplate - machine - network**，然后单击**部署**。
  - h 跟踪进度并检查成功的部署。
- 6 对模板进行版本控制并添加数据磁盘。
- a 在设计画布中打开模板。
  - b 对模板进行版本控制。
- 输入 **Machine with existing network** 作为描述。
- c 从“资源类型”窗格中，将 **vSphere 磁盘**资源类型拖动到画布中。
  - d 将磁盘连接到计算机。



请注意，YAML 现在类似于以下示例。

```
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 测试模板。
- f 使用名称 **DevTemplate - machine - network - storage** 部署模板。
- g 跟踪进度并检查成功的部署。
- h 对模板进行版本控制。

输入 **Machine with existing network and storage disk** 作为描述。

此最终版本确保可以将工作模板添加到服务目录中。

## 教程结果

您已完成将 Cloud Assembly 配置为工作系统的工作流。您现在熟悉以下概念。

- 云帐户是指将 vRealize Automation Cloud Assembly 连接到云供应商端点的凭据。
- 云区域是指帐户/区域中的所选计算资源，可以根据项目需求和成本管理目标将其分配给不同的项目。
- 基础架构资源是指与云模板中所用帐户/区域相关联的资源的定义。
- 项目是指您如何根据项目的应用程序开发目标为用户提供对云区域的访问权限。
- 云模板是指以迭代方式开发和部署的应用程序工作负载的定义。

本教程是体验 vRealize Automation Cloud Assembly 开发过程的基础。可以使用此过程构建基础架构，并掌握云模板开发技能。

## 教程：配置 vRealize Automation Cloud Assembly 以置备生产工作负载

作为云管理员，您希望自动执行项目的部署过程，以便在云模板设计人员创建和部署模板时，vRealize Automation Cloud Assembly 为您完成相关工作。例如，使用特定的自定义计算机命名模式部署工作负载，将计算机添加到特定的 Active Directory 组织单位，以及使用特定的 DNS 和 IP 范围。

通过自动执行项目部署过程，您可以更轻松跨各个数据中心和云环境管理多个项目。

您无需完成所有任务。可以根据管理目标混搭使用这些任务中的任何一个。下面列出了可能的任务。

- 自定义计算机名称
- 创建 Active Directory 计算机记录
- 设置网络 DNS 和内部 IP 范围

### 开始之前

本教程要求您配置基础架构，并成功部署了具有计算机和网络的云模板。确认已在您的系统上配置了以下项。

- 您已成功执行了基础架构教程中指定的所有步骤。请参见教程：在 vRealize Automation Cloud Assembly 中设置和测试 vSphere 基础架构和部署。
- 您具有 Cloud Assembly 管理员角色。请参见 vRealize Automation 中的组织和服务用户角色。

### 自定义计算机名称

此任务的目标是确保基于项目的成本中心、在部署时选择的资源类型和用于确保唯一性的递增数字对 Development Project 的已部署计算机进行命名。例如，DevProject-centos-021。

可以根据您的命名要求调整此示例。

有关项目的详细信息，请参见第 5 章 添加和管理 vRealize Automation Cloud Assembly 项目。



有关演示此自定义命名示例的视频，请观看[如何为部署创建自定义命名模板](#)。

- 1 选择**基础架构 > 项目**。
- 2 选择现有项目或新建一个项目。  
在本教程中，项目名称为 Development Project。
- 3 单击**创建**。
- 4 在“项目”页面上，单击图标上的项目名称，以便可以配置项目。
- 5 单击**用户**选项卡，然后添加属于该项目成员的用户。

6 单击**置备**选项卡。

- a 在“区域”部分中，单击**添加区域**，然后添加为此项目部署工作负载的可能云区域。
- b 在“自定义属性”部分中，添加名称为 **costCenter** 且值为 **DevProject** 的自定义属性。

**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:  ⓘ

Hint: Avoid conflicting names by generating digits in names: \${#####}

- c 在“自定义命名”部分中，添加以下命名模板。

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

`${resource.osType}` 基于部署云模板时所选择的操作系统。

7 单击**保存**。

## 8 使用操作系统类型的输入值更新云模板。

输入值是您可以为用户自定义部署请求表单并简化开发过程的直接方法。通过创建输入值，您可以使用单个云模板部署多个具有不同配置的工作负载。例如，大小或操作系统。

此示例使用上一教程中的开发模板。请参见步骤 5：设计并部署基本云模板。

- a 选择**设计**并打开开发模板。
- b 在“代码”窗格中，更新 **YAML**，进行以下更改。
  - 在 **Inputs** 部分中，添加 **osType**。

在下一步中，您可以看到也使用 `osType` 输入指定映像。在 `enum` 部分中添加字符串时，值（在此示例中为 `centos` 和 `ubuntu`），必须与在**基础架构 > 配置 > 映像映射**中定义的映像名称相匹配。例如，如果映像映射名称为 **CentOS**，而不是 `centos`，则应在 `inputs` 部分中使用 **CentOS**。

```
inputs:
  osType:
    type: string
    title: OS Type
```



```
description: Select the operating system.
enum:
  - centos
  - ubuntu
```

- 在 Cloud\_vSphere\_Machine\_1 部分中，将 image 更新为 osType 输入参数 ({input.osType})，然后添加具有相同输入参数的 osType 自定义属性。

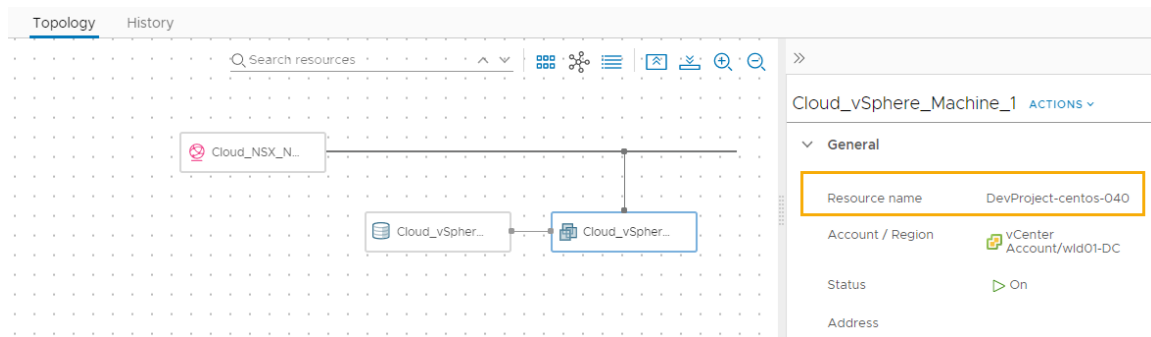
```
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: ${input.osType}
      osType: ${input.osType}
      flavor: small
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'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

- c 单击**部署**，然后输入名称 **Custom name deployment test**。
- d 单击**下一步**。
- e 从下拉菜单中选择 **centos** 操作系统。

The screenshot shows the 'Deploy Development Te...' window. On the left, a sidebar lists '1 Deployment Type' and '2 Deployment Inputs'. The main area is titled 'Deployment Inputs' and shows a form for 'OS Type' with a dropdown menu. The dropdown menu is open, showing 'centos' as the selected option, with 'centos' and 'ubuntu' as other options. At the bottom right, there are three buttons: 'CANCEL', 'PREVIOUS', and 'DEPLOY' (which is highlighted in green).

- f 单击**部署**。
- 9 跟踪进度并检查成功的部署。

在此示例中，计算机名称为 DevProject-centos-026。温馨提示：此示例基于此任务开始时引用的教程。



## 创建 Active Directory 计算机记录

置备工作负载时，可以在 Active Directory 中创建计算机记录。作为云管理员，通过配置 vRealize Automation Cloud Assembly 来为项目部署自动执行此任务，您减轻了自己的工作负载。

### 1 添加 Active Directory 集成。

#### a 选择基础架构 > 连接 > 集成。

这些步骤涵盖与此 AD 计算机记录教程相关的基本 Active Directory 配置。有关 Active Directory 集成的详细信息，请参见[如何在 vRealize Automation Cloud Assembly 中创建 Active Directory 集成](#)。

#### b 单击添加集成，然后单击 **Active Directory**。

The screenshot shows the 'Active Directory Integration' configuration page. The left sidebar has a menu with 'Resources' expanded, showing 'Compute', 'Networks', 'Security', 'Storage', 'Machines', 'Volumes', and 'Kubernetes'. The 'Activity' section is also expanded, showing 'Requests', 'Events Log', and 'Connections'. The main panel is titled 'Active Directory Integration' and has a 'Summary' tab selected. It shows the status as 'OK' and a toggle for 'Activate integration' which is turned on. The 'Name' field is 'Active Directory Integration'. The 'Description' field is empty. Under 'Active Directory Credentials', the 'LDAP host / IP' is 'ldap://cmbu-sc2dc-01.cmbu.local:389', the 'Running environment' is 'embedded-ABX-onprem', the 'Username' is 'cmbu/administrator', and the 'Password' field is empty. The 'Base DN' field is 'ou=AppDev,dc=cmbu,dc=local'. There is a 'VALIDATE' button and a warning message 'Validate credentials before making changes'.

#### c 输入用于此集成的名称。

#### d 输入 **LDAP 主机/IP** 和关联的凭据。

#### e 输入**基本 DN**。

在本教程中，示例为 **ou=AppDev,dc=cmbu,dc=local**。AppDev 是为项目添加的计算机 OU 的父 OU。

f 单击**添加**。

2 将项目添加到集成。

3 在 Active Directory 集成中，单击**项目**选项卡，然后单击**添加项目**。

#### Add Projects

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

Project \*

Relative DN \*  ⓘ

Tags  ⓘ

Matching zones

CANCEL

ADD

a 选择 App Development 项目。

b 输入相对 DN。例如，**OU=AppDev-Computers**。

c 单击**添加**。

4 要将更改保存到集成，请单击**保存**。

5 为项目部署云模板，并验证是否已将计算机添加到正确的 Active Directory OU。

## 设置网络 DNS 和内部 IP 范围

添加或更新网络配置文件，以包括 DNS 服务器和内部 IP 范围。

您必须已为 vSphere、NSX-V 或 NSX-T 创建云帐户。请参见教程：在 [vRealize Automation Cloud Assembly](#) 中设置和测试 vSphere 基础架构和部署或将云帐户添加到 vRealize Automation Cloud Assembly。

1 选择**基础架构 > 配置 > 网络配置文件**。

2 选择现有配置文件或创建一个配置文件。

3 在**摘要**选项卡上，选择**帐户/区域**，然后输入名称。

在本教程中，网络配置文件名称为 Network Profile。

4 添加网络。

a 单击**网络**选项卡。

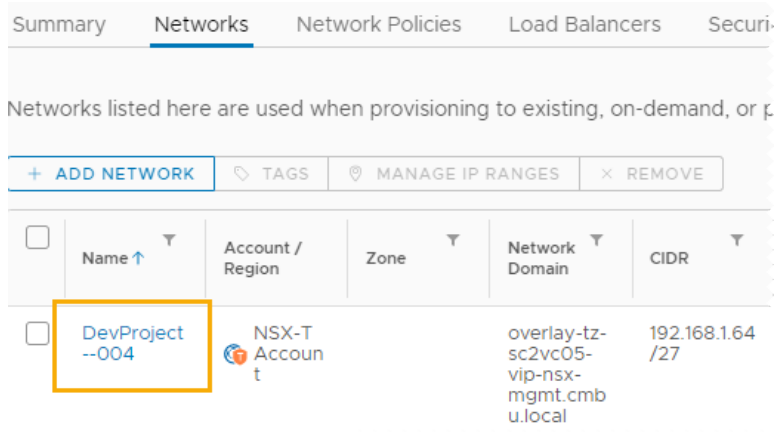
b 单击**添加网络**。

c 添加一个或多个 NSX 或 vSphere 网络。

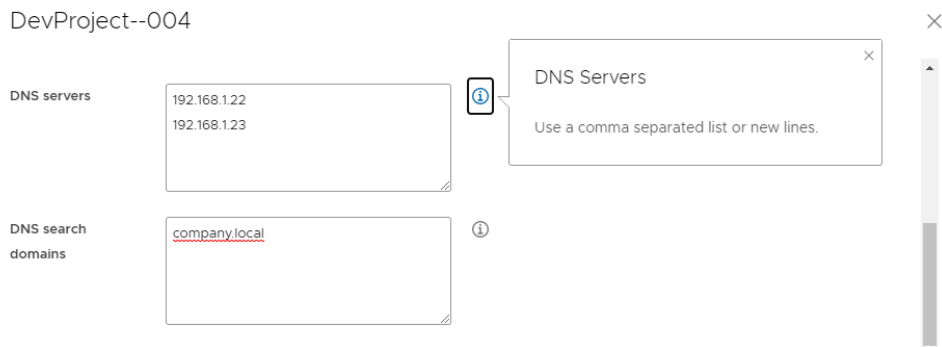
d 单击**添加**。

## 5 配置 DNS 服务器。

- a 在**网络**选项卡上的网络列表中，单击网络名称。



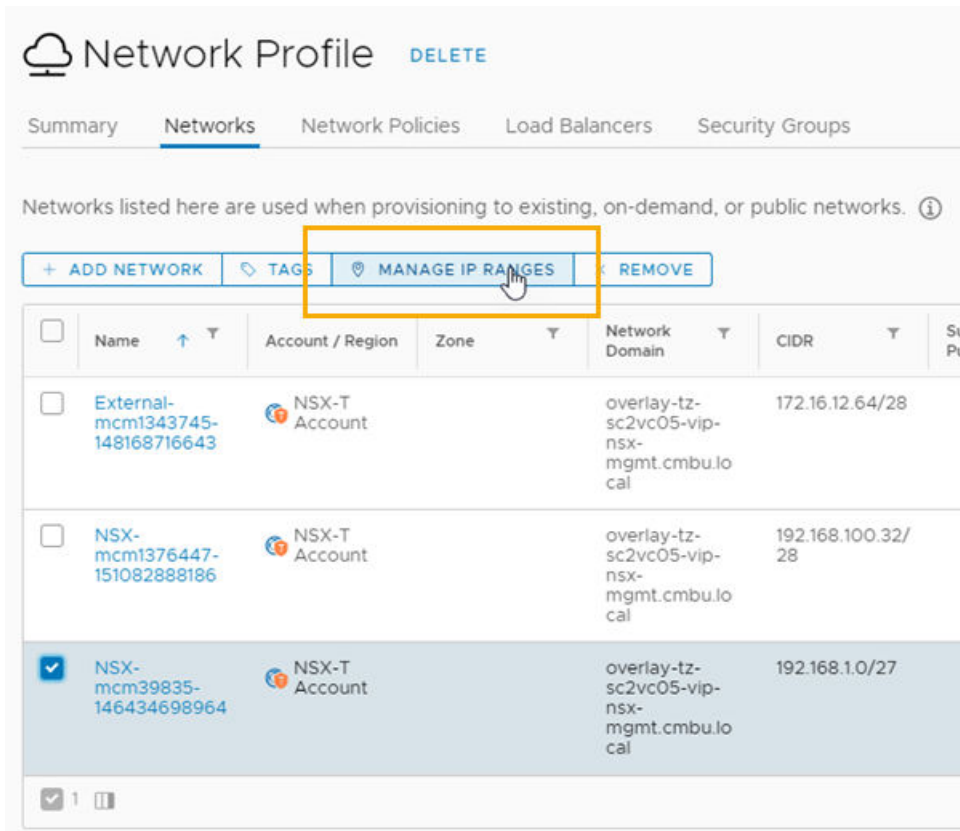
- b 输入希望此网络使用的 DNS 服务器 IP 地址。



- c 单击**保存**。

## 6 指定网络的 IP 范围。

- a 在网络列表中，选中网络名称旁边的复选框。



- b 单击**管理 IP 范围**。
- c 在“管理 IP 范围”对话框中，单击**新建 IP 范围**。

## New IP Range

**Network \*** NSX-mcm1376447-151082888186

**Source** ☒ Internal ☐ External

**Name \*** DevProject Range

**Description**

**CIDR** 192.168.100.32/28

**Start IP address \*** 192.168.100.34

**End IP address \*** 192.168.100.46

- d 输入名称。

例如 **DevProject Range**。

- e 要定义范围，请输入**起始 IP 地址**和**结束 IP 地址**。
  - f 单击**添加**。
  - g 添加其他范围，或单击**关闭**。
- 7 将包含所配置的关联网络帐户/区域的云区域添加到 Development Project 中。
  - 8 为项目部署云模板，并验证是否已在指定的 IP 范围内置备计算机。

## 教程：在 vRealize Automation Cloud Assembly 中设置和测试多云基础架构和部署

此端到端 vRealize Automation Cloud Assembly 教程说明了如何在多云设置中进行部署。可以将同一个云模板部署到多个提供程序，在本例中为 AWS 和 Microsoft Azure。

在此示例中，应用程序是一个 WordPress 站点。查看顺序设置，了解完成整个设计的过程。

请记住，显示的名称和值仅为示例而已。不能在您自己的环境中逐字使用这些名称和值。

要满足您自己的云计算基础架构和部署需求，请考虑在哪些方面对示例值进行替换。

### 第 1 部分：配置示例 vRealize Automation Cloud Assembly 基础架构

首先需要配置资源，随后 vRealize Automation Cloud Assembly 工程用户可以在这些资源中开发和测试应用程序以及将其投入生产。

基础架构包含云目标，以及有关 WordPress 站点所需的可用计算机、网络 and 存储的定义。

#### 1. 添加云帐户

在此步骤，云管理员需要添加两个云帐户。示例项目需要在 AWS 上执行开发和测试工作，然后在 Azure 上投入生产。

##### 步骤

- 1 转到**基础架构 > 连接 > 云帐户**。
- 2 单击**添加云帐户**，选择“Amazon Web Services”，然后输入值。

设置	示例值
访问密钥 ID	R5SDR3PXVV2ZW8B7YNSM
私有访问密钥	SZXAINXU4UHNQAQ1E156S
名称	OurCo-AWS
说明	WordPress

请记住，所有值都仅为示例而已。您的帐户详细信息将与此不同。

- 3 要验证凭据，请单击**验证**。

- 4 单击**添加**。
- 5 编辑新添加的帐户**配置**，并允许置备到 us-east-1 和 us-west-2 区域。
- 6 单击**添加云帐户**，选择“Microsoft Azure”，然后输入值。

设置	示例值
订阅 ID	ef2avpf-dfdv-zxlugi1i-g4h0-i8ep2jwp4c9arbfe
租户 ID	dso9wv3-4zgc-5nrcy5h3m-4skf-nnovp40wfxsro22r
客户端应用程序 ID	bg224oq-3ptp-mbhi6aa05-q511-uflyjr2sttyik6bs
客户端应用程序密钥	7uqxi57-0wtn-kymgf9wcj-t2l7-e52e4nu5fig4pmdd
名称	OurCo-Azure
说明	WordPress

- 7 要验证凭据，请单击**验证**。
- 8 单击**添加**。
- 9 编辑新添加的帐户**配置**，并允许置备到 East US 区域。

## 2. 添加云区域

在此示例步骤中，云管理员将添加三个云区域，分别用于开发、测试和生产。

云区域是项目为了支持 WordPress 站点而将计算机、网络 and 存储部署到的资源。

### 步骤

- 1 转到**基础架构 > 配置 > 云区域**。
- 2 单击**新建云区域**，并输入开发环境的值。

云区域设置	示例值
帐户/区域	OurCo-AWS/us-east-1
名称	OurCo-AWS-US-East
说明	WordPress
布置策略	默认
能力标记	env:dev

请记住，所有值都仅为示例而已。您的区域详细信息将与此不同。

- 3 单击**计算资源**，并验证其中是否列出了预期的区域。
- 4 单击**创建**。

- 5 分别使用用于测试环境的值和用于生产环境的值重复以上过程两次。

云区域设置	示例值
帐户/区域	OurCo-AWS/us-west-2
名称	OurCo-AWS-US-West
说明	WordPress
布置策略	默认
能力标记	env:test

云区域设置	示例值
帐户/区域	OurCo-Azure/East US
名称	OurCo-Azure-East-US
说明	WordPress
布置策略	默认
能力标记	env:prod

### 3. 添加特定实例映射

在此示例步骤中，云管理员将添加特定实例映射，以考虑可能因部署而异的容量需求。

特定实例映射会考虑不同大小的计算机部署，通俗地称为 T 恤调整大小。

#### 步骤

- 1 转到**基础架构 > 配置 > 特定实例映射**。每个云区域都必须能够容纳小型、中型和大型特定实例。
- 2 单击**新建特定实例映射**，并输入开发云区域的值。

设置	示例值
特定实例名称	small
帐户/区域 值	OurCo-AWS/us-east-1 t2.micro
帐户/区域 值	OurCo-AWS/us-west-2 t2.micro
帐户/区域 值	OurCo-Azure/East US Standard_A0

请记住，所有值都仅为示例而已。您的特定实例将与此不同。

- 3 单击**创建**。



- 4 分别使用用于中型特定实例的值和用于大型特定实例的值重复以上过程两次。

设置	示例值
特定实例名称	medium
帐户/区域 值	OurCo-AWS/us-east-1 t2.medium
帐户/区域 值	OurCo-AWS/us-west-2 t2.medium
帐户/区域 值	OurCo-Azure/East US Standard_A3

设置	示例值
特定实例名称	large
帐户/区域 值	OurCo-AWS/us-east-1 t2.large
帐户/区域 值	OurCo-AWS/us-west-2 t2.large
帐户/区域 值	OurCo-Azure/East US Standard_A7

## 4. 添加映像映射

在此示例步骤中，云管理员为 Ubuntu 添加映像映射，以及 WordPress 服务器及其 MySQL 数据库服务器的主机。

通过添加映像映射，对操作系统进行计划。每个云区域都需要一个 Ubuntu 映像映射。

### 步骤

- 1 转到**基础架构 > 配置 > 映像映射**。
- 2 单击**新建映像映射**，然后输入 Ubuntu 服务器的值。

设置	示例值
映像名称	ubuntu
帐户/区域 值	OurCo-AWS/us-east-1 ubuntu-16.04-server-cloudimg-amd64
帐户/区域 值	OurCo-AWS/us-west-2 ubuntu-16.04-server-cloudimg-amd64
帐户/区域 值	OurCo-Azure/East US azul-zulu-ubuntu-1604-923eng

请记住，所有值都仅为示例而已。您的映像会有变化。

### 3 单击创建。

## 5. 添加网络配置文件

在此示例步骤中，云管理员需要将网络配置文件添加到每个云区域。

在每个配置文件中，管理员可以为 WordPress 计算机添加一个网络，并添加位于最终负载均衡器另一端的另一个网络。第二个网络将是用户最终连接到的网络。

### 步骤

- 1 转到**基础架构 > 配置 > 网络配置文件**。
- 2 单击**新建网络配置文件**，然后创建用于开发云区域的配置文件。

网络配置文件设置	示例值
帐户/区域	OurCo-AWS/us-east-1
名称	devnets
说明	WordPress

- 3 单击**网络**，然后单击**添加网络**。
- 4 选择 wpnet 和 appnet-public，然后单击**添加**。  
请记住，所有值都仅为示例而已。您的网络名称将与此不同。
- 5 单击**创建**。

此 Wordpress 示例不要求指定网络策略或网络安全设置。

- 6 重复上述过程两次，以创建用于 WordPress 示例测试云区域的配置文件和用于生产云区域的配置文件。在每种情况下，都需要添加 wpnet 网络和 appnet-public 网络。

网络配置文件设置	示例值
帐户/区域	OurCo-AWS/us-west-2
名称	testnets
说明	WordPress

网络配置文件设置	值
帐户/区域	OurCo-Azure/East US
名称	prodnets
说明	WordPress

## 6. 添加存储配置文件

在此示例步骤中，云管理员需要将存储配置文件添加到每个云区域。

管理员将快速存储放置到生产区域，而将一般存储放置到开发区域和测试区域。

### 步骤

- 1 转到**基础架构 > 配置 > 存储配置文件**。
- 2 单击**新建存储配置文件**，然后创建用于开发云区域的配置文件。

选择帐户/区域之后，将显示其他字段。

存储配置文件设置	示例值
帐户/区域	OurCo-AWS/us-east-1
名称	OurCo-AWS-US-East-Disk
说明	WordPress
设备类型	EBS
卷类型	通用 SSD
能力标记	storage:general

请记住，所有值都仅为示例而已。

- 3 单击**创建**。
- 4 重复上述过程以创建用于测试云区域的配置文件。

存储配置文件设置	示例值
帐户/区域	OurCo-AWS/us-west-2
名称	OurCo-AWS-US-West-Disk
说明	WordPress
设备类型	EBS
卷类型	通用 SSD
能力标记	storage:general

- 5 重复上述过程以创建用于生产云区域的配置文件，生产云区域具有不同的设置，因为它是 Azure 区域。

存储配置文件设置	示例值
帐户/区域	OurCo-Azure/East US
名称	OurCo-Azure-East-US-Disk

存储配置文件设置	示例值
说明	WordPress
存储类型	受管磁盘
磁盘类型	高级 LRS
操作系统磁盘缓存	只读
数据磁盘缓存	只读
能力标记	storage:fast

### 后续步骤

创建项目以确定用户并定义置备设置。请参见第 2 部分：[创建示例 vRealize Automation Cloud Assembly 项目](#)。

## 第 2 部分：创建示例 vRealize Automation Cloud Assembly 项目

此示例 vRealize Automation Cloud Assembly 项目指定具有置备权限的用户，并配置可能的置备量。

项目定义了用户设置和置备设置。

- 用户及其角色的权限级别
- 将部署置备到云区域时遵循的优先级
- 每个云区域的最大部署实例数

### 步骤

- 1 转到**基础架构 > 管理 > 项目**。
- 2 单击**新建项目**，然后输入名称“WordPress”。
- 3 单击**用户**，然后单击**添加用户**。
- 4 添加用户的电子邮件地址和角色。

要成功添加用户，VMware Cloud Services 管理员必须已向该用户授予 vRealize Automation Cloud Assembly 的访问权限。

请记住，此处显示的地址仅为示例而已。

- chris.ladd@ourco.com，成员
- kerry.mott@ourco.com，成员
- pat.tubb@ourco.com，管理员

- 5 单击**置备**，然后单击**添加云区域**。

## 6 添加用户可部署到的云区域。

项目云区域设置	示例值
云区域	OurCo-AWS-US-East
置备优先级	1
实例限制	5
云区域	OurCo-AWS-US-West
置备优先级	1
实例限制	5
云区域	OurCo-Azure-East-US
置备优先级	0
实例限制	1

## 7 单击**创建**。

## 8 转到**基础架构 > 配置 > 云区域**，然后打开之前创建的区域。

## 9 单击**项目**，然后验证 WordPress 项目是否可以置备到该区域。

## 10 检查您创建的其他区域。

### 后续步骤

创建基本云模板。

## 第 3 部分：设计并部署示例 vRealize Automation Cloud Assembly 模板

接下来，您将以通用云模板的形式定义示例应用程序（WordPress 站点）。模板可以部署到不同的云供应商，而无需更改其设计。

该示例包含 WordPress 应用程序服务器、MySQL 数据库服务器和支持资源。该模板从几个资源开始，然后随着您修改这些资源并添加更多资源逐渐增长。

以下是第 1 部分：**配置示例 vRealize Automation Cloud Assembly 基础架构**（由云管理员设置的基础架构）中的值：

- 两个云帐户，AWS 和 Azure。
- 三个云区域环境：
  - 开发 - OurCo-AWS-US-East
  - 测试 - OurCo-AWS-US-West
  - 生产 - OurCo-Azure-East-US
- 为每个区域配置特定实例映射且具有小型、中型和大型计算资源。
- 在每个区域中配置的 Ubuntu 映像映射。
- 为每个区域配置的包含内部子网和外部子网的网络配置文件。
- 用于部署的存储：用于开发和测试区域的常规存储，以及用于生产区域的快速存储。

- 示例项目包括全部三个云区域环境以及可以创建设计的用户。

### 前提条件

要继续操作，您必须熟悉自己的基础架构值。此示例将 **AWS** 用于开发和测试，而将 **Azure** 用于生产。创建自己的云模板时，可以替换为自己的值（通常由云管理员设置）。

### 步骤

#### 1 创建基本云模板

在此 vRealize Automation Cloud Assembly 设计示例中，您可以从仅包含最少 **WordPress** 资源（例如，仅包含一个应用程序服务器）的云模板开始。

#### 2 测试基本云模板

在设计过程中，通常先从基本组件开始构建云模板，然后随着模板的增长进行部署和测试。此示例说明了 vRealize Automation Cloud Assembly 内置的一些正在进行的测试。

#### 3 扩展云模板

创建和测试示例应用程序的基本 vRealize Automation Cloud Assembly 模板后，可将其扩展到多层应用程序，之后该应用程序可部署到开发、测试环境，最终部署到生产环境。

### 创建基本云模板

在此 vRealize Automation Cloud Assembly 设计示例中，您可以从仅包含最少 **WordPress** 资源（例如，仅包含一个应用程序服务器）的云模板开始。

vRealize Automation Cloud Assembly 是一个基础架构即代码工具。您可以通过将资源拖动到设计画布，开始入手。然后使用画布右边的代码编辑器填写详细信息。

代码编辑器允许您直接键入、剪切和粘贴代码。如果您不喜欢编辑代码，则可以在画布中选择一个资源，单击代码编辑器的**属性**选项卡，并在其中输入值。您输入的值将显示在代码中，就像直接键入它们一样。

### 步骤

- 1 转到**设计 > 云模板**，然后单击**新建自 > 空白画布**。
- 2 将云模板命名为 **Wordpress-BP**。
- 3 选择 **WordPress** 项目，然后单击**创建**。
- 4 从云模板设计页面左侧的资源中，将两台云平台无关的计算机拖动到画布中。  
这两台计算机分别用作 **WordPress** 应用程序服务器 (**WebTier**) 和 **MySQL** 数据库服务器 (**DBTier**)。
- 5 在右侧，编辑计算机 **YAML** 代码以添加名称、映像、特定实例和限制标记：

```
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 将云不可知的网络拖动到画布中，并编辑其代码：

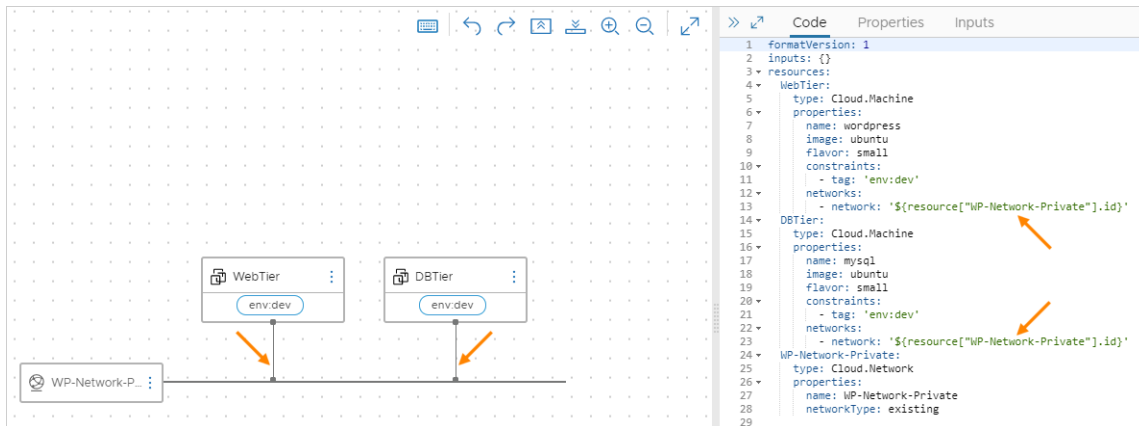
```

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

```

## 7 将两台计算机连接到该网络：

在画布中，将鼠标悬停在网络块上，单击并按住线与网络块接触的气泡，拖动到计算机块，然后释放。创建连接线时，请注意，网络代码会自动添加到编辑器中的计算机。



## 8 添加用户输入提示。

在某些位置，示例基础架构设置为用于多种方案。例如：

- 用于开发、测试和生产的云区域环境
- 用于小型、中型和大型计算机的特定实例映射

您可以直接在云模板中设置特定选项，但更好的方法是让用户在部署模板时选择选项。通过提示提供用户输入，您可以创建具有许多种部署方式的单个模板，而不必创建多个硬编码模板。

- a 在代码中创建 `inputs` 节，以便用户可以在部署时选择计算机大小和目标环境。定义可选择的值：

```
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 在代码的 `resources` 节中，添加 `${input.input-name}` 代码以提示提供用户选择：

```
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 最后，使用以下示例增强 `WebTier` 和 `DBTier` 代码。`WP-Network-Private` 代码不需要其他更改。  
请注意，增强包括对数据库服务器和部署时 `cloudConfig` 初始化脚本的登录访问。

组件	示例
其他 DBTier 输入	<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 资源	<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 资源	<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>

组件	示例
	<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 &amp;&amp; cd /var/www/html &amp;&amp;     wget https://wordpress.org/latest.tar.gz &amp;&amp; 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;" &amp;&amp;     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 &amp;&amp; sed     -i -e s/"define( 'DB_USER', 'username_here' );"/"define( 'DB_USER',     'root' );"/ /var/www/html/mywordpresssite/wp-config.php &amp;&amp; sed -i -e     s/"define( 'DB_PASSWORD', 'password_here' );"/"define( 'DB_PASSWORD',     'mysqlpassword' );"/ /var/www/html/mywordpresssite/wp-config.php &amp;&amp; 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>

### 示例：完成的基本云模板代码示例

```

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

```

## 后续步骤

通过检查语法并部署云模板来测试云模板。

## 测试基本云模板

在设计过程中，通常先从基本组件开始构建云模板，然后随着模板的增长进行部署和测试。此示例说明了 vRealize Automation Cloud Assembly 内置的一些正在进行的测试。

为了确保部署按您希望的方式运作，可以多次测试和部署云模板。您可以逐渐添加更多资源、重新测试和重新部署。

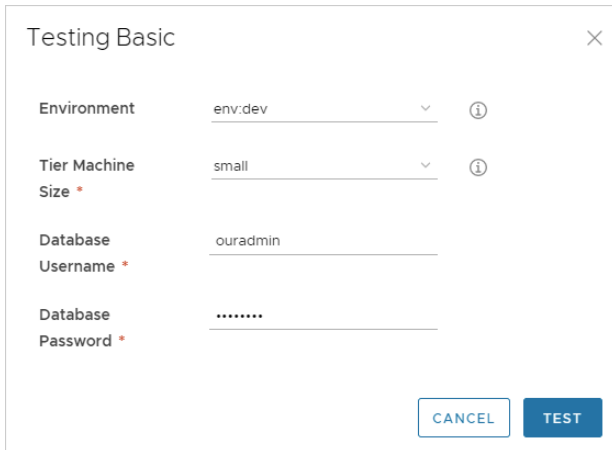
## 前提条件

创建基本云模板。请参见 [创建基本云模板](#)。

## 步骤

- 1 单击 **云模板**，然后打开 **WordPress-BP** 云模板。  
基本云模板将显示在设计画布和代码编辑器中。
- 2 要检查模板语法、布置位置和基本有效性，请单击左下角的 **测试**。

### 3 键入输入值，然后单击测试。

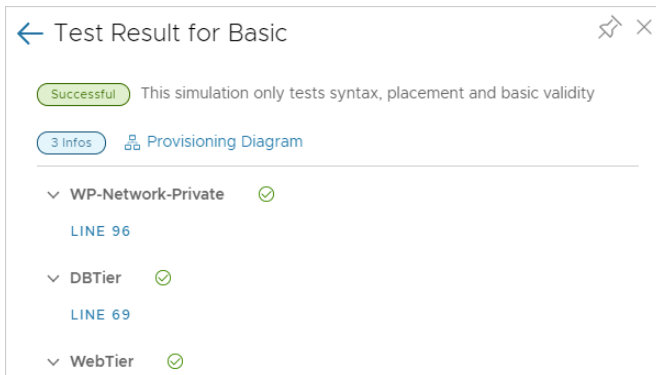


The 'Testing Basic' dialog box contains the following fields:

- Environment: env:dev (dropdown menu)
- Tier Machine Size: small (dropdown menu)
- Database Username: ouradmin (text input)
- Database Password: masked with dots (password input)

Buttons: CANCEL, TEST

测试只是一个模拟，实际上并不部署虚拟机或其他资源。







测试包括指向**置备图**的链接，您可以在其中检查模拟的部署流并查看发生的情况。模拟可发现潜在问题，例如，未定义任何与云模板中的硬性限制相匹配的资源功能。在下面的示例错误中，在所定义基础架构中的任何位置都找不到功能标记 env:dev 的云区域。



成功的模拟不保证部署模板时不出错。

- 4 在模板通过模拟后，单击左下角的**部署**。
- 5 选择**选择新部署**。
- 6 将部署命名为 **WordPress for OurCo**，然后单击**下一步**。
- 7 键入输入值，然后单击**部署**。
- 8 要验证模板是否已成功部署，请在**部署 > 部署**下进行检查。

如果某个部署失败，请单击其名称，然后单击**历史记录**选项卡以查看有助于进行故障排除的消息。

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

某些历史记录条目的最右侧可能具有**置备图**链接。该图与模拟的图类似，您可以在其中检查置备过程中 vRealize Automation Cloud Assembly 决策点的流程图。

如需查看更多流程图，请单击**基础架构 > 活动 > 请求**。

- 9 要验证应用程序是否正常工作，请在浏览器中打开 WordPress 起始页面。

- a 等待 WordPress 服务器完全创建并初始化。  
初始化可能需要 30 分钟或更长时间，具体取决于环境。
- b 要查找站点 FQDN 或 IP 地址，请转到**部署 > 部署 > 拓扑**。
- c 在画布中，单击“WebTier”，然后在右侧的面板中查找 IP 地址。
- d 输入 IP 地址，作为 WordPress 起始页面完整 URL 的一部分。

在此示例中，完整 URL 是：

`http://{IP-address}/mywordpresssite`

或

`http://{IP-address}/mywordpresssite/wp-admin/install.php`

- 10 在浏览器中检查 WordPress 后，如果需要对应用程序进行其他处理，请进行模板更改并使用**更新现有部署**选项进行重新部署。

11 考虑对云模板进行版本控制。如果更改导致部署失败，可以恢复到正常工作的版本。

- a 在云模板设计页面上，单击**版本**。
- b 在“创建版本”页面中，输入 **WP-1.0**。

请勿在版本名称中输入空格。

- c 单击**创建**。

要复查或恢复到某个版本，请在设计页面中单击**版本历史记录**选项卡。

12 基本部署现已准备就绪，可以通过增加应用程序服务器和数据库服务器的 CPU 和内存来尝试首次部署时增强。

将应用程序服务器和数据库服务器更新到中型节点大小。使用同一个模板，在部署时选择 **medium**，重新部署并重新验证应用程序。

### 后续步骤

通过添加更多资源，将云模板扩展至适用于生产的应用程序。

## 扩展云模板

创建和测试示例应用程序的基本 vRealize Automation Cloud Assembly 模板后，可将其扩展到多层应用程序，之后该应用程序可部署到开发、测试环境，最终部署到生产环境。

要扩展云模板，请添加以下增强功能。

- 用于集群应用程序服务器以增加容量的选项
- 应用程序服务器前面的公用网络和负载均衡器
- 具有存档存储的备份服务器

### 前提条件

创建基本云模板并对其进行测试。请参见[创建基本云模板](#)和[测试基本云模板](#)。

### 步骤

1 单击**云模板**，然后打开 **WordPress-BP** 云模板。

基本模板将显示在设计画布和代码编辑器中。

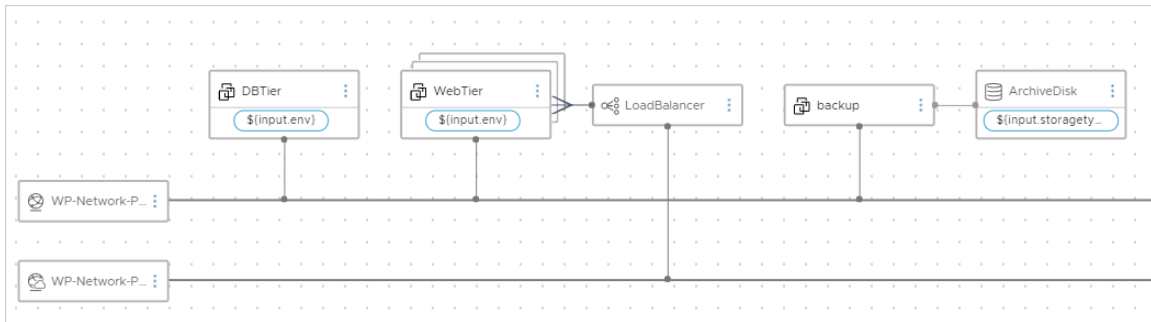
2 使用代码示例和图作为指导进行添加和更改。

您可以使用 GUI 将新资源拖到画布（如负载均衡器），然后在代码编辑器中完成配置。

- a 添加 **count** 输入提示，以使 **WordPress** 应用程序服务器加入集群。
- b 添加云不可知负载均衡器。
- c 将负载均衡器连接到 **WordPress** 应用程序服务器集群。
- d 添加云不可知的备份计算机。
- e 将备份计算机连接到专用/内部网络。
- f 添加云不可知的公用/外部网络。



- g 将负载均衡器连接到公共网络。
  - h 添加一个云不可知的存储卷，用作存档磁盘。
  - i 将存档磁盘连接到备份计算机。
  - j 为存档磁盘速度添加输入提示。
- 3 使用与基本云模板相同的方式进行部署、测试和更改。
- 您可以更新现有部署，甚至部署新实例，以便可以比较部署。
- 目标是实现可用于生产部署的可靠、可重用模板。



#### 示例：完成的扩展云模板代码示例

```
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}'

```

### 后续步骤

定义您自己的基础架构并创建自己的云模板。

请参见第 4 章 [构建您的 vRealize Automation Cloud Assembly 资源基础架构](#) 和第 6 章 [设计 vRealize Automation Cloud Assembly 部署](#)。

## 教程：为 vRealize Automation 配置 VMware Cloud on AWS

此 vRealize Automation Cloud Assembly 教程介绍定义资源基础架构和云模板设置以部署到 VMware Cloud on AWS 环境的过程。

此过程要求云管理员已按照 [VMware Cloud on AWS 入门指南文档](#) 中的部署和管理软件定义的数据中心中所述配置组织的 VMware Cloud on AWS SDDC 数据中心。

请查看顺序设置，了解为 VMware Cloud on AWS 配置环境的过程。请注意，用例中的值仅用作示例。请考虑在何处需要替换为您自己的值或从示例值外插值，以便满足您自己的云计算基础架构需求和部署需求。

如何为 [Cloud Assembly](#) 配置 [VMware Cloud on AWS](#) 的 VMware 云计算管理技术营销中提供了类似工作流的详细视频。

## 步骤

### 1 在 [vRealize Automation](#) 中配置基本 [VMware Cloud on AWS](#) 工作流

此用例显示了定义资源基础架构和相应的云模板以部署到 [VMware Cloud on AWS](#) 环境的过程。

### 2 在 [vRealize Automation](#) 的 [VMware Cloud on AWS](#) 工作流中配置隔离网络

在此过程中，您将在 [vRealize Automation](#) 中为 [VMware Cloud on AWS](#) 部署添加一个隔离网络。

## 在 [vRealize Automation](#) 中配置基本 [VMware Cloud on AWS](#) 工作流

此用例显示了定义资源基础架构和相应的云模板以部署到 [VMware Cloud on AWS](#) 环境的过程。

在此过程中，您将配置支持将云模板部署到现有 [VMware Cloud on AWS](#) 环境中资源的基础架构。

## 前提条件

- 在 [vRealize Automation Cloud Assembly](#) 中创建和配置 [VMware Cloud on AWS](#) 云帐户之前，您必须属于现有 [VMware Cloud on AWS SDDC](#) 环境中的某个组织。有关配置 [VMware Cloud on AWS](#) 服务的信息，请参见 [VMware Cloud on AWS](#) 文档。
- 为了方便在 [vCenter](#) 中的现有 [VMware Cloud on AWS](#) 主机 SDDC 与 [vRealize Automation Cloud Assembly](#) 中的 [VMware Cloud on AWS](#) 云帐户之间建立所需连接，您必须使用 VPN 或类似的网络连接方式提供网络连接并添加防火墙规则。请参见准备 [VMware Cloud on AWS SDDC](#) 连接到 [vRealize Automation](#) 中的 [VMware Cloud on AWS](#) 云帐户。

## 步骤

### 1 准备 [VMware Cloud on AWS SDDC](#) 连接到 [vRealize Automation](#) 中的 [VMware Cloud on AWS](#) 云帐户

在 [vRealize Automation Cloud Assembly](#) 内部部署环境中使用 [VMware Cloud on AWS](#) 云帐户时，您必须创建网络连接才能支持 [vCenter](#) 中的 SDDC 和 [vRealize Automation](#) 中的任何 [VMware Cloud on AWS](#) 云帐户之间的通信。

### 2 在 [vRealize Automation](#) 的示例工作流中创建 [VMware Cloud on AWS](#) 云帐户

在此步骤中，将在 [vRealize Automation](#) 中创建一个 [VMware Cloud on AWS](#) 云帐户。

### 3 为 [vRealize Automation](#) 中的 [VMware Cloud on AWS](#) 部署创建云区域

在此步骤中，您将创建一个云区域，以指定 [CloudAdmin](#) 用户在 [vRealize Automation](#) 中使用 [VMware Cloud on AWS](#) 时可以访问的计算资源。

### 4 为 [vRealize Automation](#) 中的 [VMware Cloud on AWS](#) 部署配置网络和存储配置文件

在此步骤中，您将配置网络配置文件和存储配置文件，以便指定可供 [vRealize Automation](#) 中的 [VMware Cloud on AWS CloudAdmin](#) 用户使用的资源。

## 5 在 vRealize Automation 中创建一个项目以支持 VMware Cloud on AWS 部署

在此步骤中，您将定义一个 vRealize Automation 项目，该项目可用于控制 VMware Cloud on AWS 部署可用的资源。

## 6 在云模板设计中定义 vCenter 计算机资源以支持 vRealize Automation 中的 VMware Cloud on AWS 部署

在此步骤中，您将 vCenter 计算机资源拖动到设计画布上，并为 vRealize Automation 中的 VMware Cloud on AWS 部署添加设置。

## 准备 VMware Cloud on AWS SDDC 连接到 vRealize Automation 中的 VMware Cloud on AWS 云帐户

在 vRealize Automation Cloud Assembly 内部部署环境中使用 VMware Cloud on AWS 云帐户时，您必须创建网络连接才能支持 vCenter 中的 SDDC 和 vRealize Automation 中的任何 VMware Cloud on AWS 云帐户之间的通信。

为了方便在 vCenter 中的现有 VMware Cloud on AWS 主机 SDDC 与 vRealize Automation 中的 VMware Cloud on AWS 云帐户之间建立所需连接，您必须使用 VPN 或类似的网络连接方式在这两个元素之间提供网络连接。

### 步骤

#### 1 通过公用 Internet 或 AWS Direct Connect 配置 VPN 连接。

请参见 [VMware Cloud on AWS 文档](#) 中的《VMware Cloud on AWS 网络和安全》。

#### 2 确认 vCenter Server FQDN 可在管理网络上的专用 IP 地址处解析。

请参见 [VMware Cloud on AWS 文档](#) 中的《VMware Cloud on AWS 网络和安全》。

#### 3 配置所需的防火墙规则。

您必须在 SDDC 的 VMware Cloud on AWS 控制台中配置管理网关防火墙规则，以支持通信。这些规则必须位于**管理网关**防火墙规则区域中。通过使用 SDDC 控制台中**网络和安全**选项卡上的选项创建防火墙规则。

- 将使用 HTTPS (TCP 443) 服务的 ESXi 网络流量限制到 vRealize Automation 设备/服务器或 vRealize Automation 负载均衡器 VIP 的已发现 IP 地址。
- 将使用 ICMP（全部 ICMP）、SSO (TCP 7444) 和 HTTPS (TCP 443) 服务的 vCenter 网络流量限制到 vRealize Automation 设备/服务器或 vRealize Automation 负载均衡器 VIP 的已发现 IP 地址。
- 将使用 HTTPS (TCP 443) 服务的 NSX-T Manager 网络流量限制到 vRealize Automation 设备/服务器或 vRealize Automation 负载均衡器 VIP 的已发现 IP 地址。

下表汇总了所需的防火墙规则。

表 2-1. 必需的管理网关防火墙规则摘要

名称	源	目标	服务
vCenter	内部部署数据中心的 CIDR 块	vCenter	任意（所有流量）
vCenter ping	任意	vCenter	ICMP（所有 ICMP）
NSX Manager	内部部署数据中心的 CIDR 块	NSX Manager	任意（所有流量）
内部部署到 ESXi ping	内部部署数据中心的 CIDR 块	仅 ESXi 管理	ICMP（所有 ICMP）
内部部署到 ESXi 远程控制台和置备	内部部署数据中心的 CIDR 块	仅 ESXi 管理	TCP 902
内部部署到 SDDC 虚拟机	内部部署数据中心的 CIDR 块	SDDC 逻辑网络的 CIDR 块	任意（所有流量）
SDDC 虚拟机到内部部署	SDDC 逻辑网络的 CIDR 块	内部部署数据中心的 CIDR 块	任意（所有流量）

有关相关信息，请参见 [VMware Cloud on AWS 文档](#) 中的《VMware Cloud on AWS 网络和安全》和《VMware Cloud on AWS 操作指南》。

## 结果

配置所需的网关访问和防火墙规则后，可以继续创建 VMware Cloud on AWS 云帐户的过程。

## 在 vRealize Automation 的示例工作流程中创建 VMware Cloud on AWS 云帐户

在此步骤中，将在 vRealize Automation 中创建一个 VMware Cloud on AWS 云帐户。

有关相关信息，请参见 [VMware Cloud on AWS 文档](#)。

除非另有说明，否则在此过程中输入的步骤值仅适用于此示例工作流程。

## 前提条件

- 此过程假设您具有所需的管理员凭据，包括 vCenter 中目标 SDDC 的 VMware Cloud on AWS CloudAdmin 凭据，并假设您已在端口 443 上启用 HTTPS 访问。请参见在 [vRealize Automation 中使用云帐户所需的凭据](#)。
- 此过程假设您具有云管理员用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 为了方便在 vCenter 中的现有 VMware Cloud on AWS 主机 SDDC 与 vRealize Automation 中的 VMware Cloud on AWS 云帐户之间建立所需连接，您必须使用 VPN 或类似的网络连接方式提供网络连接和防火墙规则。请参见 [准备 VMware Cloud on AWS SDDC 连接到 vRealize Automation 中的 VMware Cloud on AWS 云帐户](#)。如果您使用的是外部 HTTP Internet 代理，则必须针对 IPv4 对其进行配置。
- 如果您没有外部 Internet 访问，请配置一个 Internet 服务器代理。请参见 [如何配置 vRealize Automation 的 Internet 代理服务器](#)。

## 步骤

- 1 选择**基础架构 > 连接 > 云帐户**。
- 2 单击**添加云帐户**，选择“VMware Cloud on AWS”，然后输入值。

下表提供了示例值和支持信息。

设置	示例值和说明	说明
VMC API 令牌	<ol style="list-style-type: none"> <li>1 单击 <b>VMC API 令牌</b> 行末端的 i 帮助图标，然后在帮助文本框中单击 <b>API 令牌</b> 页面，以打开您组织的<b>我的帐户</b>页面上的 <b>API 令牌</b> 选项卡。</li> <li>2 单击<b>生成令牌</b>以显示<b>生成新的 API 令牌</b> 选项。</li> <li>3 输入新令牌名称，例如 <b>myinitials_mytoken</b>。</li> <li>4 将<b>令牌 TTL</b> 设置为<b>永不过期</b>。  如果创建设置为过期的令牌，则在令牌过期时，vRealize Automation 中的 VMware Cloud on AWS 操作将停止工作，并在您使用新令牌更新云帐户之前，这些操作将保持不工作状态。</li> <li>5 在<b>定义范围</b>部分中，选择<b>所有角色</b>。    </li> <li>6 单击<b>生成</b>。</li> <li>7 在生成的令牌页面中，单击<b>复制</b>，然后单击<b>继续</b>。</li> <li>8 返回<b>新建云帐户</b>页面，将复制的令牌粘贴到 <b>VMC API 令牌</b> 行，然后单击<b>应用 API 令牌</b>。    </li> </ol>	<p>可以在链接的 <b>API 令牌</b> 页面上为您的组织创建新令牌或使用现有令牌。</p> <p>在<b>定义范围</b>部分中，API 令牌要求的最小角色为：</p> <ul style="list-style-type: none"> <li>■ <b>组织角色</b> <ul style="list-style-type: none"> <li>■ 组织成员</li> <li>■ 组织所有者</li> </ul> </li> <li>■ <b>服务角色 - VMware Cloud on AWS</b> <ul style="list-style-type: none"> <li>■ 管理员</li> <li>■ NSX Cloud 管理员</li> <li>■ NSX Cloud 审核员</li> </ul> </li> </ul> <p><b>注</b> 复制、下载或打印生成的令牌。离开此页面后，将无法检索生成的令牌。</p> <p>应用生成的令牌或提供的令牌连接到组织 VMware Cloud on AWS 订阅中的可用 SDDC 环境，并填充 SDDC 名称列表。</p> <p>如果 vRealize Automation 和 VMware Cloud on AWS 服务位于不同组织中，应切换到 VMware Cloud on AWS 组织，然后生成令牌。</p> <p>有关 API 令牌的更多信息，请参见<b>生成 API 令牌</b>。</p>
SDDC 名称	<p>对于此示例，请选择 <b>Datacenter:Datacenter-abz</b>。</p> <p>有效的 SDDC 名称将自动填充 vCenter 和 NSX-T FQDN 条目。如果云代理已部署到该 SDDC，则云代理值也会自动填充。</p>	<p>从 VMware Cloud on AWS 订阅中的可用 SDDC 列表中进行选择。SDDC 列表基于 VMware Cloud on AWS API 令牌。</p> <p>NSX-V SDDC 不受 vRealize Automation 支持，因此不显示在可用 SDDC 列表中。</p>



设置	示例值和说明	说明
vCenter IP 地址/ FQDN	地址会根据选择的 SDDC 自动填充。	输入指定 SDDC 中的 vCenter Server 的 IP 地址或 FQDN。  IP 地址默认为专用 IP 地址。根据用于访问 SDDC 的网络连接类型，默认地址可能不同于指定 SDDC 中 NSX Manager Server 的 IP 地址。
NSX Manager IP 地址/FQDN	地址会根据选择的 SDDC 自动填充。	确定指定 SDDC 中的 NSX Manager 的 IP 地址或 FQDN。  IP 地址默认为专用 IP 地址。根据用于访问 SDDC 的网络连接类型，默认地址可能不同于指定 SDDC 中 NSX Manager Server 的 IP 地址。  VMware Cloud on AWS 云帐户支持 NSX-T。
vCenter 用户名和密码	系统会自动填充用户名 cloudadmin@vmc.local。	如果与默认用户名不同，则输入指定 SDDC 的 vCenter 用户名。  指定的用户需要 CloudAdmin 凭据。用户不需要 CloudGlobalAdmin 凭据。  输入用户密码。
验证	单击 <b>验证</b> 。	验证将确认您对指定 vCenter 的访问权限，并检查 vCenter 是否正在运行。
名称和说明	输入 <b>OurCo-VMC</b> 作为云帐户名称。  输入 <b>Sample deployment for VMC</b> 作为云帐户说明。	
允许置备到这些数据中心	此信息为只读。	列出指定 VMware Cloud on AWS SDDC 环境中的可用数据中心。
创建云区域	取消选中该复选框。对于此示例，将稍后在工作流中创建一个云区域。	请参见了解有关 <a href="#">vRealize Automation Cloud Assembly</a> 云区域的更多信息。
能力标记	将此设置留空。此工作流不使用功能标记。	请根据您组织的标记策略使用标记。请参见 <a href="#">如何使用标记来管理 vRealize Automation Cloud Assembly</a> 资源和部署和创建标记策略。

### 3 单击添加。

#### 结果

将从 VMware Cloud on AWS SDDC 数据中心收集计算机和卷等资源的数据，并列在 vRealize Automation **基础架构** 选项卡的 **资源** 部分中。

#### 后续步骤

为 [vRealize Automation](#) 中的 [VMware Cloud on AWS](#) 部署创建云区域。

## 为 vRealize Automation 中的 VMware Cloud on AWS 部署创建云区域

在此步骤中，您将创建一个云区域，以指定 CloudAdmin 用户在 vRealize Automation 中使用 VMware Cloud on AWS 时可以访问的计算资源。

在 VMware Cloud on AWS 中，两个主要管理员凭据是 CloudGlobalAdmin 和 CloudAdmin。vRealize Automation Cloud Assembly 设计为支持 CloudAdmin 用户。部署到可供 VMware Cloud on AWS CloudAdmin 用户使用的资源。不要部署到需要 VMware Cloud on AWS CloudGlobalAdmin 凭据的资源。

云区域标识项目云模板在其上部署计算机、网络 and 存储的计算资源。请参见[了解有关 vRealize Automation Cloud Assembly 云区域的更多信息](#)。

除非另有说明，否则在此过程中输入的步骤值仅适用于此示例工作流。

### 前提条件

- 完成在 vRealize Automation 的示例工作流中创建 VMware Cloud on AWS 云帐户过程。
- 此过程假设您具有所需的管理人员凭据，包括 vCenter 中目标 SDDC 的 VMware Cloud on AWS CloudAdmin 凭据。请参见在 vRealize Automation 中使用云帐户所需的凭据。
- 此过程假设您具有云管理员用户角色。请参见 vRealize Automation 用户角色是什么。

### 步骤

- 1 选择**基础架构 > 配置 > 云区域**。
- 2 单击**新建云区域**，并输入 VMware Cloud on AWS 环境的值。

设置	示例值
帐户/区域	OurCo-VMC / Datacenter:Datacenter-abz 这是您在上一在 <a href="#">vRealize Automation</a> 的示例工作流中创建 <a href="#">VMware Cloud on AWS</a> 云帐户中定义的云帐户和关联区域。
名称	VMC_cloud_zone-1
说明	仅 VMware Cloud on AWS 资源
布置策略	默认
能力标记	将此设置留空。此工作流不使用功能标记。

- 3 单击**计算**选项卡。
- 4 如下面的区域 1 中所示，查找并选择可供 CloudAdmin 用户使用的计算资源。对于此示例，使用名为 Cluster 1/ Compute-ResourcePool 的资源。

Cluster 1/ Compute-ResourcePool 是 VMware Cloud on AWS 的默认计算资源。

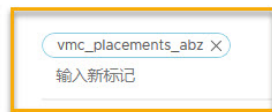


- 5 如上面的区域 2 中所示，添加标记名称 `vmc_placements_abz`。

标记

已选择 1 个对象

添加标记



移除标记

无标记 ①

- 6 通过在 **筛选标记** 部分中输入 `vmc_placements_abz` 来筛选在此云区域中使用的计算资源。

- 7 单击 **保存**。

名称	帐户/区域	类型	标记
<input type="checkbox"/> ComputeCluster A	LK-TEST 测试表为 A 中 E+ 部署 U8aU/H / NSX62-Scale-DC	common.title cluster	Cluster: ComputeClusterA
<input checked="" type="checkbox"/> ComputeCluster A-New	nsx-v 测试表为 A 中 E+ 部署 U8aU/H / NSX621-DataCenter	common.title cluster	ComputeClusterA
<input type="checkbox"/> ComputeCluster A / Scale	270_VC_account 测试表为 A 中 E+ 部署 U8aU/H / NSX62-Scale-DC	ResourcePool	ComputeClusterA

对于此示例，只有名为 `Cluster 1/ Compute-ResourcePool` 的计算资源可供 CloudAdmin 用户使用。

## 后续步骤

为 vRealize Automation 中的 VMware Cloud on AWS 部署配置网络和存储配置文件。

## 为 vRealize Automation 中的 VMware Cloud on AWS 部署配置网络和存储配置文件

在此步骤中，您将配置网络配置文件和存储配置文件，以便指定可供 vRealize Automation 中的 VMware Cloud on AWS CloudAdmin 用户使用的资源。

虽然还需要映像和特定实例值，但是它们对于 VMware Cloud on AWS 用户凭据没有任何独特之处。对于此示例，在定义云模板时，您将使用特定实例值 `small1` 和映像值 `ubuntu-16`。

有关映射和配置文件的一般信息，请参见第 4 章 [构建您的 vRealize Automation Cloud Assembly 资源基础架构](#)。

除非另有说明，否则在此过程中输入的步骤值仅适用于此示例工作流。

## 前提条件

- 创建云区域。请参见为 vRealize Automation 中的 VMware Cloud on AWS 部署创建云区域。
- 此过程假设您具有所需的管理员凭据，包括 vCenter 中目标 SDDC 的 VMware Cloud on AWS CloudAdmin 凭据。请参见在 vRealize Automation 中使用云帐户所需的凭据。
- 此过程假设您具有云管理员用户角色。请参见 vRealize Automation 用户角色是什么。

## 步骤

1 为 VMware Cloud on AWS 部署定义网络配置文件。

a 选择**基础架构 > 配置 > 网络配置文件**，然后单击**新建网络配置文件**。

设置	示例值
帐户/区域	OurCo-VMC / Datacenter:Datacenter-abz  <b>注</b> 选择在 在 vRealize Automation 的示例工作流程中创建 <b>VMware Cloud on AWS</b> 云帐户 中创建的 VMware Cloud on AWS 云帐户及其匹配的 SDDC 数据中心。
名称	vmc-network1
说明	包含拥有 VMware Cloud on AWS CloudAdmin 凭据的云模板管理员可以访问的网络。

b 单击**网络**选项卡，然后单击**添加网络**。

c 选择拥有 CloudAdmin 凭据的 VMware Cloud on AWS 用户可以部署到的网络，例如 sddc-cgw-network-1。

添加网络



<input type="checkbox"/>	名称	帐户/区域	区域	网络ID
<input checked="" type="checkbox"/>	ESO_PKS_VC01_VM_PKS	1114VCあア7中表読@肇 木 (EéÜ8äãæðeoäü#fiUse / ESO_PKS_VC01_DC01)		ESO_PKS_VC01_DVS01
<input type="checkbox"/>	ESO_PKS_VC01_Mgmt	1114VCあア7中表読@肇 木 (EéÜ8äãæðeoäü#fiUse / ESO_PKS_VC01_DC01)		ESO_PKS_VC01_DVS01

2 保存网络配置文件。

### 3 为 VMware Cloud on AWS 部署定义存储配置文件。

针对 CloudAdmin 用户可访问的数据存储/集群配置一个存储配置文件。

- a 选择**基础架构 > 配置 > 存储配置文件**，然后单击**新建存储配置文件**。

设置	示例值
帐户/区域	OurCo-VMC / Datacenter:Datacenter-abz 选择在 <a href="#">vRealize Automation</a> 的示例工作流程中创建 <b>VMware Cloud on AWS</b> 云帐户 中创建的 VMware Cloud on AWS 云帐户及其匹配的 SDDC 数据中心。
名称	vmc-storage1
说明	包含拥有 VMware Cloud on AWS CloudAdmin 凭据的云模板管理员可以部署到的数据存储集群。

- b 从**数据存储/集群**下拉菜单中，选择 **WorkloadDatastore** 数据存储。



对于 vRealize Automation Cloud Assembly 中的 VMware Cloud on AWS，存储策略必须使用 **WorkloadDatastore** 数据存储来支持 VMware Cloud on AWS 部署。

### 4 保存存储配置文件。

#### 后续步骤

在 [vRealize Automation](#) 中创建一个项目以支持 VMware Cloud on AWS 部署。

### 在 vRealize Automation 中创建一个项目以支持 VMware Cloud on AWS 部署

在此步骤中，您将定义一个 vRealize Automation 项目，该项目可用于控制 VMware Cloud on AWS 部署可用的资源。

有关项目的信息，请参见 [vRealize Automation Cloud Assembly](#) 项目在部署时的工作方式。

除非另有说明，否则在此过程中输入的步骤值仅适用于此示例工作流程。

#### 前提条件

- 完成为 [vRealize Automation](#) 中的 **VMware Cloud on AWS** 部署配置网络和存储配置文件过程。
- 此过程假设您具有所需的管理员凭据，包括 vCenter 中目标 SDDC 的 **VMware Cloud on AWS CloudAdmin** 凭据。请参见在 [vRealize Automation](#) 中使用云帐户所需的凭据。
- 此过程假设您具有云管理员用户角色。请参见 [vRealize Automation](#) 用户角色是什么。

#### 步骤

- 1 选择**基础架构 > 管理 > 项目**。
- 2 单击**新建项目**，然后输入项目名称 `VMC_proj-1_abz`。

**3 单击用户，然后单击添加用户。**

用户需要 CloudAdmin 凭据，才能访问其组织的 VMware Cloud on AWS 订阅。

- chris.gray@ourco.com，管理员
- kerry.white@ourco.com，成员

**4 单击置备，然后单击添加云区域。****5 添加在前面的步骤中配置的云区域。**

设置	示例值
云区域	VMC_cloud_zone-1 您在前面的步骤（为 vRealize Automation 中的 VMware Cloud on AWS 部署创建云区域）中创建了此云区域。
置备优先级	1
实例限制	3

**6 对于此示例，请忽略其他选项。****后续步骤**

创建要在 VMware Cloud on AWS 环境中部署的云模板。请参见在云模板设计中定义 vCenter 计算机资源以支持 vRealize Automation 中的 VMware Cloud on AWS 部署。

## 在云模板设计中定义 vCenter 计算机资源以支持 vRealize Automation 中的 VMware Cloud on AWS 部署

在此步骤中，您将 vCenter 计算机资源拖动到设计画布上，并为 vRealize Automation 中的 VMware Cloud on AWS 部署添加设置。

创建一个可以将其部署到可用 VMware Cloud on AWS 资源的云模板设计。

除非另有说明，否则在此过程中输入的步骤值仅适用于此示例工作流。

**前提条件**

- 此过程假定您拥有云模板设计人员凭据。请参见 vRealize Automation 用户角色是什么。
- 此过程假定您拥有 vCenter 中目标 SDDC (Datacenter:Datacenter-abz) 的 VMware Cloud on AWS CloudAdmin 凭据。请参见在 vRealize Automation 中使用云帐户所需的凭据。
- 按照前几节所述，配置资源基础架构和项目。

## 步骤

- 1 单击**设计**选项卡，然后单击**新建**。

设置	示例值
名称	vmc-bp_abz
说明	1
项目	VMC_proj-1_abz 这是之前创建的项目，可支持您之前创建的云区域。该项目现在与云区域相关联，而云区域又与您之前创建的 VMware Cloud on AWS 云帐户/区域相关联。

- 2 将 vSphere 计算机资源拖动到画布上。
- 3 编辑计算机资源中的以下（**粗体**）云模板资源代码。

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

image 可以是适合您的部署需求的任何值。

您必须将 `folderName: Workloads` 语句添加到云模板设计代码中才能支持 VMware Cloud on AWS 部署。`folderName: Workloads` 设置支持 VMware Cloud on AWS SDDC 环境中的 CloudAdmin 凭据，因此为必需项。

注意：虽然上述代码示例中显示的 `folderName: Workloads` 设置为必需项，但可以直接在云模板设计代码中添加该设置（如上所示），也可以在关联的云区域或项目中添加。如果在这三个位置中的多个位置指定了该设置，则优先级如下所示：

- 项目设置覆盖云模板设计设置和云区域设置。
- 云模板设置覆盖云区域设置。

注意：您可以选择将 `cpuCount` 和 `totalMemoryMB` 设置替换为 `flavor`（调整大小）条目，如下所示：

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

```
properties:
  image: ubuntu-1604
  flavor: small
  folderName: Workloads
```

如果云区域的文件夹值设置为 **Workloads**，则无需在云模板设计中设置 `folderName` 属性，除非您要替代云区域的文件夹值。

## 后续步骤

通过添加网络隔离，扩展此基本 VMware Cloud on AWS 工作流。请参见在 [vRealize Automation 的 VMware Cloud on AWS 工作流中配置隔离网络](#)。

## 在 vRealize Automation 的 VMware Cloud on AWS 工作流中配置隔离网络

在此过程中，您将在 vRealize Automation 中为 VMware Cloud on AWS 部署添加一个隔离网络。

定义您的 VMware Cloud on AWS 云帐户时，可以使用您在 VMware Cloud on AWS 服务中配置的 NSX-T 设置。有关在 VMware Cloud on AWS 服务中配置 NSX-T 设置的信息，请参见 [VMware Cloud on AWS 产品文档](#)。

vRealize Automation 支持带有 NSX-T 的 VMware Cloud on AWS。它不支持带有 NSX-V 的 VMware Cloud on AWS。

vRealize Automation 支持 VMware Cloud on AWS 部署的网络隔离。它不支持 VMware Cloud on AWS 的其他网络方法。

基本 VMware Cloud on AWS 工作流的这一扩展描述了以下创建隔离网络供在云模板中使用的方法：

- 配置基于网络的按需隔离。
- 配置基于安全组的按需隔离。

## 前提条件

此过程将扩展基本 VMware Cloud on AWS 工作流。它使用与您在 [教程：为 vRealize Automation 配置 VMware Cloud on AWS](#) 工作流中配置的相同云帐户和区域、云区域、项目和网络配置文件。

## 步骤

### 1 在 vRealize Automation 中为 VMware Cloud on AWS 部署定义隔离网络

可以使用以下任一过程为 VMware Cloud on AWS 部署配置网络隔离：

### 2 在 vRealize Automation 云模板中定义网络组件以对 VMware Cloud on AWS 支持网络隔离

在此步骤中，您将网络计算机组件拖动到 vRealize Automation 云模板画布上，并将隔离网络部署的设置添加到目标 VMware Cloud on AWS 环境中。

## 在 vRealize Automation 中为 VMware Cloud on AWS 部署定义隔离网络

可以使用以下任一过程为 VMware Cloud on AWS 部署配置网络隔离：

- 在 vRealize Automation 中配置基于按需网络的隔离



## ■ 在 vRealize Automation 中配置基于按需安全组的隔离

### 在 vRealize Automation 中配置基于按需网络的隔离

通过网络配置文件中指定和使用按需网络设置，您可以根据 VMware Cloud on AWS 部署需求配置网络隔离。

您可以使用安全组或按需网络设置来指定隔离网络。在此示例中，您可以通过在网络配置文件中指定按需网络设置来配置网络隔离。稍后，您可以在云模板中访问网络，并在 VMware Cloud on AWS 部署中使用该云模板。

除非另有说明，否则在此过程中输入的步骤值仅适用于此示例工作流。

#### 前提条件

- 完成在 vRealize Automation 中配置基本 VMware Cloud on AWS 工作流工作流。
- 请参见在 vRealize Automation 的 VMware Cloud on AWS 工作流中配置隔离网络。
- 此过程假设您具有所需的管理员凭据，包括 vCenter 中目标 SDDC 的 VMware Cloud on AWS CloudAdmin 凭据。请参见在 vRealize Automation 中使用云帐户所需的凭据。
- 此过程假设您具有云管理员用户角色。请参见 vRealize Automation 用户角色是什么。

#### 步骤

- 1 打开在基本 VMware Cloud on AWS 工作流中使用的网络配置文件，例如 vmc-network1。请参见为 vRealize Automation 中的 VMware Cloud on AWS 部署配置网络和存储配置文件。
- 2 您不需要在**网络**选项卡上进行任何选择。
- 3 单击**网络策略**选项卡。
- 4 选择**创建按需网络**选项，然后选择默认的 cgw 网络域。指定适当的 CIDR 和子网大小。
- 5 单击**保存**。

使用此网络配置文件时，计算机将部署到默认网络域中的网络。通过使用专用或出站网络访问，将该网络与其他网络隔离。

#### 后续步骤

在云模板中配置网络组件。请参见在 vRealize Automation 云模板中定义网络组件以对 VMware Cloud on AWS 支持网络隔离

### 在 vRealize Automation 中配置基于按需安全组的隔离

通过网络配置文件中指定和使用按需安全组，您可以根据 VMware Cloud on AWS 部署需求配置网络隔离。

您可以使用安全组或按需网络设置来指定隔离网络。在此示例中，您可以通过在网络配置文件中指定按需安全组来配置网络隔离。稍后，您可以在云模板中指定网络，并在 VMware Cloud on AWS 部署中使用该云模板。

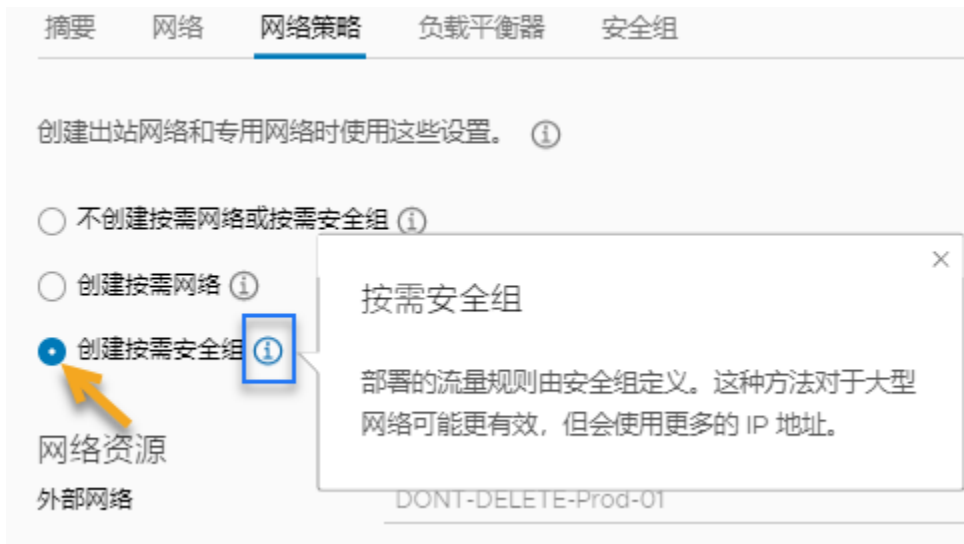
除非另有说明，否则在此过程中输入的步骤值仅适用于此示例工作流。

## 前提条件

- 完成在 vRealize Automation 中配置基本 VMware Cloud on AWS 工作流工作流。
- 请参见在 vRealize Automation 的 VMware Cloud on AWS 工作流中配置隔离网络。
- 此过程假设您具有所需的管理员凭据，包括 vCenter 中目标 SDDC 的 VMware Cloud on AWS CloudAdmin 凭据。请参见在 vRealize Automation 中使用云帐户所需的凭据。
- 此过程假设您具有云管理员用户角色。请参见 vRealize Automation 用户角色是什么。

## 步骤

- 1 打开在基本 VMware Cloud on AWS 工作流中使用的网络配置文件，例如 vmc-network1。请参见为 vRealize Automation 中的 VMware Cloud on AWS 部署配置网络和存储配置文件。
- 2 选择在基本 VMware Cloud on AWS 工作流中使用的现有网络，例如 sddc-cgw-network-1。请参见为 vRealize Automation 中的 VMware Cloud on AWS 部署配置网络和存储配置文件。
- 3 单击**网络策略**选项卡。
- 4 选择**创建按需安全组**选项。



- 5 单击**保存**。

使用此网络配置文件时，计算机将部署到选定的网络，并由新的安全组策略进行隔离。新的安全策略允许专用或出站网络访问。

## 后续步骤

在云模板中配置网络组件。请参见在 vRealize Automation 云模板中定义网络组件以对 VMware Cloud on AWS 支持网络隔离

## 在 vRealize Automation 云模板中定义网络组件以对 VMware Cloud on AWS 支持网络隔离

在此步骤中，您将网络计算机组件拖动到 vRealize Automation 云模板画布上，并将隔离网络部署的设置添加到目标 VMware Cloud on AWS 环境中。

将网络隔离添加到您之前创建的云模板中。该云模板已经与支持部署到您的 VMware Cloud on AWS 环境的项目和云区域以及您为隔离配置的网络配置文件和网络相关联。

除非另有说明，否则在此过程中输入的步骤值仅适用于此示例工作流。

### 前提条件

- 完成在 [vRealize Automation](#) 中配置基于按需安全组的隔离或在 [vRealize Automation](#) 中配置基于按需网络的隔离过程。
- 此过程假定您拥有云模板设计人员凭据。请参见 [vRealize Automation 用户角色是什么](#)。
- 此过程假定您拥有适用于 vCenter 中的目标 SDDC 的 VMware Cloud on AWS CloudAdmin 凭据。请参见在 [vRealize Automation](#) 中使用云帐户所需的凭据。

### 步骤

- 1 打开您在上一个工作流中创建的云模板。请参见在云模板设计中定义 [vCenter](#) 计算机资源以支持 [vRealize Automation](#) 中的 [VMware Cloud on AWS](#) 部署。
- 2 从云模板设计页面左侧的组件中，将网络组件拖动到画布上。
- 3 编辑网络组件 YAML 代码以指定网络类型 `private` 或 `outbound`，如粗体所示。

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

或

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

### 后续步骤

您已准备好部署或关闭云模板。

## 教程：为 vRealize Automation 配置提供程序特定的外部 IPAM 集成

您可以使用外部 IPAM 提供程序管理云模板部署的 IP 地址分配。本教程介绍如何在 vRealize Automation 中使用 Infoblox 作为外部 IPAM 提供程序来配置外部 IPAM 集成。

在此过程中，将使用现有 IPAM 提供程序软件包（在本例中为 Infoblox 软件包）和现有运行环境构建提供程序特定的 IPAM 集成点。将配置现有网络并创建网络配置文件，以支持从外部 IPAM 提供程序分配 IP 地址。最后，将创建与网络和网络配置文件匹配的云模板，并使用从外部 IPAM 提供程序获取的 IP 值部署联网计算机。

有关如何获取和配置 IPAM 提供程序软件包的信息以及如何配置访问云可扩展性代理的运行环境以支持 IPAM 提供程序集成的信息，作为参考信息包括在内。

请记住，显示的值为例值。不能在您的环境中逐字使用这些值。请考虑在何处替换为您自己的值或根据示例值进行推断，以满足您组织的需求。



要参考使用了 Infoblox IPAM 集成工作流的类似 vRealize Automation 场景的视频，请参见 [Infoblox IPAM 插件 1.1 与 vRealize Automation 8.1/vRealize Automation Cloud 集成](#)。

### 步骤

#### 1 在 Infoblox 应用程序中添加所需的可扩展属性以与 vRealize Automation 集成

您必须先要在 Infoblox 中添加所需的可扩展性属性，然后才能从 Infoblox 网站或 VMware Marketplace 下载 Infoblox 提供程序软件包 (infoblox.zip)，并进行部署以与 vRealize Automation 集成。

#### 2 下载并部署外部 IPAM 提供程序软件包以在 vRealize Automation 中使用

在 vRealize Automation 中定义外部 IPAM 集成点之前，您需要一个已配置的 IPAM 提供程序软件包。

#### 3 在 vRealize Automation 中为 IPAM 集成点创建运行环境

在 vRealize Automation 中定义外部 IPAM 集成点之前，需要创建或访问现有的运行环境以作为 IPAM 提供程序和 vRealize Automation 之间的中介。运行环境通常是 Amazon Web Services 或 Microsoft Azure 云帐户，或与云可扩展性代理相关联的基于操作的可扩展性内部部署集成点。

#### 4 在 vRealize Automation 中为 Infoblox 添加外部 IPAM 集成

vRealize Automation 支持与外部 IPAM 提供程序集成。此示例使用 Infoblox 作为外部 IPAM 提供程序。

#### 5 在 vRealize Automation 中配置网络和网络配置文件，以对现有网络使用外部 IPAM

可以将现有网络定义为使用从外部 IPAM 提供程序（而不是从 vRealize Automation 内部）获取并由其管理的 IP 地址值。

#### 6 在 vRealize Automation 中定义并部署使用外部 IPAM 提供程序范围分配的云模板

可以将云模板定义为从外部 IPAM 提供程序获取 IP 地址分配并进行管理。此示例使用 Infoblox 作为外部 IPAM 提供程序。

## 7 对 vRealize Automation 中的 IPAM 集成使用特定于 Infoblox 的属性和可扩展属性

对于包含 Infoblox 的外部 IPAM 集成的 vRealize Automation 项目，可以使用特定于 Infoblox 的属性。

## 在 Infoblox 应用程序中添加所需的可扩展属性以与 vRealize Automation 集成

您必须先添加所需的可扩展属性，然后才能从 Infoblox 网站或 VMware Marketplace 下载 Infoblox 提供程序软件包 (infoblox.zip)，并进行部署以与 vRealize Automation 集成。

如果要为 Infoblox 与 vRealize Automation Cloud Assembly 集成创建外部 IPAM 集成点时，则此过程适用。

您必须使用您组织帐户的管理员凭据登录到 Infoblox 帐户，并预创建以下 Infoblox 可扩展属性，然后才能使用下载的 infoblox.zip：

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

### 前提条件

- 确认您拥有 [Infoblox](#) 帐户，并且拥有对组织 Infoblox 帐户的正确访问凭据。
- 确认 Infoblox WAPI 版本受支持。IPAM 与 Infoblox 的集成依赖于 Infoblox WAPI 版本 2.7。支持 WAPI v2.7 的所有 Infoblox 设备均受支持。
- 查看对 [vRealize Automation 中的 IPAM 集成使用特定于 Infoblox 的属性和可扩展属性](#)。

### 步骤

- 1 使用管理员凭据登录到 Infoblox 帐户。

这些凭据是您在 vRealize Automation Cloud Assembly 中使用 **基础架构 > 连接 > 集成 >** 菜单顺序创建外部 IPAM 集成点时指定的管理员用户名和密码凭据。

- 2 按照 Infoblox 文档中所述的过程在 Infoblox 应用程序中创建所需的以下可扩展属性。

- VMware NIC index - 整数类型
- VMware resource ID - 字符串类型
- Tenant ID - 字符串类型
- CMP Type - 字符串类型
- VM ID - 字符串类型

- VM Name - 字符串类型

Infoblox 文档主题[关于可扩展属性](#)中的添加可扩展属性部分介绍了此过程。另请参见[管理可扩展属性](#)。

### 后续步骤

添加所需的属性后，可以按照 [下载并部署外部 IPAM 提供程序软件包](#) 以在 vRealize Automation 中使用中所述继续执行下载和部署 Infoblox 软件包的过程。

## 下载并部署外部 IPAM 提供程序软件包以在 vRealize Automation 中使用

在 vRealize Automation 中定义外部 IPAM 集成点之前，您需要一个已配置的 IPAM 提供程序软件包。

可以从以下位置下载提供程序特定的集成软件包：IPAM 提供程序的网站、[VMware Solution Exchange 商城](#)或者 vRealize Automation 的[商城](#)选项卡（如果可用）。

---

**注** 此示例使用 VMware 提供的 Infoblox 软件包 `Infoblox.zip`，该软件包可从 [VMware Marketplace](#) 下载，如下所示：

- [vRA Cloud Infoblox 插件版本 1.2](#) - 与 vRealize Automation 8.1.x 和 8.2.x 兼容
- [vRA Cloud Infoblox 插件版本 1.1](#) - 与 vRealize Automation 8.1.x 兼容
- [vRA Cloud Infoblox 插件版本 1.0](#) - 与 vRealize Automation 8.0.1.x 兼容，无论是否通过 Internet 连接到全球网络。
- [vRA Cloud Infoblox 插件版本 0.4](#) - 通过 Internet 连接到全球网络时与 vRealize Automation 8.0.0.x 和 8.0.1.x 兼容。

IPAM 与 Infoblox 的集成依赖于 Infoblox WAPI 版本 2.7。支持 WAPI v2.7 的所有 Infoblox 设备均受支持。

---

有关如何为其他 IPAM 提供程序创建 IPAM 集成软件包的信息（如果商场中尚不存在该软件包），请参见[如何使用 IPAM SDK 为 vRealize Automation 创建提供程序特定的外部 IPAM 集成软件包](#)。

IPAM 提供程序软件包包含与元数据和其他配置一起打包的脚本。这些脚本包含与外部 IPAM 提供程序协调时 vRealize Automation 执行的操作所使用的源代码。示例操作包括 Allocate an IP address for a virtual machine、Fetch a list of IP ranges from the provider 和 Update the MAC address of a host record in the provider。

### 前提条件

- 确认您具有云管理员凭据。请参见在 [vRealize Automation 中使用云帐户](#) 所需的凭据。
- 确认您具有云管理员用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 确认您具有外部 IPAM 提供程序（例如 [Infoblox](#) 或 [Bluecat](#)）的帐户，并且具有使用 IPAM 提供程序访问组织帐户的正确访问凭据。

- 如果您要使用 Infoblox 作为外部 IPAM 提供程序，请确认已将所需的可扩展属性添加到 Infoblox 帐户，然后再继续操作。请参见在 [Infoblox 应用程序中添加所需的可扩展属性以与 vRealize Automation 集成](#)。

**注** 存在一个证书链问题，该问题由 Infoblox 插件中的 Python 元素处理 SSL 握手的方式所致。有关该问题及其所需操作的信息，请参见知识库文章 [vRA Cloud Infoblox 插件在身份验证过程中引发证书链错误 \(88057\)](#)。

## 步骤

- 1 在 [VMware Marketplace](#) 中导航到 [vRA Cloud Infoblox 插件版本 1.1](#) 软件包页面。
- 2 登录并下载插件软件包。
- 3 如果尚未执行此操作，请在 Infoblox 中添加所需的可扩展性属性。请参见在 [Infoblox 应用程序中添加所需的可扩展属性以与 vRealize Automation 集成](#)。

## 结果

现在，可以使用 **集成 > 添加集成 > IPAM > 管理提供程序 > 导入软件包** 菜单序列，对此软件包进行部署，如在 [vRealize Automation 中为 Infoblox 添加外部 IPAM 集成](#) 中所述。

## 在 vRealize Automation 中为 IPAM 集成点创建运行环境

在 vRealize Automation 中定义外部 IPAM 集成点之前，需要创建或访问现有的运行环境以作为 IPAM 提供程序和 vRealize Automation 之间的中介。运行环境通常是 Amazon Web Services 或 Microsoft Azure 云帐户，或与云可扩展性代理相关联的基于操作的可扩展性内部部署集成点。

外部 IPAM 集成需要运行环境。定义 IPAM 集成点时，通过指定可用运行环境在 vRealize Automation Cloud Assembly 和 IPAM 提供程序之间创建连接。

在功能即服务 (FaaS) 提供程序（如 Amazon Web Services Lambda、Microsoft Azure Functions 或基于操作的可扩展性 (ABX) 内部部署嵌入式集成点）助力的运行环境中，IPAM 集成使用一组已下载的提供程序特定脚本或插件。运行环境用于连接到外部 IPAM 提供程序，例如 Infoblox。

**注** Infoblox IPAM 集成点需要一个基于操作的可扩展性 (ABX) 内部部署嵌入式集成点。

每种类型的运行时环境都有优缺点：

- 基于操作的可扩展性 (ABX) 集成点
  - 免费，无其他供应商使用成本
  - 可以连接到位于不能公开访问的 NAT/Firewall 后面的内部部署数据中心内的 IPAM 供应商设备，例如 Infoblox
  - 与商业云供应商相比，速度慢且性能可靠性稍差
- Amazon Web Services
  - 有相关的供应商 FaaS 连接/使用成本
  - 无法连接到位于不能公开访问的 NAT/Firewall 后面的内部部署数据中心内的 IPAM 供应商设备



- 快速且性能高度可靠
- Microsoft Azure
  - 有相关的供应商 FaaS 连接/使用成本
  - 无法连接到位于不能公开访问的 NAT/Firewall 后面的内部部署数据中心内的 IPAM 供应商设备
  - 快速且性能高度可靠

#### 前提条件

- 确认您具有云管理员凭据。请参见在 [vRealize Automation 中使用云帐户所需的凭据](#)。
- 确认您具有云管理员用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 确认您具有外部 IPAM 提供程序（例如 [Infoblox](#) 或 [Bluecat](#)）的帐户，并且具有使用 IPAM 提供程序访问组织帐户的正确访问凭据。
- 确认您有权访问 IPAM 提供程序（例如 [Infoblox](#) 或 [BlueCat](#)）的已部署集成软件包。部署的软件包最初从 IPAM 提供程序网站或 vRealize Automation Cloud Assembly 商城以 .zip 形式下载，然后部署到 vRealize Automation Cloud Assembly。

有关如何部署提供程序软件包 .zip 文件并使其在“IPAM 集成”页面上可作为提供程序值提供的信息，请参见 [下载并部署外部 IPAM 提供程序软件包以在 vRealize Automation 中使用](#)。

#### 步骤

- 1 要创建一个基于 FaaS 的内部部署可扩展性操作以用作 IPAM 集成运行环境，请选择 **可扩展性 > 库 > 操作**。
- 2 单击 **新建操作**，输入操作名称和描述，然后指定项目。
- 3 在 **FaaS 提供程序** 下拉菜单中，选择 **内部部署**。
- 4 填写表单以定义可扩展性操作。



有关运行环境的相关信息，请参见在视频中播插的此 [Infoblox IPAM 插件 1.1 集成](#) 博客视频（约 24 分钟）。

## 在 vRealize Automation 中为 Infoblox 添加外部 IPAM 集成

vRealize Automation 支持与外部 IPAM 提供程序集成。此示例使用 Infoblox 作为外部 IPAM 提供程序。可以使用提供程序特定的 IPAM 集成点获取并管理云模板部署的 IP 地址和相关网络特性。

在此示例中，您将创建一个外部 IPAM 集成点，以支持使用外部 IPAM 提供程序访问组织的帐户。在此示例工作流程中，IPAM 提供程序为 Infoblox，且提供程序特定的集成软件包已存在。虽然这些说明特定于 Infoblox 集成，但在为不同的外部 IPAM 提供程序创建 IPAM 集成时，也可以将其用作参考。

可以从以下位置获取提供程序特定的集成软件包：IPAM 提供程序的网站、[VMware Solution Exchange 商城](#)或者 vRealize Automation Cloud Assembly 的 [商城](#) 选项卡（如果可用）。



此示例使用 VMware 提供的 Infoblox 软件包 `Infoblox.zip`，该软件包可从 VMware Solution Exchange 商城以如下形式进行下载：

- [vRA Cloud Infoblox 插件版本 1.1](#) - 支持 vRealize Automation 8.1 及更高版本
- [vRA Cloud Infoblox 插件版本 1.0](#) - 支持 vRealize Automation 8.0.1
- [vRA Cloud Infoblox 插件版本 0.1](#) - 支持 vRealize Automation 8.0

#### 前提条件

- 确认您具有云管理员凭据。请参见在 [vRealize Automation](#) 中使用云帐户所需的凭据。
- 确认您具有云管理员用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 确认您具有外部 IPAM 提供程序的帐户，并且具有使用 IPAM 提供程序访问组织帐户的正确访问凭据。
- 确认您有权访问 IPAM 提供程序的已部署集成软件包。部署的软件包最初从 IPAM 提供程序网站或 VMware Solution Exchange 商城以 .zip 形式下载，然后部署到 vRealize Automation。  
有关如何下载和部署提供程序软件包 .zip 文件并使其在“IPAM 集成”页面上可作为提供程序值提供的信息，请参见 [下载并部署外部 IPAM 提供程序软件包以在 vRealize Automation 中使用](#)。
- 确认您有权访问为 IPAM 提供程序配置的运行环境。运行环境通常是一个基于操作的可扩展性 (ABX) 内部部署嵌入式集成点。  
有关运行环境特性的信息，请参见在 [vRealize Automation](#) 中为 IPAM 集成点创建运行环境。
- 在 Infoblox 应用程序中启用所需的可扩展属性。请参见在 [Infoblox 应用程序中添加所需的可扩展属性以与 vRealize Automation 集成](#)。
- 如果您没有外部 Internet 访问权限，则可以配置一个 Internet 服务器代理。请参见 [如何配置 vRealize Automation 的 Internet 代理服务器](#)。
- 确认您具有访问和使用 Infoblox IPAM 产品所需的用户凭据。例如，在 Infoblox 设备中打开“管理”选项卡，然后自定义管理员、组和角色条目。您必须是具有管理员或超级用户权限的组的成员，或者是具有 DHCP、DNS、IPAM 和网格权限的自定义组的成员。这些设置允许访问 Infoblox 插件中提供的所有功能，从而您能够创建 Infoblox IPAM 集成和设计器，以便在云模板和部署中使用该 IPAM 集成。有关用户权限的详细信息，请参见您的 Infoblox 产品文档。

#### 步骤

- 1 选择 **基础架构 > 连接 > 集成**，然后单击 **添加集成**。
- 2 单击 **IPAM**。
- 3 在 **提供程序** 下拉列表中，从列表中选择已配置的 IPAM 提供程序软件包，例如 `Infoblox_hrg`。

如果此列表为空，请单击 **导入提供程序软件包**，导航到现有提供程序软件包 .zip 文件，然后选择该文件。如果没有此提供程序 .zip 文件，则可以从 IPAM 提供程序的网站或从 vRealize Automation Cloud Assembly 的 **商城** 选项卡获取该文件。

有关如何在 vCenter 中部署提供程序软件包 .zip 文件并使其在“集成”页面上作为提供程序值提供的信息，请参见 [下载并部署外部 IPAM 提供程序软件包以在 vRealize Automation 中使用](#)。

有关如何升级现有 IPAM 集成以使用最新版本的供应商 IPAM 集成软件包的信息，请参见[如何在 vRealize Automation 中升级到较新的外部 IPAM 集成软件包](#)。

- 4 输入具有外部 IPAM 提供程序的帐户的管理员用户名和密码凭据以及所有其他（如果有）必填字段，如提供程序的主机名。

在此示例中，您将通过以下步骤获取 Infoblox IPAM 提供程序的主机名：

- a 在单独的浏览器选项卡中，使用您的 Infoblox 管理员凭据登录到 IPAM 提供程序帐户。
- b 复制主机名 URL。
- c 将您的主机名 URL 粘贴到“IPAM 集成”页面上的**主机名字段**中。

- 5 在**运行环境**下拉列表中，选择一个现有基于操作的可扩展性内部部署集成点，例如 *Infoblox\_abx\_intg*。

运行环境支持在 vRealize Automation 和外部 IPAM 提供程序之间进行通信。

---

**注** 如果使用 Amazon Web Services 或 Microsoft Azure 云帐户作为集成运行环境，请确保 IPAM 提供程序设备符合以下条件：可以通过 Internet 进行访问，不位于 NAT 或防火墙后面，并且具有可公开解析的 DNS 名称。如果 IPAM 提供程序不可访问，则 Amazon Web Services Lambda 或 Microsoft Azure 函数无法与其相连接，集成将失败。有关相关信息，请参见在 [vRealize Automation 中为 IPAM 集成点创建运行环境](#)。

---

IPAM 框架仅支持基于操作的可扩展性 (ABX) 内部部署嵌入式运行环境。

---

**注** Infoblox IPAM 集成点需要一个基于操作的可扩展性 (ABX) 内部部署嵌入式集成点。

---

配置的云帐户或集成点允许在 vRealize Automation 和 IPAM 提供程序之间进行通信，在此示例 Infoblox 中通过关联的云可扩展性代理进行。可以选择已创建的提供程序，也可以创建一个提供程序。

有关如何创建运行环境的信息，请参见在 [vRealize Automation 中为 IPAM 集成点创建运行环境](#)。

- 6 单击**验证**。

由于此示例对运行环境使用基于内部部署操作的可扩展性集成，因此可以查看验证操作。

- a 单击**可扩展性**选项卡。
- b 单击**活动 > 操作运行**，然后从筛选器中选择**所有运行**或**集成运行**，以查看端点验证操作是否已启动且正在运行。

- 7 当系统提示您信任来自 IPAM 提供程序的自签名证书时，单击**接受**。

接受自签名证书后，可以继续完成验证操作。

- 8 输入此 IPAM 集成点的**名称**（例如 *Infoblox\_Integration*）和**描述**（例如 *Infoblox IPAM with ABX integration for team HRG*）。

## 9 单击**添加**以保存新的外部 IPAM 集成点。

将模拟数据收集操作。将从 IPAM 提供程序收集网络 and IP 范围数据。可以按如下方式查看数据收集操作：

- a 单击**可扩展性**选项卡。
- b 单击**活动 > 操作运行**，并注意数据收集操作已启动且正在运行。可以打开并查看操作运行内容。

### 结果

提供程序特定的外部 IPAM 集成现在可用于网络和网络配置文件。

## 在 vRealize Automation 中配置网络和网络配置文件，以对现有网络使用外部 IPAM

可以将现有网络定义为使用从外部 IPAM 提供程序（而不是从 vRealize Automation 内部）获取并由其管理的 IP 地址值。

可以将网络定义为访问您在组织的外部 IPAM 提供程序帐户中定义的现有 IP 设置。此步骤将详述在上一步中创建的 Infoblox 提供程序集成。

在此示例中，将使用已从 vCenter 收集数据的现有网络配置网络配置文件。然后，将这些网络配置为从外部 IPAM 提供程序（在本例中为 Infoblox）获取 IP 信息。从 vRealize Automation 置备且可与此网络配置文件匹配的虚拟机从外部 IPAM 提供程序获取其 IP 以及其他与 TCP/IP 相关的设置。

有关网络的详细信息，请参见 [vRealize Automation 中的网络资源](#)。有关网络配置文件的详细信息，请参见 [如何在 vRealize Automation 中添加网络配置文件和了解有关 vRealize Automation 中的网络配置文件的更多信息](#)。

有关相关信息，请参见 [如何在 vRealize Automation 中配置网络配置文件以对外部 IPAM 集成支持按需网络](#)。

### 前提条件

此步骤顺序显示在 IPAM 提供程序集成工作流的上下文中。请参见教程：[为 vRealize Automation 配置提供程序特定的外部 IPAM 集成](#)。

- 确认您具有云管理员凭据。请参见在 [vRealize Automation 中使用云帐户所需的凭据](#)。
- 确认您具有云管理员用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 确认您具有外部 IPAM 提供程序（例如 Infoblox 或 Bluecat）的帐户，并且具有使用 IPAM 提供程序访问组织帐户的正确访问凭据。在此示例工作流中，IPAM 提供程序为 Infoblox。
- 确认您具有 IPAM 提供程序的 IPAM 集成点。请参见在 [vRealize Automation 中为 Infoblox 添加外部 IPAM 集成](#)。

### 步骤

- 1 要配置网络，请单击**基础架构 > 资源 > 网络**。

- 2 在**网络**选项卡上，选择要与 IPAM 提供程序集成点一起使用的现有网络。在此示例中，网络名称为 *net.23.117-only-IPAM*。

列出的网络已由 vRealize Automation 从组织中的 vCenter 进行数据收集。

- 3 要从外部 IPAM 提供程序获取值，请确认除**帐户/区域、名称和网络域**外，所有其他网络设置均为空，其中包括以下网络设置：

- 域（请参见步骤 8 中的“注意”）
- CIDR
- 默认网关
- DNS 服务器
- DNS 搜索域

- 4 单击 **IP 范围**选项卡，然后单击**添加 IPAM IP 范围**。

- 5 从**网络**菜单中，选择刚刚配置的网络，例如 *net.23.117-only-IPAM*。

- 6 从**提供程序**菜单中，选择在工作流的之前步骤中创建的 IPAM 集成点 *Infoblox\_Integration*

- 7 从现在可见的**地址空间**下拉菜单中，选择一个列出的网络视图。

Infoblox 中的地址空间称为网络视图。

网络视图从 IPAM 提供程序帐户获取。此示例使用刚刚配置的网络子网（例如 *net.23.117-only-IPAM*）、在工作流的之前步骤中创建的集成点 *Infoblox\_Integration*，以及名为 *default* 的地址空间。

列出的地址空间值从外部 IPAM 提供程序获取。

- 8 从可用于所选地址空间的已显示网络列表中，选择一个或多个网络，例如，选择 10.23.117.0/24。

对于此示例，选定网络的**域**和 **DNS 服务器**列值包含来自 Infoblox 的值。

---

**注** 如果在步骤 3 中选择的网络包含为 vRealize Automation 指定的“域”，然后从包含“域”值的外部 IPAM 提供程序地址空间选择一个网络，则外部 IPAM 提供程序网络中的“域”值优先于在 vRealize Automation 中指定的“域”。如果 IPAM IP 范围设置没有像上述那样在 Cloud Assembly 或外部 IPAM 提供程序中指定“域”值，置备将失败。

---

对于 Infoblox，可以在计算机级别使用 `Infoblox.IPAM.Network.dnsSuffix` 蓝图属性覆盖“域”值。有关相关信息，请参见[对 vRealize Automation 中的 IPAM 集成使用特定于 Infoblox 的属性和可扩展属性](#)。

- 9 单击**添加**以保存网络的 IPAM IP 范围。

范围在 **IP 范围**表中可见。

- 10 单击 **IP 地址**选项卡。

使用外部 IPAM 提供程序中的新地址范围置备计算机后，**IP 地址**表中将显示一条新记录。

- 11 要将网络配置文件配置为使用该网络，请单击**基础架构 > 配置 > 网络配置文件**。

12 为网络配置文件命名，例如 *Infoblox-NP*，然后添加以下示例设置。

- “摘要”选项卡
  - 指定 vSphere 云帐户/区域。
  - 为网络配置文件添加功能标记，例如，名为 *infoblox\_abx* 的标记。  
请记录功能标记，因为还必须将其用作云模板限制标记，才能在云模板中进行置备关联。
- “网络”选项卡
  - 添加之前创建的网络，例如 *net.23.117-only-IPAM*。

13 单击 **保存** 以保存包含这些设置的网络配置文件。

## 结果

现在，针对将用于云模板设计中 Infoblox IPAM 集成的现有网络类型的网络和网络配置文件设置的配置已经完成。

## 在 vRealize Automation 中定义并部署使用外部 IPAM 提供程序范围分配的云模板

可以将云模板定义为从外部 IPAM 提供程序获取 IP 地址分配并进行管理。此示例使用 Infoblox 作为外部 IPAM 提供程序。

这是外部 IPAM 集成工作流的最后一步，在此步骤中，将定义并部署云模板，用于将之前定义的网络和网络配置文件连接到您组织的 Infoblox 帐户，以从外部 IPAM 提供程序（而非 vRealize Automation Cloud Assembly）获取已部署虚拟机的 IP 地址分配并进行管理。

该工作流使用 Infoblox 作为外部 IPAM 提供程序，在某些步骤中，示例值为 Infoblox 所独有，但本意是该过程可应用于其他外部 IPAM 集成。



通过使用 VMware vRealize Automation 和 Infoblox DDI 自动对虚拟机执行 IPAM 和 DNS

Infoblox 博客提供了相关信息。

部署云模板并启动虚拟机后，用于部署中每个虚拟机的 IP 地址将在 **资源 > 网络** 页面中显示为一个网络条目，在 IPAM 提供程序帐户的 IPAM 提供程序网络以及主机 vCenter 中每个已部署虚拟机的 vSphere Web Client 记录中显示为一条新主机记录。

## 前提条件

外部 IPAM 提供程序集成工作流的上下文中显示了此步骤顺序。请参见教程：[为 vRealize Automation 配置提供程序特定的外部 IPAM 集成](#)。

- 确认您具有云管理员凭据。请参见在 [vRealize Automation 中使用云帐户所需的凭据](#)。
- 确认您具有云管理员用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 确认您具有外部 IPAM 提供程序（例如 Infoblox 或 BlueCat）的帐户，并且具有使用 IPAM 提供程序访问组织帐户的正确访问凭据。

- 确认您对主机帐户具有管理员访问权限，并满足在主机 vCenter 中已部署虚拟机的 vSphere Web Client 记录中显示状态记录所需的任何角色要求。
- 确认您具有外部 IPAM 提供程序的 IPAM 集成点。请参见在 [vRealize Automation](#) 中为 Infoblox 添加外部 IPAM 集成。
- 确认您已配置 vRealize Automation Cloud Assembly 网络和网络配置文件，以支持所需 IPAM 集成点的外部 IPAM 集成。请参见在 [vRealize Automation](#) 中配置网络和网络配置文件，以对现有网络使用外部 IPAM。
- 确认您的项目和云区域已添加标记，与 IPAM 集成点和网络或网络配置文件中的标记匹配。（可选）将项目配置为支持自定义资源命名。

有关项目和云区域的角色以及云模板中其他基础架构元素的角色详细信息，请参见 [教程：在 vRealize Automation Cloud Assembly 中设置和测试多云基础架构和部署](#)。有关标记的详细信息，请参见 [如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署](#)。

有关使用项目中的设置自定义命名虚拟机的信息，请参见 [如何使用 vRealize Automation Cloud Assembly 自定义已部署资源的名称](#)。

## 步骤

- 1 单击 **云模板 > 新建**，在 **新建云模板** 页面中输入以下信息，然后单击 **创建**。
  - 名称 = ipam-bpa
  - 描述 = Cloud template that uses Infoblox IPAM integration
  - 项目 = 123VC
- 2 对于此示例，将云平台无关的计算机组件和云平台无关的网络组件添加到云模板画布并连接这两个组件。
- 3 编辑云模板代码，以将限制标记添加到与您添加到网络配置文件的功能标记匹配的网络组件。对于此示例，该标记值为 *infoblox\_abx*。
- 4 编辑云模板代码，以指定网络分配类型为 *static*。

使用外部 IPAM 提供程序时，`assignment: static` 设置是必需项。

对于此示例，已知指定的 IP 地址 **10.23.117.4** 当前在为关联网络配置文件中的网络所选择的外部 IPAM 地址空间中可用。`assignment: static` 设置是必需项，而 `address: value` 设置不是。可以选择在某个特定地址值开始选择外部 IP 地址，但此操作不是必须执行。如果未指定 `address: value` 设置，外部 IPAM 提供程序将选择外部 IPAM 网络中的下一个可用地址。

- 5 根据以下示例验证云模板代码。

```
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}'

```

有关可用于在云模板中指定 DNS 和 DHCP 设置的 Infoblox 属性的示例，请参见对 [vRealize Automation](#) 中的 IPAM 集成使用特定于 Infoblox 的属性和可扩展属性。

- 6 单击云模板页面上的**部署**，将部署命名为 *Infoblox-1*，然后在**部署类型**页面上单击**部署**。
- 7 在部署云模板时，单击**可扩展性**选项卡，然后选择**活动 > 操作运行**，会看到 *Infoblox\_AllocateIP\_n* 可扩展性操作正在运行。

完成可扩展性操作并置备计算机后，*Infoblox\_Update\_n* 操作会将 MAC 地址传播到 Infoblox。

- 8 可以登录到 Infoblox 帐户并打开，以在关联的 10.23.117.0/24 网络中查看 IPAM 地址的新主机记录。还可以在 Infoblox 中打开“DNS”选项卡以查看新的 DNS 主机记录。
- 9 要验证是否正在置备虚拟机，请登录到主机 vCenter 和 vSphere Web Client，找到已置备的计算机并查看 DNS 名称和 IP 地址。

启动已置备的虚拟机后，MAC 地址将通过 *Infoblox\_AllocateIP* 可扩展性操作传播到 Infoblox。

- 10 要在 vRealize Automation Cloud Assembly 中查看新的网络记录，请选择**基础架构 > 资源 > 网络**，然后单击以打开 **IP 地址**选项卡。
- 11 如果删除部署，则会释放部署中虚拟机的 IPAM 地址，这些 IP 地址将再次供外部 IPAM 提供程序进行其他分配。vRealize Automation Cloud Assembly 中此事件的可扩展性操作为 *Infoblox\_Deallocate*。

## 对 vRealize Automation 中的 IPAM 集成使用特定于 Infoblox 的属性和可扩展属性

对于包含 Infoblox 的外部 IPAM 集成的 vRealize Automation 项目，可以使用特定于 Infoblox 的属性。

以下 Infoblox 属性可在云模板设计和部署中用于 Infoblox IPAM 集成。可以在 vRealize Automation 中使用这些属性，以便在云模板部署期间进一步控制 IP 地址的分配。这些属性的使用是可选的。

### ■ Infoblox.IPAM.createFixedAddress

此属性让您能够在 Infoblox 内创建固定地址记录。可能的值为 True 和 False。默认情况下，将创建主机记录。默认值为 False。

### ■ Infoblox.IPAM.Network.dnsView

通过此属性，您可以在 Infoblox 中创建主机记录时使用 DNS 视图。

- Infoblox.IPAM.Network.enableDns

在 Infoblox 中分配 IP 时，还可以使用此属性创建 DNS 记录。可能的值为 True 和 False。默认值为 True。

- Infoblox.IPAM.Network.enableDhcp

可以将此选项设置为 True，以便为主机地址启用 DHCP 配置。

- Infoblox.IPAM.Network.dnsSuffix

通过此属性，您可以将 Infoblox 网络的 *domain* DHCP 选项替换为新选项。如果 Infoblox 网络未设置 *domain* DHCP 选项，或者必须覆盖 *domain* DHCP 选项，此功能将非常有用。默认值为 Null（空字符串）。

只有在将 Infoblox.IPAM.Network.enableDns 设置为 True 时，Infoblox.IPAM.Network.dnsSuffix 才适用。

您可以在 vRealize Automation Cloud Assembly 中使用以下方法之一指定 Infoblox 属性：

- 您可以使用[基础架构 > 管理 > 项目](#)页面中的[自定义属性](#)部分指定项目属性。使用此方法时，指定的属性将应用于在此项目范围内置备的所有计算机。
- 您可以在云模板中的每个计算机组件上指定属性。下面的示例云模板代码介绍如何使用 Infoblox.IPAM.Network.dnsView 属性：

```
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
```

- 可以使用可扩展性订阅指定属性。

有关与此用例相关的 Infoblox 可扩展属性的相关信息，请参见在 [Infoblox 应用程序中添加所需的可扩展属性](#) 以与 [vRealize Automation 集成](#)。

## 在云模板中的不同计算机网卡上使用 Infoblox 属性

以下 Infoblox 属性针对云模板中的每个计算机网卡可具有不同的值：

- Infoblox.IPAM.Network.enableDhcp



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

例如，要对每个网卡使用不同的 Infoblox.IPAM.Network.dnsView 值，请对每个网卡使用一个 Infoblox.IPAM.Network<nicIndex>.dnsView 条目。以下示例显示两个网卡使用不同的 Infoblox.IPAM.Network.dnsView 值。

```
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
```

默认情况下，Infoblox 集成会在 Infoblox 的默认 DNS 视图中创建一条 DNS 主机记录。如果您的 Infoblox 管理员已创建自定义 DNS 视图，您可以覆盖默认集成行为，并使用计算机组件中的 Infoblox.IPAM.Network.dnsView 属性指定一个已命名的视图。例如，您可以将以下属性添加到 Cloud\_Machine\_1 组件，以在 Infoblox 中指定一个已命名的 DNS 视图。

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

有关配置和使用 DNS 视图的信息，请参见 Infoblox 产品文档中的 [DNS 视图](#)。有关 Infoblox 集成工作流程中的示例，请参见在 [vRealize Automation](#) 中定义并部署使用外部 IPAM 提供程序范围分配的云模板。

# 为您的组织设置 vRealize Automation Cloud Assembly

## 3

作为 Cloud Assembly 管理员，您必须了解用户角色，并设置与云帐户供应商和集成应用程序的连接。

当配置云帐户和集成时，您配置的是 Cloud Assembly 与这些目标系统之间的通信。

本章讨论了以下主题：

- [vRealize Automation 用户角色是什么](#)
- [将云帐户添加到 vRealize Automation Cloud Assembly](#)
- [将 vRealize Automation 与其他应用程序集成](#)
- [vRealize Automation Cloud Assembly 中的载入计划是什么](#)
- [vRealize Automation Cloud Assembly 环境的高级配置](#)

## vRealize Automation 用户角色是什么

vRealize Automation 具有多个级别的用户角色。这些不同的级别控制对以下项的访问：组织、服务、生成或使用云模板、目录项和管道的项目，以及用户使用或查看用户界面各个部分的能力。这些不同的级别为云管理员提供了不同的工具，以应用其操作需求所需的任何粒度级别。

### 常规角色描述

用户角色在不同的级别进行定义。将为每个服务定义服务级别角色。

此表介绍了有关服务角色的更多详细信息。

角色	常规权限	定义角色的位置
组织所有者	可以访问控制台并将用户添加到组织。 组织所有者无法访问服务，除非他们具有服务角色。 <a href="#">有关组织用户角色的更多信息</a>	组织控制台
组织成员	可以访问控制台。 组织成员无法访问服务，除非他们具有服务角色。 <a href="#">有关组织用户角色的更多信息</a>	组织控制台

角色	常规权限	定义角色的位置
服务管理员	<p>可以访问控制台，并在服务中拥有完整的查看、更新和删除权限。</p> <ul style="list-style-type: none"> <li>■ <a href="#">Cloud Assembly 服务角色</a></li> <li>■ <a href="#">Service Broker 服务角色</a></li> <li>■ <a href="#">Code Stream 服务角色</a></li> </ul>	组织控制台
服务用户	<p>可以访问控制台和服务，但具有有限权限。</p> <p>服务成员对用户界面的访问有限。他们可以查看的内容或可执行的操作取决于其项目成员资格。</p> <ul style="list-style-type: none"> <li>■ <a href="#">Cloud Assembly 服务角色</a></li> <li>■ <a href="#">Service Broker 服务角色</a></li> <li>■ <a href="#">Code Stream 服务角色</a></li> </ul>	组织控制台
服务查看者	<p>可以在仅查看模式下访问控制台和服务。</p> <ul style="list-style-type: none"> <li>■ <a href="#">Cloud Assembly 服务角色</a></li> <li>■ <a href="#">Service Broker 服务角色</a></li> <li>■ <a href="#">Code Stream 服务角色</a></li> </ul>	组织控制台
执行者（仅限 vRealize Automation Code Stream）	<p>可以访问控制台和管理管道执行。</p> <p><a href="#">Code Stream 服务角色</a></p>	组织控制台
vRA Migration Assistant 管理员	<p>可以访问控制台，并在 vRA Migration Assistant 和 Cloud Assembly 中拥有完整的查看、更新和删除特权。</p> <p>此角色还必须至少具有 Cloud Assembly 查看者角色。</p>	组织控制台
vRA Migration Assistant 查看者	<p>可以在仅查看模式下访问控制台、vRA Migration Assistant 和 Cloud Assembly。</p> <p>此角色还必须至少具有 Cloud Assembly 查看者角色。</p>	组织控制台
Orchestrator 管理员	<p>可以访问所有 vRealize Orchestrator 客户端功能和内容，包括由特定组创建的内容。</p>	组织控制台和 vRealize Orchestrator 客户端
Orchestrator  workflow 设计人员	<p>可以创建、运行、编辑和删除自己的 vRealize Orchestrator 客户端内容。可以将自己的内容添加到为其分配的组。无权访问 vRealize Orchestrator 客户端的管理功能和故障排除功能。</p>	组织控制台和 vRealize Orchestrator 客户端

角色	常规权限	定义角色的位置
项目角色	可以查看和管理项目资源，具体取决于项目角色。 项目角色包括管理员、成员和查看者。 <a href="#">vRealize Automation 中的组织和服务用户角色</a>	vRealize Automation Cloud Assembly、 vRealize Automation Service Broker 和 vRealize Automation Code Stream
自定义角色	这些权限由 vRealize Automation Cloud Assembly 为所有服务定义。 用户必须在相关服务中至少具有服务查看者角色，以便他们可以访问服务。自定义角色优先于服务角色。 <a href="#">vRealize Automation 中的自定义用户角色</a>	vRealize Automation Cloud Assembly 和 vRealize Automation Service Broker

## vRealize Automation 中的组织和服务用户角色

为 vRealize Automation Cloud Assembly、vRealize Automation Service Broker 和 vRealize Automation Code Stream 服务定义的组织和服务用户角色确定了用户在每个服务中可查看的内容和执行的的操作。

### 组织用户角色

由组织所有者在 vRealize Automation 控制台中为组织定义用户角色。有两种类型的角色：组织角色和服务角色。

组织角色是全局的，适用于组织中的所有服务。组织级别的角色是组织所有者或组织成员角色。

有关组织角色的详细信息，请参见《[管理 vRealize Automation](#)》。

vRealize Automation Cloud Assembly 服务角色（是特定于服务的权限）也在控制台的组织级别分配。

### 服务角色

这些服务角色由组织所有者分配。

本文包括有关全部三种服务的信息。

- [Cloud Assembly 服务角色](#)
- [Service Broker 服务角色](#)
- [Code Stream 服务角色](#)

### Cloud Assembly 服务角色

vRealize Automation Cloud Assembly 服务角色决定您在 vRealize Automation Cloud Assembly 中可以查看的内容和可以执行的操作。这些服务角色由组织所有者在控制台中定义。

表 3-1. vRealize Automation Cloud Assembly 服务角色说明

角色	说明
Cloud Assembly 管理员	对整个用户界面和 API 资源具有读取和写入访问权限的用户。这是唯一可以查看和执行所有操作的用户角色，包括添加云帐户、创建新项目以及分配项目管理员。
Cloud Assembly 用户	不具有 Cloud Assembly 管理员角色的用户。 在 vRealize Automation Cloud Assembly 项目中，管理员将用户作为项目成员、管理员或查看者添加到项目中。管理员还可以添加项目管理员。
Cloud Assembly 查看者	具有读取访问权限的用户，可以查看信息，但不能创建、更新或删除值。这是跨所有项目的只读角色。 具有查看者角色的用户可以查看管理员可使用的所有信息。除非您将他们设置为项目管理员或项目成员，否则他们无法执行任何操作。如果用户与项目关联，则他们具有与该角色相关的权限。项目查看者不会像管理员或成员角色那样扩展其权限。

除了服务角色外，vRealize Automation Cloud Assembly 还具有项目角色。在所有服务中都可以使用任何项目。

项目角色是在 vRealize Automation Cloud Assembly 中定义的，可能会因项目而异。

下表介绍了不同的服务和项目角色可以查看的内容和执行的操作，请记住，服务管理员对用户界面的所有区域具有完全权限。

项目角色说明可帮助您决定为用户提供哪些权限。

- 项目管理员利用服务管理员创建的基础架构来确保项目成员具有进行开发工作所需的资源。
- 项目成员在其项目中工作，以设计和部署云模板。
- 项目查看者仅具有只读访问权限，但在某些情况下，他们可以执行诸如下载云模板之类的非破坏性操作。

表 3-2. vRealize Automation Cloud Assembly 服务角色和项目角色

UI 上下文	任务	Cloud Assembly 管理员	Cloud Assembly 查看者	Cloud Assembly 用户 用户必须是项目管理员或成员才能查看和执行项目相关任务。		
				项目管理员	项目成员	项目查看者
访问 Cloud Assembly						
控制台	在 vRA 控制台中，您可以查看并打开 Cloud Assembly	是	是	是	是	是
基础架构						
	查看并打开“基础架构”选项卡	是	是	是	是	是
配置 - 项目	创建项目	是				

表 3-2. vRealize Automation Cloud Assembly 服务角色和项目角色（续）

UI 上下文	任务	Cloud Assembly 管理员	Cloud Assembly 查看者	Cloud Assembly 用户 用户必须是项目管理员或成员才能查看和执行项目相关任务。		
				项目管理 员	项目成员	项目查看者
	更新或删除项目摘要、置备、Kubernetes、集成和测试项目配置中的值。	是				
	在项目中添加用户和组并分配角色。	是		是。您的项目。		
	查看项目	是	是	是。您的项目	是。您的项目	是。您的项目
配置 - 云区域	创建、更新或删除云区域	是				
	查看云区域	是	是			
配置 - Kubernetes 区域	创建、更新或删除 Kubernetes 区域	是				
	查看 Kubernetes 区域	是	是			
配置 - 特定实例	创建、更新或删除特定实例	是				
	查看特定实例	是	是			
配置 - 映像映射	创建、更新或删除映像映射	是				
	查看映像映射	是	是			
配置 - 网络配置文件	创建、更新或删除网络配置文件	是				
	查看映像网络配置文件	是	是			
配置 - 存储配置文件	创建、更新或删除存储配置文件	是				
	查看映像存储配置文件	是	是			
配置 - 定价卡	创建、更新或删除定价卡	是				
	查看定价卡	是	是			
配置 - 标记	创建、更新或删除标记	是				
	查看标记	是	是			
资源 - 计算	将标记添加到已发现的计算资源	是				
	查看发现的计算资源	是	是			
资源 - 网络	修改网络标记、IP 范围、IP 地址	是				
	查看发现的网络资源	是	是			

表 3-2. vRealize Automation Cloud Assembly 服务角色和项目角色（续）

UI 上下文	任务	Cloud Assembly 管理员	Cloud Assembly 查看者	Cloud Assembly 用户 用户必须是项目管理员或成员才能查看和执行项目相关任务。		
				项目管理员	项目成员	项目查看者
资源 - 安全	将标记添加到已发现的安全组	是				
	查看已发现的安全组	是	是			
资源 - 存储	向发现的存储中添加标记	是				
	查看存储	是	是			
资源 - 计算机	添加和删除计算机	是				
	查看计算机	是	是	是。您的项目	是。您的项目	是。您的项目
资源 - 卷	删除发现的存储卷	是				
	查看发现的存储卷	是	是	是。您的项目	是。您的项目	是。您的项目。
资源 - Kubernetes	部署或添加 Kubernetes 集群，以及创建或添加命名空间	是				
	查看 Kubernetes 集群和命名空间	是	是	是。您的项目	是。您的项目	是。您的项目
活动 - 请求	删除部署请求记录	是				
	查看部署请求记录	是	是	是。您的项目	是。您的项目	是。您的项目
活动 - 事件日志	查看事件日志	是	是	是。您的项目	是。您的项目	是。您的项目
连接 - 云帐户	创建、更新或删除云帐户	是				
	查看云帐户	是	是			
连接 - 集成	创建、更新或删除集成	是				
	查看集成	是	是			
载入	创建、更新或删除载入计划	是				
	查看载入计划	是	是			是。您的项目
<b>商城</b>						
	查看并打开“商城”选项卡	是	是			
	在“设计”选项卡上使用已下载的云模板	是		是。如果与项目相关联。	是。如果与项目相关联。	

表 3-2. vRealize Automation Cloud Assembly 服务角色和项目角色 （续）

UI 上下文	任务	Cloud Assembly 管理员	Cloud Assembly 查看者	Cloud Assembly 用户 用户必须是项目管理员或成员才能查看和执行项目相关任务。		
				项目管理员	项目成员	项目查看者
商城 - 云模板	下载云模板	是				
	查看云模板	是	是			
商城 - 映像	下载映像	是				
	查看映像	是	是			
商城 - 下载	查看所有已下载项目的日志	是	是			
<b>可扩展性</b>						
	查看并打开“可扩展性”选项卡	是	是			是
事件	查看可扩展性事件	是	是			
订阅	创建、更新或删除可扩展性订阅	是				
	停用订阅	是				
	查看订阅	是	是			
库 - 事件主题	查看事件主题	是	是			
库 - 操作	创建、更新或删除可扩展性操作	是				
	查看可扩展性操作	是	是			
库 - 工作流	查看可扩展性工作流	是	是			
活动 - 操作运行	取消或删除可扩展性操作运行	是				
	查看可扩展性操作运行	是	是			是。您的项目
活动 - 工作流运行	查看可扩展性工作流运行	是	是			
<b>设计</b>						
设计	打开“设计”选项卡并查看云模板列表	是	是	是。您的项目	是。您的项目	是。您的项目
云模板	创建、更新和删除云模板	是		是。您的项目	是。您的项目	
	查看云模板	是	是	是。您的项目	是。您的项目	是。您的项目
	下载云模板	是	是	是。您的项目	是。您的项目	是。您的项目



表 3-2. vRealize Automation Cloud Assembly 服务角色和项目角色（续）

UI 上下文	任务	Cloud Assembly 管理员	Cloud Assembly 查看者	Cloud Assembly 用户 用户必须是项目管理员或成员才能查看和执行项目相关任务。		
				项目管理员	项目成员	项目查看者
	上载云模板	是		是。您的项目	是。您的项目	
	部署云模板	是		是。您的项目	是。您的项目	
	版本控制和还原云模板	是		是。您的项目	是。您的项目	
	将云模板发布到目录	是		是。您的项目	是。您的项目	
自定义资源	创建、更新或删除自定义资源	是				
	查看自定义资源	是	是	是。您的项目	是。您的项目	是。您的项目
自定义操作	创建、更新或删除自定义操作	是				
	查看自定义操作	是	是	是。您的项目	是。您的项目	是。您的项目
<b>部署</b>						
	查看并打开“部署”选项卡	是	是	是	是	是
	查看部署，包括部署详细信息、部署历史记录和故障排除信息。	是	是	是。您的项目	是。您的项目	是。您的项目
	基于策略对部署运行实施后操作。	是		是。您的项目	是。您的项目	

## Service Broker 服务角色

vRealize Automation Service Broker 服务角色决定您在 vRealize Automation Service Broker 中可以查看的内容和可以执行的操作。这些服务角色由组织所有者在控制台中定义。

表 3-3. Service Broker 服务角色说明

角色	说明
Service Broker 管理员	必须对整个用户界面和 API 资源具有读取和写入访问权限。这是唯一可以执行所有任务（包括创建新项目和分配项目管理员）的用户角色。
Service Broker 用户	不具有 vRealize Automation Service Broker 管理员角色的任何用户。 在 vRealize Automation Service Broker 项目中，管理员将用户作为项目成员、管理员或查看者添加到项目中。管理员还可以添加项目管理员。
Service Broker 查看者	具有读取访问权限的用户，可以查看信息，但不能创建、更新或删除值。 具有查看者角色的用户可以查看管理员可使用的所有信息。除非您将他们设置为项目管理员或项目成员，否则他们无法执行任何操作。如果用户与项目关联，则他们具有与该角色相关的权限。项目查看者不会像管理员或成员角色那样扩展其权限。

除了服务角色外，vRealize Automation Service Broker 还具有项目角色。在所有服务中都可以使用任何项目。

项目角色是在 vRealize Automation Service Broker 中定义的，可能会因项目而异。

下表介绍了不同的服务和项目角色可以查看的内容和执行的的操作，请记住，服务管理员对用户界面的所有区域具有完全权限。

在您决定为用户提供哪些权限时，可以使用以下项目角色描述为您提供帮助。

- 项目管理员利用服务管理员创建的基础架构来确保项目成员具有进行开发工作所需的资源。
- 项目成员在其项目中工作，以设计和部署云模板。
- 项目查看者仅限于只读访问权限。

表 3-4. Service Broker 服务角色和项目角色

UI 上下文	任务	Service Broker 管理员	Service Broker 查看者	Service Broker 用户		
				用户必须是项目管理员才能查看和执行项目相关任务。		
				项目管理员	项目成员	项目查看者
访问 Service Broker						
控制台	在控制台中，您可以查看和打开 Service Broker	是	是	是	是	是
基础架构						
	查看并打开“基础架构”选项卡	是	是			
配置 - 项目	创建项目	是				

表 3-4. Service Broker 服务角色和项目角色（续）

UI 上下文	任务	Service Broker 管理员	Service Broker 查看者	Service Broker 用户 用户必须是项目管理员才能查看和执行项目相关任务。		
				项目管理员	项目成员	项目查看者
	更新或删除项目摘要、置备、Kubernetes 和集成中的值	是				
	在项目中添加用户和组并分配角色。	是			是。您的项目。	
	查看项目	是	是			
配置 - 云区域	创建、更新或删除云区域	是				
	查看云区域	是	是			
配置 - Kubernetes 区域	创建、更新或删除 Kubernetes 区域	是				
	查看 Kubernetes 区域	是	是			
连接 - 云帐户	创建、更新或删除云帐户	是				
	查看云帐户	是	是			
连接 - 集成	创建、更新或删除集成	是				
	查看集成	是	是			
活动 - 请求	删除部署请求记录	是				
	查看部署请求记录	是				
活动 - 事件日志	查看事件日志	是				
<b>内容和策略</b>						
	查看并打开“内容和策略”选项卡	是	是			
内容源	创建、更新或删除内容源	是				
	查看内容源	是	是			
内容共享	添加或移除共享内容	是				
	查看共享内容	是	是			
内容	自定义表单和配置项目	是				
	查看内容	是	是			
策略 - 定义	创建、更新或删除策略定义	是				
	查看策略定义	是	是			
策略 - 实施	查看实施日志	是	是			

表 3-4. Service Broker 服务角色和项目角色（续）

UI 上下文	任务	Service Broker 管理员	Service Broker 查看者	Service Broker 用户 用户必须是项目管理员才能查看和执行项目相关任务。		
				项目管理员	项目成员	项目查看者
通知 - 电子邮件服务器	配置电子邮件服务器	是				
目录						
	查看并打开“目录”选项卡	是	是	是	是	是
	查看可用目录项	是	是	是。您的项目	是。您的项目	是。您的项目
	请求目录项	是		是。您的项目	是。您的项目	
部署						
	查看并打开“部署”选项卡	是	是	是。	是	是
	查看部署，包括部署详细信息、部署历史记录和故障排除信息。	是	是	是。您的项目	是。您的项目	是。您的项目
	基于策略对部署运行实施后操作	是		是。您的项目	是。您的项目	
批准						
	查看并打开“批准”选项卡	是	是	是	是	是
	响应批准请求	是		仅 Service Broker 用户角色	仅 Service Broker 用户角色	仅 Service Broker 用户角色

## Code Stream 服务角色

vRealize Automation Code Stream 服务角色决定您在 vRealize Automation Code Stream 中可以查看的内容和可以执行的操作。这些角色由组织所有者在控制台中定义。在所有服务中都可以使用任何项目。

表 3-5. Code Stream 服务角色描述

角色	说明
Code Stream 管理员	对整个用户界面和 API 资源具有读取和写入访问权限的用户。只有此用户角色才能查看所有内容以及执行所有操作，包括创建项目，集成端点，添加触发器，创建管道和自定义仪表板，将端点和变量标记为受限制资源，运行使用受限制资源的管道，以及请求在 vRealize Automation Service Broker 中发布管道。
Code Stream 开发人员	可以使用管道但无法使用受限制端点或变量的用户。如果管道包含受限制端点或变量，则此用户必须获得批准才能执行使用受限制端点或变量的管道任务。
Code Stream 执行者	可以运行管道并批准或拒绝用户操作任务的。此用户可以恢复、暂停和取消管道执行，但不能修改管道。

表 3-5. Code Stream 服务角色描述（续）

角色	说明
Code Stream 用户	可以访问 vRealize Automation Code Stream，但在 vRealize Automation Code Stream 中不具有任何其他特权的用户。
Code Stream 查看者	具有读取访问权限的用户，可以查看管道、端点、管道执行和仪表板，但不能进行创建、更新或删除。此外，具有“服务查看者”角色的用户也可以查看管理员可使用的所有信息。除非您将他们设置为项目管理员或项目成员，否则他们无法执行任何操作。如果用户与项目关联，则他们具有与该角色相关的权限。项目查看者不会像管理员或成员角色那样扩展其权限。

除了服务角色外，vRealize Automation Code Stream 还具有项目角色。在所有服务中都可以使用任何项目。

项目角色是在 vRealize Automation Code Stream 中定义的，可能会因项目而异。

下表介绍了不同的服务和项目角色可以查看的内容和执行的操作，请记住，服务管理员对用户界面的所有区域具有完全权限。

使用以下项目角色描述可帮助您决定为用户提供哪些权限。

- 项目管理员利用服务管理员创建的基础架构来确保项目成员具有进行开发工作所需的资源。项目管理员可以添加成员。
- 具有服务角色的项目成员可以使用服务。
- 项目查看者可以查看项目，但不能创建、更新或删除项目。

除受限制以外的所有操作表示此角色有权对实体执行创建、读取、更新和删除操作，但受限制的变量和端点除外。

表 3-6. vRealize Automation Code Stream 服务角色功能

UI 上下文	功能	Code Stream 管理员角色	Code Stream 开发人员角色	Code Stream 执行者角色	Code Stream 查看者角色	Code Stream 用户角色
<b>管道</b>						
	查看管道	是	是	是	是	
	创建管道	是	是			
	运行管道	是	是	是		
	运行包含受限制端点或受限制变量的管道	是				
	更新管道	是	是			
	删除管道	是	是			
<b>管道执行</b>						
	查看管道执行	是	是	是	是	
	恢复、暂停和取消管道执行	是	是	是		

表 3-6. vRealize Automation Code Stream 服务角色功能（续）

UI 上下文	功能	Code Stream 管理员角色	Code Stream 开发人员角色	Code Stream 执行者角色	Code Stream 查看者角色	Code Stream 用户角色
	恢复等待批准受限制资源的管道	是				
<b>自定义集成</b>						
	创建自定义集成	是	是			
	读取自定义集成	是	是			
	更新自定义集成	是	是			
<b>端点</b>						
	查看执行	是	是	是	是	
	创建执行	是	是			
	更新执行	是	是			
	删除执行	是	是			
<b>将资源标记为受限制</b>						
	将端点或变量标记为受限制	是				
<b>仪表板</b>						
	查看仪表板	是	是	是	是	
	创建仪表板	是	是			
	更新仪表板	是	是			
	删除仪表板	是	是			

## vRealize Automation 中的自定义用户角色

作为 vRealize Automation Cloud Assembly 管理员，您可以创建自定义角色，以定义用户可在 vRealize Automation 中查看的内容和执行的的操作。之后，您可以将用户分配到这些角色。

### 自定义用户角色权限

使用 vRealize Automation Cloud Assembly，可以定义更精细的用户角色，然后将用户分配给这些角色。自定义角色有两个类别，即查看和管理。

- 查看。分配给具有此权限的角色的用户可以查看用户界面选定部分中所有项目的项。此角色对需要查看帐户、配置或已分配值的用户非常有用。

- 管理。分配给具有此权限的角色的用户可以查看所有项，并对用户界面选定部分中的所有项目具有完全添加、编辑和删除权限。

这些权限扩展了其他角色授予的特权，并且不受项目成员资格的限制。例如，您可以扩展项目管理员权限以管理基础架构的各部分或者为服务查看者提供查看和响应批准请求的功能。

要定义用户角色并分配用户，请以服务管理员身份打开 vRealize Automation Service Broker 或 vRealize Automation Cloud Assembly，然后选择**基础架构 > 管理 > 自定义角色**。无法在 vRealize Automation Code Stream 中配置自定义角色，但这些角色适用于所有服务。

**表 3-7. 自定义角色**

用户界面	权限	说明
<b>基础架构</b>		
	查看云帐户。	查看云帐户。
	管理云帐户	创建、更新或删除云帐户。
	查看映像映射	查看映像映射。
	管理映像映射	创建、更新或删除映像映射。
	查看特定实例映射	查看特定实例映射。
	管理特定实例映射	创建、更新或删除特定实例映射。
	查看云区域	查看云区域。
	管理云区域	创建、更新或删除云区域。
	查看计算机	查看计算机。
	查看请求	查看活动请求。
	管理请求	从列表中删除请求。
	查看集成	查看集成。
	管理集成	创建、更新或删除集成。
	查看项目	查看项目。
	管理项目	创建项目。在项目中添加用户并分配角色。更新或删除项目摘要、用户、置备、Kubernetes、集成和测试项目配置中的值。
	查看载入计划	查看载入计划
	管理载入计划	创建、更新、运行或删除载入计划
<b>目录</b>		
	查看内容	

表 3-7. 自定义角色 （续）

用户界面	权限	说明
	管理内容	添加、更新、删除内容源。 共享内容。 自定义内容，包括目录图标和请求表单。
<b>策略</b>		
	查看策略	查看策略定义。
	管理策略	创建、更新或删除策略定义。
<b>部署</b>		
	查看部署	查看所有部署，包括部署详细信息、部署历史记录和故障排除信息。
	管理部署	查看所有部署并运行实施后操作策略允许管理员对部署和部署组件运行的所有实施后操作。
<b>云模板</b>		
	查看云模板	查看云模板。
	管理云模板	创建、更新、测试、删除、版本控制、共享云模板以及发布/取消发布云模板版本。
	编辑云模板	创建、更新、测试、版本控制、共享云模板以及发布/取消发布云模板版本。该角色没有删除云模板的权限。
	部署云模板	在任何项目中测试和部署任何云模板。
	部署内嵌云模板内容	在与被分配用户关联的项目中部署任何云模板。项目角色可以是管理员、成员或查看者。
<b>XaaS</b>		
	查看自定义资源	查看自定义资源。
	管理自定义资源	创建、更新或删除自定义资源
	查看资源操作	查看自定义操作。
	管理资源操作	创建、更新或删除自定义操作
<b>可扩展性</b>		
	查看可扩展性资源	查看事件、订阅、事件主题、操作、工作流、操作运行和工作流运行。
	管理可扩展性资源	创建、更新、删除和停用可扩展性订阅。 创建、更新或删除可扩展性操作。取消或删除可扩展性操作运行。



表 3-7. 自定义角色 （续）

用户界面	权限	说明
<b>管道</b>		
	管理管道	创建、编辑和删除管道、端点、变量和触发器配置。 排除受限制的模型。
	管理受限制的管道	创建、编辑和删除管道、端点、变量和触发器配置。 包括受限制的模型。
	管理自定义集成	添加、编辑和删除自定义集成。
	执行管道	运行管道模型执行和触发器，以及暂停、取消、恢复或重新运行执行和触发器。
	执行受限制的管道	运行管道模型执行和触发器，以及暂停、取消、恢复或重新运行执行和触发器。 解析受限制的端点和变量。
	管理执行	运行管道模型执行和触发器，以及暂停、取消、恢复或重新运行执行和触发器。 解析受限制的端点和变量。 删除执行。
<b>批准</b>		
	管理批准	查看用于批准或拒绝批准请求的“批准”选项卡。 具有此角色的审批者将不会收到有关批准请求的电子邮件通知，除非他们是策略中的审批者。

## 用例：用户角色如何帮助我控制 vRealize Automation 中的访问权限

作为云管理员，您希望可以控制用户可在 vRealize Automation 中执行的任务。根据您的管理目标 and 应用程序开发团队的职责，您可以通过不同方式配置用户角色以支持这些目标。

下面的 vRealize Automation Cloud Assembly 和 vRealize Automation Service Broker 示例基于三个用例。这些示例只是为了提供充分的说明，以阐述用户角色的应用。

这些用例的目标受众是云管理员和服务管理员。

这些用例互为构建基础。如果您准备直接进入用例 3，可能需要查看用例 1 和 2，以更好地了解如何以指定的方式配置角色。

这些用例是为了展示用户角色，而不是提供有关配置基础架构、管理项目、创建云模板和使用部署的详细信息。

开始之前，您必须了解云管理员在 vRealize Automation 控制台中配置的用户角色级别。

### ■ 组织角色

组织角色用于控制可以访问控制台的人员。

作为组织所有者，您必须确保为任一服务的所有用户分配至少一个组织成员角色。

角色	说明
组织所有者	管理员可以添加用户、更改用户的角色以及从组织中移除用户。所有者负责管理用户有权访问哪些服务。
组织成员	常规用户可以登录到组织控制台。要访问服务，组织所有者必须分配用户服务角色。

#### ■ 服务角色

服务角色控制哪些用户可以访问他们分配的服务。

作为组织所有者，您必须确保为需要访问服务的用户分配适当的角色。您可以使用角色来控制用户在每个服务中可以操作的程度。

**表 3-8. vRealize Automation Cloud Assembly 服务角色说明**

角色	说明
Cloud Assembly 管理员	对整个用户界面和 API 资源具有读取和写入访问权限的用户。这是唯一可以查看和执行所有操作的用户角色，包括添加云帐户、创建新项目以及分配项目管理员。
Cloud Assembly 用户	不具有 Cloud Assembly 管理员角色的用户。 在 vRealize Automation Cloud Assembly 项目中，管理员将用户作为项目成员、管理员或查看者添加到项目中。管理员还可以添加项目管理员。
Cloud Assembly 查看者	具有读取访问权限的用户，可以查看信息，但不能创建、更新或删除值。这是跨所有项目的只读角色。 具有查看者角色的用户可以查看管理员可使用的所有信息。除非您将他们设置为项目管理员或项目成员，否则他们无法执行任何操作。如果用户与项目关联，则他们具有与该角色相关的权限。项目查看者不会像管理员或成员角色那样扩展其权限。

**表 3-9. Service Broker 服务角色说明**

角色	说明
Service Broker 管理员	必须对整个用户界面和 API 资源具有读取和写入访问权限。这是唯一可以执行所有任务（包括创建新项目和分配项目管理员）的用户角色。
Service Broker 用户	不具有 vRealize Automation Service Broker 管理员角色的任何用户。 在 vRealize Automation Service Broker 项目中，管理员将用户作为项目成员、管理员或查看者添加到项目中。管理员还可以添加项目管理员。
Service Broker 查看者	具有读取访问权限的用户，可以查看信息，但不能创建、更新或删除值。 具有查看者角色的用户可以查看管理员可使用的所有信息。除非您将他们设置为项目管理员或项目成员，否则他们无法执行任何操作。如果用户与项目关联，则他们具有与该角色相关的权限。项目查看者不会像管理员或成员角色那样扩展其权限。

表 3-10. Code Stream 服务角色描述

角色	说明
Code Stream 管理员	对整个用户界面和 API 资源具有读取和写入访问权限的用户。只有此用户角色才能查看所有内容以及执行所有操作，包括创建项目，集成端点，添加触发器，创建管道和自定义仪表板，将端点和变量标记为受限制资源，运行使用受限制资源的管道，以及请求在 vRealize Automation Service Broker 中发布管道。
Code Stream 开发人员	可以使用管道但无法使用受限制端点或变量的用户。如果管道包含受限制端点或变量，则此用户必须获得批准才能执行使用受限制端点或变量的管道任务。
Code Stream 执行者	可以运行管道并批准或拒绝用户操作任务的用户。此用户可以恢复、暂停和取消管道执行，但不能修改管道。
Code Stream 用户	可以访问 vRealize Automation Code Stream，但在 vRealize Automation Code Stream 中不具有任何其他特权的用户。
Code Stream 查看者	具有读取访问权限的用户，可以查看管道、端点、管道执行和仪表板，但不能进行创建、更新或删除。此外，具有“服务查看者”角色的用户也可以查看管理员可使用的所有信息。除非您将他们设置为项目管理员或项目成员，否则他们无法执行任何操作。如果用户与项目关联，则他们具有与该角色相关的权限。项目查看者不会像管理员或成员角色那样扩展其权限。

#### ■ 项目成员资格角色

项目成员资格可确定可用的基础架构资源和云模板。

项目成员资格由具有服务管理员角色的用户在服务中定义。服务管理员必须确保在每个项目中为需要访问一个或多个项目的用户分配了相应的项目角色。

表 3-11. 项目角色

角色	说明
项目管理员	项目管理员可以管理自己的项目，创建和部署与项目关联的云模板，以及管理所有项目成员的项目部署。
项目成员	项目成员可以创建和部署与其项目关联的云模板，管理自己的部署以及管理任何共享部署。
项目查看者	项目查看者是项目的成员，对其项目资源、云模板和部署具有只读访问权限。

#### ■ 自定义角色

自定义角色由 vRealize Automation Cloud Assembly 创建，以便细化成员和查看者角色。

这些用例中提供的过程旨在突出显示用户角色，并未详细或明确介绍设置 vRealize Automation 的过程。

在配置角色时，请记住，运行 API 操作的用户会受到您在此处分配的角色制约。

#### 前提条件

- 确认您具有组织所有者角色。您在登录控制台后，必须能够查看**身份和访问管理**选项卡。否则，请与组织所有者联系。
- 
- 验证 vRealize Automation 中是否添加了用户。

安装 vRealize Automation 时，将在此过程中添加 Active Directory 用户。

- 有关各种角色的更详细的任务和角色列表，请参见 [vRealize Automation 中的组织和服务用户角色](#)。

## 步骤

### 1 用户角色用例 1：设置 vRealize Automation 用户角色以支持小型应用开发团队

作为 vRealize Automation 云管理员，您负责管理基础架构资源的访问权限和预算。您可以将自己和其他两个用户添加为管理员。此小型团队可以创建基础架构，并开发与使用云模板的团队的业务目标相匹配的云模板。然后，由您和您的小型管理员团队为您的非管理员使用者部署云模板。您不允许非管理员访问 vRealize Automation。

### 2 用户角色用例 2：设置 vRealize Automation 用户角色以支持更大型的开发团队和目录

作为 vRealize Automation 组织所有者，您负责管理基础架构资源的访问权限和预算。您有一组云模板开发人员，他们以迭代方式为不同项目创建和部署模板，直到模板可以交付给使用者。然后，您可以将可部署资源提供给目录中的使用者。

### 3 用户角色用例 3：设置 vRealize Automation 自定义用户角色以细化系统角色

作为 vRealize Automation 组织所有者或服务管理员，您可以使用组织和服务系统角色管理用户访问。但是，您还希望为所选用户创建自定义角色，并执行任务或查看其系统角色之外的内容。

## 用户角色用例 1：设置 vRealize Automation 用户角色以支持小型应用开发团队

作为 vRealize Automation 云管理员，您负责管理基础架构资源的访问权限和预算。您可以将自己和其他两个用户添加为管理员。此小型团队可以创建基础架构，并开发与使用云模板的团队的业务目标相匹配的云模板。然后，由您和您的小型管理员团队为您的非管理员使用者部署云模板。您不允许非管理员访问 vRealize Automation。

在此用例中，您是组织所有者，并且您拥有一支小团队，其中所有用户都具有服务管理员角色。

以下过程全程针对一个用户。您可以为多个用户执行每个步骤。

## 前提条件

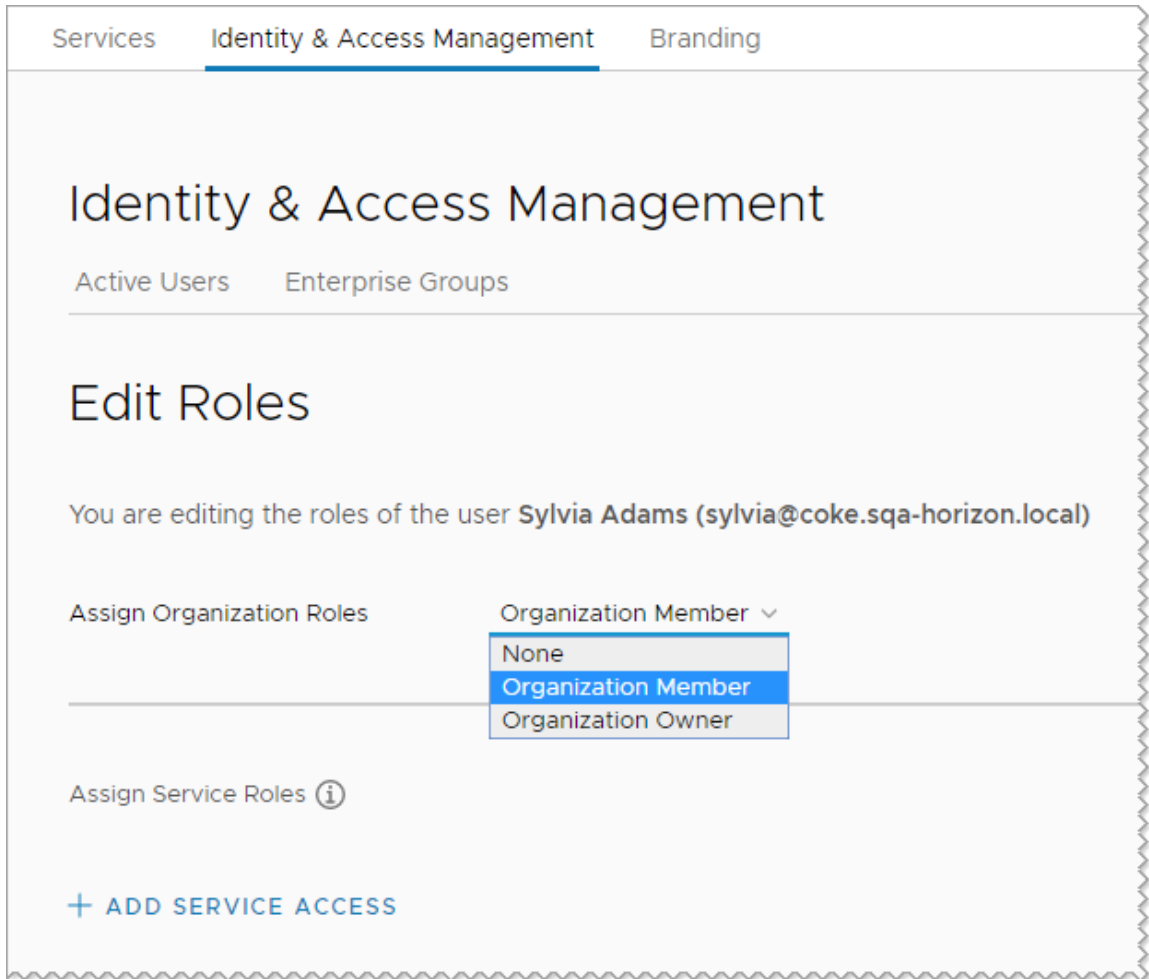
- 确认您满足用例简介中规定的所有必备条件。请参见 [用例：用户角色如何帮助我控制 vRealize Automation 中的访问权限](#)。

## 步骤

### 1 分配组织角色。单击 **身份与访问管理**。

- a 登录到 vRealize Automation 控制台。
- b 单击 **身份与访问管理**。

- c 选择用户名，然后单击**编辑角色**。
- d 在**分配组织角色**下拉菜单中，选择**组织成员**。



组织成员角色可确保用户能够访问控制台以及您将其添加到的任何服务。他们无法管理组织用户。让此用户的“编辑角色”页面保持打开状态，然后继续执行下一步。

## 2 将 Cloud Assembly 管理员角色分配给您自己以及此方案中的一个或两个其他管理员。

服务管理员角色具有添加、编辑和删除基础架构、项目、云模板和部署的全部特权。在方案 2 中，为一个人定义管理员角色，为另一个人定义用户角色。此示例使用 **Sylvia**。

- a 单击**添加服务访问权限**。
- b 使用以下值配置用户。

服务	角色
vRealize Automation Cloud Assembly	vRealize Automation Cloud Assembly 管理员

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 在 Cloud Assembly 中创建一个项目，用于对资源进行分组和管理不同业务组的资源计费。

- a 在控制台中，单击**服务**选项卡，然后单击 **Cloud Assembly**。
- b 选择**基础架构 > 项目 > 新建项目**。

此用户角色用例侧重于提供有关如何实施用户角色的示例，而不是创建完全定义的系统。

有关配置基础架构的信息，请参见[构建资源基础架构](#)。有关项目的详细信息，请参见[添加和管理项目](#)。

- c 输入 **WebAppTeam** 作为项目名称。
- d 单击**用户**，然后单击**添加用户**。
- e 输入可帮助您构建和管理基础架构和云模板的个人的电子邮件地址。  
例如，tony@mycompany.com,sylvia@mycompany.com。

- f 在**分配角色**下拉菜单中，选择**管理员**。

作为 vRealize Automation Cloud Assembly 管理员，这两个用户已具有云帐户、基础架构和所有项目的管理员访问权限。此步骤可帮助您了解后续方案中使用的角色。在后续的方案中，您可以定义项目管理员和具有不同权限的项目成员角色。

- g 单击**置备**选项卡，然后添加一个或多个云区域。

此外，还要提醒您，此用例与用户角色相关。

- 4 请开发一个简单的云模板，以便您可以测试 WebAppTeam 项目。

此云模板部分比较简短。重点是项目定义的用户和用户角色，而不是创建云模板的方式。

- a 选择**云模板 > 新建**。
- b 对于新云模板名称，输入 **WebApp**。
- c 对于**项目**，选择 WebAppTeam。

- d 选择**仅与项目共享**。

此设置可确保云模板仅可供项目成员使用。当您准备好向其他团队提供云模板时，可以选择“允许管理员与此组织中的任何项目共享”。与其他项目共享云模板，意味着您无需维护同一基础模板的重复实例。您可以将云模板从开发项目移动到生产项目，以便目录使用者可以将其部署到生产基础架构资源。

- e 单击**创建**。
- f 在云模板设计器中，将**云平台无关 > 计算机**组件拖动到画布中。  
有关配置云模板的详细信息，请参见**设计部署**。
- g 单击**部署**。
- h 继续在云模板上重复操作，直到您准备好将其提供给使用者为止。
- i 单击**版本**，然后发布云模板并对其进行版本控制。

- 5 使用最常用的方法向用户发送登录信息。



## 结果

在此用例中，您将两个同事设置为了组织成员。然后，将 Sylvia 设置为了 vRealize Automation Cloud Assembly 管理员。将 Tony 设置为了 WebApp 项目管理员。此用户角色配置仅适用于小团队场景，即您将向使用者提供已部署的应用程序，而不是为他们提供自助访问权限或目录。

## 用户角色用例 2：设置 vRealize Automation 用户角色以支持更大型的团队和目录

作为 vRealize Automation 组织所有者，您负责管理基础架构资源的访问权限和预算。您有一组云模板开发人员，他们以迭代方式为不同项目创建和部署模板，直到模板可以交付给使用者。然后，您可以将可部署资源提供给目录中的使用者。

此用例假设您了解用例 1 是一个仅限管理员的用例。现在，您希望扩展系统，以支持更多团队和更大的目标。

- 允许开发人员在开发过程中创建并部署自己的应用程序云模板。您可以将自己添加为管理员，然后添加其他具有服务用户和服务查看者角色的用户。接下来，您将用户添加为项目成员。项目成员可以开发和部署自己的云模板。
- 将云模板发布到目录，使其可供非开发人员部署。现在，您要为 Service Broker 分配用户角色。Service Broker 可为云模板使用者提供目录。您还可以使用该功能创建策略（包括租约和授权），但该功能不属于此用户角色用例。

## 前提条件

- 查看第一个用例。请参见[用户角色用例 1：设置 vRealize Automation 用户角色以支持小型应用开发团队](#)。
- 根据您希望用户拥有的权限来标识以下用户：
  - 将成为 vRealize Automation Cloud Assembly 用户和查看者的云模板开发人员
  - vRealize Automation Service Broker 管理员
  - 将以 vRealize Automation Service Broker 用户的身份成为目录使用者的非开发者用户

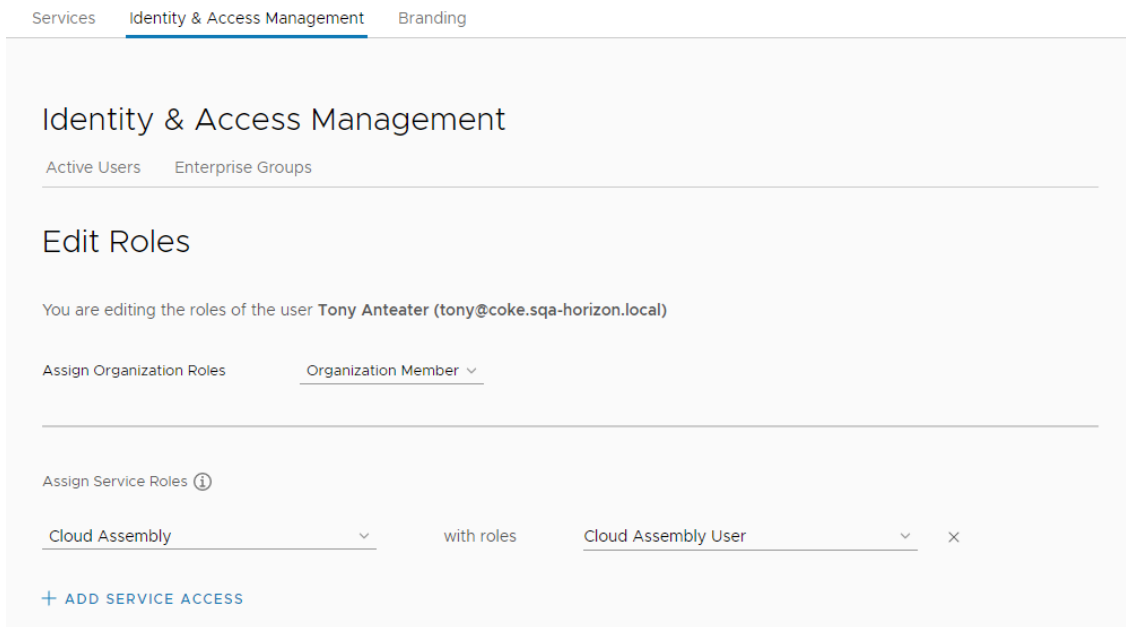
## 步骤

- 1 将组织成员角色分配给云模板开发人员用户。

如果您需要说明，请参见[用户角色用例 1：设置 vRealize Automation 用户角色以支持小型应用开发团队](#)。

## 2 将 vRealize Automation Cloud Assembly 服务成员角色分配给云模板开发人员。

### a 单击添加服务访问权限。



### b 使用以下值配置用户。

服务	角色
vRealize Automation Cloud Assembly	vRealize Automation Cloud Assembly 用户
vRealize Automation Cloud Assembly	vRealize Automation Cloud Assembly 查看者

在此用例中，开发人员需要查看基础架构，以确保他们正在构建可部署的云模板。您将在下一步中将他们分配为项目管理员和项目成员的用户，因此他们看不到基础架构。作为服务查看者，他们可以查看基础架构的配置方式，但不能进行任何更改。作为云管理员，您仍保留控制权，但授予他们访问开发云模板所需信息的权限。

## 3 在 vRealize Automation Cloud Assembly 中创建用于对资源用户进行分组的项目。

在此用例中，您创建两个项目。第一个项目是 PersonnelAppDev，第二个是 PayrollAppDev。

- 在控制台中，单击**服务**选项卡，然后单击 **Cloud Assembly**。
- 选择**基础架构 > 项目 > 新建项目**。
- 输入 **PersonnelAppDev** 作为名称。
- 单击**用户**，然后单击**添加用户**。

- e 添加项目成员并指定项目管理员。

项目角色	说明
项目用户	项目成员是项目中的主要开发人员用户角色。项目可在您准备好通过部署云模板来测试开发工作时确定可用的云资源。
项目管理员	项目管理员可通过为项目添加和移除用户来支持其开发人员。您还可以删除项目。要创建项目，您必须具有服务管理员特权。

- f 对于要添加为项目成员的用户，请输入每个用户的电子邮件地址（以逗号分隔），然后在**分配角色**下拉菜单中选择**用户**。

例如，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 对于指定的管理员，请在**分配角色**下拉菜单中选择**管理员**，然后提供必要的电子邮件地址。

- h 单击**置备**选项卡，然后添加一个或多个云区域。

当属于此项目的云模板开发人员部署模板时，模板将部署到云区域中的可用资源。您必须确保云区域资源符合项目开发团队模板的需求。

- i 重复此过程，以添加具有必要用户和管理员的 PayrollAppDev 项目。

- 4 向服务用户提供必要的登录信息，并验证每个项目的成员能否执行以下任务。

- 打开 vRealize Automation Cloud Assembly。
- 查看所有项目的基础架构。
- 为其所属的项目创建云模板。
- 将云模板部署到项目中定义的云区域资源。
- 管理其部署。

5 将组织成员角色分配给云模板开发人员用户。

如果您需要说明，请参见[用户角色用例 1：设置 vRealize Automation 用户角色以支持小型应用开发团队](#)。

6 根据目录管理员、目录使用者和云模板开发人员的工作向他们分配角色。

a 单击**添加服务访问权限**。

b 使用以下值配置目录管理员。

此角色可能是您（云管理员），也可能是应用程序开发团队中的其他人。

服务	角色
vRealize Automation Service Broker	vRealize Automation Service Broker 管理员

c 使用以下值配置云模板使用者。

服务	角色
vRealize Automation Service Broker	vRealize Automation Service Broker 用户

Identity & Access Management

Active Users Enterprise Groups

### Edit Roles

You are editing the roles of the user **Gloria Martinez (gloria@coke.sqa-horizon.local)**

Assign Organization Roles Organization Member ▼

---

Assign Service Roles ⓘ

Service Broker ▼ with roles Service Broker User ▼ ×

[+ ADD SERVICE ACCESS](#)

d 使用以下值配置云模板开发人员。

服务	角色
Cloud Assembly vRealize Automation Cloud Assembly	vRealize Automation Cloud Assembly 用户

7 在 vRealize Automation Cloud Assembly 中创建用于对资源和用户进行分组的项目。

在此用例中，您创建两个项目。第一个项目是 **PersonnelAppDev**，第二个是 **PayrollAppDev**。

如果您需要说明，请参见[用户角色用例 2：设置 vRealize Automation 用户角色以支持更大型的开发团队和目录](#)。

## 8 为每个项目团队创建和发布云模板。

如果您需要说明，请参见[用户角色用例 1：设置 vRealize Automation 用户角色以支持小型应用开发团队](#)。

## 9 将 vRealize Automation Cloud Assembly 云模板导入到 vRealize Automation Service Broker。

必须以具有 vRealize Automation Service Broker 管理员角色的用户身份登录。

- a 以具有 vRealize Automation Service Broker 管理员角色的用户身份登录。
- b 在控制台中，单击 vRealize Automation Service Broker。
- c 选择[内容和策略 > 内容源](#)，然后单击[新建](#)。

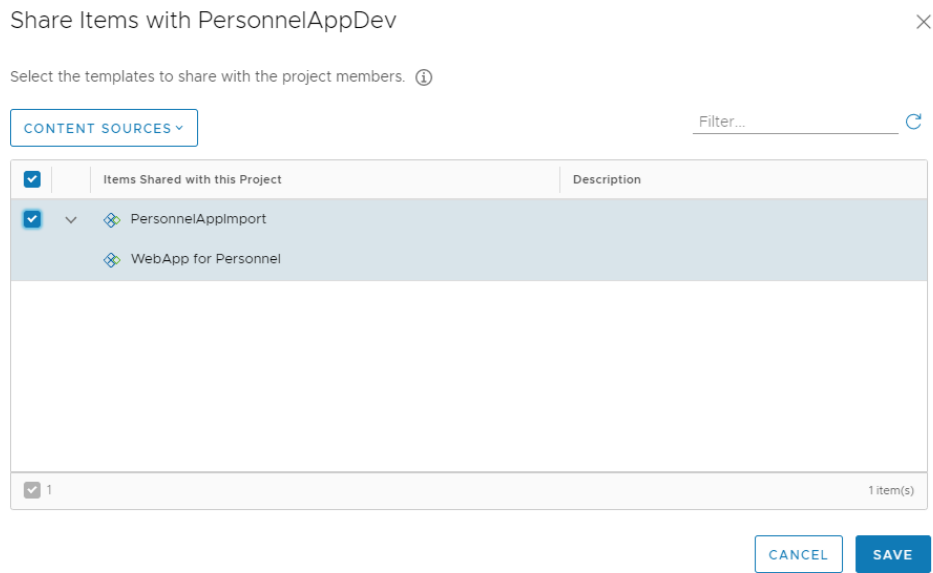
- d 选择 **Cloud Assembly** 云模板。
- e 输入 **PersonnelAppImport** 作为名称。
- f 在[源项目](#)下拉菜单中，选择“PersonnelAppDev”，然后单击[验证](#)。
- g 验证源后，单击[创建并导入](#)。
- h 使用 PayrollAppImport 作为内容源名称，对 PayrollAppDev 重复此过程。

## 10 与项目共享导入的云模板。

虽然云模板已与项目关联，但您可以在 vRealize Automation Service Broker 中共享该云模板，使其在目录中可用。

- a 以具有 vRealize Automation Service Broker 管理员角色的用户身份继续。
- b 在 vRealize Automation Service Broker 中，选择[内容和策略 > 内容共享](#)。
- c 选择 **PersonnelAppDev** 项目，其中包括必须能够从目录部署云模板的用户。

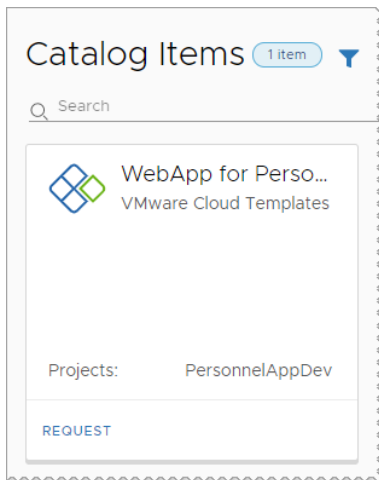
- d 单击**添加项**，然后选择 PersonnelApp 云模板以与项目成员共享。



- e 单击**保存**。

- 11 确认云模板在 vRealize Automation Service Broker 目录中可供项目成员使用。

- a 请求项目成员登录，然后单击**目录**选项卡。

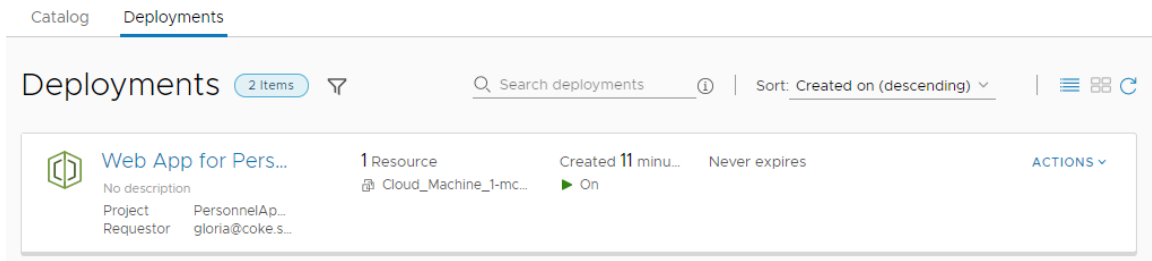


- b 单击 PersonnelApp 云模板卡视图上的“请求”。

- c 填写表单，然后单击**提交**。

## 12 确认项目成员可以监控部署过程。

- a 请求项目成员单击**部署**选项卡，然后找到其置备请求。



- b 部署云模板后，确认请求用户可以访问应用程序。

## 13 对其他项目重复此过程。

### 结果

在此用例中，您意识到需要将云模板开发工作委派给开发人员，因此添加了更多组织成员。您将他们设置为 **vRealize Automation Cloud Assembly** 用户。然后，您将他们设置为相关项目的成员，使其能够创建和部署云模板。项目成员无法查看或更改您继续管理的基础架构，但您授予其完整的服务查看者权限，因此他们知道所设计的基础架构的限制。

在此用例中，您可以配置具有各种角色的用户，包括 **vRealize Automation Service Broker** 管理员和用户。然后，向非开发人员用户提供 **vRealize Automation Service Broker** 目录。

### 后续步骤

要了解如何定义自定义角色并将其分配给用户，请参见[用户角色用例 3：设置 vRealize Automation 自定义用户角色以细化系统角色](#)。

## 用户角色用例 3：设置 vRealize Automation 自定义用户角色以细化系统角色

作为 **vRealize Automation** 组织所有者或服务管理员，您可以使用组织和服务系统角色管理用户访问。但是，您还希望为所选用户创建自定义角色，并执行任务或查看其系统角色之外的内容。

此方案假设您了解服务用户和查看者，以及用例 2 中定义的项目成员和查看者角色。您会发现，他们比用例 1 中使用的服务和项目管理员角色更受限。现在，您已经标识了某些本地用例，希望某些用户对某些功能具有完全管理权限和查看他人的权限，但是您不希望他们查看另一组功能。您可以使用自定义角色来定义这些权限。

此用例基于三个可能的本地用例。此过程说明了如何为以下自定义角色创建权限。

- **受限基础架构管理员。**您希望某些服务用户（而非服务管理员）具有更广泛的基础架构权限。作为管理员，您希望他们能够帮助设置云区域、映像和特定实例。您还希望他们能够载入和管理已发现的资源。请注意，他们不能添加云帐户或集成，只能为这些端点定义基础架构。
- **可扩展性开发人员。**您希望某些服务用户拥有完整权限，以便在为项目团队和其他项目开发云模板的过程中使用可扩展性操作和订阅。他们还将为多个项目开发自定义资源类型和自定义操作。
- **XaaS 开发人员。**您希望某些服务用户具有完全权限，以便为多个项目开发自定义资源类型和自定义操作。

- 部署故障排除人员。您希望您的项目管理员具有对失败的部署进行故障排除和执行根本原因分析的权限。您可以为他们提供对非破坏性或较低成本的类别（如映像和特定实例映射）的管理权限。您还希望项目管理员有权设置批准和实施后策略，这是失败部署故障排除角色的一部分权限。

### 前提条件

- 查看 [vRealize Automation 用户角色是什么](#) 中的 vRealize Automation Cloud Assembly 和 vRealize Automation Service Broker 服务角色和项目角色表。您必须了解每个服务用户角色可在这些服务中查看的内容和执行的操作。
- 查看 [vRealize Automation 中的自定义用户角色说明](#)，了解有关如何细化用户权限的更多信息。
- 查看第一个用例，以便了解组织角色和服务管理员角色。请参见 [用户角色用例 1：设置 vRealize Automation 用户角色以支持小型应用开发团队](#)。
- 查看第二个用例，帮助您了解服务用户和项目成员角色。请参见 [用户角色用例 2：设置 vRealize Automation 用户角色以支持更大型的开发团队和目录](#)。
- 熟悉 vRealize Automation Service Broker。请参见 [将内容添加到目录](#)。

### 步骤

- 1 将组织成员角色分配给云模板开发人员用户。  
如果您需要说明，请参见 [用户角色用例 1：设置 vRealize Automation 用户角色以支持小型应用开发团队](#)。
- 2 为云模板开发人员和目录使用者分配 vRealize Automation Cloud Assembly 和 vRealize Automation Service Broker 服务角色。  
如果您需要说明，请参见 [用户角色用例 2：设置 vRealize Automation 用户角色以支持更大型的开发团队和目录](#)。
- 3 在 vRealize Automation Cloud Assembly 中创建用于对资源和用户进行分组的项目。  
以下针对自定义角色的步骤还包括项目角色。  
如果您需要有关创建项目的说明，请参见 [用户角色用例 2：设置 vRealize Automation 用户角色以支持更大型的开发团队和目录](#)。
- 4 为每个项目团队创建和发布云模板。  
如果您需要说明，请参见 [用户角色用例 1：设置 vRealize Automation 用户角色以支持小型应用开发团队](#)。
- 5 以服务管理员身份登录到 vRealize Automation Cloud Assembly，然后选择 **基础架构 > 管理 > 自定义角色**。



## 6 创建受限的基础架构管理员角色。

在本示例中，您有一个擅长为各种项目设置基础架构的用户 **Tony**，但您不希望授予他全部服务权限。**Tony** 构建的核心基础架构支持所有项目工作。您可以为其提供有限的基础架构管理权限。**Tony** 或外部承包商可能还具有类似的权限，可用于载入发现的计算机并将其纳入 vRealize Automation 管理范围。

- a 将 **Tony** 作为服务用户和查看者添加到 vRealize Automation Cloud Assembly。

他拥有查看者权限，因此如果他需要对其工作进行故障排除，则可以查看底层云帐户和集成，但无法进行更改。

- b 创建项目并将 **Tony** 添加为项目成员。

- c 要创建自定义角色，请选择**基础架构 > 管理 > 自定义角色**，然后单击**新建自定义角色**。

- d 输入名称 **Restricted Infrastructure Administrator**，然后选择以下权限。

选择此权限...	用户可以...
基础架构 > 管理云区域	创建、更新和删除云区域。
基础架构 > 管理特定实例映射	创建、更新和删除特定实例映射。
基础架构 > 管理映像映射	创建、更新和删除映像映射。

- e 单击**创建**。

- f 在“自定义角色”页面上，选择 **Restricted Infrastructure Administrator** 角色，然后单击**分配**。

- g 输入 **Tony** 的电子邮件帐户，然后单击**添加**。

例如，输入 **Tony@yourcompany.com**。

您也可以输入任何已定义的 **Active Directory** 用户组。

- h 让 **Tony** 确认登录后能够在自定义角色定义的区域中添加、编辑和删除值。

## 7 创建可扩展性开发人员角色。

在本示例中，您有多个云模板开发人员（**Sylvia** 和 **Igor**），他们熟悉如何使用可扩展性操作和订阅来管理日常开发任务。他们也熟知 vRealize Orchestrator，因此可以完成为各种项目提供自定义资源和操作的任务。您可以通过管理自定义资源和操作以及管理可扩展性操作和订阅，为他们提供其他权限来管理可扩展性。

- a 将 **Sylvia** 和 **Igor** 添加为 vRealize Automation Cloud Assembly 用户。

- b 在他们发挥可扩展性技能的项目中将他们添加为项目成员。

- c 创建自定义用户角色并命名为 **Extensibility Developer**，然后选择以下权限。

选择此权限...	用户可以...
XaaS > 管理自定义资源	创建、更新或删除自定义资源。
XaaS > 管理资源操作	创建、更新或删除自定义操作。
可扩展性 > 管理可扩展性资源	创建、更新或删除可扩展性操作和订阅。禁用订阅。取消和删除操作运行。

- d 单击**创建**。
- e 将 Sylvia 和 Igor 分配给 Extensibility Developer 角色。
- f 确认 Sylvia 和 Igor 能够管理自定义资源和操作，且能够管理“可扩展性”选项卡上的各个选项。

## 8 创建部署故障排除人员角色。

在本示例中，您为项目管理员提供了更多管理权限，以便他们可以修复其团队的部署失败问题。

- a 将项目管理员、Shauna、Pratap 和 Wei 添加为 vRealize Automation Cloud Assembly 和 vRealize Automation Service Broker 服务用户。
- b 在他们的项目中，将他们添加为项目管理员。
- c 创建一个自定义用户角色，并将其命名为 **部署故障排除人员**，并选择以下权限。

选择此权限...	用户可以...
基础架构 > 管理特定实例映射	创建、更新和删除特定实例映射。
基础架构 > 管理映像映射	创建、更新和删除映像映射。
部署 > 管理部署	跨项目查看所有部署以及对部署和部署组件运行实施后操作。
策略 > 管理策略	创建、更新或删除策略定义。

- d 单击**创建**。
- e 将 Shauna、Pratap 和 Wei 分配到部署故障排除人员角色。
- f 验证他们是否可以在 vRealize Automation Service Broker 中管理特定实例映射、映像映射和策略。

## 结果

在此用例中，您可以配置具有各种角色的不同用户，包括扩展其服务和项目角色的自定义角色。

## 后续步骤

创建满足您的本地用例要求的自定义角色。

# 将云帐户添加到 vRealize Automation Cloud Assembly

云帐户是已配置的权限，vRealize Automation Cloud Assembly 可使用此权限从区域或数据中心收集数据并将云模板部署到这些区域。

收集的数据包括您稍后与云区域关联的区域。

稍后配置云区域、映射和配置文件时，可以选择与其关联的云帐户。

作为云管理员，您可以为项目创建云帐户，以便团队成员可以使用这些云帐户进行工作。将从云帐户收集网络 and 安全性、计算资源、存储以及标记内容等资源信息的数据。

**注** 如果云帐户具有已在区域中部署的关联计算机，则可以使用载入计划将这些计算机载入到 vRealize Automation Cloud Assembly 中进行管理。请参见 [vRealize Automation Cloud Assembly 中的载入计划是什么](#)。

如果移除部署中使用的云帐户，则属于该部署的资源将变为非受管。

## 在 vRealize Automation 中使用云帐户所需的凭据

要在 vRealize Automation 中配置和使用云帐户，请确认您具有以下凭据。

### 所需的云帐户凭据

要执行的操作...	所需内容 ...
注册并登录到 vRealize Automation Cloud Assembly	VMware ID。 <ul style="list-style-type: none"> <li>■ 使用公司电子邮件地址设置 <a href="#">My VMware</a> 帐户。</li> </ul>
连接到 vRealize Automation 服务	对出站流量打开并具有透过防火墙对以下域的访问权限的 HTTPS 端口 443: <ul style="list-style-type: none"> <li>■ *.vmwareidentity.com</li> <li>■ gaz.csp-vidm-prod.com</li> <li>■ *.vmware.com</li> </ul> 有关端口和协议的详细信息，请参见 <a href="#">VMware 端口和协议</a> 。 有关所需端口和协议的相关信息，请参见 <a href="#">端口要求</a> 。

要执行的操作...	所需内容 ...
添加 Amazon Web Services (AWS) 云帐户	<p>提供具有读取和写入权限的超级用户帐户。用户帐户必须是 AWS 标识与访问管理 (IAM) 系统中的电源访问策略 (PowerUserAccess) 的成员。</p> <ul style="list-style-type: none"> <li>■ 20 位访问密钥 ID 和相应的私有访问密钥</li> </ul> <p>如果您使用的是外部 HTTP Internet 代理，则必须针对 IPv4 对其进行配置。</p> <p>vRealize Automation 基于操作的可扩展性 (ABX) 和外部 IPAM 集成可能需要额外的权限。</p> <p>要允许 Auto Scaling 功能，建议具备以下 AWS 权限：</p> <ul style="list-style-type: none"> <li>■ Auto Scaling 操作： <ul style="list-style-type: none"> <li>■ autoscaling:DescribeAutoScalingInstances</li> <li>■ autoscaling:AttachInstances</li> <li>■ autoscaling&gt;DeleteLaunchConfiguration</li> <li>■ autoscaling:DescribeAutoScalingGroups</li> <li>■ autoscaling&gt;CreateAutoScalingGroup</li> <li>■ autoscaling:UpdateAutoScalingGroup</li> <li>■ autoscaling&gt;DeleteAutoScalingGroup</li> <li>■ autoscaling:DescribeLoadBalancers</li> </ul> </li> <li>■ Auto Scaling 资源： <ul style="list-style-type: none"> <li>■ *</li> </ul> <p>提供所有 Auto Scaling 资源权限。</p> </li> </ul> <p>要允许 AWS Security Token Service (AWS STS) 功能对 AWS 身份和访问支持临时、有限特权凭据，需要具备以下权限：</p> <ul style="list-style-type: none"> <li>■ AWS STS 资源： <ul style="list-style-type: none"> <li>■ *</li> </ul> <p>提供所有 STS 资源权限。</p> </li> </ul> <p>要允许 EC2 功能，需要具备以下 AWS 权限：</p> <ul style="list-style-type: none"> <li>■ EC2 操作： <ul style="list-style-type: none"> <li>■ ec2:AttachVolume</li> <li>■ ec2:AuthorizeSecurityGroupIngress</li> <li>■ ec2&gt;DeleteSubnet</li> <li>■ ec2&gt;DeleteSnapshot</li> <li>■ ec2:DescribeInstances</li> <li>■ ec2&gt;DeleteTags</li> <li>■ ec2:DescribeRegions</li> <li>■ ec2:DescribeVolumesModifications</li> <li>■ ec2&gt;CreateVpc</li> <li>■ ec2:DescribeSnapshots</li> <li>■ ec2:DescribeInternetGateways</li> <li>■ ec2&gt;DeleteVolume</li> <li>■ ec2:DescribeNetworkInterfaces</li> <li>■ ec2:StartInstances</li> <li>■ ec2:DescribeAvailabilityZones</li> <li>■ ec2:CreateInternetGateway</li> <li>■ ec2:CreateSecurityGroup</li> <li>■ ec2:DescribeVolumes</li> <li>■ ec2&gt;CreateSnapshot</li> </ul> </li> </ul>

## 要执行的操作...

## 所需内容 ...

- 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

[注](#) vRealize Automation 基于操作的可扩展性 (ABX) 或外部 IPAM 集成不需要 SpotFleet 请求权限。

- EC2 资源:

- \*

提供所有 EC2 资源权限。

要允许弹性负载均衡功能，需要具备以下 AWS 权限：

- 负载均衡器操作：

- elasticloadbalancing:DeleteLoadBalancer
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:RemoveTags
- elasticloadbalancing:CreateLoadBalancer
- elasticloadbalancing:DescribeTags
- elasticloadbalancing:ConfigureHealthCheck
- elasticloadbalancing:AddTags
- elasticloadbalancing:CreateTargetGroup
- elasticloadbalancing>DeleteLoadBalancerListeners
- elasticloadbalancing:DeregisterInstancesFromLoadBalancer
- elasticloadbalancing:RegisterInstancesWithLoadBalancer

**要执行的操作...****所需内容 ...**

- elasticloadbalancing:CreateLoadBalancerListeners
- 负载均衡器资源:
  - \*

提供所有负载均衡器资源权限。

可以启用以下 AWS 身份与访问管理 (IAM) 权限，但这些权限不是必需权限：

- iam:SimulateCustomPolicy
- iam:GetUser
- iam:ListUserPolicies
- iam:GetUserPolicy
- iam:ListAttachedUserPolicies
- iam:GetPolicyVersion
- iam:ListGroupsForUser
- iam:ListGroupPolicies
- iam:GetGroupPolicy
- iam:ListAttachedGroupPolicies
- iam:ListPolicyVersions

要执行的操作...	所需内容 ...
添加 Microsoft Azure 云帐户	<p>配置 Microsoft Azure 实例，并获取可以在其中使用订阅 ID 的有效 Microsoft Azure 订阅。</p> <p>按照 Microsoft Azure 产品文档中的<a href="#">如何：使用门户创建可访问资源的 Azure AD 应用程序和服务主体</a>所述创建 Active Directory 应用程序。</p> <p>如果您使用的是外部 HTTP Internet 代理，则必须针对 IPv4 对其进行配置。</p> <p>记录以下信息：</p> <ul style="list-style-type: none"> <li>■ 订阅 ID <ul style="list-style-type: none"> <li>允许您访问 Microsoft Azure 订阅。</li> </ul> </li> <li>■ 租户 ID <ul style="list-style-type: none"> <li>在 Microsoft Azure 帐户中创建的 Active Directory 应用程序的授权端点。</li> </ul> </li> <li>■ 客户端应用程序 ID <ul style="list-style-type: none"> <li>用于访问 Microsoft Azure 个人帐户中的 Microsoft Active Directory。</li> </ul> </li> <li>■ 客户端应用程序密钥 <ul style="list-style-type: none"> <li>生成的唯一的密钥，用于与客户端应用程序 ID 配对。</li> </ul> </li> </ul> <p>创建和验证 Microsoft Azure 云帐户需要以下权限：</p> <ul style="list-style-type: none"> <li>■ Microsoft 计算 <ul style="list-style-type: none"> <li>■ Microsoft.Compute/virtualMachines/extensions/write</li> <li>■ Microsoft.Compute/virtualMachines/extensions/read</li> <li>■ Microsoft.Compute/virtualMachines/extensions/delete</li> <li>■ Microsoft.Compute/virtualMachines/deallocate/action</li> <li>■ Microsoft.Compute/virtualMachines/delete</li> <li>■ Microsoft.Compute/virtualMachines/powerOff/action</li> <li>■ Microsoft.Compute/virtualMachines/read</li> <li>■ Microsoft.Compute/virtualMachines/restart/action</li> <li>■ Microsoft.Compute/virtualMachines/start/action</li> <li>■ Microsoft.Compute/virtualMachines/write</li> <li>■ Microsoft.Compute/availabilitySets/write</li> <li>■ Microsoft.Compute/availabilitySets/read</li> <li>■ Microsoft.Compute/availabilitySets/delete</li> <li>■ Microsoft.Compute/disks/delete</li> <li>■ Microsoft.Compute/disks/read</li> <li>■ Microsoft.Compute/disks/write</li> </ul> </li> <li>■ Microsoft 网络 <ul style="list-style-type: none"> <li>■ Microsoft.Network/loadBalancers/backendAddressPools/join/action</li> <li>■ Microsoft.Network/loadBalancers/delete</li> <li>■ Microsoft.Network/loadBalancers/read</li> <li>■ Microsoft.Network/loadBalancers/write</li> <li>■ Microsoft.Network/networkInterfaces/join/action</li> <li>■ Microsoft.Network/networkInterfaces/read</li> <li>■ Microsoft.Network/networkInterfaces/write</li> <li>■ Microsoft.Network/networkInterfaces/delete</li> <li>■ Microsoft.Network/networkSecurityGroups/join/action</li> <li>■ Microsoft.Network/networkSecurityGroups/read</li> <li>■ Microsoft.Network/networkSecurityGroups/write</li> </ul> </li> </ul>

要执行的操作...	所需内容 ...
	<ul style="list-style-type: none"> <li>■ Microsoft.Network/networkSecurityGroups/delete</li> <li>■ Microsoft.Network/publicIPAddresses/delete</li> <li>■ Microsoft.Network/publicIPAddresses/join/action</li> <li>■ Microsoft.Network/publicIPAddresses/read</li> <li>■ Microsoft.Network/publicIPAddresses/write</li> <li>■ Microsoft.Network/virtualNetworks/read</li> <li>■ Microsoft.Network/virtualNetworks/subnets/delete</li> <li>■ Microsoft.Network/virtualNetworks/subnets/join/action</li> <li>■ Microsoft.Network/virtualNetworks/subnets/read</li> <li>■ Microsoft.Network/virtualNetworks/subnets/write</li> <li>■ Microsoft.Network/virtualNetworks/write</li> <li>■ Microsoft 资源 <ul style="list-style-type: none"> <li>■ Microsoft.Resources/subscriptions/resourcegroups/delete</li> <li>■ Microsoft.Resources/subscriptions/resourcegroups/read</li> <li>■ Microsoft.Resources/subscriptions/resourcegroups/write</li> </ul> </li> <li>■ Microsoft 存储 <ul style="list-style-type: none"> <li>■ Microsoft.Storage/storageAccounts/delete</li> <li>■ Microsoft.Storage/storageAccounts/listKeys/action</li> <li>■ Microsoft.Storage/storageAccounts/read</li> <li>■ Microsoft.Storage/storageAccounts/write</li> </ul> </li> <li>■ Microsoft Web <ul style="list-style-type: none"> <li>■ Microsoft.Web/sites/read</li> <li>■ Microsoft.Web/sites/write</li> <li>■ Microsoft.Web/sites/delete</li> <li>■ Microsoft.Web/sites/config/read</li> <li>■ Microsoft.Web/sites/config/write</li> <li>■ Microsoft.Web/sites/config/list/action</li> <li>■ Microsoft.Web/sites/publishxml/action</li> <li>■ Microsoft.Web/serverfarms/write</li> <li>■ Microsoft.Web/serverfarms/delete</li> <li>■ Microsoft.Web/sites/hostruntime/functions/keys/read</li> <li>■ Microsoft.Web/sites/hostruntime/host/read</li> <li>■ Microsoft.web/sites/functions/masterkey/read</li> </ul> </li> </ul>
	<p>如果要将 Microsoft Azure 与基于操作的可扩展性配合使用，除了最小权限外，还需要以下权限：</p> <ul style="list-style-type: none"> <li>■ Microsoft.Web/sites/read</li> <li>■ Microsoft.Web/sites/write</li> <li>■ Microsoft.Web/sites/delete</li> <li>■ Microsoft.Web/sites/*/action</li> <li>■ Microsoft.Web/sites/config/read</li> <li>■ Microsoft.Web/sites/config/write</li> <li>■ Microsoft.Web/sites/config/list/action</li> <li>■ Microsoft.Web/sites/publishxml/action</li> <li>■ Microsoft.Web/serverfarms/write</li> <li>■ Microsoft.Web/serverfarms/delete</li> </ul>



**要执行的操作...****所需内容 ...**

- 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

如果要与 Microsoft Azure 一起使用包含扩展的可扩展性，还需要以下权限：

- Microsoft.Compute/virtualMachines/extensions/write
- Microsoft.Compute/virtualMachines/extensions/read
- Microsoft.Compute/virtualMachines/extensions/delete

要执行的操作...	所需内容 ...
添加 Google Cloud Platform (GCP) 云帐户	<p>Google Cloud Platform 云帐户与 Google Cloud Platform 计算引擎交互。</p> <p>创建和验证 Google Cloud Platform 云帐户需要项目管理员和所有者凭据。</p> <p>如果您使用的是外部 HTTP Internet 代理，则必须针对 IPv4 对其进行配置。</p> <p>必须启用计算引擎服务。在 vRealize Automation 中创建云帐户时，请使用在初始化计算引擎时创建的服务帐户。</p> <p>还需要以下计算引擎权限，具体取决于用户可以执行的操作：</p> <ul style="list-style-type: none"> <li>■ roles/compute.admin <ul style="list-style-type: none"> <li>用于完全控制所有计算引擎资源。</li> </ul> </li> <li>■ roles/iam.serviceAccountUser <ul style="list-style-type: none"> <li>用于访问管理已配置为作为服务帐户运行的虚拟机实例的用户。授予对以下资源和服务的访问权限： <ul style="list-style-type: none"> <li>■ compute.*</li> <li>■ resourceManager.projects.get</li> <li>■ resourceManager.projects.list</li> <li>■ serviceUsage.quotas.get</li> <li>■ serviceUsage.services.get</li> <li>■ serviceUsage.services.list</li> </ul> </li> </ul> </li> <li>■ roles/compute.imageUser <ul style="list-style-type: none"> <li>提供列出和读取映像的权限，而无需对映像具有其他权限。在项目级别授予 compute.imageUser 角色，使用户能够列出项目中的所有映像。它还允许用户根据项目中的映像创建实例和永久磁盘等资源。 <ul style="list-style-type: none"> <li>■ compute.images.get</li> <li>■ compute.images.getFromFamily</li> <li>■ compute.images.list</li> <li>■ compute.images.useReadOnly</li> <li>■ resourceManager.projects.get</li> <li>■ resourceManager.projects.list</li> <li>■ serviceUsage.quotas.get</li> <li>■ serviceUsage.services.get</li> <li>■ serviceUsage.services.list</li> </ul> </li> </ul> </li> <li>■ roles/compute.instanceAdmin <ul style="list-style-type: none"> <li>提供创建、修改和删除虚拟机实例的权限。这包括创建、修改和删除磁盘以及配置受防护 VMBETA 设置的权限。</li> <li>对于管理虚拟机实例（但不是网络或安全设置或作为服务帐户运行的实例）的用户，将此角色授予包含实例的组织、文件夹或项目，或者授予单个实例。</li> <li>管理已配置为作为服务帐户运行的虚拟机实例的用户还需要 roles/iam.serviceAccountUser 角色。 <ul style="list-style-type: none"> <li>■ compute.acceleratorTypes</li> <li>■ compute.addresses.get</li> <li>■ compute.addresses.list</li> <li>■ compute.addresses.use</li> <li>■ compute.autoscalers</li> <li>■ compute.diskTypes</li> <li>■ compute.disks.create</li> <li>■ compute.disks.createSnapshot</li> <li>■ compute.disks.delete</li> <li>■ compute.disks.get</li> </ul> </li> </ul> </li> </ul>

## 要执行的操作...

## 所需内容 ...

- compute.disks.list
- compute.disks.resize
- compute.disks.setLabels
- compute.disks.update
- compute.disks.use
- compute.disks.useReadOnly
- compute.globalAddresses.get
- compute.globalAddresses.list
- compute.globalAddresses.use
- compute.globalOperations.get
- compute.globalOperations.list
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instanceGroupManagers
- compute.instanceGroups
- compute.instanceTemplates
- compute.instances
- compute.licenses.get
- compute.licenses.list
- compute.machineTypes
- compute.networkEndpointGroups
- compute.networks.get
- compute.networks.list
- compute.networks.use
- compute.networks.useExternallp
- compute.projects.get
- compute.regionOperations.get
- compute.regionOperations.list
- compute.regions
- compute.reservations.get
- compute.reservations.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternallp
- compute.targetPools.get
- compute.targetPools.list
- compute.zoneOperations.get
- compute.zoneOperations.list
- compute.zones
- resourcemanager.projects.get
- resourcemanager.projects.list

要执行的操作...	所需内容 ...
	<ul style="list-style-type: none"> <li>■ serviceusage.quotas.get</li> <li>■ serviceusage.services.get</li> <li>■ serviceusage.services.list</li> <li>■ roles/compute.instanceAdmin.v1</li> </ul> <p>用于完全控制计算引擎实例、实例组、磁盘、快照和映像。还提供对所有计算引擎网络资源的读取访问权限。</p> <hr/> <p><b>注</b> 如果在实例级别为用户授予此角色，则该用户无法创建新的实例。</p> <hr/> <ul style="list-style-type: none"> <li>■ compute.acceleratorTypes</li> <li>■ compute.addresses.get</li> <li>■ compute.addresses.list</li> <li>■ compute.addresses.use</li> <li>■ compute.autoscalers</li> <li>■ compute.backendBuckets.get</li> <li>■ compute.backendBuckets.list</li> <li>■ compute.backendServices.get</li> <li>■ compute.backendServices.list</li> <li>■ compute.diskTypes</li> <li>■ compute.disks</li> <li>■ compute.firewalls.get</li> <li>■ compute.firewalls.list</li> <li>■ compute.forwardingRules.get</li> <li>■ compute.forwardingRules.list</li> <li>■ compute.globalAddresses.get</li> <li>■ compute.globalAddresses.list</li> <li>■ compute.globalAddresses.use</li> <li>■ compute.globalForwardingRules.get</li> <li>■ compute.globalForwardingRules.list</li> <li>■ compute.globalOperations.get</li> <li>■ compute.globalOperations.list</li> <li>■ compute.healthChecks.get</li> <li>■ compute.healthChecks.list</li> <li>■ compute.httpHealthChecks.get</li> <li>■ compute.httpHealthChecks.list</li> <li>■ compute.httpsHealthChecks.get</li> <li>■ compute.httpsHealthChecks.list</li> <li>■ compute.images</li> <li>■ compute.instanceGroupManagers</li> <li>■ compute.instanceGroups</li> <li>■ compute.instanceTemplates</li> <li>■ compute.instances</li> <li>■ compute.interconnectAttachments.get</li> <li>■ compute.interconnectAttachments.list</li> <li>■ compute.interconnectLocations</li> <li>■ compute.interconnects.get</li> </ul>

要执行的操作...	所需内容 ...
	<ul style="list-style-type: none"> <li>■ compute.interconnects.list</li> <li>■ compute.licenseCodes</li> <li>■ compute.licenses</li> <li>■ compute.machineTypes</li> <li>■ compute.networkEndpointGroups</li> <li>■ compute.networks.get</li> <li>■ compute.networks.list</li> <li>■ compute.networks.use</li> <li>■ compute.networks.useExternallp</li> <li>■ compute.projects.get</li> <li>■ compute.projects.setCommonInstanceMetadata</li> <li>■ compute.regionBackendServices.get</li> <li>■ compute.regionBackendServices.list</li> <li>■ compute.regionOperations.get</li> <li>■ compute.regionOperations.list</li> <li>■ compute.regions</li> <li>■ compute.reservations.get</li> <li>■ compute.reservations.list</li> <li>■ compute.resourcePolicies</li> <li>■ compute.routers.get</li> <li>■ compute.routers.list</li> <li>■ compute.routes.get</li> <li>■ compute.routes.list</li> <li>■ compute.snapshots</li> <li>■ compute.sslCertificates.get</li> <li>■ compute.sslCertificates.list</li> <li>■ compute.sslPolicies.get</li> <li>■ compute.sslPolicies.list</li> <li>■ compute.sslPolicies.listAvailableFeatures</li> <li>■ compute.subnetworks.get</li> <li>■ compute.subnetworks.list</li> <li>■ compute.subnetworks.use</li> <li>■ compute.subnetworks.useExternallp</li> <li>■ compute.targetHttpProxies.get</li> <li>■ compute.targetHttpProxies.list</li> <li>■ compute.targetHttpsProxies.get</li> <li>■ compute.targetHttpsProxies.list</li> <li>■ compute.targetInstances.get</li> <li>■ compute.targetInstances.list</li> <li>■ compute.targetPools.get</li> <li>■ compute.targetPools.list</li> <li>■ compute.targetSslProxies.get</li> <li>■ compute.targetSslProxies.list</li> <li>■ compute.targetTcpProxies.get</li> </ul>

要执行的操作...	所需内容 ...
	<ul style="list-style-type: none"> <li>■ compute.targetTcpProxies.list</li> <li>■ compute.targetVpnGateways.get</li> <li>■ compute.targetVpnGateways.list</li> <li>■ compute.urlMaps.get</li> <li>■ compute.urlMaps.list</li> <li>■ compute.vpnTunnels.get</li> <li>■ compute.vpnTunnels.list</li> <li>■ compute.zoneOperations.get</li> <li>■ compute.zoneOperations.list</li> <li>■ compute.zones</li> <li>■ resourceManager.projects.get</li> <li>■ resourceManager.projects.list</li> <li>■ serviceusage.quotas.get</li> <li>■ serviceusage.services.get</li> <li>■ serviceusage.services.list</li> </ul>
添加 NSX-T 云帐户	<p>提供具有以下读取和写入权限的帐户：</p> <ul style="list-style-type: none"> <li>■ NSX-T 企业级管理员角色和访问凭据</li> <li>■ NSX-T IP 地址或 FQDN</li> </ul> <p>管理员还需要访问 vCenter Server，如此页面上以下“基于 vCenter 的云帐户的 vSphere 代理要求”部分中所述。</p>
添加 NSX-V 云帐户	<p>提供具有以下读取和写入权限的帐户：</p> <ul style="list-style-type: none"> <li>■ NSX-V 企业级管理员角色和访问凭据</li> <li>■ NSX-V IP 地址或 FQDN</li> </ul> <p>管理员还需要访问 vCenter Server，如此页面上以下“基于 vCenter 的云帐户的 vSphere 代理要求”部分中所述。</p>
添加 vCenter 云帐户	<p>提供具有以下读取和写入权限的帐户：</p> <ul style="list-style-type: none"> <li>■ vCenter IP 地址或 FQDN</li> </ul> <p>管理员还需要访问 vCenter Server，如此页面上以下“基于 vCenter 的云帐户的 vSphere 代理要求”部分中所述。</p>
添加 VMware Cloud on AWS (VMC) 云帐户	<p>提供具有以下读取和写入权限的帐户：</p> <ul style="list-style-type: none"> <li>■ cloudadmin@vmc.local 帐户或 CloudAdmin 组中的任何用户帐户</li> <li>■ NSX 企业级管理员角色和访问凭据</li> <li>■ 对您组织的 VMware Cloud on AWS SDDC 环境的 NSX 云管理员访问权限</li> <li>■ 对您组织的 VMware Cloud on AWS SDDC 环境的管理员访问权限</li> <li>■ 您组织的 VMware Cloud on AWS 服务中的 VMware Cloud on AWS 环境的 VMware Cloud on AWS API 令牌</li> <li>■ vCenter IP 地址或 FQDN</li> </ul> <p>管理员还需要访问您的目标 VMware Cloud on AWS SDDC 使用的 vCenter，它具有本页以下“基于 vSphere 的云帐户的 vCenter 代理要求”部分中列出的所有权限。</p> <p>有关创建和使用 VMware Cloud on AWS 云帐户所需的权限的详细信息，请参见 <a href="#">VMware Cloud on AWS 产品文档</a> 中的管理 VMware Cloud on AWS 数据中心。</p>

## 基于 vCenter 的云帐户的 vSphere 代理要求

下表列出了管理 VMware Cloud on AWS 和 vCenter 云帐户所需的权限。必须对 vCenter Server 中的所有集群启用这些权限，而不仅仅是托管端点的集群。

对于所有基于 vCenter Server 的云帐户（包括 NSX-V、NSX-T、vCenter 和 VMware Cloud on AWS），管理员必须拥有 vSphere 端点凭据，或者在 vCenter 中运行代理服务的凭据，从而提供对主机 vCenter Server 的管理访问权限。

有关 vSphere 代理要求的详细信息，请参见 [VMware vSphere 产品文档](#)。

**表 3-12. vSphere 代理管理 vCenter Server 实例所需的权限**

属性值	权限
数据存储	<ul style="list-style-type: none"> <li>■ 分配空间</li> <li>■ 浏览数据存储</li> <li>■ 低级别文件操作</li> </ul>
数据存储集群	配置数据存储集群
文件夹	<ul style="list-style-type: none"> <li>■ 创建文件夹</li> <li>■ 删除文件夹</li> </ul>
全局	<ul style="list-style-type: none"> <li>■ 管理自定义属性</li> <li>■ 设置自定义属性</li> </ul>
网络	分配网络
权限	修改权限
资源	<ul style="list-style-type: none"> <li>■ 将虚拟机分配给资源池</li> <li>■ 迁移已关闭电源的虚拟机</li> <li>■ 迁移已打开电源的虚拟机</li> </ul>

表 3-12. vSphere 代理管理 vCenter Server 实例所需的权限（续）

属性值	权限
内容库	<p>要分配内容库的权限，管理员必须将该权限作为全局权限授予用户。有关相关信息，请参见位于 <a href="#">VMware vSphere 文档</a> 内《vSphere 虚拟机管理》中的<a href="#">内容库权限的层次结构继承</a>。</p> <ul style="list-style-type: none"> <li>■ 添加库项目</li> <li>■ 创建本地库</li> <li>■ 创建已订阅库</li> <li>■ 删除库项目</li> <li>■ 删除本地库</li> <li>■ 删除已订阅库</li> <li>■ 下载文件</li> <li>■ 逐出库项目</li> <li>■ 逐出已订阅库</li> <li>■ 探查订阅信息</li> <li>■ 读取存储</li> <li>■ 同步库项目</li> <li>■ 同步已订阅库</li> <li>■ 类型自检</li> <li>■ 更新配置设置</li> <li>■ 更新文件</li> <li>■ 更新库</li> <li>■ 更新库项目</li> <li>■ 更新本地库</li> <li>■ 更新已订阅库</li> <li>■ 查看配置设置</li> </ul>
标记	<ul style="list-style-type: none"> <li>■ 分配或取消分配 vSphere 标记</li> <li>■ 创建 vSphere 标记</li> <li>■ 创建 vSphere 标记类别</li> <li>■ 删除 vSphere 标记</li> <li>■ 删除 vSphere 标记类别</li> <li>■ 标记 vSphere 标记</li> <li>■ 编辑 vSphere 标记类别</li> <li>■ 修改类别的使用者字段</li> <li>■ 修改标记的使用者字段</li> </ul>
vApp	<ul style="list-style-type: none"> <li>■ 导入</li> <li>■ vApp 应用程序配置</li> </ul> <p>OVF 模板以及从内容库置备虚拟机时都需要使用 <code>vApp.Import</code> 应用程序配置。</p> <p>使用 <code>cloud-init</code> 执行云配置脚本时，需要 <code>vApp.vApp</code> 应用程序配置。此设置允许修改 vApp 的内部结构，例如产品信息和属性。</p>
虚拟机 - 清单	<ul style="list-style-type: none"> <li>■ 从现有项创建</li> <li>■ 新建</li> <li>■ 移动</li> <li>■ 移除</li> </ul>



表 3-12. vSphere 代理管理 vCenter Server 实例所需的权限（续）

属性值	权限
虚拟机 - 交互	<ul style="list-style-type: none"> <li>■ 配置 CD 媒体</li> <li>■ 控制台交互</li> <li>■ 设备连接</li> <li>■ 关闭电源</li> <li>■ 打开电源</li> <li>■ 重置</li> <li>■ 挂起</li> <li>■ 工具安装</li> </ul>
虚拟机 - 配置	<ul style="list-style-type: none"> <li>■ 添加现有磁盘</li> <li>■ 添加新磁盘</li> <li>■ 移除磁盘</li> <li>■ 高级</li> <li>■ 更改 CPU 数目</li> <li>■ 更改资源</li> <li>■ 扩展虚拟磁盘</li> <li>■ 磁盘更改跟踪</li> <li>■ 内存</li> <li>■ 修改设备设置</li> <li>■ 重命名</li> <li>■ 设置注释</li> <li>■ 设置</li> <li>■ 交换文件位置</li> </ul>
虚拟机 - 置备	<ul style="list-style-type: none"> <li>■ 自定义</li> <li>■ 克隆模板</li> <li>■ 克隆虚拟机</li> <li>■ 部署模板</li> <li>■ 读取自定义规范</li> </ul>
虚拟机 - 状态	<ul style="list-style-type: none"> <li>■ 创建快照</li> <li>■ 移除快照</li> <li>■ 恢复到快照</li> </ul>

## 配置 Microsoft Azure 以与 vRealize Automation Cloud Assembly 配合使用

要在 vRealize Automation Cloud Assembly 中创建 Microsoft Azure 云帐户，您必须收集一些信息并执行一些配置。

### 步骤

1 找到并记录您的 Microsoft Azure 订阅 ID 和租户 ID。

- 订阅 ID - 单击 Azure 门户左侧工具栏上的“订阅”图标可查看订阅 ID。
- 租户 ID - 单击 Azure 门户中的“帮助”图标，然后选择“显示诊断”。搜索租户并在找到后记录该 ID。

## 2 您可以创建新存储帐户和资源组以开始执行操作。或者，也可以稍后在蓝图中创建。

### ■ 存储帐户 - 使用以下过程配置帐户。

- 1 在 Azure 门户中，找到侧栏上的“存储帐户”图标。确保选择正确的订阅，然后单击**添加**。还可以在 Azure 搜索字段中搜索存储帐户。
- 2 输入存储帐户的必填信息。您需要提供订阅 ID。
- 3 选择是使用现有资源组还是创建新资源组。记下您的资源组名称，因为稍后需要用到该名称。

---

**注** 保存您的存储帐户位置，因为稍后需要用到该位置。

---

## 3 创建虚拟网络。或者，如果您有合适的现有网络，则可以选择该网络。

如果要创建网络，必须选择“使用现有资源组”并指定在上一步中创建的组。此外，选择以前指定的相同位置。如果对象将使用的所有适用组件之间的位置不匹配，Microsoft Azure 将不会部署虚拟机或其他对象。

- a 在左侧面板中找到“虚拟网络”图标并单击，或搜索虚拟网络。确保选择正确的订阅，然后单击**添加**。
- b 输入新虚拟网络的唯一名称，并进行记录以供稍后使用。
- c 在**地址空间**字段中输入虚拟网络的相应 IP 地址。
- d 确保选择正确的订阅，然后单击**添加**。
- e 输入其余的基本配置信息。
- f 您可以根据需要修改其他选项，但对于大多数配置，可以保留默认值。
- g 单击**创建**。

## 4 设置 Azure Active Directory 应用程序，以便 vRA 可以进行身份验证。

- a 在 Azure 左侧菜单中找到 Active Directory 图标，然后单击该图标。
- b 单击**应用注册**，然后选择**添加**。
- c 键入符合 Azure 名称验证的应用程序的名称。
- d 保留“Web 应用/API”作为“应用程序类型”。
- e “登录 URL”可以是适合您使用情况的任何值。
- f 单击**创建**。

## 5 创建密钥以在 Cloud Assembly 中对应用程序进行身份验证。

- a 在 Azure 中单击应用程序的名称。  
记下应用程序 ID，供稍后使用。
- b 单击下一个窗格中的**所有设置**，然后从设置列表中选择“密钥”。
- c 输入新密钥的描述并选择持续时间。
- d 单击**保存**并确保将该密钥值复制到安全位置，因为稍后将无法检索该密钥值。

- e 在左侧菜单中，选择应用程序的 **API 权限**，然后单击**添加权限**以创建新权限。
  - f 在“选择 API”页面上选择“Azure 服务管理”。
  - g 单击**委派的权限**。
  - h 在“选择权限”下，选择 `user_impersonation`，然后单击**添加权限**。
- 6 授权您的 Active Directory 应用程序连接到 Azure 订阅，以便可以部署和管理虚拟机。**
- a 在左侧菜单中，单击“订阅”图标，然后选择新订阅。  
您可能需要单击名称文本才能使面板侧拉。
  - b 选择“访问控制 (IAM)”选项以查看对订阅的权限。
  - c 单击“添加角色分配”标题下的**添加**。
  - d 从“角色”下拉列表中选择“参与者”。
  - e 在“将访问权限分配给”下拉列表中，保留默认选择。
  - f 在“选择”框中键入应用程序的名称。
  - g 单击**保存**。
  - h 添加其他角色，使新应用程序具有“所有者”、“参与者”和“读者”角色。
  - i 单击**保存**。

## 后续步骤

您必须安装 Microsoft Azure 命令行界面工具。对于 Windows 和 Mac 操作系统，可免费使用这些工具。有关下载和安装这些工具的详细信息，请参见 Microsoft 文档。

安装命令行界面后，必须对新订阅进行身份验证。

- 1 打开终端窗口，然后键入您的 Microsoft Azure 登录信息。您将收到一个 URL 以及一个可供您进行身份验证的短代码。
- 2 在浏览器中，输入从设备上的应用程序收到的代码。
- 3 输入您的“身份验证代码”，然后单击**继续**。
- 4 选择您的 Azure 帐户并登录。

如果您有多个订阅，请确保使用 `azure account set <subscription-name>` 命令选择正确的订阅。

- 5 在继续操作之前，必须使用 `azure provider register microsoft.compute` 命令将 Microsoft.Compute 提供程序注册到新 Azure 订阅。

如果命令在首次运行时超时并生成错误，请重新运行。

完成配置后，可以使用 `azure vm image list` 命令检索可用的虚拟机映像名称。您可以选择所需映像，记录为其提供的 URN，并稍后在蓝图中使用。

## 在 vRealize Automation 中创建 Microsoft Azure 云帐户

作为云管理员，您可以为团队将在其中部署 vRealize Automation 云模板的帐户区域创建 Microsoft Azure 云帐户。

要查看 Microsoft Azure 云帐户在 vRealize Automation 中的工作方式示例用例，请参见 [教程：在 vRealize Automation Cloud Assembly 中设置和测试多云基础架构和部署](#)。

### 前提条件

- 确认您具有所需的管理员凭据，并且已在端口 443 上启用 HTTPS 访问。请参见在 [vRealize Automation 中使用云帐户所需的凭据](#)。
- 确认您具有所需的用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 配置 Microsoft Azure 帐户与 vRealize Automation 配合使用。请参见 [配置 Microsoft Azure 以与 vRealize Automation Cloud Assembly 配合使用](#)。
- 如果您没有外部 Internet 访问，请配置一个 Internet 服务器代理。请参见 [如何配置 vRealize Automation 的 Internet 代理服务器](#)。

### 步骤

- 1 选择 **基础架构 > 连接 > 云帐户**，然后单击 **添加云帐户**。
- 2 选择 Microsoft Azure 帐户类型，然后输入凭据和其他值。
- 3 单击 **验证**。  
将收集与该帐户相关联的帐户区域。
- 4 选择要将此资源置备到的区域。
- 5 为了提高效率，单击 **为选定区域创建云区域**。
- 6 如果需要添加标记以支持标记策略，请输入功能标记。请参见 [如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署和创建标记策略](#)。



有关功能标记和限制标记如何帮助控制部署布置的详细信息，请参见 [限制标记和布置视频教程](#)。

- 7 单击 **保存**。

### 结果

该帐户将添加到 vRealize Automation 中，所选区域可用于指定的云区域。

### 后续步骤

为此云帐户创建基础架构资源。

## 在 vRealize Automation 中创建 Amazon Web Services 云帐户

作为云管理员，您可以为团队将在其中部署 vRealize Automation 云模板的帐户区域创建 Amazon Web Services (AWS) 云帐户。

对于授权用户，AWS 云帐户支持访问 AWS GovCloud 配置。此配置支持与项目配置、标记和基础架构有关的大多数标准 vRealize Automation 云帐户功能。在 Cloud Assembly 云模板中，支持使用 AWS 平台即服务 (PaaS) 属性。

以下过程介绍了如何配置 AWS 云帐户。

### 前提条件

- 确认您具有所需的管理员凭据，并且已在端口 443 上启用 HTTPS 访问。请参见在 [vRealize Automation 中使用云帐户所需的凭据](#)。
- 确认您具有所需的用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 确认您具有所需的 AWS 管理员凭据。
- 如果您没有外部 Internet 访问，请配置一个 Internet 服务器代理。请参见 [如何配置 vRealize Automation 的 Internet 代理服务器](#)。

### 步骤

- 1 选择**基础架构 > 连接 > 云帐户**，然后单击**添加云帐户**。
- 2 选择 AWS 帐户类型，然后输入凭据和其他值。
- 3 单击**验证**。  
将收集与该帐户相关联的帐户区域。
- 4 选择要将此资源置备到的区域。
- 5 为了提高效率，单击**为选定区域创建云区域**。
- 6 如果需要添加标记以支持标记策略，请输入功能标记。请参见 [如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署和创建标记策略](#)。



有关功能标记和限制标记如何帮助控制部署布置的详细信息，请参见[限制标记和布置视频教程](#)。

- 7 单击**添加**。

### 结果

该帐户将添加到 vRealize Automation 中，所选区域可用于指定的云区域。

### 后续步骤

为此云帐户配置基础架构资源。

## 在 vRealize Automation 中创建 Google Cloud Platform 云帐户

作为云管理员，您可以为团队将在其中部署 vRealize Automation 云模板的帐户区域创建 Google Cloud Platform (GCP) 云帐户。

### 前提条件

- 确认您具有所需的管理员凭据，并且已在端口 443 上启用 HTTPS 访问。请参见在 [vRealize Automation 中使用云帐户所需的凭据](#)。
- 确认您具有所需的用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 确认您有权访问 Google Cloud Platform JSON 安全密钥。
- 确认您拥有 Google Cloud Platform 实例所需的安全信息。这些信息大部分可以从您的实例或 Google 文档获取。
- 如果您没有外部 Internet 访问，请配置一个 Internet 服务器代理。请参见 [如何配置 vRealize Automation 的 Internet 代理服务器](#)。

### 步骤

- 1 选择**基础架构 > 连接 > 云帐户**，然后单击**添加云帐户**。
- 2 选择 Google Cloud Platform 帐户类型，并输入相应的凭据和相关信息。使用在初始化源 GCP 帐户计算引擎时创建的服务帐户。

如上面的**必备条件**部分中所述，可从在 [vRealize Automation 中使用云帐户所需的凭据](#)了解凭据要求。要在 vRealize Automation 中成功创建云帐户，源 GCP 帐户必须启用计算引擎服务。

在 vRealize Automation 中，项目 ID 是 Google Cloud Platform 端点的一部分。您可以在创建云帐户时指定该 ID。在对特定于项目的专用映像收集数据期间，vRealize Automation GCP 适配器会查询 Google Cloud Platform API。

- 3 单击**验证**。  
将收集与该帐户相关联的帐户区域。
- 4 选择要将此资源置备到的区域。
- 5 为了提高效率，单击**为选定区域创建云区域**。
- 6 如果需要标记以支持标记策略，请输入功能标记。请参见[如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署和创建标记策略](#)。



有关功能标记和限制标记如何帮助控制部署布置的详细信息，请参见[限制标记和布置视频教程](#)。

- 7 单击**添加**。

### 结果

该帐户将添加到 vRealize Automation 中，所选区域可用于指定的云区域。

## 后续步骤

为此云帐户创建基础架构资源。

## 在 vRealize Automation 中创建 vCenter 云帐户

可以为要部署 vRealize Automation 云模板的帐户区域添加 vCenter 云帐户。

出于网络和安全目的，您可以将 vCenter 云帐户与 NSX-T 或 NSX-V 云帐户相关联。

一个 NSX-T 云帐户可与一个或多个 vCenter 云帐户相关联。但是，一个 NSX-V 云帐户只能与一个 vCenter 云帐户相关联。

### 前提条件

- 确认您具有所需的管理员凭据，并且已在端口 443 上启用 HTTPS 访问。请参见在 [vRealize Automation 中使用云帐户所需的凭据](#)。
- 确认您具有云管理员用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 确认您已正确配置端口和协议以支持云帐户。请参阅 [vRealize Automation 产品文档中的使用 vRealize Easy Installer 安装 vRealize Automation 中的 vRealize Automation 的端口和协议主题](#)以及《vRealize Automation 参考架构指南》中的端口要求主题。

### 步骤

- 1 选择**基础架构 > 连接 > 云帐户**，然后单击**添加云帐户**。
- 2 选择 vCenter 帐户类型，然后输入 vCenter Server 主机 IP 地址。
- 3 输入您的 vCenter Server 管理员凭据，然后单击**验证**。

将从与该帐户关联的数据中心收集数据。以下是进行数据收集的元素，其中包括以下元素的所有 vSphere 标记：

- 计算机
- 集群和主机
- 端口组
- 数据存储

- 4 在指定的 vCenter Server 上至少选择一个可用数据中心，以便置备此云帐户。
- 5 为了提高效率，创建一个云区域，以便置备到选定的数据中心。

您还可以根据组织的云策略，在单独的步骤中创建云区域。

有关云区域的信息，请参见[了解有关 vRealize Automation Cloud Assembly 云区域的更多信息](#)。

- 6 选择现有的 NSX 云帐户。

您可以现在或稍后编辑云帐户时选择 NSX 帐户。

有关 NSX-V 云帐户的信息，请参见在 [vRealize Automation 中创建 NSX-V 云帐户](#)。

有关 NSX-T 云帐户的信息，请参见在 [vRealize Automation 中创建 NSX-T 云帐户](#)。

有关在部署云模板后进行关联更改的信息，请参见[如果在 vRealize Automation 中移除 NSX 云帐户关联，会发生什么情况](#)。

- 7 如果要添加标记以支持标记策略，请输入功能标记。

您可以现在或稍后编辑云帐户时添加标记。有关标记的信息，请参见[如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署](#)。



有关功能标记和限制标记如何帮助控制部署布置的详细信息，请参见[限制标记和布置视频教程](#)。

- 8 单击**保存**。

## 结果

将添加云帐户，并且选定的数据中心可用于指定的云区域。收集的数据（例如计算机、网络、存储和卷）将列在[基础架构](#)选项卡的**资源**部分中。

## 后续步骤

为此云帐户配置其余基础架构资源。请参见第 4 章 [构建您的 vRealize Automation Cloud Assembly 资源基础架构](#)。

## 在 vRealize Automation 中创建 NSX-V 云帐户

出于网络和安全目的，您可以创建 NSX-V 云帐户并将其与 vCenter 云帐户相关联。

一个 NSX-V 云帐户只能与一个 vCenter 云帐户相关联。

NSX-V 与 vCenter 云帐户之间的关联必须在 vRealize Automation 外部进行配置，具体而言，在 NSX 应用程序中进行配置。vRealize Automation 不会在 NSX 和 vCenter 之间创建关联。在 vRealize Automation 中，可以指定 NSX 中已存在的关联。

## 前提条件

- 确认您具有所需的管理员凭据，并且已在端口 443 上启用 HTTPS 访问。请参见在 [vRealize Automation 中使用云帐户所需的凭据](#)。
- 确认您具有云管理员用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 确认您具有与此 NSX 云帐户配合使用的 vCenter 云帐户。请参见在 [vRealize Automation 中创建 vCenter 云帐户](#)。
- 确认您已正确配置端口和协议以支持云帐户。请参阅 [vRealize Automation 产品文档](#)中的使用 vRealize Easy Installer 安装 vRealize Automation 中的 vRealize Automation 的端口和协议主题以及《vRealize Automation 参考架构指南》中的端口要求主题。

## 步骤

- 1 选择[基础架构](#) > [连接](#) > [云帐户](#)，然后单击**添加云帐户**。
- 2 选择 NSX-V 帐户类型，然后输入 NSX-V 主机 IP 地址。



- 3 输入您的 NSX 管理员凭据，然后单击**验证**。

将收集与该帐户关联的资产。

如果 NSX 主机 IP 地址不可用，则验证将失败。

- 4 如果可用，请选择表示要与此 NSX-V 帐户关联的 vCenter 云帐户的 vCenter 端点。

仅当前未与 NSX-T 或 NSX-V 云帐户关联的 vCenter 云帐户可供选择。

有关在部署云模板后进行关联更改的信息，请参见[如果在 vRealize Automation 中移除 NSX 云帐户关联，会发生什么情况](#)。

- 5 如果要添加标记以支持标记策略，请输入功能标记。

可以稍后添加或移除功能标记。请参见[如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署](#)。



有关功能标记和限制标记如何帮助控制部署布置的信息，请参见[限制标记和布置视频教程](#)。

- 6 单击**保存**。

#### 后续步骤

可以创建或编辑 vCenter 云帐户，以便与此 NSX 云帐户关联。请参见在[vRealize Automation 中创建 vCenter 云帐户](#)。

创建并配置一个或多个云区域，以便与此云帐户使用的数据中心配合使用。请参见[了解有关 vRealize Automation Cloud Assembly 云区域的更多信息](#)。

为此云帐户配置基础架构资源。请参见第 4 章 [构建您的 vRealize Automation Cloud Assembly 资源基础架构](#)。

## 在 vRealize Automation 中创建 NSX-T 云帐户

出于网络和安全目的，您可以创建一个 NSX-T 云帐户，并将其与一个或多个 vCenter 云帐户相关联。

一个 NSX-T 云帐户可与一个或多个 vCenter 云帐户相关联。但是，一个 NSX-V 云帐户只能与一个 vCenter 云帐户相关联。

NSX-T 与一个或多个 vCenter 云帐户之间的关联必须在 vRealize Automation 外部进行配置，具体而言，是在 NSX 应用程序中进行配置。vRealize Automation 不会在 NSX 和 vCenter 之间创建关联。在 vRealize Automation 中，可以指定 NSX 中已存在的一个或多个配置关联。

您可以定义一个 NSX-T 云帐户以支持 NSX-T Manager API 方法或 NSX-T Policy API 方法。有关这两种方法的详细信息，请参见相关主题，例如 [NSX-T Data Center 产品文档](#) 内《NSX-T Data Center 管理指南》中的“NSX Manager 概述”。下面还按步骤顺序提供了信息。

创建 NSX-T 云帐户后，无法将其从一种 API 方法转换为另一种方法。而是，需要删除云帐户，然后使用另一种 API 模式重新创建。

为了促进部署中的容错能力和高可用性，每个 NSX-T Data Center 端点都表示一个由 3 个 NSX Manager 构成的集群。

- vRealize Automation 可以指向其中一个 NSX Manager。使用此选项时，一个 NSX Manager 将收到 vRealize Automation 发出的 API 调用。
- vRealize Automation 可以指向集群的虚拟 IP。使用此选项时，一个 NSX Manager 假设具有 VIP 的控制权。该 NSX Manager 将收到 vRealize Automation 发出的 API 调用。如果出现故障，集群中的另一个节点将接管 VIP，并收到来自 vRealize Automation 的 API 调用。

有关为 NSX 配置 VIP 的详细信息，请参见 [VMware NSX-T Data Center 文档](#) 内《NSX-T Data Center 安装指南》中的“为集群配置虚拟 IP (VIP) 地址”。

- vRealize Automation 可以指向负载均衡器 VIP，以将调用负载均衡分配到 3 个 NSX Manager。使用此选项时，所有三个 NSX Manager 都将收到 vRealize Automation 发出的 API 调用。

您可以在第三方负载均衡器或 NSX-T 负载均衡器上配置 VIP。

对于规模较大的环境，请考虑使用此选项，以在 3 个 NSX Manager 之间分配 vRealize Automation API 调用。

#### 前提条件

- 确认您具有所需的管理员凭据，并且已在端口 443 上启用 HTTPS 访问。请参见在 [vRealize Automation 中使用云帐户所需的凭据](#)。
- 确认您具有云管理员用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 确认您具有与此 NSX 云帐户配合使用的 vCenter 云帐户。请参见在 [vRealize Automation 中创建 vCenter 云帐户](#)。
- 确认您已正确配置端口和协议以支持云帐户。请参阅 [vRealize Automation 产品文档](#) 中的使用 vRealize Easy Installer 安装 vRealize Automation 中的 vRealize Automation 的端口和协议主题以及《vRealize Automation 参考架构指南》中的端口要求主题。

#### 步骤

- 1 选择**基础架构 > 连接 > 云帐户**，然后单击**添加云帐户**。
- 2 选择 NSX-T 帐户类型，然后输入 NSX-T Manager 端点实例的主机 IP 地址或 VIP（请参见上文，了解与 NSX Manager 和 VIP 选项相关的预期行为信息）。
- 3 输入您的 NSX 用户名和密码管理员凭据，然后单击**验证**。

将收集与该帐户关联的资产。

如果 NSX 主机 IP 地址不可用，则验证将失败。

- 4 在 **NSX-T API 方法** 中，选择 **Manager 方法** 或 **Policy 方法**。

- **Manager API 方法**

从早期版本的 vRealize Automation 载入或迁移的现有 NSX-T 端点或云帐户将视为 Manager API 方法 NSX-T 云帐户。

NSX-T 2.4、NSX-T 3.0 和 NSX-T 3.1 及更高版本支持 Manager API 方法。

如果现在使用的是 NSX-T Manager API 方法，则建议继续使用 Manager API 方法，直到 vRealize Automation 引入了 Manager API 到 Policy API 迁移路径。

NSX-T 的某些 vRealize Automation 选项需要 NSX-T 3.0 或更高版本，包括将标记添加到云模板中的虚拟机网卡组件。

#### ■ Policy API 方法（默认值）

Policy API 方法适用于 NSX-T 3.0 和 NSX-T 3.1 及更高版本。此选项允许 vRealize Automation 使用 NSX-T Policy API 中提供的其他功能。

如果您现有的 NSX-T 云帐户是在 vRealize Automation 8.2 中引入 Policy API 方法之前创建的，则可以使用 Manager API 方法。建议您等待 Manager API 到 Policy API 迁移工具在 vRealize Automation 中可用。如果您不想等待，则应将现有 NSX-T 云帐户替换为指定 Policy API 方法的新 NSX-T 云帐户。

- 5 在**关联**中，添加一个或多个 vCenter 云帐户，以便与此 NSX-T 云帐户相关联。此外，还可以移除现有的 vCenter 云帐户关联。

仅在 vRealize Automation 中当前未与 NSX-T 或 NSX-V 云帐户关联的 vCenter 云帐户可供选择。

请参见在 [vRealize Automation](#) 中，[NSX-T 映射到多个 vCenter](#) 有哪些用途。

有关在部署云模板后进行关联更改或在云模板蓝图后删除云帐户的信息，请参见[如果在 vRealize Automation 中移除 NSX 云帐户关联，会发生什么情况](#)。

- 6 如果要添加标记以支持标记策略，请输入功能标记。

可以稍后添加或移除功能标记。请参见[如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署](#)。



有关功能标记和限制标记如何帮助控制部署布置的详细信息，请参见[限制标记和布置视频教程](#)。

- 7 单击**保存**。

#### 后续步骤

可以创建或编辑 vCenter 云帐户，以便与此 NSX 云帐户关联。请参见在 [vRealize Automation](#) 中创建 vCenter 云帐户。

创建并配置一个或多个云区域，以便与此云帐户使用的数据中心配合使用。请参见[了解有关 vRealize Automation Cloud Assembly 云区域的更多信息](#)。

为此云帐户配置基础架构资源。请参见第 4 章 [构建您的 vRealize Automation Cloud Assembly 资源基础架构](#)。

## 在 vRealize Automation 中创建 VMware Cloud on AWS 云帐户

作为云管理员，您可以为团队将在其中部署 vRealize Automation 云模板的帐户区域创建 VMware Cloud on AWS 云帐户。

在 vRealize Automation 中，VMware Cloud on AWS 需要一些独特的配置过程。要针对 VMware Cloud on AWS 正确配置 vRealize Automation，包括为云帐户设置 API 令牌值以及为其云代理设置网关防火墙规则，请参见 [教程：为 vRealize Automation 配置 VMware Cloud on AWS 工作流](#)。

### 前提条件

- 确认您具有所需的 VMware Cloud on AWS 管理员凭据，包括 vCenter 中目标 SDDC 的 VMware Cloud on AWS CloudAdmin 凭据，并确认已在端口 443 上启用 HTTPS 访问。请参见在 [vRealize Automation 中使用云帐户所需的凭据](#)。
- 确认您具有云管理员用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 如果您没有外部 Internet 访问，请配置一个 Internet 服务器代理。请参见 [如何配置 vRealize Automation 的 Internet 代理服务器](#)。
- 确认您已在 SDDC 中配置了所需的访问权限和防火墙规则。请参见 [准备 VMware Cloud on AWS SDDC 连接到 vRealize Automation 中的 VMware Cloud on AWS 云帐户](#)。

### 步骤

- 1 选择 **基础架构 > 连接 > 云帐户**，单击 **添加云帐户** 并选择 VMware Cloud on AWS 帐户类型。
- 2 为您的组织添加 **VMC API 令牌** 以访问可用的 SDDC。

可以在链接的 **API 令牌** 页面上为您的组织创建新令牌或使用现有令牌。有关详细信息，请参见在 [vRealize Automation 的示例工作流中创建 VMware Cloud on AWS 云帐户](#)。

- 3 选择可用于部署的 SDDC。

NSX-V SDDC 不受支持，不会出现在列表中。

将根据 SDDC 自动填充 vCenter 和 NSX-T Manager IP 地址/FQDN 值。

- 4 输入指定 SDDC 的 vCenter 用户名和密码（如果不是默认值 cloudadmin@vmc.local）。

- 5 单击 **验证** 确认您对指定 vCenter 的访问权限，并检查 vCenter 是否正在运行。

将收集与该帐户关联的数据中心。

- 6 为了提高效率，创建一个云区域，以便置备到选定的 SDDC。

您还可以根据组织的云策略，在单独的步骤中创建云区域。

- 7 如果要添加标记以支持标记策略，请输入功能标记。

可以稍后添加或移除功能标记。请参见 [如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署](#)。



有关功能标记和限制标记如何帮助控制部署布置的详细信息，请参见 [限制标记和布置视频教程](#)。

- 8 单击 **保存**。

## 结果

将添加云帐户，并且选定的 SDDC 可用于指定的云区域。

## 后续步骤

要针对 VMware Cloud on AWS 正确配置 vRealize Automation，请参见 [教程：为 vRealize Automation 配置 VMware Cloud on AWS](#)。

有关 vRealize Automation 之外的 VMware Cloud on AWS 的相关信息，请参见 [VMware Cloud on AWS 文档](#)。

## 创建 VMware Cloud Foundation 云帐户

可以将 VMware Cloud Foundation (VCF) 配置为 vRealize Automation Cloud Assembly 中的云帐户，以便使用工作负载域。

通过 VCF 云帐户，可以将工作负载整合到 Cloud Assembly 中，以便于形成一个全面的混合云管理解决方案。Cloud Assembly 提供多个入口点，您可以从这些入口点激活 VCF 云帐户配置页面。如果使用 SDDC 集成“工作负载域”选项卡上的**添加云帐户**按钮访问此页面，则会预选工作负载作为 vCenter 和 NSX Manager 的基本信息。

## 前提条件

您必须将 VMware SDDC Manager 4.1 或更高版本的实例配置为 vRealize Automation Cloud Assembly 集成，才能在此云帐户中使用。有关详细信息，请参见[配置 VMware SDDC Manager 集成](#)。

## 步骤

- 1 选择**基础架构 > 连接 > 云帐户**，然后单击**添加云帐户**。
- 2 选择“VCF 云帐户”类型，然后输入**名称**和**描述**。
- 3 输入要在此云帐户中使用的 SDDC Manager 实例的 FQDN 和凭据。  
如果您已配置将用于此帐户的 SDDC Manager 实例，则可以跳过此步骤。
- 4 选择要在此 VCF 云帐户中使用的一个或多个工作负载域。
- 5 如果希望 Cloud Assembly 对 vCenter 和 NSX 使用 Cloud Foundation 受管服务凭据，请选择**自动创建服务凭据**。之后，如果要更改这些凭据，则必须使用 VCF 机制管理密码。  
如果选择此选项，则可以跳过步骤 7 和 8。
- 6 输入访问与此云帐户关联的 vCenter 所需的凭据。
- 7 在“NSX Manager”标题下，如果要手动输入 VCF 云帐户的凭据，请输入 NSX 凭据；如果希望 Cloud Assembly 创建并验证 NSX 凭据，请单击“创建并验证服务凭据”。
- 8 输入访问与此云帐户关联的 NSX-T 网络所需的凭据。
- 9 （如果适用）选择 NSX 模式。
- 10 单击**验证**以确认与 SDDC Manager 的连接。

- 11 （如果适用）在“配置”标题下选择要置备到的数据中心。如果要为所选数据中心创建云区域，请单击以下复选框：
- 12 如果使用标记以支持标记策略，请输入功能标记。请参见[如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署和创建标记策略](#)。
- 13 单击**保存**。

### 结果

此云帐户会将与指定 SDDC Manager 关联的所选工作负载域整合到 vRealize Automation Cloud Assembly 中以供使用。

如果要使用 vRealize Automation 管理其他工作负载域，必须对每个域重复此过程。

### 后续步骤

配置 VCF 云帐户后，可以在主云帐户页面上选择该帐户，然后单击**设置云**，启动 VMware Cloud Foundation 快速入门向导以便配置云。

有关快速入门向导的详细信息，请参见[../Getting-Started-Cloud-Assembly/GUID-BDC673B9-D2AD-47BC-93C5-8C500074F931.html](#)。

## 将 vRealize Automation 与其他应用程序集成

集成使您能够将外部系统添加到 vRealize Automation。

集成包括 vRealize Orchestrator、配置管理和其他外部系统，例如 GitHub、Ansible、Puppet 和外部 IPAM 提供程序（如 Infoblox）。

---

**注** 如果您没有外部 Internet 访问权限，但您的集成需要该权限，则可以配置一个 Internet 服务器代理。请参见[如何配置 vRealize Automation 的 Internet 代理服务器](#)。

---

## 如何在 vRealize Automation Cloud Assembly 中使用 Git 集成

vRealize Automation Cloud Assembly 支持与 GitLab、GitHub 和 BitBucket 存储库集成，以便您可以在源控制下管理 VMware Cloud Templates 和操作脚本。此功能可简化对部署流程的审计和财务责任落实。

vRealize Automation Cloud Assembly 提供了三种不同风格的 Git 集成：GitLab、GitHub 和 BitBucket。每个选项都是一个单独的集成。

您必须具有相应的本地 Git 存储库并为指定的所有用户配置了访问权限，以便设置 Git 与 vRealize Automation Cloud Assembly 的集成。此外，您还必须在特定结构中保存云模板，以便 Git 能够检测到它们。要创建与 GitLab 或 GitHub 的集成，请在 vRealize Automation Cloud Assembly 中选择**基础架构 > 连接 > 集成**，然后进行相应的选择。您需要目标存储库的 url 和令牌。

使用现有存储库配置 Git 集成时，与所选项目关联的所有云模板将对合格用户可用。您可以将这些模板用于现有部署，也可以将其用作新部署的基础。添加项目时，您必须选择与该项目在 Git 中的存储位置和存储方式相关的属性。



您可以直接从 vRealize Automation Cloud Assembly 将操作保存到 Git 存储库。您可以直接在 Git 中对操作脚本进行版本控制，也可以在 vRealize Automation Cloud Assembly 中创建版本。如果在 vRealize Automation Cloud Assembly 中创建操作的版本，则会自动将其作为版本保存到 Git 中。云模板稍微复杂一些，因为不能从 vRealize Automation Cloud Assembly 将它们直接添加到 Git 集成中。您必须将它们直接保存到 Git 实例中，然后在使用 vRealize Automation Cloud Assembly 中的云模板管理页面时可以从 Git 中检索它们。

## 开始前

您必须在特定结构中创建并保存云模板，以便 GitLab 或 GitHub 检测到它们。

- 配置和存储云模板，以便正确地与 GitLab 集成。只有有效模板才会导入到 GitLab。
  - 为云模板创建一个或多个指定文件夹。
  - 所有云模板都必须存储在 `blueprint.yaml` 文件中。
  - 确保模板的顶部包括 `name:` 和 `version:` 属性。
- 为适用的存储库提取 API 密钥。在 Git 帐户中，选择右上角的登录名，然后导航到“设置”菜单。选择 **访问令牌**，并命名您的令牌，设置到期日期。然后，选择 **API** 并创建令牌。复制生成的值并保存它。

对于用于 Git 集成的所有云模板，必须遵守以下准则。

- 每个云模板必须驻留在单独的文件夹中。
- 所有云模板都必须按 `blueprint.yaml` 命令。
- 所有云模板 YAML 文件都必须使用 `name` 字段和 `version` 字段。
- 只会导入有效的云模板。
- 如果您更新从 Git 导入的草稿云模板，而且该云模板的内容与最高版本中的不同，则在后续的同步不会更新草稿，并且会创建新版本。如果要更新模板并同时允许来自 Git 的后续同步，您必须在完成最终更改之后创建新版本。

- [在 vRealize Automation Cloud Assembly 中配置 GitLab 云模板集成](#)

此过程说明了如何在 vRealize Automation Cloud Assembly 中配置 GitLab 集成，以便您可以使用存储库中的云模板，并自动下载与指定项目关联的已保存模板。要将云模板与 GitLab 配合使用，您必须创建与相应 GitLab 实例的连接，然后将所需模板保存到该实例。

- [在 vRealize Automation Cloud Assembly 中配置 GitHub 集成](#)

可以在 vRealize Automation Cloud Assembly 中集成 GitHub 云端存储库托管服务

- [在 vRealize Automation Cloud Assembly 中配置 Bitbucket 集成](#)

vRealize Automation Cloud Assembly 支持与 Bitbucket 集成，可将其用作 ABX 操作脚本和 VMware Cloud Templates 的基于 Git 的存储库。

## 在 vRealize Automation Cloud Assembly 中配置 GitLab 云模板集成

此过程说明了如何在 vRealize Automation Cloud Assembly 中配置 GitLab 集成，以便您可以使用存储库中的云模板，并自动下载与指定项目关联的已保存模板。要将云模板与 GitLab 配合使用，您必须创建与相应 GitLab 实例的连接，然后将所需模板保存到该实例。

使用现有存储库配置 GitLab 集成时，与所选项目关联的所有云模板将对合格用户可用。您可以将这些模板用于现有部署，也可以将其用作新部署的基础。添加项目时，必须选择与该项目在 GitLab 中的存储位置和存储方式相关的属性。

---

**注** 您无法从 vRealize Automation Cloud Assembly 将新的或已更新的云模板推送到 Git 存储库。此外，您也无法从 vRealize Automation Cloud Assembly 将新模板推送到存储库。要将云模板添加到存储库，开发人员必须使用 Git 界面。

---

如果您更新从 Git 导入的草稿云模板，而且该云模板的内容与最高版本中的不同，则在后续的同步不会更新草稿，并且会创建新版本。如果要更新云模板并同时允许来自 Git 的后续同步，您必须在完成最终更改之后创建新版本。

设置要与 GitLab 一起使用的云模板并收集所需信息后，您必须设置与 GitLab 实例的集成。然后，您可以将指定的云模板导入 GitLab。您可以在 <https://www.youtube.com/watch?v=h0vqo63Sdgg> 中查看此过程的视频演示。

### 前提条件

- 为适用的存储库提取 API 密钥。在 GitLab 帐户中，选择右上角的登录名，然后导航到“设置”菜单。选择“访问令牌”，并命名您的令牌，设置到期日期。然后，选择 API 并创建令牌。复制生成的值并保存它。

您必须具有相应的本地 Git 存储库并为指定的所有用户配置了访问权限，以便设置 Git 与 vRealize Automation Cloud Assembly 的集成。此外，您还必须在特定结构中创建并保存云模板，以便 GitLab 检测到它们。

- 配置和存储云模板，以便正确地与 GitLab 集成。只有有效模板才会导入到 GitLab。请参见 [如何在 vRealize Automation Cloud Assembly 中使用 Git 集成](#)。

### 步骤

- 1 在 vRealize Automation Cloud Assembly 中设置与 GitLab 环境的集成。
  - a 选择**基础架构 > 集成 > 新增**，然后选择 GitLab。
  - b 输入您的 GitLab 实例的 URL。对于软件即服务 GitLab 实例，大多数情况下，它是 `gitlab.com`。
  - c 输入指定 GitLab 实例的**令牌**（也称为 API 密钥）。有关从 GitLab 实例中提取令牌的信息，请参见上述必备条件。
  - d 添加相应的名称和说明。
  - e 单击**验证**以验证连接。



- f 如果需要，添加功能标记。有关详细信息，请参见在 [vRealize Automation Cloud Assembly 中使用功能标记](#)。
  - g 单击**添加**。
- 2 配置 GitLab 连接，以便接受相应存储库中的云模板。
- a 选择**基础架构 > 集成**，然后选择相应的 GitLab 集成。
  - b 选择**项目**。
  - c 选择**新建项目**，并为该项目创建一个名称。
  - d 在 GitLab 中输入**存储库**路径。通常情况下，这是附加到存储库名称的主帐户的用户名。
  - e 输入要使用的相应 GitLab **分支**。
  - f 如果适用，请输入**文件夹**名称。如果留空，则所有文件夹都可用。
  - g 输入相应的**类型**。如果适用，请输入文件夹名称。如果留空，则所有文件夹都可用。
  - h 单击**下一步**完成存储库的添加。
- 单击**下一步**时，会启动自动同步任务，可将云模板导入到平台中。
- 同步任务完成后，会显示一条消息，指示已导入云模板。

## 结果

现在，可以从 GitLab 检索云模板。

## 在 vRealize Automation Cloud Assembly 中配置 GitHub 集成

可以在 vRealize Automation Cloud Assembly 中集成 GitHub 云端存储库托管服务

您需要有效的 GitHub 令牌才能在 vRealize Automation Cloud Assembly 中配置 GitHub 集成。有关创建和查找令牌的信息，请参见 [GitHub 文档](#)。

### 前提条件

- 您必须能够访问 GitHub。
- 配置和存储云模板，以便正确地与 GitHub 集成。只有有效云模板才会导入到 GitHub。请参见[如何在 vRealize Automation Cloud Assembly 中使用 Git 集成](#)。

### 步骤

- 1 选择**基础架构 > 连接 > 集成**，然后单击**添加集成**。
- 2 选择“GitHub”。
- 3 在 GitHub 配置页面上输入必填信息。
- 4 单击**验证**以检查集成。
- 5 如果需要添加标记以支持标记策略，请输入功能标记。请参见[如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署和创建标记策略](#)。
- 6 单击**添加**。

## 7 配置 GitLab 连接，以便接受相应存储库中的云模板。

- a 选择**基础架构 > 集成**，然后选择相应的 GitHub 集成。
- b 选择**项目**。
- c 选择**新建项目**，并为该项目创建一个名称。
- d 在 GitHub 中输入**存储库**路径。通常情况下，这是附加到存储库名称的主帐户的用户名。
- e 输入要使用的相应 GitHub **分支**。
- f 如果适用，请输入**文件夹**名称。如果留空，则所有文件夹都可用。
- g 输入相应的**类型**。
- h 单击**下一步**完成存储库的添加。

将启动可将云模板导入到平台中的自动同步任务。

同步任务完成后，会显示一条消息，指示已导入云模板。

### 结果

GitHub 可在 vRealize Automation Cloud Assembly 蓝图中使用。

### 后续步骤

现在，可以从 GitHub 检索云模板。

## 在 vRealize Automation Cloud Assembly 中配置 Bitbucket 集成

vRealize Automation Cloud Assembly 支持与 Bitbucket 集成，可将其用作 ABX 操作脚本和 VMware Cloud Templates 的基于 Git 的存储库。

在 vRealize Automation Cloud Assembly 中，可以使用 Bitbucket 集成处理两种类型的存储库项目：VMware Cloud Templates 或 ABX 操作脚本。在使用 Bitbucket 集成之前，必须同步要使用的项目。ABX 操作支持写回到 Bitbucket 存储库，但无法从集成写回云模板。如果要创建新版本的云模板文件，必须手动执行此操作。

### 前提条件

- 在要用于部署的一个或多个基于 ABX 或云模板的项目中设置内部 Bitbucket 服务器部署。当前不支持 Bitbucket 云。
- 创建或指定 vRealize Automation Cloud Assembly 项目以关联您的 Bitbucket 集成。
- 要同步到 Bitbucket 集成的云模板文件必须命名为 `blueprint.yaml`。

### 步骤

- 1 选择**基础架构 > 连接 > 集成**，然后单击**添加集成**。
- 2 选择“Bitbucket”。
- 3 在 Bitbucket 新集成“摘要”页面上输入摘要信息和 Bitbucket 凭据。
- 4 要检查集成，请单击**验证**。

- 5 如果使用添加标记以支持标记策略，请输入功能标记。请参见[如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署和创建标记策略](#)。
- 6 单击**添加**。
- 7 在 Bitbucket 集成的主页面上选择“项目”选项卡，以将项目与此 Bitbucket 集成相关联。
- 8 选择要与此 Bitbucket 集成关联的项目。
- 9 单击**下一步**将存储库添加到 Bitbucket 项目，并指示要添加的存储库类型，然后指定**存储库名称和分支以及文件夹**。
- 10 单击**添加**。

如果要将一个或多个存储库添加到项目，请单击**添加存储库**。

## 结果

Bitbucket 集成配置了指定的存储库配置，您可以查看和使用已配置的存储库中包含的 ABX 操作和云模板。将项目添加到 Bitbucket 集成时，同步操作将运行，以从指定的存储库提取最新版本的 ABX 操作脚本和云模板文件。Bitbucket 集成页面上的“历史记录”选项卡显示了集成的所有同步操作的记录。默认情况下，文件每 15 分钟自动同步一次，但您可以随时选择某文件并单击**同步**来手动同步该文件。

## 后续步骤

可以在 vRealize Automation Cloud Assembly “可扩展性”页面上使用 ABX 操作，也可以在“设计”页面上使用云模板。如果在 vRealize Automation Cloud Assembly 的“可扩展性”区域中保存 ABX 操作的更改版本，则会创建新版本的脚本并写回到存储库。

## 如何在 vRealize Automation 中配置外部 IPAM 集成

可以创建提供程序特定的外部 IPAM 集成点，以管理云模板部署中使用的 IP 地址。使用外部 IPAM 集成点时，将从指定的 IPAM 提供程序（而非 vRealize Automation）获取 IP 地址并由其管理。

可以在 vRealize Automation 中创建提供程序特定的 IPAM 集成点，以管理云模板部署和虚拟机的 IP 地址和 DNS 设置。

有关如何配置必备条件的信息，以及如何在示例工作流的上下文中创建提供程序特定的外部 IPAM 集成点的示例，请参见在[vRealize Automation 中为 Infoblox 添加外部 IPAM 集成](#)。请注意，此工作流适用于 Infoblox IPAM 集成，但可以用作任何外部 IPAM 供应商的参考。

有关如何创建所需资产以使外部 IPAM 合作伙伴和供应商能够将其 IPAM 解决方案与 vRealize Automation 集成的信息，请参见[如何使用 IPAM SDK 为 vRealize Automation 创建提供程序特定的外部 IPAM 集成软件包](#)。

## 前提条件

- 确认您具有云管理员凭据。请参见在[vRealize Automation 中使用云帐户所需的凭据](#)。
- 确认您具有云管理员用户角色。请参见[vRealize Automation 用户角色是什么](#)。
- 确认您具有外部 IPAM 提供程序（例如 Infoblox 或 Bluecat）的帐户，并且具有使用 IPAM 提供程序访问组织帐户的正确访问凭据。

- 确认您有权访问 IPAM 提供程序（例如 Infoblox 或 BlueCat）的已部署集成软件包。部署的软件包最初从 IPAM 提供程序或 vRealize Automation 商城以 .zip 形式下载，然后部署到 vRealize Automation。
- 确认您有权访问为 IPAM 提供程序配置的运行环境。
- 如果使用的是基于操作的可扩展性 (ABX) 内部部署嵌入式运行环境，请确认 vRealize Automation 网络中具有能够将出站流量传递到外部站点（如 gcr.io 和 storage.googleapis.com）的 HTTP 代理服务器。有关详细信息，请参见在 [vRealize Automation 8.x 中通过代理提取 Docker 映像 \(75180\)](#)。
- 确认您具有访问和使用 IPAM 供应商产品所需的用户凭据。有关所需用户权限的信息，请参见集成供应商的产品文档。

### 步骤

- 1 选择**基础架构 > 连接 > 集成**，然后单击**添加集成**。
- 2 单击 **IPAM**。
- 3 在**提供程序**下拉列表中，选择已配置的 IPAM 提供程序软件包。

如果此列表为空，请单击**导入提供程序软件包**，导航到现有提供程序软件包 .zip 文件，然后选择该文件。如果没有此 .zip 文件，则可以从提供程序的网站或从 vRealize Automation 的**商城**选项卡获取该文件。

- 4 输入具有外部 IPAM 提供程序的帐户的管理员用户名和密码凭据以及所有其他（如果有）必填字段，如提供程序的主机名。
- 5 在**运行环境**下拉列表中选择一个现有的运行环境，例如基于操作的可扩展性内部部署集成点。

运行环境支持 vRealize Automation 和 IPAM 提供程序之间的通信。

IPAM 框架仅支持基于操作的可扩展性 (ABX) 内部部署嵌入式运行环境。

---

**注** 如果使用 Amazon Web Services 或 Microsoft Azure 云帐户作为集成运行环境，请确保 IPAM 提供程序设备符合以下条件：可以通过 Internet 进行访问，不位于 NAT 或防火墙后面，并且具有可公开解析的 DNS 名称。如果 IPAM 提供程序不可访问，则 Amazon Web Services Lambda 或 Microsoft Azure 函数无法与其相连接，集成将失败。

---

- 6 单击**验证**。
- 7 当系统提示您信任来自外部 IPAM 提供程序的自签名证书时，单击**接受**。  
接受自签名证书后，可以继续完成验证操作。
- 8 为此 IPAM 集成点输入一个名称，然后单击**添加**以保存新的 IPAM 集成点。  
将模拟数据收集操作。将从外部 IPAM 提供程序收集网络和 IP 地址数据。

## 如何在 vRealize Automation 中升级到较新的外部 IPAM 集成软件包

您可以升级现有的外部 IPAM 集成点升级，以获取供应商特定的 IPAM 集成软件包的较新版本。

外部 IPAM 提供程序或 VMware 可以升级特定供应商的源 IPAM 集成软件包。例如，Infoblox 的外部 IPAM 集成软件包已多次升级。要保留使用命名的 IPAM 集成点的任何现有 vRealize Automation 基础架构设置，您可以编辑 IPAM 集成点以获取更新的 IPAM 集成软件包，而不是创建新的 IPAM 集成点。

### 前提条件

此过程假定您已创建外部 IPAM 集成点，并希望升级该集成点，以使用供应商的 IPAM 集成软件包的较新版本。

有关如何创建外部 IPAM 集成点的信息，请参见在 [vRealize Automation 中为 Infoblox 添加外部 IPAM 集成](#)。

- 确认您具有云管理员凭据。请参见在 [vRealize Automation 中使用云帐户所需的凭据](#)。
- 确认您具有云管理员用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 确认您具有外部 IPAM 提供程序的帐户，并且具有使用 IPAM 提供程序访问组织帐户的正确访问凭据。
- 确认您有权访问 IPAM 提供程序的已部署集成软件包。部署的软件包最初从 IPAM 提供程序网站或 vRealize Automation 商城以 .zip 形式下载，然后部署到 vRealize Automation。

有关如何下载和部署提供程序软件包 .zip 文件并使其在“IPAM 集成”页面上可作为提供程序值提供的信息，请参见 [下载并部署外部 IPAM 提供程序软件包以在 vRealize Automation 中使用](#)。

- 确认您有权访问为 IPAM 提供程序配置的运行环境。运行环境通常是一个基于操作的可扩展性 (ABX) 内部部署嵌入式集成点。

有关运行环境特性的信息，请参见在 [vRealize Automation 中为 IPAM 集成点创建运行环境](#)。

### 步骤

- 1 选择**基础架构 > 连接 > 集成 IPAM**，然后打开现有的 IPAM 集成点。
- 2 单击**管理提供程序**。
- 3 导航到更新的 IPAM 集成软件包并将其导入。
- 4 单击**验证**，然后单击**保存**。

## 在 vRealize Automation Cloud Assembly 中配置 My VMware 集成

您可以将 My VMware 与 vRealize Automation Cloud Assembly 集成，以支持 VMware 相关的操作和功能，例如访问 VMware Marketplace 以获取云模板。

每个组织只能创建一个 My VMware 集成。

### 前提条件

您必须拥有对 My VMware 具有相应权限的用户帐户。

- 有关邀请用户加入 My VMware 帐户的信息，请参见[知识库文章 2070555](#)。

- 有关在 My VMware 帐户中分配用户权限的信息，请参见[知识库文章 2006977](#)。

#### 步骤

- 1 选择**基础架构 > 连接 > 集成**，然后单击**添加集成**。
- 2 选择 My VMware。
- 3 在 My VMware 配置页面上输入所需的信息。
- 4 如果需要标记以支持标记策略，请输入功能标记。请参见[如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署和创建标记策略](#)。
- 5 单击**添加**。

#### 结果

My VMware 可与云模板配合使用。

#### 后续步骤

将 My VMware 组件添加到所需的云模板。

## 在 Cloud Assembly 中配置 vRealize Orchestrator 集成

您可以配置一个或多个 vRealize Orchestrator 集成，以便可以使用工作流作为可扩展性的一部分。

vRealize Automation 包含可用于可扩展性订阅的预配置 vRealize Orchestrator 实例。还可以从 vRealize Automation 云服务控制台访问嵌入式 vRealize Orchestrator 的客户端。

通过将 vRealize Orchestrator 集成到 vRealize Automation Cloud Assembly，您可以添加外部 vRealize Orchestrator 实例，并使用可扩展性订阅中包含的工作流库。有关详细信息，请参见[可扩展性工作流订阅](#)。

#### 前提条件

- 确认您具有云管理员凭据。有关详细信息，请参见 [vRealize Automation 用户角色是什么](#)。
- 升级或迁移到 vRealize Orchestrator 8.1。请参见《[升级和迁移 VMware vRealize Orchestrator](#)》。

#### 步骤

- 1 选择**基础架构 > 连接 > 集成**。
- 2 单击**添加集成**。
- 3 选择 vRealize Orchestrator。
- 4 在 vRealize Automation Cloud Assembly 中，输入 vRealize Orchestrator 实例的 URL。
- 5 要验证集成，请单击**验证**。
- 6 输入 vRealize Orchestrator 集成的名称。
- 7 （可选）输入 vRealize Orchestrator 集成的描述。

- 8 (可选) 添加功能标记。有关功能标记的详细信息, 请参见在 [vRealize Automation Cloud Assembly 中使用功能标记](#)。

---

**注** 可使用功能标记管理多个 vRealize Orchestrator 集成。请参见[使用项目限制管理多个 vRealize Orchestrator 集成](#)。

---

- 9 单击**添加**。

将保存 vRealize Orchestrator 集成。

#### 后续步骤

要验证集成是否已配置且工作流是否已添加, 请选择**可扩展性 > 库 > 工作流**。

## 使用项目限制管理多个 vRealize Orchestrator 集成

您可以使用项目限制来管理在工作流订阅中使用的 vRealize Orchestrator 集成。

vRealize Automation Cloud Assembly 支持集成多个可在工作流订阅中使用的 vRealize Orchestrator 服务器。可以使用软或硬项目限制管理由项目置备的云模板中使用的 vRealize Orchestrator 集成。有关项目限制的详细信息, 请参见[使用 vRealize Automation Cloud Assembly 项目标记和自定义属性](#)。

#### 前提条件

- 确认您具有云管理员凭据。请参见 [vRealize Automation 用户角色是什么](#)。
- 在 vRealize Automation Cloud Assembly 中配置两个或更多 vRealize Orchestrator 集成。请参见在 [Cloud Assembly 中配置 vRealize Orchestrator 集成](#)。
- 将功能标记添加到您的 vRealize Orchestrator 集成。请参见在 [vRealize Automation Cloud Assembly 中使用功能标记](#)。

#### 步骤

- 1 导航到**基础架构 > 管理 > 项目**, 然后选择您的项目。
- 2 选择**置备**选项卡。
- 3 在**可扩展性限制**文本框中输入 vRealize Orchestrator 集成的功能标记, 然后将其设置为软或硬项目限制。
- 4 单击**保存**。

#### 结果

当部署云模板时, vRealize Automation Cloud Assembly 使用项目限制来管理在工作流订阅中使用的 vRealize Orchestrator 集成。

#### 后续步骤

或者, 也可以使用功能标记在云帐户级别管理多个 vRealize Orchestrator 集成。有关详细信息, 请参见[使用云帐户功能标记管理多个 vRealize Orchestrator 集成](#)。



## 使用云帐户功能标记管理多个 vRealize Orchestrator 集成

您可以使用功能标记来管理在工作流订阅中使用的 vRealize Orchestrator 集成。

vRealize Automation Cloud Assembly 支持集成多个可在工作流订阅中使用的 vRealize Orchestrator 服务器。您可以通过向您的云帐户添加功能标记来管理在工作流订阅中使用的 vRealize Orchestrator 集成。

### 前提条件

- 确认您具有云管理员凭据。请参见 [vRealize Automation 用户角色是什么](#)。
- 在 vRealize Automation Cloud Assembly 中配置两个或更多 vRealize Orchestrator 集成。有关详细信息，请参见在 [Cloud Assembly 中配置 vRealize Orchestrator 集成](#)。
- 将功能标记添加到您的 vRealize Orchestrator 集成。请参见在 [vRealize Automation Cloud Assembly 中使用功能标记](#)。

### 步骤

- 1 导航到**基础架构 > 连接 > 云帐户**。
- 2 选择您的云帐户。
- 3 输入要使用的 vRealize Orchestrator 集成的功能标记。

功能标记将自动转换为软限制。要在管理集成时使用硬限制，您必须使用项目限制。有关详细信息，请参见[使用项目限制管理多个 vRealize Orchestrator 集成](#)。

- 4 单击**保存**。

### 结果

当部署云模板时，vRealize Automation Cloud Assembly 使用关联云帐户中的标记来管理在工作流订阅中使用的 vRealize Orchestrator 集成。

## 如何在 vRealize Automation Cloud Assembly 中使用 Kubernetes

vRealize Automation Cloud Assembly 提供了多种用于管理和部署 Kubernetes 资源的选项。

在 vRealize Automation Cloud Assembly 中有两个使用 Kubernetes 资源的主要选项。可以将 VMware Tanzu Kubernetes Grid Integrated Edition (TKGI)（以前称为 PKS）或 Red Hat OpenShift 与 vRealize Automation Cloud Assembly 相集成，以便配置、管理和部署 Kubernetes 资源。使用第二个选项，可以利用 vCenter 云帐户访问主管命名空间，以便使用基于 vSphere Project Pacific Kubernetes 的功能。此外，还可以在 vRealize Automation Cloud Assembly 中集成外部 Kubernetes 资源。

### 使用 VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) 或 Openshift 集成

对于 TKGI、外部集群或 Openshift 配置，vRealize Automation Cloud Assembly 提供了一个 Kubeconfig，让用户能够访问适用的 Kubernetes 集群。

创建 TKGI 或 OpenShift 集成后，适用的 Kubernetes 集群将在 vRealize Automation Cloud Assembly 中变得可用，您可以在 vRealize Automation Cloud Assembly 中添加和创建 Kubernetes 组件以支持集群和容器应用程序的管理。这些应用程序构成了可从 Service Broker 目录中获得的自助服务部署的基础。



## 使用 vSphere Project Pacific Kubernetes 集群

Project Pacific 是 vSphere 增强功能，使用 Kubernetes 作为其控制平面。借助该功能，您可以通过一个界面同时管理虚拟机和容器。vRealize Automation Cloud Assembly 让用户能够利用已嵌入到 vSphere 中的 Pacific Kubernetes 功能。您可以通过创建包含主管集群的 vSphere 实施与 vCenter 部署的集成来访问 Pacific 功能。借助 Pacific，您可以从 vCenter 同时管理常规虚拟机和 Kubernetes 集群。

对于基于 Pacific 的主管命名空间，用户必须能够访问适用的 vSphere SSO，以便登录所提供的主管命名空间详细信息链接。然后，用户可以下载使用 vSphere 身份验证的自定义 Kubectl，以便能够使用其主管命名空间。

要使用此功能，您的 vCenter 中必须具有配置了主管命名空间的 vSphere 云帐户。用户登录后，可以开始使用适用的命名空间。

- [在 vRealize Automation Cloud Assembly 中配置 PKS 集成](#)

可以在内部部署和云中配置 PKS 资源连接，以在 vRealize Automation Cloud Assembly 中支持 Kubernetes 集成和管理功能。

- [在 vRealize Automation Cloud Assembly 中配置 Red Hat OpenShift 集成](#)

可以在内部部署和云中配置 Red Hat OpenShift 资源连接，以在 vRealize Automation Cloud Assembly 中支持企业级 Kubernetes 集成和管理功能。

- [在 vRealize Automation Cloud Assembly 中配置 Kubernetes 区域](#)

通过 Kubernetes 区域，云管理员可以定义如何基于策略布置在 vRealize Automation Cloud Assembly 部署中使用的 Kubernetes 集群和命名空间以及主管命名空间。管理员可以使用此页面指定哪些集群可用于置备 Kubernetes 命名空间，以及可接受哪些属性用于集群。

- [在 vRealize Automation Cloud Assembly 中使用 Pacific 主管集群和命名空间](#)

管理员可以将 vRealize Automation Cloud Assembly 配置为使用已启用 Pacific 的现有 vSphere 集成中的主管命名空间，以使用户可以在云模板中部署命名空间并在 Service Broker 目录中进行请求。

- [在 vRealize Automation Cloud Assembly 中使用 Kubernetes 集群和命名空间](#)

Kubernetes 集群和命名空间是 Kubernetes 部署的基础，无论是常规型还是基于 Pacific，都可以在 vRealize Automation Cloud Assembly 中添加、查看和管理其配置。

- [在 vRealize Automation Cloud Assembly 中将 Kubernetes 组件添加到云模板](#)

将 Kubernetes 组件添加到 vRealize Automation Cloud Assembly 云模板时，可以选择添加集群或允许用户在各种配置中创建命名空间。通常，此选择取决于您的访问控制要求、Kubernetes 组件的配置方式以及您的部署要求。

- [配合使用 vRealize Automation Cloud Assembly 可扩展性与 Kubernetes](#)

vRealize Automation Cloud Assembly 提供一组标准事件主题，它们对应于与 Kubernetes 集群部署相关的典型操作。用户可以根据需要订阅这些主题，他们会在发生与已订阅主题相关的事件时收到通知。您还可以将 vRO 工作流配置为基于事件通知运行。

## 在 vRealize Automation Cloud Assembly 中配置 PKS 集成

可以在内部部署和云中配置 PKS 资源连接，以在 vRealize Automation Cloud Assembly 中支持 Kubernetes 集成和管理功能。

通过 PKS 集成，您可以管理内部部署和云中的 PKS 实例以及在 PKS 上置备的 Kubernetes 集群和外部集群。您必须创建 Kubernetes 配置文件并将其与项目相关联，以支持基于策略的资源布置。

### 前提条件

- 您必须使用 UAA 身份验证设置适当配置的 Pivotal Container Service (PKS) 服务器。
- 确认您具有云管理员凭据。有关详细信息，请参见 [vRealize Automation 用户角色是什么](#)。

### 步骤

- 1 选择**基础架构 > 连接 > 集成**，然后单击**添加集成**。
- 2 选择“VMware Enterprise PKS”。
- 3 输入要创建的 PKS 云帐户的 IP 地址或 FQDN 以及 PKS 地址。
  - IP 地址是 PKS 用户身份验证服务器的 FQDN 或 IP 地址。
  - PKS 地址是主 PKS 服务器的 FQDN 或 IP 地址。
- 4 选择此 PKS 服务器是位于本地，还是位于公有云或私有云上。
- 5 输入 PKS 服务器的相应**用户名**和**密码**及其他相关信息。
- 6 如果使用标记以支持标记策略，请输入功能标记。请参见[如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署和创建标记策略](#)。
- 7 单击**添加**。

### 结果

您可以创建 Kubernetes 区域并将其分配给项目，也可以发现外部 Kubernetes 集群并将这些集群分配给项目。此外，还可以添加或创建 Kubernetes 命名空间，以便于管理大型组和组织中的集群。

### 后续步骤

创建或选择相应的 Kubernetes 区域，然后选择一个或多个集群或命名空间，并将其分配给项目。之后，您可以创建并发布云模板，以使用户能够生成使用 Kubernetes 的自助服务部署。

## 在 vRealize Automation Cloud Assembly 中配置 Red Hat OpenShift 集成

可以在内部部署和云中配置 Red Hat OpenShift 资源连接，以在 vRealize Automation Cloud Assembly 中支持企业级 Kubernetes 集成和管理功能。

vRealize Automation Cloud Assembly 支持与 OpenShift 版本 3.x 集成。

### 前提条件

- 您必须具有适当配置的 Red Hat OpenShift 实现。
- 确认您具有云管理员凭据。有关详细信息，请参见 [vRealize Automation 用户角色是什么](#)。

- VMware 在以下位置提供了可用于使用云模板创建 OpenShift 集群的资源：<https://flings.vmware.com/enterprise-openshift-as-a-service-on-cloud-automation-services>。您可以将使用这些资源创建的集群用作 Kubernetes 区域中的全局集群以创建自助命名空间。

### 步骤

- 1 选择**基础架构 > 连接 > 集成**，然后单击**添加集成**。
- 2 选择“Red Hat OpenShift”。
- 3 输入 OpenShift 服务器的**地址**和**位置**。
- 4 选择适当的**凭据类型**并输入相应的凭据。  
OpenShift 集成支持 OAuth 用户名/密码、公钥或持有者令牌身份验证。
- 5 为 OpenShift 集成输入适当的**名称**和**描述**。
- 6 如果使用标记以支持标记策略，请输入适当的功能标记。请参见[如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署和创建标记策略](#)。
- 7 单击**添加**。

### 结果

创建集成时，新的 Kubernetes 集群将显示在 Kubernetes 页面的相关部分中。可以创建 Kubernetes 区域并将其分配给项目。此外，还可以配置 Kubernetes 命名空间，以便于在大型组和组织之间管理集群。

### 后续步骤

创建或选择相应的 Kubernetes 区域，然后选择一个或多个集群或命名空间，并将其分配给项目。之后，您可以创建并发布云模板，以使用户能够生成使用 Kubernetes 的自助服务部署。

## 在 vRealize Automation Cloud Assembly 中配置 Kubernetes 区域

通过 Kubernetes 区域，云管理员可以定义如何基于策略布置在 vRealize Automation Cloud Assembly 部署中使用的 Kubernetes 集群和命名空间以及主管命名空间。管理员可以使用此页面指定哪些集群可用于置备 Kubernetes 命名空间，以及可接受哪些属性用于集群。

云管理员可以将 Kubernetes 区域与为 Cloud Assembly 配置的 PKS 云帐户关联，或者与尚未和项目关联的外部 Kubernetes 集群关联。

创建 Kubernetes 区域时，您可以为该区域分配提供程序特定的多个资源，这些资源将指示可以根据工作线程数、主节点、可用 CPU 数、内存和其他配置设置为新置备的集群设置哪些属性。对于 PKS 提供程序，这些提供程序与 PKS 计划相对应。管理员还可以向将用于布置新置备的 Kubernetes 命名空间的 Kubernetes 区域分配多个集群。管理员只能分配未载入或不受 CMX 管理，并通过预选集群提供程序进行置备的集群。管理员可以向单个项目分配多个 Kubernetes 区域，从而使它们全部可用于在此项目中发生的布置操作。

云管理员可以分多个级别分配优先级。

- 项目内的 Kubernetes 区域优先级。
- Kubernetes 区域内的资源优先级。

- Kubernetes 区域内的集群优先级。

云管理员还可以分多个级别分配标记：

- 每个 Kubernetes 区域的功能标记。
- 每个资源分配的标记。
- 每个集群分配的标记。

可以使用与常规 Kubernetes 命名空间相同的方式，使用 vSphere 上主管命名空间创建 Kubernetes 区域。要将主管命名空间添加到 Kubernetes 区域，必须将该区域与包含所需 Pacific 命名空间资源的 vSphere 7 端点相关联。

Service Broker 包含“Kubernetes 区域”页面的一个版本，使 Service Broker 管理员能够访问现有的 Kubernetes 区域，以便他们可以为从目录置备的 Kubernetes 命名空间和集群创建布置策略。

### 前提条件

配置与合适 PKS 部署的集成。请参见在 [vRealize Automation Cloud Assembly 中配置 PKS 集成](#)

### 步骤

- 1 选择**基础架构 > 配置 > Kubernetes 区域**，然后单击**新建 Kubernetes 区域**。

- 2 输入要将此区域应用到的 PKS 集成**帐户**名称。

这将定义与该区域关联的云帐户或端点。只能为每个区域分配一个端点。如果使用的是 vSphere 上的主管命名空间，则只能在此处选择包含主管命名空间的 vSphere 实例。

- 3 为 Kubernetes 区域添加**名称**和**描述**。

- 4 如果适用，添加功能标记。有关详细信息，请参见在 [vRealize Automation Cloud Assembly 中使用功能标记](#)。

- 5 单击**保存**。

- 6 单击“按需”选项卡，然后根据需要为要用于集群置备的区域添加 PKS 计划。

您可以选择一个或多个计划，并为其分配优先级。数字越小，优先级越高。优先级分配次于基于标记的选择。

- 7 单击“集群”选项卡，然后单击**添加计算资源**按钮将 Kubernetes 集群或主管集群添加到区域。如果使用的是外部集群，则在选择时会将其自动载入到 vRealize Automation Cloud Assembly。

您可以在 vRealize Automation Cloud Assembly 中的“Kubernetes 集群”页面上向集群添加 Kubernetes 命名空间。

### 结果

Kubernetes 区域已配置，可与 vRealize Automation Cloud Assembly 部署配合使用。

### 后续步骤

向项目分配 Kubernetes 区域。

- 1 选择**基础架构 > 管理 > 项目**，然后选择要与 Kubernetes 区域关联的项目。

- 2 单击“项目”页面上的“Kubernetes 置备”选项卡。
- 3 单击**添加 Kubernetes 区域**并添加刚刚创建的区域。如果适用，您可以设置多个区域，还可以对区域设置优先级。
- 4 单击**保存**。

将区域分配给项目后，您可以使用“设计”选项卡下的“云模板”页面，根据 Kubernetes 区域和项目配置来置备部署。此“云模板”页面包括用于添加 K8S 集群、K8S 命名空间和主管命名空间的选项。根据使用的 Kubernetes 资源选择适当的选项。

## 在 vRealize Automation Cloud Assembly 中使用 Pacific 主管集群和命名空间

管理员可以将 vRealize Automation Cloud Assembly 配置为使用已启用 Pacific 的现有 vSphere 集成中的主管命名空间，以便用户可以在云模板中部署命名空间并在 Service Broker 目录中进行请求。

此任务将介绍如何使用 vRealize Automation Cloud Assembly 添加主管集群以便在部署中使用，以及如何创建或添加用于定义哪些 vRealize Automation Cloud Assembly 项目和用户可以访问特定 Kubernetes 资源的命名空间。此功能依赖于合适的 vSphere 云帐户，而不是 PKS 或 Openshift 等集成。主管集群是与 vSphere 关联的自定义 Kubernetes 集群。它们向最终用户公开 Kubernetes API，并将 ESXi（而非 Linux）用作 Worker 节点的平台。主管命名空间有助于对 Kubernetes 资源进行访问控制，因为将策略应用于命名空间通常比应用于各个虚拟机更容易。可以为每个主管集群创建多个命名空间。

与已启用 Pacific 的 vSphere 实例一起使用时，Kubernetes 区域将定义哪些主管集群可用于通过主管命名空间进行置备。主管命名空间特定于已启用 Pacific 的 vSphere 实例。无法将通用 Kubernetes 资源置备到已启用 Pacific 的 vSphere 实例。

指定为项目查看者的 vRealize Automation Cloud Assembly 用户对命名空间具有仅查看访问权限，而项目成员可以编辑命名空间。

如果需要，可以配置与命名空间关联的主管集群。

### 前提条件

- 要在 vRealize Automation Cloud Assembly 中使用 Pacific 命名空间，必须配置 vSphere 7.x 端点。vSphere 作为 vCenter 云帐户的一部分进行安装。请参见在 [vRealize Automation 中创建 vCenter 云帐户](#)。
- Pacific 项目必须在 vSphere 云帐户上启用，并且必须包含相应的主管命名空间。
- 您的 vCenter 和 vRealize Automation 部署应对要同步的用户使用相同的 Active Directory。尽管这种情况并非如此时置备仍会起作用，但 vRealize Automation 用户将无法自动访问命名空间。

### 步骤

- 1 在 vRealize Automation Cloud Assembly 中选择**基础架构 > 配置 > Kubernetes 区域**。  
此页面将显示可供使用的受管集群，且您可以在其中添加其他集群。可以单击任意集群以查看其详细信息。
- 2 选择**新建 Kubernetes 区域**。

- 3 指定目标 vSphere 云帐户的**帐户**详细信息。
- 4 单击文本框中的“搜索”图标，以查看所有 vSphere 帐户或按名称搜索帐户。
- 5 键入新区域的**名称**和**描述**。
- 6 如果适用，添加功能标记。有关详细信息，请参见在 [vRealize Automation Cloud Assembly](#) 中使用**功能标记**。
- 7 单击“置备”选项卡以选择将与命名空间关联的主管集群。
- 8 单击**添加计算资源**以查看并选择可用的主管集群。
- 9 单击**添加**。
- 10 选择**基础架构 > 管理 > 项目**，然后选择要与 Kubernetes 区域关联的项目。
- 11 单击“项目”页面上的“Kubernetes 置备”选项卡。
- 12 单击**添加 Kubernetes 区域**并添加刚刚创建的区域。如果适用，您可以设置多个区域，还可以对区域设置优先级。
- 13 单击**保存**。

#### 后续步骤

配置命名空间后，vRealize Automation Cloud Assembly 中适用用户的**基础架构 > 资源 > Kubernetes** 页面将显示该命名空间。用户可以单击“摘要”选项卡上的“地址”链接，打开 vSphere Kubernetes CLI 工具以管理命名空间。用户必须是云管理员或指定项目的命名空间的成员才能访问主管命名空间详细信息的链接。此外，用户还可以下载自定义 Kubectl 以使用主管命名空间。用户可以登录到主管命名空间，并像使用任何其他命名空间一样使用该命名空间，然后创建云模板并部署应用程序。

要将命名空间添加到云模板，请选择**设计 > 云模板**，然后选择现有云模板或创建新云模板。之后，可以在左侧菜单中选择“主管命名空间”项，并将其拖动到画布上。

部署包含主管命名空间的云模板后，用户也可以从 Service Broker 目录请求主管命名空间。此外，还可以在 Cloud Assembly 中单击“部署”页面，查看有关部署的信息以及访问包含对 vSphere 上的命名空间运行 kubectl 的命令的链接。

## 在 vRealize Automation Cloud Assembly 中使用 Kubernetes 集群和命名空间

Kubernetes 集群和命名空间是 Kubernetes 部署的基础，无论是常规型还是基于 Pacific，都可以在 vRealize Automation Cloud Assembly 中添加、查看和管理其配置。

您可以在**基础架构 > 资源 > Kubernetes** 页面上查看、添加和管理您有权访问的 Kubernetes 集群和命名空间。最常见的情况是，此页面可帮助管理部署的集群和命名空间。

- **集群**：集群是分布在一个或多个物理机上的**一组 Kubernetes 节点**。此页面显示已配置为可在 vRealize Automation Cloud Assembly 实例上使用的已置备但未部署的集群。您可以单击集群查看有关其当前状态的信息。部署集群时，包含指向 Kubconfig 文件的链接，此文件只能由云管理员进行访问。此文件授予对集群的完全管理员特权，包括命名空间列表。

主管集群为 vSphere 实例所独有，并使用 ESXi 作为其 Worker 节点，而不使用 Linux。



- **命名空间：**命名空间是虚拟集群，它为管理员提供了一种分隔集群资源的方法。它们有助于在大型用户组和组织之间管理资源。作为基于角色进行访问控制的一种形式，云管理员可以让用户在请求部署时将命名空间添加到项目，然后从“Kubernetes 集群”页面管理这些命名空间。部署命名空间时，包含指向 kubeconfig 文件的链接，该文件让有效用户（如开发人员）能够查看和管理该命名空间的某些方面。

主管命名空间仅存在于 vSphere 实例上，并提供对 vSphere 对象的类似 Kubernetes 的访问权限。

如果要配置新集群或现有集群，必须选择是使用主 IP 地址还是主节点主机名进行连接。

### 在 vRealize Automation Cloud Assembly 中使用常规 Kubernetes 集群

您可以使用此页面上的选项向 vRealize Automation Cloud Assembly 添加新集群、现有集群或外部集群。

- 1 选择**基础架构 > 资源 > Kubernetes**，并确认“集群”选项卡处于活动状态。

如果当前已为您的 vRealize Automation Cloud Assembly 实例配置任何集群，这些集群将显示在此页面上。

- 2 如果要添加新集群或现有集群，或者部署集群，请根据下表选择适当的选项。

选项	说明	详细信息
部署	向 vRealize Automation Cloud Assembly 添加新集群	您必须指定要将此集群部署到的 TKGI 云帐户以及所需计划和节点数。
添加现有项	配置现有集群以使用您的项目。	您必须指定 TKGI 云帐户、要使用的集群以及适用于目标开发人员的相应项目。此外，您还需要指定共享范围。如果要全局共享，必须相应地配置 Kubernetes 区域和命名空间。
添加外部项	将可能与 TKGI 没有关联的 vanilla Kubernetes 集群添加到 vRealize Automation Cloud Assembly。	您必须指定与集群关联的项目，输入所需集群的 IP 地址，然后选择连接到此集群所需的云代理和证书信息。

- 3 单击**添加**以使集群可在 vRealize Automation Cloud Assembly 中使用。

### 在 vRealize Automation Cloud Assembly 中使用 Kubernetes 命名空间

如果您是云管理员，则命名空间可帮助您对 Kubernetes 集群资源进行分组和管理。如果您是用户，则命名空间是 Kubernetes 集群内供您进行部署的区域。管理员和用户可以使用位于**基础架构 > 资源 > Kubernetes** 页面上的“命名空间”选项卡访问命名空间。

可通过多种方式将 Kubernetes 命名空间添加到 vRealize Automation Cloud Assembly 中的资源。以下过程概述了一种典型方法。

- 1 选择**基础架构 > 资源 > Kubernetes**，然后单击“命名空间”选项卡。
- 2 要添加新命名空间，请单击**新建命名空间**。要添加现有命名空间，请单击**添加命名空间**。
- 3 输入命名空间的**名称**和**描述**。

此时，您已添加一个可用于 Kubernetes 资源的命名空间，但此命名空间尚未与任何特定内容相关联。

- 4 指定要与此命名空间关联的**集群**。

5 单击**创建**将此命名空间添加到 vRealize Automation Cloud Assembly。

### 使用主管集群和主管命名空间

可以在 vRealize Automation Cloud Assembly 中的“Kubernetes”页面上查看和更改主管集群和命名空间的配置。

- 1 在 vRealize Automation Cloud Assembly 中选择**基础架构 > 资源 > Kubernetes**。
- 2 选择**添加主管集群**。
- 3 指定目标 vSphere 云帐户的帐户详细信息。
- 4 单击“主管集群”文本框中的“搜索”图标，以查看所有主管集群或按名称搜索集群。
- 5 选择所需的集群，然后单击**添加**。
- 6 选择“主管命名空间”选项卡，然后单击**新建主管命名空间**按钮以添加新的命名空间。
- 7 选择“主管命名空间”选项卡，然后单击**新建主管命名空间**按钮以添加新的命名空间。
  - a 如果要创建新命名空间，请添加**名称**和**描述**。
  - b 选择要与此命名空间关联的适当云**帐户**。
  - c 选择要与此命名空间关联的**主管集群**。
  - d 选择要与此命名空间关联的**项目**。
  - e 单击**创建**。
- 8 查看新命名空间的相关详细信息。

将在“用户”选项卡中列出当前有权访问 vSphere 中命名空间的用户和组。如果将新用户或组添加到项目中，请单击此选项卡上的**更新用户**按钮以更新列表。列表不会自动更新，因此必须使用按钮进行更新。

---

**注** 仅当 vRealize Automation Cloud Assembly 和 vCenter 配置了一个通用 Active Directory/LDAP 服务时，同步用户才有意义。

---

配置命名空间后，vRealize Automation Cloud Assembly 中适用用户的**基础架构 > 资源 > Kubernetes**页面将显示该命名空间。用户可以单击“摘要”选项卡上的“地址”链接，打开 vSphere Kubernetes CLI 工具以管理命名空间。用户必须是云管理员或指定项目的命名空间的成员才能访问主管命名空间详细信息的链接。此外，用户还可以下载自定义 Kubectl 以使用主管命名空间。用户可以登录到主管命名空间，并像使用任何其他命名空间一样使用该命名空间，然后创建云模板并部署应用程序。

### 在 vRealize Automation Cloud Assembly 中将 Kubernetes 组件添加到云模板

将 Kubernetes 组件添加到 vRealize Automation Cloud Assembly 云模板时，可以选择添加集群或允许用户在各种配置中创建命名空间。通常，此选择取决于您的访问控制要求、Kubernetes 组件的配置方式以及您的部署要求。

要在 vRealize Automation Cloud Assembly 中将 Kubernetes 组件添加到云模板，请选择**设计 > 云模板**，单击**新建**，然后在左侧菜单中找到并展开 Kubernetes 选项。然后，通过将所需选项（集群或 KBS 命名空间）拖动到画布做出选择。



将与项目关联的 **Kubernetes** 集群添加到云模板是使 **Kubernetes** 资源可供有效用户使用的最简单方法。您可以在集群上使用标记来控制其部署位置，就像处理其他 **Cloud Assembly** 资源一样。在集群部署的分配阶段，可以使用标记选择区域和 **VMware Tanzu Kubernetes Grid Integrated Edition (TKGI)** 计划。通过这种方式添加集群后，该集群将自动可供所有有效用户使用。

### 云模板示例

第一个云模板示例显示了通过标记控制的简单 **Kubernetes** 部署的模板。创建的 **Kubernetes** 区域包含两个部署计划，并在“新建 **Kubernetes** 区域”页面上进行配置。在此示例中，一个名为 `placement:tag` 的标记添加为该区域中的一个功能，并用于匹配云模板上的类似限制。如果有多个区域配置了此标记，将选择具有最低优先级编号的区域。

```
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
```

第二个云模板示例显示了如何使用名为 `$(input.hostname)` 的变量设置模板，以便用户可以在请求部署时输入所需的集群主机名。在集群部署的资源分配阶段，也可以使用标记选择区域和 **TKGI** 计划。

```
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
```

如果要使用命名空间管理集群使用情况，可以在云模板中设置一个名为 `name: ${input.name}` 的变量来替代用户在请求部署时输入的命名空间名称。对于此类部署，您需要创建一个如下示例所示的模板：

```
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}

```

用户可以通过 kubeconfig 文件管理部署的集群，这些文件可从[基础架构 > 资源 > Kubernetes 集群](#)页面访问。在页面上找到所需集群对应的卡视图，然后单击 **Kubeconfig**。

## VMware Cloud Templates 中的主管命名空间

以下是 vRealize Automation Cloud Assembly 云模板中基本主管命名空间的结构定义。

```

{
  "title": "Supervisor namespace schema",
  "description": "Request schema for provisioning of Supervisor namespace resource",
  "type": "object",
  "properties": {
    "name": {
      "title": "Name",
      "description": "Alphabetic (a-z and 0-9) string with maximum length of 63 characters. The character '-' is allowed anywhere except the first or last position of the identifier.",
      "type": "string",
      "pattern": "^[a-z0-9-]{1,63}$",
      "ignoreOnUpdate": true
    },
    "description": {
      "title": "Description",
      "description": "An optional description of this Supervisor namespace.",
      "type": "string",
      "ignoreOnUpdate": true
    },
    "constraints": {
      "title": "Constraints",
      "description": "To target the correct resources, blueprint constraints are matched against infrastructure capability tags. Constraints must include the key name. Options include value, negative [!], and hard or soft requirement.",
      "type": "array",
      "recreateOnUpdate": true,
      "items": {
        "type": "object",
        "properties": {
          "tag": {
            "title": "Tag",
            "description": "Constraint definition in syntax `[!]tag_key[:tag_value][:hard|:soft]` \nExamples:\n!location:eu:hard\n location:us:soft\n!pci\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 支持对主管命名空间使用限制。通过使用限制，可以控制 CPU 和内存资源的使用，以及已部署计算机在命名空间中允许的最大 pod 数。

```

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

```

## 配合使用 vRealize Automation Cloud Assembly 可扩展性与 Kubernetes

vRealize Automation Cloud Assembly 提供一组标准事件主题，它们对应于与 Kubernetes 集群部署相关的典型操作。用户可以根据需要订阅这些主题，他们会在发生与已订阅主题相关的事件时收到通知。您还可以将 vRO 工作流配置为基于事件通知运行。

以下主题可在 vRealize Automation Cloud Assembly 中的**可扩展性 > 库 > 事件主题**页面上进行订阅。要查看这些主题，请在“事件主题搜索”文本框中搜索 Kubernetes。

- Kubernetes 集群分配
- Kubernetes 集群置备后
- Kubernetes 集群移除后
- Kubernetes 集群置备
- Kubernetes 集群移除

单击这些主题之一以查看该主题的结构定义，其中显示了收集和传输的所有信息。您可以使用任何结构定义信息来设置各种通知和管理任务及报告任务。

您可以在**可扩展性 > 库 > 操作**页面上设置 CMX 相关操作的操作脚本。操作脚本可用于各种用途：例如创建 Kubernetes 集群置备的 DNS 记录。如果要创建 DNS 记录，可以使用操作脚本中具有 REST 命令的 Kubernetes 集群置备后主题中的 `masternodeips` 字段来创建 DNS 记录。

“订阅”页面定义事件主题和操作脚本之间的关系。您可以在 vRealize Automation Cloud Assembly 中的“订阅”页面上查看和管理这些组件。

## 什么是 vRealize Automation Cloud Assembly 中的配置管理

vRealize Automation Cloud Assembly 支持与 Puppet Enterprise、Ansible 开源和 Ansible Tower 集成，以便您可以根据配置和偏差管理部署。

### Puppet 集成

要集成基于 Puppet 的配置管理，必须在具有 vSphere 工作负载的公共或私有云上安装一个有效的 Puppet Enterprise 实例。必须在此外部系统与 vRealize Automation Cloud Assembly 实例之间建立连接。然后，可以通过将 Puppet 配置管理添加到相应的蓝图，使其供 vRealize Automation Cloud Assembly 使用。

vRealize Automation Cloud Assembly 蓝图服务 Puppet 提供程序在已部署的计算资源上安装、配置和运行 Puppet 代理。Puppet 提供程序同时支持 SSH 和 WinRM 连接，并具备以下必备条件：

- SSH 连接：
  - 要运行具有 NOPASSWD 的命令，用户名必须是超级用户或具有 `sudo` 权限的用户。
  - 针对给定用户禁用 `requiretty`。
  - cURL 必须在部署计算资源上可用。
- WinRM 连接：
  - PowerShell 2.0 必须在部署计算资源上可用。
  - 按照 vRealize Orchestrator 文档中的说明配置 Windows 模板。

DevOps 管理员负责管理与 Puppet Master 的连接，并将 Puppet 角色或配置规则应用于特定部署。执行以下部署后，配置为支持配置管理的虚拟机将注册到指定的 Puppet Master。

部署虚拟机时，用户可以添加或删除作为外部系统的 Puppet Master 或更新分配给 Puppet Master 的项目。最后，当虚拟机取消配置时，相应的用户可以从 Puppet Master 取消注册已部署的虚拟机。

## Ansible 开源集成

设置 Ansible 集成时，请按照 Ansible 安装说明安装 Ansible 开源。有关安装的更多信息，请参见 Ansible 文档。

默认情况下，Ansible 启用主机密钥检查。如果重新安装 known\_hosts 文件中的主机时使用不同的密钥，则会出现错误消息。如果主机未列在 known\_hosts 文件中，则您必须在启动时提供密钥。您可以通过 /etc/ansible/ansible.cfg 或 ~/.ansible.cfg 文件中的以下设置禁用主机密钥检查：

```
[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
```

要避免主机密钥检查错误，请将 host\_key\_checking 和 record\_host\_keys 设置为 False，包括添加在 ssh\_args 中设置的额外选项 UserKnownHostsFile=/dev/null。此外，如果清单最初为空，Ansible 会警告主机列表为空。这会导致 Playbook 语法检查失败。

通过 Ansible 保管库，可以加密文件而非纯文本形式存储敏感信息（如密码或密钥）。保管库使用密码进行加密。在 vRealize Automation Cloud Assembly 中，Ansible 使用保管库对主机的 ssh 密码等数据进行加密。它会假设已设置保管库密码的路径。

可以修改 ansible.cfg 文件，使用以下格式指定密码文件的位置。

```
vault_password_file = /path to/file.txt
```

还可以设置 ANSIBLE\_VAULT\_PASSWORD\_FILE 环境变量，以便 Ansible 自动搜索密码。例如，ANSIBLE\_VAULT\_PASSWORD\_FILE=~/.vault\_pass.txt

vRealize Automation Cloud Assembly 管理 Ansible 清单文件，因此必须确保 vRealize Automation Cloud Assembly 用户对清单文件具有 rwx 访问权限。

```
cat ~/var/tmp/vmware/provider/user_defined_script/$(ls -t ~/var/tmp/vmware/provider/
user_defined_script/ | head -1)/log.txt
```

如果要使用具有 vRealize Automation Cloud Assembly 开源集成的非 root 用户，则用户需要一组权限来运行 vRealize Automation Cloud Assembly 开源提供程序所使用的命令。必须在用户的 sudoers 文件中设置以下命令。

```
Defaults:myuser !requiretty
```

如果用户不属于未指定 `askpass` 应用程序的管理员组，请在用户的 `sudoers` 文件中设置以下命令。

```
myuser ALL=(ALL) NOPASSWD: ALL
```

如果在设置 Ansible 集成时遇到错误或其他问题，请参阅位于 Ansible 控制计算机上的 `'cat~/var/tmp/vmware/provider/user_defined_script/$(ls -t ~/var/tmp/vmware/provider/user_defined_script/ | head -1)'` 中的 `log.txt` 文件。

## Ansible Tower 集成

支持的操作系统类型

- Red Hat Enterprise Linux 8.0 或更高版本 64 位 (x86) 仅支持 Ansible Tower 3.5 及更高版本。
- Red Hat Enterprise Linux 7.4 或更高版本 64 位 (x86)。
- CentOS 7.4 或更高版本 64-位 (x86)。

以下是在 Ansible Tower 安装期间生成的示例清单文件。您可能需要对其进行修改，以便 vRealize Automation Cloud Assembly 集成使用。

```
[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
```

## 在 vRealize Automation Cloud Assembly 中配置 Puppet Enterprise 集成

vRealize Automation Cloud Assembly 支持与 Puppet Enterprise 集成配置管理集成。

将 Puppet Enterprise 作为外部系统添加到 Cloud Assembly 后，默认情况下可在所有项目中使用。可以将其限制到特定项目。

要添加 Puppet Enterprise 集成，您必须具有 Puppet 主节点名称以及主节点的主机名或 IP 地址。

您可以在以下位置找到 Puppet 日志，以防需要检查它们是否存在错误或出于信息目的。

说明	日志位置
面向创建和安装相关事件的日志	这些日志位于已部署计算机上的 <code>~/var/tmp/vmware/provider/user_defined_script/\$(ls -t ~/var/tmp/vmware/provider/user_defined_script/   head -1)/`</code> 。 有关完整日志，请参考 <b>log.txt</b> 文件。有关详细的 Puppet 代理日志，请参阅 <a href="https://puppet.com/docs/puppet/4.8/services_agent_unix.html#logging">https://puppet.com/docs/puppet/4.8/services_agent_unix.html#logging</a>
面向 Puppet 删除和运行相关任务的日志	这些日志位于 PE 上的 <code>~/var/tmp/vmware/provider/user_defined_script/\$(ls -t ~/var/tmp/vmware/provider/user_defined_script/   head -1)/`</code> 。有关完整日志，请参考 <b>log.txt</b> 文件。

## 步骤

- 1 选择**基础架构 > 连接 > 集成**，然后单击**添加集成**。
- 2 选择 Puppet。
- 3 在 Puppet 配置页面上输入所需的信息。
- 4 单击**验证**以检查集成。
- 5 单击**添加**。

## 结果

Puppet 可与云模板配合使用。

## 后续步骤

将 Puppet 组件添加到所需云模板。

- 1 在 Cloud Assembly 中的“云模板”下，选择云模板菜单上“内容管理”标题下的“Puppet”，然后将 Puppet 组件拖动到画布。
- 2 在右侧的窗格中输入“Puppet 属性”。

属性	说明
Master	输入要与此云模板一起使用的 Puppet 主计算机的名称。
环境	为 Puppet 主计算机选择环境。
角色	选择要与此云模板一起使用的 Puppet 角色。
代理运行间隔	希望 Puppet 代理轮询 Puppet 主计算机以获取配置详细信息的频率，该配置详细信息将应用于与此云模板相关的已部署虚拟机。

- 3 单击右侧窗格中的“代码”选项卡以查看 Puppet 配置属性的 YAML 代码。

## 在 vRealize Automation Cloud Assembly 中配置 Ansible 开源集成

vRealize Automation Cloud Assembly 支持与 Ansible 开源配置管理集成。配置集成后，可以将 Ansible 组件添加到新部署或现有部署中。

将 Ansible 开源与 vRealize Automation Cloud Assembly 集成时，可以将其配置为置备新计算机时按给定顺序运行一个或多个 Ansible playbook，以自动执行配置管理。可以在云模板中为部署指定所需的 playbook。

设置 Ansible 集成时，必须指定 Ansible 开源主机，以及可为管理资源定义信息的清单文件路径。此外，还必须提供用于访问 Ansible 开源实例的名称和密码。稍后，在将 Ansible 组件添加到部署时，可以更新连接以使用基于密钥的身份验证。

默认情况下，Ansible 使用 ssh 连接到物理计算机。如果使用的是在云模板中通过 `osType Windows` 属性指定的 Windows 计算机，则 `connection_type` 变量将自动设置为 `winrm`。

最初，Ansible 集成使用集成中提供的用户/密码或用户/密钥凭据连接到 Ansible 控制计算机。连接成功后，将验证云模板中所提供 Playbook 的语法。

如果验证成功，则会在 Ansible 控制计算机中的 `~/var/tmp/vmware/provider/user_defined_script/` 下创建执行文件夹。将从此文件夹运行脚本，以将主机添加到清单，创建主机变量文件（包括设置身份验证模式以连接到主机），最后运行 Playbook。此时，云模板中提供的凭据用于从 Ansible 控制计算机连接到主机。

Ansible 集成支持不使用 IP 地址的物理计算机。对于在公有云（如 AWS、Azure 和 GCP）上置备的计算机，仅当计算机连接到公共网络时，才会在所创建资源的 `address` 属性中填充计算机的公共 IP 地址。对于未连接到公共网络的计算机，Ansible 集成将从连接到该计算机的网络查找 IP 地址。如果连接了多个网络，Ansible 集成将查找 `deviceIndex`（即，连接到计算机的网卡 (NIC) 的索引）为最小的网络。如果蓝图中未指定 `deviceIndex` 属性，则集成将使用第一个连接的网络。

有关为 vRealize Automation Cloud Assembly 中的集成配置 Ansible 开源的更多详细信息，请参见[什么是 vRealize Automation Cloud Assembly 中的配置管理](#)。

### 前提条件

- Ansible 控制机必须使用 Ansible 版本 2.6.0 或更高版本。
- 用户必须具有 Ansible 清单文件所在目录的读取/写入权限。此外，如果已存在清单文件，用户也必须具有该文件的读取/写入权限。
- 如果使用的是具有 `sudo` 选项的非 root 用户，请确保在 `sudoers` 文件中设置以下内容：

```
Defaults:user_name !requiretty
```

和

```
username ALL=(ALL) NOPASSD: ALL
```

- 通过在 `/etc/ansible/ansible.cfg` 或 `~/.ansible.cfg` 中设置 `host_key_checking = False`，确保禁用主机密钥检查。

- 通过将以下行添加到 `/etc/ansible/ansible.cfg` 或 `~/.ansible.cfg` 文件，确保设置保管库密码：

```
vault_password_file = /path/to/password_file
```

保管库密码文件包含纯文本格式的密码，仅当云模板或部署提供在 ACM 和节点之间使用的用户名和密码组合时，才会使用该密码，如下示例中所示。

```
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
```

- 为避免在尝试运行 **playbook** 时出现主机密钥故障，建议您在 `/etc/ansible/ansible config` 中包含以下设置。

```
[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.
```

## 步骤

- 1 选择**基础架构 > 连接 > 集成**，然后单击**添加集成**。
  - 2 单击“Ansible”。
- 此时将显示 Ansible 配置页面。
- 3 输入 Ansible 开源实例的主机名、清单文件路径和其他必填信息。
  - 4 单击**验证**以检查集成。
  - 5 单击**添加**。

## 结果

Ansible 可与云模板一同使用。

## 后续步骤

将 Ansible 组件添加到所需云模板。

- 1 在云模板画布页面上，选择云模板选项菜单上“配置管理”标题下的“Ansible”，然后将 Ansible 组件拖动到画布。
- 2 使用右侧面板配置适当的 Ansible 属性，例如，指定要运行的 **playbook**。

在 Ansible 中，用户可以为单个主机分配一个变量，然后在 `playbook` 中使用该变量。通过 Ansible 开源集成，可以在云模板中指定这些主机变量。`hostVariables` 属性必须采用正确的 YAML 格式（Ansible 控制计算机要求采用此格式），且此内容将放置在以下位置：

```
parent_directory_of_inventory_file/host_vars/host_ip_address/vra_user_host_vars.yml
```

Ansible 清单文件的默认位置在 Cloud Assembly 的“集成”页面中添加的 Ansible 帐户中进行定义。Ansible 集成不会在云模板中验证 `hostVariable` YAML 语法，但如果在格式或语法错误的情况下运行 `playbook`，Ansible 控制计算机将出现异常。

以下云模板 YAML 代码段显示了 `hostVariables` 属性的示例用法。

```
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 集成要求使用以下方法之一在云模板中显示身份验证凭据：

- Ansible 资源中的用户名和密码。
- Ansible 资源中的用户名和 `privateKeyFile`。
- Ansible 资源中的用户名和计算资源中的 `privatekey`，方法是将 `remoteAccess` 指定为 `generatedPublicPrivateKey`。

在云模板中，确保在集成帐户中指定的用户可以访问 Ansible Playbook 的路径。可以使用绝对路径指定 Playbook 位置，但这不是必需操作。建议使用用户主文件夹的绝对路径，这样，即使 Ansible 集成凭据随时间发生更改，路径仍保持有效。

## 在 vRealize Automation Cloud Assembly 中配置 Ansible Tower 集成

您可以将 Ansible Tower 与 vRealize Automation Cloud Assembly 集成，以支持已部署资源的配置管理。配置集成后，可以从云模板编辑器将 Ansible 组件添加到新部署或现有部署中。

vRealize Automation Cloud Assembly 支持与 Ansible Tower 版本 3.5、3.6 和 3.7 集成。

## 前提条件

- 授予非管理员用户访问 **Ansible Tower** 的适当权限。对于大多数配置，有两种适用方法。请选择最适合您配置的方法。
  - 在组织级别为用户授予清单管理员和作业模板管理员角色。
  - 为用户授予特定清单的管理员权限，以及用于置备的所有作业模板的执行角色。
- 您必须在 **Ansible Tower** 中配置相应的凭据和模板，以与您的部署配合使用。模板定义了用于部署的清单和 **playbook**。作业模板和 **playbook** 之间存在 1:1 映射。**Playbook** 使用类似 **YAML** 的语法来定义与模板关联的任务。对于大多数典型部署，请使用计算机凭据进行身份验证。
  - a 登录到 **Ansible Tower** 并导航到“作业模板”部分。
  - b 选择“添加新作业”模板。
    - 选择已创建的凭据。这些是将由 **Ansible Tower** 管理的计算机的凭据。每个作业模板可以有一个凭据对象。
    - 对于“限制”选择，选择“启动时提示”。这可确保作业模板针对正从 **vRealize Automation Cloud Assembly** 置备或取消置备的节点运行。如果未选择此选项，则在部署包含作业模板的蓝图时，将显示“未设置限制”错误。
- 您可以在 **Ansible Tower** 的“作业”选项卡上查看从 **vRealize Automation Cloud Assembly** 调用的作业模板的执行情况。

## 步骤

- 1 选择**基础架构 > 连接 > 集成**，然后单击**添加集成**。
- 2 单击 **Ansible Tower**。  
此时将显示 **Ansible** 配置页面。
- 3 输入**主机名**（可以是 IP 地址）以及 **Ansible Tower** 实例所需的其他信息。
- 4 为适用的 **Ansible Tower** 实例输入基于 UI 的身份验证**用户名和密码**。
- 5 单击**验证**以验证集成。
- 6 为集成键入适当的**名称和描述**。
- 7 单击**添加**。

## 结果

**Ansible Tower** 可在云模板中使用。

## 后续步骤

将 **Ansible Towe** 组件添加到所需云模板。确保为在集成帐户中指定的用户指定适用的作业模板和执行权限。

- 1 在云模板画布页面上，选择蓝图选项菜单上“配置管理”标题下的“**Ansible**”，然后将 **Ansible Tower** 组件拖动到画布。

- 2 使用右侧面板配置适当的 Ansible 属性，例如作业模板。

## 如何在 vRealize Automation Cloud Assembly 中创建 Active Directory 集成

vRealize Automation Cloud Assembly 支持与 Active Directory 服务器集成，以便在置备虚拟机之前在 Active Directory 服务器内的指定组织单位 (OU) 中现成创建计算机帐户。Active Directory 只支持与 Active Directory 服务器建立 LDAP 连接。

与项目关联的 Active Directory 策略将应用于在该项目范围内置备的所有虚拟机。用户可以指定一个或多个标记，以便有选择地将策略应用于已置备到具有匹配功能标记的云区域的虚拟机。

对于内部部署，通过 Active Directory 集成，可以设置运行状况检查功能，以显示集成的状态及其所依赖的底层 ABX 集成（包括所需的可扩展性云代理）。在应用 Active Directory 策略之前，vRealize Automation Cloud Assembly 会检查底层集成的状态。如果集成正常，vRealize Automation Cloud Assembly 将在指定的 Active Directory 中创建已部署的计算机对象。如果集成不正常，则部署操作会在置备期间跳过 Active Directory 阶段。

### 前提条件

- Active Directory 集成需要与 Active Directory 服务器建立 LDAP 连接。
- 如果要配置与 vCenter 内部部署的 Active Directory 集成，则必须配置与可扩展性云代理的 ABX 集成。选择**可扩展性 > 活动 > 集成**，然后选择**可扩展性操作内部部署**。
- 如果要在云中配置与 Active Directory 的集成，您必须拥有 Microsoft Azure 或 Amazon Web Services 帐户。
- 您必须为项目配置适当的云区域以及映像映射和特定实例映射，才能与 Active Directory 搭配使用。
- 在将 Active Directory 集成与项目关联之前，必须在 Active Directory 上预先创建所需的 OU。

### 步骤

- 1 选择**基础架构 > 连接 > 集成**，然后选择**新建集成**。
- 2 单击 **Active Directory**。
- 3 在**摘要**选项卡上，输入适当的 LDAP 主机和环境名称。
- 4 输入 LDAP 服务器的用户名和密码。
- 5 为 Active Directory 中的所需用户和组输入适当的“基本 DN”。

---

**注** 每个 Active Directory 集成只能指定一个 DN。

---

- 6 单击**验证**以确保集成正常运行。
- 7 输入此集成的名称和说明。
- 8 单击**保存**。

- 9 单击**项目**选项卡，将项目添加到 Active Directory 集成。

在**添加项目**对话框中，必须选择项目名称和相对 DN（即在“摘要”选项卡上指定的“基本 DN”中存在的 DN）。

- 10 单击**保存**。

## 结果

现在，可以将具有 Active Directory 集成的项目关联到云模板。使用此云模板置备计算机时，该计算机将预转储在指定的 Active Directory 和组织单位中。

此外，还可以按照以下方式对内部部署 Active Directory 集成执行基于标记的运行状况检查。

- 1 按照前面步骤所述创建 Active Directory 集成。
- 2 单击**项目**选项卡，将项目添加到 Active Directory 集成。
- 3 在“添加项目”对话框中，选择项目名称和相对 DN。相对 DN 必须存在于指定的基本 DN 中。
- 4 添加适当标记。这些标记适用于可能应用 Active Directory 策略的云区域。
- 5 单击“保存”。

vRealize Automation Cloud Assembly 中的**基础架构 > 连接 > 集成**页面上将显示每个集成的 Active Directory 集成状态。

可以将具有 Active Directory 集成的项目与云模板相关联。使用此模板置备计算机时，该计算机将预转储在指定的 Active Directory 和 OU 中。

## 配置 VMware SDDC Manager 集成

可以将 VMware SDDC Manager 集成添加到 vRealize Automation，以便于将工作负载域作为 vRealize Automation 中的 VMware Cloud Foundation (VCF) 云帐户的一部分使用。

### 前提条件

- vRealize Automation 仅支持与 VMware SDDC Manager 4.1 及更高版本集成。

### 步骤

- 1 选择**基础架构 > 连接 > 集成**，然后单击**添加集成**。
- 2 选择“SDDC Manager”。  
此时将显示 SDDC Manager 集成配置页面。
- 3 在“摘要”部分中，输入集成的**名称**和**描述**。
- 4 在“SDDC Manager 凭据”部分中，输入 SDDC Manager 服务器计算机的 **SDDC Mgr IP 地址/FQDN**。



- 5 输入用于初始连接到 SDDC Manager 的管理员帐户的用户名和密码。最佳做法是避免使用管理员帐户进行连接。使用在 SDDC Manager 中具有管理员特权的其他帐户创建服务角色。

这些凭据用于初始设置与 SDDC Manager 的连接，然后创建服务凭据，以便在从 VCF 云帐户进行连接时使用。

- 6 单击**验证**以验证与 SDDC Manager 的连接。

- 7 单击**添加**。

## 结果

创建集成后，可在已完成的集成页面上显示的“工作负载域”选项卡上查看与 SDDC 关联的工作负载。此外，还可以查看和选择与集成相关联的工作负载，然后单击**添加云帐户**按钮以打开一个页面，可以在该页面上创建将使用所选工作负载的 VCF 云帐户。

## 后续步骤

配置 VCF 云帐户后，页面顶部将显示**设置云**按钮。单击此按钮可启动 VCF 云设置向导。

## 与 vRealize Operations Manager 集成

vRealize Automation 可以与 vRealize Operations Manager 配合使用来执行高级工作负载布置，提供部署运行状况和虚拟机衡量指标以及显示定价。

### 集成的数量和类型

这两个产品之间的集成必须是内部部署到内部部署，而不是内部部署和云的混合。

可以将一个 vRealize Automation 实例与多个 vRealize Operations Manager 实例集成，但一个 vRealize Operations Manager 实例只能连接到一个 vRealize Automation 实例。

无法将聚合 vRealize Operations Manager 集群连接到 vRealize Automation。

### 集成的基本要求

要与 vRealize Operations Manager 集成，请转到**基础架构 > 连接 > 集成**。要添加集成，需要 vRealize Operations Manager URL 和下一部分所述的登录帐户的凭据。此外，vRealize Automation 和 vRealize Operations Manager 需要管理同一个 vSphere 端点。

### 用于集成的登录帐户

在 vRealize Operations Manager 中，需要一个本地或非本地 vRealize Operations Manager 登录帐户，才能使用集成。该帐户需要对 vSphere 端点的 vCenter 适配器实例具有只读特权。请注意，非本地帐户可能需要导入到 vRealize Operations Manager 并分配其只读角色。对于集成，非本地帐户登录的用户名格式为 `username@domain@authenticated-source`，如 `jdoe@company.com@workspaceone`。身份验证源在 vRealize Operations Manager 服务器初始设置期间进行定义。

有关详细信息，请参见以下部分。有关定价信息，请参见 [什么是定价卡](#)。

## 使用 vRealize Operations Manager 执行高级工作负载布置

vRealize Automation 和 vRealize Operations Manager 可以配合工作，以最佳方式放置部署工作负载。

您可以在基于 vSphere 的云区域级别启用工作负载布置。云区域中只有已启用 Distributed Resource Scheduler (DRS) 的集群才有资格使用 vRealize Operations Manager 执行高级布置。

- vRealize Automation 布置 - vRealize Automation 布置引擎基于应用程序意图。它考虑基于标记的限制、项目成员资格和关联的云区域，以及与网络、存储和计算资源相关的关联性筛选器。资源布置取决于所有这些因素以及同一部署中是否存在其他相关目标资源。
- vRealize Operations Manager 布置 - vRealize Operations Manager 会考虑运维意图，以实现最佳布置。运维意图可以将过去的工作负载和未来的假设预测考虑在内。

使用高级工作负载布置时，必须应用 vRealize Automation 标记才能实施业务意图决策，而不使用 vRealize Operations Manager 业务意图选项。

与 vRealize Operations Manager 集成后，vRealize Automation 会继续遵循其应用程序意图模型及其相关的限制来筛选目标布置。然后，它会根据这些结果，使用 vRealize Operations Manager 建议进一步优化布置。

### 没有建议时

如果启用高级工作负载布置，并且 vRealize Operations Manager 分析未返回任何建议，则可以将 vRealize Automation 配置为回退到其默认的应用程序意图布置。

### 工作负载布置限制

使用 vRealize Operations Manager 放置工作负载时，有一些限制适用。

- vRealize Operations Manager 不支持将工作负载布置在 vCenter Server 中的资源池上。
- 如果 vRealize Operations Manager 处于关闭状态，则工作负载布置时调用 vRealize Operations Manager 的超时可能会过期。
- 布置不能跨多个云区域。vRealize Automation 将一个云区域发送到 vRealize Operations Manager，以获取该单个云区域内的布置建议。

### 如何启用工作负载布置

要启用工作负载布置，需要为 vSphere、vRealize Operations Manager 和 vRealize Automation 执行相应步骤。

- 1 在 vRealize Automation Cloud Assembly 中，连接到您的 vCenter Server 云帐户。  
选项位于**基础架构 > 连接 > 云帐户**下。
- 2 在 vCenter Server 中，确认已启用 DRS 的集群存在并设置为全自动。
- 3 在 vRealize Operations Manager 中，确认正在管理同一个 vCenter Server。  
您需要 vRealize Operations Manager 8 或更高版本。
- 4 在 vRealize Automation Cloud Assembly 中，添加 vRealize Operations Manager 集成。  
选项位于**基础架构 > 连接 > 集成**下。

要添加集成，您需要以下 vRealize Operations Manager 主节点 URL 以及登录用户名和密码。

`https://operations-manager-IP-address-or-FQDN/suite-api`

输入值后，单击“验证”。

- 单击“同步”，将集成同步到 vCenter Server。

也可在 vRealize Automation Cloud Assembly 和 vRealize Operations Manager 开始管理新 vCenter Server 的任何时间进行同步。

- 在 vRealize Automation Cloud Assembly 中，为 vCenter Server 帐户创建云区域。

选项位于**基础架构 > 配置 > 云区域**下。

- 在云区域“摘要”选项卡下，将“布置策略”设置为“高级”。

- 在“布置策略”下，选择是否让 vRealize Automation 在 vRealize Operations Manager 不返回任何建议时恢复到其默认布置。

### 工作负载布置故障排除

如果 vRealize Operations Manager 不建议按您的预期方式布置工作负载，请查看 vRealize Automation Cloud Assembly 或 vRealize Automation Service Broker 中的部署请求详细信息。

- 转到**基础架构 > 活动 > 请求**，然后单击请求。

- 在“请求详细信息”中，查看分配阶段。

查找已成功或未成功识别的目标。

- 在“请求详细信息”中，从右上角启用开发模式。

- 按照请求路径查找筛选器块。

- 单击筛选器块，然后查看以下部分。

```
filterName: ComputePlacementPolicyAffinityHostFilter
  V computeLinksBefore
  V computeLinksAfter
  V filteredOutHostsReasons
```

条目	说明
computeLinksBefore	基于 vRealize Automation 算法的潜在布置主机列表。
computeLinksAfter	所选布置主机。
filteredOutHostsReasons	描述选择或拒绝主机的原因的消息。 当 vRealize Operations Manager 选择主机时，将显示以下消息。 advance policy filter: Filtered hosts based on recommendation from vROPS.

### 使用 vRealize Operations Manager 连续优化

在 vRealize Operations Manager 中添加 vRealize Automation 适配器时，vRealize Operations Manager 会自动为基于 vRealize Automation 的工作负载创建新的自定义数据中心 (CDC)。

使用连续优化，您可以充分利用工作负载重新平衡和重新布置，并且除初始工作负载布置外，还可以将 vRealize Automation 和 vRealize Operations Manager 结合使用。当虚拟化资源移动到或进入更重或更轻的负载时，vRealize Automation 置备的工作负载可以根据需要进行移动。

- 连续优化会自动在 vRealize Operations Manager 中创建新的 CDC。
- 每个 vRealize AutomationvSphere 云区域都有一个新的 CDC。
- 新创建的 CDC 包含与云区域关联的每个 vRealize Automation 受管集群。

---

**注** 请勿手动创建包含 vRealize Automation 和非 vRealize Automation 集群的混合型 CDC。

---

- 可以使用 vRealize Operations Manager 对基于 vRealize Automation 的新建 CDC 运行连续优化。
- 工作负载只能在同一云区域或 CDC 中重新平衡或重新放置。
- 优化永远不会制造新的违反 vRealize Automation 或 vRealize Operations Manager 布置要求的情况。
  - 如果存在布置违规情况，优化可以修复 vRealize Operations Manager 运维意图问题。
  - 如果存在布置违规情况，优化无法修复 vRealize Operations Manager 业务意图问题。

例如，如果使用 vRealize Operations Manager 将虚拟机手动移至不支持限制的集群，则 vRealize Operations Manager 不检测违规情况，也不尝试进行解决。
- 本版本在 CDC 级别遵循运维意图。所有成员 vRealize Automation 集群已优化为相同的设置。
 

要为集群设置不同的运维意图，必须在与不同 vSphere 云区域关联的不同 vRealize Automation CDC 中进行配置。采用不同的测试和生产集群可能就是一个示例情况。
- 在任何优化重新平衡或重新放置操作期间，将遵循在 vRealize Automation 中定义的 vRealize Automation 应用程序意图和限制。
- vRealize Operations Manager 布置标记无法应用于 vRealize Automation 置备的工作负载。

此外，支持涉及多个计算机的调度优化。定期调度的优化不是全有或全无的进程。如果条件中断计算机移动，已成功重新放置的计算机将保持已重新放置状态，并且下一个 vRealize Operations Manager 周期将像 vRealize Operations Manager 往常一样尝试重新放置其余计算机。这样部分完成的优化不会在 vRealize Automation 中造成任何负面影响。

#### 如何启用连续优化

当您在 vRealize Operations Manager 中添加 vRealize Automation 适配器时，vRealize Operations Manager 会为基于 vRealize Automation 的工作负载自动创建新的专用数据中心。

除了在 vRealize Automation Cloud Assembly 内添加集成，连续优化不需要执行单独的安装步骤。您可以开始配置和使用 vRealize Operations Manager 在新数据中心中进行工作负载重新放置。请参见[连续优化示例](#)。

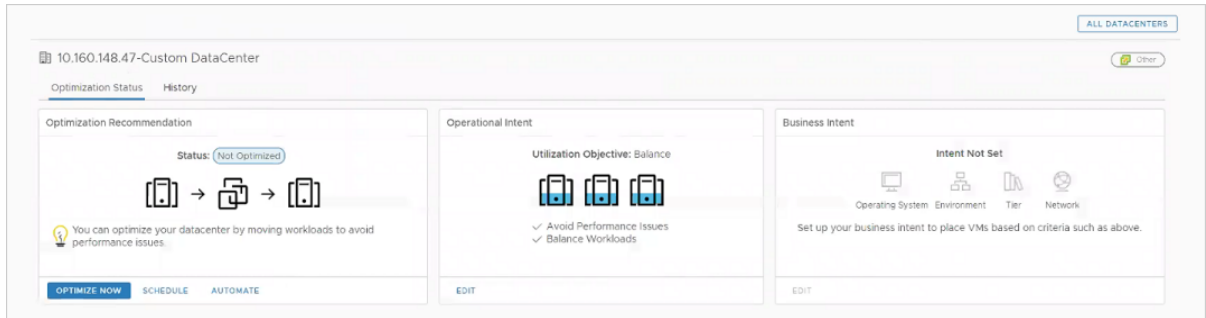
#### 连续优化示例

以下示例显示了使用 vRealize Operations Manager 进行 vRealize Automation 连续优化的重新均衡工作流。

- 1 在 vRealize Operations Manager 主页中，单击**工作负载优化**。
- 2 选择自动创建的 vRealize Automation 数据中心。

### 3 在运维视图下，单击编辑，然后选择均衡。

您无法选择或编辑业务意图，在数据中心进行 vRealize Automation 优化时已禁用这些操作。



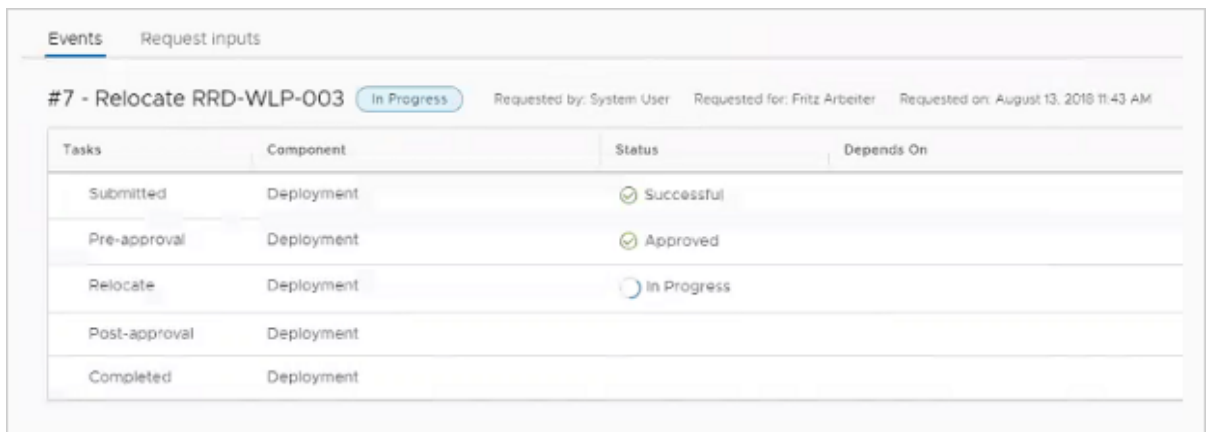
### 4 在优化建议下，单击立即优化。

vRealize Operations Manager 将显示建议操作的前后对比图。

### 5 单击下一步。

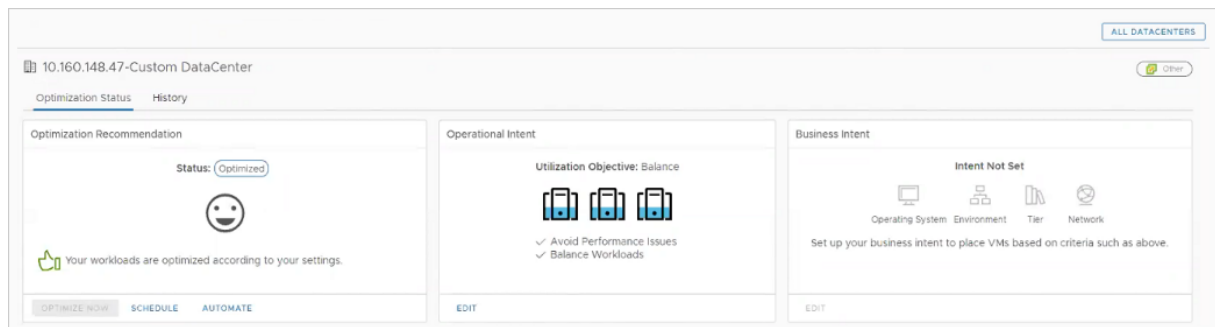
### 6 单击开始操作。

### 7 在 vRealize Automation 中，通过单击部署并查看事件状态来监控正在进行的操作。



重新均衡完成后，vRealize Automation 将刷新系统。“计算资源”页面将显示计算机已移动。

在 vRealize Operations Manager 中，下一次收集数据时将刷新显示屏以显示优化已完成。



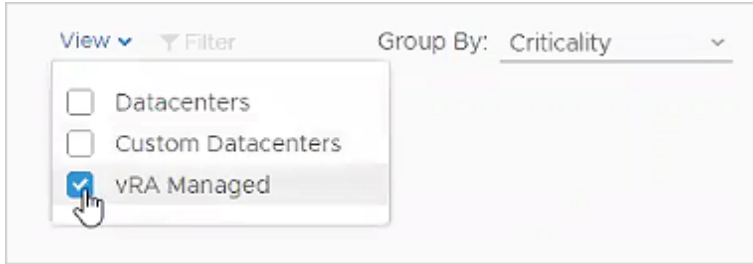
在 vRealize Operations Manager 中，可以通过单击**管理 > 历史记录 > 近期任务**来查看该操作。

#### 查找 vRealize Automation 管理的数据中心

您可以使用 vRealize Operations Manager 仅显示 vRealize Automation 管理的数据中心。

##### 步骤

- 1 在 vRealize Operations Manager 主页中，单击**工作负载优化**。
- 2 单击右上角附近的**查看**下拉菜单。
- 3 仅选择 vRealize Automation 管理的数据中心。



#### 基于 vRealize Operations Manager 的部署监控

vRealize Automation 可以显示有关您的部署的 vRealize Operations Manager 数据。

直接 在 vRealize Automation 中查看筛选的一组衡量指标可为您节省访问或搜索 vRealize Operations Manager 的任务。尽管无法在 vRealize Operations Manager 的上下文中启动，但您当然可以自由登录并根据需要使用 vRealize Operations Manager 提供其他数据。

#### 启用 vRealize Operations Manager 数据

要使 vRealize Automation 显示 vRealize Operations Manager 数据，请添加 vRealize Operations Manager 集成。

##### 步骤

- 1 在 vRealize Operations Manager 中，转到**管理 > 解决方案**。
- 2 在**配置的适配器实例**下，确认对于 vRealize Automation 置备到的以及它正在接收数据的 vSphere 云区域有 **vCenter 适配器**。
- 3 在 vRealize Automation Cloud Assembly 中，转到**基础架构 > 连接 > 集成**。
- 4 输入 vRealize Operations Manager 主节点 URL 以及 vRealize Operations Manager 登录用户名和密码。

`https://operations-manager-IP-address-or-FQDN/suite-api`

- 5 单击**部署**，选择部署，然后确认显示“监控”选项卡。

## vRealize Operations Manager 提供的运行状况和警示

启用监控后，vRealize Automation 将检索有关您的部署的 vRealize Operations Manager 运行状况和关联警示。

要访问监控，请单击部署，然后选择**监控**选项卡。如果缺少该选项卡，请参见[启用 vRealize Operations Manager 数据](#)。

要查看警示，请在左侧面板中的组件树顶部突出显示部署名称。

- 可以查看警示的严重性和文本。
- 要重点关注某些方面，请筛选并排序列中的数据。
- 仅显示运行状况标志和运行状况警示。不支持效率或风险等其他警示类型。

## vRealize Operations Manager 提供的衡量指标

启用监控后，vRealize Automation 将检索有关您的部署的 vRealize Operations Manager 衡量指标。

要访问监控，请单击部署，然后选择**监控**选项卡。如果缺少该选项卡，请参见[启用 vRealize Operations Manager 数据](#)。

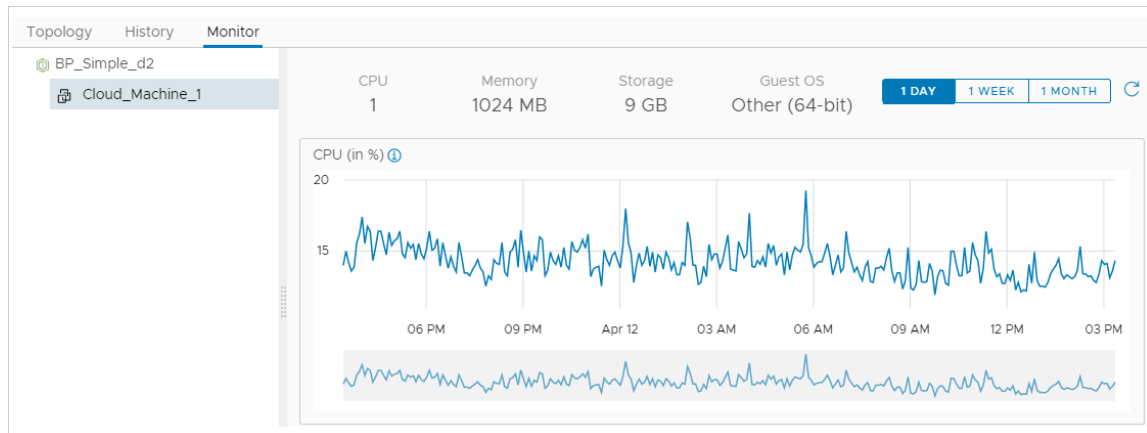
要查看衡量指标，请展开左侧的组件树，并突出显示某个虚拟机。

- 不缓存衡量指标。它们直接来自 vRealize Operations Manager，可能需要几分钟才能加载。
- 仅显示虚拟机衡量指标。不支持来自 vCloud Director、软件或 XaaS 等其他组件的衡量指标。
- 仅显示 vSphere 虚拟机衡量指标。不支持 AWS 或 Azure 等其他云提供商。

衡量指标显示为时间轴图，在其中显示以下衡量指标的高低值。

- CPU
- 内存
- 存储 IOPS
- 网络 MBPS

要显示特定衡量指标名称，请单击时间轴左上角的蓝色信息图标。



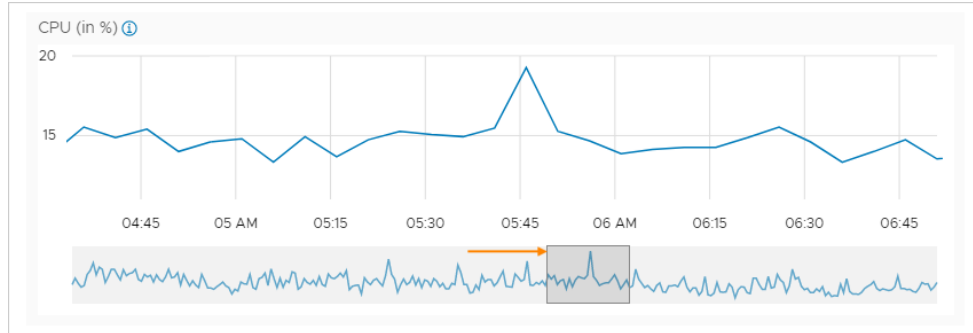


## 处理 vRealize Operations Manager 提供的数据

当 vRealize Operations Manager 提供的衡量指标暴露出问题时，您可以直接在 vRealize Automation 中确定故障区域。

要查看 vRealize Operations Manager 提供的衡量指标，请单击部署，然后选择**监控**选项卡。如果缺少该选项卡，请参见[启用 vRealize Operations Manager 数据](#)。

过去一天、一周或一月的衡量指标可供使用。要放大关注区域，请选择任何衡量指标时间轴下方阴影部分的小区域：



## vRealize Automation Cloud Assembly 中的载入计划是什么

您可以使用工作负载载入计划来确定已从目标区域或数据中心的云帐户类型收集数据但尚未由 vRealize Automation Cloud Assembly 项目管理的计算机。

添加包含在 vRealize Automation Cloud Assembly 之外部署的计算机的云帐户时，这些计算机不会由 Cloud Assembly 进行管理，直到您载入它们。使用载入计划将非受管计算机载入到 vRealize Automation Cloud Assembly 中进行管理。您需要创建一个计划，将计算机填充到该计划中，然后运行该计划以导入这些计算机。使用载入计划，您可以创建云模板，还可以创建一个或多个部署。

您可以在一个计划中载入一个或多个非受管计算机。您可以手动或使用筛选规则选择计算机。筛选规则根据计算机名称、状态、IP 地址和标记等条件选择要载入的计算机。

- 每小时可在单个载入计划中载入多达 3,500 个非受管计算机。
- 每小时可在多个载入计划中同时载入多达 17000 个非受管计算机。

可用于工作负载载入的计算机将在与特定云帐户类型和区域相关的**资源 > 计算机**页面中列出，并且在“来源”列中标记为 Discovered。只会列出已收集数据的计算机。在载入计算机后，它们会在“来源”列中显示为 Deployed。

系统会自动将运行工作负载载入计划的人员指定为计算机所有者。

### 载入示例

有关载入方法的示例，请参见[示例：将选定的计算机载入为 vRealize Automation Cloud Assembly 中的单个部署](#)和[示例：将规则筛选的计算机作为单独部署载入 vRealize Automation Cloud Assembly](#)。

### 载入事件订阅



运行计划时，将创建 Deployment Onboarded 事件。使用“可扩展性”选项卡中的选项，您可以订阅这些部署事件并对其执行操作。

## 示例：将选定的计算机载入为 vRealize Automation Cloud Assembly 中的单个部署

在本示例中，您将两台非受管计算机载入为单个 vRealize Automation Cloud Assembly 部署，并为计划中的所有计算机创建一个云模板。

创建云帐户时，将对与该云帐户关联的所有计算机收集数据，然后在**基础架构 > 资源 > 计算机**页面中显示这些计算机。如果云帐户包含在 vRealize Automation Cloud Assembly 外部部署的计算机，您可以使用载入计划允许 vRealize Automation Cloud Assembly 管理计算机部署。

**注** 只能在载入部署之前对其进行重命名。载入后，**重命名**选项将处于禁用状态。

### 前提条件

- 确认您具有所需的用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 请参见 [vRealize Automation Cloud Assembly 中的载入计划是什么](#)。
- 创建并准备 vRealize Automation Cloud Assembly 项目。

此过程涉及基本 Wordpress 用例中的一些步骤。请参见教程：[在 vRealize Automation Cloud Assembly 中设置和测试多云基础架构和部署](#)。

- 创建项目，在项目中添加用户并分配用户角色。请参见第 2 部分：[创建示例 vRealize Automation Cloud Assembly 项目](#)。
- 为项目创建 Amazon Web Services 云帐户。请参见 [1. 添加云帐户](#)。

此过程中的 Amazon Web Services 云帐户包含在将云帐户添加到 vRealize Automation Cloud Assembly 之前部署的计算机，以及由 vRealize Automation Cloud Assembly 以外的应用程序部署的计算机。

- 验证**计算机**页面是否包含要载入的计算机。请参见 [vRealize Automation 中的计算机资源](#)。

### 步骤

- 1 转到**基础架构 > 载入**。
- 2 单击**新建载入计划**并输入示例值。

设置	示例值
计划名称	VC-sqa-deployments
说明	OurCo-AWS 云帐户的 AWS 计算机的示例载入计划
云帐户	OurCo-AWS
默认项目	WordPress

- 3 单击**创建**。

- 4 在计划的**部署**选项卡中，单击**选择计算机**，选择一台或多台计算机，然后单击**确定**。



- 5 选择**创建一个包含所有计算机的部署**，然后单击**创建**。
- 6 单击新部署名称旁边的复选框，然后单击**云模板...**。
- 7 单击以 **Cloud Assembly** 格式创建云模板。
- 8 输入云模板名称，然后单击**保存**。

**注** 当您的载入计划使用 vSphere 计算机时，必须在载入过程完成后编辑云模板。载入过程无法链接源 vSphere 计算机及其计算机模板，且生成的云模板将在云模板代码中包含 `imageRef: "no image available"` 条目。在 `imageRef` 字段中指定正确的模板名称之前，无法部署云模板。为了在载入过程完成后更轻松地查找和更新云模板，请使用部署的**云模板配置**页面上的**云模板名称**选项。记录自动生成的云模板名称，或输入并记录您选择的云模板名称。载入完成后，找到并打开云模板，并将 `imageRef` 字段中的 `"no image available"` 条目替换为正确的模板名称。

- 9 单击部署名称复选框，单击**运行**，然后在**运行计划**页面中再次单击**运行**。
- 所选的 Amazon Web Services 计算机将作为单个部署与随附的云模板一起载入。
- 10 通过单击**云模板**选项卡，然后单击云模板名称，打开并检查云模板。
- 11 通过单击**部署**选项卡，然后单击部署名称，打开并检查部署。

## 示例：将规则筛选的计算机作为单独部署载入 vRealize Automation Cloud Assembly

在此示例中，您将使用筛选规则来载入状态为 On 且名称以字母 BG 开头的计算机。您还将为计划中的每台计算机创建单独的 vRealize Automation Cloud Assembly 云模板和部署。

创建云帐户时，将对与该云帐户关联的所有计算机收集数据，然后在**基础架构 > 资源 > 计算机**页面中显示这些计算机。如果云帐户包含在 vRealize Automation Cloud Assembly 外部部署的计算机，您可以使用载入计划允许 vRealize Automation Cloud Assembly 管理计算机部署。

### 前提条件

- 确认您具有所需的用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 请参见 [vRealize Automation Cloud Assembly 中的载入计划是什么](#)。

- 创建并准备一个 vRealize Automation Cloud Assembly 项目，然后将一个或多个云帐户填充到该项目中。

这涉及到引导式设置过程中的一些基本步骤。

- 创建项目，在项目中添加用户并分配用户角色。请参见第 2 部分：创建示例 vRealize Automation Cloud Assembly 项目。
- 在项目的指定区域中创建一个或多个云帐户。
- 验证计算机页面是否包含要载入的计算机。请参见 vRealize Automation 中的计算机资源。

## 步骤

- 1 转到**基础架构 > 载入**。
- 2 单击**新建载入计划**并输入值。

设置	示例值
计划名称	ob_rules_1
说明	Machine onboarding with rules1
云帐户	rs-aws
默认项目	rs-project

### 新建载入计划



计划名称

描述

#### 必备条件

添加云帐户，并为要载入的计算机所在的计算资源创建云区域。  
创建至少具有一个用户的项目，并为该项目授予对云区域的访问权限。

云帐户

默认项目

取消

创建

### 3 单击创建。

### 4 单击规则选项卡，然后单击添加规则。

您可以创建一个或多个规则以根据特定计算机特性选择一组计算机进行载入。

### 5 输入规则名称，例如 ob\_rules\_1。

添加 规则

创建 基于筛选器的规则，将用于在此计划中填充计算机。

规则名称 \*

### 6 添加筛选器以生成规则。

对于此示例，请使用**筛选器**下拉菜单上的**状态**和**名称**筛选器指定名称包含 BG\* 且状态为 On 的所有计算机。

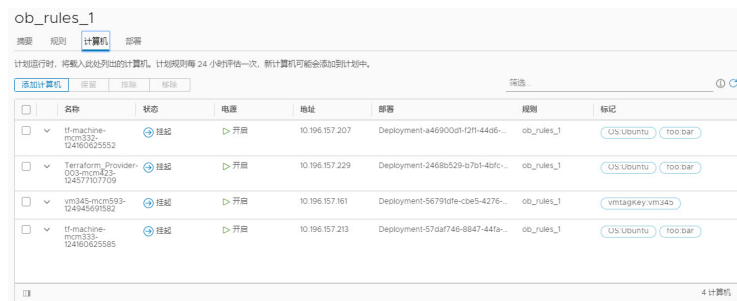


## 7 单击保存。

虽然您可以创建其他规则，但此示例使用单个规则。



## 8 单击计算机选项卡。在此示例中，选择了 4 台计算机，其中 3 台计算机的名称以字母 BG 开头，一台计算机的名称包含字母 BG。



## 9 通过选中对应的复选框并单击排除，移除名称不以 BG 开头的那台计算机。



## 10 单击部署选项卡。

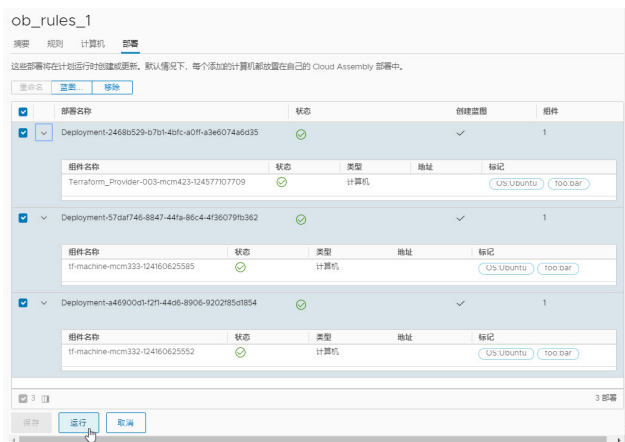
名称以字母 BG 开头且状态为 on 的 3 台计算机已准备好进行部署。默认情况下，将为每台计算机创建单独的云模板和部署。



- 11 选中三个部署名称旁边的复选框，然后依次单击云模板、以 Cloud Assembly 格式创建云模板和保存。

**注** 当您的载入计划使用 vSphere 计算机时，必须在载入过程完成后编辑云模板。载入过程无法链接源 vSphere 计算机及其计算机模板，且生成的云模板将在云模板代码中包含 `imageRef: "no image available"` 条目。在 `imageRef`: 字段中指定正确的模板名称之前，无法部署云模板。为了在载入过程完成后更轻松地查找和更新云模板，请使用部署的云模板配置页面上的云模板名称选项。记录自动生成的云模板名称，或输入并记录您选择的云模板名称。载入完成后，找到并打开云模板，并将 `imageRef`: 字段中的 "no image available" 条目替换为正确的模板名称。

- 12 在部署页面中，选中三个部署名称旁边的复选框，然后单击运行。



13 当系统提示您确认时，单击**运行**以载入计算机。



将运行该计划，并将计算机载入到 vRealize Automation Cloud Assembly 中进行管理。将为每台计算机创建单独的云模板和部署。

## vRealize Automation Cloud Assembly 环境的高级配置

可以配置 vRealize Automation Cloud Assembly 环境以进一步支持项目配置、集成和部署。

有关管理方法（如使用用户和日志以及加入或退出客户体验计划）的相关信息和其他信息，请参见《[管理 vRealize Automation](#)》帮助。

## 如何配置 vRealize Automation 的 Internet 代理服务器

对于无法直接访问 Internet 的隔离网络上的 vRealize Automation 安装，可以使用 Internet 代理服务器，以便允许通过代理访问 Internet 功能。Internet 代理服务器支持 HTTP 和 HTTPS。

要配置和使用公有云提供程序（如 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP)）以及外部集成点（如 IPAM、Ansible 和 Puppet），对于 vRealize Automation，您必须配置 Internet 代理服务器，以访问 vRealize Automation Internet 代理服务器。

vRealize Automation 包含一个可与 Internet 代理服务器通信的内部代理服务器。如果使用 `vracli proxy set ...` 命令对代理服务器进行了相应配置，则该服务器可与代理服务器通信。如果您尚未为组织配置 Internet 代理服务器，则 vRealize Automation 内部代理服务器会尝试直接连接到 Internet。

可以使用提供的 `vracli` 命令行实用程序将 vRealize Automation 设置为使用 Internet 代理服务器。有关如何使用 `vracli API` 的信息，可通过在 `vracli` 命令行中使用 `--help` 参数获得，例如 `vracli proxy --help`。

访问 Internet 代理服务器需要使用 vRealize Automation 中内置的基于操作的可扩展性 (ABX) 内部部署嵌入式控制。

**注** 不支持通过 Internet 代理访问 Workspace ONE Access（以前称为 VMware Identity Manager）。您无法使用 `vracli set vidm` 命令通过 Internet 代理服务器访问 Workspace ONE Access。

内部代理服务器要求将 IPv4 作为其默认 IP 格式。不要求对 TLS (HTTPS) 证书流量执行 Internet 协议限制、身份验证或中间人操作。

## 前提条件

- 确认您已有 HTTP 或 HTTPS 服务器，且可在能够将出站流量传递到外部站点的 vRealize Automation 网络中将其用作 Internet 代理服务器。必须针对 IPv4 配置连接。
- 确认目标 Internet 代理服务器已配置为支持 IPv4 作为其默认 IP 格式，而非 IPv6。
- 如果 Internet 代理服务器使用 TLS，并且需要与其客户端建立 HTTPS 连接，则必须先使用以下命令之一导入服务器证书，然后再设置代理配置。

```
■ vracli certificate proxy --set path_to_proxy_certificate.pem
```

```
■ vracli certificate proxy --set stdin
```

使用 stdin 参数执行交互式输入。

## 步骤

- 1 为 Kubernetes 使用的 pod 或容器创建代理配置。在此示例中，使用 HTTP 方案访问代理服务器。

```
vracli proxy set --host http://proxy.vmware.com:3128
```

- 2 显示代理配置。

```
vracli proxy show
```

结果将类似于以下内容：

```
{
  "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\nacl proxy-exclude dstdomain 192.168.\n\nacl proxy-exclude dstdomain kubernetes\n\nacl proxy-exclude dstdomain 10.192.204.9\n\nacl proxy-exclude dstdomain .eng.vmware.com\n\nacl
```



```
proxy-exclude dstdomain 10.192.213.146\nacl proxy-exclude dstdomain
10.192.213.151\nalways_direct allow proxy-exclude\nhttp_access allow mylan\nhttp_access
deny all\n# End autogen configuration\n",
    "internal.proxy.config.type": "default"
}
```

**注** 如果您已为组织配置 Internet 代理服务器，则上例中将显示 "internal.proxy.config.type": "non-default"，而不是 'default'。为安全起见，不会显示密码。

**注** 如果使用 -proxy-exclude 参数，则必须编辑默认值。例如，如果要将 acme.com 添加为无法使用 Internet 代理服务器访问的域，请执行以下步骤：

- a 输入 `vracli proxy default-no-proxy` 以获取默认的 `proxy-exclude` 设置。这是自动生成的域和网络列表。
- b 编辑值以添加 `.acme.com`。
- c 输入 `vracli proxy set .... --proxy-exclude ...` 以更新配置设置。
- d 运行 `/opt/scripts/deploy.sh` 命令以重新部署环境。

### 3 （可选）排除 DNS 域、FQDN 和 IP 地址，使其无法通过 Internet 代理服务器进行访问。

始终使用 `parameter --proxy-exclude` 修改 `proxy-exclude` 变量的默认值。要添加域 `exclude.vmware.com`，请先使用 `vrali proxy show` 命令，然后复制 `proxy-exclude` 变量，并使用 `vracli proxy set ...` 命令添加域值，如下所示：

```
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"
```

**注** 将元素添加到 `proxy-exclude`，而不是替换值。如果删除 `proxy-exclude` 默认值，vRealize Automation 将无法正常运行。如果发生这种情况，请删除代理配置，然后重新开始。

- 4 使用 `vracli proxy set ...` 命令设置 Internet 代理服务器后，可以使用 `vracli proxy apply` 命令更新 Internet 代理服务器配置，并使最新的代理设置处于活动状态。
- 5 如果尚未执行此操作，请运行以下命令以激活脚本更改：

```
/opt/scripts/deploy.sh
```

- 6 （可选）如果需要，请配置代理服务器以支持端口 22 上的外部访问。

要支持 Puppet 和 Ansible 等集成，代理服务器必须允许使用端口 22 访问相关主机。

## 示例： Squid 配置示例

相对于步骤 1，如果设置的是 Squid 代理，可以在 /etc/squid/squid.conf 中调整配置，根据以下示例进行调整：

```
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
```

## 在 vRealize Automation 中，NSX-T 映射到多个 vCenter 有哪些用途

可以将一个 NSX-T 云帐户与一个或多个 vCenter 云帐户相关联，以支持各种部署目标。

可以将同一个现有 NSX-T 网络与不同 vCenter 的网络配置文件相关联，并根据限制在任一 vCenter 中置备部署。下面列出了几个示例：

- 云模板包含具有多个网卡的单个计算机且这些网卡使用同一个网络配置文件，该网络配置文件包含跨多个 vCenter 的 NSX-T 网络。
- 云模板包含一个位于专用网络上的计算机，该网络使用具有基于子网的隔离的网络配置文件且使用跨多个 vCenter 的 NSX-T 现有网络。
- 云模板包含单个位于专用网络上的计算机，该网络使用具有基于安全组的隔离的网络配置文件且使用跨 vCenter 的 NSX-T 网络。

- 云模板包含单个位于路由网络上的计算机，该网络使用包含跨多个 vCenter 的 NSX-T 网络的网络配置文件。
- 云模板包含在网络配置文件中定义的按需负载均衡器，该负载均衡器应用于网络上的所有 vCenter 计算机。
- 云模板包含在网络配置文件中定义的按需网络，该按需网络由使用该网络配置文件的所有 vCenter 使用。
- 云模板包含按需安全组，该安全组可选择性地包含防火墙规则，并且该安全组与网络上的所有 vCenter 相关联。

可以在 NSX-T 网络上配置 vRealize Automation 内部或外部 IPAM，并对在不同 vCenter 中置备的计算机共享同一 IP 地址。

如果未在系统中定义任何网络配置文件，则可以置备一个云模板，该云模板包含位于不同 vCenter 上且共享单个现有 NSX-T 网络的多个计算机。

## 如果在 vRealize Automation 中移除 NSX 云帐户关联，会发生什么情况

如果移除 NSX 云帐户与 vCenter 云帐户之间的关联，还需要更新相关的网络配置文件才能移除关联的 NSX 对象。

如果移除 NSX 云帐户与 vCenter 云帐户之间的关联，vRealize Automation 不会自动更新基础架构元素。您必须更新现有的网络配置文件，才能移除关联的 NSX 对象。

用户界面提供的信息可帮助突出显示受影响的网络配置文件元素，如下所示：

- 如果网络配置文件选择了 NSX 现有网络：
  - 对象标记为无效，并显示消息“某些网络对象丢失或无效 (Some network objects are missing or invalid)。”。
  - 保存网络配置文件时，将移除对象。
- 如果网络配置文件配置了应用程序隔离，则必须先更新隔离策略设置，才能保存网络配置文件。
- 如果网络配置文件选择了安全组或负载均衡器，则在保存网络配置文件时，将移除对象。

对于现有组件，现有部署将继续按设计的方式运行，但在创建新组件（例如在横向扩展操作中）时将失败。

如果重新建立关联，则会重新填充网络配置文件，且现有部署按设计的方式运行。

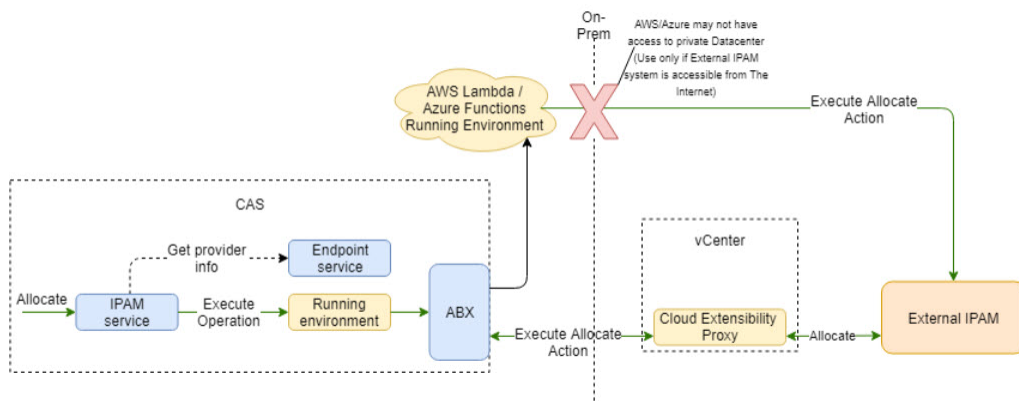
如果移除 NSX 云帐户，上述行为不变，但网络对象标记为缺少，而不是无效。

## 如何使用 IPAM SDK 为 vRealize Automation 创建提供程序特定的外部 IPAM 集成软件包

外部 IPAM 供应商和合作伙伴可以下载并使用 IPAM SDK 创建 IPAM 集成软件包，以便 vRealize Automation 支持其提供程序特定的 IPAM 解决方案。

有关使用提供的 IPAM SDK 为 vRealize Automation 构建和部署自定义 IPAM 集成软件包的过程，请参见为 [VMware Cloud Assembly](#) 创建和部署提供程序特定的 IPAM 集成软件包文档。按照文档中所述，可以从 [VMware code](#) 站点下载最新的 VMware vRealize Automation Third-Party IPAM SDK。以下 IPAM SDK 软件包可供下载：

- [VMware vRealize Automation Third-Party IPAM SDK 1.1.0](#)
- [VMware vRealize Automation Third-Party IPAM SDK 1.0.0](#)



在花时间使用 IPAM SDK 创建供应商特定的 IPAM 集成软件包之前，请检查 vRealize Automation 是否已存在这样一个集成软件包。可从以下位置检查提供程序特定的 IPAM 集成软件包：IPAM 提供程序的网站、[VMware Marketplace](#) 以及 vRealize Automation 的 [商城](#) 选项卡。

虽然教程：[为 vRealize Automation 配置提供程序特定的外部 IPAM 集成](#) 示例特定于供应商，但也包含有用的参考信息。

# 构建您的 vRealize Automation Cloud Assembly 资源基础架构

# 4

在 vRealize Automation Cloud Assembly 资源基础架构中，您可以将云帐户区域定义为可在其中部署云模板及其工作负载的区域。

此外，资源基础架构还涉及创建映像和计算机大小的通用映射，以及创建定义跨云帐户区域或数据中心的网络和存储功能的配置文件。

本章讨论了以下主题：

- 如何添加定义 vRealize Automation Cloud Assembly 目标布置区域或数据中心的云区域
- 如何在 vRealize Automation 中添加特定实例映射以指定通用计算机大小
- 如何在 vRealize Automation 中添加映像映射以访问通用操作系统
- 如何在 vRealize Automation 中添加网络配置文件
- 如何添加负责不同需求的 vRealize Automation Cloud Assembly 存储配置文件
- 如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署
- 如何使用 vRealize Automation 中的资源
- 使用 vRealize Automation 配置多提供者租户资源

## 如何添加定义 vRealize Automation Cloud Assembly 目标布置区域或数据中心的云区域

vRealize Automation Cloud Assembly 云区域是云帐户类型（例如 AWS 或 vSphere）中的一组资源。

特定帐户区域中的云区域是您的云模板部署工作负载的位置。每个云区域均与一个 vRealize Automation Cloud Assembly 项目相关联。

选择**基础架构 > 配置 > 云区域**，然后单击**添加新区域**。

## 了解有关 vRealize Automation Cloud Assembly 云区域的更多信息

vRealize Automation Cloud Assembly 云区域是特定于云帐户类型（如 AWS 或 vSphere）的计算资源区域。

云区域特定于某个区域，必须将其分配给项目。云区域和项目之间存在多对多关系。vRealize Automation Cloud Assembly 支持部署到最常用的公有云，包括 Azure、AWS、GCP 和 vSphere。请参见[将云帐户添加到 vRealize Automation Cloud Assembly](#)。

其他布置控制包括布置策略选项、能力标记和计算标记。

## ■ 布置策略

布置策略有助于为指定云区域内的部署选择主机。

- **default** - 在集群和主机之间随机分发计算资源。此选项在单个计算机级别工作。例如，特定部署中的所有计算机在满足要求的可用集群和主机之间随机分发。
- **binpack** - 将计算资源放置在负载最多但仍有足够资源运行给定计算资源的主机上。
- **spread** - 在部署级别将计算资源置备到虚拟机数量最少的集群或主机。对于 vSphere，Distributed Resource Scheduler (DRS) 会在主机之间分发虚拟机。例如，部署中所有请求的计算机都放置在同一个集群上，但下一次部署可能会根据当前负载选择另一个 vSphere 集群。

例如，假设您具有以下配置：

- DRS 集群 1 具有 5 个虚拟机
- DRS 集群 2 具有 9 个虚拟机
- DRS 集群 3 具有 6 个虚拟机

如果您请求具有 3 个虚拟机的集群，并且选择了 **Spread** 策略，则应将它们全部置于集群 1 上。更新的负载将成为集群 1 的 8 个虚拟机，而集群 2 和 6 的负载仍为 9 个虚拟机和 6 个虚拟机。

随后，如果您请求额外的 2 个虚拟机，则这些虚拟机将放置在 DRS 集群 3 上，该集群现在将有 8 个虚拟机。集群 1 和 3 的负载仍为 8 个虚拟机和 9 个虚拟机。

如果两个云区域都满足置备所需的所有条件，则布置逻辑将选择具有较高优先级的云区域。

## ■ 能力标记

蓝图包含有助于确定部署布置的限制标记。在部署过程中，蓝图限制标记将映射到云区域中匹配的能力标记，以确定哪些云区域可用于计算资源布置。

## ■ 计算资源

可以查看和管理可用于将工作负载（如 AWS 可用区和 vCenter 集群）置备到此云区域的计算资源。

如果 vCenter 计算集群已启用 DRS，则云区域仅显示计算资源列表中的集群，不显示子主机。如果 vCenter 计算集群未启用 DRS，则云区域仅显示独立 ESXi 主机（如果存在）。

根据需要为云区域添加计算资源。最初，筛选器选择是“包括所有计算资源”，下面列表中会显示所有可用的计算资源，且这些资源分配给适用区域。此外，还可以使用两个其他选项将计算资源添加到云区域。

- **手动选择计算资源** - 如果要从下面列表中手动选择计算资源，请选择此选项。选择计算资源后，单击“添加计算资源”以将资源添加到区域。
- **按标记动态包括计算资源** - 如果要根据标记选择要添加到区域的计算资源，请选择此选项。在添加适当的标记之前，将显示所有计算资源。可以在“使用这些标记包括计算资源”选项中选择或输入一个或多个标记。

对于任何一个计算资源选项，都可以通过选择右侧的框并单击“移除”来移除页面上显示的一个或多个计算资源。

计算机标记有助于进一步控制布置。您可以使用标记来筛选可用的计算资源，以便仅列出与一个或多个标记匹配的计算机资源，如以下示例中所示。

- 计算资源不包含任何标记，并且未使用任何筛选。



- 两个计算资源包含同一个标记，但未使用任何筛选。



- 两个计算资源包含同一个标记，并且标记筛选器与两个计算资源上使用的标记匹配。



## ■ 项目

您可以查看哪些项目已配置为支持将工作负载置备到该云区域。创建云区域后，您可以验证其配置。

## 如何在 vRealize Automation 中添加特定实例映射以指定通用计算机大小

在 vRealize Automation 特定实例映射中，您可以使用自然语言为特定的云帐户/区域定义目标部署大小。

特定实例映射表示对您的环境有意义的部署大小。一个示例可能是，对于已命名数据中心中的 vCenter 帐户，以及已命名区域中的 Amazon Web Services 帐户的 t2.nano 实例，small 表示 1 个 CPU 和 2 GB 内存，large 表示 2 个 CPU 和 8 GB 内存。

选择**基础架构 > 配置 > 特定实例映射**，然后单击**新建特定实例映射**。

### 了解有关 vRealize Automation 中的特定实例映射的更多信息

通过使用自然语言命名，特定实例映射对 vRealize Automation 中的特定云帐户/区域所使用的一组目标部署大小进行分组。

使用特定实例映射，您可以创建包含各个帐户区域的相似特定实例大小的命名映射。例如，名为 standard\_small 的特定实例映射可能包含项目中部分或全部可用帐户/区域的相似特定实例大小（例如，1 个 CPU，2GB RAM）。构建云模板时，可以选择适合您需求的可用特定实例。

按部署意图组织项目的特定实例映射。

要简化云模板创建，可以在添加新的云帐户时选择预配置选项。选择预配置选项时，将选择指定区域的组织最常用的特定实例映射和映像映射。

对于包含 vSphere 资源的云模板中的映像映射，如果没有为 vSphere 云区域定义特定实例映射，则可以使用云模板中的 vSphere 特定设置配置无限内存和 CPU。如果为 vSphere 云区域定义了特定实例映射，则特定实例映射将用作云模板中 vSphere 特定配置的限制。

## 如何在 vRealize Automation 中添加映像映射以访问通用操作系统

在 vRealize Automation 映像映射中，您可以使用自然语言为特定的云帐户/区域定义目标部署操作系统。

选择**基础架构 > 配置 > 映像映射**，然后单击**新建映像映射**。

### 了解有关 vRealize Automation 中的映像映射的更多信息

映像映射使用自然语言命名对 vRealize Automation 中特定云帐户/区域使用的一组预定义目标操作系统规范进行分组。

诸如 Microsoft Azure 和 Amazon Web Services 等云供应商帐户使用映像将一组目标部署条件（包括操作系统和相关配置设置）分组到一起。基于 vCenter 和 NSX 的环境（包括 VMware Cloud on AWS）使用类似的分组机制定义一组操作系统部署条件。生成并最终部署和迭代云模板时，您可以选择最符合需求的可用映像。

可以按相似操作系统设置、标记策略和功能部署意向组织项目的映像映射。

要简化云模板创建，可以在添加新的云帐户时选择预配置选项。选择预配置选项时，将选择指定区域的组织最常用的特定实例映射和映像映射。



将映像信息添加到云模板时，可以使用计算机组件 properties 部分中的 image 或 imageRef 条目。例如，如果要从快照克隆，请使用 imageRef 属性。

有关云模板代码中的 image 和 imageRef 条目的示例，请参见第 6 章 [设计 vRealize Automation Cloud Assembly 部署](#)。

要分配内容库的权限，管理员必须将该权限作为全局权限授予用户。有关相关信息，请参见位于 [VMware vSphere 文档](#) 内《vSphere 虚拟机管理》中的[内容库权限的层次结构继承](#)。

## 同步云帐户/区域的映像

您可以运行映像同步，以确保正在[基础架构 > 配置 > 映像映射](#)页面上为给定云帐户/区域添加或移除的映像为最新映像。

- 1 通过选择[基础架构 > 连接 > 云帐户](#)来打开关联的云帐户/区域。选择现有的云帐户/区域。
- 2 单击**同步映像**按钮，然后等待操作完成。



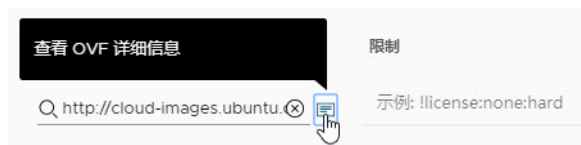
- 3 操作完成后，单击[基础架构 > 配置 > 映像映射](#)。定义新映像映射或编辑现有映像映射，然后选择步骤 1 中的云帐户/区域。
- 4 单击**映像映射**页面上的映像同步图标。



- 5 在**映像映射**页面上为指定云帐户/区域配置映像映射设置。

## 查看 OVF 详细信息

可以在 vRealize Automation Cloud Assembly 云模板对象（如 vCenter 计算机组件和映像映射）中包含 OVF 规范。如果您的映像包含 OVF 文件，则无需打开文件即可发现其内容。将鼠标指针悬停在 OVF 上可显示 OVF 详细信息，包括其名称和位置。有关 OVF 文件格式的更多信息，请参见 [vcenter ovf:property](#)。



## 使用限制和标记细化映像选择

要在云模板中进一步细化映像选择，可以添加一项或多项限制，以便对可部署的映像类型指定基于标记的限制。在创建或编辑映像映射配置时显示的**限制**示例为 `!license:none:hard`。提供的示例说明了基于标记的限制，在该示例中，仅当云模板中不存在 `license:none` 标记时，才可以使用映像。如果添加标记（例如 `license:88` 和 `license:92`），则仅当 `license:88` 和 `license:92` 标记存在于云模板中时，才能使用指定的映像。

### 限制

示例: `!license:none:hard`

## 使用云配置脚本控制部署

您可以在映像映射和/或云模板中使用云配置脚本，来定义要在 vRealize Automation Cloud Assembly 部署中使用的自定义操作系统特性。例如，基于要将云模板部署到公有云还是私有云，可以对映像应用特定的用户权限、操作系统权限或其他条件。云配置脚本遵循 `cloud-init` 格式（适用于基于 Linux 的映像）或 `cloudbase-init` 格式（适用于基于 Windows 的映像）。vRealize Automation Cloud Assembly 支持适用于 Linux 系统的 `cloud-init` 工具和适用于 Windows 系统的 `cloudbase-init` 工具。

对于 Windows 计算机，可以使用 `cloudbase-init` 支持的任何云配置脚本格式。

以下示例云模板代码中的计算机资源使用包含云配置脚本的映像，该映像的内容显示在 `image` 条目中。

```
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}
```

## 映像映射和云模板包含云配置脚本时会出现什么情况

当包含云配置脚本的云模板使用包含云配置脚本的映像映射时，这两个脚本将合并。合并操作首先处理映像映射脚本的内容，再处理云模板脚本的内容，同时考虑脚本的格式是否为 `#cloud-config`。

- 对于采用 `#cloud-config` 格式的脚本，合并会按如下方式组合每个模块（例如 `runcommand`、`users` 和 `write_files`）的内容：
  - 对于内容为列表的模块，将合并映像映射和云模板中的命令列表，不包括两个列表中相同的命令。
  - 对于内容为字典的模块，将合并命令，结果为两个字典的组合。如果两个字典中都存在相同的键，则将保留映像映射脚本字典中的键，而忽略云模板脚本字典中的键。
  - 对于内容为字符串的模块，将保留映像映射脚本中的内容值，而忽略云模板脚本中的内容值。
- 对于采用非 `#cloud-config` 格式的脚本，或者当一个脚本采用 `#cloud-config` 格式，而另一个脚本不采用此格式时，按以下方式将两个脚本组合在一起：先运行映像映射脚本，映像映射脚本完成后运行云模板脚本。

有关相关信息，请参见[合并用户数据区域](#)。

## 有关配置和使用云配置脚本的更多信息

有关使用云配置脚本的详细信息，请参见[如何在 vRealize Automation Cloud Assembly 模板中自动初始化计算机](#)。

另请参见 VMware 博客文章[使用 vRealize Automation 8 或云时通过 Cloud-init 实现 vSphere 自定义和使用 Cloud-Init 自定义 Cloud Assembly 部署](#)。

## 如何在 vRealize Automation 中添加网络配置文件

vRealize Automation 网络配置文件描述要部署的网络的行为。

例如，网络可能需要面向 Internet，而不是仅面向内部。

网络和网络配置文件特定于云。

选择[基础架构 > 配置 > 网络配置文件](#)，然后单击[新建网络配置文件](#)。

## 了解有关 vRealize Automation 中的网络配置文件的更多信息

网络配置文件定义了一组可用于特定区域中的云帐户或 vRealize Automation 中的数据中心的网络和网络设置。

您通常会定义网络配置文件以支持目标部署环境，例如，其中现有网络仅具有出站访问权限的小型测试环境，或需要一组安全策略的大型负载均衡生产环境。将网络配置文件视为特定于工作负载的网络特性的集合。

## 网络配置文件的内容

网络配置文件包含 vRealize Automation 中指定云帐户类型和区域的特定信息，其中包括以下设置：

- 网络配置文件的指定云帐户/区域和可选功能标记。

- 指定的现有网络及其设置。
- 定义网络配置文件按需方面及其他方面的网络策略。
- （可选）包含现有负载均衡器。
- （可选）包含现有安全组。

您可以根据网络配置文件确定网络 IP 管理功能。

网络配置文件功能标记与云模板中的限制标记相匹配，以帮助控制网络选择。此外，分配给网络配置文件所收集网络的所有标记也与云模板中的标记相匹配，以帮助在部署云模板时控制网络选择。

功能标记是可选的。功能标记将应用于网络配置文件中的所有网络，但仅当将这些网络用作该网络配置文件的一部分时适用。对于不包含功能标记的网络配置文件，仅在网络标记上进行标记匹配。部署云模板时，会应用匹配的网络配置文件中定义的网络和安全设置。

使用静态 IP 时，地址范围由 vRealize Automation 进行管理。对于 DHCP，IP 起始地址和结束地址由独立的 DHCP 服务器进行管理，而不是由 vRealize Automation 进行管理。使用 DHCP 或混合网络地址分配时，网络利用率值设置为零。按需网络分配范围基于网络配置文件中指定的 CIDR 和子网大小。要在部署中同时支持静态和动态地址分配，所分配的地址范围将一分为二：一个用于静态分配，另一个用于动态分配。

## 网络

网络（也称为子网）是 IP 网络的逻辑细分。网络会对云帐户、IP 地址或范围以及网络标记进行分组，以控制置备云模板部署的方式和位置。配置文件中的网络参数定义了部署中的计算机如何通过 IP 第 3 层互相进行通信。网络可以具有标记。

可以将网络添加到网络配置文件，编辑网络配置文件使用的网络各个方面，以及从网络配置文件中移除网络。

---

**注** 对于 VMware Cloud Foundation (VCF) 云帐户类型，只能将 NSX 网络添加到网络配置文件，而不能添加 vSphere 网络。NSX 网络分段是在 NSX-T 网络上本地创建的，而不是作为全局网络创建的。

---

### ■ 网络域或传输区域

网络域或传输区域是 vSphere vNetwork 分布式端口组 (dvPortGroup) 的分布式虚拟交换机 (dvSwitch)。*传输区域*是一个现有的 NSX 概念，类似于 *dvSwitch* 或 *dvPortGroup* 等术语。

使用 NSX 云帐户时，页面上的元素名称为**传输区域**，否则为**网络域**。

对于标准交换机，网络域或传输区域与交换机本身相同。网络域或传输区域定义 vCenter 内的子网边界。

传输区域控制 NSX 逻辑交换机可以访问的主机。它可以跨一个或多个 vSphere 集群。传输区域控制哪些集群及哪些虚拟机可以参与使用特定的网络。属于同一 NSX 传输区域的子网可用于相同的计算机主机。

### ■ 域

表示目标虚拟机的 vCenter Single Sign-On 域。域由 vCenter 管理员在 vSphere 配置期间配置。域确定了 vCenter 中的本地身份验证空间。

## ■ IPv4 CIDR 和 IPv4 默认网关

vSphere 云帐户和云模板中的 vSphere 计算机组件支持双 IPv6 和 IPv4 Internet 协议方法。例如，192.168.100.14/24 表示 IPv4 地址 192.168.100.14 及其关联的路由前缀 192.168.100.0，或者等效于其子网掩码 255.255.255.0，它具有 24 个前导 1 位。IPv4 块 192.168.100.0/22 表示从 192.168.100.0 到 192.168.103.255 的 1024 个 IP 地址。

## ■ IPv6 CIDR 和 IPv6 默认网关

vSphere 云帐户和云模板中的 vSphere 计算机组件支持双 IPv6 和 IPv4 Internet 协议方法。例如，2001:db8::/48 表示从 2001:db8:0:0:0:0:0:0 到 2001:db8:0:ffff:ffff:ffff:ffff:ffff 的 IPv6 地址块。

按需网络不支持 IPv6 格式。

## ■ DNS 服务器和 DNS 搜索域

## ■ 支持公共 IP

选择此选项可将网络标记为公共网络。云模板中具有 `network type: public` 属性的网络组件与标记为公共的网络匹配。将在云模板部署期间进行进一步匹配以确定网络选择。

## ■ 区域的默认值

选择此选项可将网络标记为云区域的默认网络。在云模板部署过程中，默认网络优先于其他网络。

## ■ 来源

标识网络源。

## ■ 标记

指定分配给网络的一个或多个标记。标记是可选项。标记匹配会影响可用于云模板部署的网络。

网络项本身存在网络标记，而与网络配置文件无关。网络标记应用于其添加到的网络的每个实例，以及包含该网络的所有网络配置文件。网络可以实例化到任意数量的网络配置文件中。无论网络配置文件的驻留方式如何，网络标记在使用网络的任何地方都与该网络相关联。

部署云模板时，云模板网络组件中的限制标记与网络标记（包括网络配置文件功能标记）匹配。对于包含功能标记的网络配置文件，功能标记将应用于该网络配置文件的所有可用网络。部署云模板时，会应用匹配的网络配置文件中定义的网络和安全设置。

## 网络策略

通过使用网络配置文件，您可以为包含静态、DHCP 或混合使用静态和 DHCP IP 地址设置的现有网络域定义子网。您可以使用**网络策略**选项卡定义子网并指定 IP 地址设置。

使用 NSX-V、NSX-T 或 VMware Cloud on AWS 时，如果云模板需要 `networkType: outbound` 或 `networkType: private` 或者 NSX 网络需要 `networkType: routed`，将使用网络策略设置。

根据关联的云帐户，可以使用网络策略为 `outbound`、`private` 和 `routed` 网络类型以及按需安全组定义设置。当存在与该网络关联的负载均衡器时，也可以使用网络策略控制 `existing` 网络。

出站网络允许单向访问上游网络。专用网络不允许任何外部访问。路由网络允许路由网络之间的东西向流量。此配置文件中的现有网络和公共网络都将用作底层网络或上游网络。

以下按需选择的选项在**网络配置文件**屏幕帮助中进行了说明，并汇总如下。

- **不创建按需网络或按需安全组**

在指定 `existing` 或 `public` 网络类型时，可以使用此选项。需要 `outbound`、`private` 或 `routed` 网络的云模板与此配置文件不匹配。

- **创建按需网络**

在指定 `outbound`、`private` 或 `routed` 网络类型时，可以使用此选项。

Amazon Web Services、Microsoft Azure、NSX、vSphere 和 VMware Cloud on AWS 支持此选项。

- **创建按需安全组**

在指定 `outbound` 或 `private` 网络类型时，可以使用此选项。

如果网络类型为 `outbound` 或 `private`，则会为匹配的云模板创建新的安全组。

Amazon Web Services、Microsoft Azure、NSX 和 VMware Cloud on AWS 支持此选项。

网络策略设置可以特定于云帐户类型。这些设置在屏幕上的标志帮助中进行了说明，并汇总如下：

- **网络域或传输区域**

网络域或传输区域是 vSphere vNetwork 分布式端口组 (dvPortGroup) 的分布式虚拟交换机 (dvSwitch)。*传输区域*是一个现有的 NSX 概念，类似于 *dvSwitch* 或 *dvPortGroup* 等术语。

使用 NSX 云帐户时，页面上的元素名称为**传输区域**，否则为**网络域**。

对于标准交换机，网络域或传输区域与交换机本身相同。网络域或传输区域定义 vCenter 内的子网边界。

传输区域控制 NSX 逻辑交换机可以访问的主机。它可以跨一个或多个 vSphere 集群。传输区域控制哪些集群及哪些虚拟机可以参与使用特定的网络。属于同一 NSX 传输区域的子网可用于相同的计算机主机。

- **外部子网**

具有出站访问权限的按需网络需要具有出站访问权限的外部子网。该外部子网用于提供出站访问权限（在云模板中请求时），它不控制网络布置。例如，该外部子网不影响专用网络的放置。

- **CIDR**

CIDR 表示法是 IP 地址及其关联的路由前缀的精简表示形式。CIDR 值指定了在置备期间用于创建子网的网络地址范围。**网络策略**选项卡上的此 CIDR 设置接受 IPv4 表示法，即以 `/nn` 结尾并包含介于 0-32 之间的值。

- **子网大小**

此选项为使用此网络配置文件的部署中的每个隔离网络指定按需网络大小（使用 IPv4 表示法）。子网大小设置可用于管理内部或外部 IP 地址。

按需网络不支持 IPv6 格式。

- **分布式逻辑路由器**

对于按需路由网络，使用 NSX-V 云帐户时必须指定分布式逻辑网络。

分布式逻辑路由器 (DLR) 用于在 NSX-V 上的按需路由网络之间路由东西向流量。仅当网络配置文件的帐户/区域值与 NSX-VCloud 帐户相关联时，此选项才可见。

## ■ IP 范围分配

此选项适用于支持 NSX 或 VMware Cloud on AWS 的云帐户，包括 vSphere。

在使用具有外部 IPAM 集成点的现有网络时，IP 范围设置可用。

可以选择以下三个选项之一来为部署网络指定 IP 范围分配类型：

### ■ 静态和 DHCP

默认选项，同时为推荐选项。此混合选项通过使用分配的 CIDR 和子网范围设置，将 DHCP 服务器池配置为使用 DHCP（动态）方法支持一半的地址空间分配，使用静态方法支持一半的 IP 地址空间分配。当连接到按需网络的一些计算机需要分配的静态 IP 地址，而一些计算机需要动态 IP 地址时，使用此选项。将创建两个 IP 范围。

在计算机连接到按需网络的部署（即，一些计算机分配有静态 IP，而另一些计算机由 NSXDHCP 服务器动态分配 IP）中，以及负载均衡器 VIP 为静态的部署中，此选项最为有效。

### ■ DHCP (动态)

此选项使用分配的 CIDR 在 DHCP 服务器上配置 IP 池。此网络的所有 IP 地址都动态分配。将为每个分配的 CIDR 创建一个 IP 范围。

### ■ 静态

此选项使用分配的 CIDR 静态分配 IP 地址。不需要为此网络配置 DHCP 服务器时使用此选项。将为每个分配的 CIDR 创建一个 IP 范围。

## ■ IP 段

在使用具有外部 IPAM 集成点的按需网络时，IP 段设置可用。

使用“IP 段”设置，可以将指定的 IP 段或范围添加到集成的外部 IPAM 提供程序中的网络配置文件。您还可以从网络配置文件中移除已添加的 IP 段。有关如何创建外部 IPAM 集成的信息，请参见在 [vRealize Automation 中为 Infoblox 添加外部 IPAM 集成](#)。

外部 IPAM 可用于以下云帐户/区域类型：

### ■ vSphere

#### ■ 采用 vSphere 的 NSX-T

#### ■ 采用 vSphere 的 NSX-V

## ■ 网络资源 - 外部网络

外部网络也称为现有网络。这些网络已进行数据收集，可供选择。

## ■ 网络资源 - 第 0 层逻辑路由器

NSX-T 使用第 0 层逻辑路由器作为 NSX 部署外部网络的网关。第 0 层逻辑路由器为按需网络配置出站访问权限。

## ■ 网络资源 - Edge 集群

指定的 Edge 集群提供路由服务。Edge 集群用于为按需网络和负载均衡器配置出站访问权限。它可标识要在其中部署 Edge 设备的 Edge 集群或资源池。

## ■ 网络资源 - Edge 数据存储

指定的 Edge 数据存储用于置备 Edge 设备。此设置仅适用于 NSX-V。

标记可用于指定哪些网络可用于云模板。

## 负载均衡器

可以在网络配置文件中添加负载均衡器。可根据从源云帐户收集的数据信息使用列出的负载均衡器。

如果网络配置文件中任何负载均衡器上的标记与云模板中负载均衡器组件上的标记相匹配，则会在部署过程中考虑负载均衡器。在部署云模板时，将使用匹配网络配置文件中的负载均衡器。

有关详细信息，请参见使用 [vRealize Automation Cloud Assembly](#) 的网络配置文件中的负载均衡器设置和 [vRealize Automation](#) 云模板中的网络、安全性和负载均衡器示例。

## 安全组

部署云模板时，云模板网络配置文件中的安全组将应用于已置备的计算机网卡。对于特定于 Amazon Web Services 的网络配置文件，网络配置文件中的安全组在“网络”选项卡上列出的网络所在的网络域 (VPC) 中可用。如果网络配置文件的“网络”选项卡上未列出任何网络，则会显示所有可用的安全组。

您可以使用安全组为 private 或 outbound 按需网络进一步定义隔离设置。安全组也适用于 existing 网络。

安全组基于信息（即从源云帐户收集到的数据）列出，或者在项目云模板中添加为按需安全组。有关详细信息，请参见 [vRealize Automation](#) 中的安全资源。

安全组将应用于部署中连接到与网络配置文件匹配的网络的所有计算机。由于云模板中可能存在多个网络，每个网络都与不同的网络配置文件相匹配，因此您可以对不同的网络使用不同的安全组。

通过向现有安全组添加标记，将能够在云模板 Cloud.SecurityGroup 组件中使用该安全组。安全组必须至少包含一个标记，否则无法在云模板中使用。有关详细信息，请参见 [vRealize Automation](#) 中的安全资源和 [vRealize Automation](#) 云模板中的网络、安全性和负载均衡器示例。

## 有关网络配置文件、网络、云模板和标记的更多信息

有关网络的详细信息，请参见 [vRealize Automation](#) 中的网络资源。

有关云模板中示例网络组件代码的示例，请参见 [vRealize Automation](#) 云模板中的网络、安全性和负载均衡器示例。

有关示例网络自动化工作流，请参见 [Cloud Assembly](#) 和 [NSX](#) 的网络自动化。

有关标记和标记策略的详细信息，请参见 [如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署](#)。



## 在 vRealize Automation 的网络配置文件和云模板中使用网络设置

可以在 vRealize Automation 中使用网络和网络配置文件来帮助定义部署的网络置备行为。

在 vRealize Automation 中，您可以定义特定于云的网络配置文件。请参见[了解有关 vRealize Automation 中的网络配置文件的更多信息](#)。

使用网络和网络配置文件设置，您可以控制在 vRealize Automation 云模板和部署中使用网络 IP 地址的方式。

### vRealize Automation 网络中的 IPv4 和 IPv6 支持

vRealize Automation 网络支持纯 IPv4 或双堆栈 IPv4 和 IPv6。当前不支持纯 IPv6。

虽然所有云帐户和集成类型均支持纯 IPv4，但仅 vSphere 云帐户及其端点支持双堆栈 IPv4 和 IPv6。

当前不支持将 IPv6 用于负载均衡器、NSX 按需网络或外部第三方 IPAM 提供程序。

### 外部 IPAM 提供程序支持

除了提供的内部 IPAM 支持之外，您还可以使用外部 IPAM 提供程序以动态或静态方式为网络分配 IP 地址 - 对于云模板设计和部署中的现有网络，以 IP 范围的形式分配；对于云模板设计和部署中的按需网络，以 IP 块的方式分配。

通过[基础架构 > 连接 > 添加集成 > IPAM](#) 菜单顺序创建的供应商特定的 IPAM 集成点支持外部 IPAM 提供程序（如 Infoblox）。

通过使用[网络策略 > 添加 IPAM IP 范围](#)页面上的[添加 IPAM IP 范围](#)选项，可以使用用于定义外部 IPAM 提供程序地址信息的选项。

有关如何创建外部 IPAM 集成点的信息，请参见[如何在 vRealize Automation 中配置外部 IPAM 集成](#)。有关如何为特定 IPAM 供应商创建 IPAM 集成点的示例，请参见教程：[为 vRealize Automation 配置提供程序特定的外部 IPAM 集成](#)。

### 网络类型

云模板中的网络组件定义为以下 `networkType` 类型之一。

网络类型	定义
<code>existing</code>	选择在底层云提供商（例如 vCenter、Amazon Web Services 和 Microsoft Azure）上配置的现有网络。outbound 按需网络需要现有网络。 可以在现有网络上定义一系列静态 IP 地址。
<code>public</code>	可以从 Internet 访问公共网络上的计算机。IT 管理委员会定义这些网络。对于允许通过公共网络传输网络流量的网络， <code>public</code> 网络的定义与 <code>existing</code> 网络的定义相同。
<code>private</code>	按需网络类型。 将网络流量限制为仅在已部署网络上的资源之间发生。它可防止入站和出站流量。在 NSX 中，它可以等同于按需 NAT 一对多。

网络类型	定义
outbound	<p>按需网络类型。</p> <p>将网络流量限制为在部署中的计算资源之间发生，但也允许单向出站网络流量。在 NSX 中，它可以等同于具有外部 IP 的按需 NAT 一对多。</p>
routed	<p>按需网络类型。</p> <p>路由网络包含一个可路由的 IP 空间，该空间被划分为链接在一起的多个可用子网。置备路由网络和具有相同路由网络配置文件的虚拟机既可相互通信，也可与现有网络通信。</p> <p>路由网络是可用于 NSX-V 和 NSX-T 网络的按需网络类型。默认情况下，Microsoft Azure 和 Amazon Web Services 提供此连接。</p> <p>routed 网络只能在 Cloud.NSX.Network 网络组件中用于云模板规范。</p>

有关包含网络组件数据的已填充云模板的示例，请参见 [vRealize Automation 云模板中的网络、安全性和负载均衡器示例](#)。

## 网络方案

部署使用以下网络配置文件配置的云模板时，以下是预期行为。

网络类型或方案	没有任何网络配置文件可用于云区域	多个网络配置文件可用于云区域
无网络	<p>如果在云模板中未指定任何网络，则将从与计算资源相同的置备区域中选择一个随机网络。</p> <p>标记为默认的网络优先。</p> <p>如果可用的置备区域中不存在任何网络，置备将失败。</p>	<p>从匹配的网络配置文件中选择一个网络。</p> <p>标记为默认的网络优先。</p> <p>如果没有任何网络配置文件符合条件，置备将失败。</p>
现有网络	<p>如果云模板中的网络组件包含限制标记，则会使用这些限制来筛选可用网络的列表。云模板网络组件中的限制标记将与网络标记进行匹配，如果存在网络配置文件限制标记，则还会与网络配置文件限制标记进行匹配。</p> <p>在筛选的网络列表中，从与计算资源相同的置备区域中选择一个随机网络。</p> <p>标记为默认的网络优先。</p> <p>根据限制进行筛选之后，如果置备区域中没有任何网络，置备将失败。</p>	<p>从匹配的网络配置文件中选择一个网络。</p> <p>标记为默认的网络优先。</p> <p>如果没有任何网络配置文件符合条件，置备将失败。</p> <p>可以使用网络限制根据预分配的标记筛选配置文件中的现有网络。</p>
公共网络	<p>如果网络具有限制，则使用这些限制来筛选设置了 supports public IP 属性的可用网络的列表。</p> <p>在筛选的网络列表中，从与计算资源相同的置备区域中选择一个随机网络。</p> <p>标记为默认的网络优先。</p> <p>根据限制进行筛选之后，如果置备区域中没有任何公共网络，置备将失败。</p>	<p>从匹配的网络配置文件中选择具有 supports public IP 属性的网络。</p> <p>标记为默认的网络优先。</p> <p>可以使用网络限制根据预分配的标记筛选配置文件中的现有公共网络。</p>

网络类型或方案	没有任何网络配置文件可用于云区域	多个网络配置文件可用于云区域
专用网络	置备失败，因为专用网络需要网络配置文件中的信息。	将根据匹配的网络配置文件中的设置创建新的网络或新的安全组。 可以使用网络限制标记来筛选网络配置文件和网络。
出站网络	置备失败，因为出站网络需要网络配置文件中的信息。	将根据匹配的网络配置文件中的设置创建新的网络或新的安全组。 可以使用网络限制标记来筛选网络配置文件和网络。
按需路由网络	置备失败，因为路由网络需要网络配置文件中的信息。	对于 NSX-V，我们需要选择 DLR（分布式逻辑路由器）。 对于 NSX-T 和 VMware Cloud on AWS，我们需要与专用网络和出站网络相似的按需设置。
使用现有网络或公共网络的 Wordpress 用例示例	按照现有网络或公共网络中所述进行置备。	有关使用现有网络和公共网络时的行为，请参见上述内容。 请参见教程：在 <a href="#">vRealize Automation Cloud Assembly</a> 中设置和测试多云基础架构和部署。
使用现有网络或公共网络和专用网络或出站网络的 Wordpress 用例示例	置备失败，因为网络需要网络配置文件中的信息。	有关专用网络和出站网络，请参见上述内容。 请参见教程：在 <a href="#">vRealize Automation Cloud Assembly</a> 中设置和测试多云基础架构和部署。
使用负载均衡器的 Wordpress 用例示例	置备失败，因为负载均衡器需要网络配置文件中的信息。 如果存在现有负载均衡器，则可以进行置备。	根据网络配置文件配置创建新的负载均衡器。 可以指定网络配置文件中已启用的现有负载均衡器。 如果您请求现有负载均衡器，但网络配置文件中的所有负载均衡器均不满足限制，置备将失败。 请参见教程：在 <a href="#">vRealize Automation Cloud Assembly</a> 中设置和测试多云基础架构和部署。

## 在 vRealize Automation Cloud Assembly 的网络配置文件和云模板设计中使用安全组设置

可以在网络配置文件和云模板设计中定义和更改安全组设置。

可以通过多种方式使用安全组功能：

- 网络配置文件中指定的现有安全组

您可以将现有安全组添加到网络配置文件中。当云模板设计使用该网络配置文件时，其计算机将作为安全组的成员分组在一起。此方法不要求您将安全组资源添加到云模板设计。您也可以在此配置中使用负载均衡器。相关信息请参见在 [vRealize Automation 云模板中使用负载均衡器资源](#)。

- 将安全组组件关联到云模板设计中的计算机资源

可以将安全组资源拖放到云模板设计中，并使用云模板设计中现有安全组资源上和数据收集资源中现有安全组上的限制标记将安全组资源绑定到计算机网卡。您可以通过在云模板设计画布上使用连接线将对象连接在一起来建立此关联，类似于将网络关联到设计画布上的计算机。

将安全组资源拖放到云模板设计画布中时，其类型可以是 `existing` 或 `new`。如果是 `existing` 安全组类型，则应根据提示添加标记限制值。如果是 `new` 安全组类型，则可以配置防火墙规则。

- 为现有安全组分配标记限制并与云模板中的计算机网卡关联

例如，您可以通过匹配两个资源之间的标记，将安全组资源关联到云模板设计中的计算机网卡（在计算机资源中）。

针对 `NSX-T` 举例来说，如果在源端点中指定了标记，则可以使用 `NSX-T` 应用程序中指定的 `NSX-T` 标记。然后，可以使用在云模板设计中的网络资源上指定为限制的 `NSX-T` 标记，网络资源将通过该标记连接到云模板设计中的计算机网卡。通过 `NSX-T` 标记，可以使用预定义的 `NSX-T` 标记（即已从 `NSX-T` 源端点收集数据）动态分组计算机。在 `NSX-T` 中创建 `NSX-T` 标记时，使用逻辑端口。

- 云模板设计中的按需安全组资源中的防火墙规则

您可以在云模板设计中将防火墙规则添加到按需安全组。

有关可用防火墙规则的信息，请参见在 [vRealize Automation 云模板中使用安全组资源](#)。

## 了解更多

有关在网络配置文件中定义安全组的信息，请参见 [了解有关 vRealize Automation 中的网络配置文件的更多信息](#)。

有关在基础架构资源页面中查看和更改安全组设置的信息，请参见 [vRealize Automation 中的安全资源](#)。

有关在云模板设计中定义安全组的信息，请参见在 [vRealize Automation 云模板中使用安全组资源](#)。

有关云模板设计中的安全组资源示例，请参见 [vRealize Automation 云模板中的网络、安全性和负载均衡器示例](#)。

## 使用 vRealize Automation Cloud Assembly 的网络配置文件中的负载均衡器设置

您可以在网络配置文件配置中配置负载均衡器设置。

您可以使用 **负载均衡器** 选项卡将现有负载均衡器添加到网络配置文件。

要将负载均衡器添加到云模板设计中，可以通过将负载均衡器与包含一个或多个负载均衡器的网络配置文件相关联，也可以通过在云模板设计画布或代码中直接使用负载均衡器资源。

### 包括基于网络配置文件中的安全组使用的负载均衡器 VIP 示例

您可以在网络配置文件中使用两种类型的安全组 - 从 **安全组** 选项卡中选择的现有安全组和 **网络策略** 选项卡上使用隔离策略创建的按需安全组。

当负载均衡器 VIP 关联到基于网络配置文件设置的安全组时，安全组配置由网络配置文件提供。

下表说明了一些示例场景。

云模板设计拓扑 - 关联的资源	网络配置文件配置	安全组成员资格
单臂负载均衡器，VIP 位于专用网络上，计算机位于同一个专用网络上。	所选网络配置文件使用定义为按需安全组的隔离策略。	计算机网卡和负载均衡器 VIP 添加到隔离安全组。
单臂负载均衡器，VIP 位于专用网络上，计算机位于同一个专用网络上。	所选网络配置文件使用现有的安全组，并使用定义为按需安全组的隔离策略。	计算机网卡和负载均衡器 VIP 添加到隔离安全组和现有安全组。
双臂负载均衡器，VIP 位于公共网络上，计算机位于专用网络上。	所选网络配置文件使用现有的安全组，并使用定义为按需安全组的隔离策略。	计算机网卡和负载均衡器 VIP 添加到隔离安全组和现有安全组。
双臂负载均衡器，VIP 位于公共网络上，计算机位于专用网络上。	所选网络配置文件使用现有的安全组。	计算机网卡和负载均衡器 VIP 添加到现有安全组。
双臂负载均衡器，VIP 位于网络 1 上，计算机位于网络 2 上。	两个网络配置文件： <ul style="list-style-type: none"> <li>■ 网络配置文件 1：使用现有安全组 1。</li> <li>■ 网络配置文件 2：使用现有安全组 2。</li> </ul>	负载均衡器位于网络配置文件 1 上，计算机位于网络配置文件 2 上。 负载均衡器 VIP 添加到安全组 1，计算机网卡添加到安全组 2。

## 了解更多

有关将负载均衡器资源添加到云模板设计中的信息，请参见在 [vRealize Automation 云模板中使用负载均衡器资源](#)。

有关包含负载均衡器的云模板设计示例，请参见 [vRealize Automation 云模板中的网络、安全性和负载均衡器示例](#)。

## 如何在 vRealize Automation 中配置网络配置文件以对外部 IPAM 集成支持按需网络

在使用外部 IPAM 集成的 vRealize Automation 云模板中使用网络配置文件时，可以配置该网络配置文件，对按需网络支持 IP 地址段。

对特定外部 IPAM 提供程序使用现有集成时，可以置备按需网络，以在外部 IPAM 系统中创建新网络。

通过此过程，可以配置 IP 地址块，而不是提供父 CIDR（就像使用 vRealize Automation 的内部 IPAM 时所做的那样）。在按需网络置备过程中使用该 IP 地址块，以对新网络进行分段。如果集成支持按需网络，则将从外部 IPAM 提供程序收集 IP 段数据。例如，使用 Infoblox IPAM 集成时，IP 段表示 Infoblox 网络容器。

如果在云模板中使用按需网络配置文件和外部 IPAM 集成，部署云模板时会发生以下事件：

- 在外部 IPAM 提供程序中创建网络。
- 此外，还会在 vRealize Automation 中创建一个网络，以反映 IPAM 提供程序中的新网络配置，包括 CIDR 和网关属性等设置。
- 从新创建的网络中获取已部署虚拟机的 IP 地址。

在此按需网络示例中，将配置网络配置文件，以允许云模板部署通过使用 Infoblox 作为外部 IPAM 提供程序，将计算机置备到 vSphere 中的按需网络。

有关相关信息，请参见 [如何在 vRealize Automation 中配置网络配置文件以对外部 IPAM 集成支持现有网络](#)。这两个网络配置示例都适用于 [教程：为 vRealize Automation 配置 VMware Cloud on AWS 中外部 IPAM 集成的整体供应商特定工作流](#)。

## 前提条件

虽然创建或编辑网络配置文件的人员需要满足以下必备条件，但在包含 IPAM 集成的云模板部署中使用网络配置文件时，网络配置文件本身将适用。要了解供应商特定的 IPAM 集成点，请参见[如何在 vRealize Automation 中配置外部 IPAM 集成](#)。

此步骤顺序显示在 IPAM 提供程序集成工作流的上下文中。请参见教程：[为 vRealize Automation 配置提供程序特定的外部 IPAM 集成](#)。

- 确认您具有云管理员凭据。请参见在 [vRealize Automation](#) 中使用云帐户所需的凭据。
- 确认您具有云管理员用户角色。请参见 [vRealize Automation 用户角色是什么](#)。
- 确认您具有外部 IPAM 提供程序（例如 [Infoblox](#) 或 [Bluecat](#)）的帐户，并且具有使用 IPAM 提供程序访问组织帐户的正确访问凭据。在此示例工作流中，IPAM 提供程序为 Infoblox。
- 确认您具有 IPAM 提供程序的 IPAM 集成点，以及用于创建 IPAM 集成的 IPAM 软件包支持按需网络。请参见在 [vRealize Automation](#) 中为 [Infoblox](#) 添加外部 IPAM 集成。

虽然 Infoblox IPAM 软件包支持按需网络，但如果对不同提供程序使用外部 IPAM 集成，请确认其 IPAM 集成软件包支持按需网络。

## 步骤

1 要配置网络配置文件，请单击**基础架构 > 配置 > 网络配置文件**。

2 单击**新建网络配置文件**。

3 单击**摘要**选项卡，然后指定以下示例设置：

- 指定 vSphere 的云帐户/区域，例如 **vSphere-IPAM-OnDemandA/Datacenter**。

此示例假设使用与 NSX 云帐户没有关联的 vSphere 云帐户。

- 对网络配置文件进行命名，例如 **Infoblox-OnDemandNP**。
- 为网络配置文件添加功能标记，如 **infoblox\_ondemandA**。

请记录功能标记，因为还必须将其用作云模板限制标记，才能在置备云模板时使用网络配置文件关联。

4 单击**网络策略**选项卡，然后指定以下示例设置：

- 从**隔离策略**下拉菜单中，选择**按需网络**。

此选项允许您使用外部 IPAM IP 段。根据使用的云帐户，将显示新选项。例如，使用与 NSX 云帐户关联的 vSphere 云帐户时，将显示以下选项：

- 传输区域
- 第 0 层逻辑路由器
- 边缘集群

在此示例中，vSphere 云帐户未关联到 NSX，因此将显示**网络域**菜单选项。

- 将**网络域**选项留空。



- 5 单击**外部**作为地址管理**源**。
- 6 单击**添加 IP 段**，这将打开**添加 IPAM IP 段**页面。
- 7 从**添加 IPAM IP 段**页面上的**提供程序**菜单中，选择现有的外部 IPAM 集成。例如，从示例工作流的在 [vRealize Automation 中为 Infoblox 添加外部 IPAM 集成](#) 中选择 *Infoblox\_Integration* 集成点。
- 8 从**地址空间**菜单中，选择列出的可用 IP 段之一（例如 **10.23.118.0/24**），然后将其添加。  
如果 IPAM 提供程序支持地址空间，则会显示**地址空间**菜单。对于 Infoblox 集成，地址空间由 Infoblox 网络视图表示。
- 9 选择**子网大小**，例如 **/29 (-6 个 IP 地址)**。
- 10 单击**创建**。

## 结果

将创建一个网络配置文件，可用于使用指定的外部 IPAM 集成置备按需网络。以下示例云模板显示了要部署到由该新网络配置文件定义的网络的单个计算机。

```
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
```

**注** 部署云模板时，将获取指定 IP 段中的第一个可用网络，并将其视为网络 CIDR。如果在云模板中使用 NSX 网络，可以手动设置网络的 CIDR，即使用网络属性 `networkCidr`（如下所示）手动设置 CIDR 并覆盖在关联网络配置文件中指定的 IP 段和子网大小设置。

```
Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkCidr: 10.10.0.0/16
```

## 如何在 vRealize Automation 中配置网络配置文件以对外部 IPAM 集成支持现有网络

如果在使用外部 IPAM 集成的 vRealize Automation 蓝图中使用网络配置文件，则可以配置该网络配置文件，以对现有网络支持 IP 地址范围。

在 [vRealize Automation](#) 中配置网络和网络配置文件，以对现有网络使用外部 IPAM 中供应商特定的示例工作流的上下文中提供了一个示例。有关外部 IPAM 集成的供应商特定的整体工作流，请参见[教程：为 vRealize Automation 配置 VMware Cloud on AWS](#)。

有关相关信息，请参见 [如何在 vRealize Automation 中配置网络配置文件以对外部 IPAM 集成支持按需网络](#)。

## 如何添加负责不同需求的 vRealize Automation Cloud Assembly 存储配置文件

vRealize Automation Cloud Assembly 存储配置文件描述要部署的存储的类型。

存储通常根据服务级别或成本、性能或用途（例如备份）等特性进行分析。

选择[基础架构 > 配置 > 存储配置文件](#)，然后单击[新建存储配置文件](#)。

### 了解有关 vRealize Automation 中的存储配置文件的更多信息

云帐户区域包含存储配置文件，云管理员可以使用存储配置文件在 vRealize Automation 中为该区域定义存储。

存储配置文件包含磁盘自定义，以及用于按能力标记标识存储类型的方法。标记随后将与置备服务请求限制进行匹配，以在部署时创建所需的存储。

存储配置文件在特定于云的区域下进行组织。一个云帐户可能具有多个区域，每个区域下可能有多个存储配置文件。

可以进行不受供应商约束的布置。例如，将三个不同的供应商帐户可视化，且每个帐户分别具有一个区域。每个区域包含具有 **fast** 能力标记的存储配置文件。在置备时，无论资源由哪个供应商云提供，包含 **fast** 硬性限制标记的请求都将查找匹配的 **fast** 能力。随后在创建已部署的存储项期间，匹配将应用关联的存储配置文件中的设置。

---

**注** 不同的云存储可能具有不同的性能特性，但标记了该云存储的管理员仍将其视为 **fast** 存储。

---

添加到存储配置文件的能力标记不应标识实际资源目标。相反，能力标记描述存储类型。有关实际资源的更多信息，请参见 [vRealize Automation 中的存储资源](#)。

可以创建存储配置文件，以通过使用存储配置文件页面上的[磁盘类型](#)选项或使用 vRealize Automation API 支持第一类磁盘 (FCD) 存储或标准磁盘存储。选择第一类磁盘 (FCD) 选项时，可以有效地创建 vSphere 存储配置文件。

#### ■ 第一类磁盘



可以独立于 vSphere 虚拟机创建和管理第一类磁盘。FCD 的生命周期管理功能也可独立于虚拟机运行。FCD 可以在 vSphere 版本 6.7 Update 2 及更高版本中使用，当前在 vRealize Automation 中作为一项仅 API 功能实施。

有关第一类磁盘 (FCD) 存储的信息，包括可通过 vRealize Automation API 使用的功能以及 API 文档本身的链接，请参见在 [vRealize Automation](#) 中可以对第一类磁盘存储执行哪些操作。

#### ■ 标准磁盘

标准磁盘存储作为虚拟机的集成组件进行创建和管理。

有关标准磁盘存储的信息，请参见在 [vRealize Automation](#) 中可以对标准磁盘存储执行哪些操作和在 [vRealize Automation](#) 中可以对永久磁盘存储执行哪些操作。

## 如何使用标记来管理 vRealize Automation Cloud Assembly 资源和部署

标记是 vRealize Automation Cloud Assembly 的一个关键组件，它通过匹配功能和限制来辅助部署的布置。您必须有效地了解和实施标记，才能更好地利用 vRealize Automation Cloud Assembly。

从根本上说，标记是添加到 vRealize Automation Cloud Assembly 项目的标签。您可以创建适用于您的组织和实施的任何标记。但是标记的功能比标签多得多，因为它们控制 vRealize Automation Cloud Assembly 使用资源和基础架构的方式和位置以生成可部署服务。标记还支持在 Cloud Assembly 中进行管治。

### 标记结构

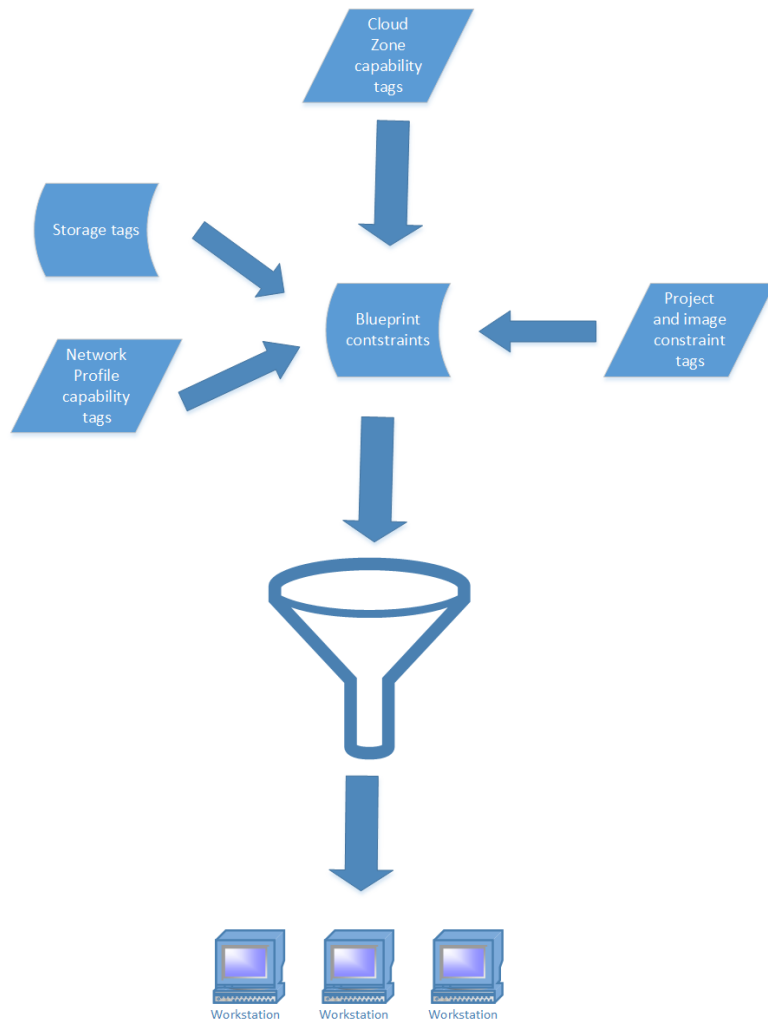
在结构上，标记必须遵循 `name:value` 的约定，但在其他方面其结构在很大程度上是自由形式。在 vRealize Automation Cloud Assembly 中，所有标记看起来都是相同的，并且标记功能由上下文确定。

例如，基础架构资源上的标记主要用作功能标记，因为 vRealize Automation Cloud Assembly 使用它们将资源与部署进行匹配。其次，它们还会标识资源。

### 标记功能

标记的主要功能是表示 vRealize Automation Cloud Assembly 用于定义部署的功能和限制。上下文确定标记的功能。放置在云区域、网络 and 存储配置文件以及各个基础架构资源上的标记用作功能标记，并定义部署中所用基础架构的所需功能。放置在云模板上的标记用作为部署定义资源的限制。此外，云管理员还可以在项目上放置限制标记，以对这些项目执行某种形式的监管。这些限制标记将添加到在云模板中表达的其他限制中。

在置备期间，vRealize Automation Cloud Assembly 将这些功能与云模板中的限制（也表示为标记）相匹配，以定义部署配置。这种基于标记的功能和限制功能用作 vRealize Automation Cloud Assembly 中部署配置的基础。例如，您可以使用标记使基础架构仅在特定区域的 PCI 资源上可用。



从辅助角度来看，标记还有助于搜索和识别存储和网络项目以及其他基础架构资源。

例如，假设您正在设置云区域，并且有许多可用的计算资源。如果您正确标记了计算资源，那么您可以使用“云区域”页面的“计算”选项卡上的搜索功能筛选与该特定云区域关联的资源。

此外，“管理标记”页面和资源配置页面中包含的搜索功能可用于按标记名称查找项目。为这些项目使用逻辑和人工可读标记是方便执行此搜索和识别功能的关键。

观看以下 Youtube 视频，了解有关使用标记的详细信息以及示例：<https://youtu.be/4zNQ33RyQio>

## 外部标记

vRealize Automation Cloud Assembly 也可能包含外部标记。这些标记是通过与 vRealize Automation Cloud Assembly 实例关联的云帐户自动导入的。这些标记可能是从 vSphere、AWS、Azure 或其他外部软件产品导入的。导入后，这些标记可与用户创建的标记相同的方式使用。

## 管理标记

您可以使用 vRealize Automation Cloud Assembly 中的“管理标记”页面来监控和管理标记库。您也可以在此页面上创建标记。此外，“管理标记”页面是唯一可以查看和标识外部标记的页面。



## 标记策略

为了最大程度地减少混淆，在 vRealize Automation Cloud Assembly 中创建标记之前，请设计适当的标记策略和标记约定，以便创建和使用标记的所有用户了解其含义以及使用方法。请参见[创建标记策略](#)。

## 创建标记策略

必须根据组织的 IT 结构和目标精心规划并实施相应的标记策略，以最大程度提高 Cloud Assembly 的功能并最大程度减少混淆。

虽然标记有几个常见的作用，但您的标记策略必须适合您的部署需求、结构和目标。

## 标记的最佳做法

有效标记策略的一些常规特征：

- 设计并实施与业务结构相关的标记的统一策略，并将此计划传达给所有适用的用户。策略必须支持您的部署需求，使用清晰的人工可读语言，并且所有适用的用户均可理解。
- 对标记使用简单、明确和有意义的名称和值。例如，存储和网络项的标记名称应该是清晰和连贯的，使用户能够轻松了解他们为已部署的资源选择或检查什么样的标记分配。
- 尽管可以使用不含值的名称创建标记，但最佳做法是为每个标记名称创建适用的值，这种做法更为合适，因为其他用户能够更清楚地了解标记的使用情况。
- 避免创建重复或无关的标记。例如，仅在与存储问题相关的存储项上创建标记。

## 标记实施

绘制基本标记策略的主要注意事项。以下列表显示了在映射策略时需要考虑的典型注意事项。请注意，这些注意事项具有代表性，但并不是最终确定的。您可能具有与用例高度相关的其他注意事项。特定策略必须适合特定用例。

- 您将部署到多少个不同的环境。通常，您将创建标记来表示每个环境。
- 计算资源是如何构造并用于支持部署的。
- 您将部署到多少个不同的区域或位置。通常，您将在配置文件级别创建标记来表示每个不同的区域或位置。
- 有多少种不同的存储选项可用于部署，您希望如何描述它们的特征。这些选项应该用标记来表示。
- 对网络连接选项进行分类并创建标记以包含所有适用的选项。

- 典型的部署变量。例如，您将部署到多少个不同的环境。通常情况下，许多组织至少具有测试、开发和生产环境。您想要创建和协调匹配的限制标记和云区域功能标记，以便轻松为一个或多个此类环境设置部署。
- 协调网络 and 存储资源上的标记，以便在使用这些标记的网络和存储配置文件环境中具有逻辑意义。资源标记可以对资源部署进行更为精细的控制。
- 将云区域和网络配置文件功能标记以及其他功能标记与限制标记进行协调。通常情况下，管理员将首先为云区域和网络配置文件创建功能标记，然后其他用户可以进行具有与这些功能标记匹配的限制的设

计。

了解组织的重要注意事项之后，您可以规划适当的标记名称，以符合逻辑的方式处理这些注意事项。然后，创建策略大纲并将其提供给所有拥有创建或编辑标记特权的用户。

在开始此过程时，可以单独标记所有计算基础架构资源，这是一种有用的实施方法。如下所述，对与特定资源相关的标记名称使用逻辑类别。例如，可以将存储资源标记为 tier1、tier2 等。此外，还可以根据其操作系统（如 Windows、Linux 等）对计算资源进行标记。

标记资源之后，可以考虑采用最适合您需求的方法来为云区域和存储和网络配置文件创建标记。

## 在 vRealize Automation Cloud Assembly 中使用功能标记

在 vRealize Automation Cloud Assembly 中，可以使用功能标记为基础架构组件定义部署功能。它们与限制一起，作为 vRealize Automation 中布置逻辑的基础。

您可以在计算资源、云区域、映像和映像映射以及网络和网络配置文件上创建功能标记。用于创建这些资源的页面包含用于创建功能标记的选项。或者，也可以使用 vRealize Automation Cloud Assembly 中的“标记管理”页面创建功能标记。云区域和网络配置文件上的功能标记会影响这些区域或配置文件中的所有资源。存储或网络组件上的功能标记仅影响应用了这些标记的组件。

通常，功能标记可能定义了计算资源的位置、网络的适配器类型或存储资源的层级等特性。此外，还可定义环境位置或类型以及任何其他业务注意事项。与总体标记策略一样，应根据业务需求以逻辑方式组织功能标记。

vRealize Automation Cloud Assembly 在部署时将云区域中的功能标记与云模板上的限制进行匹配。因此，创建和使用功能标记时，必须了解并计划创建适当的云模板限制，以便按预期进行匹配。

例如，本文中包含的教程：[在 vRealize Automation Cloud Assembly 中设置和测试多云基础架构和部署](#)中的“添加云区域”主题介绍了如何为 OurCo-AWS-US-East 和 OurCo AWS-US-West 云区域创建开发和测试标记。在该教程中，这些标记指明 OurCo-AWS-US-East 区域是一个开发环境，OurCo-AWS-US-West 区域是一个测试环境。如果在云模板中创建类似的限制标记，可以通过这些功能标记将部署定向到所需的环境。

## 在 vRealize Automation Cloud Assembly 中使用限制标记

使用添加到项目和云模板的标记与基础架构资源、配置文件和云区域上的功能标记匹配时，这些标记用作限制标记。对于云模板，vRealize Automation Cloud Assembly 使用此匹配功能为部署分配资源。

在 vRealize Automation Cloud Assembly 中，可以通过两种主要方式使用限制标记。第一种方式是在配置项目和映像时。可以使用标记作为限制将资源与项目或映像相关联。第二种方式是在使用指定为限制的标记为部署选择资源的云模板中。通过这两种方式应用的限制在云模板中合并，形成了一组部署要求，从而定义了可用于部署的资源。

### 限制标记在项目中如何工作

配置 vRealize Automation Cloud Assembly 资源时，云管理员可以在项目上应用限制标记。这样，管理员可以直接在项目级别应用监管限制。在此级别添加的所有限制都将应用于为适用项目请求的每个云模板，并且这些限制标记优先于其他标记。

如果项目中的限制标记与云模板中的限制标记冲突，将优先应用项目标记，从而云管理员可以实施监管规则。例如，如果云管理员在项目中创建 `location:london` 标记，而开发人员在云模板中放置 `location:boston` 标记，将优先应用前一个标记，并且资源会部署到包含 `location:london` 标记的基础架构。

最多可以在项目中应用三项限制。项目限制可为硬性或软性。默认情况下，项目限制为硬性。使用硬性限制可以严格执行部署限制。如果不满足一项或多项硬性限制，部署将失败。软性限制提供了一种方法用于表示将选择的首选项（如果可用），但在不满足软性限制时，部署不会失败。

### 限制标记在云模板中如何工作

在云模板中，您可以将限制标记作为 YAML 代码添加到资源，以与云管理员在资源、云区域以及存储配置文件和网络配置文件中创建的相应功能标记匹配。此外，还有其他更复杂的选项可用于实施限制标记。例如，您可以使用变量在请求中填充一个或多个标记。这使您可以在请求时指定一个或多个标记。

使用 `tag` 标签在云模板 YAML 代码中的限制标题下创建限制标记。项目中的限制标记将添加到云模板中创建的限制标记。

vRealize Automation Cloud Assembly 支持简单字符串格式设置，以使在 YAML 文件中使用限制变得更容易：

```
[!]tag_key[:tag_value][:hard|:soft]
```

默认情况下，vRealize Automation Cloud Assembly 将创建具有硬性执行的明确限制。在应用程序的剩余部分，标记值为可选，但建议提供标记值。

以下 WordPressWithMySQL 示例显示了 YAML 限制标记，这些标记表示计算资源的特定位置信息。

```
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 ...

```

有关如何使用云模板的详细信息，请参见第 3 部分：[设计并部署示例 vRealize Automation Cloud Assembly 模板](#)。

## 硬性限制和软性限制在项目以及云模板中如何工作

项目和云模板中的限制都可为硬性或软性。上述代码片段显示了硬性限制和软性限制的示例。默认情况下，所有限制均为硬性。使用硬性限制可以严格执行部署限制。如果不满足一项或多项硬性限制，部署将失败。软性限制用于表示将应用的首选项（如果可用），但如果不能满足软性限制，部署不会失败。

如果有一系列硬性限制和软性限制针对特定资源类型，则软性限制还可以用作 **Tie Breaker**。也就是说，如果多个资源满足硬性限制，则使用软性限制来选择在部署中使用的实际资源。

例如，最多可以采用网络项、存储项和可扩展性项的任意组合在项目中指定三项限制。此外，还可以选择每项限制为硬性还是软性。假设您创建具有 `location:boston` 标记的硬性存储限制。如果项目中的所有存储均不满足该限制，则任何相关的部署都将失败。

## 标准标记

vRealize Automation Cloud Assembly 对部分部署应用标准标记，以支持对已部署的资源进行分析、监控和分组。

标准标记在 vRealize Automation Cloud Assembly 中具有唯一性。与其他标记不同，用户在配置部署的过程中不使用标准标记，并且不应用任何限制。这些标记会在置备期间自动应用到 **AWS**、**Azure** 和 **vSphere** 部署。这些标记存储为系统自定义属性，并且会在置备之后添加到部署中。

下面显示了标准标记的列表。

**表 4-1. 标准标记**

说明	标记
组织	<code>org: orgID</code>
项目	<code>project: projectID</code>
请求者	<code>requester: username</code>
部署	<code>deployment: deploymentID</code>
云模板参考（如果适用）	<code>blueprint: blueprintID</code>
蓝图中的组件名称	<code>blueprintResourceName: CloudMachine_1</code>

表 4-1. 标准标记 （续）

说明	标记
布置限制：在蓝图或请求参数中应用，或者通过 IT 策略应用	<code>constraints: key:value:soft</code>
云帐户	<code>cloudAccount: accountID</code>
区域或配置文件，如果适用	<code>zone: zoneID、networkProfile: profileID、storageProfile: profileID</code>

## vRealize Automation Cloud Assembly 如何处理标记

在 vRealize Automation Cloud Assembly 中，标记表示能力和限制，这些能力和限制决定置备过程中如何将资源分配给置备的部署以及分配到何处。

vRealize Automation Cloud Assembly 在解析标记时使用特定的操作顺序和层次结构来创建置备的部署。了解此过程的基础知识有助于高效地实施标记以创建可预测的部署。

以下列表总结了 Cloud Assembly 用于解析标记和定义部署的高级别操作和顺序：

- 云区域按多个标准进行筛选，包括可用性和配置文件；区域所属地区的配置文件中的标记将在此时进行匹配。
- 区域能力标记和计算能力标记用于按硬性限制筛选其余云区域。
- 在筛选的区域中，将按优先级选择云区域。如果多个云区域具有相同优先级，则通过使用云区域能力和计算能力的组合匹配软性限制来对这些云区域进行排序。
- 选择云区域后，将通过匹配一系列筛选器（包括云模板中表示的硬性限制和软性限制）来选择主机。

## 如何设置简单的标记结构

本主题介绍逻辑 vRealize Automation Cloud Assembly 标记策略的基本方法和选项。您可以使用这些示例作为实际部署的起点，也可以计划更符合需求的不同策略。

通常，云管理员是负责创建和维护标记的主要人员。

本主题引用 vRealize Automation Cloud Assembly 文档中其他主题所述的 WordPress 用例来说明如何向某些关键项目添加标记。本主题还介绍 WordPress 用例中显示的标记示例的可能替代方法和扩展。

有关 WordPress 用例的详细信息，请参见[教程：在 vRealize Automation Cloud Assembly 中设置和测试多云基础架构和部署](#)。

WordPress 用例介绍如何在云区域以及存储配置文件和网络配置文件上放置标记。这些配置文件类似于有组织的资源包。在配置文件上放置的标记应用于该配置文件中的所有项目。还可以创建标记并将其放置在存储资源和各个网络项目以及计算资源上，但这些标记仅应用于其放置到的特定资源。设置标记时，最佳做法通常是从标记计算资源开始并在以后再向配置文件和云区域添加标记。此外，还可以使用这些标记来筛选云区域的计算资源列表。

例如，虽然可以如此用例中所示在存储配置文件上放置标记，但也可以在各个存储策略、数据存储和存储帐户上放置标记。借助这些资源上的标记，可以对存储资源的部署方式进行更精细控制。在为准备部署进行的处理过程中，这些标记将作为配置文件标记后的下一个级别进行处理。



例如，您可以通过网络配置文件上放置标记 `region: eastern` 来配置典型客户场景。此标记将应用于该配置文件中的所有资源。然后可以在配置文件中的 `pci` 网络资源上放置标记 `networktype:pci`。具有东部和 `pci` 限制的云模板将创建对东部地区使用此 `pci` 网络的部署。

## 步骤

### 1 以符合逻辑的适当方式标记计算基础架构资源。

必须以符合逻辑的方式标记计算资源，这点特别重要，以便可以在“创建云区域”页面的“计算”选项卡中使用搜索功能来查找计算资源。使用此搜索功能，可以快速筛选与云区域关联的计算资源。如果在配置文件级别标记存储和网络，可能不需要标记各个存储资源和网络资源。

- a 选择**资源 > 计算**，以查看已为 vRealize Automation Cloud Assembly 实例导入的计算资源。
- b 根据需要选择每个计算资源并单击**标记**，以向资源添加标记。如果需要，可以向每个资源添加多个标记。
- c 根据需要对存储资源和网络资源重复上一步。

### 2 创建云区域能力标记和网络配置文件能力标记。

可以为云区域和网络配置文件使用相同的标记，也可以为每个项目创建唯一的标记（如果这对您的实现更有意义）。

对于网络配置文件，可以在整个配置文件上放置标记，也可以在配置文件中的子网上放置标记。在配置文件级别应用的标记将应用于该配置文件中的所有组件，例如子网。子网上的标记仅应用于其放置到的特定子网。在处理标记的过程中，配置文件级别标记的优先级高于子网级别标记。

在此示例中，我们创建三个简单标记，这些标记在 vRealize Automation Cloud Assembly 云区域标记和网络配置文件标记的用例文档中通篇出现。这些标记标识配置文件组件的环境。

- `zone:test`
- `zone:dev`
- `zone:prod`

### 3 为存储组件创建存储配置文件标记。

通常，存储标记标识存储项目的性能级别（例如，第 1 层或第 2 层），或者标识存储项目的特性（例如 `pci`）。

有关向存储配置文件添加标记的信息，请参见 [6. 添加存储配置文件](#)。

- `usage:general`
- `usage:fast`

## 结果

创建基本标记结构后，可以开始使用该标记结构，并根据需要添加或编辑标记以优化并扩展标记功能。



## 如何使用 vRealize Automation 中的资源

云管理员可以复查通过数据收集公开的 vRealize Automation 资源。

云管理员可以使用功能标记对资源进行标记，以影响 vRealize Automation 云模板的部署位置。

### vRealize Automation 中的计算资源

云管理员可以查看通过数据收集公开的计算资源。

在 vRealize Automation 中进行置备期间，云管理员可以选择直接将标记应用到资源，以标记适用于相应用途的功能。

### vRealize Automation 中的网络资源

在 vRealize Automation 中，云管理员可以查看和编辑已从映射到项目的云帐户和集成中收集数据的网络资源。

将云帐户添加到 vRealize Automation Cloud Assembly 基础架构（例如，通过使用[基础架构 > 连接 > 云帐户](#)菜单序列添加）后，数据收集会发现该云帐户的网络和安全性信息。然后，可以在网络、网络配置文件和其他定义中使用该信息。

网络是可用网络域或传输区域的特定于 IP 的组件。如果您是 Amazon Web Services 或 Microsoft Azure 用户，请将网络视为子网。

可以使用[基础架构 > 资源 > 网络](#)页面显示有关项目中网络的信息。

vRealize Automation Cloud Assembly [网络](#)页面包含如下信息：

- 在您的云帐户（例如，在 vCenter、NSX-V 或 Amazon Web Services 中）网络域外部定义的网络和负载均衡器。
- 由云管理员部署的网络和负载均衡器。
- 由云管理员定义或修改的 IP 范围和其他网络特性。
- 提供商特定外部 IPAM 集成中特定地址空间的外部 IPAM 提供程序 IP 范围。

有关网络的详细信息，请参见以下信息、[网络](#)页面上各种设置的标志帮助以及[了解有关 vRealize Automation 中的网络配置文件的更多信息](#)。

### 网络

您可以查看和编辑网络及其特性，例如添加标记或移除对公共 IP 访问的支持。也可以管理网络设置，如 DNS、CIDR、网关和标记值。此外，还可以在网络中定义新的 IP 范围并管理现有的 IP 范围。

对于现有网络，您可以通过选中网络的复选框并选择[管理 IP 范围](#)或[标记](#)来更改 IP 范围和标记设置。否则，您可以选择网络本身以编辑其信息。

标记提供了一种将相应网络（或网络配置文件）与云模板中的网络组件相匹配的方法。网络标记将应用到该网络的每个实例，而不管网络可能驻留在哪个网络配置文件中。网络可以实例化到任意数量的网络配置文件中。无论网络配置文件的驻留方式如何，网络标记在使用网络的任何地方都与该网络相关联。云模板与一个或多个网络配置文件相匹配后，云模板中的其他组件会出现网络标记匹配。

## IP 范围

使用 IP 范围可定义或更改组织中特定网络的起始和结束 IP 地址。可以显示和管理所列网络的 IP 范围。如果网络由外部 IPAM 提供程序管理，则可以管理与关联的 IPAM 集成点连接的 IP 范围。

单击**新建 IP 范围**可将其他 IP 范围添加到网络。可以指定**内部 IP 范围**，或者如果存在有效的可用 IPAM 集成，也可以指定**外部 IP 范围**。

不能将默认网关包含在 IP 范围内。子网 IP 范围不能包含子网网关值。

如果为特定 IPAM 提供程序使用外部 IPAM 集成，则可以使用**外部 IP 范围**，从可用的外部 IPAM 集成点选择 IP 范围。此过程在在 [vRealize Automation 中配置网络和网络配置文件](#)，以对现有网络使用外部 IPAM 的整体外部 IPAM 集成 workflows 上下文中进行了介绍。

## IP 地址

可以查看组织当前使用的 IP 地址，并显示其状态，例如 `available` 或 `allocated`。显示的 IP 地址是由 vRealize Automation 内部管理的 IP 地址或为包含外部 IPAM 提供程序集成的部署指定的 IP 地址。外部 IPAM 提供程序管理其自身的 IP 地址分配。

如果网络由 vRealize Automation 在内部进行管理，而不是由外部 IPAM 提供程序进行管理，则还可以释放 IP 地址。

使用内部 IPAM 并释放 IP 地址（例如，删除使用 IP 地址的计算机后）时，在释放地址与可重用这些地址之间有一个 30 分钟的等待时段。在此等待时段内，可以清除 DNS 缓存。之后，可以将 IP 地址分配给新的计算机。例如，可以置备与之前删除的计算机具有相同 IP 地址的计算机。

## 负载均衡器

可以管理组织中帐户/区域云帐户的可用负载均衡器的相关信息。您可以打开并显示为每个可用负载均衡器配置的设置。还可以添加和移除负载均衡器的标记。

## 网络域

网络域列表包含相关且不重叠的网络。

## vRealize Automation 中的安全资源

在 vRealize Automation Cloud Assembly 中添加云帐户后，数据收集会发现该云帐户的网络和安全性信息，并使该信息可用于网络配置文件和其他选项。

安全组和防火墙规则支持网络隔离。将从安全组收集数据，防火墙规则未收集数据。

## 安全组

使用**基础架构 > 资源 > 安全**菜单序列，可以查看在 vRealize Automation Cloud Assembly 云模板设计中创建的按需安全组以及在源应用程序（如 NSX-T 和 Amazon Web Services）中创建的现有安全组。可用安全组通过数据收集过程公开。

可以查看可用的安全组，并为选定的安全组添加或移除标记。云模板作者可以将一个或多个安全组分配给计算机网卡，以控制部署的安全性。

在云模板设计中，对于现有安全组，将安全组资源中的 `securityGroupType` 参数指定为 `existing`，对于按需安全组，将该参数指定为 `new`。

底层云帐户端点（如 NSX-V、NSX-T 或 Amazon Web Services 应用程序）中的现有安全组可供使用。在您组织的云模板设计中创建的按需安全组也已收集数据。按需安全组当前仅适用于 NSX-V 和 NSX-T。

现有安全组将在**来源**列中显示并归类为 `Discovered`。在 vRealize Automation Cloud Assembly 的云模板或网络配置文件中创建的按需安全组将在**来源**列中显示并归类为 `Managed by Cloud Assembly`。在网络配置文件中创建的按需安全组在内部分类为具有预配置防火墙规则的隔离安全组，不会作为安全组资源添加到云模板设计中。在云模板设计中创建的按需安全组，以及可以包含快速防火墙规则的按需安全组，将作为分类为 `new` 的安全组资源的一部分进行添加。

如果直接在源应用程序（例如源 NSX 应用程序）而非 vRealize Automation Cloud Assembly 中编辑现有安全组，则在 vRealize Automation Cloud Assembly 中不会显示更新，直到运行数据收集并在 vRealize Automation Cloud Assembly 中对关联的云帐户或集成点收集数据。数据收集每隔 10 分钟自动运行一次。

云管理员可以将一个或多个标记分配给现有安全组，以便能够在云模板中使用该安全组。云模板作者可以使用云模板设计中的 `Cloud.SecurityGroup` 资源，通过使用标记限制来分配现有安全组。现有安全组要求在云模板设计的安全资源中至少指定一个限制标记。

## 在安全组中使用防火墙规则

可以直接在云模板设计代码的安全组资源中为 NSX-V 和 NSX-T 的按需安全组创建防火墙规则。

**应用对象**列不包含由 NSX 分布式防火墙 (DFW) 分类或管理的安全组。适用于应用程序的防火墙规则适用于东西向 DFW 流量。

某些防火墙规则只能在源应用程序中进行管理，无法在 vRealize Automation Cloud Assembly 中进行编辑。例如，在 NSX-T 中管理以太网、紧急情况、基础架构和环境规则。

## 了解更多

有关在网络配置文件中安全组的详细信息，请参见[了解有关 vRealize Automation 中的网络配置文件的更多信息](#)。

有关定义防火墙规则的信息，请参见在 vRealize Automation Cloud Assembly 的网络配置文件中云模板设计中使用安全组设置和在 vRealize Automation 云模板中使用安全组资源。

有关包含安全组的云模板设计代码示例，请参见[vRealize Automation 云模板中的网络、安全性和负载均衡器示例](#)。

## vRealize Automation 中的存储资源

云管理员可以使用存储资源及其功能，这些资源和功能是通过关联的云帐户进行 vRealize Automation 数据收集发现的。

存储资源功能通过通常源自源云帐户的标记公开。通过使用 vRealize Automation Cloud Assembly，云管理员可以选择将其他标记直接应用到存储资源。在置备时，附加标记可能会为匹配目的标记特定功能。

vRealize Automation 支持标准磁盘和第一类磁盘功能。第一类磁盘仅适用于 vSphere。

- 在 vRealize Automation 中可以对标准磁盘存储执行哪些操作
- 在 vRealize Automation 中可以对第一类磁盘存储执行哪些操作

存储资源的功能会在 vRealize Automation Cloud Assembly 存储配置文件的定义中可见。请参见[了解有关 vRealize Automation 中的存储配置文件的更多信息](#)。

已进行数据收集的第一类磁盘显示在[卷资源](#)页面上。请参见 [vRealize Automation 中的卷资源](#)。

## vRealize Automation 中的计算机资源

在 vRealize Automation 中，所有用户都可以查看通过数据收集公开的计算机资源。

项目中的所有计算机都将列出。可以仅列出您的计算机，也可以通过指定筛选器来控制列出计算机的显示。

与项目中的云帐户关联的未受管计算机将与受管计算机一样显示在此列表中。“来源”列指示计算机状态。

- 已发现 - 尚未载入的计算机。
- 已部署 - 已从 vRealize Automation 载入或置备的计算机，这些计算机视为受管计算机。

您可以使用工作负载载入计划将未受管计算机引入 vRealize Automation 管理。

已断开连接的计算机网卡不会列出，因为 vRealize Automation 需要存在网络交换机或子网信息才能枚举以太网卡。例如，如果从部署中移除了计算机网卡，则不会列出该网卡。

有关使用载入计划将未受管计算机引入 vRealize Automation 管理的消息，请参见 [vRealize Automation Cloud Assembly 中的载入计划是什么](#)。

## vRealize Automation 中的卷资源

在 vRealize Automation 中，所有用户都可以查看卷资源。

vRealize Automation Cloud Assembly 显示两个来源的卷或逻辑驱动器：

- 通过源云帐户数据收集发现的卷
- 与由 vRealize Automation Cloud Assembly 置备的工作负载关联的卷

您可以根据卷或逻辑驱动器查看容量和功能。该列表还会公开源自源云帐户的功能标记或添加到 vRealize Automation Cloud Assembly 本身中的功能标记。此外，还会指明卷作为第一类磁盘的状态。有关第一类磁盘存储卷的信息，请参见在 [vRealize Automation 中可以对第一类磁盘存储执行哪些操作](#)。

## 了解有关 vRealize Automation Cloud Assembly 中的资源的更多信息

vRealize Automation Cloud Assembly 可以公开有关数据收集资源的其他信息，例如定价卡。

## vRealize Automation 中数据收集的工作原理

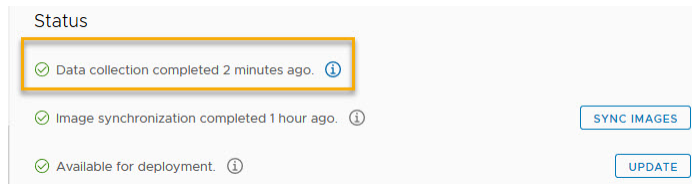
执行初步数据收集后，将每隔 10 分钟自动执行一次资源数据收集。数据收集时间间隔不可配置，且无法手动启动数据收集。

您可以在现有云帐户页面的“状态”部分中发现有关该云帐户的资源数据收集和映像同步的信息。方法是：选择**基础架构 > 连接 > 云帐户**，然后在所选的现有云帐户上单击**打开**。

您可以打开现有的云帐户，并在其页面的**状态**部分中查看其关联的端点版本。如果关联的端点已升级，则会在数据收集期间发现新的端点版本，并反映在云帐户页面的**状态**部分中。

### 资源数据收集

数据收集每隔 10 分钟执行一次。每个云帐户都会显示其数据收集上次完成的时间。

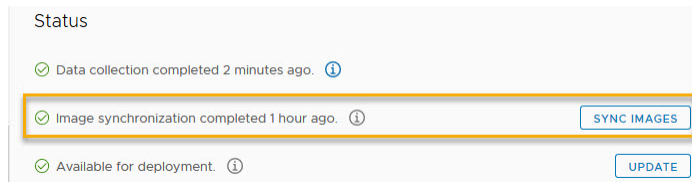


### 映像数据收集

映像同步每隔 24 小时执行一次。您可以为某些云帐户类型启动映像同步。要启动映像同步，请打开云帐户（**基础架构 > 云帐户**，然后选择并打开现有云帐户），然后单击**同步映像**按钮。没有用于 NSX 云帐户的映像同步选项。

**注** 映像在内部分类为公共映像或专用映像。公共映像是共享的，不特定于特定的云订阅或组织。专用映像不进行共享，并且特定于特定订阅。公共映像和专用映像每 24 小时自动同步一次。通过云帐户页面上的选项，您可以触发专用映像的同步。

云帐户页面将显示映像同步的上次完成时间。



为了促进部署中的容错能力和高可用性，每个 NSX-T 数据中心端点都代表由 3 个 NSX Manager 构成的集群。有关相关信息，请参见在 [vRealize Automation 中创建 NSX-T 云帐户](#)。

### 云帐户和载入计划

创建云帐户时，将对与该云帐户关联的所有计算机收集数据，然后在**基础架构 > 资源 > 计算机**页面中显示这些计算机。如果云帐户包含在 vRealize Automation Cloud Assembly 外部部署的计算机，您可以使用载入计划允许 vRealize Automation Cloud Assembly 管理计算机部署。

有关添加云帐户的信息，请参见[将云帐户添加到 vRealize Automation Cloud Assembly](#)。

有关载入非受管计算机的信息，请参见 [vRealize Automation Cloud Assembly 中的载入计划是什么](#)。

## 在 vRealize Automation 中可以对标准磁盘存储执行哪些操作

标准磁盘可以是永久磁盘，也可以是非永久磁盘。

vRealize Automation 支持两类存储 - 标准磁盘和第一类磁盘。第一类磁盘仅适用于 vSphere。

### ■ vSphere

vSphere 支持从属（默认）、独立永久和独立非永久标准磁盘。有关相关信息，请参见在 [vRealize Automation 中可以对永久磁盘存储执行哪些操作](#)。

删除虚拟机时，也会删除其从属和独立非永久磁盘。

删除虚拟机时，不会删除其独立永久磁盘。

可以创建从属和独立非永久磁盘的快照。无法创建独立永久磁盘的快照。

### ■ Amazon Web Services (AWS) EBS

可以将 EBS 卷附加到 AWS 计算实例，也可以将 EBS 卷与 AWS 计算实例分离。

删除虚拟机时，将分离其附加的 EBS 卷，但不会删除。

### ■ Microsoft Azure VHD

连接磁盘始终是永久磁盘。

删除虚拟机时，可以指定是否移除其附加的存储磁盘。

### ■ Google Cloud Platform (GCP)

连接磁盘始终是永久磁盘。

永久磁盘独立于虚拟机实例，因此，即使在删除实例之后，也可以分离或移动永久磁盘以保留数据。

删除虚拟机时，将分离其连接的磁盘，但不会删除。

有关相关信息，请参见 [了解有关 vRealize Automation 中的存储配置文件的更多信息](#)。

## 在 vRealize Automation 中可以对第一类磁盘存储执行哪些操作

第一类磁盘 (FCD) 在虚拟磁盘上以磁盘即服务或 EBS 类似的磁盘存储形式提供存储生命周期管理，以便您可以独立于 vSphere 虚拟机创建和管理磁盘。

vRealize Automation 支持两类存储磁盘 - 标准磁盘和第一类磁盘。仅 vSphere 支持第一类磁盘功能。vRealize Automation 当前将第一类磁盘功能作为仅 API 功能提供。

第一类磁盘具有自己的生命周期管理功能，可独立于虚拟机运行。第一类磁盘与独立永久磁盘的一项不同之处在于，可以使用第一类磁盘独立于虚拟机创建和管理快照。

可以创建新的 vRealize Automation 存储配置文件，以支持第一类磁盘功能或标准磁盘功能。请参见 [了解有关 vRealize Automation 中的存储配置文件的更多信息](#) 和 [vRealize Automation 中的存储资源](#)。

此外，还可以在 vRealize Automation 云模板和部署中添加 `Cloud.vSphere.Disk` 第一类磁盘元素，以支持 vSphere 第一类磁盘。已进行数据收集的第一类磁盘显示在 [卷资源](#) 页面上。请参见 [vRealize Automation 中的卷资源](#)。

在 vCenter 中，第一类磁盘也称为“增强型虚拟磁盘 (IVD)”或“受管虚拟磁盘”。



## 功能

使用 vRealize Automation API 功能，您可以：

- 创建、列出和删除第一类磁盘。
- 调整第一类磁盘的大小。
- 连接和分离第一类磁盘。
- 创建和管理第一类磁盘快照。
- 将现有标准磁盘转换为第一类磁盘

有关通过使用 vRealize Automation API 创建和管理第一类磁盘 (FCD) 存储的相关 API 信息，包括如何定义存储配置文件以使用第一类磁盘功能，请参见[什么是 vRealize Automation Cloud API 以及如何使用](#)（网址为 [code.vmware.com](https://code.vmware.com)）或从以下位置导航：

- 有关 FCD 的 API 文档，请参见《[Virtual Disk Development Kit 编程指南](#)》中的“[第一类磁盘 \(FCD\)](#)”部分。
- 有关 vRealize Automation 中 FCD 的 API 用例文档的链接，请参见与您的 vRealize Automation 版本相对应的 [vRealize Automation API 文档](#)页面。

## 注意事项和限制

第一类磁盘注意事项和限制当前包括：

- 第一类磁盘仅适用于 vSphere 虚拟机。
- 要使用第一类磁盘，需要 vSphere 6.7 Update 2 或更高版本。
- 不支持在数据存储集群上置备第一类磁盘。
- 第一类磁盘不支持卷多重附加。
- 无法调整具有快照的第一类磁盘的大小。
- 无法删除具有快照的第一类磁盘。
- 第一类磁盘快照层次结构只能使用 `createdAt` API 选项进行构建。
- 连接第一类磁盘所需的最低虚拟机硬件版本为 vmx-13（与 ESX 6.5 兼容）。

## 在 vRealize Automation 中可以对永久磁盘存储执行哪些操作

永久磁盘会保留重要数据以防止意外删除。

在云模板中的某个卷下，您可以添加 `persistent: true` 属性，以使磁盘在 vRealize Automation Cloud Assembly 或 vRealize Automation Service Broker 删除中保留下来。在部署删除期间、实施后删除或移除磁盘操作期间，永久磁盘不会被移除。

因此，即使在执行部署删除或磁盘删除后，永久磁盘仍会保留在基础架构中。要移除永久磁盘，可以使用以下技术。

- 使用 DELETE API 将清除标记作为查询参数显式传递。
- 直接从云端点中删除它们。

请注意，没有可用于删除永久磁盘的 vRealize Automation Cloud Assembly 或 vRealize Automation Service Broker 用户界面。

## 什么是定价卡

vRealize Automation Cloud Assembly 定价卡有助于云管理员定义并分配定价策略，从而了解各个部署的货币影响，以便帮助您管理资源。

在创建或分配定价卡之前，必须先在 vRealize Operations Manager 中配置并启用定价，以便使用 vRealize Automation。对 vRealize Automation 配置 vRealize Operations Manager 时，请确保这两个应用程序都设置为同一时区。要在 vRealize Operations 中配置时区，请启用 SSH 并登录到每个 vRealize Operations Manager 节点，编辑 `$ALIVE_Base/user/conf/analytics/advanced.properties` 文件，然后添加 `timeZoneUseInMeteringCalculation = <time zone>`。

---

**注** 要在多租户环境中使用定价，您必须为每个 vRealize Automation 租户提供一个单独的 vRealize Operations Manager 实例。

---

定价卡为定价策略定义费率。然后，可以将定价策略分配给特定项目以定义总价格。创建 vRealize Operations Manager 端点后，**基础架构 > 定价卡**选项卡上将显示预定义的默认费率卡，并采用配置“成本等于价格”。可以创建仅应用于项目或云区域的定价卡。默认情况下，所有新的定价卡都应用于项目。

---

**注** 如果更改**所有定价卡均应用于**设置，则会删除所有现有定价卡分配。此外，如果从 Cloud Assembly 中删除了 vRealize Operations Manager 端点，则还会删除所有定价卡和分配。

---

经过一段时间后，部署价格在部署卡视图上显示为“月累计价格”，每月月初重置为零。部署详细信息中提供了组件成本细目。在部署级别提供此信息可告知云管理员相关信息，但它还有助于成员了解其工作可能对预算和长期开发产生的影响。

可以选择向 Cloud Assembly 和 Service Broker 中的用户显示定价信息，只需选择“显示定价信息”按钮即可。如果禁用，则会对 Cloud Assembly 和 Service Broker 用户隐藏定价信息。

## 如何计算价格

您在部署级别看到的计算资源和存储资源的初始价格基于行业标准基准费率，然后根据时间计算。将费率应用于主机，服务会计算 CPU 和内存费率。服务器每 24 小时重新计算一次价格。

新策略、分配和前期定价在下一个 vROps 数据收集周期期间定价。默认情况下，数据收集周期每 5 分钟运行一次。在项目 and 部署中更新新策略或更改可能需要长达 24 小时。

您也可以在**基础架构 > 集成 > vROps 端点 >**的“vROps 端点”页面上随时手动刷新价格服务器。在 vCenter Server 部分中，单击**同步**。使用**同步**选项手动刷新价格服务器时，将为组织中的所有项目重新计算价格。根据您的组织有多少个项目，此过程可能会耗费大量资源，并且需要一些时间。

有关所支持资源的列表，请参见 [vRealize Automation Cloud Assembly 中的计费组件类型列表](#)。



## vRealize Automation Cloud Assembly 中的计费组件类型列表

vRealize Automation Cloud Assembly 提供了以下蓝图组件类型的基准成本信息。

表 4-2. 计费组件类型

蓝图组件类型	服务名称/对象类型	蓝图资源类型	注释
云不可知	计算机	Cloud.Machine	如果为不可知计算机配置了 vSphere，则可以查看部署成本。
	磁盘	Cloud.Volume	如果将不可知磁盘连接到配置了 vSphere 的虚拟机，则可以查看部署成本。
vSphere	vSphere 计算机	Cloud.vSphere.Machine	使用特定于云的蓝图进行部署。
	vSphere 磁盘	Cloud.vSphere.Disk	使用连接到虚拟机的云特定蓝图进行部署。
VMware 托管云 (VMC)	vSphere 计算机	Cloud.vSphere.Machine	VMC 仅支持基于费率的定价卡（不支持基于成本的定价卡）。
	vSphere 磁盘	Cloud.vSphere.Disk	

## 如何在 Cloud Assembly 中创建定价卡

可以创建定价卡并将其分配给项目或云区域，具体取决于云管理员确定的定价策略。

定价卡可根据用户选择的参数进行自定义。配置定价卡后，可以将其分配给由定价策略确定的一个或多个项目和云区域。

### 前提条件

在创建或分配定价卡之前，必须先在 vRealize Operations 中配置并启用定价以及配置货币，以便使用 vRealize Automation。对 vRealize Operations 配置 vRealize Automation 时，请确保这两个应用程序都设置为同一时区。要在 vRealize Operations 中配置时区，请启用 SSH 并登录到每个 vRealize Operations 节点，编辑 \$ALIVE\_Base/user/conf/analytics/advanced.properties 文件，然后添加 `timeZoneUseInMeteringCalculation = <time zone>`。

您必须先配置 vRealize Operations 端点，然后才能配置定价卡。要配置 vRealize Operations 端点，请导航到 **基础架构 > 连接 > 集成 > 添加集成**。

**注** 添加多个 vRealize Operations 端点时，这些端点不能监控同一个 vCenter。

### 步骤

- 1 导航到 **基础架构 > 定价卡 > 新建定价卡**。
- 2 在“摘要”选项卡中，输入定价卡的名称和描述。在“定价”选项卡上定义策略后，“概览”表将填充定价卡费率。

**注** 货币单位由在 vRealize Operations 中选择的值确定。

- 3 可选。选中 **未分配项目的默认值?** 复选框，默认将此定价卡分配给所有未分配的项目。

#### 4 单击定价，并配置定价策略的详细信息。

表 4-3. 定价策略配置

参数	说明
基本费用	<p>输入策略的名称和描述。选择基于成本还是基于费率。</p> <ul style="list-style-type: none"> <li>■ 成本 - 成本在 vRealize Operations 中进行定义。如果选择此选项，则需要输入乘法系数。例如，如果选择 1.1 作为系数，则成本将乘以 1.1，这样计算成本将增加 10%。使用成本的价格公式为：&lt;成本&gt; x &lt;乘法系数&gt; = 价格</li> <li>■ 费率 - 如果选择此选项，则必须使用绝对值确定成本。使用费率的价格公式为：&lt;费率&gt; = 价格。从下拉列表中选择费率时间间隔，以指定如何对此费率收费。</li> </ul> <p>在“基本费用”部分中，可以为 CPU、内存、存储和其他杂项成本定义成本或费率。</p>
客户机操作系统	<p>可以通过单击<b>添加费用</b>定义客户机操作系统费用。</p> <p>输入客户机操作系统名称，并定义计费方法和基本费率。</p> <ul style="list-style-type: none"> <li>■ 重复 - 输入基本费率并将重复时间间隔定义为费用周期。需要输入绝对费率值，并加到价格总计中。</li> <li>■ 一次性 - 定义一次性基本费率费用。需要输入绝对值，并添加为一次价格。</li> <li>■ 费率系数 - 需要输入应用于所选费用类别的乘法系数。例如，如果选择“CPU 费用”且费率系数为 2，则客户机操作系统 CPU 按标准成本值的 2 倍进行计费。</li> </ul> <p>可以通过单击<b>添加费用</b>并配置其他费用策略来添加多个具有不同费率的客户机操作系统。</p> <p><b>注</b> 客户机操作系统的前期费用不会显示在“摘要”页面上，即使属于策略的一部分也不会显示。</p>
标记	<p>可以通过单击<b>添加费用</b>定义标记费用。</p> <p>选择标记名称，并定义计费方法和基本费率。</p> <ul style="list-style-type: none"> <li>■ 重复 - 输入基本费率并将重复时间间隔定义为费用周期。需要输入绝对费率值，并加到价格总计中。</li> <li>■ 一次性 - 定义一次性基本费率费用。需要输入绝对值，并添加为一次价格。</li> <li>■ 费率系数 - 需要输入应用于所选费用类别的乘法系数。</li> </ul> <p>选择如何基于已打开电源的状态对标记计费。</p> <p>可以通过单击<b>添加费用</b>并配置其他费用策略来添加多个具有不同费率的标记。</p> <p><b>注</b> 计算出的最终价格中的其他费用包括虚拟机上的标记，不包括磁盘和网络上的标记。</p>

表 4-3. 定价策略配置（续）

参数	说明
自定义属性	<p>可以通过单击<b>添加费用</b>定义自定义属性费用。</p> <p>输入属性名称和值，并定义计费方法和基本费率。</p> <ul style="list-style-type: none"> <li>■ 重复 - 输入基本费率并将重复时间间隔定义为费用周期。需要输入绝对费率值，并加到价格总计中。</li> <li>■ 一次性 - 定义一次性基本费率费用。需要输入绝对值，并添加为一次性格。</li> <li>■ 费率系数 - 需要输入应用于所选费用类别的乘法系数。</li> </ul> <p>选择如何基于已打开电源的状态对自定义属性计费。</p> <p>可以通过单击<b>添加费用</b>并配置其他费用策略来添加多个具有不同费率的自定义属性。</p>
费用总计	定义要添加到定价策略的任何其他费用。可以添加一次性费用和重复费用。

**注** 目录项的价格估算或“摘要”选项卡不显示一次性费用。仅显示给定目录项的每日价格估算。

- 5 单击**分配**选项卡，然后单击**分配项目**。选择一个或多个要将定价卡分配给的项目。

**注** 默认情况下，定价卡应用于项目。在**基础架构 > 定价卡**选项卡上，可以选择将定价卡应用于云区域。如果选择了云区域，则将在“分配”选项卡上单击**分配云区域**。

- 6 单击**创建**以保存并创建定价策略。

## 结果




新定价策略将显示在“定价卡”页面上。要查看或编辑策略详细信息和配置，请单击**打开**。

## 如何估算部署价格

在部署目录项之前，您可以使用前期价格进行部署的价格估算。

Daily Price Estimate
×

*Guest OS and one time prices are excluded in this estimate.*

 price-service-f309c00	\$0.54
 Cloud_vSphere_Machine_1	\$0.53
Compute	\$0.39
Storage	\$0.03
Additional charges	\$0.11
 Cloud_vSphere_Disk_1	\$0.01
Storage	\$0.01

CLOSE

为进行前期价格估算，每个虚拟机的引导磁盘大小始终为 8 GB。

部署的前期价格是在部署给定目录项之前基于资源分配为该目录项得出的每日价格估算。部署目录项后，您可以在**部署和基础架构 > 项目**选项卡上以前期价格总计的形式查看月累计价格。对于私有云资源（如 vSphere 计算机和 vSphere 磁盘、Cloud Assembly 目录项及为私有云配置 vCenter 的云平台无关项），支持前期定价。

---

**注** 对于公有云资源或非 vSphere 计算机或磁盘私有云资源，不支持前期定价。

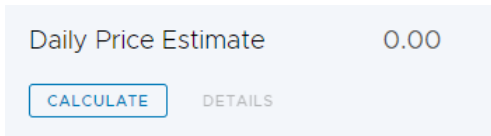
---

### 前提条件

要在 vRealize Automation Cloud Assembly 中查看价格，必须配置 vRealize Operations 集成端点：启用定价并预设货币。

### 步骤

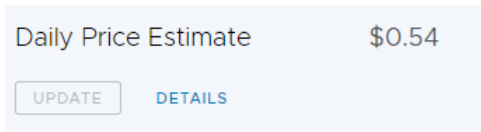
- 1 从“目录”中选择目录项，然后单击**请求**。



Daily Price Estimate 0.00

[CALCULATE](#) [DETAILS](#)

- 2 输入目录项请求的详细信息，然后单击**计算**。



Daily Price Estimate \$0.54

[UPDATE](#) [DETAILS](#)

- 3 （可选）单击**详细信息**以在“每日价格估算”窗口中查看价格细目。

### 后续步骤

如果每日价格估算可接受，请单击**提交**以继续执行部署请求。

### 如何估算所有项目的价格

作为云管理员，您可能需要估算所有项目的总价格。

为进行 showback，您可以使用项目定价卡估算所有项目的总价格。

### 步骤

- 1 在**基础架构 > 定价卡**页面上，单击**所有定价卡均应用于:**旁边的**编辑**，然后选择项目。

---

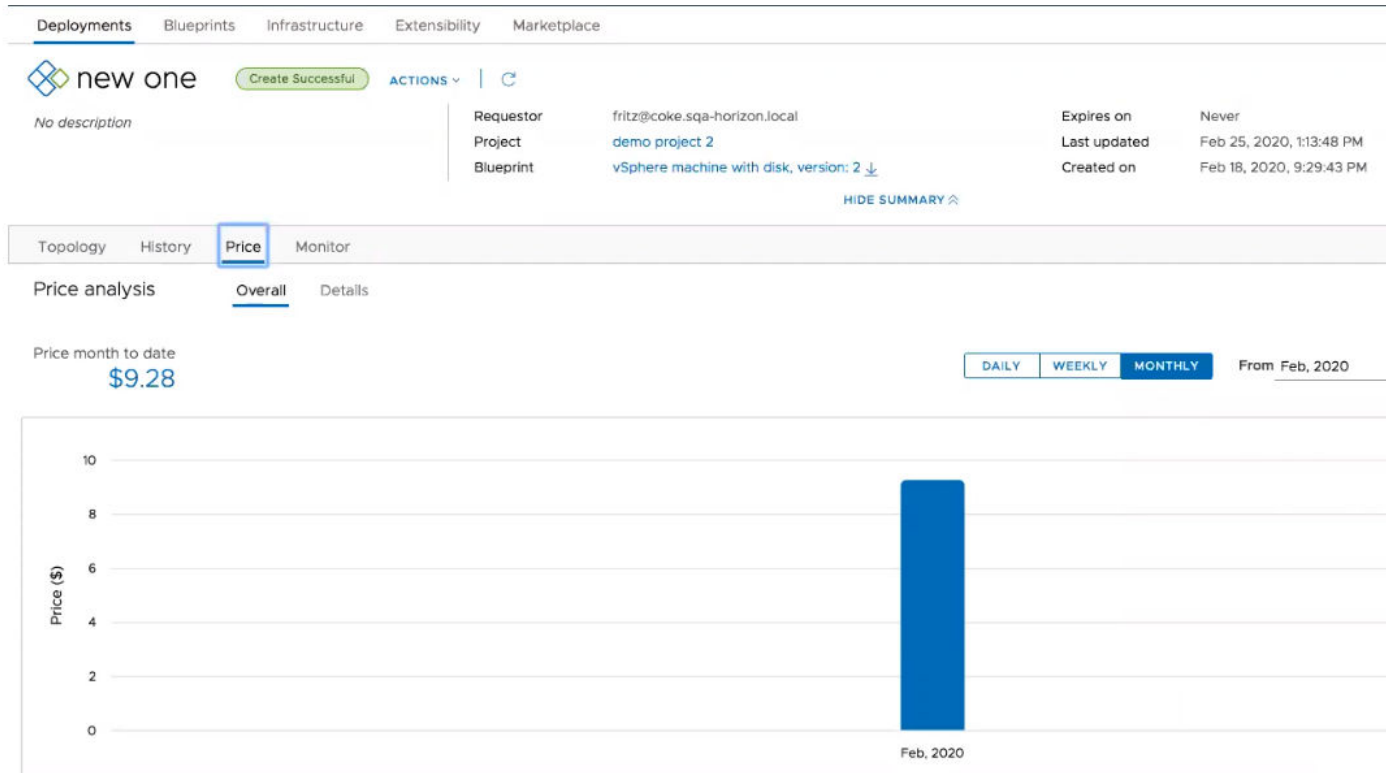
**注** 如果更改**所有定价卡均应用于**设置，则会删除所有现有定价卡分配。

---

- 2 使用基于成本的方法创建定价卡和分配。请参见**如何在 Cloud Assembly 中创建定价卡**。

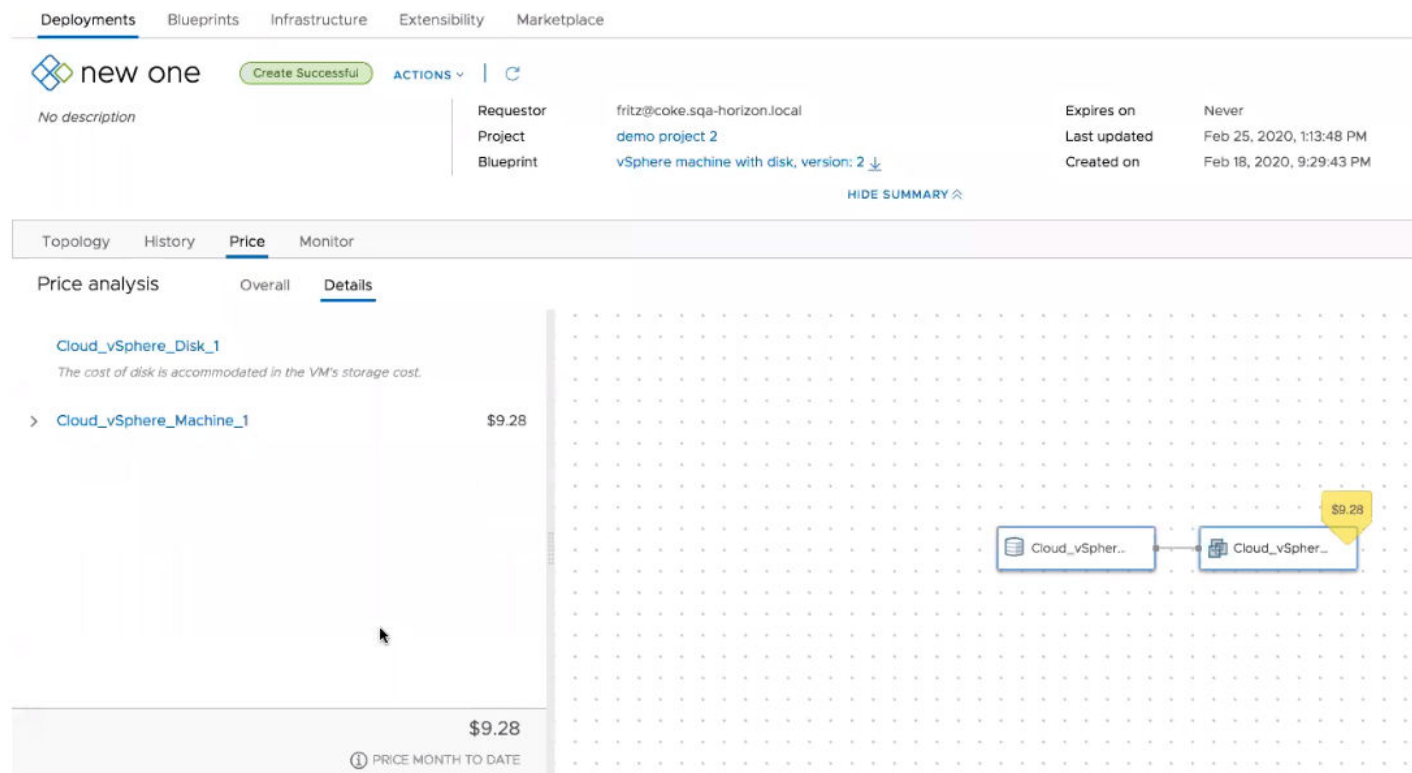
## 如何查看部署的价格历史记录

定义定价卡并将其分配给项目后，可以查看一段时间内单个部署的价格历史记录。



要查看价格历史记录，请导航到您的部署，然后单击**价格**。价格分析提供了部署价格概览和详细视图以及价格的月累计值。可以更改图形表示形式，将部署价格显示为每日、每周或每月值。此外，还可以指定价格历史记录的确切日期范围或月份。

要查看按成本构成细分的价格，请单击**详细信息**。



## 使用 vRealize Automation 配置多提供者租户资源

在多租户环境中，客户可以使用虚拟专用区域 (VPZ) 逐个租户管理资源分配。

在 vRealize Automation 8.x 中，客户可以使用 VMware Lifecycle Manager 和 Workspace ONE Access 配置多租户环境。通过这些工具，用户可以设置多租户并创建和配置租户。配置租户后，提供者管理员可以在 vRealize Automation Cloud Assembly 中创建虚拟专用区域，然后可以使用 vRealize Automation Cloud Assembly 管理租户功能将区域分配给租户。

多租户依赖于以下三个 VMware 产品的协调和配置，概述如下：

- **Workspace ONE Access**- 此产品为多租户和在租户组织内提供用户和组管理的 Active Directory 域连接提供基础架构支持。
- **vRealize Suite Lifecycle Manager**- 此产品支持为受支持的产品（如 vRealize Automation）创建和配置租户。此外，它还提供一些证书管理功能。
- **vRealize Automation**- 提供商和用户可登录到 vRealize Automation 以访问租户，并可在租户中创建和管理部署。

配置多租户时，用户应熟悉所有这三个产品及其相关文档。

有关使用 Lifecycle Manager 和 Workspace ONE Access 的详细信息，请参见[使用 VMware Identity Manager 管理用户和管理用户和组](#)。

## 如何为 vRealize Automation 创建虚拟专用区域

提供商管理员可以创建虚拟专用区域 (VPZ)，以将基础架构资源分配给多组织 vRealize Automation 环境中的租户。管理员还可以使用 VPZ 控制单个租户部署中的资源分配。

可以使用 VPZ 分配资源，例如映像、网络 and 存储资源。它们在每个租户上很像云区域，但专门设计用于多租户部署。对于任何给定项目，可以使用云区域或 VPZ，但不能同时使用两者。此外，VPZ 和租户之间也存在一对一关系。也就是说，一次只能将一个 VPZ 分配给一个租户。

创建 VPZ 时，使用或不使用 NSX 均可。如果创建区域时不使用 NSX，则 vSphere 端点上将存在 NSX 相关功能方面的限制。

- 安全性（组、防火墙）
- 网络组件 (NAT)

### 前提条件

- 使用 VMware Lifecycle Manager 和 VMware Workspace ONE Access 在 vRealize Automation 部署上启用并配置多租户。
- 根据需要为您的租户配置创建租户管理员。
- 如果要使用 NSX，您必须在提供商组织中创建适当的 NSX 云帐户。

### 步骤

#### 1 选择基础架构 > 配置 > 虚拟专用区域

“VPZ” 页面将显示所有现有区域，并允许您创建区域。

#### 2 单击新建虚拟专用区域。

页面左侧有六个选项，可用于为区域配置摘要信息和基础架构组件。

#### 3 输入新区域的“摘要”信息。

- a 添加“名称”和“描述”。
- b 选择要应用该区域的“帐户”。
- c 选择“布置策略”。

布置策略有助于为指定云区域内的部署选择主机。

- default - 在集群和主机之间随机分发计算资源。此选项在单个计算机级别工作。例如，特定部署中的所有计算机在满足要求的可用集群和主机之间随机分发。
- binpack - 将计算资源放置在负载最多但仍有足够资源运行给定计算资源的主机上。
- spread - 将部署计算资源置备到虚拟机数量最少的集群或主机。对于 vSphere，Distributed Resource Scheduler (DRS) 会在主机之间分发虚拟机。例如，部署中所有请求的计算机都放置在同一个集群上，但下一次部署可能会根据当前负载选择另一个 vSphere 集群。

#### 4 为区域选择计算资源。

根据需要为云区域添加计算资源。最初，筛选器选择是“包括所有计算资源”，下面列表中会显示所有可用的计算资源，且这些资源分配给适用区域。此外，还可以使用两个其他选项将计算资源添加到云区域。

- 手动选择计算资源 - 如果要从下面列表中手动选择计算资源，请选择此菜单项。选择计算资源后，单击“添加计算资源”以将资源添加到区域。
- 按标记动态包括计算资源 - 如果要根据标记选择要添加到区域的计算资源，请选择此菜单项。在添加适当的标记之前，将显示所有计算资源。可以在“使用这些标记包括计算资源”选项中选择或输入一个或多个标记。

对于任何一个计算资源选项，都可以通过选择右侧的框并单击“移除”来移除页面上显示的一个或多个计算资源。

#### 5 根据需要输入或选择标记。

#### 6 在左侧菜单中选择“特定实例”，然后为该区域定义一个或多个特定实例。特定实例定义了特定云帐户/区域的目标部署大小。

#### 7 在左侧菜单中选择“映像”，然后为该区域定义一个或多个映像。映像是定义可用于区域的操作系统规范的计算机模板。

#### 8 在左侧菜单中选择“存储”，然后为该区域选择存储策略和其他存储配置。

#### 9 在左侧菜单中，选择“网络”，然后定义网络和（可选）要用于此区域的网络策略。此外，还可以为所选网络策略配置负载均衡器和安全组。

网络	<ul style="list-style-type: none"> <li>■ 与此 VPZ 关联的所有现有网络都将显示在“网络”选项卡上的表中。</li> <li>■ 单击<b>添加网络</b>以查看与所选区域关联的所有网络。添加要用于此区域的网络。</li> <li>■ 选择一个网络，然后单击<b>标记</b>以将一个或多个标记添加到指定的网络。</li> <li>■ 选择<b>管理 IP 范围</b>以指定用户可通过其访问此网络的 IP 范围。</li> <li>■ （如果适用）单击“网络策略”选项卡，然后选择隔离策略。</li> </ul>
网络策略	<p>如果已配置，请选择要用于此区域的网络策略，以便为出站网络和专用网络实施隔离策略。</p> <ul style="list-style-type: none"> <li>■ 选择隔离策略（如果需要）。</li> <li>■ 选择第 0 层逻辑路由器和 Edge 集群（如果需要）。</li> </ul>
负载均衡器	单击 <b>添加负载均衡器</b> ，为帐户/区域云帐户配置负载均衡器。
安全组	单击 <b>添加安全组</b> 以使用安全组将防火墙规则应用于已置备的计算机。

#### 结果

将根据指定的资源分配创建虚拟专用区域。



## 后续步骤

云管理员可以将 VPZ 与项目相关联。

- 1 在 Cloud Assembly 中，选择**管理 > 项目**
- 2 选择“置备”选项卡。
- 3 单击**添加区域**，然后选择“添加虚拟专用区域”。
- 4 从列表中选择所需的 VPZ。
- 5 可以设置置备优先级以及实例数量、可用内存量和可用 CPU 数量方面的限制。
- 6 单击**添加**。

## 管理 vRealize Automation 租户的 VPZ 配置

提供商管理员可以在 vRealize Automation Cloud Assembly 中管理虚拟专用区域 (VPZ)，以按租户控制基础架构资源分配。使用“租户管理”页面，管理员可以查看租户和 VPZ 区域，以及为租户启用或禁用 VPZ。

默认情况下，不会将 VPZ 分配给任何租户。必须在此页面上分配 VPZ，才能将其用于租户。

初始创建时，VPZ 默认处于启用状态。已启用的 VPZ 可以进行分配，并用于指定的租户。VPZ 处于禁用状态时，无法用于置备或分配给租户。可以禁用 VPZ，但仍可分配用于租户。

当提供商管理员导航到“租户管理”页面时，该页面将显示所有可用租户，然后管理员可以选择一个租户。选择租户后，该页面将显示当前为该租户分配的 VPZ（如果有）。管理员可以使用此页面将 VPZ 分配给所选租户。

分配 VPZ 时，租户管理员可以将其添加到其项目，并可供租户用户进行置备。将 VPZ 分配给一个租户后，可以将其分配给另一个租户。

启用 VPZ 后，即可在指定的租户中使用。提供商管理员可以禁用 VPZ，以便执行维护或租户重新配置，并且可以向用户提供禁用通知。如果要使 VPZ 长期不可用于租户，则可以将其取消分配。如果出于某种原因将现有 VPZ 从租户取消分配，则无法将其用于从该租户创建部署。

## 前提条件

- 设置多租户，并根据需要为部署创建 VPZ。

## 步骤

- 1 在 vRealize Automation Cloud Assembly 中，选择“管理租户”。
- “租户管理”页面将以卡视图显示为管理员组织配置的所有租户。
- 2 单击一个租户以将其选中。
- 3 单击“基础架构管理”选项卡以查看为该租户分配的所有 VPZ
- 4 选择**分配虚拟专用区域**以打开一个对话框，其中显示了当前未分配给租户的所有区域。将区域分配给租户。
- 5 在对话框中选择一个或多个区域，然后单击**分配给租户**。

## 后续步骤

分配 VPZ 后，租户管理员可以将其分配给项目。

提供商管理员可以使用租户的卡视图监控和管理 VPZ 的状态。

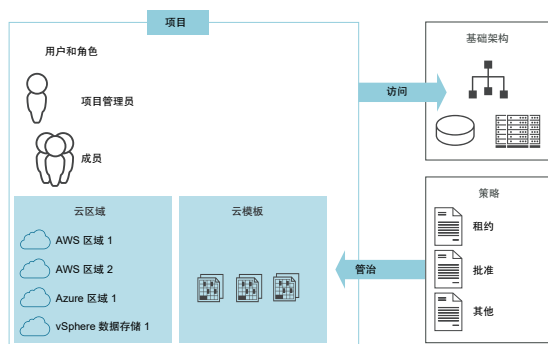
- 如果要禁用租户，请在该租户所对应的卡视图上单击**禁用**。
- 要启用租户，请在该租户所对应的卡视图上单击**启用**。
- 如果要取消分配租户，请在该租户所对应的卡视图上单击**取消分配**。

# 添加和管理 vRealize Automation Cloud Assembly 项目

## 5

项目控制哪些用户有权访问 vRealize Automation Cloud Assembly 云模板，并控制模板的部署位置。您可以使用项目来组织和管治用户可执行的操作，以及用户可在云计算基础架构中部署云模板的云区域。

云管理员设置项目，他们可以向其中添加用户和云区域。任何要创建和部署云模板的用户都必须是至少一个项目的成员。



本章讨论了以下主题：

- 如何为我的 vRealize Automation Cloud Assembly 开发团队添加项目
- 了解有关 vRealize Automation Cloud Assembly 项目的更多信息

## 如何为我的 vRealize Automation Cloud Assembly 开发团队添加项目

您可以创建一个项目，向其添加成员和云区域，以便项目成员可以将其云模板部署到关联的区域。作为 vRealize Automation Cloud Assembly 管理员，您可以为开发团队创建一个项目。然后，您可以分配项目管理员，也可以作为项目管理员进行操作。

创建云模板时，首先需要选择要与该云模板相关联的项目。该项目必须存在，您才能创建云模板。

确保您的项目满足开发团队的业务需求。

- 项目是否提供支持团队目标的资源。有关基础架构资源和项目如何支持云模板的示例，请参见 [教程：在 vRealize Automation Cloud Assembly 中设置和测试多云基础架构和部署](#)。
- 您的项目成员需要或期望其部署共享还是专用。“部署”选项卡上的所有项目成员，而不仅仅是部署成员，都可以使用共享部署。您可以随时更改部署共享状态。

当您与项目成员共享部署时，成员可以运行相同的实施后操作。要管理成员是否能够运行实施后操作，您可以在 vRealize Automation Service Broker 中创建实施后操作策略。这些策略适用于 vRealize Automation Cloud Assembly 和 vRealize Automation Service Broker 部署。

要了解有关实施后操作策略的详细信息，请参见[如何使用策略授权部署用户运行实施后操作](#)。

此过程基于创建仅包含基本配置的初始项目。当您的开发团队创建和部署云模板时，您可能要修改项目。您可以添加限制、自定义属性和其他选项，以提高部署效率。请参见[了解有关 vRealize Automation Cloud Assembly 项目的更多信息](#)中包含的文章。

### 前提条件

- 确认您配置了云区域。请参见第 4 章 [构建您的 vRealize Automation Cloud Assembly 资源基础架构](#)。
- 对于添加为此项目的云区域的区域，确认您为其配置了映射和配置文件。请参见第 4 章 [构建您的 vRealize Automation Cloud Assembly 资源基础架构](#)。
- 确认您拥有执行此任务所需的权限。请参见 [vRealize Automation 用户角色是什么](#)。
- 确定将指定为项目管理员的用户。要了解项目管理员可以在 vRealize Automation Cloud Assembly 中执行的操作，请参见 [vRealize Automation 用户角色是什么](#)。
- 如果要将 Active Directory 组添加到项目，请确认您已为组织配置了 Active Directory 组。请参见《管理 vRealize Automation》中的在 [vRealize Automation 中编辑组角色分配](#)。如果这些组未同步，则当您尝试将它们添加到项目时，这些组不可用。

### 步骤

- 1 选择**基础架构 > 管理 > 项目**，然后单击**新建项目**。
- 2 输入项目名称。
- 3 单击**用户**选项卡。
  - a 要确保项目成员执行的部署仅可供请求用户访问，请禁用**部署共享**。要确保可将部署的所有权分配给项目的其他成员，请确认已启用**部署共享**。
  - b 添加具有已分配角色的用户。
- 4 单击**置备**选项卡，然后添加一个或多个云区域。

添加任何包含支持项目用户所部署云模板的资源的云区域和虚拟专用区域。

对于每个区域，您可以设置区域优先级，并且可以限制项目可利用的资源量。可能的限制包括实例数量、内存量和 CPU 数量。您只能针对 vSphere 云区域配置存储限制。

添加每个区域并应用限制时，不要将项目资源限制到成员无法部署其云模板的程度。

当用户提交部署请求时，将评估区域以确定哪些区域具有支持部署的资源。如果有多个区域支持部署，则将评估优先级，并将工作负载放在在优先级较高（即最小整数）的区域上。

- 5 单击**创建**。

## 6 要使用项目云区域测试您的项目，请单击“项目”页面上的测试配置。

模拟将针对项目云区域资源运行标准化的假设部署测试。如果失败，您可以查看详细信息，并更正资源配置。

### 后续步骤

开始使用云模板。请参见第 6 章 设计 vRealize Automation Cloud Assembly 部署。

## 了解有关 vRealize Automation Cloud Assembly 项目的更多信息

项目是云模板和资源之间的连接器。您对它们的工作方式以及如何使它们为您工作了解得越多，您的 vRealize Automation Cloud Assembly 开发和部署过程就会越有效。

### 使用 vRealize Automation Cloud Assembly 项目标记和自定义属性

作为管理员，当项目的要求与 vRealize Automation Cloud Assembly 云模板不同时，您可以添加项目级别的监管限制或自定义属性。除了限制标记外，您还可以添加资源标记，可以在置备过程中将这些标记添加到已部署资源以便能够管理资源。

#### 什么是项目资源标记

项目资源标记作为标准化标识标记运行，可用于管理已部署的资源并确保合规性。

在项目中定义的资源标记将添加到作为该项目的一部分部署的所有组件资源。然后，您可以使用标准标记通过其他应用程序管理资源。

例如，作为云管理员，您希望使用诸如 CloudHealth 的应用程序来管理成本。您将 `costCenter:eu-cc-1234` 标记添加到专用于开发欧盟人力资源工具的项目中。当项目团队从该项目部署时，该标记将添加到已部署的资源中。然后，您可以配置成本计算工具来标识和管理包含此标记的资源。具有其他成本中心的其他项目将具有与此键匹配的替代值。

#### 什么是项目限制标记

项目限制作为管治定义运行。项目限制是一个 `key:value` 标记，用于定义部署请求在项目云区域中使用或避开的资源。

部署过程将查找与项目限制匹配的网络和存储的标记，然后根据匹配的标记进行部署。

可扩展性限制用于指定要与可扩展性工作流程配合使用的 vRealize Orchestrator 集成实例。

配置项目限制时，可以考虑以下格式。

- **key:value** 和 **key:value:hard**。如果必须在具有匹配的能力标记的资源上置备云模板，请使用此标记，任一格式皆可。如果找不到匹配的标记，部署过程将失败。例如，由项目成员部署的云模板必须在符合 PCI 的网络上置备。您将使用 `security:pci`。如果在项目云区域中找不到任何网络，部署将失败，以确保没有任何不安全部署。

- **key:value:soft**。如果您首选匹配的资源但希望部署过程继续而不失败并且可以接受具有不匹配标记的资源，请使用此标记。例如，您希望项目成员将其云模板部署到成本更低的存储，但不希望存储可用性干扰项目成员的部署能力。您将使用 `tier:silver:soft`。如果项目云区域中不存在具有 `tier:silver` 标记的存储，云模板仍会部署到其他存储资源。
- **!key:value**。如果要避免部署到具有匹配的标记的资源，请使用此标记，指定为硬性或软性皆可。

重要的是，项目限制标记具有比云模板限制标记更高的优先级，而且项目限制标记会在部署时替代云模板限制标记。如果您的云模板不允许出现这种情况，可以在该模板中使用 `failOnConstraintMergeConflict:true`。例如，您的项目有一个网络 `loc:london` 限制，但云模板是 `loc:mumbai`，您希望部署失败并显示限制冲突消息，而不希望项目位置优先，则可以添加类似下例的属性。

```
constraints:
  - tag: 'loc:mumbai'
failOnConstraintMergeConflict:true
```

## 如何使用项目自定义属性

可以使用项目自定义属性进行报告、触发和填充可扩展性操作和工作流，以及替代云模板级别属性。

通过将自定义属性添加到部署中，您可以使用用户界面中的值或使用 API 检索该属性来生成报告。

可扩展性还可以将自定义属性用于可扩展性订阅。

您可能想要针对某个项目更改云模板的特定属性值。您可以提供替代名称和值作为自定义属性。

## vRealize Automation Cloud Assembly 项目在部署时的工作方式

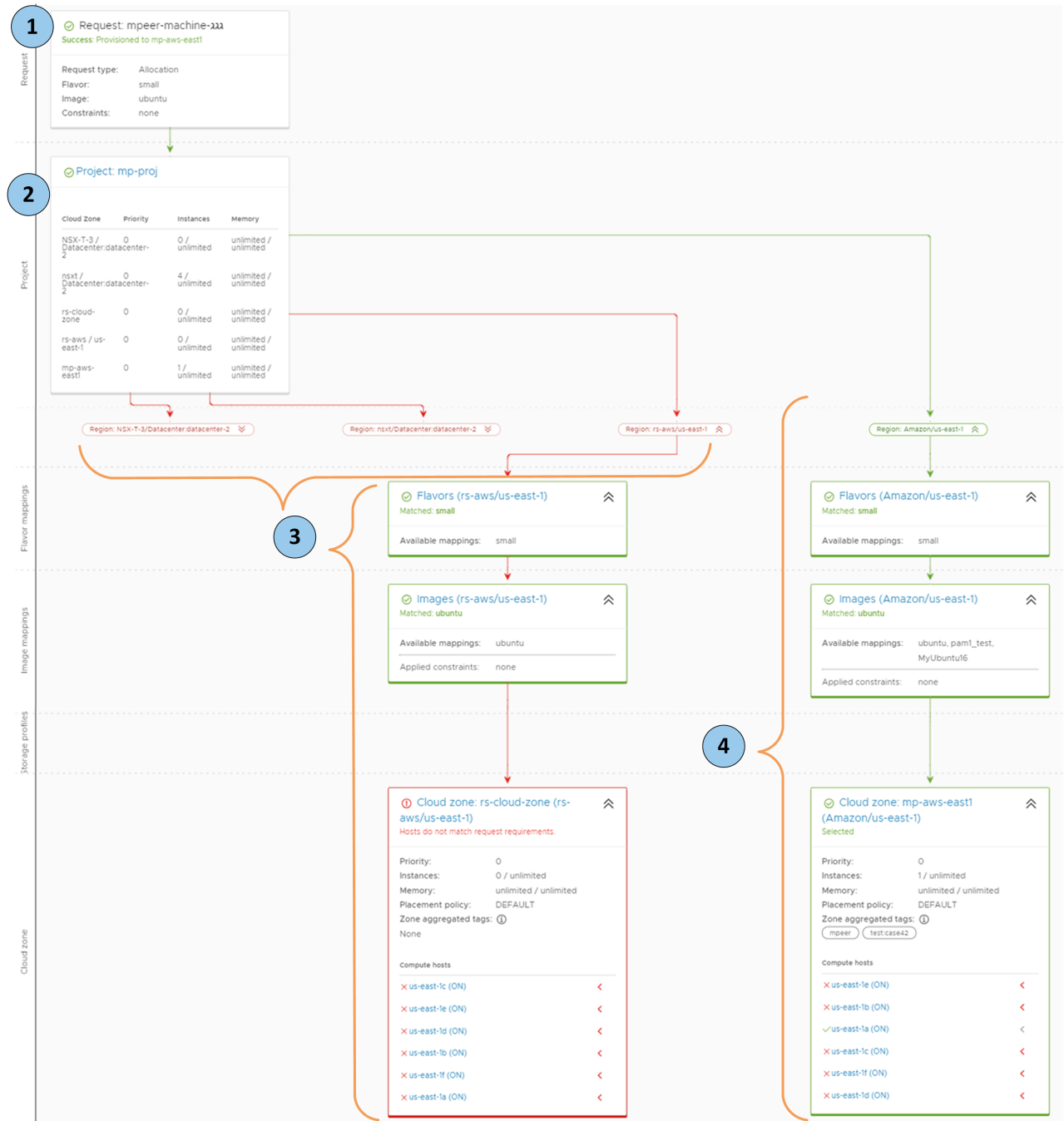
项目控制用户对云区域的访问和用户已置备资源的所有权。无论您是云管理员还是云模板开发人员，您都必须了解项目在部署时的工作方式，以便您能够管理您的部署并对任何问题进行故障排除。

作为为各种团队设置项目的云管理员，您必须了解项目如何确定云模板组件的部署位置。了解这一点可帮助您创建支持云模板开发人员的项目并对失败的部署进行故障排除。

创建云模板时，首先将其与项目关联。在部署时，将根据项目云区域评估云模板要求，以查找最佳部署位置。

以下工作流说明了该流程。

- 1 提交云模板部署请求。
- 2 项目评估模板和项目要求，例如特定实例、映像和限制标记。将要求与项目云区域进行比较，以找到支持这些要求的区域。
- 3 这些区域没有支持该请求的资源。
- 4 此云区域支持请求要求，并且模板将部署到此云区域帐户区域。



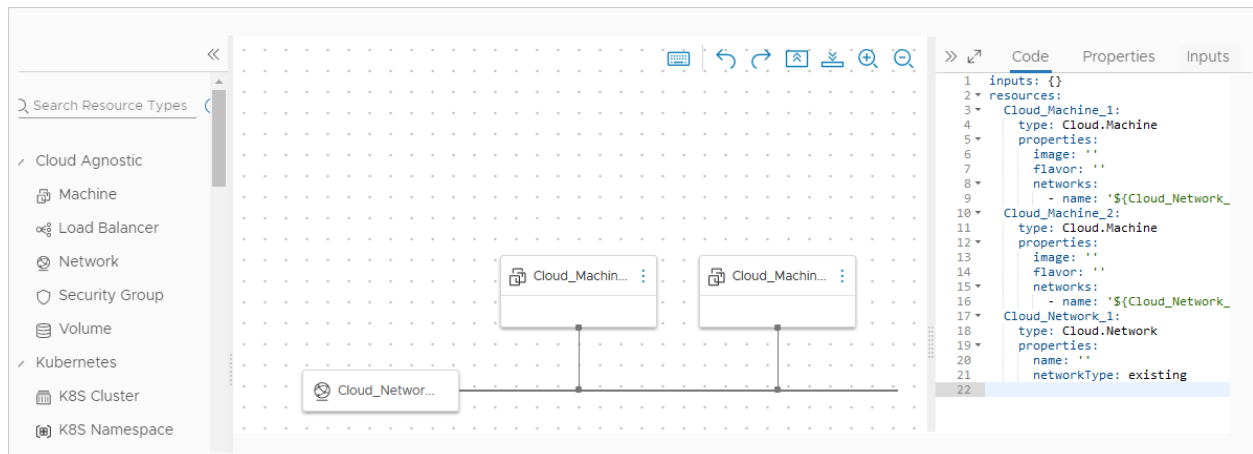
# 设计 vRealize Automation Cloud Assembly 部署

# 6

部署从云模板（以前称为蓝图）开始，这些云模板是定义通过 vRealize Automation Cloud Assembly 在云资源上创建的计算机、应用程序和服务的规范。

作为云模板开发人员，您可以设计面向特定云供应商的模板，也可以将模板设为云平台无关。分配给项目的云区域决定您可以采用的方法。请向云管理员咨询，以确保您了解构成云区域的资源类型。

请注意，vRealize Automation Cloud Assembly 模板创建是一个基础架构即代码过程。可以通过在设计画布中添加并连接资源，开始入门。然后使用画布右边的代码编辑器填写详细信息。在代码编辑器中，可以直接键入代码或将属性值输入表单。



## 创建云模板之前

您可以在任何时候创建 vRealize Automation Cloud Assembly 云模板，但首先需要定义云资源基础架构才能部署云模板。

- [第 4 章 构建您的 vRealize Automation Cloud Assembly 资源基础架构](#)

此外，您必须创建包含这些基础架构资源作为云区域的 vRealize Automation Cloud Assembly 项目。

- [第 5 章 添加和管理 vRealize Automation Cloud Assembly 项目](#)

本章讨论了以下主题：

- [创建云模板的方法](#)



- 如何从头开始创建简单的 vRealize Automation Cloud Assembly 模板
- 如何增强简单的 vRealize Automation Cloud Assembly 云模板
- 如何将高级功能添加到 vRealize Automation Cloud Assembly 设计
- 有哪些 vRealize Automation 资源属性
- 有哪些 vRealize Automation Cloud Assembly 代码示例
- 如何在 vRealize Automation Cloud Assembly 中包括 Terraform 配置
- 如何使用 vRealize Automation Cloud Assembly 商城

## 创建云模板的方法

vRealize Automation Cloud Assembly 创建云模板并将云模板另存为代码，这使您可以轻松设计和重用模板。

您可以从空白画布生成云模板，也可以利用现有代码。

## vRealize Automation Cloud Assembly 设计页面

要从头开始创建云模板，请转到**设计 > 云模板**，然后单击 **新建自 > 空白画布**。将资源拖动到画布中，连接这些资源，并在代码编辑器中完成资源配置。

代码编辑器允许您直接键入、剪切、复制和粘贴代码。如果您不喜欢编辑代码，则可以在设计画布中选择一个资源，单击代码编辑器的**属性**选项卡，并在其中输入值。您输入的属性值将显示在代码中，就像直接键入它们一样。

The screenshot displays the vRealize Automation Cloud Assembly design interface. On the left, a code editor shows the Terraform configuration for a 'WebTier' resource. On the right, the 'Properties' tab is active, showing various configuration fields for the selected resource.

**Code Editor (Left):**

```
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
```

**Properties Tab (Right):**

- Count:** "\${input.count}"
- Image Type:** ubuntu
- Flavor:** \${input.size}
- Storage:**
- Constraints:**
  - Tag: [ ]
- Maximum Capacity of the disk in GB:** 1
- Size of boot disk in GB:** 1
- Networks:**

请注意，您可以将代码从一个云模板复制并粘贴到另一个云模板。

## 云模板克隆

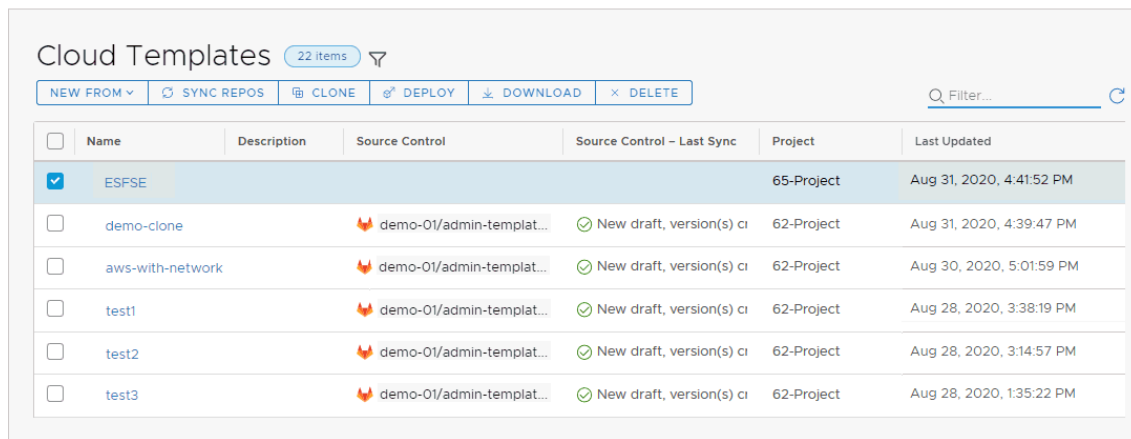
要克隆模板，请转到**设计**，选择一个源，然后单击**克隆**。可以克隆云模板来基于源创建一个副本，然后将克隆分配给新项目或将其用作新应用程序的起始代码。

## 上载和下载

vRealize Automation Cloud Assembly 商城提供了完成的云模板以快速启动您的工作。请参见[如何使用 vRealize Automation Cloud Assembly 商城](#)。

此外，您还可以采用对您的站点有效的任何方式上载、下载和共享云模板 YAML 代码。您甚至可以使用外部编辑器和开发环境修改模板代码。

**注** 验证共享模板代码的一个典型方法是，在设计页面上的 vRealize Automation Cloud Assembly 代码编辑器中对其进行检查。

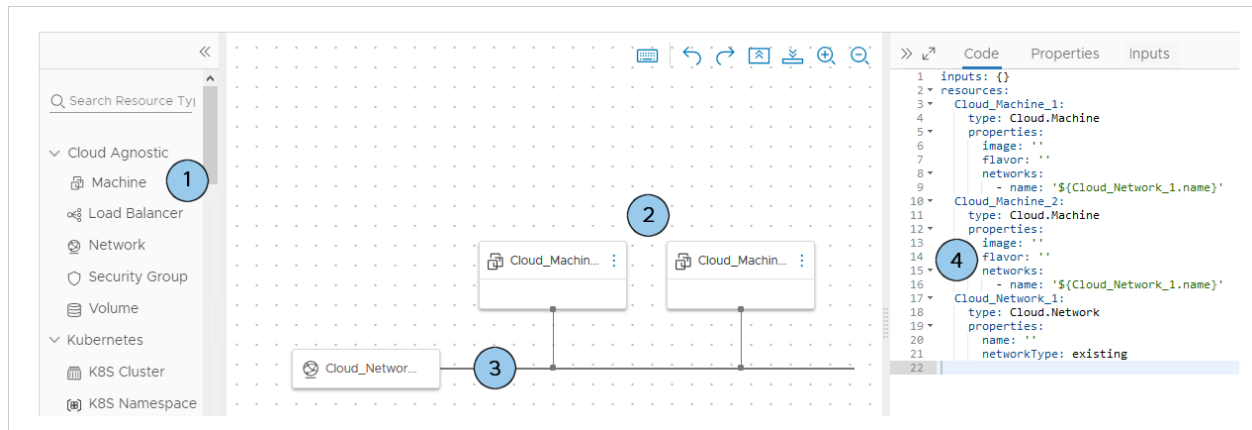


<input type="checkbox"/>	Name	Description	Source Control	Source Control - Last Sync	Project	Last Updated
<input checked="" type="checkbox"/>	ESFSE				65-Project	Aug 31, 2020, 4:41:52 PM
<input type="checkbox"/>	demo-clone		demo-01/admin-templat...	🟢 New draft, version(s) ci	62-Project	Aug 31, 2020, 4:39:47 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

## 如何从头开始创建简单的 vRealize Automation Cloud Assembly 模板

可以使用设计页面为要置备的计算机或应用程序创建 vRealize Automation Cloud Assembly 模板规范。

- 1 查找资源。
- 2 将资源拖动到画布中。
- 3 连接资源。
- 4 通过编辑云模板代码配置资源。



从设计页面中，还可以更改云模板名称和版本、恢复到某个模板版本以及克隆或部署模板。

## 如何选择 vRealize Automation Cloud Assembly 资源并将其添加到云模板

vRealize Automation Cloud Assembly 资源是云模板构建块。在设计页面中，可以使用云平台无关的资源或特定于云供应商的资源。

资源将显示在设计页面的左侧供您选择。

### 云平台无关的资源

可以将云平台无关的资源部署到任何云供应商。在置备时，部署使用匹配的特定于云的资源。例如，如果希望云模板同时部署到 AWS 云区域和 vSphere 云区域，请使用云平台无关的资源。

### 云供应商资源

供应商资源（如特定于 Amazon Web Services、Microsoft Azure、Google Cloud Platform 或 VMware vSphere 的资源）只能部署到匹配的 AWS、Azure、GCP 或 vSphere 云区域。

可以将云平台无关的资源添加到包含某特定供应商的云特定资源的云模板。请注意项目云区域在供应商方面提供的支持。

### 配置管理资源

配置管理资源依赖集成的应用程序。例如，Puppet 资源可以监控并实施其他资源的配置。

## 如何在 vRealize Automation Cloud Assembly 中连接云模板资源

可使用 vRealize Automation Cloud Assembly 图形设计画布连接云模板资源。

如果要连接的资源兼容，则可以连接这些资源。例如：

- 将负载均衡器连接到计算机集群。
- 将计算机连接到网络。

- 将外部存储连接到计算机。

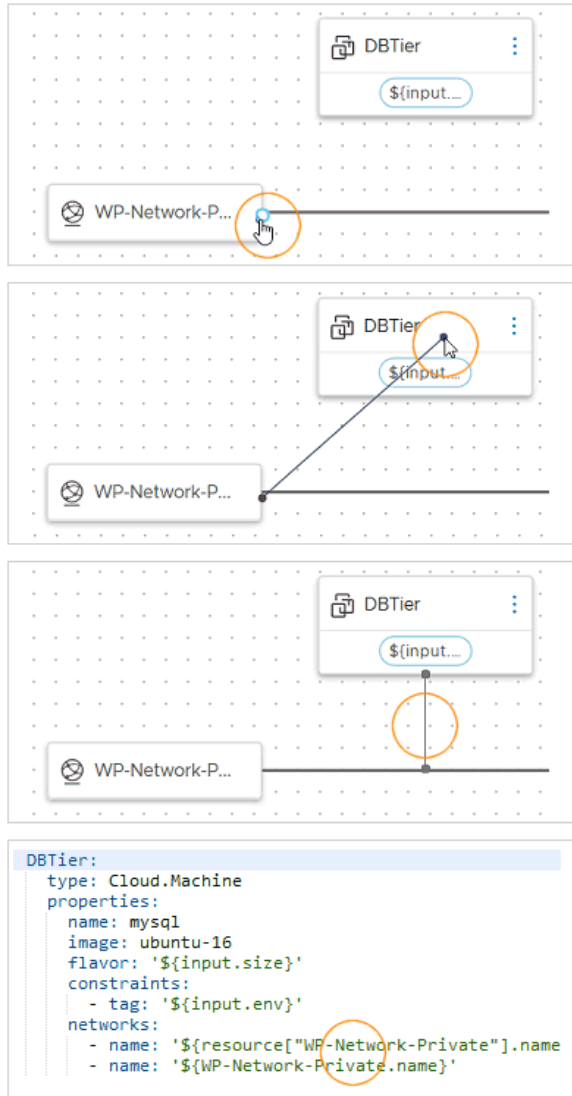
**重要说明** 实线连接器要求两个资源部署在同一个云区域中。如果向资源添加有冲突的限制，部署可能会失败。

例如，如果限制标记将一个已连接资源强制放置到 **us-west-1** 中的区域，而将另一个强制放置到 **us-east-1** 中的区域，则无法部署这两个资源。

实线或虚线箭头仅表示依赖关系，而不是连接。有关依赖关系的详细信息，请参见[如何在 vRealize Automation Cloud Assembly 中设置资源部署顺序](#)。

要进行连接，请将鼠标指针悬停在资源边缘上以显示连接气泡。之后，单击并拖动气泡到目标资源，然后释放鼠标按钮。

在代码编辑器中，源资源的其他代码将显示在目标资源的代码中。



在此图中，SQL 计算机和专用网络相连接，因此它们必须部署在同一个云区域中。

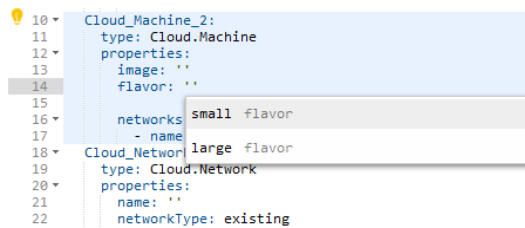
## 如何在 vRealize Automation Cloud Assembly 中创建有效的云模板代码

在画布中添加并连接 vRealize Automation Cloud Assembly 资源时，系统只会创建起始代码。要完全配置这些组件，请编辑代码。

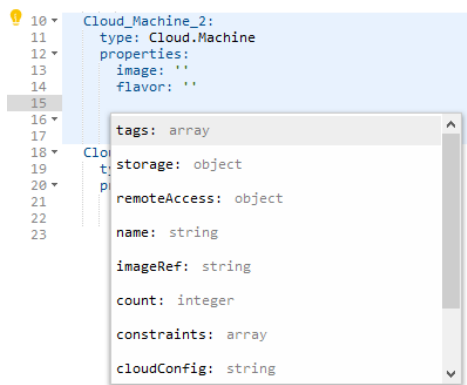
在代码编辑器中，可以直接键入代码或将属性值输入表单。为了帮助直接创建代码，vRealize Automation Cloud Assembly 编辑器包括语法完成和错误检查功能。

### 编辑器提示 示例

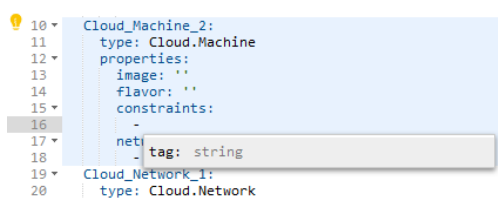
#### 可用值



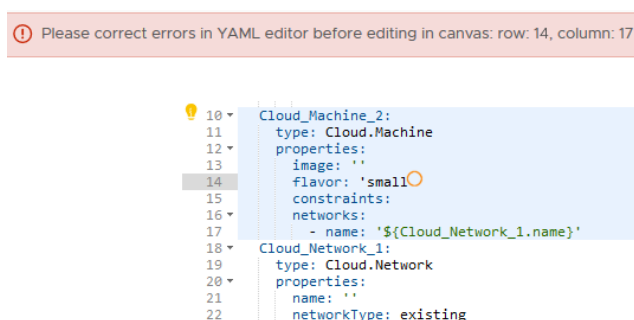
#### 允许的属性



#### 子属性



#### 语法错误



## 编辑器提示 示例

按 Ctrl+F  
可执行搜索

```

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}'

```

可选参数

插入可选参数

- + attachedDisks
- + autoScaleConfiguration
- + cloudConfig
- + cloudConfigSettings

```

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}'

```

结构定义帮助 对于所有自定义属性，还可以参阅 VMware {code} 上的 vRealize Automation 资源类型结构定义。

### cloudConfig

**类型**  
string

When provisioning an instance, machine cloud-init startup instructions from user data fields. Sample cloud config instructions:

```
#cloud-config
repo_update: true
repo_upgrade: all
packages:
- httpd
- mariadb-server

runcmd:
- [ sh, -c, "amazon-linux-extras install -y
- systemctl start httpd
- sudo systemctl enable httpd
```

```

Tier:
type: Cloud.Machine
properties:
name: mysql
image: ubuntu-16
flavor: '${input.size}'
constraints:
- tag: '${input.env}'
networks:
- name: '${resource["WP-Network-Private"]
- name: '${WP-Network-Private.name}'
remoteAccess:
authentication: usernamePassword
username: '${input.username}'
password: '${input.userpassword}'
cloudConfig:
#cloud-config
repo_update: true
repo_upgrade: all

packages:
- mysql-server

runcmd:
- sed -e '/bind-address/ s/^#/#/' -i
- service mysql restart
- mysql -e "GRANT ALL PRIVILEGES ON *.
- mysql -e "FLUSH PRIVILEGES;"
attachedDisks: []
bTier:
type: Cloud.Machine

```

## 如何使用 vRealize Automation Cloud Assembly 保存不同版本

作为云模板开发人员，您可以安全地捕获工作设计的快照，然后再冒险进行更改。

在部署时，您可以选择任一版本进行部署。

## 捕获云模板版本

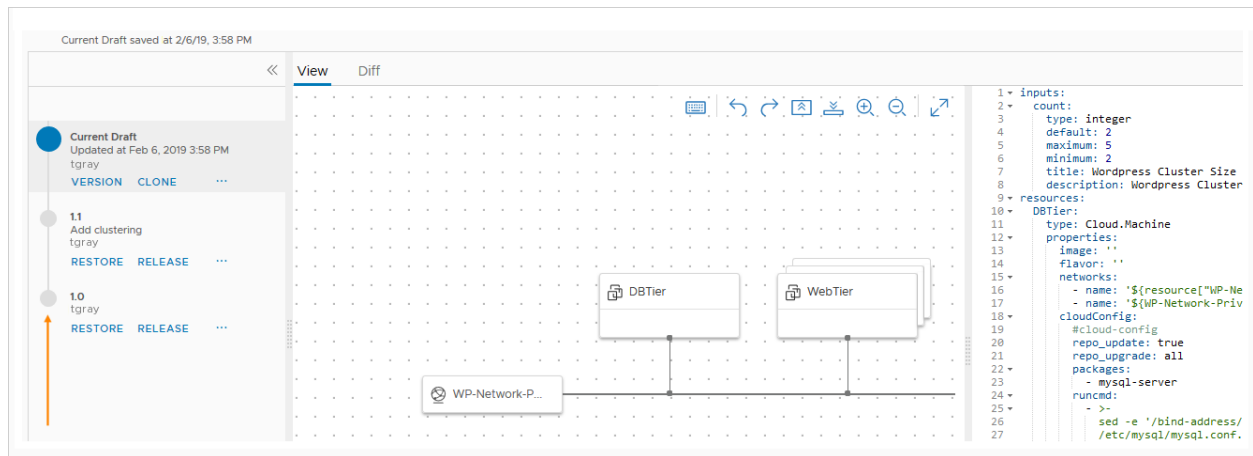
从设计页面中，单击**版本**，并提供一个名称。

该名称必须为字母数字，不含空格，并且仅允许使用句点、连字符和下划线作为特殊字符。

## 正在还原旧版本

在设计页面中，单击**版本历史记录**。

在左侧选择较旧版本以在画布和代码编辑器中对其进行检查。找到所需的版本时，单击**还原**。还原将覆盖当前草稿，而不移除任何命名版本。



## 将版本发布到 vRealize Automation Service Broker

在设计页面中，单击**版本历史记录**。

在左侧选择一个版本并发布。

对当前草稿进行版本控制后，才可发布该草稿。

## 在 vRealize Automation Service Broker 中重新导入版本

要为目录用户启用新版本，请重新导入。

在 vRealize Automation Service Broker 中，转到**内容和策略 > 内容源**。

在源列表中，单击包含具有新发布版本的云模板的项目的源。

单击**保存并导入**。

## 比较云模板版本

更改和版本累积时，您可能需要确定它们之间的差异。

在 vRealize Automation Cloud Assembly 的“版本历史记录”视图中，选择一个版本，然后单击**差异**。然后，从**差异对比**下拉列表中选择要比较的另一个版本。

请注意，您可以在查看代码差异或视觉拓扑差异之间切换。

图 6-1. 代码差异

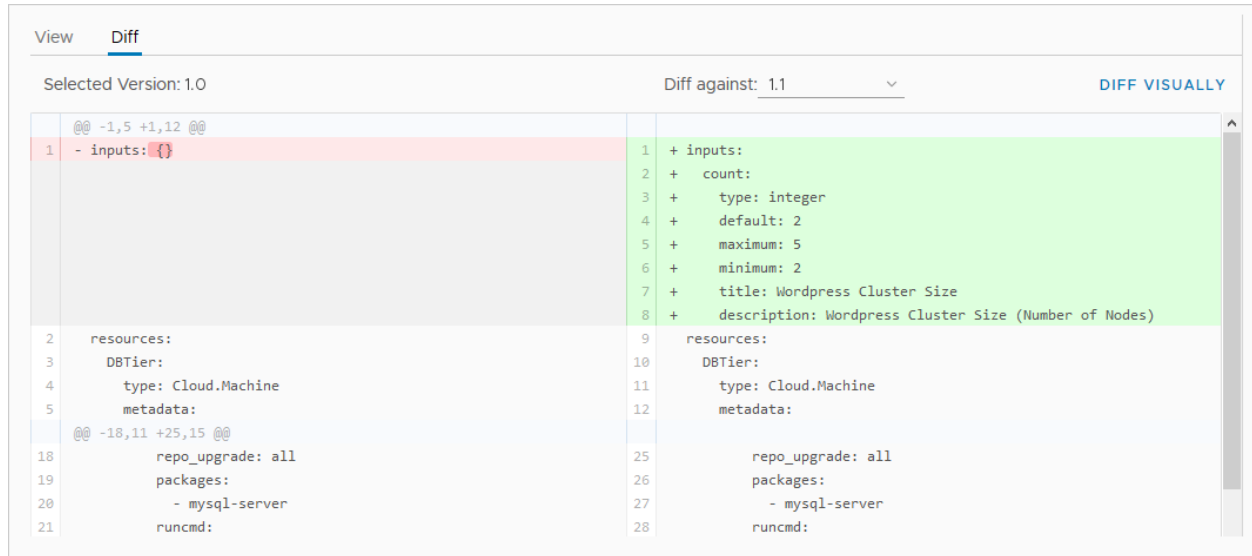
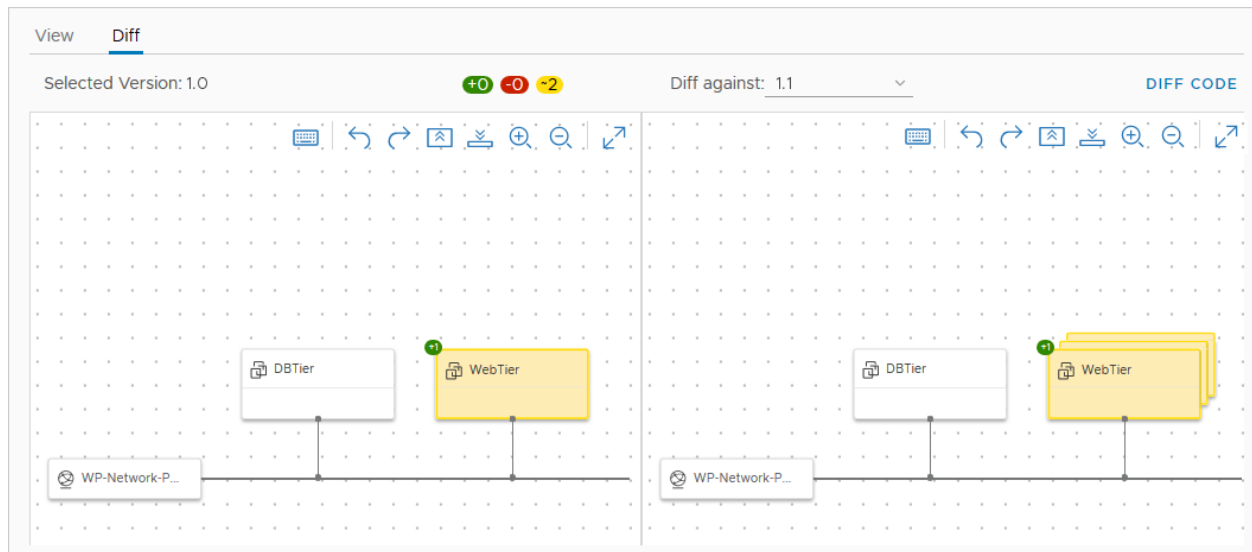


图 6-2. 视觉拓扑差异



## 克隆云模板

尽管与保存版本不同，但从设计页面中选择**操作 > 克隆**会创建当前模板的副本，供其他开发之用。

## 如何增强简单的 vRealize Automation Cloud Assembly 云模板

vRealize Automation Cloud Assembly 模板代码可以使简单的模板达到一个新的水平。

此处描述的技术需要对基础架构代码有一定的了解。幸运的是，vRealize Automation Cloud Assembly 代码是人类可读的，并且相当容易遵循。



## 用户输入如何在 vRealize Automation 中自定义云模板

作为云模板开发人员，您可以使用输入参数，以便用户可以在请求时进行自定义选择。

用户提供输入时，您不再需要保存多个仅有细微差别的模板副本。此外，输入还可以为实施后操作准备模板。请参见[如何使用云模板输入进行 vRealize Automation 实施后操作更新](#)。

以下输入介绍了如何为 MySQL 数据库服务器创建一个云模板，用户可以在其中将该模板部署到不同的云资源环境中，并且每次都应用不同的容量和凭据。

The screenshot shows a 'Testing Basic' dialog box with the following fields:

- Environment:** A dropdown menu showing 'env:dev'.
- Tier Machine Size:** A dropdown menu showing 'small'.
- Database Username:** A text input field containing 'ouradmin'.
- Database Password:** A password input field with masked characters '.....'.

At the bottom right, there are two buttons: 'CANCEL' and 'TEST'.

### 如何定义云模板输入参数

在模板代码中添加 `inputs` 部分，您可以在其中设置可选择的值。

在以下示例中，可以选择计算机大小、操作系统和集群服务器数量。

```
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)
```

如果您不擅长编辑代码，可以单击代码编辑器的**输入**选项卡，然后在其中输入设置。以下示例显示了前面提到的 MySQL 数据库的一些输入。

The screenshot shows the 'Inputs' tab in the Cloud Template editor. It displays a table of inputs with columns: Name, Title, Type, and Default Value. An 'Edit Cloud Template Input: size' dialog is open, showing fields for Name, Title, Description, Type, and Encrypted.

	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 ☐

## 如何引用云模板输入参数

然后，在 `resources` 部分中，使用 `${input.property-name}` 语法引用输入参数。

如果属性名称包含空格，请使用方括号和双引号分隔，而不是使用点表示形式：`${input["property name"]}`

**重要说明** 在云模板代码中，除了指示输入参数外，不能使用 `input` 一词。

```
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      flavor: '${input.wp-size}'
      image: '${input.wp-image}'
      count: '${input.wp-count}'
```

## 输入属性的列表

属性	说明
const	与 <b>oneOf</b> 一起使用。与友好标题关联的实际值。
default	输入的预填充值。 默认值必须为正确的类型。请勿输入单词作为整数的默认值。
description	输入的用户帮助文本。
encrypted	是否对用户键入的输入进行加密 ( <b>true</b> 或 <b>false</b> )。 密码通常是加密的。
enum	允许值的下拉菜单。 请使用以下示例作为格式指南。 <div> <pre>enum:   - value 1   - value 2</pre> </div>
format	设置所需的输入格式。例如, (25/04/19) 支持日期-时间。 允许在 vRealize Automation Service Broker 自定义表单中使用日期选择器。
items	声明数组中的项目。支持数字、整数、字符串、布尔或对象。
maxItems	数组中可选择的最大项目数。
maxLength	字符串允许使用的最大字符数。 例如, 要将字段限制在 25 个字符以内, 请输入 <code>maxLength: 25</code> 。
maximum	数字或整数的最大允许值。
minItems	数组中可选择的最小项目数。
minLength	字符串允许使用的最小字符数。
minimum	数字或整数的最小允许值。
oneOf	允许用户输入表单为不太友好的值 ( <b>const</b> ) 显示友好名称 ( <b>title</b> )。如果设置默认值, 请设置 <b>const</b> , 而不是 <b>title</b> 。 适用于字符串、整数和数字类型。
pattern	正则表达式语法中字符串输入的允许字符。 例如, '[a-z]+' 或 '[a-zA-Z0-9A-Z@#&]+'
properties	声明对象的 <b>key:value</b> 属性块。
readOnly	仅用于提供表单标签。
title	与 <b>oneOf</b> 一起使用。 <b>const</b> 值的友好名称。在部署时, 标题显示在用户输入表单上。

属性	说明
type	数字、整数、字符串、布尔或对象的数据类型。
writeOnly	在表单中隐藏星号后面的击键。不能与 <code>enum</code> 一起使用。在 vRealize Automation Service Broker 自定义表单中显示为密码字段。

## 其他示例

### 包含枚举的字符串

```
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
```

### 包含最小值和最大值的整数

```
count:
  type: integer
  title: Machine Count
  description: The number of machines that you want to deploy.
  maximum: 5
  minimum: 1
  default: 1
```

### 对象数组

```
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

```

### 包含友好名称的字符串

```

platform:
  type: string
  oneOf:
    - title: AWS
      const: platform:aws
    - title: Azure
      const: platform:azure
    - title: vSphere
      const: platform:vsphere
  default: platform:aws

```

### 包含模式验证的字符串

```

username:
  type: string
  title: Username
  description: The name for the user that will be created when the machine is provisioned.
  pattern: ^[a-zA-Z]+$

```

### 显示为密码的字符串

```

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

```

### 显示为文本区域的字符串

```

ssh_public_key:
  type: string
  title: SSH public key
  maxLength: 256

```

### 布尔

```

public_ip:
  type: boolean
  title: Assign public IP address
  description: Choose whether your machine should be internet facing.
  default: false

```

## 日期和时间日历选择器

```
leaseDate:
  type: string
  title: Lease Date
  format: date-time
```

## vRealize Automation Cloud Assembly 资源标志如何自定义请求

vRealize Automation Cloud Assembly 包含多个云模板设置，用于调整在请求时处理资源的方式。

资源标记设置不是资源对象属性架构的一部分。对于给定资源，可以在属性部分的外部添加标志设置，如下所示。

```
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
```

资源标志	说明
createBeforeDelete	<p>某些更新操作要求移除现有资源并创建新资源。默认情况下，先移除，这可能会导致出现以下情况：旧资源不存在，但由于某种原因未成功创建新资源。</p> <p>如果需要确保在删除以前的资源之前成功创建了新资源，请将此标志设置为 <b>true</b>。</p>
createTimeout	<p>资源分配、创建和规划请求的 vRealize Automation Cloud Assembly 默认超时值为 2 小时。此外，项目管理员也可以为这些请求设置自定义默认超时值，适用于整个项目。</p> <p>通过此标志，可以覆盖任何默认值并为特定的资源操作设置单独的超时值。另请参见 <a href="#">updateTimeout</a> 和 <a href="#">deleteTimeout</a>。</p>
deleteTimeout	<p>删除请求的 vRealize Automation Cloud Assembly 默认超时值为 2 小时。此外，项目管理员也可以为删除请求设置不同的默认超时值，适用于整个项目。</p> <p>通过此标志，可以覆盖任何默认值并为特定的资源删除操作设置单独的超时值。另请参见 <a href="#">updateTimeout</a> 和 <a href="#">createTimeout</a>。</p>
dependsOn	<p>此标志标识资源之间的显式依赖关系，即一个资源必须在创建下一个资源之前存在。有关详细信息，请参见 <a href="#">如何在 vRealize Automation Cloud Assembly 中设置资源部署顺序</a>。</p>

资源标志	说明
<code>dependsOnPreviousInstances</code>	<p>设置为 <b>true</b> 时，按顺序创建群集资源。默认值为 <b>false</b>，即在集群中同时创建所有资源。</p> <p>例如，对于以下数据库集群，顺序创建非常有用：必须创建主节点和辅助节点，但辅助节点创建需要将节点连接到现有主节点的配置设置。</p>
<code>forceRecreate</code>	<p>并非所有更新操作都要求移除现有资源并创建新资源。如果希望更新移除旧资源并创建新资源（与更新是否在默认情况下这样做无关），请将此标志设置为 <b>true</b>。</p>
<code>ignoreChanges</code>	<p>资源的用户可能会重新配置该资源，更改资源的已部署状态。</p> <p>如果要执行部署更新，但不使用云模板中的配置覆盖已更改的资源，请将此标志设置为 <b>true</b>。</p>
<code>preventDelete</code>	<p>如果需要保护后续删除请求中的资源，请将此标记设置为 <b>true</b>。</p>
<code>updateTimeout</code>	<p>更新请求的 vRealize Automation Cloud Assembly 默认超时值为 2 小时。此外，项目管理员也可以为更新请求设置不同的默认超时值，适用于整个项目。</p> <p>通过此标志，可以覆盖任何默认值并为特定的资源更新操作设置单独的超时值。另请参见 <code>deleteTimeout</code> 和 <code>createTimeout</code>。</p>

## 如何在 vRealize Automation Cloud Assembly 中设置资源部署顺序

部署 vRealize Automation Cloud Assembly 模板时，一个资源可能要求先提供另一个资源。

**重要说明** 实线或虚线箭头仅表示依赖关系，而不是连接。要连接资源以便它们进行通信，请参见[如何在 vRealize Automation Cloud Assembly 中连接云模板资源](#)。

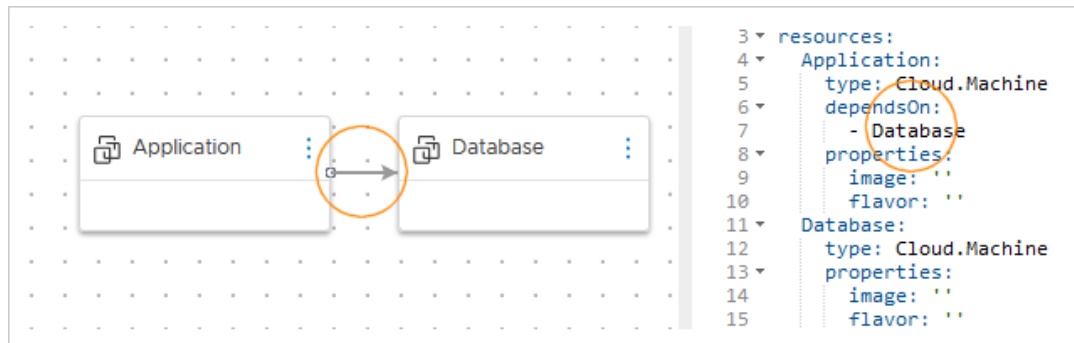
### 如何创建显式依赖关系

有时，一个资源要求先部署另一个资源。例如，可能需要先部署数据库服务器，然后才能创建应用程序服务器并将其配置为访问数据库服务器。

显式依赖关系设置部署时的生成顺序，或者设置是执行缩减操作还是扩大操作。您可以使用图形设计画布或代码编辑器添加显式依赖关系。

- 设计画布选项 - 从依赖资源开始绘制连接，然后在要先部署的资源处结束。
- 代码编辑器选项 - 将 `dependsOn` 属性添加到依赖资源，并标识要先部署的资源。

显式依赖关系会在画布中创建一个实心箭头。



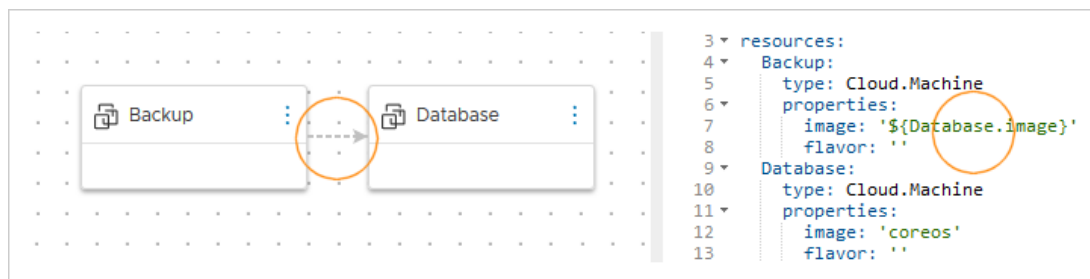
## 如何创建隐式依赖关系或属性绑定

有时，一个资源的属性要求在另一个资源的属性中找到值。例如，备份服务器可能需要正在备份的数据库服务器的操作系统映像，因此数据库服务器必须先存在。

隐式依赖关系也称为属性绑定，它通过等待所需属性可用再部署依赖资源来控制构建顺序。您可以使用代码编辑器添加隐式依赖关系。

- 编辑依赖资源，添加一个标识必须先存在的资源和属性的属性。

隐式依赖关系或属性绑定会在画布中创建一个虚线箭头。



## 如何在 vRealize Automation Cloud Assembly 中使用表达式使云模板代码更具通用性

为提高灵活性，可以在 vRealize Automation Cloud Assembly 中向云模板代码添加表达式。

表达式使用 `${expression}` 构造，如以下示例中所示。

这些示例已经过修剪，仅显示重要行。未经编辑的整个云模板显示在最后。

### 示例

在部署时，允许用户粘贴在远程访问所需的加密密钥中：

```

inputs:
  sshKey:
    type: string
    maxLength: 500
resources:
  frontend:
    type: Cloud.Machine

```



```
properties:
  remoteAccess:
    authentication: publicPrivateKey
    sshKey: '${input.sshKey}'
```

要部署到 VMware Cloud on AWS，请将文件夹名称设置为所需的 **Workload** 名称：

```
inputs:
  environment:
    type: string
    enum:
      - AWS
      - vSphere
      - Azure
      - VMC
      - GCP
    default: vSphere
  resources:
    frontend:
      type: Cloud.Machine
      properties:
        folderName: '${input.environment == "VMC" ? "Workload" : ""}'
```

部署时，使用与所选环境匹配的全小写 **env** 标记对计算机进行标记：

```
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)}'
```

将前端集群中的计算机数设置为 1（小型）或 2（大型）。请注意，大型集群是通过清除过程设置的：

```
inputs:
  envsize:
    type: string
    enum:
      - Small
      - Large
  resources:
```

```
frontend:
  type: Cloud.Machine
  properties:
    count: '${input.envsize == "Small" ? 1 : 2}'
```

通过绑定到在网络资源中找到的属性，将计算机连接到同一 Default 网络：

```
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
```

对提交到 API 的访问凭据进行加密：

```
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
```

发现 API 计算机的地址：

```
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}'
```

## 完整云模板

```

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)}'

```

## vRealize Automation Cloud Assembly 中的云模板表达式语法

表达式语法公开了 vRealize Automation Cloud Assembly 模板中表达式的所有可用功能。

如何在 [vRealize Automation Cloud Assembly](#) 中使用表达式使云模板代码更具通用性介绍的示例中仅对语法进行了部分描述。

### 文字

支持以下文字。

- 布尔（true 或 false）
- 整数
- 浮点
- 字符串

反斜杠转义双引号、单引号和反斜杠本身：

" 转义为 \"

' 转义为 \'

\ 转义为 \\

只需要在以相同类型的引号括起来的字符串中转义引号，如以下示例所示。

```
"I am a \"double quoted\" string inside \"double quotes\"."
```

- Null

### 环境变量

环境名称：

- orgId
- projectId
- projectName
- deploymentId

- deploymentName
- blueprintId
- blueprintVersion
- blueprintName
- requestedBy (用户)
- requestedAt (时间)

语法:

```
env.ENV_NAME
```

示例:

```
${env.blueprintId}
```

### 资源变量

使用资源变量可以绑定到来自其他资源的资源属性。

语法:

```
resource.RESOURCE_NAME.PROPERTY_NAME
```

示例:

- \${resource.db.id}
- \${resource.db.networks[0].address}
- \${resource.app.id} (返回非集群资源的字符串 - 未指定计数。返回集群资源的数组。)
- \${resource.app[0].id} (返回集群资源的第一个条目。)

### 资源自身变量

仅允许对支持分配阶段的资源使用资源自身变量。资源自身变量只有在分配阶段完成后才可用 (或具有值集)。

语法:

```
self.property_name
```

示例:

```
${self.address} (返回在分配阶段分配的地址。)
```

请注意, 对于名为 `resource_x` 的资源, `self.property_name` 和 `resource.resource_x.property_name` 相同, 并且都视为自引用。

### 集群计数索引

语法:

```
count.index
```

示例:

`${count.index == 0 ? "primary" : "secondary"}` (返回集群资源的节点类型。)

限制:

不支持使用 `count.index` 进行资源分配。例如，以下容量表达式在输入时创建的磁盘数组中引用位置时会失败。

```
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)}'
```

## 条件

语法:

- 相等运算符为 `==` 和 `!=`。
- 关系运算符为 `<` `>` `<=` 和 `>=`。
- 逻辑运算符为 `&&` `||` 和 `!`。
- 条件使用模式:

*condition-expression ? true-expression : false-expression*

示例:

`${input.count < 5 && input.size == 'small'}`

`${input.count < 2 ? "small" : "large"}`

## 算术运算符

语法:

运算符为 `+` `-` `/` `*` 和 `%`。

示例:

```
${(input.count + 5) * 2}
```

## 字符串串联

语法:

`${'ABC' + 'DEF'}` 的评估结果为 ABCDEF。

## 运算符 [] 和 .

在统一处理 [] 和 . 运算符方面, 表达式遵循 ECMAScript。

因此, `expr.identifier` 等效于 `expr["identifier"]`。identifier 用于构造其值为 identifier 的文字, 然后将 [] 运算符与该值一起使用。

示例:

```
${resource.app.networks[0].address}
```

此外, 当属性包含空格时, 请使用方括号和双引号分隔, 而不是使用点表示形式。

不正确:

```
input.operating system
```

正确:

```
input["operating system"]
```

## 映射构造

语法:

```
${{'key1':'value1', 'key2':input.key2}}
```

## 数组构造

语法:

```
${['key1','key2']}
```

示例:

```
${[1,2,3]}
```

## 函数

语法:

```
${function(arguments...)}
```

示例:

```
${to_lower(resource.app.name)}
```

表 6-1. 函数

函数	说明
abs(number)	数字绝对值
floor(number)	返回小于或等于参数且等于数学整数的最大（最接近正无穷大）值
ceil(number)	返回大于或等于参数且等于数学整数的最小（最接近负无穷大）值
to_lower(str)	将字符串转换为小写形式
to_upper(str)	将字符串转换为大写形式
contains(array, value)	检查数组是否包含值
contains(string, value)	检查字符串是否包含值
join(array, delim)	使用分隔符连接字符串数组并返回一个字符串
split(string, delim)	使用分隔符拆分字符串并返回字符串数组
slice(array, begin, end)	返回从开始索引到结束索引的数组片
reverse(array)	反向数组条目
starts_with(subject, prefix)	检查主题字符串是否以前缀字符串开头
ends_with(subject, suffix)	检查主题字符串是否以后缀字符串结尾
replace(string, target, replacement)	将包含目标字符串的字符串替换为目标字符串
substring(string, begin, end)	返回从开始索引到结束索引的字符串的子字符串
format(format, values...)	返回使用 Java <a href="#">Formatter</a> 类格式的带格式字符串和值。
keys(map)	返回映射的键
values(map)	返回映射的值
merge(map, map)	返回合并映射
length(string)	返回字符串长度
length(array)	返回数组长度
max(array)	返回数字数组中的最大值
min(array)	返回数字数组中的最小值
sum(array)	返回数字数组中所有值的总和
avg(array)	返回数字数组中所有值的平均值
digest(value, type)	返回使用受支持类型（md5、sha1、sha256、sha384、sha512）的值的摘要
to_string(value)	返回值的字符串表示形式



表 6-1. 函数 （续）

函数	说明
to_number(string)	将字符串解析为数字
not_null(array)	返回第一个非 null 条目
base64_encode(string)	返回 base64 编码值
base64_decode(string)	返回解码的 base64 值
now()	以 ISO-8601 格式返回当前时间
uuid()	返回随机生成的 UUID
from_json(string)	解析 json 字符串
to_json(value)	将值序列化为 json 字符串
json_path(value, path)	使用 XPath for JSON 根据值评估路径。
matches(string, regex)	检查字符串是否与正则表达式匹配
url_encode(string)	使用 url 编码规范对字符串进行编码
trim(string)	移除前导空格和尾随空格

## 如何在 vRealize Automation Cloud Assembly 模板中启用远程访问

要远程访问 vRealize Automation Cloud Assembly 已部署的计算机，请在部署之前将属性添加到该计算机的云模板中。

对于远程访问，您可以配置以下身份验证选项之一。

**注** 在需要复制密钥的情况下，您还可以在云模板中创建一个 cloudConfig 部分，以便在置备时自动复制密钥。此处没有详细说明，但[如何在 vRealize Automation Cloud Assembly 模板中自动初始化计算机](#)提供了有关 cloudConfig 的一般信息。

### 在 vRealize Automation Cloud Assembly 置备时生成密钥对

如果您没有自己的公钥-私钥对可用于远程访问身份验证的，则可以让 vRealize Automation Cloud Assembly 生成密钥对。

使用以下代码作为指导。

- 1 在 vRealize Automation Cloud Assembly 中，在置备之前，请将 remoteAccess 属性添加到云模板中，如示例中所示。

username 是可选的。如果省略它，系统会生成一个随机 ID 作为 username。

示例：

```
type: Cloud.Machine
properties:
  name: our-vm2
  image: Linux18
  flavor: small
  remoteAccess: authentication: generatedPublicPrivatekey username: testuser
```

- 2 在 vRealize Automation Cloud Assembly 中，从云模板中置备计算机，并使其进入启动状态。  
置备过程会生成密钥。

- 3 在 **部署 > 拓扑** 属性中找到密钥名称。
- 4 使用云提供商接口（如 vSphere Client）访问已置备的计算机命令行。
- 5 授予对私钥的读取权限。

```
chmod 600 key-name
```

- 6 转到 vRealize Automation Cloud Assembly 部署，选择计算机，然后单击 **操作 > 获取私钥**。
- 7 将私钥文件复制到您的本地计算机。

典型的本地文件路径是 `/home/username/.ssh/key-name`。

- 8 打开远程 SSH 会话，然后连接到已置备的计算机。

```
ssh -i key-name user-name@machine-ip
```

## 为 vRealize Automation Cloud Assembly 提供您自己的公钥-私钥对

许多企业会创建和分发自己的公钥-私钥对以进行身份验证。

使用以下代码作为指导。

- 1 在本地环境中，获取或生成您的公钥-私钥对。

现在，只需在本地生成并保存密钥。

- 2 在 vRealize Automation Cloud Assembly 中，在置备之前，请将 `remoteAccess` 属性添加到云模板中，如示例中所示。

`sshKey` 包括可在公钥文件 `key-name.pub` 中找到的长字母数字。

`username` 是可选的，创建后可用在登录时使用。如果省略它，系统会生成一个随机 ID 作为 `username`。

示例：

```
type: Cloud.Machine
properties:
  name: our-vm1
  image: Linux18
  flavor: small
  remoteAccess:
```

```
authentication: publicPrivateKey
sshKey: ssh-rsa Iq+5aQgBP3ZNT4o1baP5Ii+dstIcowRRkyobbfpA1mj9tslf
qGxvU66PX9IeZax5hZvNWFgJw6ag+Z1zndOLhVdVoW49f274/mIRild7UuW...
username: testuser
```

- 3 在 vRealize Automation Cloud Assembly 中，从云模板中置备计算机，并使其进入启动状态。
- 4 使用云供应商客户端访问置备的计算机。
- 5 将公钥文件添加到计算机上的主文件夹中。使用您在 `remoteAccess.sshKey` 中指定的密钥。
- 6 确认您的本地计算机上存在私钥文件副本。

密钥通常是不带 `.pub` 扩展名的 `/home/username/.ssh/key-name`。

- 7 打开远程 SSH 会话，然后连接到已置备的计算机。

```
ssh -i key-name user-name@machine-ip
```

## 为 vRealize Automation Cloud Assembly 提供 AWS 密钥对

通过将 AWS 密钥对名称添加到云模板，您可以远程访问 vRealize Automation Cloud Assembly 部署到 AWS 的计算机。

请注意，AWS 密钥对是区域特定的。如果您将工作负载置备到 `us-east-1`，则密钥对必须存在于 `us-east-1` 中。

使用以下代码作为指导。此选项仅适用于 AWS 云区域。

```
type: Cloud.Machine
properties:
  image: Ubuntu
  flavor: small
  remoteAccess: authentication: keyPairName keyPair: cas-test
constraints:
  - tag: 'cloud:aws'
```

## 向 vRealize Automation Cloud Assembly 提供用户名和密码

通过将用户名和密码添加到云模板，可以方便地远程访问 vRealize Automation Cloud Assembly 部署的计算机。

虽然安全性较低，但使用用户名和密码远程登录可能就是您的情况所需要的全部。请注意，某些云供应商或配置可能不支持这个不太安全的选项。

- 1 在 vRealize Automation Cloud Assembly 中，在置备之前，请将 `remoteAccess` 属性添加到云模板中，如示例中所示。

设置您希望在登录时使用的用户名和密码。

示例：

```
type: Cloud.Machine
properties:
  name: our-vm3
  image: Linux18
  flavor: small
  remoteAccess: authentication: usernamePassword username: testuser password: admin123
```

- 2 在 vRealize Automation Cloud Assembly 中，从云模板中置备计算机，并使其进入启动状态。
- 3 转到您的云供应商界面，并访问已置备的计算机。
- 4 在已置备的计算机上，创建或启用该帐户。
- 5 从本地计算机中，打开到已置备计算机 IP 地址或 FQDN 的远程会话，并像往常一样使用用户名和密码登录。

## 如何将高级功能添加到 vRealize Automation Cloud Assembly 设计

有一些高级基础架构即代码技术和 vRealize Automation Cloud Assembly 功能可以提高设计的企业就绪程度。

此处介绍的某些功能扩展了 vRealize Automation Cloud Assembly 的设计功能，其他功能则可以直接应用于云模板图编码实践。

## 如何使用 vRealize Automation Cloud Assembly 自定义已部署资源的名称

作为云或项目管理员，您有一个针对环境中资源的规定命名约定，并且您希望部署的资源遵循这些约定，而无需用户交互。您可以为 vRealize Automation Cloud Assembly 项目中的所有部署创建一个命名模板。

例如，您的主机命名约定是为资源添加 *projectname-sitecode-costcenter-whereDeployed-identifier* 前缀。您可以为每个项目的计算机配置自定义命名模板。一些模板变量在部署时从系统中提取，其他一些模板变量基于项目自定义属性。以上前缀的自定义命名模板类似于以下示例。

```
${project.name}-${resource.siteCode}-${resource.costCenter}-${endpoint.name}-${#####}
```

标识符（在模板中以 `${#####}` 的形式提供）显示一个六位数标识符。标识符是确保唯一性的计数器。该计数器对于组织而言是全局设置，在所有项目之间递增，而不仅仅是当前项目。当您有多个项目时，对于当前项目中的部署，不会获得从 000123 到 000124 的序列。您有望获得从 000123 到 000127 的增量。

所有资源名称都必须唯一。使用数字递增属性可确保唯一性。对于所有部署（包括由 vRealize Automation Cloud Assembly 命名的部署），数字都采用递增的形式。随着您的系统变得更加强健，并且由于自定义命名应用于许多资源（包括虚拟机、负载均衡器、安全组、NAT、网关、资源组和磁盘），编号可能看似随机，但值仍确保唯一性。运行测试部署时，数字也会递增。

除了此处提供的示例外，还可以添加用户名、使用的映像、其他内置选项和简单字符串。在生成模板时，会提供有关可能选项的提示。

请注意，用例中的某些值仅用作示例。不能在您的环境中逐字使用这些值。请考虑在何处需要替换为您自己的值或从示例值外插值，以便满足您自己的云计算基础架构需求和部署管理需求。

### 前提条件

- 确认您知道要用于项目中部署的命名约定。
- 此过程假定您具有或可以创建一个简单云模板，用于测试自定义主机前缀命名。

### 步骤

- 1 选择**基础架构 > 项目**。
- 2 选择现有项目或新建一个项目。
- 3 在**置备**选项卡上，找到“自定义属性”部分，并为站点代码和成本中心值创建属性。

在这里，您将在此处看到的值替换为与您的环境相关的值。

**自定义属性**  
指定应添加到此项目中的所有请求的自定义属性。 ①

定义自定义属性	名称	值
	siteCode	BGL
	costCenter	IT-research

**自定义命名**  
指定要用于在此项目中置备的计算机、网络、安全组 and 磁盘的命名模板。

模板: `${project.name}-${resource.siteCode}-${resource.costCenter}-${endpoint.name}-${#####}` ①  
Hint: Avoid conflicting names by generating digits in names. `${#####}`

- a 创建名为 **siteCode** 且值为 **BGL** 的自定义属性。
- b 添加另一个名为 **costCenter** 且值为 **IT-research** 的自定义属性。
- 4 找到“自定义命名”部分，然后添加以下模板。

```
${project.name}-${resource.siteCode}-${resource.costCenter}-${endpoint.name}-${#####}
```

您可以在字符串中复制内容，但如果这是第一个命名模板，请考虑在生成模板时使用提示文本和快速选择。

- 5 部署与项目关联的云模板，以验证自定义名称是否应用于资源。
  - a 单击**设计**选项卡，然后单击与项目关联的云模板。
  - b 部署云模板。

此时将打开**部署**选项卡，其中显示正在进行的部署。

- c 部署完成后，单击部署名称。
- d 在**拓扑**选项卡上，请注意您的自定义名称是右侧窗格中的资源名称。



6 如果部署了测试云模板以验证命名约定，则可以删除该部署。

### 后续步骤

为其他项目创建自定义命名模板。

## 如何在 vRealize Automation Cloud Assembly 模板中自动初始化计算机

可以在 vRealize Automation Cloud Assembly 中直接运行命令或者通过自定义规范（如果部署到基于 vSphere 的云区域）应用计算机初始化。

- 命令 - 云模板代码中的 `cloudConfig` 部分包含要运行的命令。
- 自定义规范 - 云模板中的属性按名称引用 vSphere 自定义规范。

### 命令和自定义规范不能混合使用

部署到 vSphere 时，如果尝试结合使用 `cloudConfig` 和自定义规范初始化，请小心进行。两者未正式兼容，因此一起使用时可能会产生不一致或不需要的结果。

有关命令和自定义规范如何交互的示例，请参见 [vRealize Automation Cloud Assembly 云模板中的 vSphere 静态 IP 地址分配](#)。

## vRealize Automation Cloud Assembly 模板中的 vSphere 自定义规范

部署到基于 vSphere 的云区域时，自定义规范可以在部署时应用客户机操作系统设置。

### 如何启用自定义规范

自定义规范必须存在于 vSphere 中您部署到的目标上。

直接编辑云模板代码。以下示例指向 vSphere 上 WordPress 主机的 `cloud-assembly-linux` 自定义规范。

```
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'
```

### 使用自定义规范还是 cloudConfig 命令

如果您希望置备体验符合您当前在 vSphere 中执行的操作，那么继续使用自定义规范可能是最佳方法。但是，要扩展到混合或多云置备，一种更中立的方法是使用 cloudConfig 初始化命令。

有关云模板中 cloudConfig 部分的详细信息，请参见 [vRealize Automation Cloud Assembly 模板中的配置命令](#)。

### 命令和自定义规范不能混合使用

部署到 vSphere 时，如果尝试结合使用嵌入式 cloudConfig 命令和自定义规范初始化，请小心进行。两者未正式兼容，因此一起使用时可能会产生不一致或不需要的结果。

有关命令和自定义规范如何交互的示例，请参见 [vRealize Automation Cloud Assembly 云模板中的 vSphere 静态 IP 地址分配](#)。

## vRealize Automation Cloud Assembly 模板中的配置命令

可以将 cloudConfig 部分添加到 vRealize Automation Cloud Assembly 模板代码中，在其中添加在部署时运行的计算机初始化脚本。

### 如何形成 cloudConfig 命令

- Linux - 初始化命令遵循开放的 [cloud-init](#) 标准。
- Windows - 初始化命令使用 [Cloudbase-init](#)。

Linux [cloud-init](#) 和 Windows [Cloudbase-init](#) 不共享相同的语法。一个操作系统的 cloudConfig 部分在其他操作系统的计算机映像中不起作用。

### cloudConfig 命令有何作用

您可以使用初始化命令在创建实例时自动应用数据或设置，以自定义用户、权限、安装或任何其他基于命令的操作。示例包括：

- 设置主机名
- 生成并设置 SSH 私钥
- 安装软件包

### 可以在何处添加 cloudConfig 命令

可以在云模板代码中添加 cloudConfig 部分，但也可以在配置基础架构时提前在计算机映像中添加一个 cloudConfig 部分。之后，引用源映像的所有云模板都将进行相同的初始化。

您可能有一个映像映射和一个云模板，这两者都包含初始化命令。在部署时，这些命令将合并，vRealize Automation Cloud Assembly 会运行合并的命令。

当两个位置中出现相同的命令但包含不同的参数时，系统只会运行映像映射命令。

有关更多详细信息，请参见[了解有关 vRealize Automation 中的映像映射的更多信息](#)。

### cloudConfig 命令示例

以下示例 cloudConfig 部分取自适用于基于 Linux 的 MySQL 服务器的 [创建基本云模板](#) 云模板代码。

**注** 为确保正确解释命令，请始终包括管道线字符 cloudConfig: |，如下所示。

```
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
```

如果 cloud-init 脚本行为异常，请在故障排除时检查 /var/log/cloud-init-output.log 中捕获的控制台输出。有关 cloud-init 的详细信息，请参见 [cloud-init 文档](#)。

### 命令和自定义规范不能混合使用

部署到 vSphere 时，如果尝试结合使用嵌入式 cloudConfig 命令和自定义规范初始化，请小心进行。两者未正式兼容，因此一起使用时可能会产生不一致或不需要的结果。

有关命令和自定义规范如何交互的示例，请参见 [vRealize Automation Cloud Assembly 云模板中的 vSphere 静态 IP 地址分配](#)。



## vRealize Automation Cloud Assembly 云模板中的 vSphere 静态 IP 地址分配

部署到 vSphere 时，可以分配一个静态 IP 地址，但必须注意不要在 cloudConfig 初始化命令和自定义规范之间引入冲突。

### 设计示例

以下设计可安全地应用静态 IP 地址，而不会在云模板初始化命令和自定义规范之间产生任何冲突。所有设计均包含 `assignment: static` 网络设置。

## 设计

## 云模板代码示例

将静态 IP 地址分配给没有 cloud-init 代码的 Linux 计算机

```
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}'
```

将静态 IP 地址分配给具有 cloud-init 代码但代码不含网络分配命令的 Linux 计算机。

注意：无论是将 customizeGuestOs 自定义规范设置为 true 还是省略

customizeGuestOs 属性，都会应用 vSphere 自定义规范。

## Ubuntu 示例

```
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}'
```

## CentOS 示例

```
resources:
  wpnet:
    type: Cloud.Network
    properties:
```

## 设计

## 云模板代码示例

```
    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}'
```

## 设计

将静态 IP 地址分配给具有 cloud-init 代码同时代码包含网络分配命令的 Linux 计算机。  
customizeGuestOs 属性必须为 false。

## 云模板代码示例

## Ubuntu 示例

```
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}'
```

## CentOS 示例

```
resources:
  wpnet:
    type: Cloud.Network
    properties:
      name: wpnet
      networkType: public
      constraints:
        - tag: sqa
  DBTier:
    type: Cloud.vSphere.Machine
    properties:
      flavor: small
      image: centos-template
```

## 设计

## 云模板代码示例

```

    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}'

```

基于引用映像部署时，将静态 IP 地址分配给具有 cloud-init 代码同时代码包含网络分配命令的 Linux 计算机。

**customizeGuestOs** 属性必须为 **false**。

此外，云模板不得包含 **ovfProperties** 属性，该属性会阻止自定义。

```

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

```

## 设计

## 云模板代码示例

```

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}'

```

## 不起作用或可能会产生不想要的结果的设计

- cloud-init 代码不包含网络分配命令，且 customizeGuestOs 属性为 false。  
既没有初始化命令也没有自定义规范用于配置网络设置。
- cloud-init 代码不包含网络分配命令，并设置了 ovfProperties 属性。  
初始化命令不存在，但 ovfProperties 阻止了自定义规范。
- cloud-init 代码包含网络分配命令，但 customizeGuestOs 属性缺失或设置为 true。  
应用自定义规范与初始化命令冲突。

## 有关 cloud-init 和自定义规范的其他解决办法

部署到 vSphere 时，还可以自定义映像，以解决 cloud-init 和自定义规范的冲突。有关详细信息，请参见以下外部存储库。

- [vSphere 映像准备脚本](#)

## 如何使 vRealize Automation Cloud Assembly 部署等待初始化

有时，在继续进行 vRealize Automation Cloud Assembly 部署之前，需要完全启动虚拟机。

例如，如果部署仍在安装软件包和启动 Web 服务器的计算机，则可能会导致快速用户试图在应用程序可用之前访问该应用程序的情况。

使用此功能时，请注意以下注意事项。

- 此功能使用 [cloud-init phone\\_home](#) 模块，并在部署 Linux 计算机时可用。

- 由于 [Cloudbase-init](#) 限制，`phone_home` 不适用于 Windows。
- `phone_home` 可以像显式依赖关系一样影响部署顺序，但在计时和处理选项方面具有更大的灵活性。请参见 [如何在 vRealize Automation Cloud Assembly 中设置资源部署顺序](#)。
- `phone_home` 需要云模板中的 `cloudConfig` 部分。
- 您的创造力是一个因素。初始化命令可能包括操作之间的嵌入等待时间，可以与 `phone_home` 协同使用。
- 如果计算机模板中已包含 `phone_home` 模块设置，则基于云模板的 `phone_home` 将无法正常工作。
- 计算机必须具有返回 vRealize Automation Cloud Assembly 的出站通信访问权限。

要在 vRealize Automation Cloud Assembly 中使用 `phone_home` 等待计算机初始化，请将 `cloudConfigSettings` 部分添加到云模板中：

```
cloudConfigSettings:
  phoneHomeShouldWait: true
  phoneHomeTimeoutSeconds: 600
  phoneHomeFailOnTimeout: true
```

属性	说明
<code>phoneHomeShouldWait</code>	是否等待初始化（ <code>true</code> 或 <code>false</code> ）。
<code>phoneHomeTimeoutSeconds</code>	何时决定是否继续部署，即使初始化仍在运行。默认值为 10 分钟。
<code>phoneHomeFailOnTimeout</code>	是否在超时后继续部署（ <code>true</code> 或 <code>false</code> ）。请注意，即使继续进行，部署仍可能因各种原因而失败。

## 如何执行 Windows 客户机自定义

要使 vRealize Automation Cloud Assembly 在部署时自动初始化 Windows 计算机，请准备一个支持 Cloudbase-Init 的映像，然后再准备一个包含适当命令的云模板。

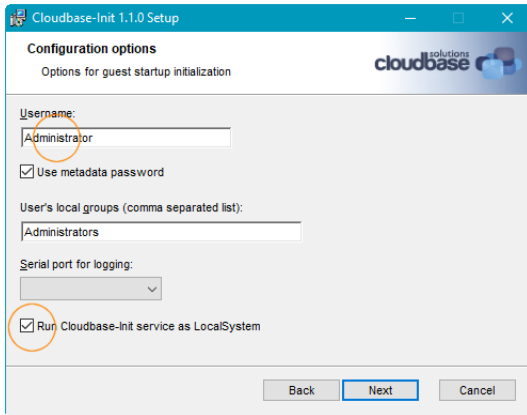
映像创建过程因云供应商而异。下面所示示例针对 vSphere。

### 如何为 vSphere 创建可初始化的 Windows 映像

要使 vRealize Automation Cloud Assembly 初始化部署到 vSphere 的 Windows 计算机，需要基于安装并配置了 Cloudbase-Init 的模板。

- 1 使用 vSphere 创建 Windows 虚拟机并打开其电源。
- 2 在虚拟机上，登录到 Windows。
- 3 下载 Cloudbase-Init。  
<https://cloudbase.it/cloudbase-init/#download>
- 4 启动 Cloudbase-Init 设置 .msi 文件。

在安装过程中，输入 **Administrator** 作为用户名，然后选择以 LocalSystem 身份运行的选项。



其他设置选项可以保留为默认值。

- 5 允许安装运行，但不关闭设置向导的最终“已完成”页面。

**重要说明** 请勿关闭设置向导的最后一个页面。

- 6 在安装向导的“已完成”页面仍处于打开状态的情况下，使用 Windows 导航到 Cloudbase-Init 安装路径，并在文本编辑器中打开以下文件。

```
conf\cloudbase-init-unattend.conf
```

- 7 将 metadata\_services 设置为 OvfService，如下所示。

```
metadata_services=cloudbaseinit.metadata.services.ovfservice.OvfService
```

- 8 保存并关闭 cloudbase-init-unattend.conf。

- 9 从同一文件夹中，使用文本编辑器打开以下文件。

```
conf\cloudbase-init.conf
```

- 10 设置 first\_logon\_behaviour、metadata\_services 和 plugins，如下所示。

```
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 保存并关闭 cloudbase-init.conf。

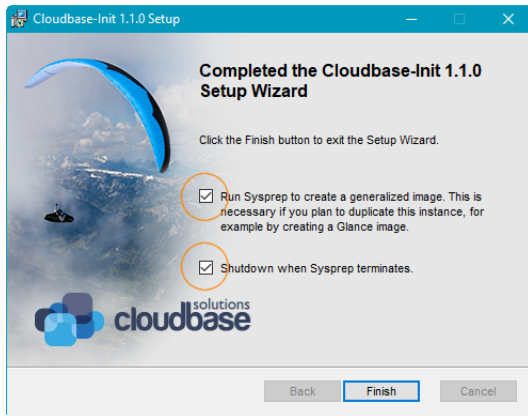


- 12 在设置向导的“已完成”页面上，选择运行 Sysprep 的选项和运行 Sysprep 之后关闭的选项，然后单击完成。

**注** VMware 曾经遇到过运行 Sysprep 会阻止映像部署正常运行的情况。

部署时，vRealize Automation Cloud Assembly 会应用动态生成的自定义规范，这会断开网络接口的连接。映像中的挂起 Sysprep 状态可能会导致自定义规范失败并使部署处于已断开连接状态。

如果您怀疑环境中发生这种情况，请尝试在创建映像时使 Sysprep 选项处于已停用状态。



- 13 虚拟机关闭后，使用 vSphere 将其转换为模板。

#### 其他详细信息

下表详述了在设置期间配置的条目。

配置设置	用途
用户名、CreateUserPlugin 和 SetUserPasswordPlugin	运行 Sysprep 后，首次引导使用 CreateUserPlugin 创建用户名 Administrator 帐户，但密码为空。 SetUserPasswordPlugin 允许 Cloudbase-Init 将空密码更改为将包含在云模板中的远程访问密码。
首次登录行为	此设置会在首次登录时提示用户更改密码。
元数据服务	通过仅列出 OvfService，Cloudbase-Init 不会尝试查找 vCenter 中不支持的其他元数据服务。这会使日志文件更干净，否则日志中将充满有关找不到那些其他服务的条目。
插件	通过仅列出具有 OvfService 所支持功能的插件，日志将再次变得更加干净。Cloudbase-Init 按指定的顺序运行插件。
以 LocalSystem 身份运行	此设置支持任何高级初始化命令，这些命令可能需要 Cloudbase-Init 才能在专用管理员帐户下运行。

#### 如何在云模板中包含 Cloudbase-Init 命令

要初始化 Windows 计算机，请在 vRealize Automation Cloud Assembly 中创建基础架构和云模板，以便可初始化的 Windows 映像运行所需命令。

下面所示示例基于 vSphere，但其他云供应商应类似。

## 必备条件

- 创建基础架构。在 vRealize Automation Cloud Assembly 中，添加 vSphere 云帐户和关联的云区域。
- 添加特定实例和映像映射，然后添加网络 and 存储配置文件。

在基础架构中，映像映射必须指向为支持 Cloudbase-Init 而创建的 Windows 模板。请参见[如何为 vSphere 创建可初始化的 Windows 映像](#)。

如果未列出该模板，请转到“云帐户”，然后同步映像。否则，将每隔 24 小时运行一次自动同步。

- 添加项目，添加用户，并确保用户可以置备到您的云区域。

有关创建基础架构和项目的详细信息，请参见[教程：在 vRealize Automation Cloud Assembly 中设置和测试多云基础架构和部署](#)中的示例。

## 过程

- 1 在 vRealize Automation Cloud Assembly 中，转到[设计](#)选项卡，然后创建新云模板。
- 2 使用所需的 Cloudbase-init 命令添加 cloudConfig 部分。

以下命令示例将在 Windows C: 驱动器上创建新文件，并设置主机名。

```
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
```

有关详细信息，请参见[Cloudbase-init 文档](#)。

- 3 添加 remoteAccess 属性，以便将计算机配置为初始登录到 Windows。
- 如创建模板时所述，元数据服务会选取登录凭据，并将其提供给 CreateUserPlugin 和 SetUserPasswordPlugin。请注意，密码必须符合 Windows 密码要求。
- 4 从 vRealize Automation Cloud Assembly 中，测试并部署云模板。
- 5 部署后，使用 Windows RDP 和模板中的凭据登录到新的 Windows 计算机并验证自定义。

在以上示例中，您将查找 C:\test.txt 文件，并检查系统属性中的主机名。

## 如何创建要在 vRealize Automation Cloud Assembly 云模板中使用的自定义资源类型

在 vRealize Automation Cloud Assembly 中创建云模板时，资源类型调色板包括受支持云帐户和集成端点的资源类型。在一些用例中，可能要根据资源类型的扩展列表创建云模板。可以创建自定义资源，将其添加到设计画布，然后创建支持设计和部署需求的云模板。

### 使用 vRealize Orchestrator 创建自定义资源

每个自定义资源都基于 vRealize Orchestrator SDK 清单类型，并通过具有所需 SDK 类型实例的输出创建的 vRealize Orchestrator 工作流创建。创建自定义资源不支持基本类型，例如 `Properties`、`Date`、`string` 和 `number`。

---

**注** SDK 对象类型可与其他属性类型区分开，它使用冒号（“:”）分隔插件名称和类型名称。例如，`AD:UserGroup` 是用于管理 Active Directory 用户组的 SDK 对象类型。

---

可以使用 vRealize Orchestrator 中的内置工作流，也可以创建自己的工作流。使用 vRealize Orchestrator 创建一切即服务/XaaS 工作流意味着，可以创建在部署时将 Active Directory 用户添加到计算机的云模板，也可以将自定义 F5 负载均衡器添加到部署。

### 自定义资源名称和资源类型

自定义资源名称可标识云模板资源类型调色板中的自定义资源。

自定义资源的资源类型必须以 **Custom.** 开头且每个资源类型必须唯一。例如，可以将 `Custom.ADUser` 设置为添加 Active Directory 用户的自定义资源的资源类型。尽管未验证文本框中是否包含 **Custom.**，但如果将其移除，会自动添加该字符串。

### 外部类型

外部类型属性定义自定义资源的类型。在 vRealize Automation Cloud Assembly 中，当您在自定义资源中选择创建工作流时，将在其下方显示“外部类型”下拉列表。下拉列表包括从 vRealize Orchestrator 工作流的输出参数中选择的外部类型属性。下拉列表包括的选定工作流输出属性必须是非数组 SDK 对象类型，例如 `VC:VirtualMachine` 或 `AD:UserGroup`。

---

**注** 创建使用动态类型插件的自定义工作流时，请验证其变量是否使用 `DynamicTypesManager.getObject()` 方法进行创建。

---

定义自定义资源时，还可以定义选择外部类型的可用性范围。选定外部类型可以：

- 在项目之间共享。
- 仅适用于所选项目。

每个定义的范围只能有一个外部类型。例如，如果在项目中创建自定义资源时使用 `VC:VirtualMachine` 作为外部类型，则无法为同一项目创建使用相同外部类型的其他自定义资源。此外，也无法创建两个使用相同外部类型的共享自定义资源。

## 工作流输入/输出验证

将创建、删除和更新工作流作为生命周期操作添加到自定义资源时，vRealize Automation Cloud Assembly 会验证所选工作流是否具有正确的输入和输出属性定义。

- 创建工作流的输出参数必须为 SDK 对象类型，例如 SSH:Host 或 SQL:Database。如果所选工作流未通过验证，将无法添加更新或删除工作流，也无法保存对自定义资源所做的更改。
- 删除工作流的输入参数必须是与自定义资源的外部类型匹配的 SDK 对象类型。
- 更新工作流的输入和输出参数必须是与自定义资源的外部类型匹配的 SDK 对象类型。

## 自定义资源属性结构定义

将 vRealize Orchestrator 工作流添加到自定义资源时，其输入和输出参数将添加为属性。可以通过选择属性选项卡查看自定义资源属性结构定义。结构定义包括名称、数据类型、属性类型以及给定属性的说明（如果可用）。此外，结构定义还定义给定属性是必需项还是可选项。

## 如何在 vRealize Automation Cloud Assembly 中创建将用户添加到 Active Directory 的云模板

除了在创建云模板时使用的 vRealize Automation Cloud Assembly 云模板资源外，还可以创建自己的自定义资源。

自定义资源是通过 vRealize Automation 和定义的主资源操作工作流管理的 vRealize Orchestrator 对象。当触发创建或删除操作时，云模板服务会自动调用相应的 vRealize Orchestrator 工作流。此外，还可以通过选择可用作实施后操作的 vRealize Orchestrator 工作流扩展资源类型的功能。

此用例使用 vRealize Orchestrator 库中提供的内置工作流。它包含指导性值或字符串，帮助演示如何执行过程。可以根据您的环境对其进行修改。

为便于参考，此用例使用名为 **DevOpsTesting** 的项目。可以将此示例项目替换为您环境中的任何项目。

### 前提条件

- 确认您已配置 vRealize Orchestrator 集成。请参见在 [Cloud Assembly 中配置 vRealize Orchestrator 集成](#)。
- 确认 vRealize Orchestrator 中存在用于创建、更新、销毁和实施后操作的工作流，并且成功运行。
- 在 vRealize Orchestrator 中，找到工作流使用的资源类型。此自定义资源中包含的工作流必须全部使用相同的资源类型。在此用例中，资源类型为 AD:User。有关资源类型验证的详细信息，请参见[如何创建要在 vRealize Automation Cloud Assembly 云模板中使用的自定义资源类型](#)。
- 通过使用 vRealize Orchestrator 集成中的内置 Active Directory 工作流，配置 Active Directory 服务器。
- 确认您知道如何配置并部署计算机云模板。

## 步骤

### 1 创建用于在组中添加用户的 Active Directory 自定义资源。

此步骤将自定义资源作为一种资源类型添加到云模板设计画布。

- a 在 vRealize Automation Cloud Assembly 中，选择**设计 > 自定义资源**，然后单击**新建自定义资源**。
- b 提供以下值。

请注意，除工作流名称外，这些值都是示例值。

设置	示例值
名称	<b>AD user</b> 这是显示在云模板资源类型调色板中的名称。
资源类型	<b>Custom.ADUser</b> 资源类型必须以 <b>Custom.</b> 开头且每个资源类型必须唯一。 尽管未验证文本框中是否包含 <b>Custom.</b> ，但如果将其移除，会自动添加该字符串。 此资源类型将添加到资源类型调色板中，以便可以在云模板中使用。

- c 要在云模板资源类型列表中启用此资源类型，请验证**激活**选项是否已打开。
- d 选择**范围**设置，使该资源类型可用于任何项目。

- e 选择定义资源和实施后操作的工作流。

**注** 所选实施后操作工作流的输入参数类型必须与外部类型相同。外部类型输入不会显示在用户请求的实施后操作自定义表单中，因为它会自动绑定到自定义资源。

设置	示例值
生命周期操作 - 创建	<p>选择<b>在组织单位中创建用户和密码</b>工作流。</p> <p>如果您有多个 vRealize Orchestrator 集成，请在用于运行这些自定义资源的集成实例上选择工作流。</p> <p>选择工作流后，“外部类型”下拉菜单将变得可用，并自动设置为 <code>AD:User</code>。</p> <p><b>注</b> 如果是共享资源，则只能使用一次外部源类型，而且每个项目只能使用一次。在此用例中，您将为所有项目提供相同的自定义资源。这意味着，您不能将 <code>AD:User</code> 用于所有项目的任何其他资源类型。如果有其他工作流需要 <code>AD:User</code> 类型，则必须为每个项目创建单独的自定义资源。</p>
生命周期操作 - 销毁	选择 <b>销毁用户</b> 工作流。
其他操作	<p>选择<b>更改用户密码</b>工作流。</p> <p>要修改用户在请求操作时响应的操作请求表单，请单击<b>请求参数</b>列中的图标。</p> <p><b>注</b> 对于其他操作工作流，请确认工作流的输入参数类型与外部类型相同。</p>

在此示例中，没有适当地应用更新工作流。更新工作流（对置备的自定义资源进行更改）的一个常见示例是横向缩减或扩展部署。

- f 查看结构定义键并在**属性**选项卡中键入值，以便了解工作流输入，从而可以在云模板中配置输入。该结构定义列出了工作流中定义的必需和可选输入值。必需输入值包含在云模板 **YAML** 中。

在“创建用户”工作流中，`accountName`、`displayName` 和 `ouContainer` 是必需输入值。其他结构定义属性不是必需项。还可以使用结构定义确定要创建与其他字段值、工作流或操作绑定的位置。此用例中不包括绑定。

- g 要完成创建自定义资源，请单击**创建**。

## 2 创建云模板，以便在部署时将用户添加到计算机。

- 选择**设计 > 云模板**，然后单击**新建自 > 空白画布**。
- 将此云模板命名为 **Machine with an AD user**。
- 选择 **DevOpsTesting** 项目，然后单击**创建**。
- 添加和配置 vSphere 计算机。

- e 从云模板设计页面左侧的“自定义资源”列表中，将 **AD user** 资源类型拖动到画布上。

**注** 选择自定义资源的方法有两种：向下滚动，然后从左侧窗格中进行选择；在**搜索资源类型**文本框中进行搜索。如果自定义资源未显示，请单击**搜索资源类型**文本框旁边的刷新按钮。

- f 在右侧，编辑 **YAML** 代码，以添加必需的输入值和密码。

在代码中添加 **inputs** 部分，以便用户可以提供所添加用户的名称。在以下示例中，其中一些值是示例数据。您的值可能会有所不同。

```
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 在 **resources** 部分中，添加 `${input.input-name}` 代码以提示提供用户选择。

```
resources:
  Custom_ADUser_1:
    type: Custom.ADUser
    properties:
      accountName: '${input.accountName}'
      displayName: '${input.displayName}'
      ouContainer: '${input.ouContainer}'
      password: '${input.password}'
      confirmPassword: '${input.confirmPassword}'
```

### 3 部署云模板。

- a 在云模板设计器页面上，单击**部署**。
- b 输入**部署名称 AD User Scott**。
- c 选择**云模板版本**，然后单击**下一步**。
- d 完成部署输入。
- e 单击**部署**。

### 4 监控置备过程，以确保用户添加到 Active Directory。

- a 单击**部署**并找到您的 **AD User Scott** 部署。
- b 监控请求的状态并验证部署是否成功。
- c 确认更改密码操作可用且正常运行。

#### 后续步骤

经过测试的云模板正常运行时，可以开始在其他云模板中使用 **AD user** 自定义资源。

## 如何在 Cloud Assembly 中创建包含 SSH 的云模板

可以使用 vRealize Orchestrator 工作流创建用于构建云模板的自定义资源。在此用例中，您将添加一个自定义资源来添加 SSH 主机。然后，可以将该资源包括在云模板中。此过程还会添加更新工作流，使用户可在部署后更改 SSH 配置，而无需执行各个实施后操作。

自定义资源是通过 vRealize Automation 和定义的主资源操作工作流管理的 vRealize Orchestrator 对象。当触发创建或删除操作时，云模板服务会自动调用相应的 vRealize Orchestrator 工作流。此外，还可以通过选择可用作实施后操作的 vRealize Orchestrator 工作流扩展资源类型的功能。

此用例使用 vRealize Orchestrator 库中提供的内置工作流。它包含指导性值或字符串，帮助演示如何执行过程。可以根据您的环境对其进行修改。

为便于参考，此用例使用名为 **DevOpsTesting** 的项目。可以将项目替换为您已有的项目。

#### 前提条件

- 确认您已配置 vRealize Orchestrator 集成。请参见在 [Cloud Assembly 中配置 vRealize Orchestrator 集成](#)。
- 确认 vRealize Orchestrator 中存在用于创建、更新、销毁和实施后操作的工作流，并且成功运行。
- 在 vRealize Orchestrator 中，找到工作流使用的资源类型。此自定义资源中包含的工作流必须全部使用相同的资源类型。在此用例中，资源类型为 `SSH:Host`。有关资源类型验证的详细信息，请参见[如何创建要在 vRealize Automation Cloud Assembly 云模板中使用的自定义资源类型](#)。
- 确认您知道如何配置并部署计算机云模板。



## 步骤

## 1 创建 SSH 主机自定义资源，以将 SSH 添加到云模板。

此步骤将自定义资源作为一种资源类型添加到云模板设计画布。

- a 在 vRealize Automation Cloud Assembly 中，选择**设计 > 自定义资源**，然后单击**新建自定义资源**。
- b 提供以下值。

请注意，除工作流名称外，这些值都是示例值。

表 6-2.

设置	示例值
名称	<b>SSH Host - DevOpsTesting Project</b> 这是显示在云模板资源类型调色板中的名称。
资源类型	<b>Custom.SSHHost</b> 资源类型必须以 <b>Custom.</b> 开头且每个资源类型必须唯一。 尽管未验证文本框中是否包含 <b>Custom.</b> ，但如果将其移除，会自动添加该字符串。 此资源类型将添加到设计画布，以便可以在云模板中使用。

- c 要在云模板资源类型列表中启用此资源类型，请验证**激活**选项是否已打开。
- d 选择使资源类型可用于 **DevOpsTesting** 项目的**范围**设置。
- e 选择定义资源的工作流。

设置	设置
生命周期操作 - 创建	选择 <b>添加 SSH 主机</b> 工作流。 如果您有多个 vRealize Orchestrator 集成，请在用于运行这些自定义资源的集成实例上选择工作流。 选择工作流后，“外部类型”下拉菜单将变得可用，并自动设置为 <b>SSH:Host</b> 。如果是共享资源，则只能使用一次外部源类型，而且每个项目只能使用一次。在此用例中，您将只为 <b>DevOpsTesting</b> 项目提供自定义资源。如果有其他工作流需要 <b>SSH:Host</b> 类型，则必须为每个项目创建单独的自定义资源。
生命周期操作 - 更新	选择 <b>更新 SSH 主机</b> 工作流。
生命周期操作 - 销毁	选择 <b>移除 SSH 主机</b> 工作流。

- f 查看结构定义键并在**属性**选项卡中键入值，以便了解工作流输入，从而可以在云模板中配置输入。该结构定义列出了工作流中定义的必需和可选输入值。必需输入值包含在云模板 YAML 中。

在**添加 SSH 主机**工作流中，hostname、port 和 username 都是必需的输入值。其他结构定义属性不是必需项。还可以使用结构定义确定要创建与其他字段值、工作流或操作绑定的位置。此用例中不包括绑定。

- g 要完成创建自定义资源，请单击**创建**。

## 2 创建云模板，以便在部署时添加 SSH 主机。

- a 选择**设计 > 云模板**，然后单击**新建自 > 空白画布**。
- b 将此云模板命名为 **Machine with SSH Host**。
- c 选择 **DevOpsTesting** 项目，然后单击**创建**。
- d 添加和配置 vSphere 计算机。
- e 从云模板设计页面左侧的“自定义资源”列表中，将 **SSH Host - DevOpsTesting Project** 资源类型拖动到画布上。

**注** 选择自定义资源的方法有两种：向下滚动，然后从左侧窗格中进行选择；在**搜索资源类型**文本框中进行搜索。如果自定义资源未显示，请单击**搜索资源类型**文本框旁边的刷新按钮。

系统会提醒该资源类型可用，因为它为该项目配置的。如果为其他项目创建云模板，则看不到该资源类型。

- f 在右侧，编辑 YAML 代码，以添加必需的输入值。

在代码中添加 inputs 部分，以便用户可在部署时提供用户名和主机名。在此示例中，端口默认值为 22。在以下示例中，其中一些值是示例数据。您的值可能会有所不同。

```
inputs:
  hostname:
    type: string
    title: The hostname of the SSH Host
  username:
    type: string
    title: Username
```

- g 在 resources 部分中，添加 `${input.input-name}` 代码以提示提供用户选择。

```
resources:
  Custom_SSHTHost_1:
    type: Custom.SSHTHost
    properties:
      port: 22
      hostname: '${input.hostname}'
      username: '${input.username}'
```

### 3 部署云模板。

- a 在云模板设计器页面上，单击**部署**。
- b 在**部署名称**中输入 **SSH Host Test**。
- c 选择**云模板版本**，然后单击**下一步**。
- d 完成部署输入。
- e 单击**部署**。

### 4 监控置备过程，以确保 SSH 主机包括在部署中。

- a 单击**部署**并找到 **SSH Host Test** 部署。
- b 监控请求的状态并验证部署是否成功。

#### 后续步骤

经过测试的云模板正常运行时，可以开始在其他云模板中使用 SSH Host 自定义资源。

## 如何在 vRealize Automation Cloud Assembly 中进行设计以为实施后更改做准备

除了已与 vRealize Automation Cloud Assembly 资源类型相关联的实施后操作，您还可以使用设计选项，提前为用户可能需要进行的自定义更新做准备。

---

**小心** 要更改部署，可以编辑其云模板并重新应用，也可以使用实施后操作。但是，在大多数情况下，应避免混合使用这两种方法。

打开/关闭电源等生命周期实施后更改通常是安全的，但其他更改则需要小心谨慎，例如添加磁盘时。

例如，如果混合使用这两种方法，先通过实施后操作添加磁盘，然后又重新应用云模板，则云模板可能会覆盖实施后更改，这可能会移除磁盘并导致数据丢失。

---

实施后准备工作可能包括直接使用云模板代码或 vRealize Automation Cloud Assembly 设计界面。

- 您可以在云模板代码中使用输入，以便在更新部署或已部署的资源时，界面会提示输入全新值。
- 您可以使用 vRealize Automation Cloud Assembly 根据 vRealize Orchestrator workflow 或操作来设计自定义操作。运行自定义操作将导致 vRealize Orchestrator 更改部署或部署的资源。

### 如何使用云模板输入进行 vRealize Automation 实施后操作更新

设计云模板时，实施后操作用户可利用 vRealize Automation 输入参数重新输入初始部署请求的选择。

---

**小心** 某些属性更改会导致重新创建资源。例如，更改 `Cloud.Service.Azure.App.Service` 下的 `connection_string.name` 会删除现有资源并创建一个新资源。

设计输入以支持实施后更改时，请决定是否允许删除和重新创建资源的输入。要了解哪些属性将重新创建资源，请访问结构定义链接：[有哪些 vRealize Automation 资源属性](#)。

---

有关如何创建输入的信息，请参见[用户输入如何在 vRealize Automation 中自定义云模板](#)。

有关具体的实施后操作示例，请参见以下部分。

### 如何将已部署的计算机移动到另一个网络

在维护部署和网络时，您可能需要能够重新放置部署了 vRealize Automation Cloud Assembly 的计算机。

例如，您可以先部署到测试网络，然后再迁移到生产网络。此处介绍的技术允许您预先设计云模板，以便为此类实施后操作做准备。请注意，计算机只是移动，不会被删除并重新部署。

此过程仅适用于 **Cloud.vSphere.Machine** 资源。对于部署到 vSphere 的云不可知的计算机，此过程不起作用。

#### 前提条件

- vRealize Automation Cloud Assembly 网络配置文件必须包含计算机将连接到的所有子网。在 vRealize Automation Cloud Assembly 中，您可以通过转到**基础架构 > 配置 > 网络配置文件**来检查网络。  
  
网络配置文件必须位于属于您的用户的相应 vRealize Automation Cloud Assembly 项目的帐户和区域中。
- 使用不同的标记标记两个子网。下面的示例假定标记名称分别为 **test** 和 **prod**。
- 部署的计算机必须保持相同的 IP 分配类型。在移动到另一个网络时，IP 无法从静态更改为 DHCP，反之亦然。

#### 步骤

- 1 在 vRealize Automation Cloud Assembly 中，转到**设计**，然后为部署创建云模板。
- 2 在代码的 **inputs** 部分中，添加一个可供用户选择网络的条目。

```
inputs:
  net-tagging:
    type: string
    enum:
      - test
      - prod
    title: Select a network
```

- 3 在代码的 **resources** 部分中，添加 **Cloud.Network** 并将 vSphere 计算机连接到该网络。
- 4 在 **Cloud.Network** 下，创建一个从 **inputs** 引用所选内容的限制。

```
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 继续进行设计，并按照通常的方式部署。在部署时，界面会提示您选择 **test** 或 **prod** 网络。
- 6 如果需要执行实施后更改，请转到**部署**，然后找到与云模板关联的部署。
- 7 在部署的右侧，单击**操作 > 更新**。
- 8 在“更新”面板中，界面会以相同的方式提示您选择 **test** 或 **prod** 网络。
- 9 要更改网络，请选择，单击**下一步**，然后单击**提交**。

## 如何创建 vRealize Automation Cloud Assembly 自定义操作以对虚拟机执行 vMotion

部署云模板后，可以运行实施后操作以对部署进行更改。vRealize Automation Cloud Assembly 包括许多实施后操作，但您可能希望提供其他操作。可以创建自定义资源操作，并将其作为实施后操作提供给用户。

自定义资源操作基于 vRealize Orchestrator 工作流。

以下自定义实施后操作示例旨在介绍创建过程。要有效地使用自定义操作，必须能够创建运行所需任务的 vRealize Orchestrator 工作流和操作。

### 前提条件

- 确认您已配置 vRealize Orchestrator 集成。请参见在 [Cloud Assembly 中配置 vRealize Orchestrator 集成](#)。
- 确认 vRealize Orchestrator 中存在用于实施后操作的工作流，并且成功运行。

### 步骤

- 1 创建一个自定义资源操作，使用 vMotion 将 vSphere 虚拟机从一个主机移至另一个主机。
  - a 在 vRealize Automation Cloud Assembly 中，选择**设计 > 资源操作**，然后单击**新建资源操作**。
  - b 提供以下值。

请注意，除工作流名称外，这些值都是示例值。

设置	示例值
名称	<b>vSphere_VM_vMotion</b> 这是显示在“资源操作”列表中的名称。
显示名称	<b>迁移虚拟机</b> 这是用户在“部署操作”菜单中看到的名称。

- c 单击**激活**选项，在“实施后操作”菜单中为与资源类型匹配的资源启用此操作。
- d 选择用于定义实施后操作的资源类型和工作流。

设置	示例值
资源类型	<p>选择 <b>Cloud.vSphere.Machine</b> 资源类型。</p> <p>这是部署为云模板组件的资源类型，但不一定是云模板中的资源。例如，您的云模板中可能存在云平台无关的计算机，但在 vCenter Server 上部署该计算机时，该计算机将为 <b>Cloud.vSphere.Machine</b>。由于该操作适用于已部署的类型，因此在定义自定义操作时，不要使用云平台无关的类型。</p> <p>在此示例中，vMotion 仅适用于 vSphere 计算机，但您可能需要在多个资源类型上运行其他操作。必须为每个资源类型创建一个操作。</p>
工作流	<p>选择<b>通过 vMotion 迁移虚拟机</b>工作流。</p> <p>如果您有多个 vRealize Orchestrator 集成，请在用于运行这些自定义资源操作的集成实例上选择工作流。</p>

- 2 创建 vRealize Orchestrator 属性与 vRealize Automation Cloud Assembly 结构定义属性的绑定。vRealize Automation Cloud Assembly 实施后操作支持三种类型的绑定。

绑定类型	说明
在请求中	默认值绑定类型。如果选择该选项，则会在请求表单中显示输入属性，并且用户必须在请求时提供其值。
使用绑定操作	<p>此选项仅适用于如下所示的引用类型输入：</p> <ul style="list-style-type: none"> <li>■ VC:VirtualMachine</li> <li>■ VC:Folder</li> </ul> <p>用户选择执行绑定的操作。所选操作必须返回与输入参数相同的类型。正确的属性定义为 \$ {properties.someProperty}。</p>
直接	此选项适用于使用基本数据类型的输入属性。如果选择该选项，将直接从输入属性的结构定义映射具有合适类型的属性。用户从结构定义树中选择属性。将禁用具有不同类型的属性。

在此用例中，绑定是一种 vRealize Orchestrator 操作，可在工作流中使用的 vRealize Orchestrator VC:VirtualMachine 输入类型与 vRealize Automation Cloud Assembly Cloud.vSphere.Machine 资源类型之间建立连接。通过设置绑定，对于请求对 vSphere VM 计算机执行 vMotion 操作的用户，您可无缝执行实施后操作。系统会在工作流中提供名称，这样用户无需执行此操作。

- a 选择**通过 vMotion 迁移虚拟机**工作流后，导航到**属性绑定**窗格。
- b 选择 vm 输入属性的绑定。

- c 在**绑定**下，选择**使用绑定操作**。

将自动选择 **findVcVmByVcAndVmUuid** 操作。此操作在 vRealize Automation Cloud Assembly 中预配置了 vRealize Orchestrator 集成。

- d 单击**保存**。

- 3 要将更改保存到实施后操作，请单击**创建**。

- 4 要考虑工作流中的其他输入参数，可以自定义用户在请求操作时看到的请求表单。

- a 从**资源操作**中，选择最近创建的**实施后操作**。
- b 单击**编辑请求参数**。

可以自定义向用户显示请求页面的方式。

默认字段名称	外观	值	限制
虚拟机的目标资源池。默认为当前资源池。	<ul style="list-style-type: none"> <li>■ 标签 = 目标资源池</li> <li>■ 显示类型 = 值选择器</li> </ul>		
要将虚拟机迁移到的目标主机	<ul style="list-style-type: none"> <li>■ 标签 = 目标主机</li> <li>■ 显示类型 = 值选择器</li> </ul>		必需 = 是
迁移任务的优先级	标签 = 任务的优先级	值选项 <ul style="list-style-type: none"> <li>■ 值源 = 常数</li> </ul> 在文本框中，输入逗号分隔列表。 <pre>lowPriority Low,defaultPriority Default,highPriority High</pre>	必需 = 是
(可选) 仅当虚拟机的打开电源状态符合指定的状态时才迁移虚拟机	删除此文本框。 <b>vMotion</b> 可移动处于任何电源状态的计算机。		

- c 单击**保存**。

- 5 要限制操作可用的时间，可以配置条件。

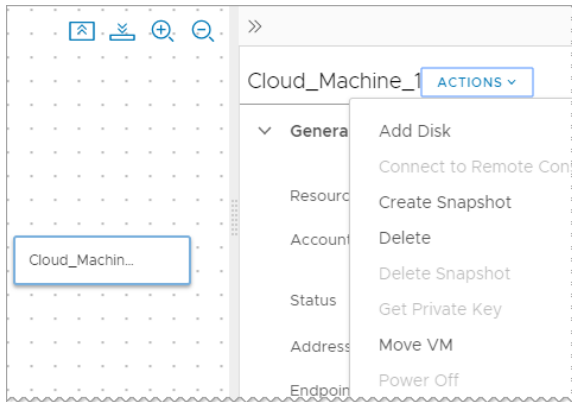
例如，您只希望 vMotion 操作在计算机有四个或更少的 CPU 时可用。

- a 打开**需要条件**。
- b 输入条件。

Key	运算符	值
<code>\${properties.cpuCount}</code>	lessThan	4

- c 单击**更新**。

- 6 验证“迁移虚拟机”操作是否可用于符合条件的已部署计算机。
  - a 选择部署。
  - b 找到包含与已定义条件匹配的已部署计算机的部署。
  - c 打开该部署并选择计算机。
  - d 在右侧窗格中单击“操作”，然后确认存在 Move VM 操作。



- e 运行该操作。

## 如何使用可扩展性扩展应用程序生命周期并实现自动化

可以将可扩展性操作或 vRealize Orchestrator 工作流与可扩展性订阅一起使用来扩展应用程序生命周期。

借助 vRealize Automation Cloud Assembly 可扩展性，您可以使用订阅为事件分配可扩展性操作或 vRealize Orchestrator 工作流。发生指定的事件时，订阅将启动该操作或工作流以使其运行，并通知所有订阅者。

### 可扩展性操作

可扩展性操作是小型的轻量级代码脚本，用于指定操作和操作执行方式。可以从预定义的 vRealize Automation Cloud Assembly 操作模板或从 ZIP 文件导入可扩展性操作。您还可以使用操作编辑器为您的可扩展性操作创建自定义脚本。在一个脚本中将多个操作脚本链接到一起时，就创建了一个操作流。通过使用操作流，可以创建操作序列。有关使用操作流的信息，请参见[操作流是什么](#)。

### vRealize Orchestrator 工作流

通过将 vRealize Automation Cloud Assembly 与现有的 vRealize Orchestrator 环境相集成，您可以在可扩展性订阅中使用工作流。

### 可扩展性操作订阅

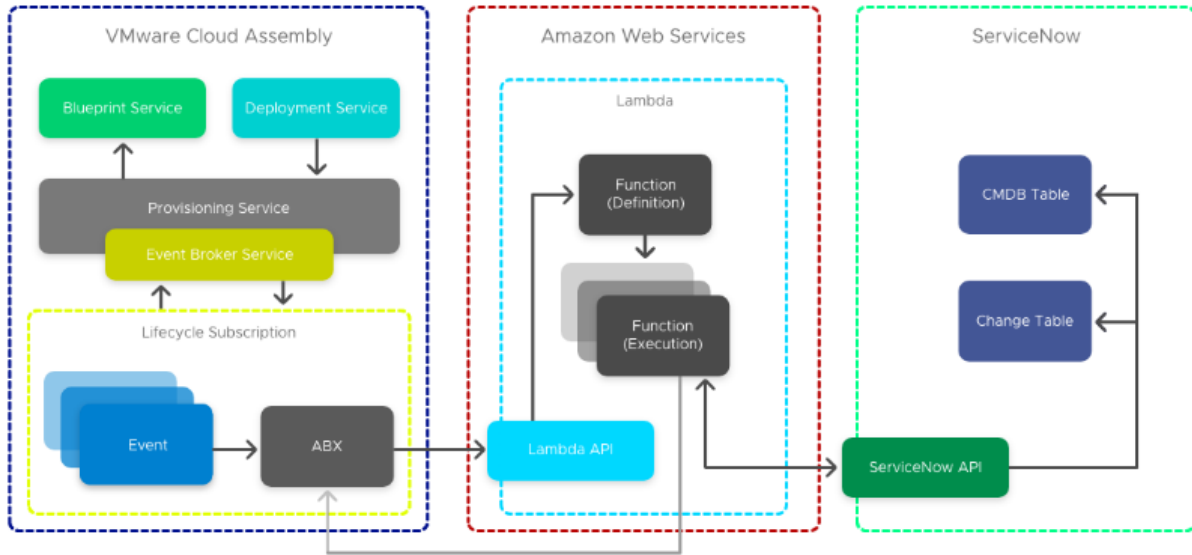
可以为 vRealize Automation Cloud Assembly 订阅分配可扩展性操作，以扩展应用程序生命周期。

**注** 以下订阅只是一些用例示例，未涵盖所有可扩展性操作功能。



## 如何使用可扩展性操作将 Cloud Assembly 与 ServiceNow 集成

使用可扩展性操作，可以将 vRealize Automation Cloud Assembly 与企业 ITSM（例如 ServiceNow）集成。

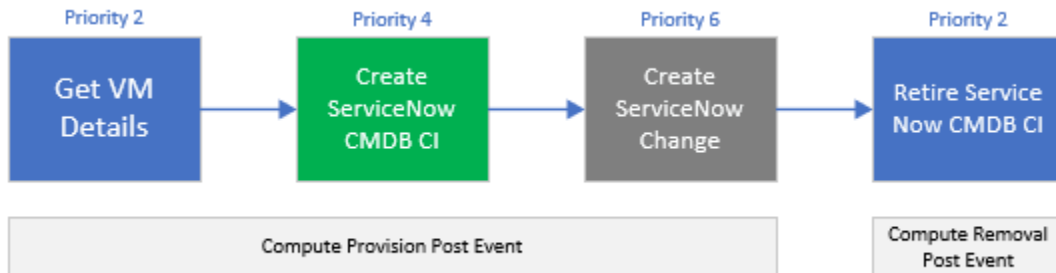


企业用户通常将其云计算管理平台与 IT 服务管理 (IT Service Management, ITSM) 和配置管理数据库 (Configuration Management Database, CMDB) 平台集成以实现合规性。按照此示例，可以使用可扩展性操作脚本将 vRealize Automation Cloud Assembly 与适用于 CMDB 和 ITSM 的 ServiceNow 集成。

**注** 还可以使用 vRealize Orchestrator workflows 将 ServiceNow 与 vRealize Automation Cloud Assembly 集成。有关使用 workflows 集成 ServiceNow 的信息，请参见[如何使用 vRealize Orchestrator workflows 将适用于 ITSM 的 Cloud Assembly 与 ServiceNow 集成](#)。

要创建此集成，需要使用四个可扩展性操作脚本。在置备期间，前三个脚本在发生计算资源置备后事件时按顺序启动。第四个脚本在发生计算资源移除后事件时触发。

有关事件主题的详细信息，请参阅[随 vRealize Automation Cloud Assembly 提供的事件主题](#)。



### 获取虚拟机详细信息

“获取虚拟机详细信息”脚本可获取创建 CI 所需的其他负载详细信息，以及存储在 Amazon Web Services Systems Manager 参数存储 (SSM) 中的标识令牌。此外，此脚本还可以使用其他属性更新 customProperties 供以后使用。

### 创建 ServiceNow CMDB CI

“创建 ServiceNow CMDB CI”脚本将 ServiceNow 实例 URL 作为输入传递，并将实例存储在 SSM 中以满足安全要求。此脚本还会读取 ServiceNow CMDB 唯一记录标识符响应 (sys\_id)。此脚本将该响应作为输出传递，并在创建期间写入自定义属性 serviceNowSysId。此值用于在销毁实例时将 CI 标记为已注销。

---

**注** 可能需要向 vRealize Automation services Amazon Web Services 角色分配其他权限，以允许 Lambda 访问 SSM 参数存储。

---

### 创建 ServiceNow 变更

此脚本通过将 ServiceNow 实例 URL 作为输入传递，并将 ServiceNow 凭据存储在 SSM 中以满足安全要求，完成 ITSM 集成。

### 创建 ServiceNow 变更

“注销 ServiceNow CMDB CI”脚本根据在创建脚本中创建的自定义属性 serviceNowSysId 提示 ServiceNow 停止并将 CI 标记为已注销。

### 前提条件

- 配置此集成之前，筛选具有条件云模板属性的所有事件订阅：

```
event.data["customProperties"]["enable_servicenow"] == "true"
```

---

**注** 此属性存在于需要 ServiceNow 集成的云模板上。

---

- 下载并安装 Python。

有关筛选订阅的详细信息，请参见[创建可扩展性订阅](#)。

### 步骤

- 从虚拟机打开命令提示符。
- 运行“获取虚拟机详细信息”脚本。

```
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 = baseUrl + "/iaas/machines/" + resourceId
headers = {"Accept":"application/json","Content-Type":"application/json",
"Authorization":bearer }
resultMachine = requests.get(machineUri,headers=headers)
print("machine: " + resultMachine.text)

print( "serviceNowCPUCount: " + json.loads(resultMachine.text)["customProperties"]
["cpuCount"] )
print( "serviceNowMemoryInMB: " + json.loads(resultMachine.text)["customProperties"]
["memoryInMB"] )

#update customProperties
outputs = {}
outputs['customProperties'] = inputs['customProperties']
outputs['customProperties']['serviceNowCPUCount'] = int(json.loads(resultMachine.text)
["customProperties"]["cpuCount"])
outputs['customProperties']['serviceNowMemoryInMB'] = json.loads(resultMachine.text)
["customProperties"]["memoryInMB"]
return outputs

```

### 3 运行 CMDB 配置项创建操作。

```

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 运行创建操作脚本。

```

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)

```

#### 结果

vRealize Automation Cloud Assembly 已成功与 ITSM ServiceNow 集成。

## 后续步骤

如果需要，可以使用 CMDB 配置项注销操作注销 CI:

```
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)
```

有关如何使用可扩展性操作在 vRealize Automation Cloud Assembly 中集成 ServiceNow 的更多信息，请参见 [ServiceNow 集成使用基于操作的可扩展性扩展 Cloud Assembly](#)。

## 如何使用可扩展性操作在置备期间标记虚拟机

您可以将可扩展性操作与订阅配合使用，以自动执行和简化标记虚拟机操作。

作为云管理员，您可以使用可扩展性操作和可扩展性订阅来创建使用指定的输入和输出自动标记的部署。针对包含“标记虚拟机”订阅的项目创建新部署时，部署事件将触发并运行“标记虚拟机”脚本，并且会自动应用标记。这样可以节省时间并提高效率，同时还可以简化部署管理。

## 前提条件

- 对云管理员凭据的访问权限。
- Lambda 函数的 Amazon Web Services 角色。

## 步骤

- 1 导航到 **可扩展性 > 库 > 操作 > 新建操作**，然后使用以下参数创建操作。

参数	说明
操作名称	可扩展性操作名称，最好以 <b>TagVM</b> 作为前缀或后缀。
项目	要针对其测试可扩展性操作的项目。

参数	说明
操作模板	<b>Tag VM</b>
运行时	Python
脚本源代码	编写脚本

2 输入 **Handler** 作为主函数。

3 添加标记输入以用于测试可扩展性操作。

例如, `resourceNames = ["DB_VM"]` 和 `target = world`。

4 要保存操作, 单击**保存**。

5 要测试操作, 单击**测试**。

6 要退出操作编辑器, 单击**关闭**。

7 导航到**可扩展性 > 订阅**。

8 单击**新建订阅**。

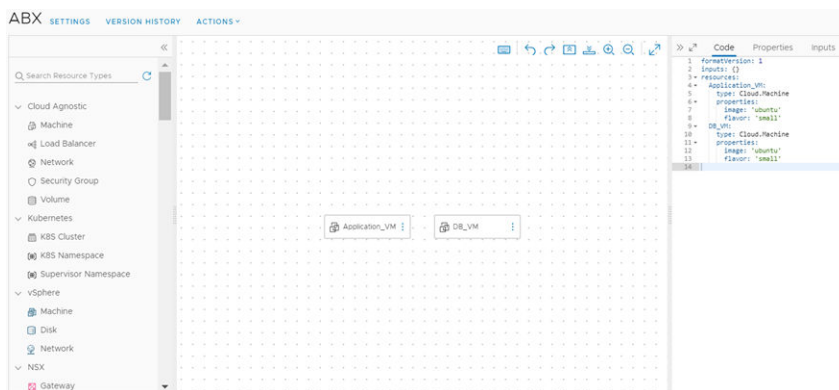
9 输入以下订阅详细信息。

详细信息	设置
事件主题	选择与虚拟机的标记阶段相关的事件主题。例如, 计算资源分配。 <b>注</b> 标记必须是所选事件主题的事件参数的一部分。
阻止	将订阅的超时设置为 1 分钟。
操作/工作流	选择可扩展性操作可运行类型, 然后选择自定义可扩展性操作。

10 要保存自定义可扩展性操作订阅, 单击**保存**。

11 导航到**设计 > 云模板**, 然后从空白画布创建云模板。

12 将两个虚拟机添加到云模板: `Application_VM` 和 `DB_VM`。



- 13 要部署虚拟机，单击**部署**。
- 14 在部署过程中，验证事件是否已启动，并验证可扩展性操作是否已运行。
- 15 要验证标记是否正确应用，导航到**基础架构 > 资源 > 计算机**。

### 了解有关可扩展性操作的更多信息

基于操作的可扩展性在 vRealize Automation Cloud Assembly 中使用简化的代码脚本自动执行可扩展性操作。

基于操作的可扩展性提供轻型灵活的运行时引擎接口，您可以在其中定义可编写脚本的小型操作并将其配置为在发生可扩展性订阅中指定的事件时启动。

您可以在 vRealize Automation Cloud Assembly 或本地环境中创建这些可扩展性操作代码脚本，并将其分配给订阅。可使用可扩展性操作脚本实现更轻型、更简单的任务和步骤自动化。有关将 vRealize Automation Cloud Assembly 与 vRealize Orchestrator 服务器集成的详细信息，请参见在 [Cloud Assembly 中配置 vRealize Orchestrator 集成](#)。

基于操作的可扩展性具有以下优势：

- 可取代 vRealize Orchestrator 工作流，使用小型且可重用的可编写脚本的操作实现轻型集成和自定义。
- 提供一种方法，可用于重用包含可重用的参数化操作的操作模板。

可以通过编写用户定义的操作脚本代码或将预定义的脚本代码导入为 ZIP 包来创建可扩展性操作。基于操作的可扩展性支持 Node.js、Python 和 PowerShell 运行时环境。Node.js 和 Python 运行时依赖于 Amazon Web Services Lambda。因此，您必须使用一个具有 Amazon Web Services 身份与访问管理 (IAM) 的有效订阅，并将 Amazon Web Services 配置为 vRealize Automation Cloud Assembly 中的端点。有关 Amazon Web Services Lambda 入门的信息，请参见 [ABX: Cloud Assembly 服务的无服务器可扩展性](#)。

---

**注** 可扩展性操作是特定于项目的。

---

### 如何创建可扩展性操作

使用 vRealize Automation Cloud Assembly，您可以创建可扩展性操作，以便在可扩展性订阅中使用。

可扩展性操作是高度可自定义、轻型且灵活的方法，用于通过用户定义的脚本代码和操作模板扩展应用程序生命周期。操作模板包含预定义的参数，这些参数帮助构成了可扩展性操作的基础。

以下两种方法可用于创建可扩展性操作：

- 为可扩展性操作脚本编写用户定义的代码。

---

**注** 在可扩展性操作编辑器中编写用户定义的代码时，可能需要有效的 Internet 连接。

---

- 为可扩展性操作导入 ZIP 软件包格式的部署软件包。有关为可扩展性操作创建 ZIP 软件包的信息，请参见 [为 Python 运行时可扩展性操作创建 ZIP 软件包](#)、[为 Node.js 运行时可扩展性操作创建 ZIP 软件包](#)或为 [PowerShell 运行时可扩展性操作创建 ZIP 软件包](#)。

以下步骤介绍了创建使用 Amazon Web Services 作为 FaaS 提供程序的可扩展性操作的过程。

## 前提条件

- 具备活动且有效项目中的成员资格。
- 已为 Lambda 函数配置 Amazon Web Services 角色。例如，AWSLambdaBasicExecutionRole。
- 已启用云管理员角色或 iam:PassRole 权限。

## 步骤

- 1 选择**可扩展性 > 库 > 操作**。
- 2 单击**新建操作**。
- 3 输入操作的名称，然后选择一个项目。
- 4 单击**下一步**。
- 5 搜索并选择操作模板。

---

**注** 要在不使用操作模板的情况下创建自定义操作，请选择**自定义脚本**。

---

此时将显示新的可配置参数。

- 6 选择**编写脚本**或**导入软件包**。
- 7 选择操作运行时。
- 8 为操作的入口点输入 **主函数**名称。

---

**注** 对于从 ZIP 软件包导入的操作，主函数还必须包括含入口点的脚本文件的名称。例如，如果主脚本文件的标题为 main.py，并且输入点为 handler (context, inputs)，则主函数的名称必须为 *main.handler*。

---

- 9 定义操作的**输入**和**输出**参数。
- 10 （可选）将应用程序依赖关系添加到操作。

---

**注** 对于 PowerShell 脚本，可以定义应用程序依赖关系，以便根据 PowerShell Gallery 存储库进行解析。要定义您的应用程序依赖关系以便可从公共存储库解析，请使用以下格式：

```
@{
    Name = 'Version'
}

e.g.

@{
    Pester = '4.3.1'
}
```

---

**注** 对于从 ZIP 软件包导入的操作，将自动添加应用程序依赖关系。

---

- 11 要定义超时和内存限制，请启用**设置自定义超时和限制**选项。



**12** 要测试操作，请单击**保存**，然后单击**测试**。

### 后续步骤

创建并验证可扩展性操作后，便可将其分配给订阅。

**注** 可扩展性订阅使用可扩展性操作的最新发布版本。创建新版本的操作后，请单击编辑器窗口右上角的**版本**。要发布您打算在订阅中使用的操作的版本，单击**发布**。

为 Python 运行时可扩展性操作创建 ZIP 软件包

可以创建一个包含 vRealize Automation Cloud Assembly 可扩展性操作所用 Python 脚本和依赖关系的 ZIP 软件包。

为可扩展性操作构建脚本的方法有两种：

- 在 vRealize Automation Cloud Assembly 的可扩展性操作编辑器中直接编写脚本。
- 在本地环境中创建脚本，然后将其与任何相关依赖关系一起添加到 ZIP 软件包。

通过使用 ZIP 软件包，可以为操作脚本和依赖关系创建自定义的预配置模板，然后可以将其导入到 vRealize Automation Cloud Assembly，以便在可扩展性操作中使用。

另外，如果与操作脚本中的依赖关系相关联的模块无法由 vRealize Automation Cloud Assembly 服务解析，例如，环境中缺少 Internet 访问权限，也可以使用 ZIP 软件包。

此外，还可以使用 ZIP 软件包创建包含多个 Python 脚本文件的可扩展性操作。使用多个脚本文件有助于组织可扩展性操作代码的结构。

### 前提条件

如果使用的是 Python 3.3 或更低版本，请下载并配置 PIP 软件包安装程序。请参见 [Python 软件包索引](#)。

### 步骤

- 1** 在本地计算机上，为操作脚本和依赖关系创建一个文件夹。

例如，/home/user1/zip-action。

- 2** 将一个或多个主 Python 操作脚本添加到该文件夹。

例如，/home/user1/zip-action/main.py。

### 3 （可选）将 Python 脚本的任何依赖关系添加到该文件夹。

- a 创建包含依赖关系的 `requirements.txt` 文件。请参见[要求文件](#)。
- b 打开 Linux shell。

---

**注** vRealize Automation Cloud Assembly 中基于操作的可扩展性的运行时基于 Linux。因此，在 Windows 环境中编译的任何 Python 依赖关系可能会导致生成的 ZIP 软件包无法用于创建可扩展性操作。因此，必须使用 Linux shell。

---

- c 运行以下命令，在脚本文件夹中安装 `requirements.txt` 文件：

```
pip install -r requirements.txt --target=home/user1/zip-action
```

### 4 在分配的文件夹中，选择您的脚本元素以及（如果适用）`requirements.txt` 文件并将其压缩为 ZIP 软件包。

---

**注** 脚本元素和依赖关系元素必须存储在 ZIP 软件包的根级别。在 Linux 环境中创建 ZIP 软件包时，可能会遇到软件包内容未存储在根级别的问题。如果遇到此问题，请通过在命令行 shell 中运行 `zip -r` 命令来创建软件包。

---

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

## 后续步骤

使用 ZIP 软件包创建可扩展性操作脚本。请参见[如何创建可扩展性操作](#)。

为 Node.js 运行时可扩展性操作创建 ZIP 软件包

可以创建一个包含 vRealize Automation Cloud Assembly 可扩展性操作所用 Node.js 脚本和依赖关系的 ZIP 软件包。

为可扩展性操作构建脚本的方法有两种：

- 在 vRealize Automation Cloud Assembly 的可扩展性操作编辑器中直接编写脚本。
- 在本地环境中创建脚本，然后将其与任何相关依赖关系一起添加到 ZIP 软件包。

通过使用 ZIP 软件包，可以为操作脚本和依赖关系创建自定义的预配置模板，然后可以将其导入到 vRealize Automation Cloud Assembly，以便在可扩展性操作中使用。

另外，如果与操作脚本中的依赖关系相关联的模块无法由 vRealize Automation Cloud Assembly 服务解析，例如，环境中缺少 Internet 访问权限，也可以使用 ZIP 软件包。

此外，还可以使用软件包创建包含多个 Node.js 脚本文件的可扩展性操作。使用多个脚本文件有助于组织可扩展性操作代码的结构。

**步骤**

- 1 在本地计算机上，为操作脚本和依赖关系创建一个文件夹。

例如，/home/user1/zip-action。

- 2 将一个或多个主 Node.js 操作脚本添加到该文件夹。

例如，/home/user1/zip-action/main.js。

- 3 （可选）将 Node.js 脚本的任何依赖关系添加到该文件夹。

- a 在脚本文件夹中创建包含依赖关系的 package.json 文件。请参见[创建 package.json 文件](#)和在 [package.json 文件中指定 dependencies 和 devDependencies](#)。

- b 打开命令行 shell。

- c 导航到为操作脚本和依赖关系创建的文件夹。

```
cd /home/user1/zip-action
```

- d 运行以下命令，在脚本文件夹中安装 package.json 文件：

```
npm install --production
```

---

**注** 此命令会在文件夹中创建 node\_modules 目录。

---

- 4 在分配的文件夹中，选择您的脚本元素以及（如果适用）node\_modules 目录并将其压缩为 ZIP 软件包。

---

**注** 脚本元素和依赖关系元素必须存储在 ZIP 软件包的根级别。在 Linux 环境中创建 ZIP 软件包时，可能会遇到软件包内容未存储在根级别的问题。如果遇到此问题，请通过在命令行 shell 中运行 `zip -r` 命令来创建软件包。

---

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

---

**后续步骤**

使用 ZIP 软件包创建可扩展性操作脚本。请参见[如何创建可扩展性操作](#)。

为 PowerShell 运行时可扩展性操作创建 ZIP 软件包

可以创建包含 PowerShell 脚本和依赖关系模块的 ZIP 软件包，以便在可扩展性操作中使用。

为可扩展性操作构建脚本的方法有两种：

- 在 vRealize Automation Cloud Assembly 的可扩展性操作编辑器中直接编写脚本。
- 在本地环境中创建脚本，然后将其与任何相关依赖关系一起添加到 ZIP 软件包。

通过使用 ZIP 软件包，可以为操作脚本和依赖关系创建自定义的预配置模板，然后可以将其导入到 vRealize Automation Cloud Assembly，以便在可扩展性操作中使用。

---

**注** 无需将 PowerCLI cmdlet 定义为依赖关系或将其捆绑到 ZIP 软件包。PowerCLI cmdlet 预配置了 vRealize Automation Cloud Assembly 服务的 PowerShell 运行时。

---

另外，如果与操作脚本中的依赖关系相关联的模块无法由 vRealize Automation Cloud Assembly 服务解析，例如，环境中缺少 Internet 访问权限，也可以使用 ZIP 软件包。

此外，还可以使用 ZIP 软件包创建包含多个 PowerShell 脚本文件的可扩展性操作。使用多个脚本文件有助于组织可扩展性操作代码的结构。

### 前提条件

确认您熟悉 PowerShell 和 PowerCLI。可以在 [Docker Hub](#) 找到具有 PowerShell Core、PowerCLI 10、PowerNSX 以及多个社区模块和脚本示例的 Docker 映像。

### 步骤

- 1 在本地计算机上，为操作脚本和依赖关系创建一个文件夹。

例如，/home/user1/zip-action。

- 2 向文件夹中添加扩展名为 .psm1 的主 PowerShell 脚本。

以下脚本提供了一个称为 main.psm1 的简单 PowerShell 函数：

```
function handler($context, $payload) {  
  
    Write-Host "Hello " $payload.target  
  
    return $payload  
}
```

---

**注** PowerShell 可扩展性操作的输出基于函数正文中显示的最后一个变量。所含函数中的所有其他变量都将放弃。

---

- 3 （可选）使用 context 参数将代理配置添加到您的主 PowerShell 脚本中。请参见[使用上下文参数在 PowerShell 脚本中添加代理配置](#)。

#### 4 （可选）添加 PowerShell 脚本的任何依赖关系。

**注** 您的 PowerShell 依赖关系脚本必须使用 .psm1 扩展名。请对脚本和保存脚本的子文件夹使用相同的名称。

- a 登录到 Linux PowerShell shell。

**注** vRealize Automation Cloud Assembly 中基于操作的可扩展性的运行时基于 Linux。在 Windows 环境中编译的任何 PowerShell 依赖关系可能会导致生成的 ZIP 软件包不可用。任何已安装的第三方依赖关系必须与 VMware Photon OS 兼容，因为 PowerShell 脚本在 Photon OS 上运行。

- b 导航到 /home/user1/zip-action 文件夹。
- c 通过运行 Save-Module cmdlet，下载并保存包含依赖关系的 PowerShell 模块。

```
Save-Module -Name <module name> -Path ./
```

- d 对任何其他依赖关系模块重复之前的子步骤。

**重要说明** 确认每个依赖关系模块位于单独的子文件夹中。有关编写和管理 PowerShell 模块的详细信息，请参见[如何编写 PowerShell 脚本模块](#)。

#### 5 在分配的文件夹中，选择您的脚本元素以及（如果适用）依赖关系模块子文件夹并将其压缩为 ZIP 软件包。

**注** 脚本和依赖关系模块子文件夹必须存储在 ZIP 软件包的根级别。在 Linux 环境中创建 ZIP 软件包时，可能会遇到软件包内容未存储在根级别的问题。如果遇到此问题，请通过在命令行 shell 中运行 `zip -r` 命令来创建软件包。

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

#### 后续步骤

使用 ZIP 软件包创建可扩展性操作脚本。请参见[如何创建可扩展性操作](#)。

使用上下文参数在 PowerShell 脚本中添加代理配置

您可以使用 `context` 参数在 PowerShell 脚本中启用网络代理通信。

某些 PowerShell cmdlet 可能要求您在 PowerShell 函数中将网络代理设置为环境变量。代理配置将通过 `$context.proxy.host` 和 `$context.proxy.port` 参数提供给 PowerShell 函数。

您可以在 PowerShell 脚本的开头添加这些 `context` 参数。

```
$proxyString = "http://" + $context.proxy.host + ":" + $context.proxy.port
$Env:HTTP_PROXY = $proxyString
$Env:HTTPS_PROXY = $proxyString
```

如果 cmdlet 支持 `-Proxy` 参数，您也可以直接将代理值传递到特定的 PowerShell cmdlet。

配置特定于云的可扩展性操作

可以将可扩展性操作配置为与您的云帐户配合使用。

当创建可扩展性操作时，可以配置该操作并将其链接到各个云端帐户：

- Microsoft Azure
- Amazon Web Services

#### 前提条件

需要有效的云帐户。

#### 步骤

- 1 选择**可扩展性 > 库 > 操作**。
- 2 单击**新建操作**。
- 3 根据需要输入操作参数。
- 4 在 **FaaS 提供程序** 下拉菜单中，选择您的云帐户提供程序或选择**自动**。

---

**注** 如果选择**自动**，操作会自动定义 FaaS 提供商。

---

- 5 单击**保存**。

#### 结果

可扩展性操作已链接，可与配置的云帐户配合使用。

配置内部部署可扩展性操作

您可以将可扩展性操作配置为使用内部部署 FaaS 提供程序，而不是 Amazon Web Services 或 Microsoft Azure 云帐户。

通过使用内部部署 FaaS 提供程序来执行可扩展性操作，您可以在 vRealize Automation Cloud Assembly 可扩展性订阅中使用内部部署服务，例如 LDAP、CMDB 或 vCenter 数据中心。

#### 步骤

- 1 选择**可扩展性 > 库 > 操作**。
- 2 单击**新建操作**。
- 3 输入可扩展性操作的名称和项目。
- 4 （可选）输入可扩展性操作的描述。
- 5 单击**下一步**。
- 6 创建或导入您的可扩展性操作脚本。
- 7 单击 **FaaS 提供程序** 下拉菜单，然后选择**内部部署**。
- 8 要保存新的可扩展性操作，单击**保存**。

## 后续步骤

在 vRealize Automation Cloud Assembly 可扩展性订阅中使用创建的可扩展性操作。

### 创建共享可扩展性操作

作为 vRealize Automation Cloud Assembly 管理员，您可以创建可扩展性操作，并且无需导出和导入，即可在项目之间共享这些操作。

有关导出和导入可扩展性操作的信息，请参见[导出和导入可扩展性操作](#)。

### 前提条件

在 vRealize Automation Cloud Assembly 组织中创建两个或更多项目。

### 步骤

- 1 选择**可扩展性 > 库 > 操作**。
- 2 单击**新建操作**。
- 3 输入可扩展性操作的名称。
- 4 （可选）输入可扩展性操作的说明。
- 5 选择要在其中创建可扩展性操作的项目。
- 6 勾选**与此组织中的所有项目共享**复选框。
- 7 单击**下一步**。
- 8 创建或导入操作脚本，并保存可扩展性操作。

---

**注** 您可以在**设置**中启用或禁用共享。如果在订阅中使用可扩展性操作，则无法禁用共享。要禁用共享，必须从您的订阅中移除可扩展性操作。

---

- 9 创建可扩展性订阅，添加共享可扩展性操作，并将订阅范围设置为**任何项目**。

---

**注** 有关创建可扩展性订阅的更多信息，请参见[创建可扩展性订阅](#)。

---

可扩展性订阅是通过匹配任意项目中的事件来触发的。

## 后续步骤

您还可以在 vRealize Automation Service Broker 目录中将共享可扩展性操作作为内容源导入。选择源项目时，输入在其中创建可扩展性操作的项目。有关将可扩展性操作添加到 vRealize Automation Service Broker 的详细信息，请参见[将可扩展性操作添加到 Service Broker 目录中](#)。

### 导出和导入可扩展性操作

使用 vRealize Automation Cloud Assembly，您可以导出和导入可扩展性操作以在不同的项目中使用。

### 前提条件

现有的可扩展性操作。

## 步骤

### 1 导出可扩展性操作。

- a 导航到**可扩展性 > 库 > 操作**。
- b 选择一个可扩展性操作，然后单击**导出**。

操作脚本及其依赖项以 ZIP 文件的形式保存在本地环境中。

### 2 导入可扩展性操作。

- a 导航到**可扩展性 > 库 > 操作**。
- b 单击**导入**。
- c 选择导出的可扩展性操作并将其分配给项目。
- d 单击**导入**。

---

**注** 如果导入的可扩展性操作已分配给指定的项目，系统会提示您选择冲突解决策略。

---

---

**备选方法** 您还可以直接从操作编辑器中选择**导入软件包**选项来导入操作脚本。

---

## 操作流是什么

操作流是一组可扩展性操作脚本，用于进一步扩展生命周期并自动化。

所有操作流均以 flow\_start 开头，并以 flow\_end 结尾。可以通过使用以下操作流元素将多个可扩展性操作脚本链接在一起：

- **顺序操作流** - 多个可扩展性操作脚本按顺序运行。
- **分叉操作流** - 多个可扩展性操作脚本或操作流拆分为多个路径并构成相同的输出。
- **联接操作流** - 多个可扩展性操作脚本或操作流联接到一起并构成相同的输出。
- **条件操作流** - 多个可扩展性操作脚本或操作流在满足某个条件后运行。

### 顺序操作流



多个可扩展性操作脚本按顺序运行。

```
version: "1"
flow:
  flow_start:
    next: action1
  action1:
    action: <action_name>
    next: action2
  action2:
    action: <action_name>
    next: flow_end
```

**注** 通过将前一个操作分配为 `next:` 操作，可以循环回到前一个操作。例如，在此示例中，输入 `next: action1` 可以重新运行 **action1** 并重新开始操作序列，而不要输入 `next: flow_end`。

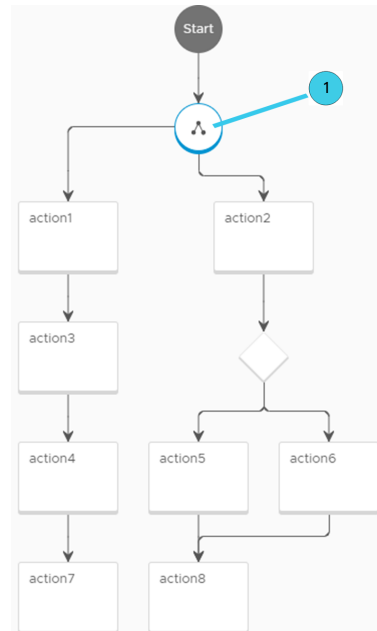


分叉操作流

多个可扩展性操作脚本或操作流拆分路径以构成相同的输出。

```
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>
```

**注** 通过将前一个操作分配为 `next: 操作`，可以循环回到前一个操作。例如，输入 `next: action1` 可以重新运行 **action1** 并重新开始操作序列，而不要输入 `next: flow_end` 来结束操作流。



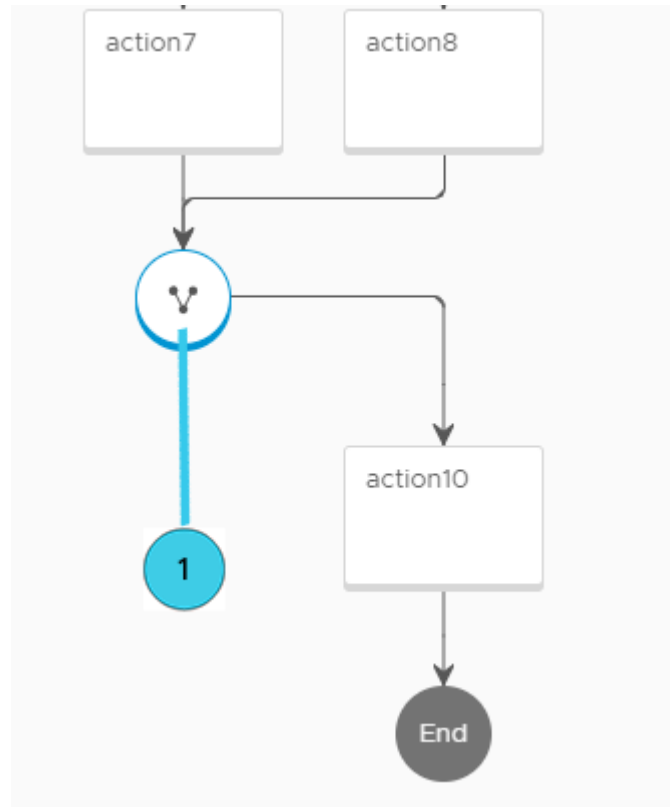
① 分叉元素

## 联接操作流

多个可扩展性操作脚本或操作流将路径联接到一起并构成相同的输出。

```
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
```

**注** 通过将前一个操作分配为 `next: 操作`，可以循环回到前一个操作。例如，在此示例中，输入 `next: action1` 可以重新运行 **action1** 并重新开始操作序列，而不要输入 `next: flow_end`。



① 联接元素

### 条件操作流

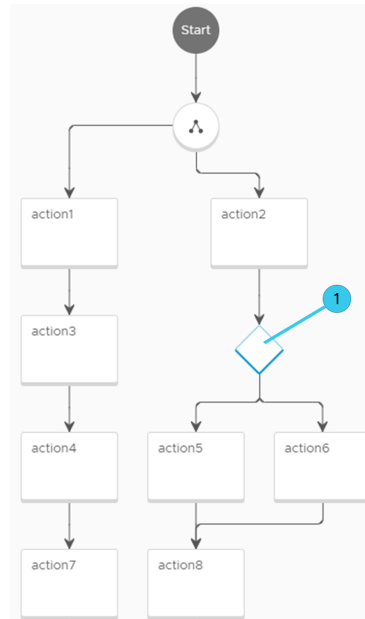
在使用开关元素满足某个条件时运行的多个可扩展性操作脚本或操作流。

在某些情况下，条件必须为 `true`，操作才能运行。而在其他情况下，如此示例中所示，必须满足参数值，操作才能运行。如果不满足任何条件，操作流将失败。

```

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 开关元素

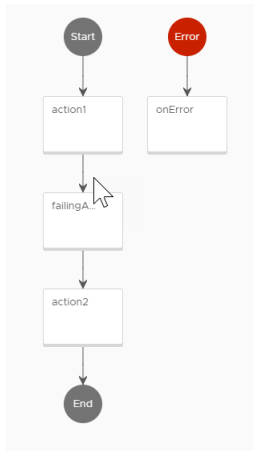
**注** 通过将前一个操作分配为 `next` 操作，可以循环回到前一个操作。例如，输入 `next: action1` 可以重新运行 **action1** 并重新开始操作序列，而不要输入 `next: flow_end` 来结束操作流。

## 如何将错误处理程序与操作流配合使用

您可以配置操作流，以在流程的指定阶段使用错误处理程序元素发出错误。

错误处理程序元素需要以下两个输入：

- 为失败操作指定的错误消息。
- 操作流输入。



如果流程中的某个操作失败并且操作流包含错误处理程序元素，则会发出错误消息以提醒您操作失败。错误处理程序自己执行操作。以下脚本是可在操作流中使用的错误处理程序的示例。

```
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
```

可以在“操作运行”窗口中查看成功和失败的运行。

状态	操作	运行 ID
已完成	AWS-ABX	8a7682b66df80a17016e115a3ef50c06
失败	AWS-ABX	8a7682b66df80a17016e1159db240c02
已完成	AWS-ABX	8a7682b66df80a17016e115612a40bfc
已完成	AWS-ABX	8a769ecc6df809c7016e1154c6f10c07

在此示例中，**flow-with-handler** 操作流包含一个错误处理程序元素，并且已成功运行。但是，该流程的其中一个操作已失败，从而启动了错误处理程序以发出错误。

## 如何跟踪操作运行

“操作运行”选项卡显示订阅触发的可扩展性操作及其状态的日志。

可以使用**可扩展性 > 活动 > 操作运行**来查看操作运行的日志。此外，还可以一次按一个或多个属性筛选操作运行的列表。要查看各次操作运行的其他详细信息，请单击运行 ID。

### 对失败的可扩展性操作运行进行故障排除

如果您的可扩展性操作运行失败，则可以执行故障排除步骤以更正该问题。

当操作运行失败时，您可能会收到错误消息、失败状态和失败日志。如果操作运行失败，则可能是由于部署或代码故障造成的。

问题	解决方案
部署故障	这些失败是与云帐户配置、操作部署或其他可能阻止该操作部署的依赖关系相关的问题造成的。确保您使用的项目是在配置的云帐户内定义的，并且已授予运行功能的权限。在重新启动该操作之前，您可以针对该操作的详细信息页面中的特定项目测试操作。
代码故障	这些故障是由于脚本或代码无效所致。使用“操作”运行日志对无效脚本进行故障排除和更正。

## 可扩展性工作流订阅

可以将 vRealize Orchestrator 托管的工作流与 vRealize Automation Cloud Assembly 一起使用来扩展应用程序生命周期。

### 如何使用 vRealize Orchestrator 工作流订阅修改虚拟机属性

可以使用现有 vRealize Orchestrator 工作流来修改虚拟机属性，以及将虚拟机添加到 Active Directory。

事件主题参数可定义事件代理服务 (EBS) 消息负载的格式。要在工作流中接收和使用 EBS 消息负载，您必须定义 `inputProperties` 工作流输入参数。

#### 前提条件

- 云管理员用户角色
- 现有 vRealize Orchestrator 内部部署工作流。
- 与 vRealize Orchestrator 客户端服务器的成功集成和连接。

#### 步骤

- 1 选择**可扩展性 > 订阅**。
- 2 单击**新建订阅**。
- 3 使用以下参数创建订阅：

参数	值
名称	<b>RenameVM</b>
事件主题	选择适用于所需 vRealize Orchestrator 集成的事件主题。例如，计算资源分配。

参数	值
阻止/非阻止	非阻止
操作/工作流	选择 vRealize Orchestrator 可运行类型。选择所需的工作流。例如，“设置虚拟机名称”。

4 要保存订阅，请单击**保存**。

5 通过创建云模板或部署现有云模板，分配并激活订阅。

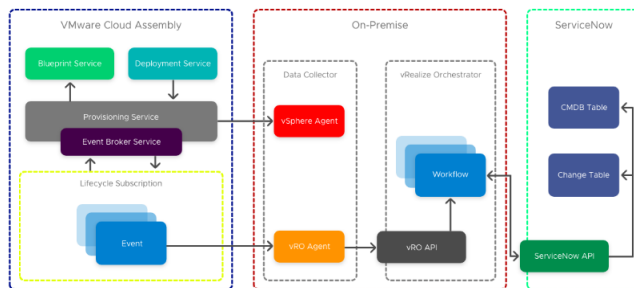
#### 后续步骤

使用以下方法之一验证工作流是否已成功启动：

- 通过导航到**可扩展性 > 活动 > 工作流运行**，验证工作流运行日志。
- 打开 vRealize Orchestrator 客户端，然后通过导航到工作流并验证状态或打开特定日志选项卡来检查工作流状态。

#### 如何使用 vRealize Orchestrator 工作流将适用于 ITSM 的 Cloud Assembly 与 ServiceNow 集成

使用 vRealize Orchestrator 托管的工作流，可以将 vRealize Automation Cloud Assembly 与 ServiceNow 集成以实现 ITSM 合规性



企业用户通常将其云计算管理平台与 IT 服务管理 (IT Service Management, ITSM) 和配置管理数据库 (Configuration Management Database, CMDB) 平台集成以实现合规性。按照此示例，可以使用 vRealize Orchestrator 托管的工作流将 vRealize Automation Cloud Assembly 与适用于 CMDB 和 ITSM 的 ServiceNow 集成。使用 vRealize Orchestrator 集成和工作流时，如果您有多个用于不同环境的实例，则功能标记特别有用。有关功能标记的详细信息，请参见在 [vRealize Automation Cloud Assembly](#) 中使用功能标记。

**注** 还可以使用可扩展性操作脚本将 ServiceNow 与 vRealize Automation Cloud Assembly 集成。有关使用可扩展性操作脚本集成 ServiceNow 的信息，请参见 [如何使用可扩展性操作将 Cloud Assembly 与 ServiceNow 集成](#)。

在此示例中，ServiceNow 集成由三个顶级工作流组成。每个工作流都有自己的订阅，以便您可以单独更新和迭代每个组件。

- 事件订阅入口点 - 基本日志记录，标识请求用户和 vCenter VM（如果适用）。
- 集成工作流 - 分离对象并将输入传递到技术工作流，处理日志记录、属性和输出更新。

- 技术工作流 - 下游系统集成，供 ServiceNow API 用于创建具有负载和其他虚拟机属性的 CMDB CI、CR 和 vRealize Automation Cloud Assembly IaaS API。

### 前提条件

- 独立或集群 vRealize Orchestrator 环境。
- vRealize Automation Cloud Assembly 中的 vRealize Orchestrator 集成。有关将独立 vRealize Orchestrator 与 vRealize Automation Cloud Assembly 集成的信息，请参见在 [Cloud Assembly 中配置 vRealize Orchestrator 集成](#)。

### 步骤

- 1 在 vRealize Orchestrator 中创建并保存包含多个工作流中常用配置的配置文件。
- 2 将 vRealize Automation Cloud Assembly API 令牌保存到与步骤 1 中的配置文件相同的位置。

---

**注** vRealize Automation Cloud Assembly API 令牌会过期。

---

- 3 使用提供的脚本元素在 vRealize Orchestrator 中创建工作流。此脚本将引用并查找 REST 主机。此脚本还将使用令牌可选参数的 REST 操作标准化，该参数添加为额外的授权标头。

```
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"];

```

此脚本将输出 `cpuCount` 和 `memoryMB` 发送到父工作流，并更新现有 `customProperties` 属性。创建 CMDB 时，可以在后续工作流中使用这些值。

- 4 将“创建 ServiceNow CMDB CI”脚本元素添加到工作流中。此元素使用配置项查找 ServiceNow REST 主机，为 `cmdb_ci_vmware_instance` 表创建 REST 操作，基于 `post` 数据的工作流输入创建一系列内容对象，并输出返回的 `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,attributeName)

//REST Template
var opName = "serviceNowCreatCI";
var opTemplate = "/api/now/table/" + tableName;
var opMethod = "POST";

```

```

// create the REST operation:
var opCI =
System.getModule("au.com.cs.example").createOp(restHost,opName,opMethod,opTemplate);

//cmdb_ci_vm_vmware table content to post;
var contentObject = {};
contentObject["name"] = hostname;
contentObject["cpus"] = cpuTotalCount;
contentObject["memory"] = MemoryInMB;
contentObject["correlation_id"]= deploymentId
contentObject["disks_size"]= diskProvisionGB
contentObject["location"] = "Sydney";
contentObject["vcenter_uuid"] = vcUuid;
contentObject["state"] = "On";
contentObject["owned_by"] = owner;

postContent = JSON.stringify(contentObject);
System.log("JSON: " + postContent);

// (Rest Operation, Params, Content, Auth Token)
var ciResponse =
System.getModule("au.com.cs.example").executeOp(opCI,null,postContent,null) ;

try{
    var cmdbCI = JSON.parse(ciResponse);
} catch (ex) {
    throw ex + " failed to parse ServiceNow CMDB response";
}

serviceNowSysId = cmdbCI['result']['sys_id'];

```

- 5 使用来自子工作流的输出，使用现有 `customProperties` 创建一个属性对象并使用来自 `ServiceNow` 的值覆盖 `serviceNowSysId` 属性。此唯一 ID 在 CMDB 中用于将实例标记为销毁时注销。

## 结果

vRealize Automation Cloud Assembly 已成功与 ITSM ServiceNow 集成。有关如何使用工作流在 vRealize Automation Cloud Assembly 中集成 ServiceNow 的更多信息，请参见[使用 vRealize Orchestrator 为 ServiceNow 集成扩展 Cloud Assembly](#)。

## 了解有关工作流订阅的更多信息

借助 vRealize Orchestrator 与 vRealize Automation Cloud Assembly 的集成，您可以使用工作流来扩展应用程序的生命周期。

vRealize Automation 包括嵌入式 vRealize Orchestrator 部署。可以在订阅中使用嵌入式 vRealize Orchestrator 部署的工作流库。可以使用 vRealize Orchestrator 客户端创建、修改和删除工作流。

还可以在 vRealize Automation Cloud Assembly 中集成外部 vRealize Orchestrator 部署。请参见《使用嵌入式 vRealize Orchestrator 客户端》中的“如何集成外部 vRealize Orchestrator 客户端”。

## 创建 vRealize Orchestrator 工作流的最佳做法

工作流订阅基于特定事件主题和该主题的事件参数。要确保订阅可以启动 vRealize Orchestrator 工作流，您必须为这些订阅配置正确的输入参数，以使它们能够使用事件数据。

### 工作流输入参数

自定义工作流的负载中可以包含所有参数或单个参数（使用所有数据）。

要使用单个参数，请配置一个类型为 `Properties` 且名称为 `inputProperties` 的参数。

### 工作流输出参数

自定义工作流可以包含回复事件主题类型所需的后续事件的相关输出参数。

如果事件主题需要回复，则工作流输出参数必须与回复结构定义的参数匹配。

## 如何跟踪工作流运行

“工作流运行”窗口显示订阅触发的工作流及其状态的日志。

可以通过导航到 **可扩展性 > 活动 > 工作流运行** 查看工作流运行的日志。

## 对失败的工作流订阅进行故障排除

如果工作流订阅失败，您可以执行故障排除步骤来纠正它。

失败的工作流运行可能会导致工作流订阅无法成功启动或完成。工作流运行失败可能是由几个常见问题导致的。

问题	原因	解决方案
vRealize Orchestrator 工作流订阅未启动，或者未成功完成。	您已将工作流订阅配置为在收到事件消息时运行自定义工作流，但该工作流未运行，或者未成功完成。	<ol style="list-style-type: none"> <li>1 验证工作流订阅是否已正确保存。</li> <li>2 验证工作流订阅的条件是否正确配置。</li> <li>3 验证 vRealize Orchestrator 包含指定的工作流。</li> <li>4 验证是否已在 vRealize Orchestrator 中正确配置了工作流。</li> </ol>
您的批准请求 vRealize Orchestrator 工作流订阅未运行。	已将批准前或批准后工作流订阅配置为运行 vRealize Orchestrator 工作流，但在服务目录中请求满足已定义的条件时，该工作流未运行。	<p>要成功运行批准工作流订阅，您必须验证所有组件已正确配置。</p> <ol style="list-style-type: none"> <li>1 验证批准策略是否处于活动状态并且正确应用。</li> <li>2 验证工作流订阅是否正确配置并保存。</li> <li>3 检查事件日志以查看与批准相关的消息。</li> </ol>
您的批准请求 vRealize Orchestrator 工作流订阅被拒绝。	<p>您配置了批准前或批准后工作流订阅，用于运行指定的 vRealize Orchestrator 工作流，但该请求在外部批准级别上被拒绝。</p> <p>一个可能的原因是 vRealize Orchestrator 中存在内部工作流运行错误。例如，该工作流缺失或 vRealize Orchestrator 服务器未在运行。</p>	<ol style="list-style-type: none"> <li>1 检查日志以查看与批准相关的消息。</li> <li>2 验证 vRealize Orchestrator 服务器是否正在运行。</li> <li>3 验证 vRealize Orchestrator 包含指定的工作流。</li> </ol>

## 了解有关可扩展性订阅的更多信息

可以通过将可扩展性操作或 vRealize Orchestrator 托管的工作流与可扩展性订阅一起使用来延长应用程序生命周期。

当环境中发生触发事件时，将启动订阅并运行指定的工作流或可扩展性操作。您可以在事件日志中查看系统事件，在工作流运行窗口中查看工作流运行，以及在操作运行窗口中查看操作运行。订阅特定于项目，这意味着订阅通过指定的项目链接到云模板和部署。

### 可扩展性术语

在 vRealize Automation Cloud Assembly 中使用可扩展性和订阅时，您可能会遇到一些特定于订阅和事件代理服务的术语。

**表 6-3. 可扩展性术语**

术语	说明
事件主题	描述一组具有相同逻辑意图和相同结构的事件。每个事件是事件主题的一个实例。 可以为某些事件主题分配阻止参数。有关详细信息，请参见 <a href="#">阻止事件主题</a> 。
事件	指示生成者或由其管理的任意实体的状态更改。事件是记录有关事件出现的信息的实体。
事件代理服务	此服务负责将生成者发布的消息发送给已订阅使用者。
负载	事件数据，其中包含与该事件主题相关的所有属性。
订阅	指示订户希望通过订阅事件主题并定义通知的触发条件来接收有关事件的通知。订阅将可扩展性操作或工作流链接到用于使应用程序生命周期各个部分自动化的触发事件。
订户	根据订阅定义，这些用户将收到与发布到事件代理服务的事件相关的通知。订阅者也称为使用者。
系统管理员	拥有使用 vRealize Automation Cloud Assembly 来创建、读取、更新和删除租户工作流订阅与系统工作流订阅的特权的用户。
工作流订阅	指定事件主题和 vRealize Orchestrator 工作流的触发条件。
操作订阅	指定事件主题以及触发可扩展性操作运行的条件。
工作流	集成到 vRealize Automation Cloud Assembly 中的 vRealize Orchestrator 工作流。可以将这些工作流链接到订阅中的事件。
可扩展性操作	简化的代码脚本，可在订阅中触发事件之后运行。可扩展性操作与工作流类似，但更加轻型。可扩展性操作可从 vRealize Automation Cloud Assembly 中进行自定义。
操作运行	可通过 <a href="#">操作运行</a> 选项卡访问。操作运行是为响应触发事件而运行的可扩展性操作的详细日志。

## 阻止事件主题

有些事件主题支持阻止事件。可扩展性订阅的行为取决于主题是否支持这些事件类型以及订阅的配置方式。

vRealize Automation Cloud Assembly 可扩展性订阅可以使用两大类事件主题：非阻止事件主题和阻止事件主题。事件主题类型定义了可扩展性订阅的行为。

### 非阻止事件主题

非阻止事件主题仅允许创建非阻止订阅。系统以异步方式触发非阻止订阅，您不能依赖订阅的触发顺序。

### 阻止事件主题

有些事件主题支持阻止。如果订阅标记为阻止，则运行阻止订阅的可运行项之前，任何其他具有匹配条件的订阅都不会收到符合设置条件的所有消息。

阻止订阅按优先级顺序运行。最高优先级值是 0（零）。如果同一个事件主题有多个优先级相同的阻止订阅，这些订阅将基于订阅名称按反向字母顺序运行。处理完所有阻止订阅后，消息会同时发送到所有非阻止订阅。由于阻止订阅以同步方式运行，因此当后续订阅收到通知时，已更改的事件负载包含已更新的事件。

可以使用阻止事件主题管理相互依赖的多个订阅。

例如，您有两个置备 workflow 订阅，其中第二个订阅取决于第一个订阅的结果。如果第一个订阅在置备期间更改某个属性，则第二个订阅会在文件系统中记录该新属性（例如计算机名称）。如果 **ChangeProperty** 订阅的优先级值设置为 0，则 **RecordProperty** 的优先级值设置为 1，因为第二个订阅使用第一个订阅的结果。置备计算机时，**ChangeProperty** 订阅会开始运行。由于 **RecordProperty** 订阅条件基于置备后条件，因此事件会触发 **RecordProperty** 订阅。但是，由于 **ChangeProperty** 工作流是阻止工作流，因此在完成之前，此工作流不会收到该事件。当计算机名称已更改并且第一个 workflow 订阅已完成，第二个 workflow 订阅会开始运行并在文件系统中记录该计算机名称。

### 恢复可运行项

对于阻止事件主题，可以将恢复可运行项添加到订阅。如果主可运行项失败，则订阅中的恢复可运行项将运行。例如，您可以创建一个 workflow 订阅，其中主可运行项是在 CMDB 系统（如 ServiceNow）中创建记录的工作流。即使该 workflow 订阅失败，也可能在 CMDB 系统中创建一些记录。在这种情况下，可以使用恢复可运行项清理失败的可运行项在 CMDB 系统中留下的记录。

对于包含相互依赖的多个订阅的用例，可以将 `ebs.recover.continuation` 属性添加到恢复可运行项。使用此属性，可以指示在当前订阅失败时可扩展性服务是否必须继续执行链中的下一个订阅。

## 随 vRealize Automation Cloud Assembly 提供的事件主题

vRealize Automation Cloud Assembly 包含预定义的事件主题。

### 事件主题

事件主题是相似事件分组到一起形成的类别。分配给订阅时，事件主题将定义哪个事件会触发订阅。默认情况下，以下事件主题随 vRealize Automation Cloud Assembly 一起提供。所有主题均可用于添加或更新资源的自定义属性或标记。如果 vRealize Orchestrator 工作流或可扩展性操作失败，则相应的任务也会失败。

表 6-4. Cloud Assembly 事件主题

事件主题	可阻止	说明
Cloud template configuration	否	当云模板配置事件（如创建或删除云模板）发生时发出。此事件主题可用于向外部系统通知此类事件。
Cloud template version configuration	否	当新的云模板版本控制事件（如创建、发布、取消发布或还原版本）发生时发出。此事件主题在集成第三方版本控制系统时很有用。
Compute allocation	是	在分配 <code>resourcenames</code> 和 <code>hostselections</code> 之前发出。可以在此阶段修改这两个属性。
Compute post provision	是	在已成功置备资源之后发出。
Compute post removal	是	在移除计算资源之后发出。
Compute provision	是	在 Hypervisor 层置备资源之前发出。 <b>注</b> 可以更改分配的 IP 地址。
Compute removal	是	在移除资源之前发出。
Compute reservation	是	在预留时发出。 <b>注</b> 可以更改布置顺序。
Deployment action completed	是	在部署操作完成之后发出。
Deployment action requested	是	在部署操作完成之前发出。
Deployment completed	是	在部署云模板或目录请求之后发出。
Deployment onboarded	否	在载入新部署时发出。
Deployment requested	是	在部署云模板或目录请求之前发出。
Deployment resource action completed	是	在部署资源操作之后发出。
Deployment resource action requested	是	在部署资源操作之前发出。
Deployment resource completed	是	在置备部署资源之后发出。
Deployment resource requested	是	在置备部署资源之前发出。
Disk allocation	是	针对磁盘资源预分配发出。

表 6-4. Cloud Assembly 事件主题（续）

事件主题	可阻止	说明
Disk attach	是	<p>在将磁盘连接到计算机之前发出。Disk attach 是一个读写事件。支持写回的磁盘属性包括：</p> <ul style="list-style-type: none"> <li>■ diskFullPaths</li> <li>■ diskDatastoreNames</li> <li>■ diskParentDirs</li> </ul> <p>更新需要具有全部三个 vSphere 特定的磁盘属性。所有其他属性均为只读。</p> <p><b>注</b> 对于 vSphere 第一类磁盘，写回为可选操作。</p>
Disk detach	是	在从计算机分离磁盘之后发出。Disk detach 是一个只读事件。
Disk post removal	是	在删除磁盘资源之后发出。
Disk post resize	是	在调整磁盘资源大小之后发出。
EventLog	是	针对日志记录相关事件发出。
Kubernetes cluster allocation	是	针对 Kubernetes 集群资源预分配发出。
Kubernetes cluster post provision	是	在置备 Kubernetes 集群之后发出。
Kubernetes cluster post removal	是	在删除 Kubernetes 集群之后发出。
Kubernetes cluster provision	是	在置备 Kubernetes 集群之前发出。
Kubernetes cluster removal	是	在启动删除 Kubernetes 集群过程之前发出。
Load balancer post provision	是	在置备负载均衡器之后发出。
Load balancer post removal	是	在移除负载均衡器之后发出。
Load balancer provision	是	在置备负载均衡器之前发出
Load balancer removal	是	在移除负载均衡器之前发出。
Network Configure	是	<p>在计算资源分配过程中配置网络时发出。</p> <p><b>注</b> “配置网络”主题支持多个 IP 地址/网卡。</p>
Network post provisioning	是	在置备网络资源之后发出。
Network post removal	是	在移除网络资源之后发出。
Network provisioning	是	在置备网络资源之前发出。
Network removal	是	在移除网络资源之前发出。

表 6-4. Cloud Assembly 事件主题（续）

事件主题	可阻止	说明
Security group post provisioning	是	在置备安全组之后发出。
Security group post removal	是	在移除安全组之后发出。
Security group provisioning	是	在置备安全组之前发出。
Security group removal	是	在移除安全组之前发出。
Project Lifecycle	否	在创建、更新或删除项目时发生的事件。

### 事件参数

添加事件主题后，可以查看该事件主题的参数。这些事件参数将定义事件负载或 `inputProperties` 的结构。某些事件参数无法修改，并标记为只读。您可以通过单击参数右侧的信息图标来识别这些只读参数。

### 可扩展性事件日志

可扩展性事件窗格显示环境中发生的所有事件列表。

可以通过导航到**可扩展性 > 事件**查看可扩展性事件日志。此外，还可以按一个或多个属性筛选事件列表。要查看各个事件的其他详细信息，请选择事件 ID。

ID	Timestamp	Event Topic	User Name	Target ID	Description
cb156ce-a324-f5ae-5dd1-66d1e591f1a6	04/28/20, 1:10 PM	N/A	N/A	endpoints	CREATE
6f621f51-2906-dce2-14ab-68c17132d756	03/25/20, 4:22 PM	N/A	N/A	endpoints	CREATE
468e8e55-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
385b4d40-a663-631f-7098-3747aa528d12	01/30/20, 5:35 PM	N/A	N/A	endpoints	CREATE

### 创建可扩展性订阅

通过将 vRealize Orchestrator 集成或可扩展性操作与 vRealize Automation Cloud Assembly 一起使用，可以创建订阅来扩展应用程序。

借助可扩展性订阅，您可以通过在发生特定生命周期事件时触发工作流或操作来扩展应用程序。还可以对订阅应用筛选器来为指定的事件设置布尔条件。例如，仅当布尔表达式为 'true' 时，事件和工作流或操作才会触发。这对于要控制何时触发事件、操作或工作流的场景非常有用。

### 前提条件

- 云管理员用户角色
- 如果使用的是 vRealize Orchestrator 工作流：
  - 嵌入式 vRealize Orchestrator 客户端的库或任何集成外部 vRealize Orchestrator 实例的库。



- 如果使用的可扩展性操作：
  - 现有可扩展性操作脚本。有关详细信息，请参见[如何创建可扩展性操作](#)。

## 步骤

- 1 选择**可扩展性 > 订阅**。
- 2 单击**新建订阅**。
- 3 输入订阅的详细信息。
- 4 选择**事件主题**。
- 5 （可选）设置事件主题的条件。

---

**注** 可以使用 javascript 语法表达式创建条件。此表达式可以包含布尔运算符，例如 "&&" (AND)、"||" (OR)、"^" (XOR) 和 "!" (NOT)。此外，还可以使用算术运算符，例如 "==" (equal to)、"!=" (not equal to)、">=" (greater than or equal)、"<=" (less than or equal)、">" (greater than) 和 "<" (lesser than)。更复杂的布尔表达式可以由更简单的表达式构建而成。要根据指定的主题参数访问事件的负载（数据），请使用 'event.data' 或事件的任何标头属性：sourceType、sourceIdentity、timeStamp、eventType、eventTopicId、correlationType、correlationId、description、targetType、targetId、userName 和 orgId。

---

- 6 在**操作/工作流**下，为可扩展性订阅选择可运行项。
- 7 （可选）如果适用，请为事件主题配置阻止行为。
- 8 （可选）要定义可扩展性订阅的项目范围，请禁用**任何项目**，然后单击**添加项目**。
- 9 要保存订阅，请单击**保存**。

## 结果

已创建订阅。发生按所选事件主题分类的事件时，将启动链接的 vRealize Orchestrator 工作流或可扩展性操作，并通知所有订阅者。

## 后续步骤

创建订阅之后，您可以创建或部署云模板以链接并使用订阅。此外，还可以在 vRealize Automation Cloud Assembly 的**可扩展性**选项卡中验证工作流运行的状态。对于包含 vRealize Orchestrator 工作流的订阅，还可以从 vRealize Orchestrator 客户端监控运行和工作流状态。

## 对可扩展性订阅进行故障排除

对可扩展性订阅失败进行故障排除。

当您的订阅失败时，通常是因为您的工作流或可扩展性操作脚本出现错误。

## 查看主题参数和负载

可以使用转储订阅主题参数脚本在任何给定的事件阶段查看虚拟机的特定参数和负载。

此脚本主要用于调试和验证可用于您的 vRealize Orchestrator 工作流的输入。要查看虚拟机的所有参数，请对您的工作流使用以下脚本：

```
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)

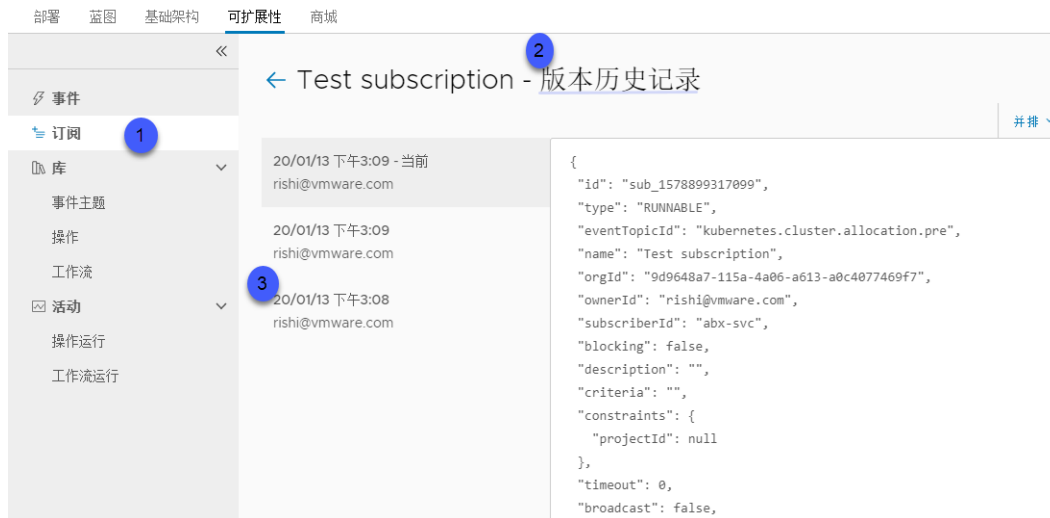
customProps = inputProperties.get("customProperties")
```

## 订阅版本历史记录

如果您的订阅失败，您可以查看版本历史记录。

查看订阅版本历史记录

“版本历史记录”选项卡可显示您的订阅的更改历史记录，以及更改的用户和日期。如果您的订阅失败或运行不正确，则版本历史记录有助于确定原因。



1

从**订阅**选项卡打开您的订阅。

2

要查看版本历史记录，请单击**版本历史记录**。

3

您可以单击每个更改条目以查看与更改关联的相应订阅代码。

## 有哪些 vRealize Automation 资源属性

在 vRealize Automation 基础架构即代码编辑器中，可以通过单击或悬停鼠标指标，查看语法和代码完成帮助。然而，要查看完整的云模板资源属性集（有时称为自定义属性），请参阅整合的资源结构定义。

该结构定义可从 VMware {code} 站点获得。访问链接，然后单击**模型**，即会列出可用于云模板（以前称为蓝图）的资源对象。

- [VMware {code} 上的 vRealize Automation 资源类型结构定义](#)

## 有哪些 vRealize Automation Cloud Assembly 代码示例

vRealize Automation Cloud Assembly 中的云模板代码在组合与应用方面几乎无限制。

通常，成功代码的示例是进行进一步开发的最佳起点。遵照示例时，请进行替换，以便在资源名称、值等方面应用您的站点设置。

## vRealize Automation Cloud Assembly 云模板中的 vSphere 资源示例

以下代码示例说明了 vRealize Automation Cloud Assembly 云模板中的 vSphere 计算机资源。

资源	云模板示例
具有 CPU、内存和操作系统的 vSphere 虚拟机	<pre>resources:   demo-machine:     type: Cloud.vSphere.Machine     properties:       name: demo-machine       cpuCount: 1       totalMemoryMB: 1024       image: ubuntu</pre>
具有数据存储资源的 vSphere 计算机	<pre>resources:   demo-vsphere-disk-001:     type: Cloud.vSphere.Disk     properties:       name: DISK_001       type: 'HDD'       capacityGb: 10       dataStore: 'datastore-01'       provisioningType: thick</pre>
具有连接磁盘的 vSphere 计算机	<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: &gt;-         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>

资源	云模板示例
具有动态磁盘数量的 vSphere 计算机	<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>
从快照映像生成的 vSphere 计算机。附加正斜杠和快照名称。快照映像可以是链接克隆。	<pre> resources:   demo-machine:     type: Cloud.vSphere.Machine     properties:       imageRef: 'demo-machine/snapshot-01'       cpuCount: 1       totalMemoryMB: 1024 </pre>
在 vCenter 中位于特定文件夹的 vSphere 计算机	<pre> resources:   demo-machine:     type: Cloud.vSphere.Machine     properties:       name: demo-machine       cpuCount: 2       totalMemoryMB: 1024       imageRef: ubuntu       resourceGroupName: 'myFolder' </pre>

资源	云模板示例
具有多个网卡的 vSphere 计算机	<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>
在 vCenter 中附加了标 记的 vSphere 计算机	<pre>resources:   demo-machine:     type: Cloud.vSphere.Machine     properties:       flavor: small       image: ubuntu       tags:         - key: env           value: demo</pre>

资源	云模板示例
具有自定义规范的 vSphere 计算机	<pre> resources:   demo-machine:     type: Cloud.vSphere.Machine     properties:       name: demo-machine       image: ubuntu       flavor: small       customizationSpec: Linux </pre>
启用远程访问的 vSphere 计算机	<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: &gt;-         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" &gt;&gt; /etc/sudoers.d/\${input.username} </pre>

## 已记录的 vRealize Automation Cloud Assembly 模板示例

此示例包含一组完整的评论，让您能够查看 vRealize Automation Cloud Assembly 模板（以前称为蓝图）中各部分的结构和用途。

```

# *****
#
# This WordPress cloud template is enhanced with comments to explain its
# parameters.
#

```

```

# Try cloning it and experimenting with its YAML code. If you're new to
# YAML, visit yaml.org for general information.
#
# The cloud template deploys a minimum of 3 virtual machines and runs scripts
# to install packages.
#
# *****
#
# -----
# Templates need a descriptive name and version if
# source controlled in git.
# -----
name: WordPress Template with Comments
formatVersion: 1
version: 1
#
# -----
# Inputs create user selections that appear at deployment time. Inputs
# can set placement decisions and configurations, and are referenced
# later, by the resources section.
# -----
inputs:
#
# -----
# Choose a cloud endpoint. 'Title' is the visible
# option text (oneOf allows for the friendly title). 'Const' is the
# tag that identifies the endpoint, which was set up earlier, under the
# Cloud Assembly Infrastructure tab.
# -----
platform:
  type: string
  title: Deploy to
  oneOf:
    - title: AWS
      const: aws
    - title: Azure
      const: azure
    - title: vSphere
      const: vsphere
  default: vsphere
#
# -----
# Choose the operating system. Note that the Cloud Assembly
# Infrastructure must also have an AWS, Azure, and vSphere Ubuntu image
# mapped. In this case, enum sets the option that you see, meaning there's
# no friendly title feature this time. Also, only Ubuntu is available
# here, but having this input stubbed in lets you add more operating
# systems later.
# -----
osimage:
  type: string
  title: Operating System
  description: Which OS to use
  enum:
    - Ubuntu

```



```

#
# -----
# Set the number of machines in the database cluster. Small and large
# correspond to 1 or 2 machines, respectively, which you see later,
# down in the resources section.
# -----
dbenvsize:
  type: string
  title: Database cluster size
  enum:
    - Small
    - Large
#
# -----
# Dynamically tag the machines that will be created. The
# 'array' of objects means you can create as many key-value pairs as
# needed. To see how array input looks when it's collected,
# open the cloud template and click TEST.
# -----
Mtags:
  type: array
  title: Tags
  description: Tags to apply to machines
  items:
    type: object
    properties:
      key:
        type: string
        title: Key
      value:
        type: string
        title: Value
#
# -----
# Create machine credentials. These credentials are needed in
# remote access configuration later, in the resources section.
# -----
username:
  type: string
  minLength: 4
  maxLength: 20
  pattern: '[a-z]+'
  title: Database Username
  description: Database Username
userpassword:
  type: string
  pattern: '[a-z0-9A-Z@#\$]+'
  encrypted: true
  title: Database Password
  description: Database Password
#
# -----
# Set the database storage disk size.
# -----
databaseDiskSize:

```

```

    type: number
    default: 4
    maximum: 10
    title: MySQL Data Disk Size
    description: Size of database disk
#
# -----
# Set the number of machines in the web cluster. Small, medium, and large
# correspond to 2, 3, and 4 machines, respectively, which you see later,
# in the WebTier part of the resources section.
# -----
clusterSize:
  type: string
  enum:
    - small
    - medium
    - large
  title: Wordpress Cluster Size
  description: Wordpress Cluster Size
#
# -----
# Set the archive storage disk size.
# -----
archiveDiskSize:
  type: number
  default: 4
  maximum: 10
  title: Wordpress Archive Disk Size
  description: Size of Wordpress archive disk
#
# -----
# The resources section configures the deployment of machines, disks,
# networks, and other objects. In several places, the code pulls from
# the preceding interactive user inputs.
# -----
resources:
#
# -----
# Create the database server. Choose a cloud agnostic machine 'type' so
# that it can deploy to AWS, Azure, or vSphere. Then enter its property
# settings.
# -----
  DBTier:
    type: Cloud.Machine
    properties:
#
# -----
# Descriptive name for the virtual machine. Does not become the hostname
# upon deployment.
# -----
    name: mysql
#
# -----
# Hard-coded operating system image to use. To pull from user input above,
# enter the following instead.

```

```

# image: '${input.osimage}'
# -----
#     image: Ubuntu
#
# -----
# Hard-coded capacity to use. Note that the Cloud Assembly
# Infrastructure must also have AWS, Azure, and vSphere flavors
# such as small, medium, and large mapped.
# -----
#     flavor: small
#
# -----
# Tag the database machine to deploy to the cloud vendor chosen from the
# user input. Tags are case-sensitive, so 'to_lower' forces the tag to
# lowercase to ensure a match with a site's tagging convention. It's
# important if platform input were to contain any upper case characters.
# -----
#     constraints:
#       - tag: '${"env:" + to_lower(input.platform)}'
#
# -----
# Also tag the database machine with any free-form tags that were created
# during user input.
# -----
#     tags: '${input.Mtags}'
#
# -----
# Set the database cluster size by referencing the dbenvsize user
# input. Small is one machine, and large defaults to two.
# -----
#     count: '${input.dbenvsize == "Small" ? 1 : 2}'
#
# -----
# Add a variable to connect the machine to a network resource based on
# a property binding to another resource. In this case, it's the
# 'WP_Network' network that gets defined further below.
# -----
#     networks:
#       - network: '${resource.WP_Network.id}'
#
# -----
# Enable remote access to the database server. Reference the credentials
# from the user input.
# -----
#     remoteAccess:
#       authentication: usernamePassword
#       username: '${input.username}'
#       password: '${input.userpassword}'
#
# -----
# You are free to add custom properties, which might be used to initiate
# an extensibility subscription, for example.
# -----
#     ABC-Company-ID: 9393
#

```

```

# -----
# Run OS commands or scripts to further configure the database machine,
# via operations such as setting a hostname, generating SSH private keys,
# or installing packages.
# -----

cloudConfig: |
  #cloud-config
  repo_update: true
  repo_upgrade: all
  packages:
    - mysql-server
  runcmd:
    - sed -e '/bind-address/ s/^#*#/' -i /etc/mysql/mysql.conf.d/mysqld.cnf
    - service mysql restart
    - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'mysqlpassword';"
    - mysql -e "FLUSH PRIVILEGES;"
  attachedDisks: []

#
# -----
# Create the web server. Choose a cloud agnostic machine 'type' so that it
# can deploy to AWS, Azure, or vSphere. Then enter its property settings.
# -----

WebTier:
  type: Cloud.Machine
  properties:

#
# -----
# Descriptive name for the virtual machine. Does not become the hostname
# upon deployment.
# -----

  name: wordpress

#
# -----
# Hard-coded operating system image to use. To pull from user input above,
# enter the following instead:
# image: '${input.osimage}'
# -----

  image: Ubuntu

#
# -----
# Hard-coded capacity to use. Note that the Cloud Assembly
# Infrastructure must also have AWS, Azure, and vSphere flavors
# such as small, medium, and large mapped.
# -----

  flavor: small

#
# -----
# Set the web server cluster size by referencing the clusterSize user
# input. Small is 2 machines, medium is 3, and large defaults to 4.
# -----

  count: '${input.clusterSize== "small" ? 2 : (input.clusterSize == "medium" ? 3 : 4)}'

#
# -----
# Set an environment variable to display object information under the
# Properties tab, post-deployment. Another example might be

```

```

# {env.blueprintID}
# -----
#   tags:
#     - key: cas.requestedBy
#       value: '${env.requestedBy}'
#
# -----
# You are free to add custom properties, which might be used to initiate
# an extensibility subscription, for example.
# -----
#   ABC-Company-ID: 9393
#
# -----
# Tag the web server to deploy to the cloud vendor chosen from the
# user input. Tags are case-sensitive, so 'to_lower' forces the tag to
# lowercase to ensure a match with your site's tagging convention. It's
# important if platform input were to contain any upper case characters.
# -----
#   constraints:
#     - tag: '${"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
#
# *****

```

## vRealize Automation 云模板中的网络、安全性和负载均衡器示例

可以在云模板设计和部署中使用网络、安全性和负载均衡器资源和设置。

有关云模板设计代码选项的摘要信息，请参见 [vRealize Automation 资源类型结构定义](#)。

相关信息，请参见：

- [在 vRealize Automation 云模板中使用网络资源](#)
- [在 vRealize Automation 云模板中使用安全组资源](#)

## ■ 在 vRealize Automation 云模板中使用负载均衡器资源

这些示例说明了基本云模板设计中的示例网络、安全组和负载均衡器资源。

资源场景	云模板设计代码示例
多个网卡关联到一个 NSX 网络资源的 vSphere 计算机。	<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>
通过在出站网络上使用 Cloud.NSX.Gateway 云模板资源来启用 NAT 端口转发。	<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>
指定负载均衡日志记录级别、算法和大小。	<p>显示使用日志记录级别、算法和大小的 NSX 负载均衡器示例：</p> <pre>resources:   Cloud_LoadBalancer_1:     <b>type: Cloud.NSX.LoadBalancer</b>     properties:       name: myapp-lb       network: '\${appnet-public.name}'       instances: '\${wordpress.id}'       routes:         - protocol: HTTP port: '80'           <b>loggingLevel: CRITICAL</b>           <b>algorithm: LEAST_CONNECTION</b>           <b>type: MEDIUM</b></pre>

资源场景	云模板设计代码示例
<p>将负载均衡器与指定的计算机或指定的计算机网卡相关联。可以指定 machine ID 或 machine network ID, 以将计算机添加到负载均衡器池。实例属性支持计算机 (machine by ID) 和网卡 (machine by network ID)。</p> <p>在第一个示例中, 在任何网络上部署计算机时, 部署都使用 machine by ID 设置对计算机进行负载均衡。</p> <p>在第二个示例中, 仅当计算机部署在指定的计算机网卡上时, 部署才使用 machine by network ID 设置对计算机进行负载均衡。</p> <p>第三个示例显示了同一 instances 选项中使用的两个设置。</p>	<p>可以使用 instances 属性定义计算机 ID 或计算机网络 ID:</p> <ul style="list-style-type: none"> <li>■ 计算机 ID <pre>Cloud_LoadBalancer_1:   type: Cloud.LoadBalancer   properties:     network: '\${resource.Cloud_Network_1.id}'     instances: '\$ {resource.Cloud_Machine_1.id}'</pre> </li> <li>■ 计算机网络 ID <pre>Cloud_LoadBalancer_1:   type: Cloud.LoadBalancer   properties:     network: '\${resource.Cloud_Network_1.id}'     instances: '\$ {resource.Cloud_Machine_1.networks[0].id}'</pre> </li> <li>■ 为包含负载均衡器指定一个计算机, 为包含负载均衡器指定另一个计算机网卡: <pre>instances:   - resource.Cloud_Machine_1.id   - resource.Cloud_Machine_2.networks[2].id</pre> </li> </ul>
<p>使用内部 IP (而非公共 IP) 的公有云计算机。此示例使用特定网络 ID。</p> <p>注意: network: 选项在 networks: 设置中用于指定目标网络 ID。networks: 设置中的 name: 选项已弃用, 不应使用。</p>	<pre>resources:   wf_proxy:     type: Cloud.Machine     properties:       image: ubuntu 16.04       flavor: small       constraints:         - tag: 'platform:vsphere'     networks:       - network: '\${resource.wf_net.id}'         assignPublicIpAddress: false</pre>
<p>使用 NSX 网络资源类型的 NSX-V 或 NSX-T 路由网络。</p>	<pre>Cloud_NSX_Network_1:   type: Cloud.NSX.Network   properties:     networkType: routed</pre>



资源场景	云模板设计代码示例
<p>将标记添加到云模板中的计算机网卡资源。</p>	<pre>formatVersion: 1 inputs: {} resources:   Cloud_Machine_1:     type: Cloud.vSphere.Machine     properties:       flavor: small       image: ubuntu     networks:       - name: '\${resource.Cloud_Network_1.name}'         deviceIndex: 0         tags:           - key: 'nic0'             value: null           - key: internal             value: true       - name: '\${resource.Cloud_Network_2.name}'         deviceIndex: 1         tags:           - key: 'nic1'             value: null           - key: internal             value: false</pre>
<p>为出站网络标记 NSX-T 逻辑交换机。</p> <p>NSX-T 和 VMware Cloud on AWS 支持标记。</p> <p>有关此方案的详细信息，请参见社区博客帖子<a href="#">使用 Cloud Assembly 在 NSX 中创建标记</a>。</p>	<pre>Cloud_NSX_Network_1:   type: Cloud.NSX.Network   properties:     networkType: outbound   tags:     - key: app       value: opencart</pre>
<p>对计算机网卡应用了限制标记的现有安全组。</p> <p>要使用现有安全组，请针对 securityGroupType 属性输入 <i>existing</i>。</p> <p>可以为 Cloud.SecurityGroup 资源分配标记，以使用标记限制分配现有安全组。不能在云模板设计中使用不包含标记的安全组。</p> <p>必须为 securityGroupType: existing 安全组资源设置限制标记。这些限制必须与在现有安全组上设置的标记相匹配。无法为 securityGroupType: new 安全组资源设置限制标记。</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>

## 资源场景

按需安全组，其中包含两个用于说明 Allow 和 Deny 访问选项的防火墙规则。

## 云模板设计代码示例

```
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
```

## 资源场景

具有 2 个安全组的复杂云模板，其中包括：

- 1 个现有安全组
- 1 个具有多个防火墙规则示例的按需安全组
- 1 个 vSphere 计算机
- 1 个现有网络

此示例说明了以下项的各种不同组合：协议和端口、服务、IP CIDR 作为源和目标，IP 范围作为源或目标以及任意、IPv6 和 (::/0) 选项。

对于计算机网卡，可以指定已连接的网络和安全组。此外，还可以指定网卡索引或 IP 地址。

## 云模板设计代码示例

```
formatVersion: 1
inputs: {}
resources:
  DEMO_ESG : (现有安全组 - 安全组 1)
    type: Cloud.SecurityGroup
    properties:
      constraints:
        - tag: BlockAll
      securityGroupType: existing (为安全组 1 指定
现有)
  DEMO_ODSG: (按需安全组 - 安全组 2)
    type: Cloud.SecurityGroup
    properties:
      rules: (此部分包含多个防火墙规则)
        - name: IN-ANY (规则 1)
          source: any
          service: any
          direction: inbound
          access: Deny
        - name: IN-SSH (规则 2)
          source: any
          service: SSH
          direction: inbound
          access: Allow
        - name: IN-SSH-IP (规则 3)
          source: 33.33.33.1-33.33.33.250
          protocol: TCP
          ports: 223
          direction: inbound
          access: Allow
        - name: IPv-6-ANY-SOURCE (规则 4)
          source: ':::/0'
          protocol: TCP
          ports: 223
          direction: inbound
          access: Allow
        - name: IN-SSH-IP (规则 5)
          source: 44.44.44.1/24
          protocol: UDP
          ports: 22-25
          direction: inbound
          access: Allow
        - name: IN-EXISTING-SG (规则 6)
          source: '${resource["DEMO_ESG"].id}'
          protocol: ICMPv6
          direction: inbound
          access: Allow
        - name: OUT-ANY (规则 7)
          destination: any
          service: any
          direction: outbound
          access: Deny
        - name: OUT-TCP-IPv6 (规则 8)
          destination:
'2001:0db8:85a3::8a2e:0370:7334/64'
          protocol: TCP
          ports: 22
          direction: outbound
          access: Allow
        - name: IPv6-ANY-DESTINATION (规则 9)
```

## 资源场景

## 云模板设计代码示例

```

        destination: '::/0'
        protocol: UDP
        ports: 23
        direction: outbound
        access: Allow
    - name: OUT-UDP-SERVICE (规则 10)
      destination: any
      service: NTP
      direction: outbound
      access: Allow
    securityGroupType: new (为安全组 2 指定按需)
DEMO_VC_MACHINE: (计算机资源)
  type: Cloud.vSphere.Machine
  properties:
    image: PHOTON
    cpuCount: 1
    totalMemoryMB: 1024
    networks: (计算机网卡)
    - network: '${resource.DEMO_NW.id}'
  securityGroups: - '${resource.DEMO_ODSG.id}' -
    '${resource.DEMO_ESG.id}'
DEMO_NETWORK: (网络资源)
  type: Cloud.vSphere.Network
  properties:
    networkType: existing
    constraints:
      - tag: nsx62

```

资源场景	云模板设计代码示例
包含单臂负载均衡器的按需网络。	<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>
包含负载均衡器的现有网络。	<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>

## 资源场景

## 云模板设计代码示例

```

- 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

```

## 了解更多

有关网络 and 安全性实施场景，请参见如下等 VMware 博客：

- [vRealize Automation Cloud Assembly 负载均衡器与 NSX-T 配合使用深入探讨](#)
- [使用 Cloud Assembly 和 NSX 实现网络自动化 - 第 1 部分](#)（包括使用 NSX-T 和 vCenter 云帐户和网络 CIDR）
- [使用 Cloud Assembly 和 NSX 实现网络自动化 - 第 2 部分](#)（包括使用现有的出站网络类型）
- [使用 Cloud Assembly 和 NSX 实现网络自动化 - 第 3 部分](#)（包括使用现有的按需安全组）
- [使用 Cloud Assembly 和 NSX 实现网络自动化 - 第 4 部分](#)（包括使用现有的按需负载均衡器）

## 在 vRealize Automation 云模板中使用网络资源

创建或编辑 vRealize Automation 云模板设计时，请为您的目标使用最合适的网络资源。了解云模板中可用的 NSX 网络和云平台无关的网络选项。

根据 vRealize Automation 云模板中的计算机和相关条件，选择可用的网络资源类型之一。

## 云平台无关的网络资源

可以在云模板设计页面上使用**云平台无关 > 网络**资源，添加云平台无关的网络。资源在云模板代码中显示为 `Cloud.Network` 资源类型。默认资源显示为：

```
Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkType: existing
```

如果要为未连接或可能未连接到 NSX 网络的目标计算机类型指定网络特性，请使用云平台无关的网络。

云平台无关的网络资源适用于以下资源类型：

- 云平台无关的计算机
- vSphere
- Google Cloud Platform (GCP)
- Amazon Web Services (AWS)
- Microsoft Azure
- VMware Cloud on AWS (VMC)

云平台无关的网络资源适用于以下网络类型 (`networkType`) 设置：

- 公用
- 专用
- 出站
- 现有

## vSphere 网络资源

可以在云模板设计页面上使用**vSphere > 网络**资源，添加 vSphere 网络。资源在云模板代码中显示为 `Cloud.vSphere.Network` 资源类型。默认资源显示为：

```
Cloud_vSphere_Network_1:
  type: Cloud.vSphere.Network
  properties:
    networkType: existing
```

如果要为 vSphere 计算机类型 (`Cloud.vSphere.Machine`) 指定网络特性，请使用 vSphere 网络。

vSphere 网络资源仅适用于 `Cloud.vSphere.Machine` 计算机类型。

vSphere 资源适用于以下网络类型 (`networkType`) 设置：

- 公用
- 专用
- 现有

有关网络类型的详细信息，请参见在 [vRealize Automation](#) 的网络配置文件和云模板中使用网络设置。

## NSX 网络资源

可以在云模板设计页面上使用 **NSX > 网络资源**，添加 NSX 网络。资源在云模板代码中显示为 `Cloud.NSX.Network` 资源类型。默认资源显示为：

```
Cloud_NSX_Network_1:
  type: Cloud.NSX.Network
  properties:
    networkType: existing
```

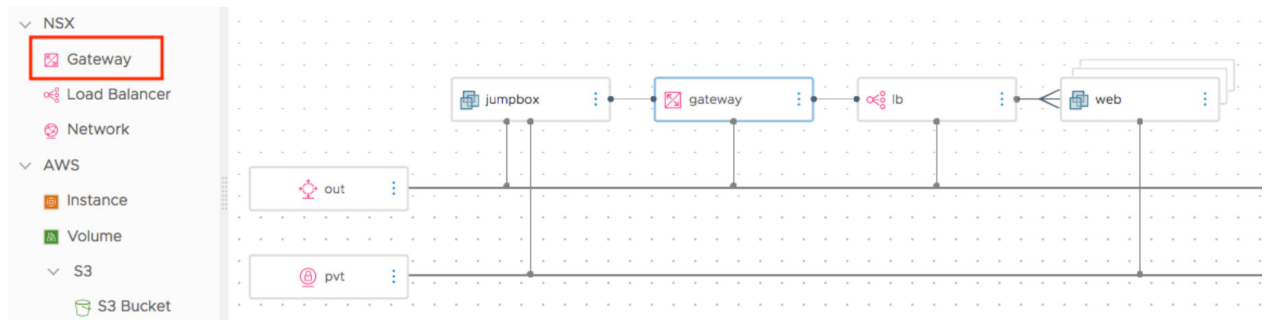
如果要将网络资源连接到已与 NSX-V 或 NSX-T 云帐户关联的一个或多个计算机，请使用 NSX 网络。通过 NSX 网络资源，可以为与 NSX-V 或 NSX-T 云帐户关联的 vSphere 计算机资源指定 NSX 网络特性。

`Cloud.NSX.Network` 资源适用于以下网络类型 (`networkType`) 设置：

- 公用
- 专用
- 出站
- 现有
- 路由 - 路由网络仅适用于 NSX-V 和 NSX-T。

每个按需 NSX-T 网络都会创建一个新的第 1 层逻辑路由器。每个按需 NSX-V 网络都会创建一个新的 Edge。

要支持 NAT 规则和 NAT 端口转发，可以添加一个 `Cloud.NSX.Gateway` 云模板资源，以允许为连接到出站 NSX-V 或 NSX-T 网络的网关/路由器指定 DNAT 规则。网关必须连接到单个出站网络，但可以连接到与同一出站网络连接的多个计算机或负载均衡器。在网关上指定的 DNAT 规则将这些计算机或负载均衡器作为其目标进行引用。无法为集群计算机指定 NAT 规则，但作为实施后操作，可以为集群中的单个计算机指定这些规则。



相关信息，请参见 [vRealize Automation](#) 云模板中的网络、安全性和负载均衡器示例。

## 外部 IPAM 集成选项

有关可在云模板设计和部署中用于 Infoblox IPAM 集成的属性的信息，请参见对 [vRealize Automation](#) 中的 IPAM 集成使用特定于 Infoblox 的属性和可扩展属性。



## 可用的实施后操作

有关可用于云模板和部署资源的常用实施后操作列表，请参见[可以对 vRealize Automation Cloud Assembly 部署运行哪些操作](#)。

有关如何从一个网络移至另一个网络的示例，请参见[如何将已部署的计算机移动到另一个网络](#)。

## 了解更多

有关定义网络资源的信息，请参见 [vRealize Automation 中的网络资源](#)。

有关定义网络配置文件的信息，请参见[了解有关 vRealize Automation 中的网络配置文件的更多信息](#)。

有关说明示例网络资源和设置的云模板设计示例，请参见 [vRealize Automation 云模板中的网络、安全性和负载均衡器示例](#)。

## 在 vRealize Automation 云模板中使用安全组资源

创建或编辑 vRealize Automation 云模板时，请为您的目标使用最合适的安全组资源。了解云模板中可用的安全组选项。

### 云平台无关的安全组资源

目前只有一种类型的安全组资源。可以在云模板“设计”页面上使用[云平台无关 > 安全组](#)资源添加安全组资源。资源在云模板代码中显示为 `Cloud.SecurityGroup` 资源类型。默认资源显示为：

```
Cloud_SecurityGroup_1:
  type: Cloud.SecurityGroup
  properties:
    constraints: []
    securityGroupType: existing
```

可以在云模板设计中将安全组资源指定为现有类型 (`securityGroupType: existing`) 或按需类型 (`securityGroupType: new`)。

可以将现有安全组直接添加到云模板设计，也可以使用已添加到网络配置文件的现有安全组。各种云帐户类型都支持现有安全组。

对于 NSX-V 和 NSX-T，可以在设计或修改云模板时添加现有安全组或定义新的安全组。NSX-T 和 NSX-V 仅支持按需安全组。

对于除 Microsoft Azure 以外的所有云帐户类型，可以将一个或多个安全组关联到一个计算机网卡。Microsoft Azure 虚拟机网卡 (`machineName`) 只能关联到一个安全组。

默认情况下，安全组属性 `securityGroupType` 设置为 `existing`。要创建按需安全组，请为 `securityGroupType` 属性输入 `new`。要为按需安全组指定防火墙规则，请在安全组资源的 `Cloud.SecurityGroup` 部分中使用 `rules` 属性。

## 现有安全组

现有安全组在源云帐户资源（如 NSX-T 或 Amazon Web Services）中创建。vRealize Automation 会从源中收集它们的数据。可以从可用资源列表中选择一个现有安全组作为 vRealize Automation 网络配置文件的一部分。在云模板设计中，可以通过以下两种方式指定现有安全组：通过其在指定网络配置文件中的成员资格内在指定；使用安全组资源中的 `securityGroupType: existing` 设置通过名称具体指定。如果将安全组添加到网络配置文件，请至少将一个功能标记添加到该网络配置文件。按需安全组资源在云模板设计中使用时需要限制标记。

在云模板设计中，可以将一个安全组资源关联到一个或多个计算机资源。

---

**注** 如果要在云模板设计中使用某计算机资源置备到 Microsoft Azure 虚拟机网卡 (`machineName`)，则只能将该计算机资源关联到一个安全组。

---

## 按需 NSX-V 和 NSX-T 安全组

可在定义或修改云模板设计时使用安全组资源代码中的 `securityGroupType: new` 设置定义按需安全组。

可以使用按需 NSX-V 或 NSX-T 安全组将一组特定的防火墙规则应用于一个联网计算机资源或一组分组资源。每个安全组可以包含多个指定的防火墙规则。可以使用按需安全组指定服务或者协议和端口。请注意，可以指定服务或协议，但不能同时指定两者。如果指定协议，还可以指定端口。如果指定服务，则无法指定端口。如果规则既不包含服务也不包含协议，则默认服务值为“任意”。

此外，还可以在防火墙规则中指定 IP 地址和 IP 范围。vRealize Automation 云模板中的网络、安全性和负载均衡器示例中显示了一些防火墙规则示例。

在 NSX-V 或 NSX-T 按需安全组中创建防火墙规则时，默认设置不仅允许指定的网络流量，还允许其他网络流量。要控制网络流量，必须为每个规则指定一个访问类型。规则访问类型包括：

- 允许（默认值）- 允许在此防火墙规则中指定的网络流量。
- 拒绝 - 阻止在此防火墙规则中指定的网络流量。主动告知客户端连接被拒绝。
- 丢弃 - 拒绝此防火墙规则中指定的网络流量。以静默方式丢弃数据包，就好像侦听器未联机一样。

有关使用 `access: Allow` 和 `access: Deny` 防火墙规则的示例设计，请参见 vRealize Automation 云模板中的网络、安全性和负载均衡器示例。

---

**注** 云管理员可以创建仅包含 NSX 按需安全组的云模板设计，并可以部署该设计以创建可重用的现有安全组资源，组织成员可以将该资源作为现有安全组添加到网络配置文件和云模板设计。

---

对于源和目标 IP 地址，防火墙规则支持 IPv4 或 IPv6 格式的 CIDR 值。有关在防火墙规则中使用 IPv6 CIDR 值的示例设计，请参见 vRealize Automation 云模板中的网络、安全性和负载均衡器示例。

## 在按需安全组防火墙规则中使用应用程序隔离策略

可以使用应用程序隔离策略仅允许通过云模板置备的资源之间的内部流量。使用应用程序隔离，通过云模板置备的计算机可以相互通信，但无法连接到防火墙外部。可以在网络配置文件中创建应用程序隔离策略。此外，还可以通过使用具有拒绝防火墙规则或者专用或出站网络的按需安全组，在云模板设计中指定应用程序隔离。

创建的应用程序隔离策略的优先级较低。如果应用多个策略，将优先使用具有较高权重的策略。

创建应用程序隔离策略时，会为该策略分配一个自动生成的策略名称。此外，还可以在特定于关联资源端点和项目的其他云模板设计和设计迭代中重用该策略。应用程序隔离策略名称在云模板设计代码中不可见，但在部署云模板设计后将在项目页面（**基础架构 > 管理 > 项目**）上显示为自定义属性。

对于项目中的同一个关联端点，需要使用按需安全组进行应用程序隔离的任何部署都可以使用同一个应用程序隔离策略。策略创建后，便无法删除。指定应用程序隔离策略时，vRealize Automation 会在项目中针对关联端点搜索策略，如果找到策略，则重用，如果找不到策略，则进行创建。仅当应用程序隔离策略初始部署后，策略名称才显示在项目的自定义属性列表中。

### 在迭代式云模板开发中使用安全组

在迭代式开发过程中更改安全组限制时，如果安全组未与云模板中的计算机相关联，则会在迭代中按指定的方式更新安全组。但是，如果安全组已与计算机相关联，则重新部署将失败。必须在迭代式云模板开发期间将现有安全组和/或 securityGroupType 资源属性与关联的计算机分离，并在每次重新部署之间重新关联。假设您已经初步部署云模板，则所需的工作流如下所示：

- 1 在 Cloud Assembly 模板设计器中，将安全组与云模板中的所有关联计算机分离。
- 2 单击**更新现有部署**以重新部署模板。
- 3 移除模板中的现有安全组限制标记和/或 securityGroupType 属性。
- 4 在模板中添加新的安全组限制标记和/或 securityGroupType 属性。
- 5 将新的安全组限制标记和/或 securityGroupType 属性实例与模板中的计算机相关联。
- 6 单击**更新现有部署**以重新部署模板。

### 可用的实施后操作

有关可用于云模板和部署资源的常用实施后操作列表，请参见[可以对 vRealize Automation Cloud Assembly 部署运行哪些操作](#)。

### 了解更多

有关使用安全组进行网络隔离的相关信息，请参见 [vRealize Automation 中的安全资源](#)。

有关在网络配置文件中使用安全组设置的信息，请参见[了解有关 vRealize Automation 中的网络配置文件的更多信息和在 vRealize Automation Cloud Assembly 的网络配置文件和云模板设计中使用安全组设置](#)。

有关说明示例安全资源和设置的云模板设计示例，请参见 [vRealize Automation 云模板中的网络、安全性和负载均衡器示例](#)。

### 在 vRealize Automation 云模板中使用负载均衡器资源

创建或编辑 vRealize Automation 云模板时，请为您的目标使用最合适的负载均衡器资源。

可以在云模板中使用 NSX 负载均衡器资源和云平台无关的负载均衡器资源，控制部署中的负载均衡。

云平台无关的负载均衡器可以跨多个云部署。特定于云的负载均衡器可以指定仅可用于特定云/拓扑的高级设置和功能。特定于云的属性在 **NSX 负载均衡器 (Cloud.NSX.LoadBalancer)** 资源类型中可用。如果在云平台无关的负载均衡器 (**Cloud.LoadBalancer**) 上添加这些属性，例如，在置备 **Amazon Web Services** 或 **Microsoft Azure** 负载均衡器时，会忽略这些属性；在置备 **NSX-V** 或 **NSX-T** 负载均衡器时，会遵守这些属性。根据 vRealize Automation 云模板中的条件，选择可用的负载均衡器资源类型之一。

无法将负载均衡器资源直接连接到设计画布中的安全组资源。

### 云平台无关的负载均衡器资源

如果要为任何类型的目标计算机指定网络特性，请使用云平台无关的负载均衡器。

可以在云模板“设计”页面上使用**云平台无关 > 负载均衡器**资源，添加云平台无关的负载均衡器。资源在云模板代码中显示为 **Cloud.LoadBalancer** 资源类型。默认资源显示为：

```
Cloud_LoadBalancer_1:
  type: Cloud.LoadBalancer
  properties:
    routes: []
    network: ''
    instances: []
    internetFacing: false
```

### NSX 负载均衡器资源

如果云模板包含特定于 **NSX-V** 或 **NSX-T** 的特性（**Policy API** 或 **Manager API** 方法），请使用 **NSX** 负载均衡器。可以将一个或多个负载均衡器连接到 **NSX-V** 或 **NSX-T** 网络，或者连接到与 **NSX-V** 或 **NSX-T** 网络关联的计算机。

可以通过使用 **NSX > 负载均衡器**资源来添加 **NSX** 负载均衡器。资源在云模板代码中显示为 **Cloud.NSX.LoadBalancer** 资源类型。默认资源显示为：

```
Cloud_NSX_LoadBalancer_1:
  type: Cloud.NSX.LoadBalancer
  properties:
    routes: []
    network: ''
    instances: []
```

### 云模板代码中的负载均衡器选项

将一个或多个负载均衡器资源添加到云模板后，可以指定以下设置。[vRealize Automation 云模板中的网络、安全性和负载均衡器示例](#)中提供了一些示例。

#### ■ 计算机规范

可以指定要加入负载均衡池的指定计算机资源。或者，也可以指定特定的计算机网卡加入负载均衡池。

此选项仅适用于 **NSX** 负载均衡器资源 (**Cloud.NSX.LoadBalancer**)。

此选项适用于 existing 和 public 网络类型。也支持按需 private、routed 和 outbound 网络类型。

- `resource.Cloud_Machine_1.id`

指定负载均衡器包括云模板代码中标识为 `Cloud_Machine_1` 的计算机。

- `resource.Cloud_Machine_2.networks[2].id`

指定负载均衡器仅当在云模板代码中标识为 `Cloud_Machine_2` 的计算机部署到计算机网卡 `Cloud_Machine_2.networks[2]` 时才包括该计算机。

- 日志记录级别

日志记录级别值指定错误日志的严重性级别。选项包括 NONE、EMERGENCY、ALERT、CRITICAL、ERROR、WARNING、INFO、DEBUG 和 NOTICE。日志记录级别值将应用于云模板中的所有负载均衡器。此选项特定于 NSX。对于具有父项的负载均衡器，父日志记录级别设置将覆盖其子项中的任何日志记录级别设置。

有关相关信息，请参见 NSX 产品文档中的[添加负载均衡器](#)等主题。

- 类型

使用负载均衡器类型可指定规模大小。默认值为小型。此选项特定于 NSX。对于具有父项的负载均衡器，父类型设置将覆盖其子项中的任何类型设置。

- 小型

相当于 NSX-V 中的精简型和 NSX-T 中的小型。

- 中型

相当于 NSX-V 中的大型和 NSX-T 中的中型。

- 大型

相当于 NSX-V 中的四倍大和 NSX-T 中的大型。

- 超大型

相当于 NSX-V 中的超大型和 NSX-T 中的大型。

有关相关信息，请参见 NSX 产品文档中的[扩展负载均衡器资源](#)等主题。

此选项仅适用于 **NSX** 负载均衡器资源 (Cloud.NSX.LoadBalancer)。

- 算法（服务器池）

使用算法均衡方法可控制如何在服务器池成员之间分发入站连接。可以在服务器池使用该算法，也可以在服务器上使用。所有负载均衡算法均跳过满足以下任何条件的服务器：

- 管理状态设置为 DISABLED。
- 管理状态设置为 GRACEFUL\_DISABLED，并且没有匹配的持久性条目。
- 主动或被动运行状况检查状态为 DOWN。
- 达到服务器池最大并发连接数的连接限制。

此选项特定于 NSX。

- **IP\_HASH**

根据源 IP 地址的哈希值以及所有运行的服务器的总权重选择服务器。

相当于 NSX-V 和 NSX-T 中的 IP-HASH。

- **LEAST\_CONNECTION**

根据服务器上已存在的连接数将客户端请求分发给多个服务器。新连接将发送到连接最少的服务器。将忽略服务器池成员权重，即使配置了这些权重也是如此。

相当于 NSX-V 中的 LEASTCONN 和 NSX-T 中的 LEAST\_CONNECTION。

- **ROUND\_ROBIN**

在能够处理入站客户端请求的可用服务器列表中循环遍历请求。忽略服务器池成员权重（即使已配置）。默认值。

相当于 NSX-V 和 NSX-T 中的 ROUND\_ROBIN。

- **WEIGHTED\_LEAST\_CONNECTION**

为每个服务器分配一个权重值，此值表示该服务器相对于池中其他服务器的性能。此值可确定与池中其他服务器相比，向某个服务器发送的客户端请求数。此负载均衡算法侧重于使用权重值在可用服务器资源之间公平分配负载。默认情况下，如果未配置权重值且已启用缓慢启动，则权重值为 1。

相当于 NSX-T 中的 WEIGHTED\_LEAST\_CONNECTION。NSX-V 中无对应项。

- **WEIGHTED\_ROUND\_ROBIN**

为每个服务器分配一个权重值，此值表示该服务器相对于池中其他服务器的性能。此值可确定与池中其他服务器相比，向某个服务器发送的客户端请求数。此负载均衡算法侧重于在可用服务器资源之间公平分配负载。

相当于 NSX-T 中的 WEIGHTED\_ROUND\_ROBIN。NSX-V 中无对应项。

- **URI**

对 URI 左侧部分进行哈希并除以运行的服务器的总权重。结果指定了哪个服务器接收请求。这样可以确保如果没有服务器启动或关闭，URI 将始终定向到同一服务器。URI 算法参数具有两个选项：uriLength=<len> 和 uriDepth=<dep>。长度参数范围应为 1<=len<256。深度参数范围应为 1<=dep<10。长度和深度参数后跟一个正整数。这些选项可以仅根据 URI 开头平衡服务器。长度参数指示算法只应考虑在 URI 开头定义的字符以计算哈希值。深度参数指示用于计算哈希值的最大目录深度。请求中的每个斜杠都会计为一个级别。如果指定了两个参数，在到达其中一个参数时，计算将停止。

相当于 NSX-V 中的 URI。NSX-T 中无对应项。

- **HTTPHEADER**



在每个 HTTP 请求中查找 HTTP 标头名称。括号中的标头名称不区分大小写。如果标头不存在或不包含任何值，将应用循环算法。HTTPHEADER 算法参数具有一个选项：

```
headerName=<name>。
```

相当于 NSX-V 中的 HTTPHEADER。NSX-T 中无对应项。

#### ■ URL

在每个 HTTP GET 请求的查询字符串中查找参数中指定的 URL 参数。如果参数后跟等号 = 和一个值，则对该值进行哈希并除以运行的服务器的总权重。结果指定了哪个服务器接收请求。该过程用于跟踪请求中的用户标识符，并确保始终将相同的用户 ID 发送到相同的服务器，但前提是没有启动或关闭服务器。如果找不到任何值或参数，则应用循环算法。URL 算法参数具有一个选项：

```
urlParam=<url>。
```

相当于 NSX-V 中的 URL。NSX-T 中无对应项。

有关信息，请参见 NSX 产品文档中的[添加用于负载均衡的服务器池](#)。

### NSX-V 和 NSX-T 网络和负载均衡器选项

负载均衡器选项取决于负载均衡器资源在云模板中与之关联的网络。可以根据网络类型和网络条件配置负载均衡器。

#### ■ 按需出站网络

如果负载均衡器计算资源连接到按需 outbound 网络，则会为按需网络的第 1 层路由器创建负载均衡器。

#### ■ 按需专用网络

如果负载均衡器计算资源连接到按需 private 网络，将创建新的第 1 层路由器并将其连接到网络配置文件中指定的第 0 层路由器。负载均衡器随后将连接到第 1 层路由器。如果 VIP 位于 existing 网络中，则启用第 1 层路由器 VIP 通告。如果为 DHCP 配置 private 网络，则该 private 网络和负载均衡器将共享第 1 层路由器。

#### ■ 现有网络

如果负载均衡器连接到 existing 网络，将使用现有网络的第 1 层路由器创建负载均衡器。如果没有任何负载均衡器连接到第 1 层路由器时，则会创建新的负载均衡器。如果负载均衡器已存在，则新的虚拟服务器会连接到该负载均衡器。如果 existing 网络未连接到第 1 层路由器，则会创建新的第 1 层路由器并将其连接到网络配置文件中定义的第 0 层路由器，并且不会启用第 1 层路由器 VIP 通告。

#### ■ 网络配置文件中定义的网络隔离

对于 outbound 或 private 网络类型，可以在网络配置文件中指定网络隔离设置以模拟新的安全组。由于计算机连接到现有网络并且在配置文件中定义隔离设置，此选项类似于在现有网络中创建的负载均衡器。区别在于，为了启用数据路径，会将第 1 层上行链路端口 IP 添加到隔离安全组中。

可以在云模板设计中使用 NSX 负载均衡器资源为 NSX 关联的网络指定负载均衡器设置。

要了解更多信息，请参见 VMware 博客帖子 [vRA Cloud Assembly 负载均衡器与 NSX-T 配合使用深入探讨](#)。

## 在多个负载均衡器共享 NSX-T 第 1 层或 NSX-V Edge 时重新配置日志记录级别或类型设置

使用包含多个负载均衡器（在 NSX-T 端点中共享第 1 层路由器或在 NSX-V 端点中共享 Edge 路由器）的云模板时，在其中一个负载均衡器资源中重新配置日志记录级别或类型设置不会更新其他负载均衡器的设置。不匹配的设置会导致 NSX 中存在不一致。为避免在重新配置这些日志记录级别和/或类型设置时出现不一致，请对云模板中的所有负载均衡器资源（在关联的 NSX 端点中共享第 1 层或 Edge）使用相同的重新配置值。

### 可用的实施后操作

横向缩减/扩展包含负载均衡器的部署时，该负载均衡器会配置为包含新添加的计算机或停止对指定为卸除目标的计算机进行负载均衡。

有关可用于云模板和部署的常用实施后操作列表，请参见[可以对 vRealize Automation Cloud Assembly 部署运行哪些操作](#)。

### 了解更多

有关在网络配置文件中定义负载均衡器设置的信息，请参见[了解有关 vRealize Automation 中的网络配置文件的更多信息](#)

有关包含负载均衡器的云模板设计示例，请参见[vRealize Automation 云模板中的网络、安全性和负载均衡器示例](#)。

## Puppet 支持的具有用户名和密码访问权限的云模板

在本示例中，您将 Puppet 配置管理添加到在具有用户名和密码访问权限的 vCenter 计算资源上部署的云模板。

此过程显示的示例是关于如何创建 Puppet 支持的可部署资源，该资源需要用户名和密码身份验证。用户名和密码访问权限意味着，用户必须从计算资源手动登录到 Puppet 主计算机，才能调用 Puppet 配置管理。

或者，您可以配置远程访问身份验证，从而在云模板中设置配置管理，以便计算资源能在 Puppet 主计算机上进行身份验证。启用远程访问后，计算资源会自动生成密钥以满足密码身份验证。仍需要使用有效的用户名。

有关如何在 vRealize Automation Cloud Assembly 蓝图中配置不同 Puppet 场景的更多示例，请参见[AWS Puppet 配置管理云模板示例](#)和[vCenter Puppet 配置云模板示例](#)。

### 前提条件

- 在有效的网络上设置 Puppet Enterprise 实例。
- 使用集成功能将 Puppet Enterprise 实例添加到 vRealize Automation Cloud Assembly。请参见在[vRealize Automation Cloud Assembly 中配置 Puppet Enterprise 集成](#)
- 设置 vSphere 帐户和 vCenter 计算资源。



**步骤**

- 1 将 Puppet 配置管理组件添加到所需云模板的画布上的 vSphere 计算资源中。
  - a 选择**基础架构 > 管理 > 集成**。
  - b 单击**添加集成**，然后选择 Puppet。
  - c 在 Puppet 配置页面上输入相应的信息。

配置	说明	示例值
主机名	Puppet 主计算机的主机名或 IP 地址	Puppet-Ubuntu
SSH 端口	用于在 vRealize Automation Cloud Assembly 和 Puppet 主计算机之间进行通信的 SSH 端口。（可选）	不适用
Autosign 密钥	Puppet 主计算机上配置的共享密钥，节点应提供此共享密钥以支持 autosign 证书请求。	特定于用户
位置	指示 Puppet 主计算机是位于私有云还是公有云上。  <b>注</b> 仅当部署计算资源与 Puppet 主计算机之间存在连接时，才支持跨云部署。	
Cloud proxy	公有云帐户（如 Microsoft Azure 或 Amazon Web Services）不需要此配置。如果您使用的是基于 vCenter 的云帐户，请为您的帐户选择相应的 cloud proxy。	不适用
用户名	Puppet 主计算机的 SSH 和 RBAC 用户名。	特定于用户。YAML 值为 “\${input.username}”
密码	Puppet 主计算机的 SSH 和 RBAC 密码。	特定于用户。YAML 值为 “\${input.password}”
Use sudo commands for this user	选择对 procidd 使用 sudo 命令。	true
名称	Puppet 主计算机名称。	PEMasterOnPrem
说明		

- 2 将用户名和密码属性添加到 Puppet YAML，如以下示例中所示。
- 3 确保 Puppet 云模板 YAML 的 remoteAccess 属性值设置为 authentication: username and password，如以下示例中所示。

**示例：vCenter 用户名和密码 YAML 代码**

以下示例显示了用于在 vCenter 计算资源上添加用户名和密码身份验证的具有代表性的 YAML 代码。

```
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 配置管理云模板示例

有多个选项可用于配置云模板，以支持对 AWS 计算资源进行基于 Puppet 的配置管理。

### 使用用户名和密码对 AWS 进行 Puppet 管理

示例...	示例蓝图 YAML
<p>对任何受支持的 Amazon 计算机映像进行云配置身份验证。</p>	<pre>inputs:   username:     type: string     title: Username     default: puppet   password:     type: string     title: Password     encrypted: true     default: VMware@123 resources:   Webserver:     type: Cloud.AWS.EC2.Instance     properties:       flavor: small       image: centos       cloudConfig:           #cloud-config         ssh_pwauth: yes         chpasswd:           list:               \${input.username}:\${input.password}           expire: false       users:         - default         - name: \${input.username}           lock_passwd: false           sudo: ['ALL=(ALL) NOPASSWD:ALL']           groups: [wheel, sudo, admin]           shell: '/bin/bash'           ssh-authorized-keys:             - ssh-rsa               AAAAB3NzaC1yc2EAAAADAQABAAQDytVL+Q6/+vGbmKXoRpX               dmettem@dmettem-m01.vmware.com       runcmd:         - echo "Defaults:\${input.username} !requiretty"         &gt;&gt; /etc/sudoers.d/\${input.username}   Puppet_Agent:     type: Cloud.Puppet     properties:       provider: PEOonAWS       environment: production       role: 'role::linux_webserver'       host: '\${Webserver.*}'       osType: linux       username: '\${input.username}'       password: '\${input.password}'       useSudo: true</pre>
<p>使用现有用户对自定义 Amazon 计算机映像进行云配置身份验证。</p>	<pre>inputs:   username:     type: string     title: Username     default: puppet</pre>

示例...

示例蓝图 YAML

```

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
        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

```

## 使用 generatedPublicPrivateKey 对 AWS 进行 Puppet 管理

示例...

示例蓝图 YAML

使用 generatedPublicPrivateKey  
访问权限对 AWS 进行  
remoteAccess.authentication 身份  
验证

```

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

```

## **vCenter Puppet 配置云模板示例**

有多种方式可配置云模板，以支持对 vCenter 计算资源进行基于 Puppet 的配置管理。

### **vSphere 上的 Puppet，具有用户名和密码身份验证**

以下示例显示了 vSphere OVA 上 Puppet 的示例 YAML 代码，该 Puppet 具有用户名和密码身份验证。

表 6-5.

示例...	示例蓝图 YAML
<p>vSphere OVA 上 Puppet 的 YAML 代码，该 Puppet 具有用户名和密码身份验证。</p>	<pre> inputs:   username:     type: string     title: Username     default: puppet   password:     type: string     title: Password     encrypted: true     default: VMware@123 resources:   Puppet_Agent:     type: Cloud.Puppet     properties:       provider: PEonAWS       environment: dev       role: 'role::linux_webserver'       username: '\${input.username}'       password: '\${input.password}'       useSudo: true       host: '\${Webserver.*}'       osType: linux       agentConfiguration:         runInterval: 15m         certName: '\${Machine.address}'   Webserver:     type: Cloud.vSphere.Machine     properties:       cpuCount: 1       totalMemoryMB: 1024       imageRef: &gt;- 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>vSphere OVA 上 Puppet 的 YAML 代码，该 Puppet 对计算资源进行用户名和密码身份验证。</p>	<pre> inputs:   username:     type: string     title: Username     default: puppet </pre>

表 6-5. (续)

示例...	示例蓝图 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: &gt;- 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>vCenter 上 Puppet 的 YAML 代码，该 Puppet 对计算资源启用了远程访问密码身份验证。</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>

表 6-5. (续)

示例...	示例蓝图 YAML
	<pre>description: Password for the given username to install Puppet agent resources:   Puppet-Ubuntu:     type: Cloud.vSphere.Machine     properties:       flavor: small       imageRef: &gt;-         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>



## vSphere 上的 Puppet，具有生成的 PublicPrivateKey 身份验证

表 6-6.

示例...	示例蓝图 YAML
vSphere OVA 上 Puppet 的 YAML 代码，具有针对计算资源的生成的 PublicPrivateKey 身份验证。	<pre> inputs: {} resources:   Machine:     type: Cloud.vSphere.Machine     properties:       flavor: small       imageRef: &gt;- 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>

## 如何在 vRealize Automation Cloud Assembly 中包括 Terraform 配置

可以在 vRealize Automation Cloud Assembly 中将 Terraform 配置作为资源嵌入到云模板中。

### 准备 vRealize Automation Cloud Assembly Terraform 运行时环境

包含 Terraform 配置的设计需要访问与 vRealize Automation Cloud Assembly 内部部署产品集成的 Terraform 运行时环境。

#### 如何添加 Terraform 运行时

运行时环境包含一个 Kubernetes 集群，该集群通过运行 Terraform CLI 命令执行请求的操作。此外，运行时还会收集日志并返回 Terraform CLI 命令生成的结果。

vRealize Automation 内部部署产品需要用户配置自己的 Terraform 运行时 Kubernetes 集群。每个组织仅支持一个 Terraform 运行时。该组织的所有 Terraform 部署都使用同一个运行时。

1 验证您是否具有要在其上运行 Terraform CLI 的 Kubernetes 集群。

- 所有用户均可提供 kubeconfig 文件，以在非受管 Kubernetes 集群上运行 Terraform CLI。
- Enterprise 许可证用户可以选择在 vRealize Automation 管理的 Kubernetes 集群上运行 Terraform CLI。

- 在 vRealize Automation Cloud Assembly 中，转到[基础架构 > 资源 > Kubernetes](#)，然后验证您是否具有 Kubernetes 集群。如果需要添加一个集群，请参见[如何在 vRealize Automation Cloud Assembly 中使用 Kubernetes](#)。
- 如果新添加或修改了 Kubernetes 集群，请等待其数据收集完成。  
数据收集将检索命名空间列表和其他信息，并且可能需要长达 5 分钟的时间，具体取决于提供商。
  - 数据收集完成后，请转到[基础架构 > 集成 > 添加集成](#)，然后选择 **Terraform 运行时**卡视图。
  - 输入设置。

图 6-3. Terraform 运行时集成示例

New Integration

Name \*

OurOrg TF Runtime

Description

Terraform Runtime Integration

Kubernetes cluster \*

OurK8Cluster

Kubernetes namespace \*

OurK8Namespace

Runtime Container Settings

Image

docker.io/hashicorp/terraform:0.12.24

CPU request (Millicores)

250

CPU limit (Millicores)

250

Memory request (MB)

512

Memory limit (MB)

512

VALIDATE

设置	说明
名称	为运行时集成提供唯一的名称。
说明	阐明集成的目标。
Terraform 运行时集成:	
运行时类型（仅限 Enterprise）	Enterprise 许可证用户可以选择是在 vRealize Automation 管理的 Kubernetes 集群上运行 Terraform CLI 还是在非受管集群上运行。

设置	说明
Kubernetes kubeconfig（所有用户）	对于非受管 Kubernetes 集群，请粘贴外部集群的 kubeconfig 文件的全部内容。 要通过代理服务器使用外部 Kubernetes 运行时，请参见 <a href="#">如何添加代理支持</a> 。 此选项适用于所有用户。
Kubernetes 集群（仅限 Enterprise）	对于 vRealize Automation 管理的 Kubernetes，请选择要在其中运行 Terraform CLI 的集群。 集群及其 kubeconfig 文件必须可访问。可以在 /cmx/api/resources/k8s/clusters/{clusterId}/kube-config 上使用 GET 验证是否可以访问 kubeconfig。 此选项仅适用于 Enterprise 许可证。
Kubernetes 命名空间	选择要在集群中使用的命名空间，以便创建运行 Terraform CLI 的 Pod。
运行时容器设置：	
映像	输入要运行的 Terraform 版本的容器映像的路径。 <b>注</b> “验证”按钮不会检查容器映像。
CPU 请求	输入运行容器的 CPU 量。默认值为 250 个毫核。
CPU 限制	输入运行容器允许的最大 CPU 量。默认值为 250 个毫核。
内存请求	输入运行容器的内存量。默认值为 512 MB。
内存限制	输入运行容器允许的最大内存量。默认值为 512 MB。

5 单击**验证**并根据需要调整设置。

6 单击**添加**。

将缓存设置。添加集成后，可以修改集群或命名空间等设置，但可能需要长达 5 分钟的时间才能检测到更改，且 Terraform CLI 才能在新设置下运行。

## Terraform 运行时故障排除

某些 Terraform 配置部署问题可能与运行时集成有关。

问题	原因	解决方案
验证失败，并显示错误，指出命名空间无效。	您修改了集群，但在 UI 中仍保留以前的命名空间。	始终在修改集群选择后重新选择命名空间。
“命名空间”下拉列表为空或不列出新添加的命名空间。	集群的数据收集尚未完成。输入或修改集群后，数据收集需要长达 5 分钟才能完成，输入或修改命名空间后，需要长达 10 分钟才能完成。	对于具有现有命名空间的新集群，请等待 5 分钟，以便数据收集完成。 对于现有集群中的新命名空间，请等待 10 分钟，以便数据收集完成。 如果问题仍然存在，请移除集群，然后在 <b>基础架构 &gt; 资源 &gt; Kubernetes</b> 下重新添加集群。

问题	原因	解决方案
Terraform CLI 容器在以前的集群、以前的命名空间或使用以前的运行时设置创建，即使更新集成帐户后也是如此。	vRealize Automation 使用的 Kubernetes API 客户端将缓存 5 分钟。	所做的更改可能需要长达 5 分钟的时间才会生效。
验证或 Terraform 部署操作失败，并显示错误，指出 kubeconfig 不可用。	有时，由于无法从 vRealize Automation 访问集群，会出现这些错误。 在其他一些情况下，用户凭据、令牌或证书无效也会导致出现这些错误。	导致出现 Kubeconfig 错误的可能原因有很多，可能需要技术支持介入才能进行故障排除。

## 如何添加代理支持

要通过代理服务器连接外部 Kubernetes 运行时集群，请执行以下步骤。

- 1 登录到 Kubernetes 群集服务器。
- 2 创建一个空文件夹。
- 3 在新文件夹中，将以下行添加到名为 Dockerfile 的新文件中。

```
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 修改占位符值，以便 https\_proxy 和 http\_proxy 环境变量包括用于访问 Internet 的代理服务器设置。

*protocol* 将为 http 或 https，具体取决于代理服务器使用的协议，这可能与 https\_proxy 或 http\_proxy 的环境变量名称不匹配。

- 5 保存并关闭 Dockerfile。
- 6 从空文件夹中，运行以下命令。根据您的帐户特权，您可能需要在 sudo 模式下运行该命令。

```
docker build --file Dockerfile --tag custom-terraform-runtime:1.0 .
```

该命令将创建本地 custom-terraform-runtime:1.0 Docker 映像。

- 7 在 vRealize Automation Cloud Assembly 中的 **基础架构 > 连接 > 集成** 下，转到您的 Terraform 运行时集成。
- 8 创建或编辑运行时容器设置以使用 custom-terraform-runtime:1.0 映像：

Runtime Container Settings

Image  ⓘ

## 无法访问 Internet 情况下的 vRealize Automation Cloud Assembly Terraform 运行时

如果 vRealize Automation Cloud Assembly 用户需要设计并运行 Terraform 集成但 Internet 连接已断开，则可以按照以下示例设置其运行时环境。

**注** 必须在设置过程中暂时连接到 Internet。

此过程假设您具有自己的 [Docker 注册表](#)，无需 Internet 连接即可访问其存储库。

### 创建自定义容器映像

- 1 构建包括 Terraform 提供程序插件二进制文件的自定义容器映像。

以下 Dockerfile 显示了使用 Terraform GCP 提供程序创建自定义映像的示例。

Dockerfile 中的基础映像 `projects.registry.vmware.com/vra/terraform:latest` 下载需要暂时通过 Internet 访问位于 `projects.registry.vmware.com` 的 VMware Harbor 注册表。

防火墙设置或代理设置可能会导致映像构建失败。可能需要启用对 `releases.hashicorp.com` 的暂时访问，以下载 Terraform 提供程序插件二进制文件。但是，可以选择使用专用注册表提供插件二进制文件。

```
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 构建、标记自定义容器映像，以及将自定义容器映像推送到您自己的 Docker 存储库。
- 3 在 vRealize Automation Cloud Assembly 中的 **基础架构 > 连接 > 集成** 下，转到您的 Terraform 运行时集成。
- 4 创建或编辑运行时容器设置，以将您的存储库添加到自定义容器映像上。构建的自定义容器映像名称示例为 `registry.ourcompany.com/project1/image1:latest`。

Runtime Container Settings

Image	<input type="text" value="registry.ourcompany.com/project1/image1:latest"/> ⓘ
-------	---

## 在本地托管 Terraform CLI

- 1 下载 Terraform CLI 二进制文件。
- 2 将 Terraform CLI 二进制文件上传到本地 Web 服务器。
- 3 在 vRealize Automation Cloud Assembly 中，转到[基础架构 > 配置 > Terraform 版本](#)。
- 4 创建或编辑 Terraform 版本，以便包含在本地 Web 服务器上托管的 Terraform CLI 二进制文件的 URL。

0.12.29 DELETE	
Version *	0.12.29 ⓘ
Description	<input type="text"/>
Enabled	<input checked="" type="checkbox"/> ⓘ
URL *	http://host1.ourcompany.com:8080/tf/0.12.29/terraform_0.12.29_linux_amd64.zip ⓘ
SHA256 Checksum *	872245d9c6302b24dc0d98a1e010aef1e4ef60865a2d1f60102c8ad03e9d5a1d ⓘ

## 设计和部署 Terraform 配置

运行时准备就绪后，可以将 Terraform 配置文件添加到 git，为其设计云模板并进行部署。

要开始使用，请参见在 [vRealize Automation Cloud Assembly 中准备 Terraform 配置](#)。

## 故障排除

部署时，在 vRealize Automation Cloud Assembly 中打开部署。在“历史记录”选项卡下，查找 Terraform 事件，然后单击右侧的[显示日志](#)。本地 Terraform 提供程序正常运行时，日志中会显示以下消息。

```
Initializing provider plugins
```

```
Terraform has been successfully initialized
```

要获得更可靠的日志，可以手动编辑云模板代码以添加 `TF_LOG: DEBUG`，如以下示例所示。

```
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
```

## 在 vRealize Automation Cloud Assembly 中准备 Terraform 配置

将 Terraform 配置添加到 vRealize Automation Cloud Assembly 模板之前，请先设置并集成版本控制存储库。

- 1 必备条件
- 2 将 Terraform 配置文件存储在版本控制存储库中
- 3 启用云区域映射
- 4 将存储库与 vRealize Automation Cloud Assembly 集成

### 必备条件

要使 vRealize Automation 内部部署产品运行 Terraform 操作，需要 Terraform 运行时集成。请参见[准备 vRealize Automation Cloud Assembly Terraform 运行时环境](#)。

### 将 Terraform 配置文件存储在版本控制存储库中

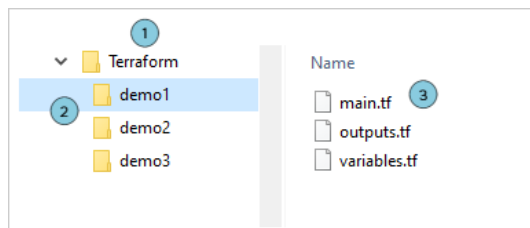
vRealize Automation Cloud Assembly 对 Terraform 配置支持以下版本控制存储库。

- GitHub 云，GitHub Enterprise 内部部署
- GitLab 云
- Bitbucket 内部部署

在版本控制存储库中，创建具有一层子目录的默认目录，每个子目录中都有 Terraform 配置文件。为每个 Terraform 配置创建一个子目录。

- 1 默认目录
- 2 单个子目录层
- 3 部署就绪的 Terraform 配置文件

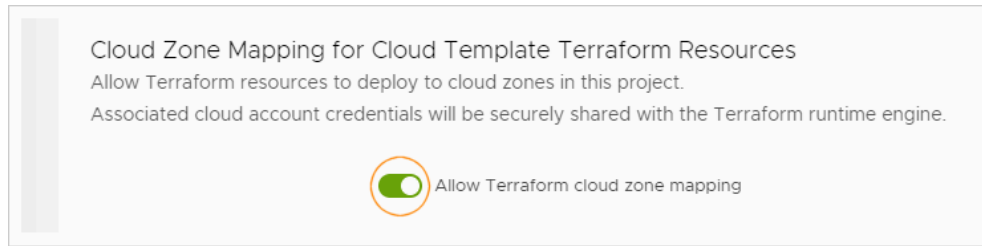
不要在配置文件中包含 Terraform 状态文件。如果存在 `terraform.tfstate`，则部署时将出错。



### 启用云区域映射

如果希望部署到云帐户，Terraform 运行时引擎需要这些云区域凭据。

在项目的**置备**选项卡中，启用**允许 Terraform 云区域映射**。



即使已安全地传输凭据，为加强安全性，也应在项目用户不需要部署到云帐户的情况下将该选项保持停用状态。

## 将存储库与 vRealize Automation Cloud Assembly 集成

在 vRealize Automation Cloud Assembly 中，转到**基础架构 > 连接 > 集成**。

将集成添加到存储 Terraform 配置的存储库产品类型：**GitHub**、**GitLab** 或 **Bitbucket**。

将项目添加到集成时，请选择 **Terraform 配置** 类型，然后确定存储库和分支。

**文件夹**是之前结构的默认目录。

Add Repository: testProject

Configure a repository to be used for this project.

Type *	Terraform Configurations	ⓘ
Repository *	parnassusdemo/repository1	ⓘ
Branch *	master	
Folder	/Terraform	

## 在 vRealize Automation Cloud Assembly 中为 Terraform 配置进行设计

存储库和 Terraform 配置文件准备就绪后，可以为其设计 vRealize Automation Cloud Assembly 模板。

- 1 必备条件
- 2 启用 Terraform 运行时版本
- 3 将 Terraform 资源添加到设计中
- 4 部署云模板

### 必备条件

设置和集成您的版本控制存储库。请参见在 [vRealize Automation Cloud Assembly 中准备 Terraform 配置](#)。



## 启用 Terraform 运行时版本

可以定义在部署 Terraform 配置时可供用户使用的 Terraform 运行时版本。请注意，Terraform 配置可能还包括内部编码的版本限制。

要创建允许的版本列表，请转到**基础架构 > 配置 > Terraform 版本**。仅支持版本 0.12.x。

## 将 Terraform 资源添加到设计中

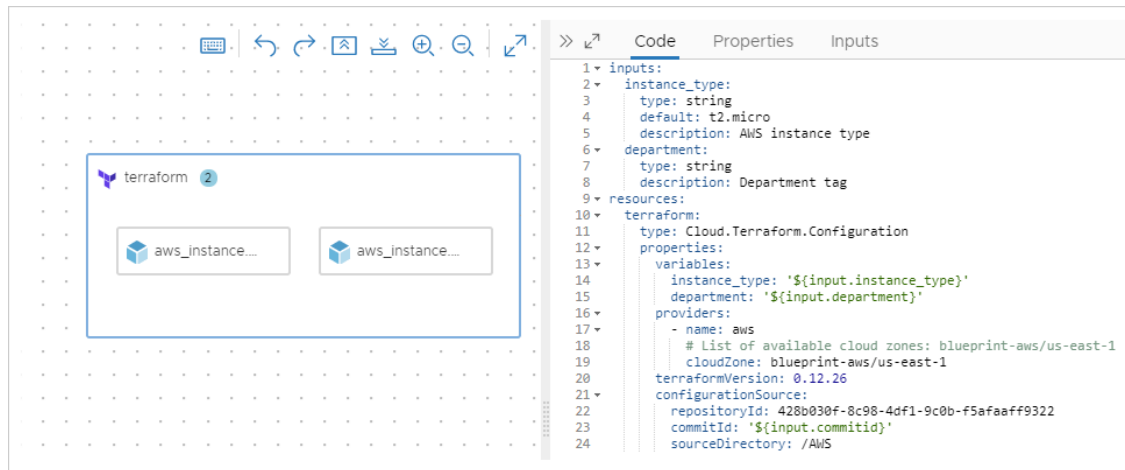
创建包含 Terraform 配置的云模板。

- 1 在 vRealize Automation Cloud Assembly 中，转到**设计 > 云模板**，然后单击**新建自 > Terraform**。  
将显示“Terraform 配置”向导。
- 2 按照提示进行操作。

向导页面	设置	值
新建云模板	名称	为设计提供一个标识名称。
	说明	阐明设计的目标。
	项目	选择包含存储 Terraform 配置的存储库集成的项目。
配置源	存储库	选择存储 Terraform 配置的集成存储库。
	提交	选择存储库提交，或将该条目留空以使用存储库 HEAD 的 Terraform 配置。 <b>Bitbucket 限制</b> - 由于 Bitbucket 存储库服务器配置，可选择的提交数量可能会被截断。
	源目录	从所创建的存储库结构选择一个子目录。前面设置中显示的示例子目录为 demo1、demo2 和 demo3。
完成配置	存储库	验证是否选择了正确的存储库。
	源目录	验证是否选择了正确的目录。
	Terraform 版本	选择部署 Terraform 配置时要运行的 Terraform 运行时版本。
	提供商	如果 Terraform 配置包括提供商块，请验证此云模板将部署到的提供商和云区域。 没有提供商不是问题。完成向导后，只需在模板属性中编辑提供商和云区域即可添加或更改部署目标。
	变量	选择要加密的敏感值，例如密码。
	输出	验证 Terraform 配置的输出，该输出可转换为您的设计代码可进一步引用的表达式。

- 3 单击**创建**。

Terraform 资源将显示在云模板画布中，其中包含反映了要部署的 Terraform 配置的 vRealize Automation Cloud Assembly 代码。



如果需要，可以向云模板中添加其他 vRealize Automation Cloud Assembly 资源，以将 Terraform 和非 Terraform 代码组合为混合设计。

**注** 更新存储库中的 Terraform 配置不会将所做的更改同步到云模板。自动同步可能会带来安全风险，例如新添加的敏感变量。

要捕获 Terraform 配置更改，请重新运行向导，选择新的提交，然后识别任何新的敏感变量。

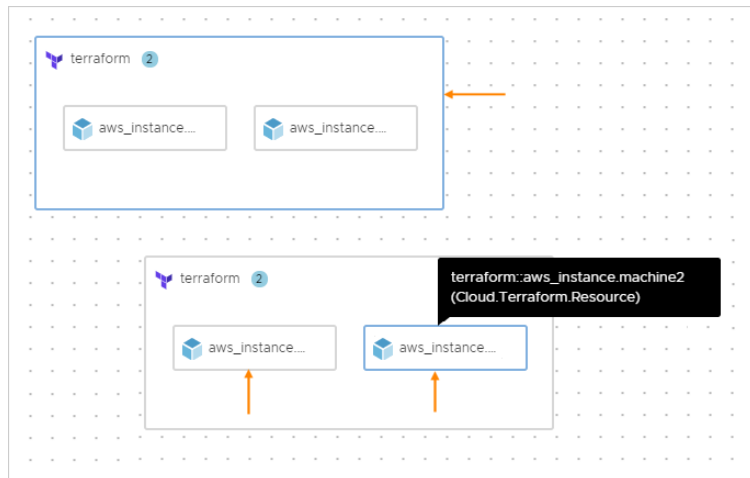
## 部署云模板

部署云模板时，可以在部署的**历史记录**选项卡中展开事件（例如分配或创建阶段），以查看 Terraform CLI 消息日志。

批准 - 除了预期 Terraform 阶段（如计划、分配或创建）外，vRealize Automation Cloud Assembly 还通过批准阶段引入了监管。有关请求批准的详细信息，请参见[如何配置 Service Broker 批准策略](#)。

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	<a href="#">Hide Logs</a> <pre> 2:24:23 PM * provider.random: version = "&gt; 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> <a href="#">View as plain text</a>
Aug 3, 202...	INITIALIZATION_FINISH...			
Aug 3, 202...	INITIALIZATION_IN_PRO...			

部署后，您会看到一个表示整个 Terraform 组件的外部资源，其中包含 Terraform 创建的单个组件的子资源。父 Terraform 资源控制子资源的生命周期。



## 了解有关 vRealize Automation 中 Terraform 配置的更多信息

在 vRealize Automation 中将 Terraform 配置作为资源嵌入时，请注意某些限制和故障排除。

### Terraform 配置限制

- 验证包含 Terraform 配置的设计时，“测试”按钮会检查 vRealize Automation Cloud Assembly 语法，但不会检查本机 Terraform 代码语法。

此外，“测试”按钮不会验证与 Terraform 配置关联的提交 ID。

- 对于包含 Terraform 配置的云模板，将模板克隆到其他项目需要应用以下解决办法。
  - 在新项目中，在**集成**选项卡下，复制您的集成的 repositoryId。
  - 打开克隆模板。在代码编辑器中，将 repositoryId 替换为所复制的值。
- 在版本控制存储库中，不要在配置文件中包含 Terraform 状态文件。如果存在 terraform.tfstate，则部署时将出错。

### 对父 Terraform 资源支持的实施后操作

对于父 Terraform 资源，可以查看或刷新 Terraform 状态文件。有关状态文件操作的详细信息，请参见[可以对 vRealize Automation Cloud Assembly 部署运行哪些操作](#)中的完整操作列表。

### 对子资源支持的实施后操作

部署 Terraform 配置后，可能需要长达 20 分钟才能对子资源执行实施后操作。

对于 Terraform 配置中的子资源，仅支持以下部分实施后操作。有关这些操作的详细信息，请在[可以对 vRealize Automation Cloud Assembly 部署运行哪些操作](#)中的完整操作列表中查找这些操作。

提供商	Terraform 资源类型	支持的实施后操作
AWS	aws_instance	打开电源
		关闭电源
		重新引导

提供商	Terraform 资源类型	支持的实施后操作
		重置
Azure	azurerm_virtual_machine	打开电源
		关闭电源
		重新启动
		挂起
vSphere	vsphere_virtual_machine	打开电源
		关闭电源
		重新引导
		重置
		关机
		挂起
		创建快照
		删除快照
GCP	google_compute_instance	恢复快照
		打开电源
		关闭电源
		创建快照
		删除快照

## 对实施后操作可用性进行故障排除

如果即时可用 (OOTB) 实施后操作缺失或处于停用状态，可能需要进行故障排除。

问题	原因	解决方案
Terraform 资源在“操作”菜单上没有预期的 OOTB 实施后操作。	上述列表中提到的提供者或资源类型可能不支持该操作。或者，根据资源发现和资源缓存计时，可能需要长达 20 分钟才能显示该操作。	检查设计中的提供者和资源类型。 等待 20 分钟，以完成数据收集。
即使在数据收集所用的 20 分钟后，Terraform 资源也没有预期的实施后操作。	资源发现问题导致该操作无法显示。 在项目外的云区域中意外创建资源时，会发生此问题。例如，您的项目仅包括云帐户和区域 us-east-1 云区域，但 Terraform 配置包括 us-west-1 提供商块，并且您在设计时未进行更改。 另一种可能的情况是数据收集不起作用。	根据设计中的云区域检查项目云区域。 转到 <a href="#">基础架构 &gt; 连接 &gt; 云帐户</a> ，然后检查云帐户的数据收集状态和上次成功收集时间。

问题	原因	解决方案
即使资源状态和数据收集没有明显的问题，实施后操作也会处于停用状态（灰显）。	偶尔会出现间歇性计时问题和数据收集失败，这些是已知问题。	该问题应会在 20 分钟内自行解决。
错误的实施后操作处于停用状态，该操作应基于资源状态处于活动状态。 例如，“关闭电源”处于启用状态，“打开电源”处于停用状态，即使使用提供商界面关闭了资源的电源也是如此。	数据收集计时可能会导致暂时不匹配。如果从 vRealize Automation 外部更改电源状态，则需要一些时间才能正确反映所做的更改。	等待 20 分钟。

## 在 vRealize Automation 中使用自定义 Terraform 提供程序

如果创建了自定义 Terraform 提供程序并希望使用，请执行以下步骤。

- 1 在 git 版本控制存储库中的默认 Terraform 目录下，添加以下子目录结构。

```
terraform.d/plugins/linux_amd64
```

- 2 将自定义 Terraform 提供程序 Go 二进制文件添加到 linux\_amd64 目录。

默认情况下，terraform init 将在该目录中搜索自定义提供程序插件。

**注** VMware 遇到过自定义 Terraform 提供程序无法运行并发布 no such file or directory 消息的情况。

如果发生这种情况，请尝试重新编译自定义提供程序 Go 二进制文件并停用 CGO（设置为零）。CGO 适用于调用 C 代码的 Go 软件包。

## 如何使用 vRealize Automation Cloud Assembly 商城

要快速启动资源库，请从 vRealize Automation Cloud Assembly 商城下载文件。商城提供了完成的云模板和开放的虚拟化映像。

### 如何访问商城

在 vRealize Automation Cloud Assembly 中，选择**基础架构 > 连接 > 集成**。单击**添加集成**，单击**My VMware**，并提供您的 My VMware 帐户凭据。

### 如何下载和使用商城云模板文件

在**商城**选项卡中，单击**获取**，并接受云模板 EULA。然后，您可以将云模板添加到 vRealize Automation Cloud Assembly 项目，或仅下载。您可以在**设计**选项卡中上载云模板。

对于基于项目的示例，假设您是大数据工作的项目管理员。为了帮助您的团队，您可以找到添加到团队项目中的商城 Hadoop 模板。然后，自定义您的资源环境的云模板，并发布。之后，将模板导入 vRealize Automation Service Broker 目录，以便您的团队可以进行部署。

## 如何下载和使用商城映像文件

在**商城**选项卡中，单击**获取**，并接受 OVF 或 OVA 映像 EULA。之后，您可以下载 OVF 或 OVA 映像，并在云模板代码中引用该映像。

继续前一示例，您的团队可能需要访问 Hadoop 本身的版本。您可以下载 Hadoop OVF，并将它添加到云帐户资源，例如 vCenter Server Content Library。然后，您可以更新需要指向 OVF 映像的任何模板代码。

# 管理 vRealize Automation Cloud Assembly 部署

7

作为 vRealize Automation Cloud Assembly 云模板开发人员，您可以使用“部署”选项卡来管理您的部署。您可以对失败的置备过程进行故障排除，进行更改，并销毁未使用的部署。

部署是云模板的已置备实例。“部署”选项卡显示成功的部署和失败的部署。您可以使用该页面管理成功的部署，或开始对任何失败的请求进行故障排除。

## 使用部署卡

可以使用卡列表来查找和管理部署。您可以筛选或搜索特定部署，然后对这些部署运行操作。

- 1 根据属性筛选请求。
- 2 根据关键字或请求者搜索部署。
- 3 对列表进行排序，以便按时间或名称排序。
- 4 对部署运行部署级别操作，包括删除未使用的部署以回收资源。

还可以查看部署成本、到期日期和状态。



本章讨论了以下主题：

- 如何监控 vRealize Automation Cloud Assembly 中的部署
- vRealize Automation Cloud Assembly 部署失败时可以执行哪些操作
- 如何管理已完成 vRealize Automation Cloud Assembly 部署的生命周期
- 可以对 vRealize Automation Cloud Assembly 部署运行哪些操作

## 如何监控 vRealize Automation Cloud Assembly 中的部署

部署 vRealize Automation Cloud Assembly 云模板后，可以监控请求以确保资源已置备且正在运行。从部署卡开始，您可以验证资源的置备。接下来，您可以检查部署详细信息。最后，您可以查看已删除的部署。

### 步骤

- 1 如果需要，单击**部署**，并使用筛选和搜索找到您的进行中的部署卡。
- 2 查看卡状态。

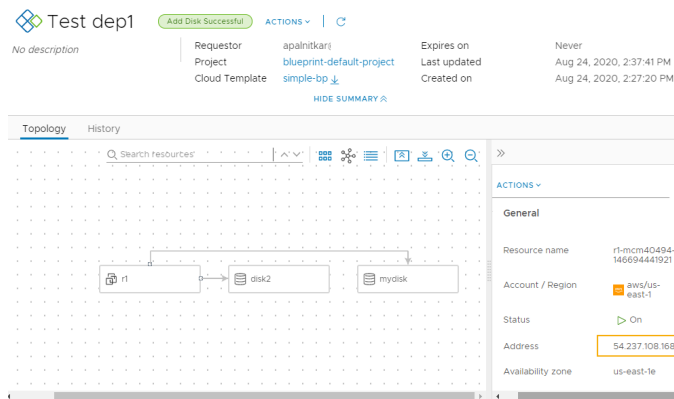
如果部署正在进行中，则进程栏会指示剩余任务数。如果部署成功完成，则卡会显示有关部署的基本详



细信息。

- 3 要确定资源的部署位置，请单击部署名称，然后在“拓扑”页面上查看详细信息。

您可能需要主要组件的 IP 地址。单击每个组件时，请注意提供的特定于组件的信息。在此示例中，将突出显示 IP 地址。



外部链接的可用性取决于云提供商。如果外部链接可用，您必须具有该提供商的凭据才能访问相应的组件。

### 后续步骤

- 您可以对部署进行更改。请参见如何管理已完成 vRealize Automation Cloud Assembly 部署的生命周期。
- 如果部署失败，请参见 vRealize Automation Cloud Assembly 部署失败时可以执行哪些操作。



## vRealize Automation Cloud Assembly 部署失败时可以执行哪些操作

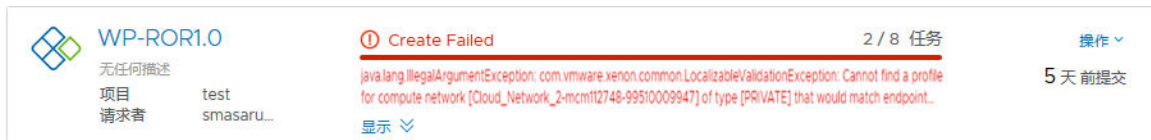
您的部署请求可能由于多种原因而失败。失败可能由网络流量、目标云提供商缺少资源或部署规范存在缺陷导致。或者，部署已成功，但部署无法正常工作。可以使用 vRealize Automation Cloud Assembly 检查部署，查看任何错误消息，并确定问题由环境、请求的工作负载规范还是其他因素导致。

您可以使用此工作流程来开始调查。该过程可能表明失败是由于暂时的环境问题造成的。确认情况改善后重新部署请求可以解决此类问题。在其他情况下，调查可能要求您详细检查其他方面。

作为项目成员，您可以在 vRealize Automation Cloud Assembly 中查看请求详细信息。

### 步骤

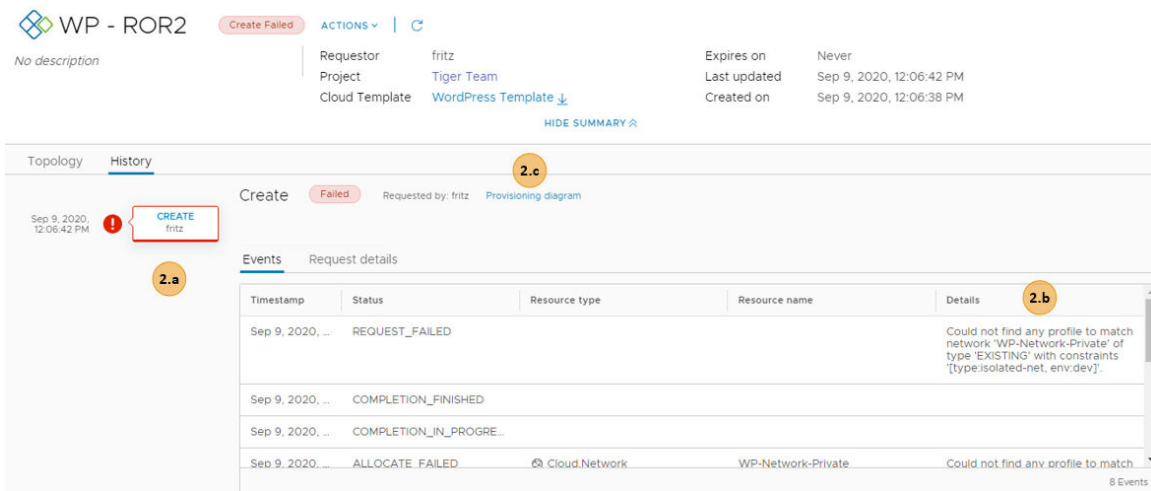
- 要确定某个请求是否失败，单击**部署**选项卡，然后找到部署卡。



该卡指明了失败的部署。

- 查看错误消息。
- 有关详细信息，请单击部署名称以了解部署详细信息。

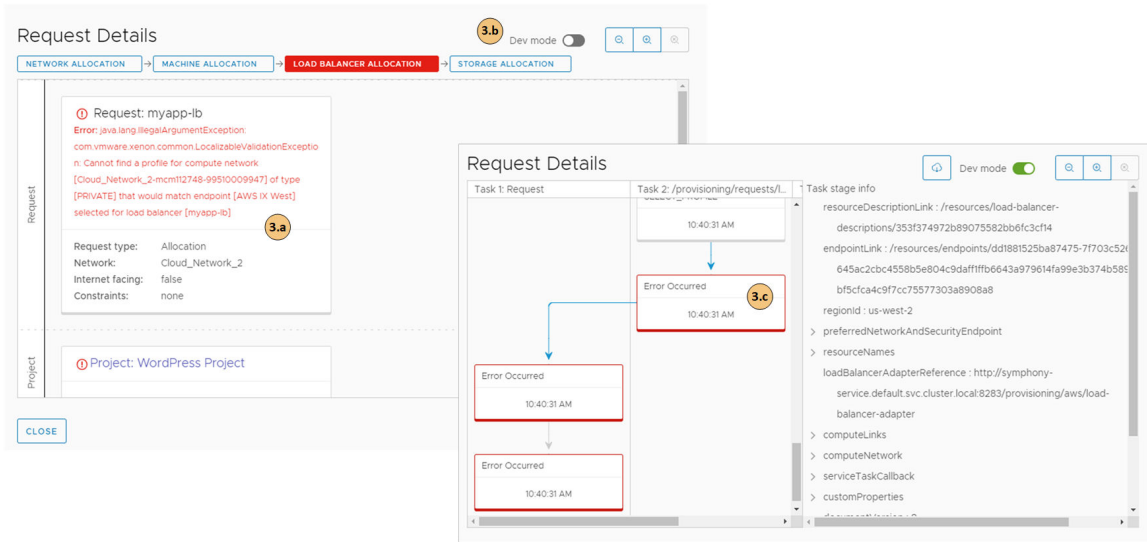
- 在部署详细信息页面中，单击**历史记录**选项卡。



- 查看事件树以确定置备过程失败的位置。在修改部署但更改失败时，该树很有用。该树还显示了运行部署操作的时间。您可以使用该树对失败的更改进行故障排除。
- 详细信息**提供错误消息的更详细版本。
- 如果请求的项是 vRealize Automation Cloud Assembly 云模板，则消息右侧的链接将打开 vRealize Automation Cloud Assembly，以便您可以查看**请求详细信息**。

### 3 请求详细信息提供故障组件的置备 workflow，以便您可以研究问题。

请求历史记录将保留一周。



- 查看错误消息。
- 打开**开发模式**可在简单置备 workflow 和更详细的流程图之间切换。
- 单击该卡以查看部署脚本。

### 4 解决错误并重新部署云模板。

这些错误可能存在于模板构造中，也可能与基础架构的配置方式有关。

#### 后续步骤

解决错误并部署云模板后，您可以在“请求详细信息”中看到类似以下示例的信息。要查看请求详细信息，请选择**基础架构 > 活动 > 请求**。



## 如何管理已完成 vRealize Automation Cloud Assembly 部署的生命周期

置备并运行部署后，您可以运行多个操作来管理部署。生命周期管理可以包括打开电源或关闭电源、调整部署大小以及删除部署。您还可以对各个组件运行各种操作以对其进行管理。

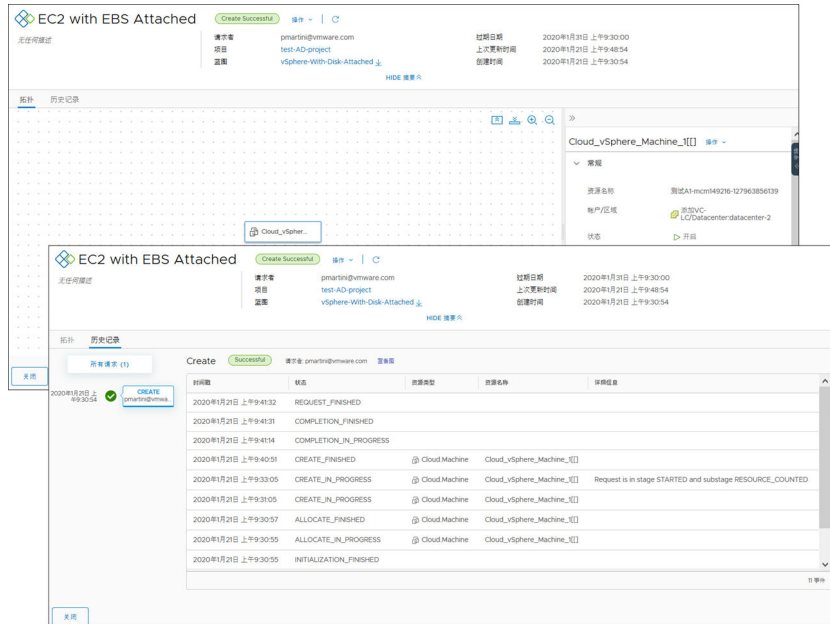
### 步骤

- 1 单击**部署**，并找到您的部署。
- 2 要访问部署详细信息，请单击部署名称。

可以使用“拓扑”选项卡来可视化部署结构和资源。

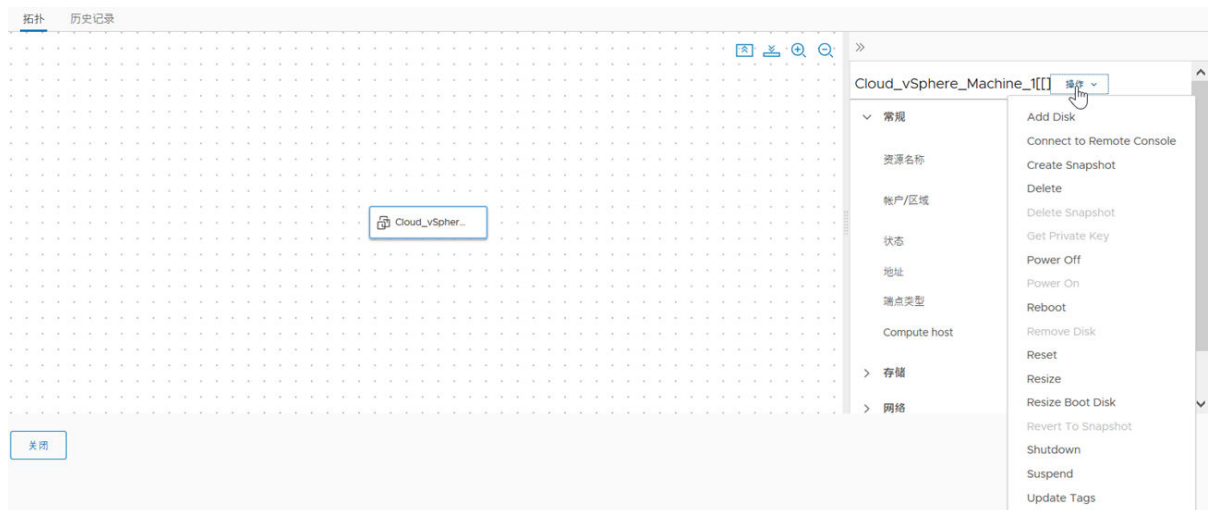
“历史记录”选项卡包含所有置备事件，以及与您部署请求后运行的操作相关的任何事件。如果置备过程存在任何问题，“历史记录”选项卡中的事件可帮助您对故障进行故障排除。

“成本”选项卡提供部分组件自部署以来的当前成本。



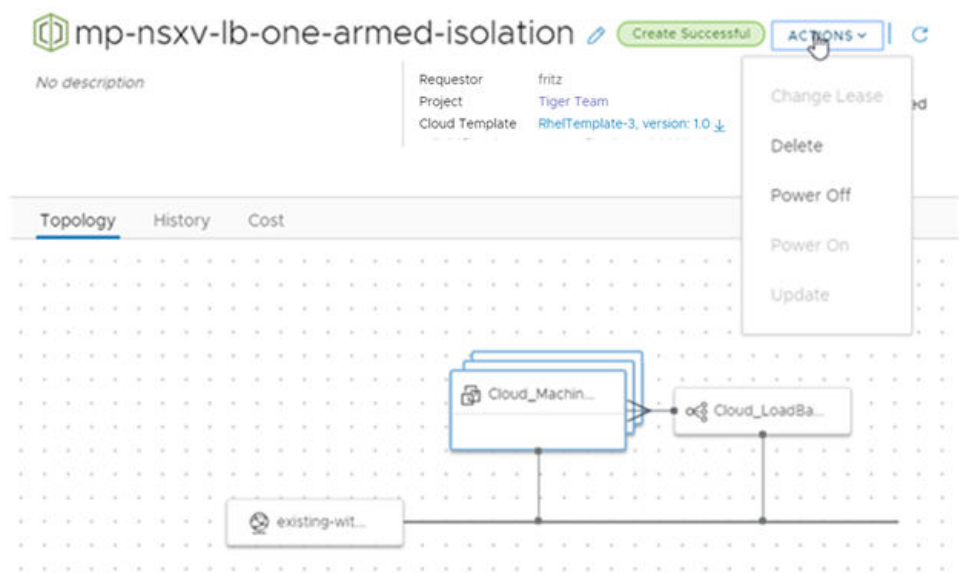
- 3 如果您确定部署的当前配置成本太高，并且希望调整组件大小，则可以在拓扑页面上选择该组件，然后在组件页面上选择**操作 > 调整大小**。

可用操作取决于组件、云帐户和您的权限。



- 4 作为开发生命周期的一部分，不再需要您的其中一个部署。要移除部署并回收资源，选择**操作 > 删除**。

可用操作取决于部署的状态。



后续步骤

要了解有关可能操作的详细信息，请参见[可以对 vRealize Automation Cloud Assembly 部署运行哪些操作](#)。

# 可以对 vRealize Automation Cloud Assembly 部署运行哪些操作

部署云模板之后，可以在 vRealize Automation Cloud Assembly 中运行操作来管理资源。可用操作取决于资源类型，以及这些操作在特定云帐户或集成平台上是否受支持。

可用操作还取决于管理员授权您运行的操作。

作为管理员或项目管理员，您可以在 vRealize Automation Service Broker 中设置“实施后操作”策略。请参见[如何授权使用者使用 Service Broker 实施后操作策略](#)

您可能还会看到列表中未包含的操作。这些操作可能是您的管理员添加的自定义操作。例如，[如何创建 vRealize Automation Cloud Assembly 自定义操作以对虚拟机执行 vMotion](#)。

表 7-1. 可能操作的列表

操作	应用到以下资源类型	适用于以下云帐户或集成	说明
添加磁盘	计算机	<ul style="list-style-type: none"><li>■ Amazon Web Services</li><li>■ Google Cloud Platform</li><li>■ Microsoft Azure</li><li>■ VMware vSphere</li></ul>	将其他磁盘添加到现有虚拟机。
更改租约	部署	<ul style="list-style-type: none"><li>■ Amazon Web Services</li><li>■ Microsoft Azure</li><li>■ VMware vSphere</li></ul>	<p>更改租约过期日期和时间。</p> <p>当租约过期时，将销毁部署并回收资源。</p> <p>租约策略在 vRealize Automation Service Broker 中设置。</p>

表 7-1. 可能操作的列表（续）

操作	应用到以下资源类型	适用于以下云帐户或集成	说明
更改安全组	计算机	<ul style="list-style-type: none"> <li>VMware vSphere</li> </ul>	<p>可以将安全组与部署中的计算机网络关联和解除关联。更改操作适用于 NSX-V 和 NSX-T 的现有安全组和按需安全组。此操作仅适用于单个计算机，而不适用于计算机集群。</p> <p>要将安全组与计算机网络相关联，部署中必须存在该安全组。</p> <p>将安全组与部署中所有计算机的所有网络解除关联不会从部署中移除安全组。</p> <p>这些更改不会影响作为网络配置文件一部分应用的安全组。</p> <p>此操作会更改计算机的安全组配置，但不会重新创建计算机。这是一项非破坏性更改。</p> <p>更改计算机上的安全组</p> <ul style="list-style-type: none"> <li>要更改计算机的安全组配置，请在拓扑窗格中选择计算机，然后在右侧窗格中单击<b>操作</b>菜单，并选择<b>更改安全组</b>。现在，您可以在安全组上添加或移除与计算机网络的关联。</li> </ul>
连接到远程控制台	计算机	<ul style="list-style-type: none"> <li>VMware vSphere</li> </ul>	<p>在所选计算机上打开远程会话。</p> <p>检查以下成功连接的要求。</p> <ul style="list-style-type: none"> <li>作为部署使用者，确认置备的计算机已打开电源。</li> </ul>
创建快照	计算机	<ul style="list-style-type: none"> <li>Google Cloud Platform</li> <li>VMware vSphere</li> </ul>	<p>创建虚拟机的快照。</p> <p>如果 vSphere 中仅允许您拥有两个快照且您已拥有它们，则该命令只有在删除一个快照之后才可用。</p>
删除	部署	<ul style="list-style-type: none"> <li>Amazon Web Services</li> <li>Google Cloud Platform</li> <li>Microsoft Azure</li> <li>VMware vSphere</li> </ul>	<p>销毁部署。</p> <p>将删除并回收所有资源。</p> <p>如果删除失败，则可以再次对部署运行删除操作。在第二次尝试期间，您可以选择<b>忽略删除失败</b>。如果选择此选项，则会删除部署，但可能无法回收资源。您应检查置备了部署的系统，以确保移除所有资源。如果没有，则必须手动删除这些系统上的剩余资源。</p>
	NSX 网关	<ul style="list-style-type: none"> <li>NSX</li> </ul>	从 NSX-T 或 NSX-V 网关删除 NAT 端口转发规则。
	计算机和负载均衡器	<ul style="list-style-type: none"> <li>Amazon Web Services</li> <li>Microsoft Azure</li> <li>VMware vSphere</li> <li>VMware NSX</li> </ul>	从部署中删除计算机或负载均衡器。此操作可能会导致部署不可用。
	安全组	<ul style="list-style-type: none"> <li>NSX-T</li> <li>NSX-V</li> </ul>	<p>如果安全组未与部署中的任何计算机相关联，则该过程会从部署中移除安全组。</p> <ul style="list-style-type: none"> <li>如果安全组为按需安全组，则会在端点上销毁。</li> <li>如果安全组为共享安全组，则操作将失败。</li> </ul>
删除快照	计算机	<ul style="list-style-type: none"> <li>VMware vSphere</li> <li>Google Cloud Platform</li> </ul>	删除虚拟机的快照。
编辑标记	部署	<ul style="list-style-type: none"> <li>Amazon Web Services</li> <li>Microsoft Azure</li> <li>VMware vSphere</li> </ul>	添加或修改应用于单个部署资源的资源标记。

表 7-1. 可能操作的列表（续）

操作	应用到以下资源类型	适用于以下云帐户或集成	说明
获取 Terraform 状态	Terraform 配置	<ul style="list-style-type: none"> <li>Amazon Web Services</li> <li>Google Cloud Platform</li> <li>Microsoft Azure</li> <li>VMware vSphere</li> </ul>	<p>显示 Terraform 状态文件。</p> <p>要查看对在云平台上部署的 Terraform 计算机所做的任何更改并更新部署，请先运行“刷新 Terraform 状态”操作，然后再运行此“获取 Terraform 状态”操作。</p> <p>该文件在对话框中显示时。该文件的可用时间大约为 1 小时，之后您需要运行新的刷新操作。如果以后需要该文件，可以进行复制。</p> <p>您还可以在“部署历史记录”选项卡上查看该文件。在“事件”选项卡上选择“获取 Terraform 状态”事件，然后单击<a href="#">请求详细信息</a>。如果文件未过期，请单击<a href="#">查看内容</a>。如果文件已过期，请重新运行“刷新”和“获取”操作。</p> 
关闭电源	部署	<ul style="list-style-type: none"> <li>Amazon Web Services</li> <li>Microsoft Azure</li> <li>VMware vSphere</li> </ul>	关闭部署，而不关闭客户机操作系统。
	计算机	<ul style="list-style-type: none"> <li>Amazon Web Services</li> <li>Google Cloud Platform</li> <li>Microsoft Azure</li> <li>VMware vSphere</li> </ul>	关闭计算机电源，而不关闭客户机操作系统。
打开电源	部署	<ul style="list-style-type: none"> <li>Amazon Web Services</li> <li>Microsoft Azure</li> <li>VMware vSphere</li> </ul>	打开部署。如果资源已挂起，则从资源挂起的时间点恢复正常操作。
	计算机	<ul style="list-style-type: none"> <li>Amazon Web Services</li> <li>Google Cloud Platform</li> <li>Microsoft Azure</li> <li>VMware vSphere</li> </ul>	打开计算机电源。如果计算机已挂起，则从计算机挂起的时间点恢复正常操作。
重新引导	计算机	<ul style="list-style-type: none"> <li>Amazon Web Services</li> <li>VMware vSphere</li> </ul>	<p>在虚拟机上重新引导客户机操作系统。</p> <p>对于 vSphere 计算机，要使用此操作，必须在计算机上安装 VMware Tools。</p>
重新配置	负载均衡器	<ul style="list-style-type: none"> <li>Amazon Web Services</li> <li>Microsoft Azure</li> <li>VMware NSX</li> </ul>	<p>更改负载均衡器大小和日志记录级别。</p> <p>此外，还可以添加或移除路由，以及更改协议、端口、运行状况配置和成员池设置。</p>
	NSX 网关端口转发	<ul style="list-style-type: none"> <li>NSX-T</li> <li>NSX-V</li> </ul>	对 NSX-T 或 NSX-V 网关添加、编辑或删除 NAT 端口转发规则。

表 7-1. 可能操作的列表（续）

操作	应用到以下资源类型	适用于以下云帐户或集成	说明
刷新 Terraform 状态	Terraform 配置	<ul style="list-style-type: none"> <li>■ Amazon Web Services</li> <li>■ Google Cloud Platform</li> <li>■ Microsoft Azure</li> <li>■ VMware vSphere</li> </ul>	<p>检索 Terraform 状态文件的最新迭代。</p> <p>要检索对在云平台上部署的 Terraform 计算机所做的任何更改并更新部署，请先运行此“刷新 Terraform 状态”操作。</p> <p>要查看文件，请对配置运行<b>获取 Terraform 状态</b>操作。</p> <p>使用“部署历史记录”选项卡监控刷新过程。</p>
移除磁盘	计算机	<ul style="list-style-type: none"> <li>■ Amazon Web Services</li> <li>■ Google Cloud Platform</li> <li>■ Microsoft Azure</li> <li>■ VMware vSphere</li> </ul>	从现有虚拟机中移除磁盘。
重置	计算机	<ul style="list-style-type: none"> <li>■ Amazon Web Services</li> <li>■ Google Cloud Platform</li> <li>■ VMware vSphere</li> </ul>	强制虚拟机重新启动，而不关闭客户机操作系统。
调整大小	计算机	<ul style="list-style-type: none"> <li>■ Amazon Web Services</li> <li>■ Microsoft Azure</li> <li>■ Google Cloud Platform</li> <li>■ VMware vSphere</li> </ul>	增加或减少虚拟机的 CPU 和内存。
调整引导磁盘大小	计算机	<ul style="list-style-type: none"> <li>■ Amazon Web Services</li> <li>■ Google Cloud Platform</li> <li>■ Microsoft Azure</li> <li>■ VMware vSphere</li> </ul>	增加或减少引导磁盘介质的大小。
调整磁盘大小	存储磁盘	<ul style="list-style-type: none"> <li>■ Amazon Web Services</li> <li>■ Google Cloud Platform</li> </ul>	增加存储磁盘的容量。
重新启动	计算机	<ul style="list-style-type: none"> <li>■ Microsoft Azure</li> </ul>	先关闭再重新启动正在运行的计算机。
恢复到快照	计算机	<ul style="list-style-type: none"> <li>■ Google Cloud Platform</li> <li>■ VMware vSphere</li> </ul>	<p>恢复到该计算机的上一个快照。</p> <p>要使用此操作，必须存在现有快照。</p>
运行 Puppet 任务	受管资源	<ul style="list-style-type: none"> <li>■ Puppet Enterprise</li> </ul>	<p>在部署中的计算机上运行所选任务。</p> <p>任务在 Puppet 实例中定义。您必须能够确定任务并提供输入参数。</p>
关机	计算机	<ul style="list-style-type: none"> <li>■ VMware vSphere</li> </ul>	关闭客户机操作系统并关闭计算机电源。要使用此操作，必须在计算机上安装 <b>VMware Tools</b> 。
挂起	计算机	<ul style="list-style-type: none"> <li>■ Microsoft Azure</li> <li>■ VMware vSphere</li> </ul>	暂停计算机，使其无法使用，并且不使用除所用存储之外的任何其他系统资源。
更新	部署	<ul style="list-style-type: none"> <li>■ Amazon Web Services</li> <li>■ Microsoft Azure</li> <li>■ VMware vSphere</li> </ul>	<p>根据输入参数更改部署。</p> <p>有关示例，请参见<a href="#">如何将已部署的计算机移动到另一个网络</a>。</p>
更新标记	计算机和磁盘	<ul style="list-style-type: none"> <li>■ Amazon Web Services</li> <li>■ Microsoft Azure</li> <li>■ VMware vSphere</li> </ul>	添加、修改或删除应用于单个资源的标记。